

A thick black L-shaped frame is positioned on the left and bottom edges of the slide, framing the central text.

FUNDAMENTOS DE LA CAPA DE APLICACIÓN

DNS y otros servicios

Índice

- Introducción al nivel de aplicación
- Servicios de red: Asignación Dinámica de Direcciones (DHCP)
- Servicios de red: Resolución de nombre de dominio (DNS)
 - *El protocolo DNS: Cuándo se utiliza y conceptos fundamentales*
 - *Práctica de DNS: Configurar DNS en un equipo Windows y utilizar NSLOOKUP*
 - *Práctica de DNS: Capturar y analizar peticiones y respuestas DNS con Wireshark*
- Servicios de red: Transferencia de archivos (FTP)
- Servicios de red: Páginas web (HTTP/HTTPS)
- Servicios de red: Correo (SMTP, POP3/IMAP4)
- Servicios de red: Streaming (RTSP)
- Servicios de red: Monitorización de red (SNMP)
- Servicios de red: Directorio (LDAP)

INTRODUCCIÓN AL NIVEL DE APLICACIÓN



Conceptos capa de aplicación

- La capa de aplicación es la última tanto en OSI como en TCP/IP.
- Su función es proporcionar al usuario servicios de cualquier tipo.
 - *Es decir, este nivel es el único que interactúa directamente con el usuario.*
- Servicios más comunes y estándares asociados:

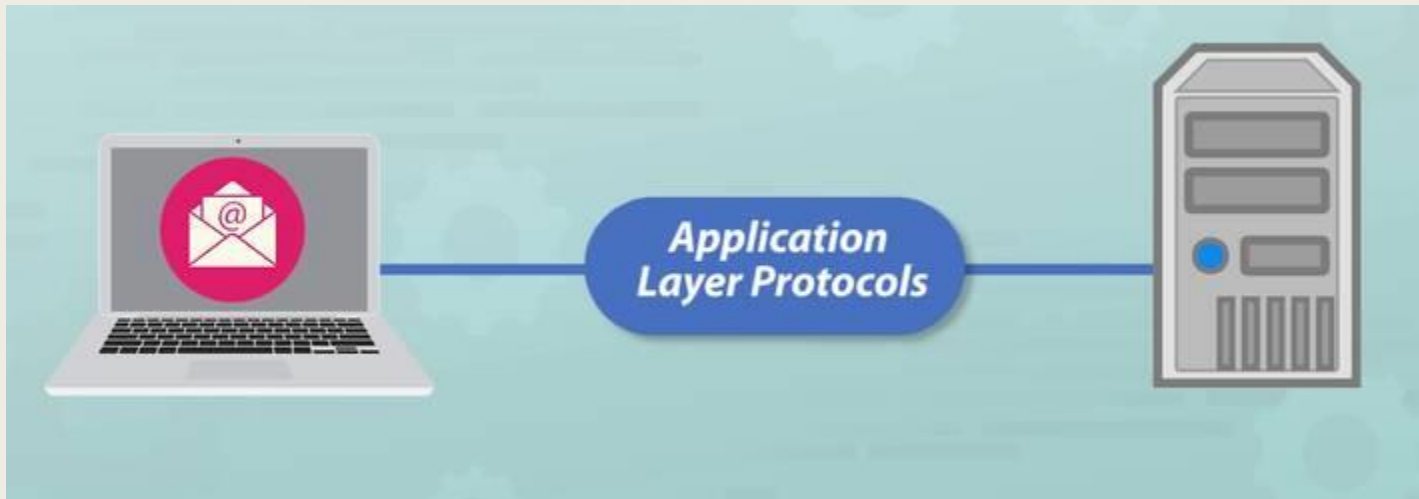


Servicio de red	Protocolos
Resolución de nombres de dominio	DNS
Configuración dinámica de host	APIPA, AVAHI, BOOTP, DHCP
Transferencia de ficheros	FTP, TFTP
Páginas web	HTTP, HTTPS
Correo	SMTP, POP3, IMAP4
Mensajería instantánea (Chat)	IRC, XMPP
Streaming de audio/vídeo	RTSP
Monitorización de redes	SNMP
Directorio	LDAP
Administración remota	Telnet, SSH, RDP

- Importante:
 - *Servicio es distinto de Protocolo.*
- Servicio: Funcionalidad que se ofrece al usuario.
- Protocolo: Implementación concreta para llevar a cabo dicha función del servicio.

¿Qué vamos a ver en esta sesión?

- En esta presentación se pretende tratar de modo básico los servicios principales de la capa de aplicación.
- Nos detendremos algo más en el servicio DNS para poder comprenderlo mejor.

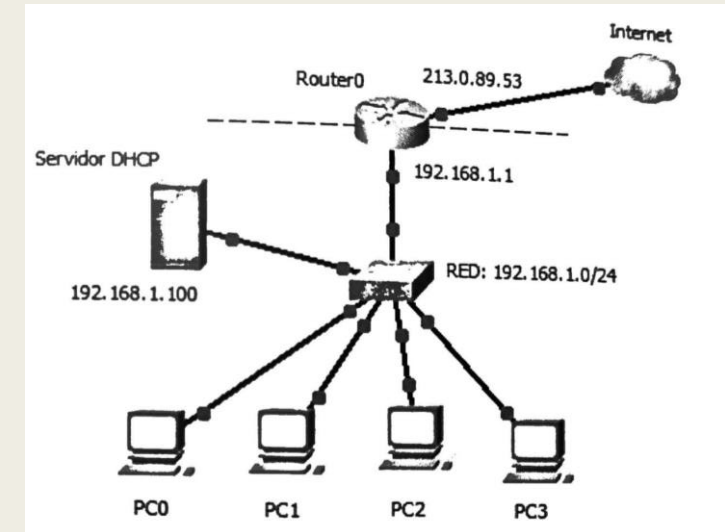


SERVICIOS DE RED: ASIGNACIÓN DINÁMICA DE DIRECCIONES (DHCP)



Servicio DHCP 1 / 2

- DHCP es un protocolo de capa de aplicación que ya hemos visto en clase.
- Su función principal es asignar los parámetros de la red de forma automática.
 - *Evitando que el administrador tenga que configurarlos manualmente en cada equipo.*
- Configuración de DHCP a nivel de aplicación en el siguiente escenario:
 1. *Selecciona en todos los PC la opción de recibir configuración IP por DHCP.*
 2. *Asigna dirección IP estática 192.168.1.100/24 al servidor DHCP.*
 3. *Asigna dirección IP estática 192.168.1.1/24 al puerto LAN del router, que será la puerta de enlace de los equipos.*



Servidor DHCP 2/2

4. Configura el servidor DHCP como aparece en la figura

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Number	TFTP Sever
serverPool	192.168.1.1	213.0.43.36	192.168.1.10	255.255.255.0	100	192.168.1.100

DNS lo veremos en la siguiente sección

TFTP puede ser él mismo u otro

Al terminar, pulsamos save

- Para comprobar que funciona, podemos hacer un ipconfig /all en algún PC

```
Command Prompt

Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection:(default port)
Physical Address.....: 0001.4242.BC21
Link-local IPv6 Address.....: FE80::201:42FF:FE42:BC21
IP Address.....: 192.168.1.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1
DNS Servers.....: 213.0.43.36
DHCP Servers.....: 192.168.1.100
```


EL PROTOCOLO DNS: CUÁNDO SE UTILIZA Y CONCEPTOS FUNDAMENTALES

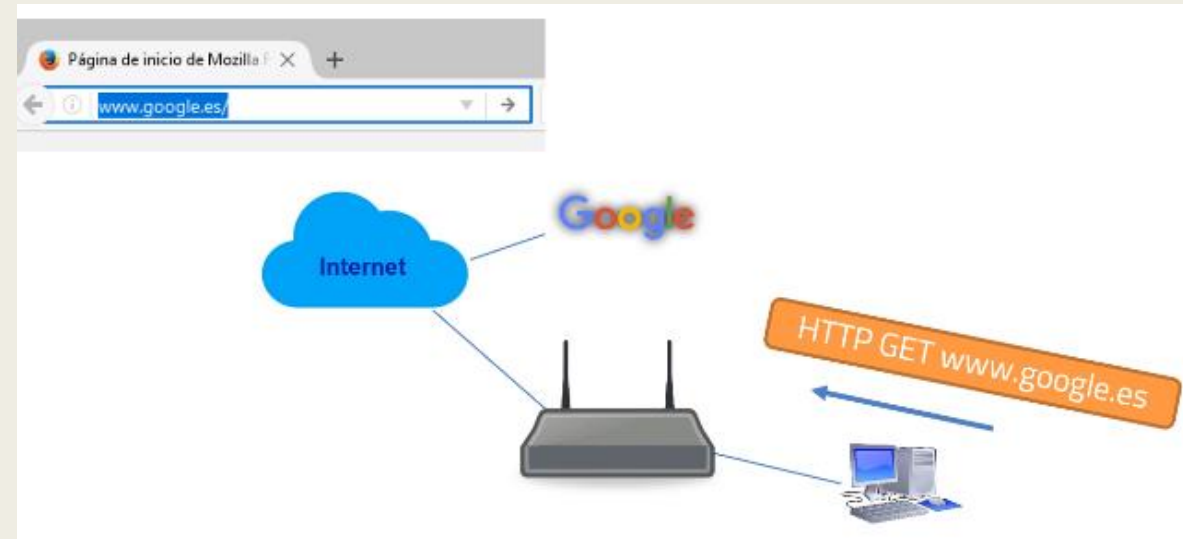


Introducción

- Con DNS sucede algo que no sucede con otros protocolos:
 - *Si pensamos en el switching y el routing, nos viene a la mente el técnico o ingeniero de redes.*
 - *Si pensamos en servidores de Windows o Linux, y servicios de bases de datos o de correo electrónico, nos viene a la mente el técnico o ingeniero de sistemas.*
 - *Con DNS no está claro quién lo gestiona.*
 - En algunas empresas se encarga el equipo de redes y el resto se desentiende.
 - En otras se encarga el de sistemas y el resto se desentiende.
- No entraremos en gran complejidad para explicar este servicio, pero vamos a formar una idea de base para que tengáis claro en qué casos se utiliza el DNS y cómo funciona.

