

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Ejercicio 1: Sistemas de direccionamiento (I).

a) Usando Wireshark, captura una pantalla de un paquete donde aparezcan en la misma imagen los siguientes seis campos a la vez, e indica la longitud en bytes y bits de cada dirección:

- MAC origen y destino: 6 bytes (o 48 bits) cada MAC
- IPv4 origen y destino: 4 bytes (o 32 bits) cada IPv4
- Puerto origen y destino: 2 bytes (o 16 bits) cada puerto

b) Indica cuál sería la dirección mínima y máxima posible de cada sistema de direccionamiento:

- Primera MAC: 00:00:00:00:00:00
- Última MAC: FF:FF:FF:FF:FF:FF
- Primera IPv4: 0.0.0.0
- Última IPv4: 255.255.255.255
- Primer n.º de puerto: 0
- Último n.º de puerto: 65535

c) Asocia cada sistema de direccionamiento (direcciones MAC, direcciones IP, puertos) con la razón adecuada:

Necesitamos MAC para distinguir cada elemento de una LAN

Necesitamos puertos para distinguir entre aplicaciones en un mismo equipo

Necesitamos IP para distinguir entre equipos tanto en la LAN como en la WAN

Ejercicio 2: Encapsulamiento en los niveles de red y transporte.

a) Escribe el tamaño en bytes típico de cada cabecera en estos dos paquetes:

Ethernet (14 bytes)	IPv4 (20 bytes)	TCP (20 bytes)	Aplicación
----------------------	------------------	-----------------	------------

Ethernet (14 bytes)	IPv4 (20 bytes)	UDP (8 bytes)	Aplicación
----------------------	------------------	----------------	------------

b) Aquí tienes el contenido en hexadecimal de un paquete que usa UDP en la capa de transporte (no aparece el checksum final):

849ca658cfaeb8763f0b24570800450000447879000008011e7e4c0a800c74a7dce
5ef69c01bb003021210c47bf88cd47ec253c040308c562101fb5b772e5b87b449d
99f3b8093b5f21970012772747e1de39

Colorea cada cabecera del paquete usando los siguientes colores de fondo: **enlace**, **red**, **transporte**, **aplicación**.

¿Cuántos bytes ocupa la capa de aplicación? 40 bytes

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Ejercicio 3: Análisis de cabeceras IPv4.

a) Aquí tienes resaltadas las cabeceras IPv4 de 3 paquetes. Completa las tablas con los valores adecuados y en el formato correcto (por ejemplo, escribe un 0 ó 1 en el valor de los flags ya que cada flag es un bit, las IP en decimal, el checksum en hexadecimal, etc):

```
0000  b8 76 3f 0b 24 57 10 62 d0 8c a4 95 08 00 45 00  ·v?·$W·b ······E·
0010  01 31 a8 89 00 00 79 06 19 9c ac d9 11 14 c0 a8  ·1·····y· ······
0020  00 0c 00 50 c0 e8 a3 13 77 58 ea 02 76 3a 50 18  ····P···· wX··v:P·
```

Campo	Longitud en bits	Valor
Versión	4	4
Longitud cabecera	4	5
DSCP	6	0
ECN	2	0
Longitud paquete	16	0x0131 (305)
Identificación	16	0xA889
Flag DF	1	0
Flag MF	1	0
Offset	13	0
TTL	8	0x79 (121)
Siguiente Protocolo	8	0x06 (6)
Checksum	16	0x199C
IP origen	32	0xAC D9 11 14 (172.217.17.20)
IP destino	32	0x C0 A8 00 0C (192.168.0.12)

```
0000  b8 76 3f 0b 24 57 10 62 d0 8c a4 95 08 00 45 00  ·v?·$W·b ······E·
0010  00 35 fa 9a 40 00 31 11 e0 bd b9 1e f4 8c c0 a8  ·5··@·1· ······
0020  00 0c 1b 47 37 2d 00 21 fc e0 01 00 13 19 67 5b  ····G7-·! ······g[
```

Campo	Longitud en bits	Valor
Versión	4	4
Longitud cabecera	4	5
DSCP	6	0
ECN	2	0
Longitud paquete	16	0x0035 (53)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Identificación	16	0xFA9A
Flag DF	1	1
Flag MF	1	0
Offset	13	0
TTL	8	0x31 (49)
Siguiente Protocolo	8	0x11 (17)
Checksum	16	0xE0BD
IP origen	32	0x B9 1E F4 8C (185.30.244.140)
IP destino	32	0x C0 A8 00 0C (192.168.0.12)

```

0000  b8 76 3f 0b 24 57 10 62 d0 8c a4 95 08 00 45 20  ·v?·$W·b ······E
0010  00 30 5a 8c 00 00 31 11 fa a8 31 90 42 24 c0 a8  ·0Z···1· ··1·8$··
0020  00 0c 58 05 37 2d 00 1c 29 db 21 00 3a 12 c7 41  ··X·7-·· )!·:··A

```

Campo	Longitud en bits	Valor
Versión	4	4
Longitud cabecera	4	5
DSCP	6	001000 (8)
ECN	2	0
Longitud paquete	16	0x0030 (48)
Identificación	16	0x5A8C
Flag DF	1	0
Flag MF	1	0
Offset	13	0
TTL	8	0x31 (49)
Siguiente Protocolo	8	0x11 (17)
Checksum	16	0xFAA8
IP origen	32	0x 31 90 42 24 (49.144.66.36)
IP destino	32	0x C0 A8 00 0C (192.168.0.12)

b) Ahora escribe el contenido completo en hexadecimal de cuatro cabeceras IPv4, sabiendo que cada una cumple los siguientes requisitos especificados. Si no se te proporciona el valor de alguno de los campos, usa el valor por defecto más común o valores aleatorios si es necesario:

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

- Paquete enviado por 25.46.98.124 (un servidor web) a 192.168.0.13, con una longitud total de 1000 bytes y un TTL de 80

Contenido cabecera: 45 00 03 E8 XX XX 00 00 50 06 XX XX 19 2E 62 7C C0 A8 00 00

- Paquete enviado por un servidor FTP cuya IP es 212.15.68.93 a 10.0.0.5, con longitud total de 400 bytes y un TTL de 50. Es el segundo y último fragmento de un paquete. El primer fragmento tenía una longitud de 700 bytes de datos

Contenido cabecera: 45 00 01 90 XX XX 00 57 32 06 XX XX D4 0F 44 5D 0A 00 00 05

- Paquete de un cliente HTTPS enviado desde 43.21.203.65 a 180.12.12.4 con un TTL de 5 y longitud de 400 bytes

Contenido cabecera: 45 00 01 90 XX XX 00 00 05 06 XX XX 2B 15 CB 41 B4 0C 0C 04

- Paquete DNS que ha de ser entregado de manera inmediata desde 8.8.8.8 a tu ordenador, con un TTL de 19 y longitud total de 60 bytes. Este paquete debe reaccionar si encuentra congestión en la ruta

Contenido cabecera: 45 49 3C XX XX 00 00 13 17 XX XX 08 08 08 08 XX XX XX XX

Puede serte útil rellenar una tabla para cada cabecera (como la del apartado anterior), y cuando tengas todos los campos, escribe entonces todo el contenido completo en hexadecimal, de manera que el resultado sea una secuencia de bytes.

Ejercicio 4: Práctica: Filtros IP en Wireshark.

Averigua primero los datos de tu conexión, adjuntando los pantallazos adecuados:

- Mi MAC es: _____
- Mi IPv4 es: _____
- Mi máscara es: _____
- Mi puerta de enlace es: _____

Con ayuda de los datos obtenidos, escribe el filtro Wireshark de cada apartado:

a) Paquetes enviados a tu IP

`ip.dst==(mi IP)`

b) Paquetes enviados por tu IP a tu puerta de enlace

`ip.src==(mi IP) && ip.dst==(IP puerta enlace)`

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

c) Paquetes que tengan parte opcional al final de la cabecera IP

`ip.hlen>5`

d) Paquetes cuya longitud total de la zona de IP esté entre 500 y 1000 bytes

`ip.len>500 && ip.len<1000`

e) Paquetes con TTL mayor que 10

`ip.ttl>10`

f) Paquetes que no usen TCP en la capa de transporte

`ip.proto!=6`

g) Paquetes que no puedan fragmentarse

`ip.flags.df==1`

h) Paquetes enviados por tu IP y tu MAC, con TTL menor que 20 y que usen UDP

`ip.src==(mi IP) && eth.src==(mi MAC) && ip.ttl<20 && ip.proto==17`

Ejercicio 5: Fragmentación en IP.

a) Supón que quieres enviar un paquete de 5000 bytes de datos a través de una red Ethernet. Indica, para cada fragmento, el valor de los siguientes campos de las cabeceras:

Fragmento n.º 1 : Identificador=X, MF=1, offset=0

Fragmento n.º 2 : Identificador=X, MF=1, offset=1480/8=185

Fragmento n.º 3 : Identificador=X, MF=1, offset=2*1480/8=370

Fragmento n.º 4 : Identificador=X, MF=0, offset=3*1480/8=555

(Utiliza tantos fragmentos como necesites. Como identificador de todos, puedes usar un número aleatorio)

Explicación:

Como MTU=1500, cada paquete tiene 1500 (total paquete)-20(cabecera)=1480 (datos)

Queremos enviar 5000 bytes en paquetes de 1480 bytes cada uno

Por tanto, necesitaremos $5000/1480=3,37$ (3 paquetes enteros y uno más pequeño)

3 paquetes de 1480= 4440 bytes

Hasta 5000 quedan $5000-4440=560$

Enviaremos 3 de 1480 y 1 de 560

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

b) En una red se capturan los siguientes paquetes, correspondientes a los dos últimos fragmentos de una transmisión. Solo se muestran los datos necesarios de su cabecera IPv4:

- Penúltimo: Identificador=1352, MF=1, offset=375, longitud total=620
- Último: Identificador=1352, MF=0, offset=450, longitud total=120

Averigua:

- La MTU de la red: 620 bytes
- El nº total de fragmentos en los que se dividió el paquete inicial: 7 fragmentos
- La longitud de los datos del paquete inicial sin fragmentar: 3700 bytes

Explicación:

Penúltimo: 620 bytes (600 +20 cabecera). Como no puede haber paquetes más grandes, esa es la MTU.

último: 120 bytes (100 +20 cabecera)

Cada fragmento, excepto el último, tiene 600 bytes de datos.

Como el offset del último es 450, quiere decir que se han enviado antes de él $450 \times 8 = 3600$ bytes de datos. Como el último tiene 100 el total es de $3600 + 100 = 3700$ bytes

Como cada paquete tiene 600, se necesitaron $3700 / 600 = 6,16$ fragmentos, es decir, 6 paquetes enteros y el último más pequeño. Total: 7 paquetes

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Ejercicio 8: Sistemas de direccionamiento (II).

Completa la siguiente tabla teniendo en cuenta que:

- La MAC origen/destino puede ser: “mi MAC”, “la MAC del router”, “la MAC del servidor” o “difusión”
- La IP origen/destino puede ser: “mi IP”, “la IP del router”, “la IP del servidor” o “difusión”
- El puerto origen/destino puede ser: “aleatorio” o un número concreto (consultar tabla de puertos en el PDF o las diapositivas de la unidad)

Colorea en amarillo las filas que usan TCP en el nivel de transporte y en verde las que usan UDP.

	MAC origen	MAC destino	IP origen	IP destino	Puerto origen	Puerto destino
Petición para ver una web externa	Mi MAC	MAC router	Mi IP	IP servidor	x	443
Petición para usar el servidor FTP de la LAN	Mi MAC	MAC servidor	Mi IP	IP servidor	x	21
Respuesta de un servidor DNS externo	MAC router	Mi MAC	IP servidor	Mi IP	53	x
Respuesta del servidor web de Google	MAC router	Mi MAC	IP servidor	Mi IP	443	x
Petición para obtener una IP	Mi MAC	difusión	Mi IP	difusión	68	67

Explicación:

En la última fila, por las peculiaridades del servicio DHCP, se realiza por difusión y sin puerto aleatorio. Si has puesto que la petición va dirigida al servidor, se tomará como válida también (aunque realmente no es correcto).

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Ejercicio 9: Análisis de cabeceras TCP y UDP.

a) Aquí tienes una serie de paquetes en los que aparece resaltada la cabecera UDP en cada uno de ellos. Para cada paquete, indica si se trata de una petición o una respuesta, e indica también de qué servicio (HTTPS, DNS, etc).

```
0000 10 62 d0 8c a4 95 b8 76 3f 0b 24 57 08 00 45 00
0010 00 3c 04 b6 00 00 80 11 cd 9b c0 a8 00 0c d4 a6
0020 d3 04 e9 31 00 35 00 28 4c 32 ce 01 01 00 00 01
0030 00 00 00 00 00 00 00 03 77 77 77 06 65 6c 70 61 69
0040 73 03 63 6f 6d 00 00 01 00 01
```

- Es una __petición__ del servicio __DNS (puerto destino=53)

```
0000 ff ff ff ff ff ff b8 76 3f 0b 24 57 08 00 45 00
0010 01 48 14 12 00 00 80 11 25 94 00 00 00 00 ff ff
0020 ff ff 00 44 00 43 01 34 c8 e6 01 01 06 00 ec ef
0030 f5 84 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 b8 76 3f 0b 24 57 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

- Es una __petición__ del servicio __DHCP (puerto destino=67)

```
0000 b8 76 3f 0b 24 57 10 62 d0 8c a4 95 08 00 45 00
0010 00 74 04 ce 00 00 fc 11 51 4b d4 a6 d3 04 c0 a8
0020 00 0c 00 35 e7 b4 00 60 23 f6 ef 1a 81 80 00 01
0030 00 03 00 00 00 00 08 70 72 69 73 61 63 6f 6d 02
0040 73 63 06 6f 6d 74 72 64 63 03 6e 65 74 00 00 01
0050 00 01 c0 0c 00 01 00 01 00 00 00 8e 00 04 6c 80
0060 82 e0 c0 0c 00 01 00 01 00 00 00 8e 00 04 34 31
0070 64 bd c0 0c 00 01 00 01 00 00 00 8e 00 04 34 1f
0080 be 3a
```

- Es una __respuesta__ del servicio __DNS (puerto origen=53)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

b) Aquí tienes resaltadas las cabeceras TCP de 3 paquetes. Completa las tablas con los valores adecuados y en el formato correcto (por ejemplo, escribe un 0 ó 1 en el valor de los flags ya que cada flag es un bit, escribe los puertos en decimal, el checksum en hexadecimal, etc):

```
0000 10 62 d0 8c a4 95 b8 76 3f 0b 24 57 08 00 45 00
0010 00 28 b5 d3 40 00 80 06 72 a9 c0 a8 00 0c 0d 6b
0020 04 34 cb e8 00 50 29 bb 1e e3 32 d9 5d 30 50 10
0030 02 05 36 9c 00 00
```

Campo	Longitud en bits	Valor
Puerto origen	16	0x CB E8 (52200)
Puerto destino	16	0x 00 50 (80: HTTP)
Flag ACK	1	1
Flag SYN	1	0
Checksum	16	0x 36 9C

```
0000 b8 76 3f 0b 24 57 10 62 d0 8c a4 95 08 00 45 00
0010 00 ff ab 51 40 00 32 06 25 f3 a2 7d 13 83 c0 a8
0020 00 0c 01 bb cb df f7 47 7f ed 95 d1 e7 94 50 18
0030 ae 60 ea 3e 00 00 17 03 03 00 d2 00 00 00 00 00
0040 00 00 02 79 e2 67 73 f0 6b 33 1a 1f 0b 55 20 c5
```

Campo	Longitud en bits	Valor
Puerto origen	16	0x 01 BB (443: HTTPS)
Puerto destino	16	0x CB DF (52191)
Flag ACK	1	1
Flag SYN	1	0
Checksum	16	0x EA 3E

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