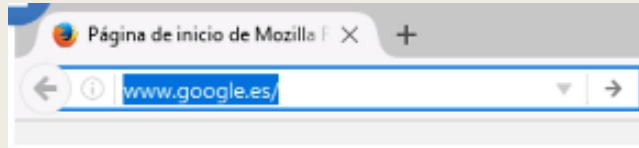
DNS - DOMAIN NAME SYSTEM

- La traducción de DNS al español es Sistema de Nombres de Dominio.
- Supongamos el siguiente escenario:
- Desde un equipo, abrimos el navegador y buscamos www.google.es
- A nivel de aplicación, se lanza una petición HTTP GET www.google.es
- Y esto irá añadiendo cabeceras por cada capa del modelo TCP/IP.
- Detengámonos en la capa 3. Aquí necesitamos una dirección IP destino y una dirección IP origen.
 - ¿Qué ponemos en la IP destino?
 - No sabemos qué IP corresponde a *Google.es*

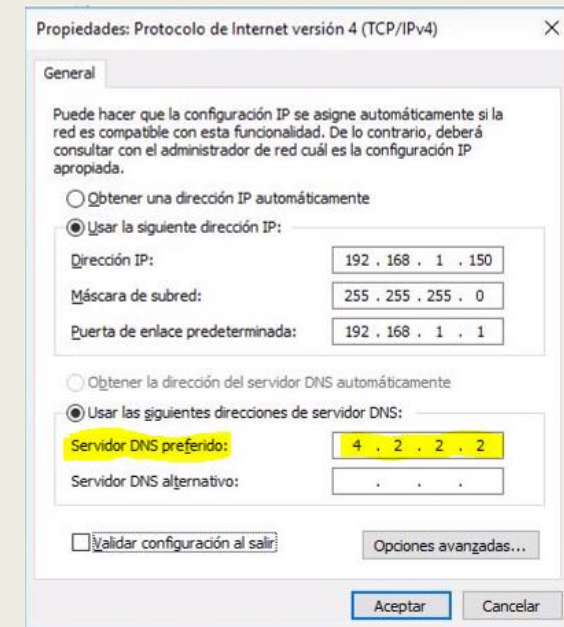


La solución a este problema nos la va a dar un servidor DNS, que contiene una BBDD que relaciona Nombres con IPs

¿Cómo funciona DNS?



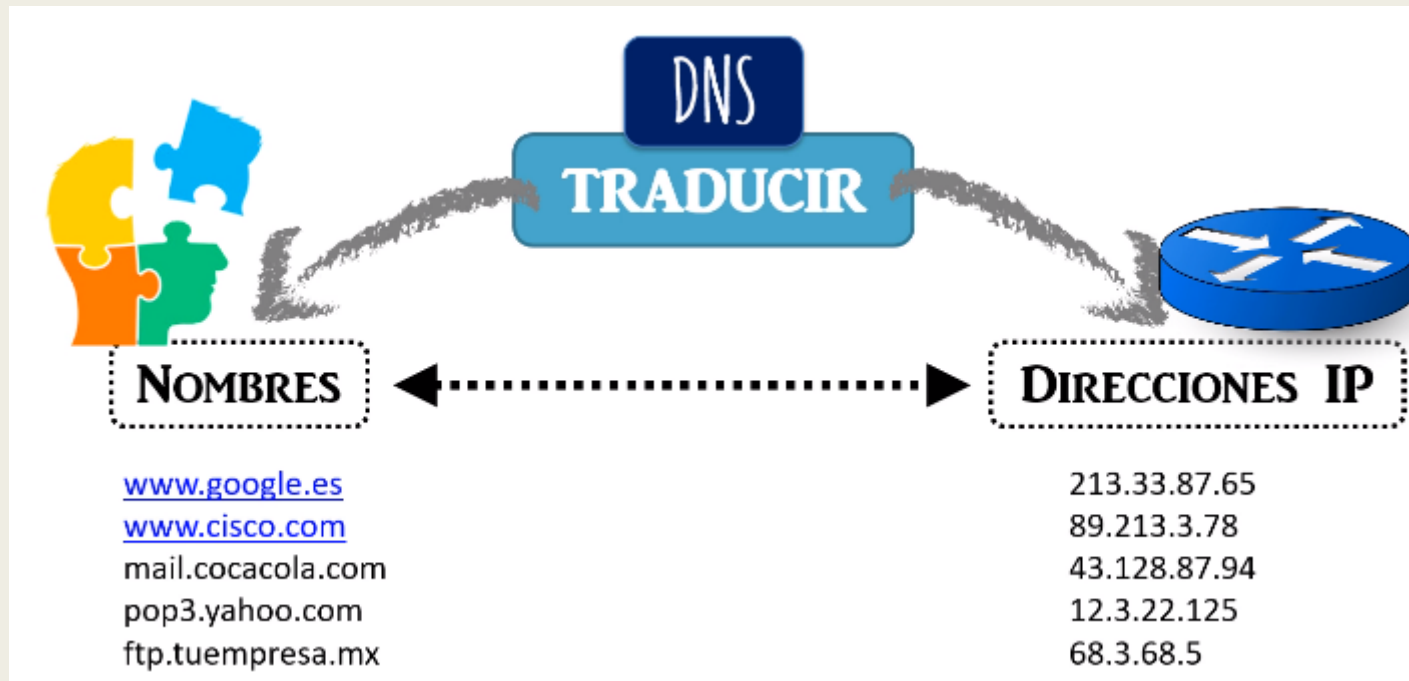
1. Al introducir www.google.es en el navegador, se produce una petición DNS.
 - *La petición se hace contra un servidor DNS (ejemplo 4.2.2.2)*
2. El servidor DNS busca en su BBDD el nombre www.google.es
 - *Y responde con la IP que tiene asociada*



3. El PC inicia el 3-way-handshake y posteriormente genera la petición HTTP GET a la dirección IP de Google

Resumen para aclararlo mejor

- A modo de resumen: DNS se encarga de traducir nombres por direcciones IP.
 - *También puede hacer el proceso inverso, pero es poco habitual.*



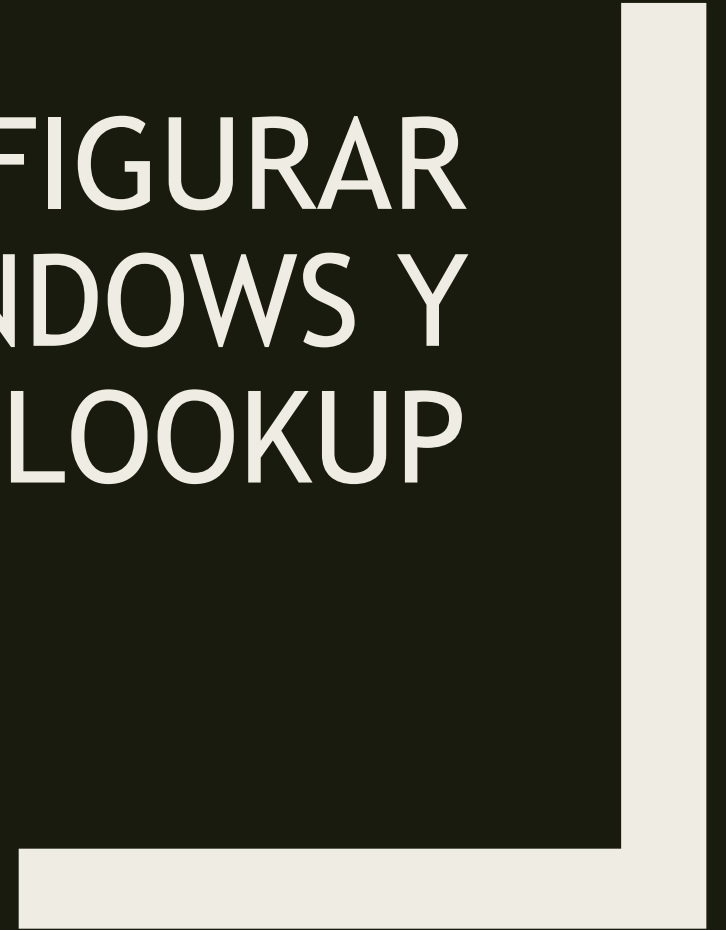
Pregunta

- DNS pertenece al nivel de aplicación.
 - *Es decir, trabajará sobre todas las capas inferiores.*
- A nivel de la capa de transporte:
 - ***¿Pensáis que DNS trabaja con TCP o con UDP?***
- Recordatorio:
- TCP → Confiable y Orientado a conexión
- UDP → No Confiable y No Orientado a conexión