```
0000 b8 76 3f 0b 24 57 10 62 d0 8c a4 95 08 00 45 00
0010 00 34 80 75 40 00 77 06 b0 fb 0d 6b 04 34 c0 a8
0020 00 0c 00 50 cb e8 32 d9 5d 2f 29 bb 1e e3 80 12
0030 ff ff f7 e1 00 00 02 04 05 a0 01 03 03 08 01 01
0040 04 02
```

Campo	Longitud en bits	Valor
Puerto origen	16	0x 00 50 (80: HTTP)
Puerto destino	16	0x CB E8 (52200)
Flag ACK	1	1
Flag SYN	1	1
Checksum	16	0x F7 E1

Ejercicio 10: Práctica: Filtros TCP y UDP en Wireshark.

a) Escribe el filtro Wireshark para obtener...

- Respuestas DNS enviadas por tu ordenador
`udp.srcport==53&&ip.src==(mi IP)`
- Peticiones HTTPS enviadas por tu ordenador
`tcp.dstport==443&&ip.src==(mi IP)`
- Paquetes SYN+ACK enviados por cualquier servidor web HTTPS
`tcp.flags.syn==1 && tcp.srcport==443`
- Respuestas DHCP enviadas por tu servidor DHCP (tu router)
`udp.srcport==67 && ip.src==(IP router)`
- Paquetes FTP (tanto preguntas como respuestas) con TTL mayor que 10
`ip.ttl>10 && tcp.port==21`

b) Captura paquetes y guarda en un fichero de Wireshark únicamente estos 4 paquetes:

- Un paquete SYN
- Un paquete SYN+ACK
- Una petición DNS
- Una respuesta DNS

➔ Adjunta el fichero de Wireshark a tu entrega

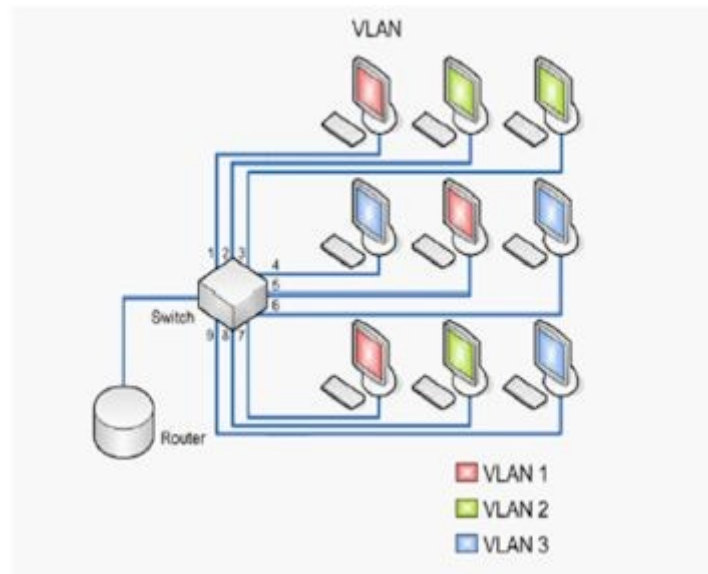
Ejercicio 11: VLAN.

Una VLAN (Virtual LAN) es una manera de crear grupos de dispositivos en una LAN, aunque físicamente no estén en la misma área de trabajo. De ahí el nombre de redes

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

“virtuales”, ya que están formadas por equipos independientemente de su posición en la LAN.

Por ejemplo, en el siguiente esquema puedes ver una red con 9 equipos, todos conectados al mismo switch, pero divididos en 3 VLAN diferentes dependiendo del color:



De esta forma, podemos organizar los equipos en grupos y, por ejemplo, aplicarles reglas de seguridad diferentes sin pensar dónde están situados. Los equipos pertenecientes a una VLAN creerán que están juntos, y separados de los equipos de otra VLAN (como si cada grupo tuviera un switch dedicado). Además de ayudar a gestionar la seguridad y simplificar la administración de la red, minimiza las molestias producidas por el tráfico por difusión. Sin VLAN, cuando un equipo envía un paquete por broadcast, llega a todos los demás equipos. Con VLAN, la difusión solo llega a los equipos de su mismo grupo. Es una manera de establecer dominios de difusión, que propagan los paquetes de broadcast solo por algunos puertos del switch, no por todos.

La creación de varias redes virtuales en los equipos conectados al mismo switch de una LAN ha de hacerse accediendo a la configuración del switch. Para ello, basta con definir cada grupo e indicar los n.º de los puertos del switch donde se conectan los equipos de cada grupo o VLAN.

a) Accede a la configuración del switch de la unidad anterior (ejercicio 6 de la unidad 5) y busca la sección para configurar una VLAN. Aparece ya creada una VLAN por defecto.

- ¿Cómo se llama la VLAN ya creada? _Default VLAN_
- ¿Cuál es su número identificador? _1_
- ¿Qué puertos del switch pertenecen a esa VLAN? _2, 5, 9, 11, 13_

Adjunta una captura de la pantalla donde aparezca la configuración de VLAN en el switch.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

The screenshot shows the 'VLAN Config' tab for a TL-SL5428E switch. On the left is a navigation menu with options like System, Switching, VLAN, 802.1Q VLAN, MAC VLAN, Protocol VLAN, VLAN VPN, Private VLAN, and GVRP. The main area displays the 'VLAN Table' with a search bar for 'VLAN ID' and a 'Select' button. Below is a table with columns: Select, VLAN ID, Name, Members, and Operation. One entry is shown: VLAN ID 1, Name 'Default VLAN', Members '1-28', and an 'Edit | Detail' link. At the bottom, there are buttons for 'Create', 'All', 'Delete', and 'Help', and a status 'Total VLAN: 1'.

Select	VLAN ID	Name	Members	Operation
<input type="checkbox"/>	1	Default VLAN	1-28	Edit Detail

This screenshot shows the 'VLAN Info' and 'VLAN Members' sections of the TL-SL5428E configuration interface. The 'VLAN Info' section has fields for 'VLAN ID' (set to 1) and 'Name' (set to 'System VLAN'). The 'VLAN Members' section contains a table for assigning ports to the VLAN. The table has columns: Select, Port, Link Type, Egress Rule, and LAG. Ports 2, 5, 8, 11, and 13 are selected. The 'Egress Rule' column has dropdown menus for some ports, showing options like UNTAG and TAG. The 'LAG' column shows associations like LAG1 and LAG2. Buttons for 'Apply', 'All', 'Back', and 'Help' are at the bottom.

Select	Port	Link Type	Egress Rule	LAG
<input type="checkbox"/>	1	ACCESS	UNTAG	---
<input checked="" type="checkbox"/>	2	ACCESS	UNTAG	---
<input type="checkbox"/>	3	ACCESS	UNTAG	---
<input type="checkbox"/>	4	ACCESS	UNTAG	---
<input checked="" type="checkbox"/>	5	GENERAL	UNTAG	LAG1
<input type="checkbox"/>	6	GENERAL	UNTAG	LAG1
<input type="checkbox"/>	7	GENERAL	UNTAG	LAG1
<input type="checkbox"/>	8	GENERAL	UNTAG	LAG1
<input checked="" type="checkbox"/>	9	ACCESS	UNTAG	---
<input type="checkbox"/>	10	TRUNK	TAG	---
<input checked="" type="checkbox"/>	11	GENERAL	TAG	LAG2
<input type="checkbox"/>	12	ACCESS	UNTAG	LAG2
<input checked="" type="checkbox"/>	13	GENERAL	UNTAG	LAG2
<input type="checkbox"/>	14	ACCESS	UNTAG	LAG2

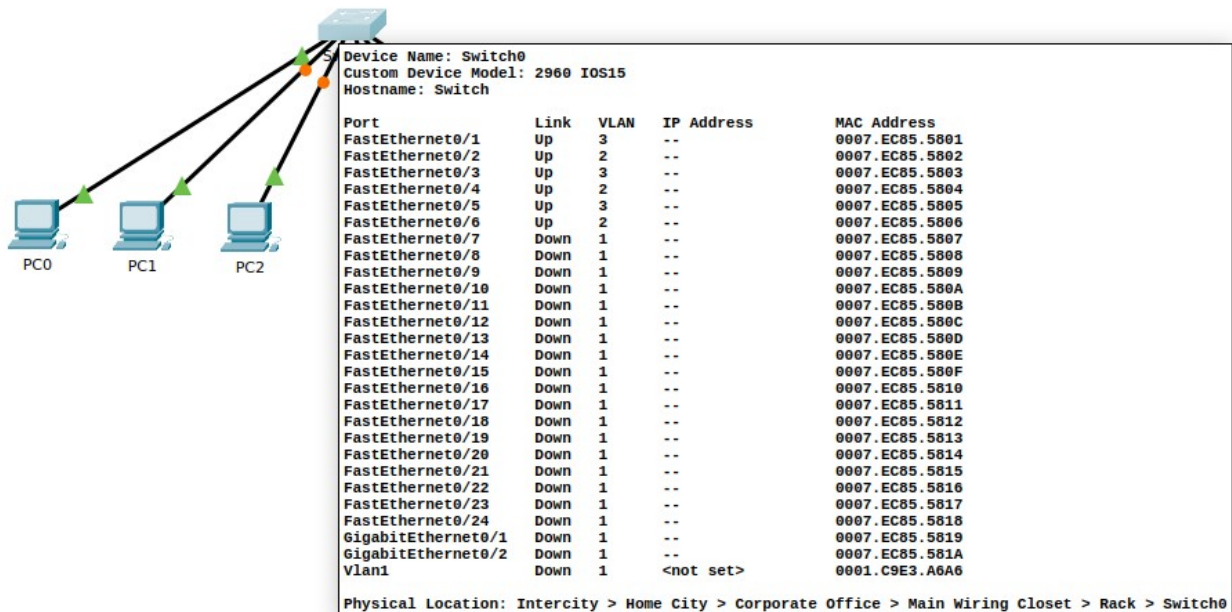
b) Para crear una VLAN en PT, sigue los siguientes pasos:

- Crea una LAN con un switch 2960 y 6 PC conectados al switch
- Asigna a los PC las IP estáticas de la 192.168.0.1 a la 6, y la misma máscara (255.255.255.0) en todos
- Ve a la configuración del switch, Config, VLAN Database
- Por defecto, aparecen ya creadas varias VLAN. Crea dos VLAN nuevas: una con n.º identificador 2 y nombre "Pares" y otra con n.º identificador 3 y nombre "Impares"
- Aún en el switch, ve en Config a cada uno de sus puertos (FastEthernet0/1, FastEthernet0/2, etc) y asigna la VLAN 2 a los que tienen IP par y la VLAN 3 a los que tienen IP impar

Adjunta una captura de pantalla donde aparezca la distribución de los equipos en las dos VLAN. Para ello, cuando termines todos los pasos, deja el ratón quieto sobre el switch y aparecerá una tabla con la VLAN asociada a cada puerto.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Adjunta también otra captura de pantalla con los comandos CLI que se han usado internamente para configurar las VLAN del switch.