Respuesta

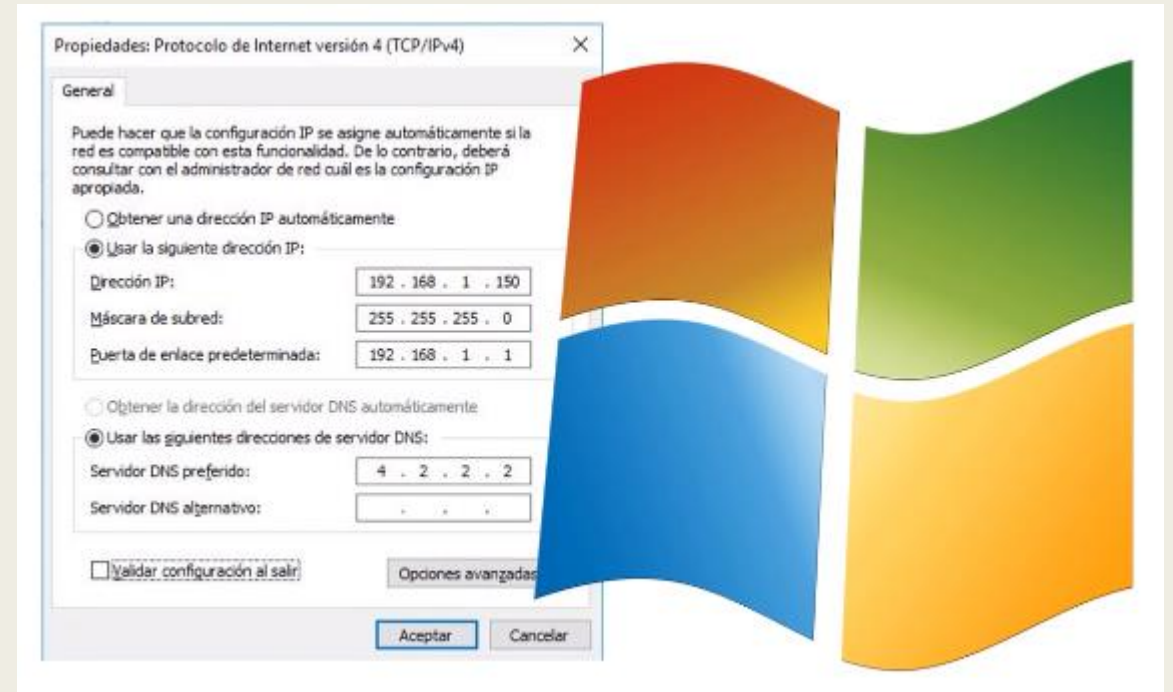
- DNS funcionará normalmente sobre UDP
- ¿Por qué?
 - *Porque es una petición sencilla de poco tamaño.*
 - *La comunicación se resume en dos datagramas, una petición y una respuesta.*
 - *No tiene mucho sentido utilizar el 3-way-handshake antes de lanzar la petición.*
 - Y más teniendo en cuenta que la cabecera TCP es considerablemente más grande por los números de SEQ y ACK
 - Y teniendo en cuenta que después de la comunicación habría que finalizar la conexión.
 - Es generar mucho tráfico para algo muy pequeño, y aunque no se garantice la entrega del mensaje, y no llegara, se vuelve a hacer otra petición. No es crítico.
- DNS correría por TCP solo en los casos en los que la respuesta sea compleja y hubiera que partirla en varios trozos (muy poco habitual).

PRÁCTICA DE DNS: CONFIGURAR DNS EN UN EQUIPO WINDOWS Y UTILIZAR NSLOOKUP



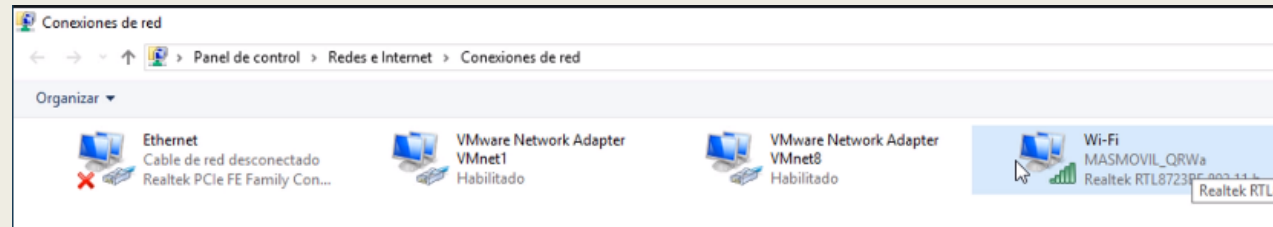
Introducción

- Ahora que ya tenemos una idea de cómo funciona DNS, vamos a ver cómo configurarlo en un equipo.
 - *Lo vamos a ver en Windows 10*



Paso 1 - Acceder a las conexiones de red

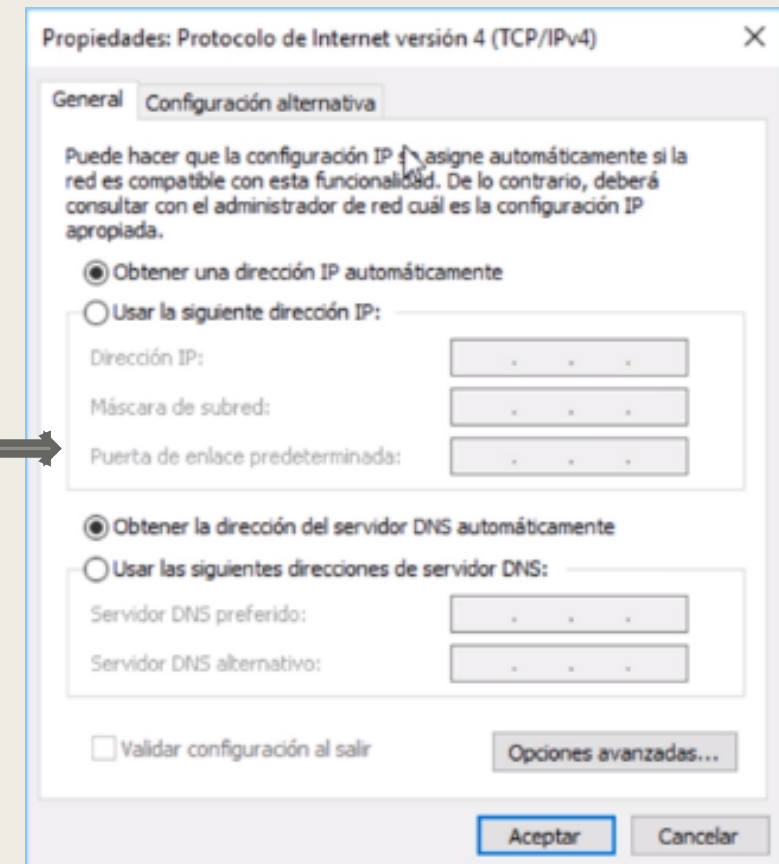
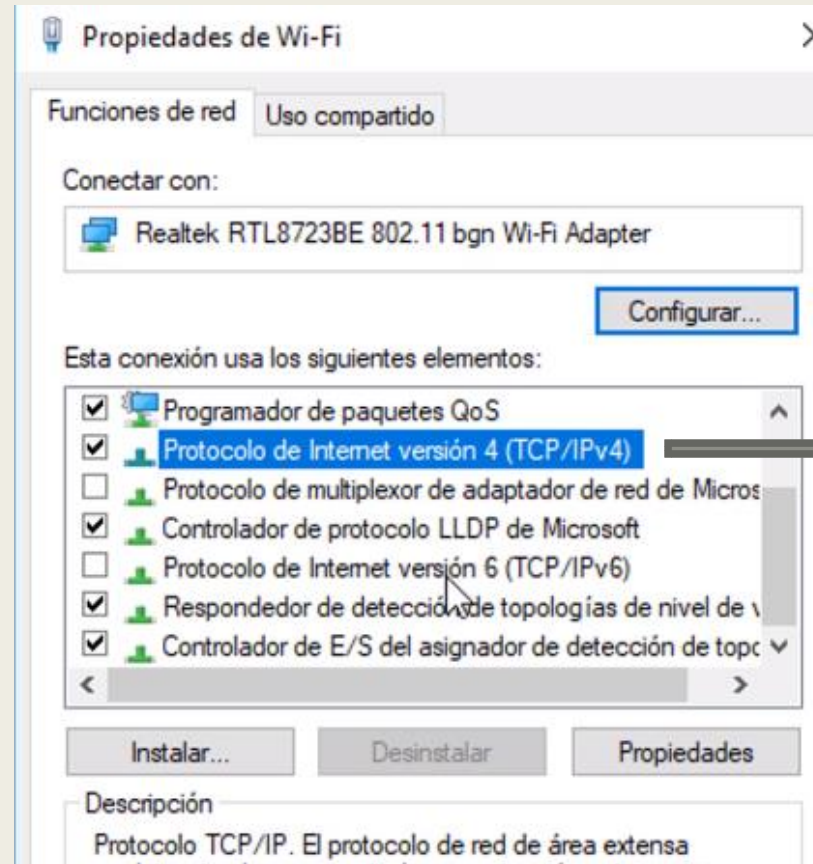
- El primer paso para poder realizar la configuración es acceder a las “Conexiones de red”



- Según si estáis conectados por Wi-Fi o Ethernet, seleccionaréis la opción adecuada.
 - *Clic derecho → Propiedades*

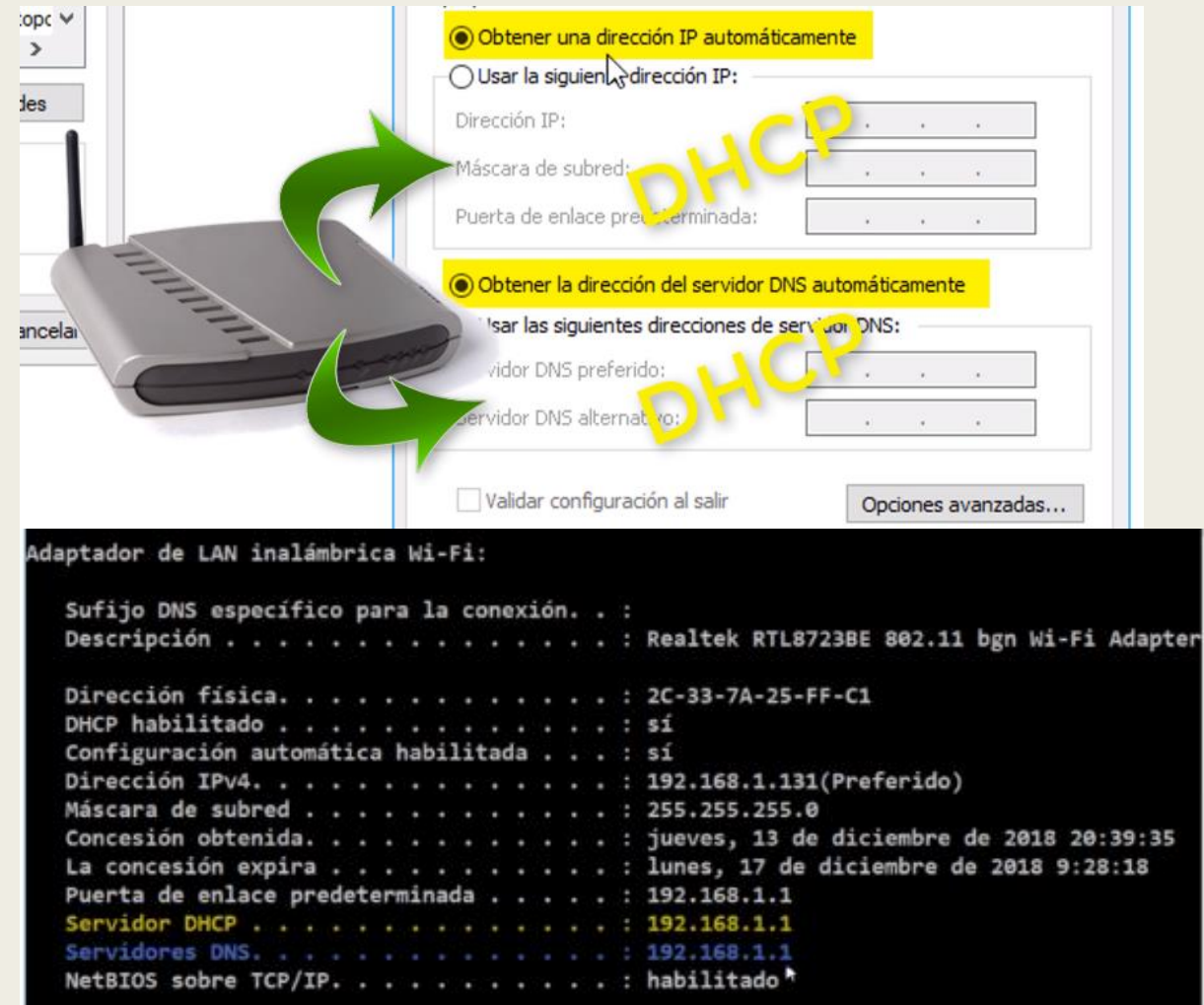
Paso 2 - Acceder a la configuración de DNS

- Al abrir las propiedades, nos aparecerá una serie de elementos en una lista.
- Elegiremos el Protocolo de Internet versión 4 (TCP/IPv4)
 - *Doble clic*
 - *O clic en propiedades*



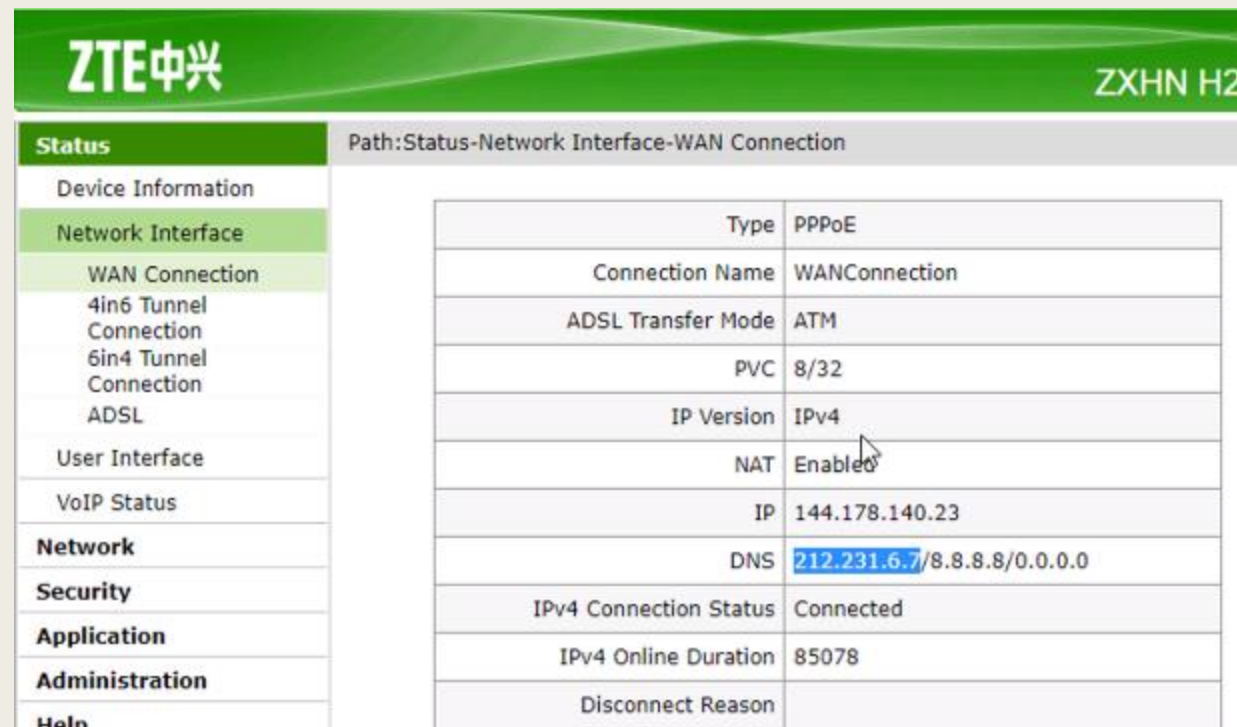
Paso 3 - Configurar el DNS automático

- En la configuración del DNS vemos que tanto la IP como el DNS se asignan automáticamente.
- Esta asignación automática nos la proporcionaría el router mediante DHCP.
- Si consultamos con `ipconfig /all` nuestra configuración de red, es posible que el servidor DHCP y el servidor DNS tengan el mismo valor.
 - *Es decir, en este caso lo que ocurre es que todas las peticiones DNS no se enviarán a un servidor DNS, sino que se enviarán al router, y él hará de intermediario.*
 - *Y él reenviará la información a un DNS*



Mini inciso - Qué DNS asigna nuestro router

- Si accedemos a la configuración del router para consultar qué DNS tenemos asignado, para este caso concreto, se están asignando los siguientes:
- 212.231.6.7 (principal en este router)
 - *DNS compartido por varias compañías de ISP*
- 8.8.8.8 (DNS de Google)
- 0.0.0.0 ← Este no existe, es simplemente que el router podía asignar 3 y solo ha asignado 2.



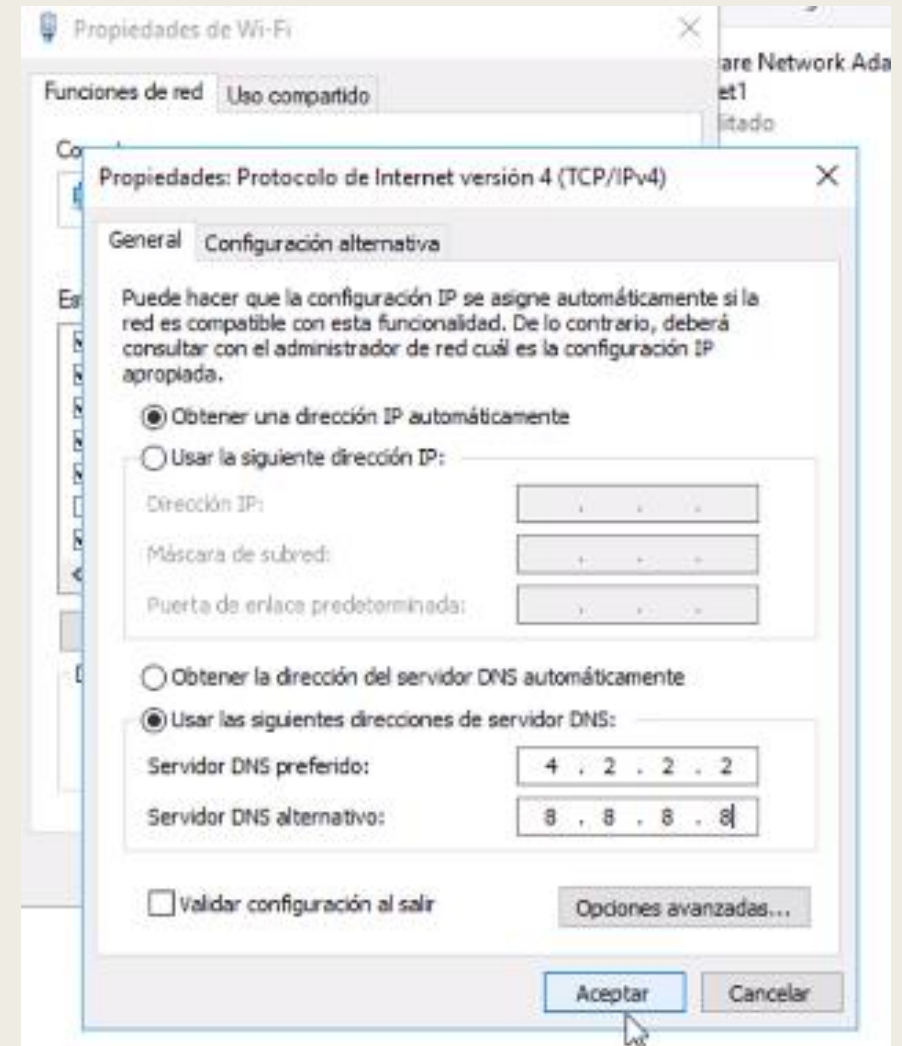
The screenshot shows the ZTE 中兴 ZXHN H2 router's status page. The left sidebar contains a menu with items like Device Information, Network Interface, WAN Connection, 4in6 Tunnel Connection, 6in4 Tunnel Connection, ADSL, User Interface, VoIP Status, Network, Security, Application, Administration, and Help. The main content area is titled 'Path: Status-Network Interface-WAN Connection' and displays a table of connection parameters.