```

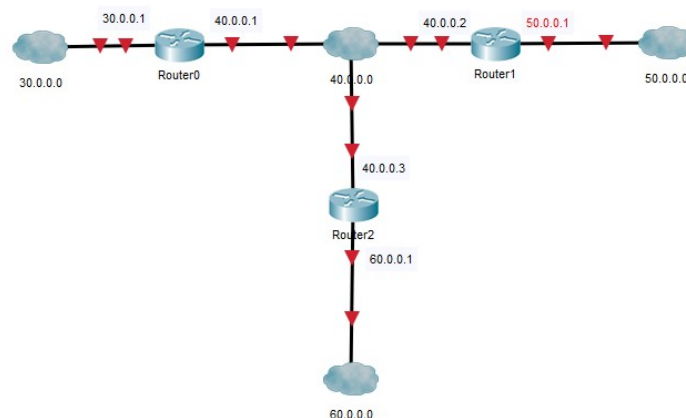
Physical  Config  CLI  Attributes
IOS Command Line Interface
Switch(config-if)#switchport access vlan 3
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 3
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/5
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 3
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/6
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport access vlan 2
Switch(config-if)#

```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Ejercicio 6: Tablas de enrutamiento.

a) Completa las tablas de enrutamiento estático de cada uno de los routers de esta LAN:



Router R0	
Red destino	Siguiente salto
30.0.0.0	30.0.0.1
40.0.0.0	40.0.0.1
50.0.0.0	40.0.0.2
60.0.0.0	40.0.0.3

Router R1	
Red destino	Siguiente salto
30.0.0.0	40.0.0.1
40.0.0.0	40.0.0.2
50.0.0.0	50.0.0.1
60.0.0.0	40.0.0.3

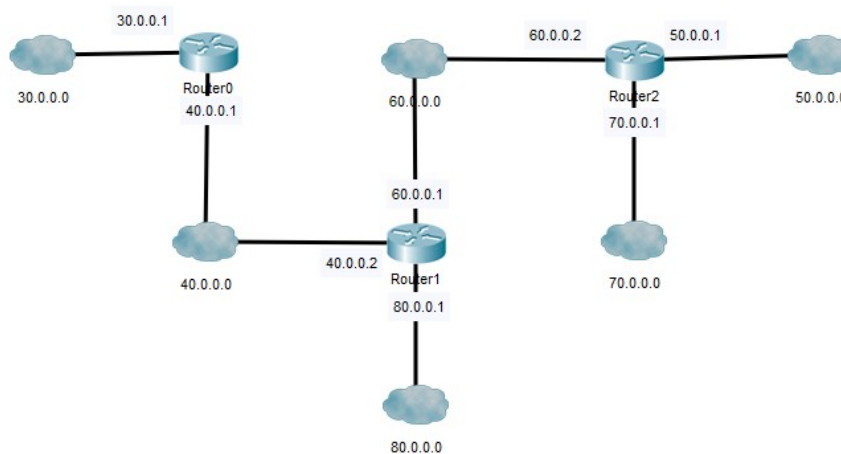
Router R2	
Red destino	Siguiente salto
30.0.0.0	40.0.0.1
40.0.0.0	40.0.0.3
50.0.0.0	40.0.0.2
60.0.0.0	60.0.0.1

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

En resumen, para rellenar la columna “Siguiete salto”:

- Si el destino es una red directamente conectada al router X, el siguiete salto es la IP del router X correspondiente a la red a la que queremos ir
- Si el destino no es una red directamente conectada al router X, se pone la IP del siguiete router cercano al que saltar (teniendo en cuenta que solo podemos usar IP en los rangos que conoce el router X)

b) Escribe las tablas de enrutamiento estático de todos los routers de esta red:



Router R0	
Red destino	Siguiete salto
30.0.0.0	30.0.0.1
40.0.0.0	40.0.0.1
50.0.0.0	40.0.0.2
60.0.0.0	40.0.0.2
70.0.0.0	40.0.0.2
80.0.0.0	40.0.0.2

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Router R1	
Red destino	Siguiente salto
30.0.0.0	40.0.0.1
40.0.0.0	40.0.0.2
50.0.0.0	60.0.0.2
60.0.0.0	60.0.0.1
70.0.0.0	60.0.0.2
80.0.0.0	80.0.0.1

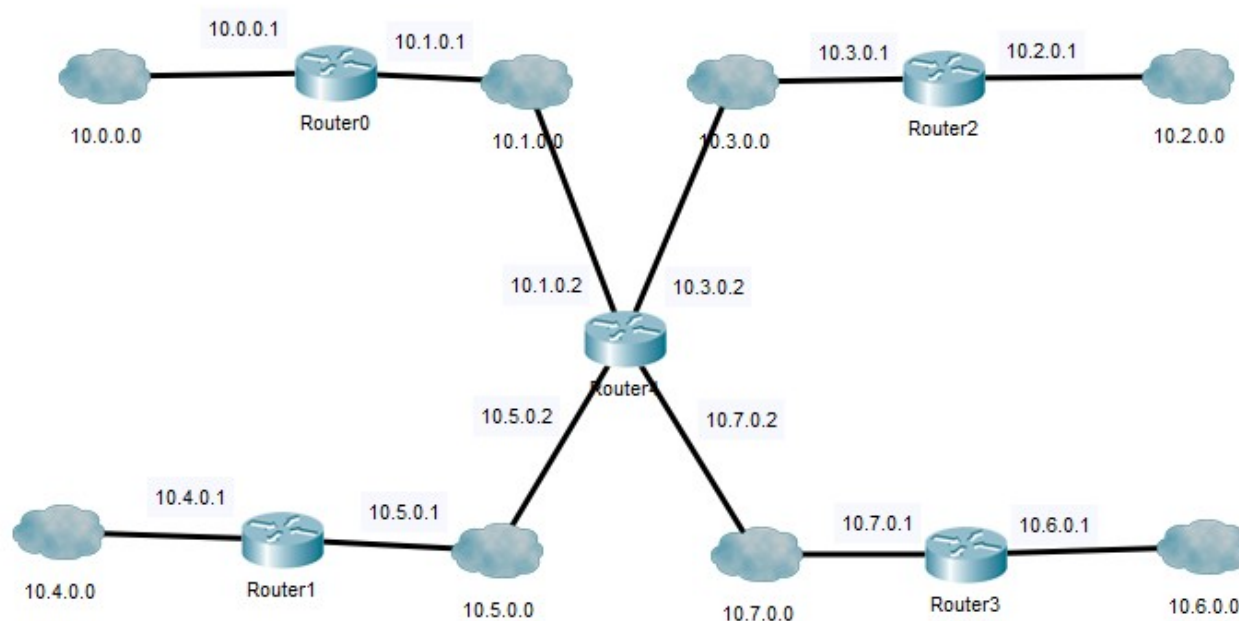
Router R2	
Red destino	Siguiente salto
30.0.0.0	60.0.0.1
40.0.0.0	60.0.0.1
50.0.0.0	50.0.0.1
60.0.0.0	60.0.0.2
70.0.0.0	70.0.0.1
80.0.0.0	60.0.0.1

Como puede verse, todas las tablas tienen la columna “red destino” idéntica, por lo que en lugar de escribir cada tabla por separado, vamos a organizarlas todas en una para mayor claridad (aunque recuerda que en realidad cada router tiene su tabla por separado con sus dos columnas):

Red destino	R0: Siguiente salto	R1: Siguiente salto	R2: Siguiente salto
30.0.0.0	30.0.0.1	40.0.0.1	60.0.0.1
40.0.0.0	40.0.0.1	40.0.0.2	60.0.0.1
50.0.0.0	40.0.0.2	60.0.0.2	50.0.0.1
60.0.0.0	40.0.0.2	60.0.0.1	60.0.0.2
70.0.0.0	40.0.0.2	60.0.0.2	70.0.0.1
80.0.0.0	40.0.0.2	80.0.0.1	60.0.0.1

CIPFP Ausiàs March (Valencia)
 1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

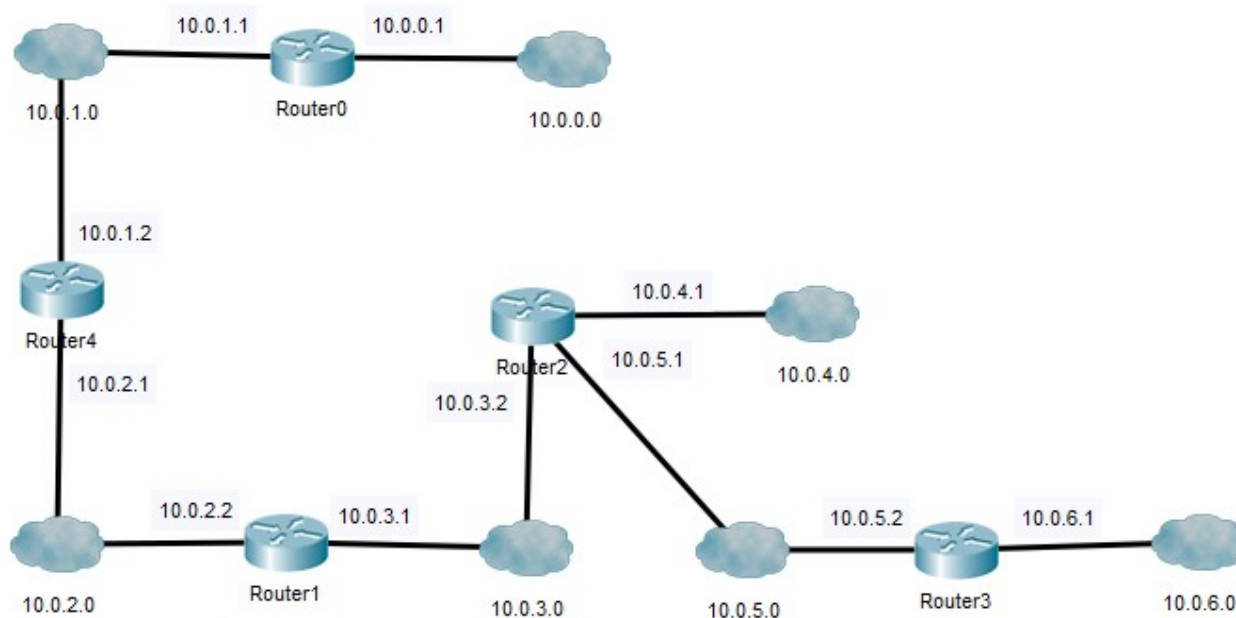
c) Escribe las tablas de enrutamiento estático de todos los routers de esta red:



Red destino	R0: Sig. salto	R1: Sig. salto	R2: Sig. salto	R3: Sig. salto	R4: Sig. salto
10.0.0.0	10.0.0.1	10.5.0.2	10.3.0.2	10.7.0.2	10.1.0.1
10.1.0.0	10.1.0.1	10.5.0.2	10.3.0.2	10.7.0.2	10.1.0.2
10.2.0.0	10.1.0.2	10.5.0.2	10.2.0.1	10.7.0.2	10.3.0.1
10.3.0.0	10.1.0.2	10.5.0.2	10.3.0.1	10.7.0.2	10.3.0.2
10.4.0.0	10.1.0.2	10.4.0.1	10.3.0.2	10.7.0.2	10.5.0.1
10.5.0.0	10.1.0.2	10.5.0.1	10.3.0.2	10.7.0.2	10.5.0.2
10.6.0.0	10.1.0.2	10.5.0.2	10.3.0.2	10.6.0.1	10.7.0.1
10.7.0.0	10.1.0.2	10.5.0.2	10.3.0.2	10.7.0.1	10.7.0.2

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

d) Escribe las tablas de enrutamiento estático de todos los routers de esta red:



Red destino	R0: Sig. salto	R1: Sig. salto	R2: Sig. salto	R3: Sig. salto	R4: Sig. salto
10.0.0.0	10.0.0.1	10.0.2.1	10.0.3.1	10.0.5.1	10.0.1.1
10.0.1.0	10.0.1.1	10.0.2.1	10.0.3.1	10.0.5.1	10.0.1.2
10.0.2.0	10.0.1.2	10.0.2.2	10.0.3.1	10.0.5.1	10.0.2.1
10.0.3.0	10.0.1.2	10.0.3.1	10.0.3.2	10.0.5.1	10.0.2.2
10.0.4.0	10.0.1.2	10.0.3.2	10.0.4.1	10.0.5.1	10.0.2.2
10.0.5.0	10.0.1.2	10.0.3.2	10.0.5.1	10.0.5.2	10.0.2.2
10.0.6.0	10.0.1.2	10.0.3.2	10.0.5.2	10.0.6.1	10.0.2.2

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

e) Ahora escribe la tabla de encaminamiento de un host para cada “nube” de cada una de las redes de a), b), c) y d). Por ejemplo, esta sería la tabla de enrutamiento del host cuya IP es 30.0.0.2, de la red del apartado a)

Host 30.0.0.2	
Red destino	Siguiente salto
30.0.0.0	directa
default	30.0.0.1

Las tablas de los host son muy sencillas. Un host solo está conectado a una red, por tanto, únicamente hay dos opciones: o entrega a alguien de su misma red (primera fila, entrega directa) o lo envía al router que hace de puerta de enlace (segunda fila, línea default). La IP del host (30.0.0.2) es cualquiera que pertenezca a esa red excepto la 30.0.0.1, que ya está ocupada por el router. Podríamos haber usado 30.0.0.20 o 30.0.0.18, por ejemplo. Las tablas de encaminamiento de todos los host de una misma “nube” son idénticas. Puedes imaginarte cada “nube” como un switch al que están conectados un conjunto de equipos. Para simplificar el diseño, en el enrutamiento se usan “nubes” para representar las subredes dentro de una red. Incluye aquí la tabla de encaminamiento para cada host de cada subred de cada una de las cuatro LAN anteriores. En total, son 24 tablas.

Tablas de enrutamiento de los hosts del apartado a)

Host 30.0.0.2	
Red destino	Siguiente salto
30.0.0.0	directa
default	30.0.0.1

Host 40.0.0.4	
Red destino	Siguiente salto
30.0.0.0	40.0.0.1
40.0.0.0	directa
50.0.0.0	40.0.0.2
60.0.0.0	40.0.0.3

(La tabla anterior no puede resumirse porque en la columna “siguiente salto” las IP son diferentes)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Host 50.0.0.2	
Red destino	Siguiente salto
50.0.0.0	directa
default	50.0.0.1

Host 60.0.0.2	
Red destino	Siguiente salto
60.0.0.0	directa
default	60.0.0.1

Tablas de enrutamiento de los hosts del apartado b)

Host 30.0.0.2	
Red destino	Siguiente salto
30.0.0.0	directa
default	30.0.0.1

Host 40.0.0.3	
Red destino	Siguiente salto
40.0.0.0	directa
30.0.0.0	40.0.0.1
default	40.0.0.2

Host 50.0.0.2	
Red destino	Siguiente salto
50.0.0.0	directa
default	50.0.0.1

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Host 60.0.0.3	
Red destino	Siguiente salto
60.0.0.0	Directa
50.0.0.0	60.0.0.2
70.0.0.0	60.0.0.2
Default	60.0.0.1

Host 70.0.0.2	
Red destino	Siguiente salto
70.0.0.0	Directa
Default	70.0.0.1

Host 80.0.0.2	
Red destino	Siguiente salto
80.0.0.0	Directa
Default	80.0.0.1

Tablas de enrutamiento de los hosts del apartado c)

Host 10.0.0.2	
Red destino	Siguiente salto
10.0.0.0	directa
default	10.0.0.1

Host 10.1.0.3	
Red destino	Siguiente salto
10.1.0.0	directa
10.0.0.0	10.1.0.1
default	10.1.0.2

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Host 10.2.0.2	
Red destino	Siguiente salto
10.2.0.0	directa
default	10.2.0.1

Host 10.3.0.3	
Red destino	Siguiente salto
10.3.0.0	directa
10.2.0.0	10.3.0.1
Default	10.3.0.2

Host 10.4.0.2	
Red destino	Siguiente salto
10.4.0.0	directa
default	10.4.0.1

Host 10.5.0.3	
Red destino	Siguiente salto
10.5.0.0	directa
10.4.0.0	10.5.0.1
Default	10.5.0.2

Host 10.6.0.2	
Red destino	Siguiente salto
10.6.0.0	directa
Default	10.6.0.1

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Host 10.7.0.3	
Red destino	Siguiente salto
10.7.0.0	directa
10.6.0.0	10.7.0.1
Default	10.7.0.2

Tablas de enrutamiento de los hosts del apartado d)

Host 10.0.0.2	
Red destino	Siguiente salto
10.0.0.0	directa
default	10.0.0.1

Host 10.0.1.3	
Red destino	Siguiente salto
10.0.1.0	directa
10.0.0.0	10.0.1.1
default	10.0.1.2

Host 10.0.2.3	
Red destino	Siguiente salto
10.0.2.0	Directa
10.0.1.0	10.0.2.1
10.0.0.0	10.0.2.1
Default	10.0.2.2

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

Host 10.0.3.3	
Red destino	Siguiente salto
10.0.3.0	directa
10.0.4.0	10.0.3.2
10.0.5.0	10.0.3.2
10.0.6.0	10.0.3.2
Default	10.0.3.1

(También se podrían haber incluido en default las otras tres rutas y obtener otra tabla distinta)

Host 10.0.4.2	
Red destino	Siguiente salto
10.0.4.0	directa
default	10.0.4.1

Host 10.0.5.3	
Red destino	Siguiente salto
10.0.5.0	directa
10.0.6.0	10.0.5.2
Default	10.0.5.1

Host 10.0.6.2	
Red destino	Siguiente salto
10.0.6.0	directa
Default	10.0.6.1

f) Añade a **todas** las tablas de encaminamiento obtenidas una columna nueva llamada máscara, como en el ejemplo siguiente, para que tanto routers como hosts sepan qué parte de la IP corresponde a la subred.

La máscara será 255.0.0.0, 255.255.0.0 ó 255.255.255.0, dependiendo de si en las IP la parte de la subred ocupa uno, dos o tres bytes. (Este concepto será ampliado con detalle en la unidad siguiente)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

(No copies y pegues todas las tablas de nuevo aquí, puedes añadir directamente la columna nueva a cada una de las tablas ya obtenidas)

Máscara en todas las tablas del apartado a) = 255.0.0.0

Máscara en todas las tablas del apartado b) = 255.0.0.0

Máscara en todas las tablas del apartado c) = 255.255.0.0

Máscara en todas las tablas del apartado d) = 255.255.255.0

g) Supongamos que en la red del apartado c) se realiza un cambio: añadir un nuevo router (Router5) entre las subredes 10.0.0.0 y 10.4.0.0. ¿Qué modificaciones habría que hacer para que las tablas de enrutamiento reflejaran este cambio? Copia aquí las tablas que han de modificarse, resaltando en amarillo las filas que han cambiado. Incluye también la tabla del nuevo router.

Los principales cambios serían:

- Un nuevo router5 que tendrá las IP 10.0.0.2 y 10.4.0.2.
- Su tabla de enrutamiento sería:

Router R5	
Red destino	Siguiente salto
10.0.0.0	10.0.0.2
10.1.0.0	10.0.0.1
10.2.0.0	10.0.0.1
10.3.0.0	10.0.0.1
10.4.0.0	10.4.0.2
10.5.0.0	10.4.0.1
10.6.0.0	10.4.0.1
10.7.0.0	10.4.0.1

- Podrían haberse escogido otras rutas diferentes siempre que el n.º de saltos ni aumente.
- Habría que modificar también las tablas de los hosts pertenecientes a las subredes 10.0.0.0 y 10.4.0.0

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

h) Supongamos que en la red del apartado d) se realizan dos cambios: añadir un nuevo router (Router5) entre las subredes 10.0.0.0 y 10.0.4.0, y eliminar el cable entre el Router2 y la subred 10.0.4.0. ¿Qué modificaciones habría que hacer para que las tablas de enrutamiento reflejaran estos cambios? Copia aquí las tablas que han de modificarse, resaltando en amarillo las filas que han cambiado. Incluye también la tabla del nuevo router.

Los principales cambios serían:

- Un nuevo router5 que tendrá las IP 10.0.0.2 y 10.0.4.1.
- Su tabla de enrutamiento sería:

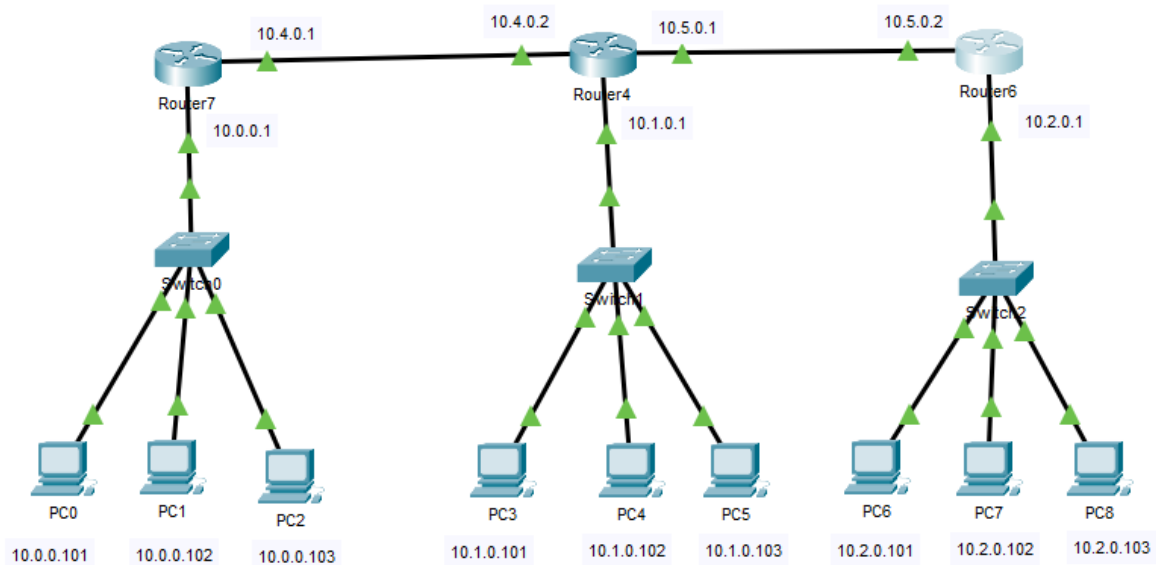
Router R5	
Red destino	Siguiente salto
10.0.0.0	10.0.0.2
10.0.1.0	10.0.0.1
10.0.2.0	10.0.0.1
10.0.3.0	10.0.0.1
10.0.4.0	10.0.4.1
10.0.5.0	10.0.4.1
10.0.6.0	10.0.4.1
10.0.7.0	10.0.4.1

- Habría que modificar también las tablas de los hosts pertenecientes a las subredes 10.0.0.0 y 10.0.4.0
- Habría que modificar la tabla de enrutamiento del router2, concretamente la fila correspondiente a 10.0.4.0, cuyo siguiente salto pasa a ser 10.0.3.2

Ejercicio 7: Práctica: Enrutamiento estático y dinámico con Packet Tracer

Parte 3: Enrutamiento estático

Para probar el enrutamiento, modifica la red anterior para que sea como la de la siguiente figura.



- ➔ Como resolución de esta actividad, adjunta a tu entrega el fichero .pkt con la red final (no olvides añadir etiqueta con nombre y fecha, así como poner etiquetas con las IP de todos los PC y routers).

Además, escribe aquí los comandos CLI para configurar las tres tablas de encaminamiento:

Router izquierdo:

```
ip route 10.1.0.0/16 10.4.0.2
ip route 10.2.0.0/16 10.4.0.2      (o usando 255.255.0.0 en lugar de /16)
ip route 10.5.0.0/16 10.4.0.2
```

Router derecho:

```
ip route 10.0.0.0/16 10.5.0.1
ip route 10.1.0.0/16 10.5.0.1      (o usando 255.255.0.0 en lugar de /16)
ip route 10.4.0.0/16 10.5.0.1
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 6: Capas de red y transporte

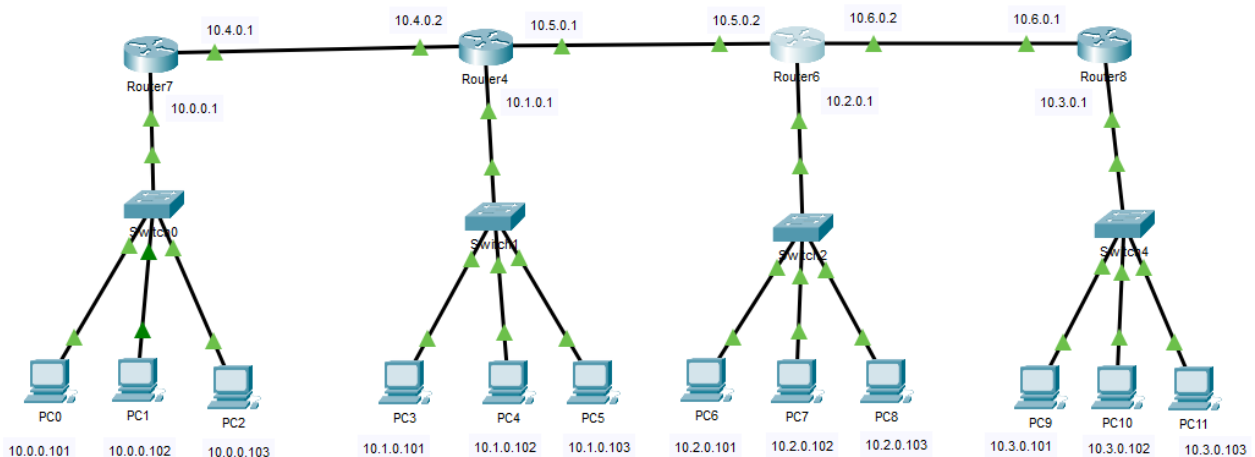
Router central:

```
ip route 10.0.0.0/16 10.4.0.1  
ip route 10.2.0.0/16 10.5.0.2      (o usando 255.255.0.0 en lugar de /16)
```

Parte 4: Enrutamiento dinámico

Mientras que en el enrutamiento estático has tenido que añadir a mano las filas de cada tabla de encaminamiento en cada router, usando protocolos de enrutamiento dinámico las tablas se rellenan automáticamente gracias al uso de protocolos como RIP.

Para probarlo en PT, haz una copia del fichero anterior y en la copia añade a tu red una nueva subred a la derecha, con la misma estructura (un switch, tres PC con IP 10.3.0.101 a la 10.3.0.103, etc), haciendo las modificaciones que consideres necesarias.



Ahora en todos los routers, ve a Config, Routing, RIP y añade únicamente la nueva red: 10.3.0.0. Prueba ahora a hacer pings desde varios PC de varias subredes a un equipo de la red nueva, y al cabo de unos instantes, debería funcionar, aunque no hayas rellenado la tabla del router nuevo.