Type	PPPoE
Connection Name	WANConnection
ADSL Transfer Mode	ATM
PVC	8/32
IP Version	IPv4
NAT	Enabled
IP	144.178.140.23
DNS	212.231.6.7/8.8.8.8/0.0.0.0
IPv4 Connection Status	Connected
IPv4 Online Duration	85078
Disconnect Reason	

Paso 3 - Configurar el DNS manual

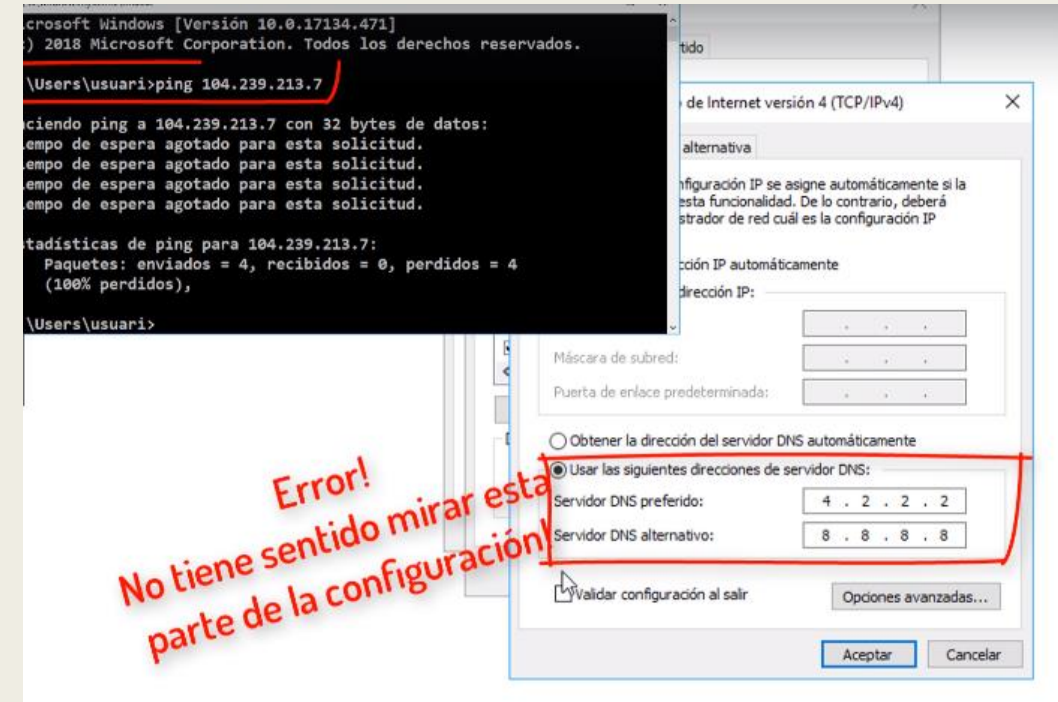
- Si queremos asignar un DNS específico, podemos hacerlo manualmente en lugar de tener la opción marcada de DNS automático.
- De esta forma, la petición DNS se hará directamente al servidor 4.2.2.2, en lugar de hacérsela al router y que él se encargue. Y si falla, al 8.8.8.8.
 - *Obviamente pasará por el router, pero el destino ya no es el router, así que el router lo único que hará es el forwarding de capa 3, y NO capas superiores.*

```
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv4. . . . . : 192.168.1.131(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : jueves, 13 de diciembre de 2018 20:39:34
La concesión expira . . . . . : lunes, 17 de diciembre de 2018 9:51:26
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS. . . . . : 4.2.2.2
                        8.8.8.8
NetBIOS sobre TCP/IP. . . . . : habilitado
```



Mini inciso: Consejo antiN00b

- Puede darse el caso que en vuestro equipo de redes estéis probando la conectividad a nivel IP de un PC.
 - *Es decir, hacer un ping de un equipo a otro (ICMP, capa 3).*
- Y a la hora de revisar la configuración, en vuestro equipo no solo se fijan en configuración IP, sino que también se fijan en el servidor DNS y hacen cambios en él.
 - *Cuando estamos simplemente haciendo simplemente un ping a una IP.*
- ESO ES UN FALLO GORDO, significa que no tenemos claro para qué sirve el DNS



Si ya sabemos la IP, no tenemos que traducir nada.

NSLOOKUP

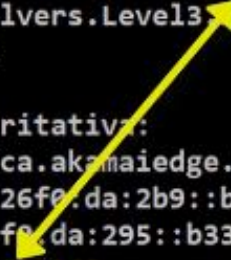
- Ahora que ya sabemos cómo configurar un DNS en un equipo, vamos a ver la herramienta nslookup.
- Esta herramienta nos permite conocer la IP asociada a algún nombre de dominio.
- En el campo Address viene nuestro servidor DNS, esto NO es la IP del dominio.
- Respuesta no autoritativa significa que nuestro DNS no tenía directamente la respuesta, sino que ha pasado por otros previamente.
- Los alias son otros nombres del dominio asociados a la misma/s IPs.
- Puede darnos IPv6 también.

```
C:\Users\usuari>nslookup www.asdf.com
Servidor:  b.resolvers.Level3.net
Address:  4.2.2.2

Respuesta no autoritativa:
Nombre:  www.asdf.com
Address:  64.90.40.65
```

```
C:\Users\usuari>nslookup www.cisco.com
Servidor:  b.resolvers.Level3.net
Address:  4.2.2.2

Respuesta no autoritativa:
Nombre:  e2867.dsca.akamaiedge.net
Addresses:  2a02:26f0:da:2b9::b33
            2a02:26f0:da:295::b33
            23.198.68.160
Alias:  www.cisco.com
        www.cisco.com.akadns.net
        wwwds.cisco.com.edgekey.net
        wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```



Pregunta

- Si ponemos en el navegador la IP que nos da el NSLOOKUP, ¿funcionará?

```
C:\Users\usuari>nslookup www.asdf.com
Servidor:  b.resolvers.Level3.net
Address:  4.2.2.2

Respuesta no autoritativa:
Nombre:  www.asdf.com
Address:  64.90.40.65
```

Respuesta

- Puede que sí, puede que no.
- Es diferente lanzar una petición GET a una IP que a un dominio.
- ¿Por qué?
 - *Porque el servidor Web está preparado para trabajar con rutas, y es posible que no tenga configurado cómo resolver las rutas con la IP directamente.*



Nombre: www.asdf.com
Address: 64.90.40.65



Site Not Found

Well, this is awkward. The site you're looking for is not here.

Is this your site? [Get more info](#) or [contact support](#).

 DreamHost

Nombre: www.google.com
Addresses: 2a00:1450:4003:809::2004
216.58.211.36

Google

🔍 | 

Buscar con Google

Voy a tener suerte

Ofrecido por Google en: [English](#) [català](#) [galego](#) [euskara](#)

¿Por qué NSLOOKUP? ¿Hay alguna forma más?

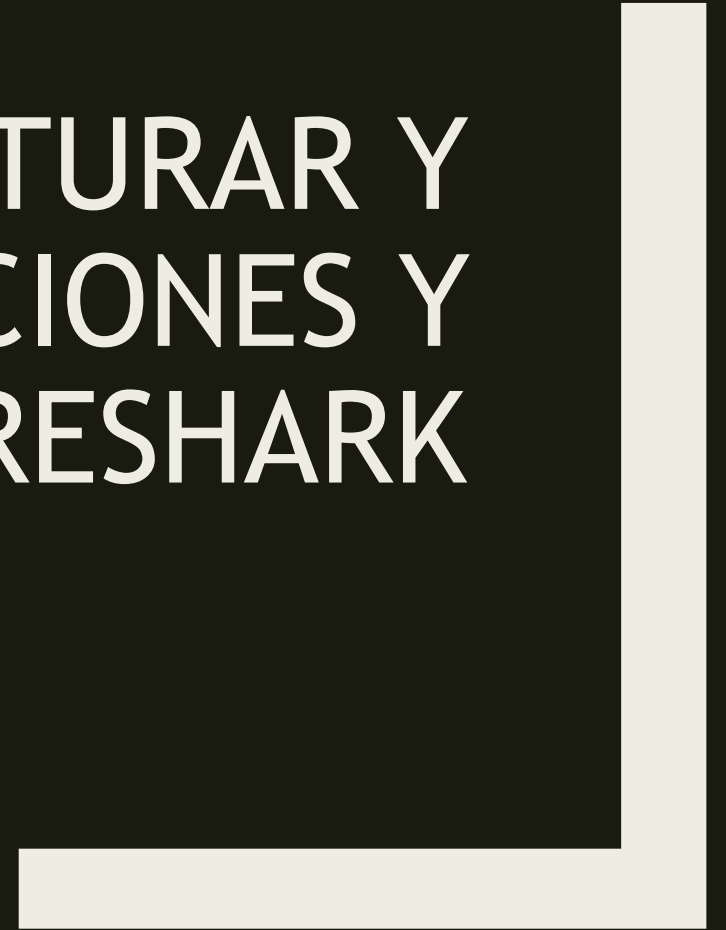
- La herramienta nslookup es la más profesional para determinar en el día a día cuál es la IP de algún dominio.
- Sin embargo, también es posible conocer la IP de un dominio haciéndole directamente un ping:

```
C:\Users\chema>ping www.google.es
```

```
Haciendo ping a www.google.es [216.58.215.131] con 32 bytes de datos:
```

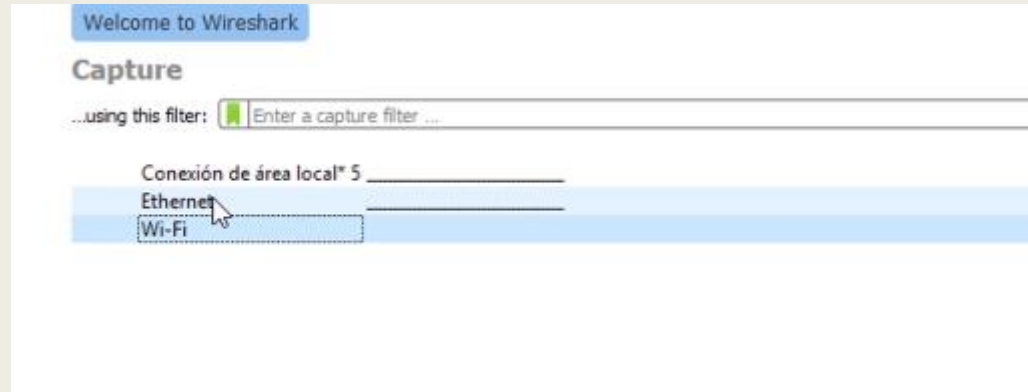
- *Esta opción también es válida, especialmente si queremos no solo conocer el dominio, sino probar la conectividad con él.*

PRÁCTICA DE DNS: CAPTURAR Y ANALIZAR PETICIONES Y RESPUESTAS DNS CON WIRESHARK



Introducción

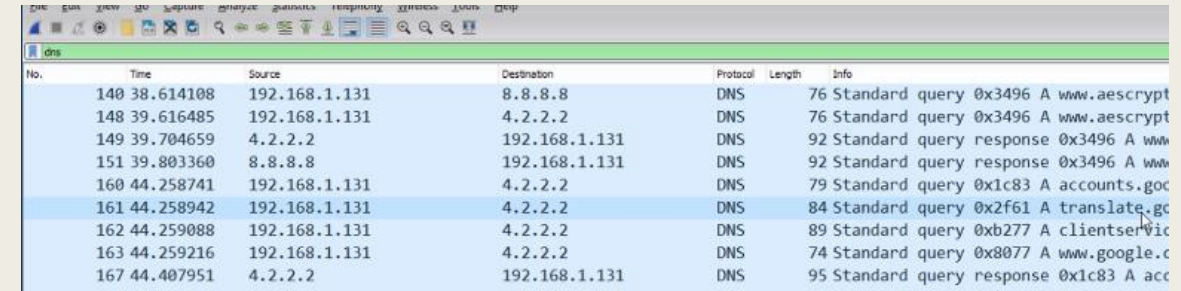
- Ahora lo que vamos a hacer en Wireshark es analizar cómo aparece esa petición y esa respuesta DNS



- Elegimos la interfaz y empezamos a capturar tráfico.

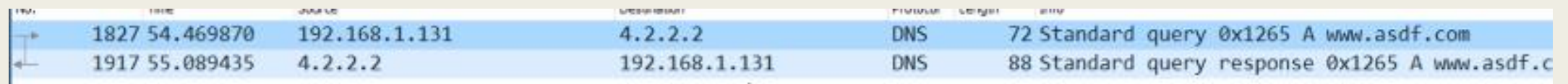
Capturar el tráfico

- Abrimos en el navegador una web:
 - Por ejemplo: www.asdf.com
- Cuando termine de cargar la página, detenemos la captura de tráfico en Wireshark.
- Y para poder analizar qué tráfico corresponde al dns, escribimos el siguiente filtro de visualización:
 - *dns*
- Podríamos aplicar algún filtro más específico, pero a simple vista seremos capaces de encontrarlo.
- Cuando lo encontremos, aplicamos un filtro solo para esa conexión UDP:
 - *Clic derecho → conversion filter → UDP*



A screenshot of the Wireshark network protocol analyzer interface. The 'dns' filter is applied to the packet list. The table shows several DNS packets, including queries and responses for various domains like www.aescript.com and accounts.google.com.

No.	Time	Source	Destination	Protocol	Length	Info
140	38.614108	192.168.1.131	8.8.8.8	DNS	76	Standard query 0x3496 A www.aescript
148	39.616485	192.168.1.131	4.2.2.2	DNS	76	Standard query 0x3496 A www.aescript
149	39.704659	4.2.2.2	192.168.1.131	DNS	92	Standard query response 0x3496 A www
151	39.803360	8.8.8.8	192.168.1.131	DNS	92	Standard query response 0x3496 A www
160	44.258741	192.168.1.131	4.2.2.2	DNS	79	Standard query 0x1c83 A accounts.goc
161	44.258942	192.168.1.131	4.2.2.2	DNS	84	Standard query 0x2f61 A translate.gc
162	44.259088	192.168.1.131	4.2.2.2	DNS	89	Standard query 0xb277 A clientservic
163	44.259216	192.168.1.131	4.2.2.2	DNS	74	Standard query 0x8077 A www.google.c
167	44.407951	4.2.2.2	192.168.1.131	DNS	95	Standard query response 0x1c83 A acc



A screenshot of the Wireshark network protocol analyzer interface showing a specific DNS query and response. The packet list shows two packets: a query from 192.168.1.131 to 4.2.2.2 for www.asdf.com, and a response from 4.2.2.2 to 192.168.1.131.

No.	Time	Source	Destination	Protocol	Length	Info
1827	54.469870	192.168.1.131	4.2.2.2	DNS	72	Standard query 0x1265 A www.asdf.com
1917	55.089435	4.2.2.2	192.168.1.131	DNS	88	Standard query response 0x1265 A www.asdf.c

Analizar el tráfico - Petición DNS

Time	Source	Destination	Protocol	Length	Info
1827.54.469870	192.168.1.131	4.2.2.2	DNS	72	Standard query 0x1265 A www.asdf.com

- Si analizamos los datos de la petición DNS...
 - *La parte correspondiente a Domain Name System (query)*

- Veremos lo siguiente

```
▼ Domain Name System (query)
  Transaction ID: 0x1265
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ www.asdf.com: type A, class IN
      Name: www.asdf.com
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 1917]
```

- Si analizamos los datos de la petición DNS...
 - *La parte correspondiente a Domain Name System (query)*
- Nos centraremos en Queries, que es donde está la consulta:
 - *En la consulta veremos el nombre a resolver.*
 - *Y como type veremos A → Esto se refiere a IPv4*
 - IPv6 sería AAAA (hay muchos tipos, no entramos en detalle)
 - *No entraremos en mucho detalle con Class: IN = internet*
- La consulta indica que tenemos un nombre y esperamos como respuesta una IPv4

Analizar el tráfico - Respuesta DNS

1917 55.089435 4.2.2.2 192.168.1.131 DNS 88 Standard query response 0x1265 A www.as

- Lo que vemos en la respuesta es que tenemos:

- *La query que se nos hizo en la petición DNS.*
- *La respuesta.*

- En la respuesta nos indican:

- *La información solicitada (name, type A).*
- *La dirección IP que tiene asociada.*

```
Domain Name System (response)
  Transaction ID: 0x1265
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.asdf.com: type A, class IN
      Name: www.asdf.com
      [Name Length: 12]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  > Answers
    > www.asdf.com: type A, class IN, addr 64.90.40.65
      Name: www.asdf.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 13188
      Data length: 4
      Address: 64.90.40.65
      [Request In: 1827]
```

Capa 3

Dirección IP
DESTINO

Dirección IP
ORIGEN

HTTP GET www.asdf.com

Es decir, tendremos que enviar ese get HTTP al servidor en IP 64.90.40.65

Analizar el tráfico - Inicio del 3-way-handshake y tráfico HTTP

- Vamos a ver cómo continúa la captura de tráfico a partir de esa petición DNS, para comprobar que efectivamente el HTTP GET se hace a 64.90.40.65
- Dejamos seleccionado el paquete DNS, y borramos el filtro de visualización.
- A partir de ahí, buscamos la comunicación que nos interesa (entre todo el tráfico)

1947	55.267033	192.168.1.131	64.90.40.65	TCP	66 57836 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
------	-----------	---------------	-------------	-----	---

- Si filtramos por ahí: clic derecho → conversation filter → IPv4

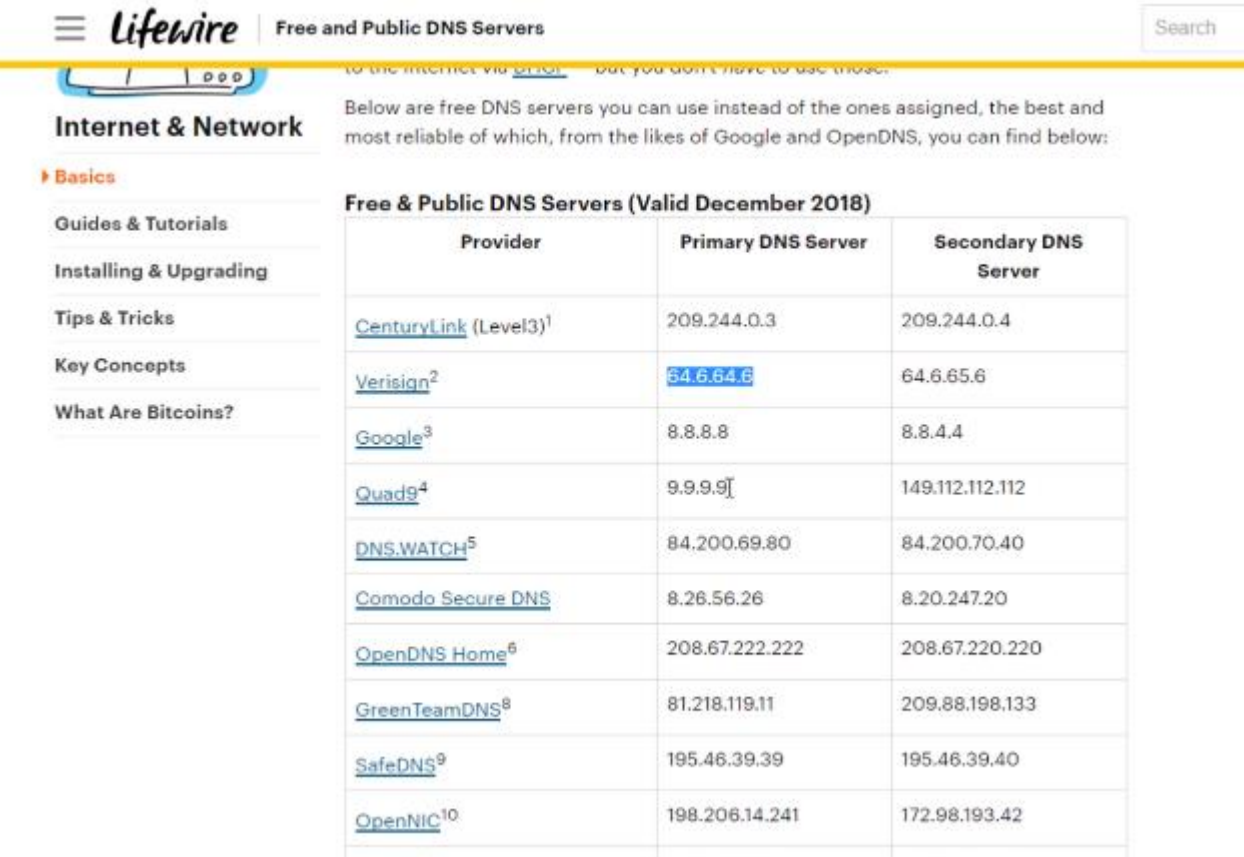
- Vemos que se produce el 3-way-handshake (en este caso triple por la configuración del servidor).

- Y posteriormente el HTTP con el envío de la web.

1947	55.267033	192.168.1.131	64.90.40.65	TCP	66 57836 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
1948	55.267179	192.168.1.131	64.90.40.65	TCP	66 57837 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
1979	55.472571	192.168.1.131	64.90.40.65	TCP	66 57838 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
2012	55.637570	64.90.40.65	192.168.1.131	TCP	66 80 → 57836 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2013	55.637571	64.90.40.65	192.168.1.131	TCP	66 80 → 57836 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2014	55.637640	192.168.1.131	64.90.40.65	TCP	54 57836 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
2015	55.637685	192.168.1.131	64.90.40.65	TCP	54 57837 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
2017	55.638484	192.168.1.131	64.90.40.65	HTTP	438 GET / HTTP/1.1
2042	55.793315	64.90.40.65	192.168.1.131	TCP	66 80 → 57838 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
2043	55.793383	192.168.1.131	64.90.40.65	TCP	54 57838 → 80 [ACK] Seq=1 Ack=1 Win=17408 Len=0
2068	55.985642	64.90.40.65	192.168.1.131	TCP	54 80 → 57837 [ACK] Seq=1 Ack=385 Win=30720 Len=0
2070	55.993089	64.90.40.65	192.168.1.131	HTTP	1053 HTTP/1.1 200 OK (text/html)
2075	56.033786	192.168.1.131	64.90.40.65	TCP	54 57837 → 80 [ACK] Seq=385 Ack=1000 Win=16384 Len=0
2164	57.387292	192.168.1.131	64.90.40.65	HTTP	403 GET /89asdf.gif HTTP/1.1
2175	57.627959	64.90.40.65	192.168.1.131	TCP	1502 80 → 57837 [ACK] Seq=1000 Ack=734 Win=31744 Len=0
2176	57.639976	64.90.40.65	192.168.1.131	TCP	1502 80 → 57837 [ACK] Seq=2448 Ack=734 Win=31744 Len=0

Extra: Servidores DNS públicos

- Puede que nos interese asignar manualmente un DNS a nuestro equipo.
- Una web para consultarlos es la [siguiente](#).
- Para casos de privacidad puede interesarnos elegir un DNS diferente al de la compañía telefónica.
 - *Si tenemos el del ISP, ellos tendrán un registro de tus peticiones y actividad.*
- También, según qué casos, habrá DNS que nos den una respuesta más rápida que otros.



The screenshot shows the Lifewire website with the title "Free and Public DNS Servers". It includes a sidebar with navigation links like "Internet & Network", "Basics", "Guides & Tutorials", "Installing & Upgrading", "Tips & Tricks", "Key Concepts", and "What Are Bitcoins?". The main content area lists various DNS providers with their primary and secondary IP addresses.

Provider	Primary DNS Server	Secondary DNS Server
CenturyLink (Level3) ¹	209.244.0.3	209.244.0.4
Verisign ²	64.6.64.6	64.6.65.6
Google ³	8.8.8.8	8.8.4.4
Quad9 ⁴	9.9.9.9	149.112.112.112
DNS.WATCH ⁵	84.200.69.80	84.200.70.40
Comodo Secure DNS	8.26.56.26	8.20.247.20
OpenDNS Home ⁶	208.67.222.222	208.67.220.220
GreenTeamDNS ⁸	81.218.119.11	209.88.198.133
SafeDNS ⁹	195.46.39.39	195.46.39.40
OpenNIC ¹⁰	198.206.14.241	172.98.193.42

DNS tiene mucho más

- Con esta sesión hemos visto a nivel básico cómo funciona DNS.
- Sin embargo, DNS tiene mucho más material:
 - *Cómo se guarda la información a nivel de servidores.*
 - *Cómo se comunican entre ellos los servidores DNS.*
 - *Que la información en realidad es jerárquica.*
 - *También son jerárquicos los dominios.*
- Es contenido para >10 horas y con la introducción que hemos hecho tenemos la información fundamental que todo técnico o persona que trabaje con las TIC debe conocer.



SERVICIOS DE RED: TRANSFERENCIA DE ARCHIVOS (FTP)

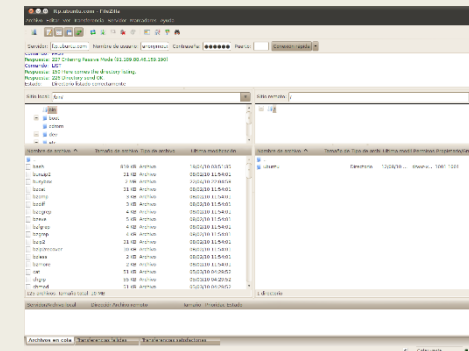


FTP. File Protocol Transfer

- FTP es un protocolo multiplataforma que sirve para transferir grandes bloques de datos por la red.
- La mayoría de páginas web se suben al servidor mediante FTP.
- Por defecto utiliza los puertos 20 y 21.
- Si se interrumpe la sesión puede generarse algún error, lo cual puede ser problemático si se hacen transferencias muy grandes.