¿Qué comando CLI se ha ejecutado al añadir una fila en la sección RIP de cada router?

```
network 10.3.0.0    (que internamente se traduce a network 10.0.0.0)
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

Ejercicio 1: Direcciones IPv4 (puntos 1.1 a 1.5 de la unidad)

a) Para cada una de las siguientes IP, pasa el primer byte a binario e indica su clase (A, B o C):

- 10.0.3.2: 00001010 (A)
- 128.45.7.1: 1000000 (B)
- 192.200.5.4: 11000000 (C)
- 215.23.32.50: 11010111 (C)
- 147.50.3.2: 10010011 (B)
- 100.90.80.70: 01100100 (A)

b) Escribe la IP anterior y siguiente de cada dirección de la tabla. Ten en cuenta que el rango de números en cada una de las cuatro cifras de una IP oscila entre el 0 y el 255. Si te resulta complicado, se hace de manera similar a los minutos y segundos en un reloj, que varían entre el 0 y el 59, y, por ejemplo, el “siguiente” de 13:25:59 es 13:26:00 (es decir, ponemos un 0 en los segundos, no un 60, y aumentamos una unidad los minutos).

Anterior	Dirección IP	Siguiente
<u>45.21.89.37</u>	<u>45.21.89.38</u>	<u>45.21.89.39</u>
<u>37.20.239.254</u>	<u>37.20.239.255</u>	<u>37.20.240.0</u>
<u>119.42.77.255</u>	<u>119.42.78.0</u>	<u>119.42.78.1</u>
<u>2.255.255.255</u>	<u>3.0.0.0</u>	<u>3.0.0.1</u>
<u>40.0.0.254</u>	<u>40.0.0.255</u>	<u>40.0.1.0</u>
<u>140.0.39.254</u>	<u>140.0.39.255</u>	<u>140.0.40.0</u>
<u>140.0.255.254</u>	<u>140.0.255.255</u>	<u>140.1.0.0</u>
<u>52.26.1.255</u>	<u>52.26.2.0</u>	<u>52.26.2.1</u>
<u>10.20.255.254</u>	<u>10.20.255.255</u>	<u>10.21.0.0</u>
<u>100.89.255.255</u>	<u>100.90.0.0</u>	<u>100.90.0.1</u>

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

130.20.0.254	130.20.0.255	130.20.1.0
215.40.254.255	215.40.255.0	215.40.255.1
5.255.255.254	5.255.255.255	6.0.0.0
190.38.200.254	190.38.200.255	190.38.201.0
127.255.255.255	128.0.0.0	128.0.0.1
191.255.255.254	191.255.255.255	192.0.0.0

c) Colorea en rojo, amarillo o verde cada celda de la tabla del apartado b) según sean IP de clase A, B o C.

d) Pon en negrita la parte de red y subraya la parte de host de cada IP de la tabla del apartado b)

e) ¿Cuáles de las siguientes IP **no** pueden ser asignadas a un dispositivo? ¿Por qué?

- 150.100.255.255 NO (es de broadcast, tiene a 1 toda la parte de host)
- 175.100.255.18
- 195.234.253.0 NO (es de red, tiene a 0 toda la parte de host)
- 100.0.0.23
- 188.258.221.176 NO (no puede haber n.º mayor que 255)
- 127.34.25.189 NO (es de loopback, ya que todo el rango 127.x.x.x está reservado para loopback aunque solo se use 127.0.0.1)
- 224.156.217.73 NO (es de clase D)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

f) Completa la tabla:

IP	Clase	N.º bits red	N.º bits host	N.º máximo de hosts que caben en la red	Máscara por defecto	Máscara (formato CIDR)	Dirección de red	Dirección de difusión	Rango de IP válidas (desde X.X.X.X hasta Y.Y.Y.Y)
216.14.55.137	C	24	8	254 ($2^8 - 2$)	255.255.255.0	/24	216.14.55.0	216.14.55.255	Desde 216.14.55.1 hasta 216.14.55.254
123.1.1.15	A	8	24	$2^{24} - 2$	255.0.0.0	/8	123.0.0.0	123.255.255.255	Desde 123.0.0.1 hasta 123.255.255.254
150.127.221.244	B	16	16	$2^{16} - 2$	255.255.0.0	/16	150.127.0.0	150.127.255.255	Desde 150.127.0.1 hasta 150.127.255.254
194.125.35.199	C	24	8	$2^8 - 2$	255.255.255.0	/24	194.125.35.0	194.125.35.255	Desde 194.125.35.1 hasta 194.125.35.254
175.12.239.244	B	16	16	$2^{16} - 2$	255.255.0.0	/16	175.12.0.0	175.12.255.255	Desde 175.12.0.1 hasta 175.12.255.254
18.43.9.147	A	8	24	$2^{24} - 2$	255.0.0.0	/8	18.0.0.0	18.255.255.255	Desde 18.0.0.1 hasta 18.255.255.254
97.46.22.135	A	8	24	$2^{24} - 2$	255.0.0.0	/8	97.0.0.0	97.255.255.255	Desde 97.0.0.1 hasta 97.255.255..254
203.0.7.x	C	24	8	$2^8 - 2$	255.255.255.0	/24	203.0.7.0	203.0.7.255	Desde 203.0.7.1 hasta 203.0.7.254
56.x.x.x	A	8	24	$2^{24} - 2$	255.0.0.0	/8	56.0.0.0	56.255.255.255	Desde 56.0.0.1 hasta 56.255.255.254
(cualquier IP de clase B)	B	16	16	$2^{16} - 2$	255.255.0.0	/16	(depende de la IP escogida)	(depende de la IP escogida)	(dependen de la IP escogida)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

(cualquier IP de clase C)	C	24	8	2^8-2	255.255.255.0	/24	(depende de la IP escogida)	(depende de la IP escogida)	(dependen de la IP escogida)
(cualquier IP de clase A)	A	8	24	$2^{24}-2$	255.0.0.0	/8	(depende de la IP escogida)	(depende de la IP escogida)	(dependen de la IP escogida)
(cualquier IP de clase B)	B	16	16	$2^{16}-2$	255.255.0.0	/16	(depende de la IP escogida)	(depende de la IP escogida)	(dependen de la IP escogida)
(cualquier IP de clase C)	C	24	8	2^8-2	255.255.255.0	/24	(depende de la IP escogida)	(depende de la IP escogida)	(dependen de la IP escogida)
La IP de tu PC (escríbela)									

Ejercicio 2: Subnetting (punto 1.6 de la unidad)

a) Los números que ves en la siguiente tabla son muy comunes al trabajar con máscaras de subred en IPv4. Completa la tabla:

Binario	Decimal
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

b) Completa también la siguiente tabla, con la equivalencia entre máscaras expresadas como direcciones IP y como CIDR:

Máscara (dir. IP)	Máscara (CIDR)
255.0.0.0	/8
255.192.0.0	/10
255.255.192.0	/18
255.255.255.0	/24
255.255.255.224	/27

c) Crea 8 subredes para la red 192.168.30.0. Como es el primer ejercicio que haces de subnetting, iremos paso a paso:

- La clase de la IP es C.
- Sin subredes, la parte de red ocuparía 24 bits y la parte de host ocuparía el resto, o sea, 8 bits.
- Como queremos hacer 8 subredes, necesitamos 3 bits para hacer las 8 combinaciones posibles.
- Por tanto, con subredes, la parte de red ocupa 24 bits, la parte de subred ocupa 3 bits y la parte de host ocupa 5 bits.
- La máscara de subred será 255.255.255.224 (o /27 usando CIDR).

Completa la siguiente tabla, usando binario para las partes de subred y host. No es necesario que coloreaes cada elemento. Puedes mezclar decimal y binario para aclararte, aunque indica siempre al final la dirección IP totalmente en decimal (entre paréntesis).

N.º subred	Dirección de subred	Dirección de broadcast
<u>000</u>	192.168.30. <u>000 00000</u> (192.168.30.0)	192.168.30. <u>000 11111</u> (192.168.30.31)
<u>001</u>	192.168.30. <u>001 00000</u> (192.168.30.32)	192.168.30. <u>001 11111</u> (192.168.30.63)
<u>010</u>	192.168.30. <u>010 00000</u> (192.168.30.64)	192.168.30. <u>010 11111</u> (192.168.30.95)
<u>011</u>	192.168.30. <u>011 00000</u> (192.168.30.96)	192.168.30. <u>011 11111</u> (192.168.30.127)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

100	192.168.30.100 00000 (192.168.30.128)	192.168.30.100 11111 (192.168.30.159)
101	192.168.30.101 00000 (192.168.30.160)	192.168.30.101 11111 (192.168.30.191)
110	192.168.30.110 00000 (192.168.30.192)	192.168.30.110 11111 (192.168.30.223)
111	192.168.30.111 00000 (192.168.30.224)	192.168.30.111 11111 (192.168.30.255)

Recuerda:

- En una dirección de subred, la parte de **host** está totalmente a 0.
- En una dirección de broadcast, la parte de **host** está totalmente a 1.

Repite la tabla, ahora solamente con todos los nº completamente en decimal:

N.º subred	Dirección de subred	Dirección de broadcast
0	192.168.30.0	192.168.30.31
1	192.168.30.32	192.168.30.63
2	192.168.30.64	192.168.30.95
3	192.168.30.96	192.168.30.127
4	192.168.30.128	192.168.30.159
5	192.168.30.160	192.168.30.191
6	192.168.30.192	192.168.30.223
7	192.168.30.224	192.168.30.255

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

Finalmente, incluye el rango de IP válido para cada subred:

N.º subred	Dirección de subred	Rango de IP válidas	Dirección de broadcast
0	192.168.30.0	Desde 192.168.30.1 hasta 192.168.30.30	192.168.30.31
1	192.168.30.32	Desde 192.168.30.33 hasta 192.168.30.62	192.168.30.63
2	192.168.30.64	Desde 192.168.30.65 hasta 192.168.30.94	192.168.30.95
3	192.168.30.96	Desde 192.168.30.97 hasta 192.168.30.126	192.168.30.127
4	192.168.30.128	Desde 192.168.30.129 hasta 192.168.30.158	192.168.30.159
5	192.168.30.160	Desde 192.168.30.161 hasta 192.168.30.190	192.168.30.191
6	192.168.30.192	Desde 192.168.30.193 hasta 192.168.30.222	192.168.30.223
7	192.168.30.224	Desde 192.168.30.225 hasta 192.168.30.254	192.168.30.255

d) Completa las siguientes tablas con tantas filas como sea necesario, escribiendo también la máscara para cada caso. Puedes mezclar inicialmente binario y decimal para calcular los números, pero entrega las tablas únicamente con n.º decimales:

- 150.40.0.0/18. Máscara de subred = 255.255.192.0

Network Address	Usable Host Range	Broadcast Address:
150.40.0.0	150.40.0.1 - 150.40.63.254	150.40.63.255
150.40.64.0	150.40.64.1 - 150.40.127.254	150.40.127.255
150.40.128.0	150.40.128.1 - 150.40.191.254	150.40.191.255
150.40.192.0	150.40.192.1 - 150.40.255.254	150.40.255.255

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

- 120.0.0.0/10. Máscara de subred = 255.192.0.0

Network Address	Usable Host Range	Broadcast Address:
120.0.0.0	120.0.0.1 - 120.63.255.254	120.63.255.255
120.64.0.0	120.64.0.1 - 120.127.255.254	120.127.255.255
120.128.0.0	120.128.0.1 - 120.191.255.254	120.191.255.255
120.192.0.0	120.192.0.1 - 120.255.255.254	120.255.255.255

- 174.23.0.0/19. Máscara de subred = 255.255.224.0

Network Address	Usable Host Range	Broadcast Address:
174.23.0.0	174.23.0.1 - 174.23.31.254	174.23.31.255
174.23.32.0	174.23.32.1 - 174.23.63.254	174.23.63.255
174.23.64.0	174.23.64.1 - 174.23.95.254	174.23.95.255
174.23.96.0	174.23.96.1 - 174.23.127.254	174.23.127.255
174.23.128.0	174.23.128.1 - 174.23.159.254	174.23.159.255
174.23.160.0	174.23.160.1 - 174.23.191.254	174.23.191.255
174.23.192.0	174.23.192.1 - 174.23.223.254	174.23.223.255
174.23.224.0	174.23.224.1 - 174.23.255.254	174.23.255.255

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

- 195.4.102.0/27. Máscara de subred = 255.255.255.224

Network Address	Usable Host Range	Broadcast Address:
195.4.102.0	195.4.102.1 - 195.4.102.30	195.4.102.31
195.4.102.32	195.4.102.33 - 195.4.102.62	195.4.102.63
195.4.102.64	195.4.102.65 - 195.4.102.94	195.4.102.95
195.4.102.96	195.4.102.97 - 195.4.102.126	195.4.102.127
195.4.102.128	195.4.102.129 - 195.4.102.158	195.4.102.159
195.4.102.160	195.4.102.161 - 195.4.102.190	195.4.102.191
195.4.102.192	195.4.102.193 - 195.4.102.222	195.4.102.223
195.4.102.224	195.4.102.225 - 195.4.102.254	195.4.102.255

- 77.0.0.0/11. Máscara de subred = 255.224.0.0

Network Address	Usable Host Range	Broadcast Address:
77.0.0.0	77.0.0.1 - 77.31.255.254	77.31.255.255
77.32.0.0	77.32.0.1 - 77.63.255.254	77.63.255.255
77.64.0.0	77.64.0.1 - 77.95.255.254	77.95.255.255
77.96.0.0	77.96.0.1 - 77.127.255.254	77.127.255.255
77.128.0.0	77.128.0.1 - 77.159.255.254	77.159.255.255
77.160.0.0	77.160.0.1 - 77.191.255.254	77.191.255.255
77.192.0.0	77.192.0.1 - 77.223.255.254	77.223.255.255
77.224.0.0	77.224.0.1 - 77.255.255.254	77.255.255.255

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

- 200.3.48.0 con sólo las 6 primeras subredes. Máscara de subred = 255.255.255.224

Network Address	Usable Host Range	Broadcast Address:
200.3.48.0	200.3.48.1 - 200.3.48.30	200.3.48.31
200.3.48.32	200.3.48.33 - 200.3.48.62	200.3.48.63
200.3.48.64	200.3.48.65 - 200.3.48.94	200.3.48.95
200.3.48.96	200.3.48.97 - 200.3.48.126	200.3.48.127
200.3.48.128	200.3.48.129 - 200.3.48.158	200.3.48.159
200.3.48.160	200.3.48.161 - 200.3.48.190	200.3.48.191

- 25.0.0.0 con sólo las 3 primeras subredes. Máscara de subred = 255.192.0.0

Network Address	Usable Host Range	Broadcast Address:
25.0.0.0	25.0.0.1 - 25.63.255.254	25.63.255.255
25.64.0.0	25.64.0.1 - 25.127.255.254	25.127.255.255
25.128.0.0	25.128.0.1 - 25.191.255.254	25.191.255.255

e) Indica, para cada apartado, si las IP pertenecen a la misma subred o no:

- 145.53.29.12 y 145.53.34.15, con máscara /19
Ejemplo: es de clase B. Red=16 bits, subred=3 bits (ya que 19-16=3), host=13 bits. Como 29 es 00011101 y 34 es 00100010, pertenecen a subredes diferentes.
- 145.53.29.12 y 145.53.34.15, con máscara 255.255.240.0
29=00011101, 34=00100010, Diferentes subredes

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

- 10.7.2.15 y 10.38.43.59, con máscara /12
7=00000111, 38=00100110, Diferentes subredes
- 10.7.2.15 y 10.38.43.59, con máscara /10
7=00000111, 38=00100110, Misma subred
- 215.134.220.99 y 215.134.220.105, con máscara /27
99=01100011, 105=01101001, Misma subred
- 215.134.220.99 y 215.134.220.105, con máscara 255.255.255.252
99=01100011, 105=01101001, Diferentes subredes
- 29.45.67.124 y 29.138.100.49, con máscara /17
45=00101101, 138=10001010, Diferentes subredes
- 195.42.27.90, 195.42.27.100 y 195.42.27.105, con máscara /29
90=01011010, 100=01100100, 105=01101001, Diferentes subredes

f) Indica, para cada IP, a qué subred pertenece (la 0, la 1, la 2, etc), sabiendo que se usa la máscara /27:

192.168.0.10, 192.168.0.20, 192.168.0.90, 192.168.0.107, 192.168.0.58, 192.168.0.153, 192.168.0.64, 192.168.0.99, 192.168.0.159

Ejemplo: 192.168.0.10 es de clase C, luego red=24 bits, subred=27-24=3 bits, host=5 bits.

Por tanto, 192.168.0.10=192.168.0.00001010. Pertenece a la subred 000, es decir, la 0.

10=00001010 (subred 0), 20=00010100 (subred 0), 90=01011010 (subred 2), 107=01101011 (subred 3), 58=00111010 (subred 1), 153=10011001 (subred 4), 64=01000000 (subred 2), 99=01100011 (subred 3), 159=10011111 (subred 4)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

g) Indica una máscara de subred para cada apartado de manera que ambas IP pertenezcan a la misma subred:

- 20.7.5.3 y 20.4.2.9

Ejemplo: por ser de clase A, red=8 bits, subred=? bits, host=? bits

No sabemos la parte de subred y host, pero se nos dice que han de pertenecer a la misma subred, por tanto, la parte de subred debe ser la misma. Si pasamos a binario:

20.7.5.3=20.00000111.00000101.00000011

20.4.2.9=20.00000100.00000010.00001001

Se ha coloreado la parte que tienen en común, es decir, 6 bits. Por tanto la máscara será /14 (ya que 8 (red)+6 (subred)=14).

- 140.29.57.228 y 140.29.52.130, 57=00111001, 52=00110100, /20
- 215.34.22.16 y 215.34.22.94, 16=00010000, 94=01011110, /25
- 173.25.41.38 y 173.25.120.12, 41=00101001, 120=01111000, /17
- 92.15.113.26 y 92.24.0.28, 15=00001111, 24=00011000, /11

h) En la red 192.168.1.0 necesitas crear tantas subredes como puedas, de manera que cada subred tenga 30 equipos como máximo. Indica la máscara que usarías para conseguirlo, así como cuántas subredes crearías.

Pista: No se nos dice la parte de subred, pero indirectamente sí se nos indica la parte de host (30 equipos... ¿cuántos bits hacen falta para tener 30 combinaciones distintas?). Teniendo los bits de red y host, podemos deducir los bits para la parte de subred. Con eso, obtener la máscara y cuántas subredes hay es inmediato.

Clase C, Red=24 bits, host=5 bits (queremos 30 equipos, necesitamos 5 bits), subred=3 bits. Máscara=/27 (8 subredes)

i) Las subredes del apartado anterior crecen y ahora han de soportar hasta 50 equipos en cada subred. Indica la nueva máscara que usarías.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

50 equipos, necesitamos 6 bits para host, nos quedan 2 bits para subred. Máscara=/26

j) Supongamos que en una empresa (red 10.0.0.0) se quieren crear 3 subredes (planta baja, primer piso y segundo piso). ¿Qué máscara usarías? Indica el reparto de IP de cada subred en una tabla como las del ejercicio 2d.

Network Address	Usable Host Range	Broadcast Address:
10.0.0.0	10.0.0.1 - 10.63.255.254	10.63.255.255
10.64.0.0	10.64.0.1 - 10.127.255.254	10.127.255.255
10.128.0.0	10.128.0.1 - 10.191.255.254	10.191.255.255

La máscara sería /10.

Sin embargo, ya que en las IP de clase A tenemos 3 bytes libres para subred y host, también podríamos haberlo hecho así usando /16:

Dirección de subred	Rango de IP válidas	Dirección de difusión
10.0.0.0	Desde 10.0.0.1 hasta 10.0.255.254	10.0.255.255
10.1.0.0	Desde 10.1.0.1 hasta 10.1.255.254	10.1.255.255
10.2.0.0	Desde 10.2.0.1 hasta 10.2.255.254	10.2.255.255

De este modo, los rangos numéricos salen más fáciles para repartir, incluso viendo una IP sabemos inmediatamente a qué subred pertenece sin necesidad de realizar cálculos. Inconveniente: desperdiciamos más IP.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

k) Dada la red 170.20.0.0/19, clasifica estas IP como válidas, broadcast o direcciones de subred:

170.20.96.7, 170.20.154.254, 170.20.191.254, 170.20.96.0, 170.20.97.0, 170.20.38.255, 170.20.159.255, 170.20.192.1, 170.20.125.0

Como máscara=/19, red: 16 bits, subred: 3 bits, host: 13 bits

Dir. Subred: aquella IP que tiene toda la parte de host a 0.

Dir. Difusión: aquella IP que tiene toda la parte de host a 1.

Válidas: no son de subred ni de difusión

96.7=01100000.00000111, válida

154.254=10011010.11111110, válida

191.254=10111111.11111110, válida

96.0=01100000.00000000, dir.subred

97.0=01100001.00000000, válida

38.255=00100110.11111111, válida

159.255=10011111.11111111, dir. difusión

192.1=11000000.00000001, válida

125.0=01111101.00000000, válida

Pista: recuerda que dirección de broadcast es aquella que tiene toda la parte de host a 1 y dirección de subred es aquella que tiene toda la parte de host a 0. El resto son IP válidas para equipos.

l) Indica la máscara de subred CIDR más apropiada para cada una de estas situaciones (siempre que sea posible encontrar una):

- Queremos 4 subredes con 40 equipos cada una usando IP de clase C. Máscara: /26

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

Ejemplo: es de clase C (por tanto, 24 bits para red), hay 4 subredes (por tanto, necesitamos 2 bits para subred para poder hacer las 4 combinaciones diferentes). El resto serían $32-24-2=6$ bits. Con 6 bits podemos hacer hasta $2^6=64$ combinaciones, luego sí que es posible que quepan 40 equipos. La máscara sería /26.

- Queremos 10 subredes con 400 equipos cada una usando IP de clase B. Máscara: /20
- Queremos 6 subredes con 50 equipos cada una usando IP de clase C. Máscara: Imposible
- Queremos 20 subredes con 200 equipos cada una usando IP de clase A. Máscara: /13
- Queremos 7 subredes con 30 equipos cada una usando IP de clase B. Máscara: /19
- Queremos 4 subredes con 500 equipos cada una usando IP de clase A. Máscara: /10
- Queremos 4 subredes con 52 equipos cada una usando IP de clase C. Máscara: /26
- Queremos 15 subredes con 40 equipos cada una usando IP de clase A. Máscara: /12

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

Ejercicio 3: Supernetting (punto 1.7 de la unidad)

Realiza supernetting de cada uno de estos grupos de subredes, siempre que sea posible. Cuando puedas hacer supernetting indica la IP y máscara de la supernet resultante:

- 150.12.0.0/16, 150.13.0.0/16, 150.14.0.0/16 y 150.15.0.0/16 → 150.12.0.0/14
- 172.19.0.0/16, 172.20.0.0/16 y 172.21.0.0/16 → No es posible, ya que son 3 direcciones
- 172.16.169.0/24, 172.16.170.0/24 y 172.16.171.0/24 → No es posible, ya que son 3 direcciones
- 200.198.48.0/24, 200.198.52.0/24, 200.198.56.0/24 y 200.198.60.0/24 → No es posible, ya que los n.º no son consecutivos
- 210.6.0.0/24, 210.6.1.0/24, 210.6.2.0/24 y 210.6.3.0/24 → 210.6.0.0/22
- 210.6.2.0/24, 210.6.3.0/24, 210.6.4.0/24 y 210.6.5.0/24 → No es posible, ya que 2 no es múltiplo de 4
- 210.6.2.0/24 y 210.6.3.0/24 → 210.6.2.0/23

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

Ejercicio 4: VLSM (punto 1.8 de la unidad)

a) Dada la red 192.168.0.0, escribe las direcciones de subred, las máscaras y los rangos de IP válidos para crear una subred con 20 equipos, otra con 80, otra más con 20 y tres subredes con 2 equipos cada una. Es decir, obtén la tabla completa correspondiente usando VLSM.

Needed Size	Address	Mask	Assignable Range	Broadcast
80	192.168.0.0	/25	192.168.0.1 - 192.168.0.126	192.168.0.127
20	192.168.0.128	/27	192.168.0.129 - 192.168.0.158	192.168.0.159
20	192.168.0.160	/27	192.168.0.161 - 192.168.0.190	192.168.0.191
2	192.168.0.192	/30	192.168.0.193 - 192.168.0.194	192.168.0.195
2	192.168.0.196	/30	192.168.0.197 - 192.168.0.198	192.168.0.199
2	192.168.0.200	/30	192.168.0.201 - 192.168.0.202	192.168.0.203

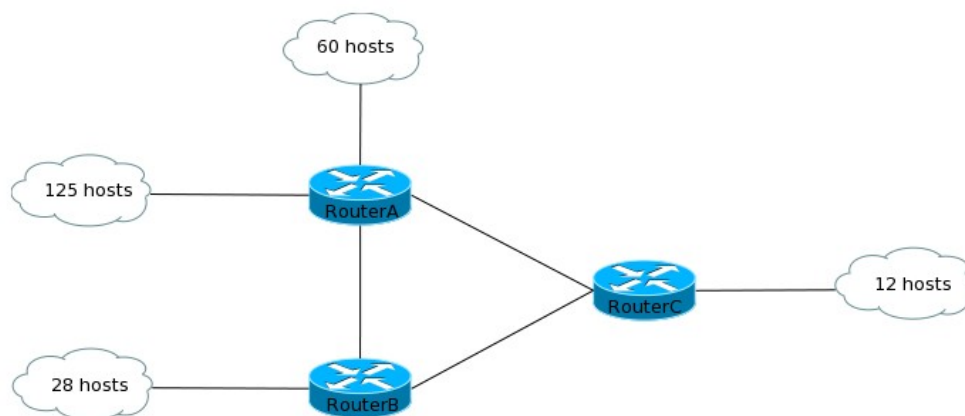
```

Tam  R  SRH  Dir.subred
80   24  1   7  192.168.0. 0 0000000
      (0)
20   24  3   5  192.168.0. 100 00000
      (128)
20   24  3   5  192.168.0. 101 00000
      (160)
2    24  6   2  192.168.0. 110000 00
      (192)
2    24  6   2  192.168.0. 110001 00
      (196)
2    24  6   2  192.168.0. 110010 00
      (200)

```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

b) Dada la red 192.168.10.0, indica en una tabla el rango de IP para cada subred. Ten en cuenta que entre dos routers hay una subred de 2 equipos.

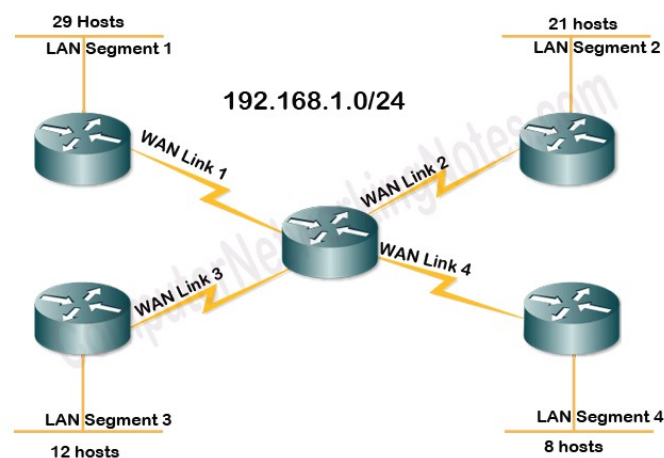


Needed Size	Address	Mask	Assignable Range	Broadcast
125	192.168.10.0	/25	192.168.10.1 - 192.168.10.126	192.168.10.127
60	192.168.10.128	/26	192.168.10.129 - 192.168.10.190	192.168.10.191
28	192.168.10.192	/27	192.168.10.193 - 192.168.10.222	192.168.10.223
12	192.168.10.224	/28	192.168.10.225 - 192.168.10.238	192.168.10.239
2	192.168.10.240	/30	192.168.10.241 - 192.168.10.242	192.168.10.243
2	192.168.10.244	/30	192.168.10.245 - 192.168.10.246	192.168.10.247
2	192.168.10.248	/30	192.168.10.249 - 192.168.10.250	192.168.10.251

Size	Net	SN	Host	Subnet address
125	24	1	7	192.168.10.0 0000000 (0)
60	24	2	6	192.168.10.10 000000 (128)
28	24	3	5	192.168.10.110 00000 (192)
12	24	4	4	192.168.10.1110 0000 (224)
2	24	6	2	192.168.10.111100 00 (240)
2	24	6	2	192.168.10.111101 00 (244)
2	24	6	2	192.168.10.111110 00 (248)

CIPFP Ausiàs March (Valencia)
 1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

c) Realiza el reparto de IP por VLSM para estas subredes, rellenando la tabla adecuada:



Needed Size	Address	Mask	Assignable Range	Broadcast
29	192.168.1.0	/27	192.168.1.1 - 192.168.1.30	192.168.1.31
21	192.168.1.32	/27	192.168.1.33 - 192.168.1.62	192.168.1.63
12	192.168.1.64	/28	192.168.1.65 - 192.168.1.78	192.168.1.79
8	192.168.1.80	/28	192.168.1.81 - 192.168.1.94	192.168.1.95
2	192.168.1.96	/30	192.168.1.97 - 192.168.1.98	192.168.1.99
2	192.168.1.100	/30	192.168.1.101 - 192.168.1.102	192.168.1.103
2	192.168.1.104	/30	192.168.1.105 - 192.168.1.106	192.168.1.107
2	192.168.1.108	/30	192.168.1.109 - 192.168.1.110	192.168.1.111

Size	Net	SN	Host	Subnet address
29	24	3	5	192.168.1.000 00000 (0)
21	24	3	5	192.168.1.001 00000 (32)
12	24	4	4	192.168.1.0100 0000 (64)
8	24	4	4	192.168.1.0101 0000 (80)
2	24	6	2	192.168.1.011000 00 (96)
2	24	6	2	192.168.1.011001 00 (100)
2	24	6	2	192.168.1.011010 00 (104)
2	24	6	2	192.168.1.011011 00 (108)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

Ejercicio 5: Tipos de IP (puntos 1.9 y 1.10 de la unidad)

a) Averigua los siguientes datos del equipo que estás usando actualmente. Pega aquí un pantallazo donde aparezcan los datos.

<div>Cancelar</div>		<div>Cableada</div>		
Detalles	Identidad	IPv4	IPv6	Seguridad
Velocidad de conexión		1000 Mb/s		
Dirección IPv4		10.5.3.183		
Dirección IPv6		fe80::101e:8d6:209b:f88e		
Dirección física		50:65:F3:2A:16:47		
Ruta predeterminada		10.5.3.1		
DNS		8.8.8.8 10.5.3.1		

```
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 50:65:f3:2a:16:47 brd ff:ff:ff:ff:ff:ff
    altname enp0s25
    inet 10.5.3.183/24 brd 10.5.3.255 scope global dynamic noprefixroute eno1
        valid_lft 5676sec preferred_lft 5676sec
    inet6 fe80::101e:8d6:209b:f88e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- Dirección MAC: 50:65:F3:2A:16:47
- Dirección IP: 10.5.3.183
- Máscara: /24 (255.255.255.0)
- Puerta de enlace: 10.5.3.1
- Servidor/es DNS: 8.8.8.8, 10.5.3.1

¿De qué clase es la IP (A/B/C)? A

¿Es estática o dinámica? Dinámica

¿Es pública o privada? Privada

¿Cuál es la dirección **de tu red**? 10.5.3.0

¿Y la dirección de difusión **de tu red**? 10.5.3.255

Viendo la máscara, ¿hay subredes en tu LAN? Sí En caso afirmativo, ¿cuántas? Hasta 2^{16}

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

b) Responde a las mismas preguntas con los datos de otro equipo que esté en tu misma LAN. Colorea en amarillo los datos que cambien respecto a la configuración de tu equipo:

- Dirección MAC: _____
- Dirección IP: _____
- Máscara: _____
- Puerta de enlace: _____
- Servidor/es DNS: _____

c) Averigua la IP privada y la IP pública del router o puerta de enlace de la LAN en la que estás conectado actualmente.

IP privada del router: 10.5.3.1

IP pública del router: 80.36.193.x (obtenida de <https://www.cual-es-mi-ip.net/>)

Tu dirección IP es **80.36.193**  

d) Usando Packet Tracer, crea en un mismo fichero dos LAN diferentes:

- La primera tendrá dos PC conectados a un switch 2960. Asigna IP estáticas a los PC (10.0.0.5 y 10.0.0.7), así como la máscara de subred por defecto. Usando ping, comprueba que hay conexión entre los dos equipos.
- La segunda será una WLAN con dos portátiles y un Home Router inalámbrico, que se encargará de repartir IP a los clientes DHCP. El rango de IP que reparte el servidor será desde la 192.168.0.21 a la 24 (similar a como se hizo en unidades anteriores). El SSID de la WLAN será “PRUEBA”. Recuerda guardar los cambios en el router. Los portátiles deberán conectarse a dicha red

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

(por tanto, deberán tener tarjetas de red inalámbricas) y obtener una IP en el rango adecuado. Usando ping, comprueba que hay conexión entre ellos.

Ahora, apaga el router de la WLAN. Abre una consola en un portátil y teclea el comando `ipconfig /release` para indicar que deseas liberar tu IP. ¿Qué IP tiene ahora el portátil? 0.0.0.0 Teclea `ipconfig /renew` para indicar que quieres obtener una IP. Recuerda que el router sigue apagado. ¿Qué error aparece? "DHCP request failed" Si tecleas ahora `ipconfig`, ¿qué IP tienes? 169.x.x.x Enciende el router. Haz que los portátiles vuelvan a tener una IP del rango que reparte el router (bien esperando a que el router se la reparta o solicitándola explícitamente tecleando `ipconfig /renew` en cada uno). Une ahora las dos redes conectando el switch y el router por cable por sus puertos Gigabit Ethernet. Cambia las IP de los PCs para que ahora se pidan dinámicamente y asegúrate de que ahora ya están repartidas desde la 21 hasta la 24 y que puedes hacer ping desde un PC a un portátil.

e) Responde Sí o No a estas tres cuestiones:

- Viendo una IP, ¿puede saberse su clase? Sí
- Viendo una IP, ¿puede saberse si es pública o privada? Sí
- Viendo una IP, ¿puede saberse si es estática o dinámica? No

Escribe un ejemplo de:

- Una IP de clase B pública: 150.30.20.12
- Una IP estática y privada: 10.1.2.3
- Una IP pública y dinámica: 80.58.35.40
- Una IP de clase C estática y pública: 200.6.9.58
- Una IP de clase A dinámica y privada: 10.9.8.7
- Un rango de IP de clase A dinámicas y públicas: desde 50.1.2.3 hasta 50.8.8.9

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

f) Averigua las IP públicas de estos equipos. Puedes hacerlo mediante el comando ping (por ejemplo: ping www.google.es), o, si los pings no responden, con Wireshark (aplicando un filtro para ver consultas y respuestas DNS):

www.google.es. IP pública: 142.250.200.67

www.elmundo.es IP pública: 199.232.193.50

www.elpais.es IP pública: 52.209.61.111

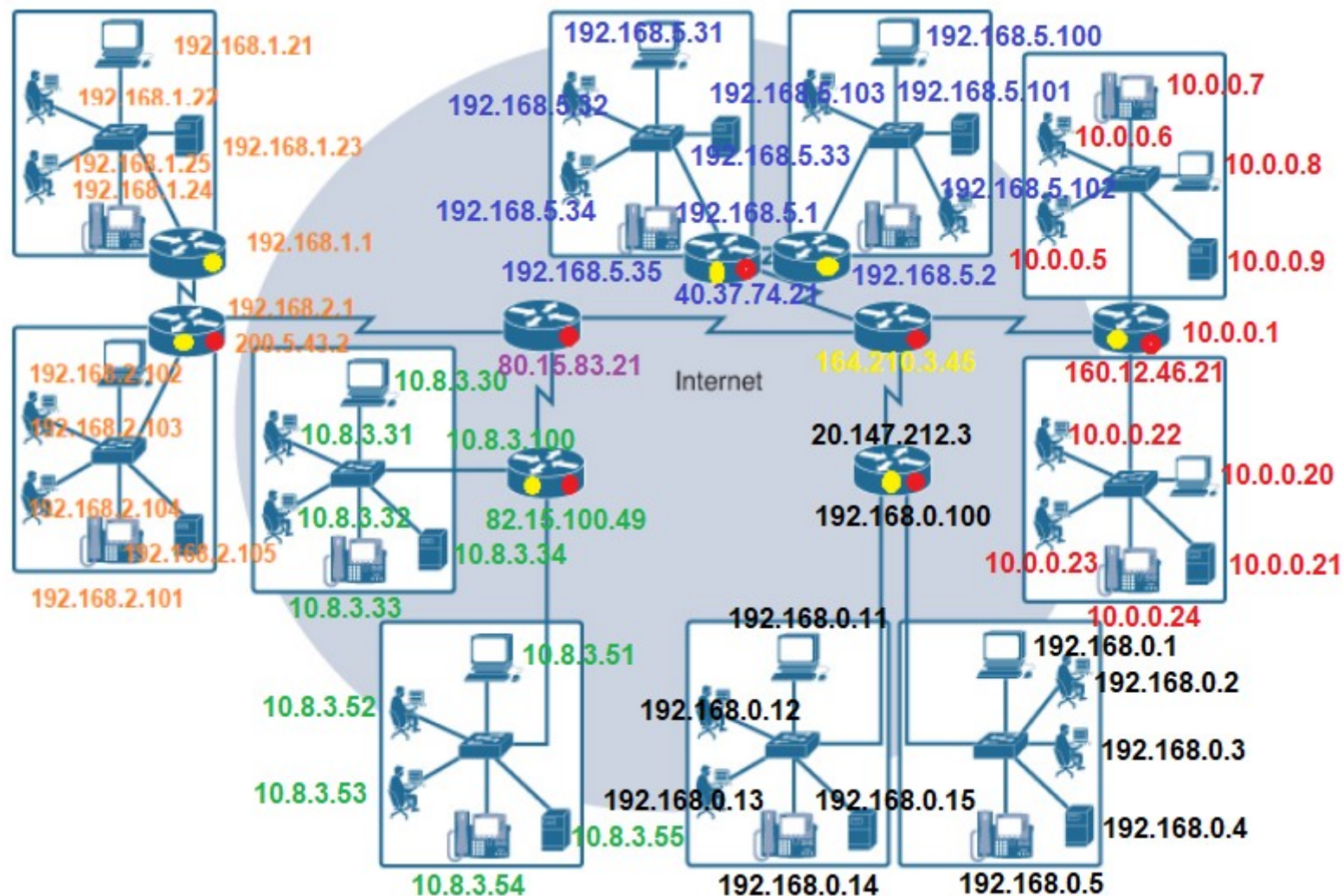
aules.edu.gva.es IP pública: 213.0.87.122

(Puede que hayas obtenido IP diferentes)

g) Edita la siguiente imagen y añade IP a **todos** los dispositivos como se te indica:

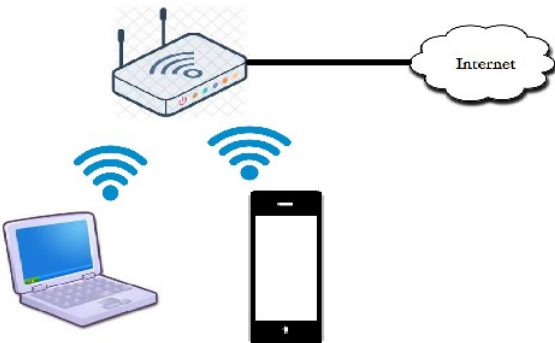

- A cada router que está en contacto con el exterior (marcados con puntos rojos), una IP pública
- A cada router dentro de una LAN (marcados con puntos amarillos), una IP privada (usa en algunas ocasiones IP privadas de clase A y en otras de clase C)
- A cada equipo dentro de una LAN, una IP privada (del mismo rango que el router de esa red)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

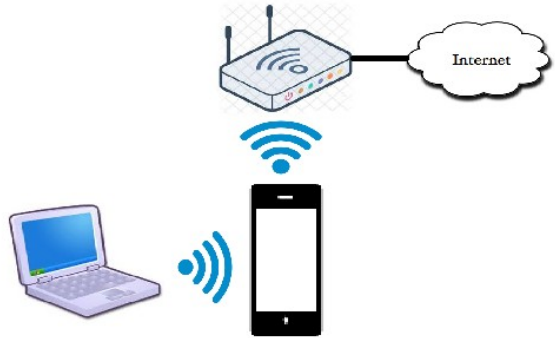


CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

h) Asigna IP de clase C (privadas: 192.168.x.x o públicas: 200.x.x.x) a los dispositivos de cada ejemplo:

	<p>Portátil y móvil conectados a un router inalámbrico</p>	<p>Portátil: IP= 192.168.1.7 Puerta de enlace= 192.168.1.1 Móvil: IP=192.168.1.10 Puerta de enlace= 192.168.1.1 Router: IP privada= 192.168.1.1 IP pública= 200.5.3.9</p>
	<p>Portátil conectado a Internet a través de la conexión 4G/5G de un móvil</p>	<p>Portátil: IP= 192.168.1.10 Puerta de enlace= 192.168.1.1 Móvil: IP privada= 192.168.1.1 IP pública= 200.4.3.2</p>

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

	<p>Portátil conectado a un móvil que está conectado a un router</p>	<p>Portátil: IP= 192.168.1.10 Puerta de enlace= 192.168.1.1 Móvil: IP privada 1=192.168.1.1 IP privada 2= 192.168.3.9 Puerta de enlace= 192.168.3.1 Router: IP privada=192.168.3.1 IP pública= 200.5.4.9</p>
---	---	--

Ejercicio 6: NAT (punto 1.11 de la unidad)

a) ¿Verdadero o falso?

- En el NAT estático o SNAT, cada IP privada siempre es traducida a la misma IP pública, única para cada equipo
- Tanto en el NAT estático como en el dinámico se necesita disponer de varias IP públicas contradas
- PAT usa el n.º de puerto para distinguir las conexiones, ya que todas salen al exterior con la misma IP pública
- La principal ventaja de usar NAT es que podemos conectar un n.º grande de equipos a Internet usando un n.º reducido de IP públicas
- El tipo de NAT más usado es el DNAT
- Cuando un paquete sale fuera de la LAN, el router solo ha de cambiar la IP origen en el paquete

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

b) Supongamos que una LAN usa el rango de IP privadas 192.168.1.5 a 192.168.1.10. Traduce las siguientes IP privadas a su correspondiente IP pública cuando se envían paquetes al exterior. Cada tipo de NAT es independiente del anterior.