```
PS C:\Users\JM> ftp ftp.rediris.es
Conectado a ftp.rediris.es.
220- Bienvenido al servicio de replicas de RedIRIS.
220- Welcome to the RedIRIS mirror service.
220 Only anonymous FTP is allowed here
200 OK, UTF-8 enabled
Usuario (ftp.rediris.es:(none)):
230- RedIRIS - Red Académica y de Investigación Española
230- RedIRIS - Spanish National Research Network
230-
230- ftp://ftp.rediris.es -- http://ftp.rediris.es
230 Anonymous user logged in
ftp>
```

Los sistemas operativos con soporte TCP/IP suelen conservar una versión primitiva del cliente FTP en línea de comandos.



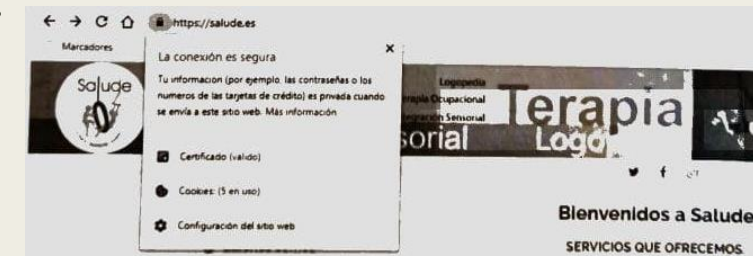
También existen muchos programas que permiten realizar FTP desde un entorno gráfico amigable, como FileZilla

SERVICIOS DE RED: PÁGINAS WEB (HTTP/HTTPS)



Páginas web. HTTP/HTTPS

- HTTP (Hyper Text Transfer Protocol) está diseñado para transferir páginas web desde un servidor a un cliente.
 - *De Lenguajes de Marcas sabemos que una página web está formada por varios tipos de archivos, principalmente un HTML con contenido diverso, como imágenes, vídeos, etc. También CSS, Javascript, etc.*
- El servidor web se mantiene a la espera de peticiones http, realizadas por un cliente (normalmente el navegador).
 - *Después de hacer la petición al servidor web, si el recurso existe, el servidor responde enviando los archivos.*
- El cliente es el que se encarga de interpretar los archivos web con su navegador.
- El protocolo que proporciona un servicio web seguro es HTTPS, para lo cual realiza un cifrado de todos los datos que intercambian cliente y servidor.
- En la página web aparece el protocolo usado y un candado.
 - *Al pulsar el candado vemos la información de cifrado.*



SERVICIOS DE RED: CORREO (SMTP, POP3/IMAP4)

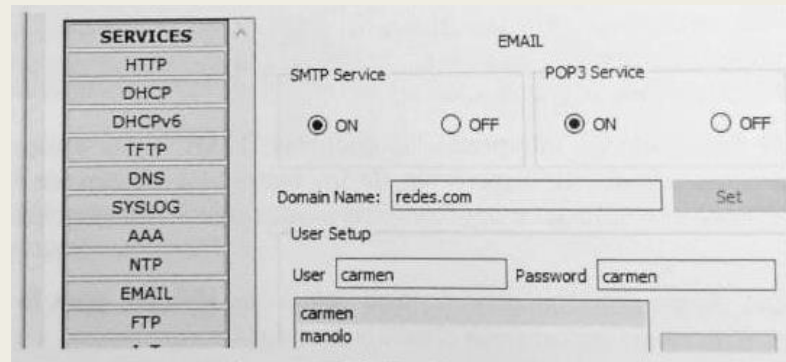


Correo. SMTP, y POP3/IMAP4

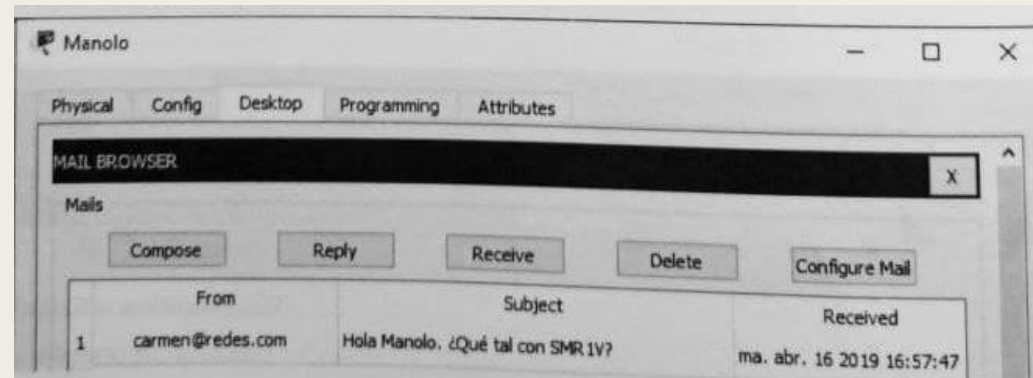
- SMTP es un protocolo para enviar mensajes desde un usuario a su servidor de correo y para el envío entre servidores.
 - *Orientado a conexión.*
 - *Se intercambian secuencias de comandos y datos.*
- POP3 e IMAP4 son protocolos para recibir correo por parte de un usuario final.
 - *Con **POP3** un cliente de correo realiza una solicitud, y si hay un correo pendiente el servidor se lo envía. Después el servidor borra todos los mensajes de modo que solo están disponibles de forma local.*
 - *Con **IMAP4** el correo no se descarga automáticamente en el equipo del cliente (solo las cabeceras), sino que espera a que el usuario haga clic en él para descargarse el cuerpo del correo. Esto permite, por ejemplo, eliminar un mensaje en el servidor sin haberlo descargado.*

Configurar un servidor de correo

- Podemos configurar un servidor de correo fácilmente en Packet Tracer.



- Una vez configurado, tenemos que configurar la cuenta de correo en cada cliente:



SERVICIOS DE RED: STREAMING (RTSP)



Streaming. RTSP

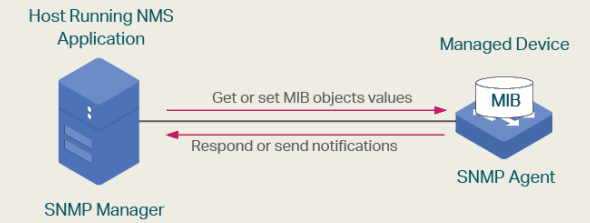


- RTSP es un protocolo no orientado a conexión.
 - *El servidor mantiene la sesión asociada a un identificador.*
- En la mayoría de casos utiliza:
 - *Audio y vídeo → UTP*
 - *Datos de control → Puerto 554 de TCP*
- En una misma sesión de RTSP puede haber varias conexiones del cliente hacia el servidor (ya sabemos de NAT y PAT que no tiene por qué solo haber 1 conexión por cliente) y viceversa.
- RTSP es similar a HTTP en sintaxis y en forma de operar:
 - *Pero RTSP necesita mantener el estado de la conexión.*
 - *En RTSP tanto cliente como servidor pueden lanzar peticiones.*

SERVICIOS DE RED: MONITORIZACIÓN DE RED (SNMP)



Monitorización de red. SNMP.

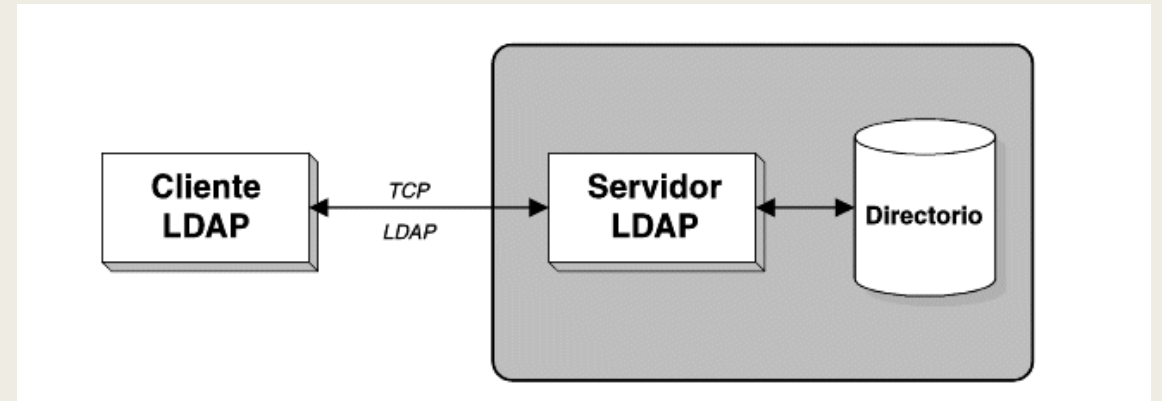


- SNMP son las siglas de Protocolo Simple de Administración de Red (Simple Network Management Protocol).
- Se trata de un protocolo que facilita el intercambio de información de administración entre dispositivos de red.
 - *De esta forma, los administradores de redes pueden supervisar el funcionamiento de esta, y buscar y resolver problemas.*
- Equipos que soportan SNMP: Routers, Switches, Servidores, estaciones de trabajo, etc.
- Uso típico de SNMP:
 - *Uno o más equipos administrativos, llamados GERENTES, supervisan un grupo de hosts.*
 - *En cada sistema gestionado se ejecuta en todo momento un componente de software llamado AGENTE, que reporta la información a través de SNMP al gerente.*
 - *La información recopilada se almacena en Bases de Información de Gestión (MIB)*

SERVICIOS DE RED: DIRECTORIO (LDAP)



Directorio. LDAP



- LDAP son las siglas de Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol).
- Un servicio de directorio es un servicio de red que identifica todos los recursos que hay en ella, y los vuelve accesibles a los usuarios y a las aplicaciones.
 - *Por ejemplo, el Directorio Activo (Active Directory) es el servicio de directorio incorporado en Windows.*
- Un directorio permite:
 - *Almacenar información acerca de los objetos de la red en el directorio.*
 - *Facilitar la búsqueda de información en cualquier punto de la red, con independencia de su ubicación física.*
 - *Facilita la administración de la red.*

¿Preguntas?



FUNDAMENTOS DE LA CAPA 5

DNS y otros servicios