- NAT estático con el rango de IP públicas 200.13.42.5 a 200.13.42.10, usando el mismo cuarto número que la IP interna:

IP origen antes del router: 192.168.1.7
IP origen después del router: 200.13.42.7

IP origen antes del router: 192.168.1.5
IP origen después del router: 200.13.42.5

IP origen antes del router: 192.168.1.10
IP origen después del router: 200.13.42.10

- NAT dinámico con el rango de IP públicas 200.13.42.5 a 200.13.42.10 (sabiendo que la 200.13.42.6 está ocupada):

IP origen antes del router: 192.168.1.7
IP origen después del router: 200.13.42.9

IP origen antes del router: 192.168.1.6
IP origen después del router: 200.13.42.5

IP origen antes del router: 192.168.1.9
IP origen después del router: 200.13.42.8

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

- PAT usando la IP pública 200.13.42.5:

IP y puerto origen antes del router: 192.168.1.7:42316
IP y puerto origen después del router: 200.13.42.5:42316

IP y puerto origen antes del router: 192.168.1.8:13542
IP y puerto origen después del router: 200.13.42.5:13542

IP y puerto origen antes del router: 192.168.1.5:9842
IP y puerto origen después del router: 200.13.42.5:9842

Ejercicio 7: IPv6 (punto 2 de la unidad)

a) Señala cuáles de las siguientes IPv6 son incorrectas:

- 2001:db8:123:ab:b450:0:4de3:b24
- 2001:db8:f0::3d0:ff
- 20:8:f3c::a2::23 Incorrecta (se ha usado dos veces el ::)
- ab43:e3e3:24a:123a:5324:1e:2ae1 Incorrecta (hay 7 grupos y debería haber 8)
- 53::35e:e2e3:21
- 872a:1237:a:e:231:948:af10e:4 Incorrecta (hay un grupo demasiado largo, af10e, cada grupo son 16 bits)
- ::1

b) Simplifica las siguientes IPv6 tanto como puedas:

- 2001:0db8:0000:0000:0000:0000:0c50 → 2001:db8::c50
- 2001:0db8:0000:0000:b450:0000:0000:00b4 → 2001:db8::b450:0:0:b4 o también 2001:db8:0:0:b450::b4
- 2001:0db8:00f0:0000:0000:03d0:0000:00ff → 2001:db8:f0::3d0:0:ff
- 2001:0db8:0f3c:00d7:7dab:03d0:0000:00ff → 2001:db8:f3c:d7:7dab:3d0:0:ff

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

c) Dadas las siguientes capturas de cabeceras IPv6, completa las tablas con la información adecuada. En el caso de las IP origen y destino, escríbelas simplificadas (usando ::) siempre que puedas:

0000	22 1a 95 d6 7a 23 86 93	23 d3 37 8e 86 dd 60 0d	"...z#... #7...`.
0010	68 4a 00 7d 06 40 fc 00	00 02 00 00 00 02 00 00	hJ·}·@·.....
0020	00 00 00 00 00 01 fc 00	00 02 00 00 00 01 00 00
0030	00 00 00 00 00 01 a9 a0	1f 90 02 1b 63 8d ba 31c·1

Campo	Longitud en bits	Valor
Versión	4	6
Traffic Class	8	00
Flow label	20	d684a
Payload length	16	007d
Next header	8	06
Hop limit	8	40
IPv6 origen	128	FC00:2:0:2::1
IPv6 destino	128	FC00:2:0:1::1

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

```

0020  80 54 c0 58 63 01 46 37 d5 d3 60 00 00 00 04 d0  ·T·Xc·F7· ······
0030  06 3c 20 01 48 60 00 00 20 01 00 00 00 00 00  ·<·H`· ······
0040  00 68 20 02 46 37 d5 d3 00 00 00 00 00 00 46 37  ·h·F7· ······F7
0050  d5 d3 00 50 05 07 3a c0 12 1d 22 ec 58 2e 50 10  ···P· ·· ··"·X·P·

```

Campo	Longitud en bits	Valor
Versión	4	6
Traffic Class	8	00
Flow label	20	00000
Payload length	16	04d0
Next header	8	06
Hop limit	8	3c
IPv6 origen	128	2001:4860:0:2001::68
IPv6 destino	128	2002:4637:d5d3::4637:d5d3

d) Escribe los filtros Wireshark (formato "ipv6.campo" como en las unidades 5 y 6) para obtener los paquetes adecuados:

- Paquetes IPv6 enviados a tu ordenador (en ipconfig aparece tu IPv6) → `ipv6.dst=="mi IPv6"`
- Paquetes IPv6 enviados por tu ordenador con TTL mayor que 10 → `ipv6.src=="mi IPv6" && ipv6.hlim>10`
- Paquetes IPv6 con zona de datos entre 500 y 1000 → `ipv6.plen>500 && ipv6.plen<1000`
- Paquetes IPv6 que no usan TCP en la capa de transporte → `ipv6.nxt!=6`

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 7: Asignación de direcciones IP

e) ¿Verdadero o falso?

- La cabecera IPv6 siempre tiene la misma longitud: 40 bytes
- Una dirección IPv6 ocupa cuatro veces más que una IPv4
- El checksum sigue estando como un campo dentro de la cabecera IPv6
- Tanto TTL (IPv4) como Hop Limit (IPv6) se usan para lo mismo: evitar que los paquetes estén viajando indefinidamente
- Tanto Protocol (IPv4) como Next Header (IPv6) se usan para lo mismo: indicar el protocolo del nivel de red

Ejercicio 8: Práctica: Configuración de routers

Usando el router de la unidad 5 (el TL-WR1043ND, versión 4) disponible en <https://www.tp-link.com/en/support/emulator/>, adjunta pantallazos donde aparezcan las siguientes opciones:

- Averiguar la IPv4 privada del router → Status
- Cambiar la IPv4 privada del router → Network, LAN
- Indicar el rango de IP y la puerta de enlace que reparte el servidor DHCP → DHCP, DHCP settings
- Averiguar los clientes que actualmente tienen asignada una IP por DHCP → DHCP, DHCP client list
- Reservar, para una MAC concreta, la misma IP (reparto semidinámico) → DHCP, address reservation
- Configurar NAT → NAT boost
- Ver la tabla de encaminamiento del router → Advanced routing, System routing table
- Añadir filas a la tabla de encaminamiento estático del router → Advanced routing, Static routing list
- Averiguar la dirección IPv6 del router → IPv6 support, IPv6 status

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

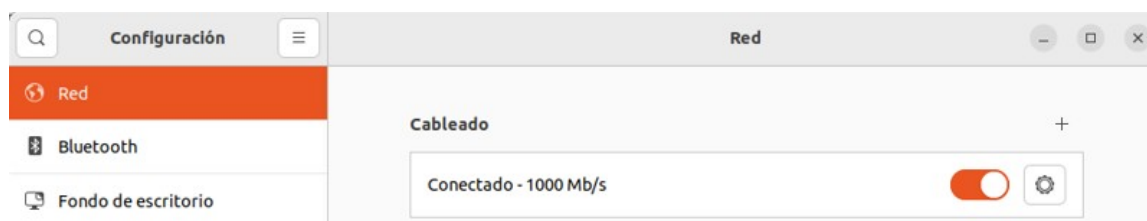
Ejercicio 1: DHCP

a) Para entender el funcionamiento interno del protocolo DHCP y cómo se comunican clientes y servidores, vas a capturar paquetes DHCP empleando Wireshark. En primer lugar, recuerda que, como ahora tienes conexión a la red y dirección IP, el proceso DHCP ya ha finalizado, por lo que debemos forzar al ordenador para que solicite de nuevo una IP al servidor. **Ten en cuenta que durante la ejecución de esta práctica, vas a perder la conexión a la red momentáneamente.**

Abre Wireshark e inicia una captura de paquetes. Mientras capturas, desde la consola de Windows (comando cmd) teclea `ipconfig /release`. Este comando fuerza al equipo a liberarse de su IP, pasando entonces a tener la dirección especial 0.0.0.0. A continuación teclea el comando `ipconfig /renew` para pedir de nuevo una IP al servidor DHCP. Comprueba que vuelves a tener una dirección IP y que ya has recuperado la conexión. Puedes parar de capturar con Wireshark. Deberían haberte aparecido, entre otros, los cuatro paquetes básicos de DHCP: DISCOVER, OFFER, REQUEST y ACK.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

(En Linux, puedes simular la liberación de IP y la petición de dirección desactivando y activando temporalmente la conexión haciendo clic en el icono correspondiente, cuya ubicación puede variar según la distribución Linux empleada)



Si lo prefieres, en lugar de capturar por tu cuenta, también puedes usar la captura de prueba **dhcp.pcap** disponible en el aula virtual, que ya incluye los cuatro paquetes.

b) Completa la tabla analizando las cabeceras de los niveles de enlace (Ethernet), red (IP) y transporte (UDP) de los cuatro mensajes DHCP:

Mensaje	MAC origen	MAC destino	IP origen	IP destino	Puerto origen	Puerto destino
DISCOVER	Mi MAC	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	68	67
OFFER	MAC servidor	Mi MAC	IP servidor	Futura IP cliente	67	68
REQUEST	Mi MAC	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	68	67
ACK	MAC servidor	Mi MAC	IP servidor	Futura IP cliente	67	68

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

c) Completa también esta tabla analizando el contenido del nivel de aplicación de los mensajes DHCP:

Mensaje	Message Type	HW type	HW address length	Hops	Transaction ID	Your (client) IP address	Server IP address	Client MAC address
DISC	1	1	6	0	nº	0.0.0.0	0.0.0.0	MAC cliente
OFFER	2	1	6	0	nº	Futura IP	IP servidor	MAC cliente
REQ	1	1	6	0	nº	0.0.0.0	0.0.0.0	MAC cliente
ACK	2	1	6	0	nº	Futura IP	IP servidor	MAC cliente

d) Contesta las siguientes preguntas sobre los campos de los mensajes DHCP:

- ¿Cuál es el valor del campo “Message Type” en los mensajes DISCOVER y REQUEST? 1
- ¿Cuál es el valor del campo “Message Type” en los mensajes OFFER y ACK? 2
- ¿Cuál es el valor de “HW type”? 1 ¿Qué tecnología de LAN está asociada a dicho valor? Ethernet
- ¿Cuál es el valor de “HW address length”? 6 ¿Por qué? Es la longitud de una MAC

e) Asocia cada nombre de campo con su longitud en bytes y la letra (A, B o C) correspondiente a su definición:

- Message type (_1_ byte): definición __B__
- Hardware type (_1_ byte): definición __C__
- Hardware address length (_1_ byte): definición __A__

Definiciones: A) “Es el tamaño de la dirección usada en el nivel de enlace. En redes Ethernet, cada MAC ocupa 6 bytes”, B) “Es el tipo de mensaje DHCP. Es 1 para los mensajes enviados por el cliente y 2 para los mensajes enviados por el servidor”, C) “Representa el tipo de tecnología usada en la LAN. Si es 1, indica que estamos usando Ethernet”

f) Selecciona el mensaje ACK, inspecciona su contenido e indica qué datos (además de la IP) son proporcionados por el servidor.

Máscara, fecha y hora de concesión, duración de la concesión...

g) Para cada uno de estos filtros de Wireshark, indica cuál o cuáles de los 4 mensajes DHCP básicos son recogidos por cada filtro:

- (eth.src=="tu MAC") && (udp.srcport==68) → DISCOVER y REQUEST
- (ip.src=="IP del servidor DHCP") && (udp.srcport==67) → OFFER y ACK
- (eth.src=="tu MAC") && (eth.dst==ff:ff:ff:ff:ff:ff) → DISCOVER y REQUEST
- (udp.port==67) || (udp.port==68) → Todos
- ip.dst=="IP del servidor DHCP" → Ninguno
- (udp.dstport==68)&&(ip.src==0.0.0.0) → Ninguno
- (ip.dst!=255.255.255.255) → OFFER y ACK

h) Crea en Packet Tracer una LAN con un servidor y 4 PC, todos conectados por cable a un switch 2960. Ve a la configuración del servidor y asígnale la IP estática 10.0.0.1, y a los PC asígnales IP dinámicas. De nuevo en el servidor DHCP, ve a la pestaña Services, y configura el servicio DHCP para que reparta en el pool que tiene por defecto desde la IP 10.0.0.101 hasta la 10.0.0.200 y que también reparta la máscara por defecto (sin subredes).

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	10.0.0.101	255.0.0.0	100	0.0.0.0	0.0.0.0

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

Usando el modo Simulación (ver Unidad 6, ejercicio 7, parte 2), pega aquí dos pantallazos: uno con el contenido de todas las cabeceras OSI del ACKNOWLEDGMENT, y otro con el contenido de la zona de datos, del mismo mensaje ACKNOWLEDGMENT. En las dos siguientes imágenes se muestra lo mismo pero para un DISCOVER. Recuerda aplicar un filtro antes de simular, para que solo se muestren los mensajes DHCP y no todos los mensajes de todos los protocolos. Para forzar el uso de DHCP en los PC, deberás cambiar la IP a estática y a continuación a dinámica (o teclear `ipconfig /release` y después `ipconfig /renew` en la consola de un PC).

Layer 7: DHCP Packet Server: 10.0.0.1, Client: 0.0.0.0
Layer6
Layer5
Layer 4: UDP Src Port: 67, Dst Port: 68
Layer 3: IP Header Src. IP: 10.0.0.1, Dest. IP: 255.255.255.255
Layer 2: Ethernet II Header 0090.215C.EAC2 >> FFFF.FFFF.FFFF
Layer 1: Port FastEthernet0

DHCP				Bytes
0	8	16	24	
OP:0x00000000 00000002	HW TYPE:1	HW LEN:6	HOPS:0	
TRANSACTION ID				
SECS:0	FLAGS:0x000000000000000000000000 000008000			
CLIENT ADDRESS:0.0.0.0				
YOUR CLIENT ADDRESS:10.0.0.102				
SERVER ADDRESS:10.0.0.1				
RELAY AGENT ADDRESS:0.0.0.0				
CLIENT HARDWARE ADDRESS:00D0.97A0.053E				
SERVER HOSTNAME (64 BYTES)				
FILE (128 BYTES)				
OPTIONS (312 BYTES)				

ACK:

In Layers
Layer 7: DHCP Packet Server: 10.0.0.1, Client: 0.0.0.0
Layer6
Layer5
Layer 4: UDP Src Port: 67, Dst Port: 68
Layer 3: IP Header Src. IP: 10.0.0.1, Dest. IP: 255.255.255.255
Layer 2: Ethernet II Header 0004.9A42.5E14 >> FFFF.FFFF.FFFF
Layer 1: Port FastEthernet0

0				8				16				24				Bytes
OP:0x00000000 00000002				HW TYPE:1				HW LEN:6				HOPS:0				
TRANSACTION ID																
SECS:0								FLAGS:0x000000000000000000000000 000008000								
CLIENT ADDRESS:0.0.0.0																
YOUR CLIENT ADDRESS:10.0.0.102																
SERVER ADDRESS:10.0.0.1																
RELAY AGENT ADDRESS:0.0.0.0																
CLIENT HARDWARE ADDRESS:000A.F31C.8E5B																
SERVER HOSTNAME (64 BYTES)																
FILE (128 BYTES)																
OPTIONS (312 BYTES)																

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

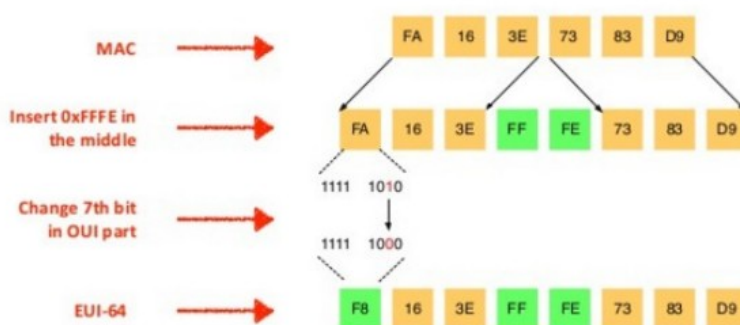
i) DHCPv6 es la adaptación del protocolo DHCP tradicional para que reparta IPv6. Uno de los nuevos tipos de reparto introducidos en DHCPv6 se denomina SLAAC, que consiste en obtener una IPv6 sin pedírsela al servidor DHCP, para ahorrar difusiones. Para obtener una IPv6 sin interactuar con el servidor, el proceso es el siguiente:

Paso 1. Obtener la MAC del equipo.

Paso 2. Insertar en medio de la MAC “FFFE”

Paso 3. En el primer byte, cambiar el séptimo bit (si es 0, cambiarlo a 1, y si es 1, cambiarlo a 0).

Paso 4. Traducir a hexadecimal el resultado obtenido.



Así se obtiene el EUI64, que correspondería a los últimos 64 bits de una IPv6. Respecto a los primeros 64 bits (recuerda que una IPv6 tiene 128 bits en total), también llamados “prefijo”, se puede obtener de dos formas: o bien el prefijo es difundido por el router de vez en cuando por toda la red, o bien se usa el prefijo local FE80:: que está reservado para uso interno en una LAN (de forma parecida a las IP privadas en IPv4, cuyo ámbito de actuación es únicamente la red local). La unión del prefijo y el EUI64 formarán la IPv6 completa.

A partir de tu MAC, obtén cuál sería tu IPv6 usando el prefijo local, siguiendo los cuatro pasos del proceso SLAAC:

- Dirección MAC: 00:0A:F3:1C:8E:5B

00:0A:F3:1C:8E:5B → 00:0A:F3:FF:FE:1C:8E:5B → 02:0A:F3:FF:FE:1C:8E:5B (EUI64)

Prefijo=FE80::

- IPv6 local: FE80::20A:F3FF:FE1C:8E5B (prefijo+EUI64)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

Ejercicio 2: DNS

a) Busca en Google el significado de los siguientes dominios gTLD:

.aero: Aviación
.biz: Negocios (business)
.info: Páginas informativas

b) Busca en Google a qué países pertenecen los siguientes dominios geográficos ccTLD:

.mt: Malta
.tr: Turquía
.za: Sudáfrica
.kr: Corea del Sur

c) Busca en Google los dominios correspondientes a los siguientes países:

Dinamarca: .dk
Marruecos: .ma
Rusia: .ru

d) Ve a <https://root-servers.org/> y contesta estas preguntas:

¿Cuál es la IPv4 de k.root-servers.org? 193.0.14.129
¿Y la IPv6? 2001:7fd::1
¿Cuántas “copias” de f.root-servers.org existen en el mundo? 336
¿Cuántos servidores raíz hay en total en España? 19
¿En qué ciudades? Madrid (10), Barcelona (8), Málaga (1)

e) Averigua la/s IP de tu/s servidor/es DNS (por ejemplo, con `ipconfig /all`).

Mi/s servidor/es DNS: 8.8.8.8, 8.8.4.4 (respuesta variable según la conexión del alumno)

f) Captura paquetes DNS con Wireshark. Para ello, inicia una captura y visita varias webs que no hayas visitado recientemente, para forzar que haya nuevas consultas DNS (si las visitaste hace poco, no se usará DNS ya que las respuestas recientes se guardan en la caché DNS para ahorrar consultas). Cuando hayas capturado varios paquetes DNS, termina de capturar. También puedes usar el fichero **dns.pcap**, disponible en el aula virtual, con varios paquetes DNS capturados de prueba.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

Escoge una pregunta DNS (también llamada “query”) y una respuesta DNS (“response”) y completa la siguiente tabla analizando las cabeceras correspondientes:

	<i>IP origen</i>	<i>IP destino</i>	<i>Puerto origen</i>	<i>Puerto destino</i>
Pregunta DNS	Mi IP	IP serv. DNS	x	53
Respuesta DNS	IP serv. DNS	Mi IP	53	x

g) Ahora responde estas preguntas analizando el interior de los mensajes DNS (capa de aplicación):

- ¿Cuánto mide (en bytes) el campo “Transaction ID”? 2
- ¿Qué valor tiene el flag “Response” en las preguntas? 0
- ¿Y en las respuestas? 1
- Abre el campo Query de varias consultas DNS. ¿Qué tipo (“type”) suele aparecer más frecuentemente? A/AAAA
- Abre el campo Answer de una respuesta DNS. ¿Cuál es el “data length” asociado a una dirección? 4 ó 16 ¿Por qué? Porque una IPv4 mide 4 bytes y una IPv6 mide 16 bytes

h) Escribe un filtro Wireshark para que aparezcan:

- Solo las consultas DNS: `dns.flags.response==0`
- Solo las respuestas DNS: `dns.flags.response==1`

(Puede haber más filtros, por ejemplo, para las consultas: `ip.src==IP_servidor_DNS` o también `udp.dstport==53`)

i) Añade a la LAN que creaste con Packet Tracer en el ejercicio anterior otro servidor, también conectado al switch, que usaremos como servidor DNS. Asígnale la IP estática 10.0.0.2. Modifica el pool del servidor DHCP para que el servidor DNS repartido a todos los clientes sea el 10.0.0.2. Haz que los clientes soliciten de nuevo IP para que se les reparta ahora también el nuevo servidor DNS.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	10.0.0.101	255.0.0.0	100	0.0.0.0	0.0.0.0

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

En el servidor DNS, configura el servicio para añadir tres registros de tipo A: www.ejemplo.com con la IP 10.0.0.51, www.pruebas.es con la IP 10.0.0.61 y www.paginaweb.es con la IP 10.0.0.71.

No.	Name	Type	Detail
0	www.ejemplo.com	A Record	10.0.0.51
1	www.paginaweb.es	A Record	10.0.0.71
2	www.pruebas.es	A Record	10.0.0.61

Desde cualquier PC de la LAN, en su consola haz ping usando el nombre (por ejemplo, `ping www.pruebas.es`) y debería aparecerte la IP resuelta. Es normal que los pings no respondan, ya que esos equipos no existen en la red y por tanto no hay conexión con ellos, pero sí que debería traducirse el nombre a IP (eso indica que el servidor DNS funciona).

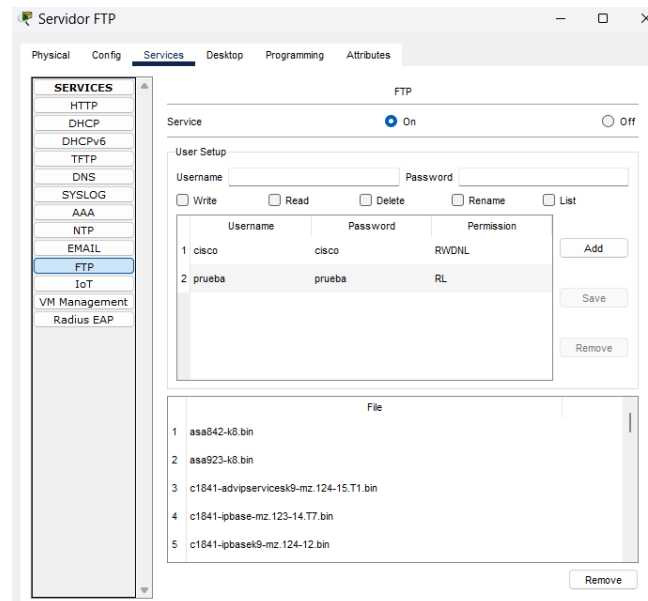
```
C:\>ping www.pruebas.es

Pinging 10.0.0.61 with 32 bytes of data:
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

Ejercicio 3: FTP

a) Añade un servidor más a la red de PT, conéctalo al switch y asígnale la IP estática 10.0.0.81. Configura en el servidor el servicio FTP, creando una cuenta de usuario (login “prueba” y password “prueba”), con permisos de lectura y listar.



Ahora desde cualquier PC, abre una consola y conéctate al servidor FTP tecleando “ftp 10.0.0.81”. Introduce el login y el password de la cuenta que acabas de crear. Lista el contenido del directorio home del servidor con el comando “dir”. Aparecerá un listado de ficheros y su tamaño en bytes. Para descargarte uno desde el servidor FTP al PC, teclea “get nombre_de_fichero”. Dependiendo del tamaño del fichero escogido, la transferencia puede tardar bastante tiempo. Cuando termine, desconéctate del servidor tecleando “quit”. Una vez desconectado, teclea “dir” en la consola y aparecerá el fichero descargado, indicando que la transferencia FTP ha funcionado.

```
C:\>ftp 10.0.0.81
Trying to connect...10.0.0.81
Connected to 10.0.0.81
220- Welcome to PT Ftp server
Username:prueba
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get asa842-k8.bin

Reading file asa842-k8.bin from 10.0.0.81:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 18.761 secs (68046 bytes/sec)
ftp>quit

221- Service closing control connection.
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

1/1/1970   1:0 PM                5571584   asa842-k8.bin
1/1/1970   1:0 PM                  26      sampleFile.txt
                    5571610 bytes          2 File(s)

C:\>
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

b) Modifica la configuración del servidor DNS para que se pueda acceder al servidor mediante el nombre “ftp.servidor.es” además de con su IP (10.0.0.81). Compruébalo desde un PC.

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record ▾

Address

No.	Name	Type	Detail
0	ftp.servidor.es	A Record	10.0.0.81
1	www.ejemplo.com	A Record	10.0.0.51
2	www.paginaweb.es	A Record	10.0.0.71
3	www.pruebas.es	A Record	10.0.0.61

```
C:\>ping ftp.servidor.es

Pinging 10.0.0.81 with 32 bytes of data:

Reply from 10.0.0.81: bytes=32 time<1ms TTL=128
Reply from 10.0.0.81: bytes=32 time<1ms TTL=128
Reply from 10.0.0.81: bytes=32 time<1ms TTL=128
Reply from 10.0.0.81: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.81:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

c) Crea un nuevo usuario en el servidor FTP llamado “prueba2” con la contraseña que quieras, y otórgale permisos de lectura, escritura y listado.

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	prueba	prueba	RL
3	prueba2	prueba2	RWL

Desde cualquier PC de la LAN, crea un fichero de texto con cualquier contenido, desde el editor de textos:



Al cerrar el editor, te preguntará el nombre del fichero de texto que quieres crear (ejemplo.txt). Abre la consola de ese PC y, tras ejecutar “dir” comprueba que aparece el fichero recién creado. Ahora conéctate al servidor FTP usando el nombre del servidor (no su IP) y con la cuenta “prueba2”. Sube el fichero del cliente al servidor mediante el comando “put ejemplo.txt”. Tras subirlo, haz un “dir” para verificar que se ha subido el fichero al servidor FTP. Desconéctate del servidor con “quit” para acabar.

```
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

1/1/1970   1:0 PM                5571584   aaa842-k8 bin
1/1/1970   1:0 PM                  5          ejemplo.txt
1/1/1970   1:0 PM                  26      sample11e.txt
                               5571615 bytes    3 File(s)

C:\>ftp ftp.servidor.es
Trying to connect...ftp.servidor.es
Connected to ftp.servidor.es
220- Welcome to FT Ftp server
Username:prueba2
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp:put ejemplo.txt

Writing file ejemplo.txt to ftp.servidor.es:
File transfer in progress...

[Transfer complete - 5 bytes]

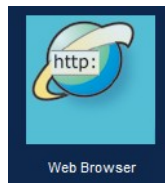
5 bytes copied in 0.092 secs (54 bytes/sec)
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

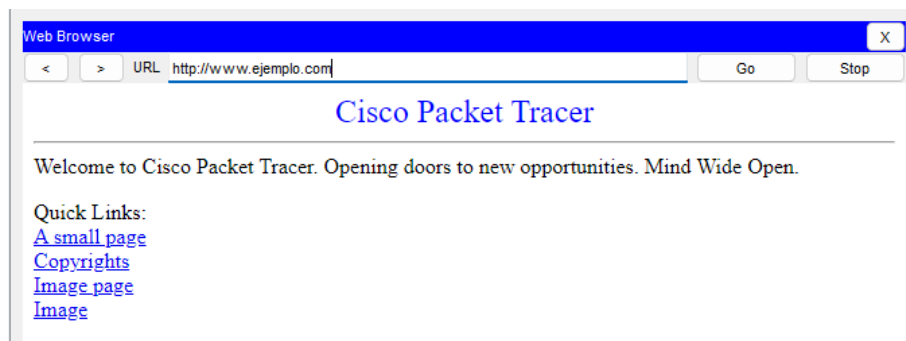
Ejercicio 4: HTTPS

a) Añade a la red tres servidores más, con IP estáticas 10.0.0.51, 10.0.0.61 y 10.0.0.71 y nombres www.ejemplo.com, www.pruebas.es y www.paginaweb.es, respectivamente. Deberás configurar el servidor DNS para que se resuelven los nombres. Asegúrate de que los tres servidores tienen activado tanto el servicio HTTP como HTTPS.

b) Ve a cualquier PC y abre su navegador:

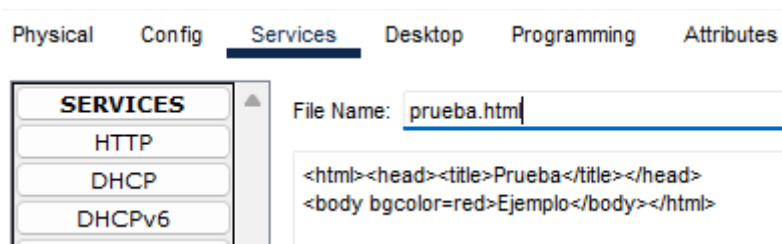


Accede a www.ejemplo.com para ver la página web que Cisco pone por defecto en un servidor HTTPS.



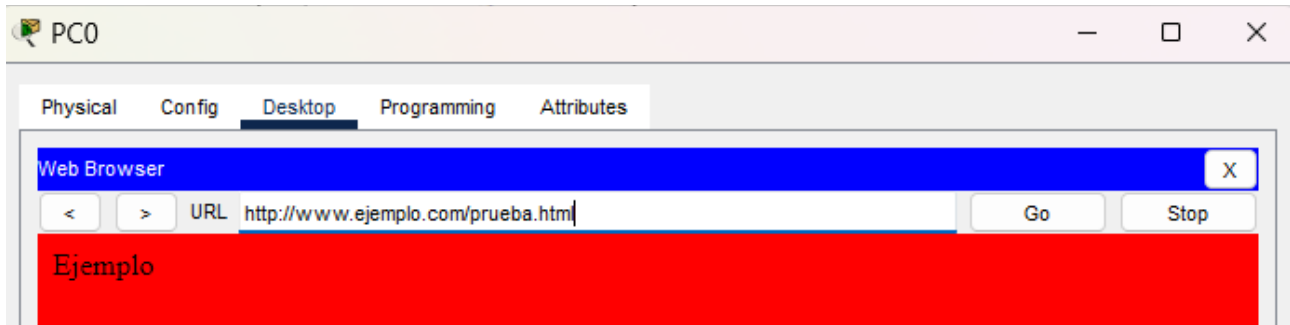
c) Ve al servidor www.ejemplo.com y configura su servicio HTTP para añadir un nuevo fichero llamado prueba.html con el siguiente contenido:

```
<html><head><title>Prueba</title></head>
<body bgcolor=red>Ejemplo</body></html>
```



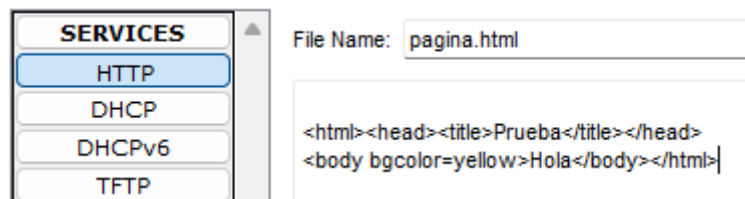
CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

Graba el fichero, ve a un PC y desde su navegador accede a www.ejemplo.com/prueba.html. Deberías ver una página web con fondo rojo.

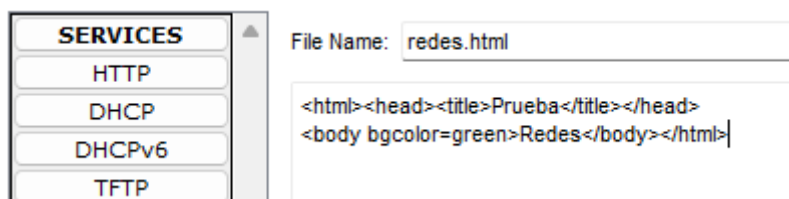


d) Crea dos páginas web más:

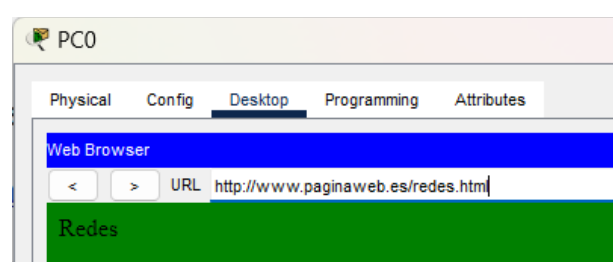
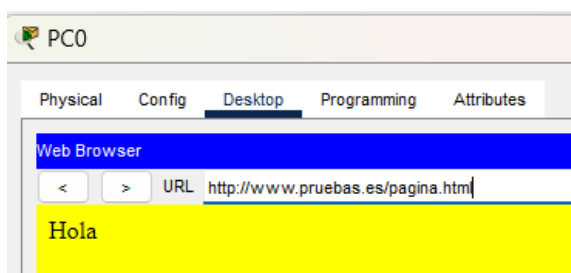
www.pruebas.es/pagina.html, donde ponga “hola” con fondo amarillo



www.paginaweb.es/redes.html donde ponga “Redes” con fondo verde

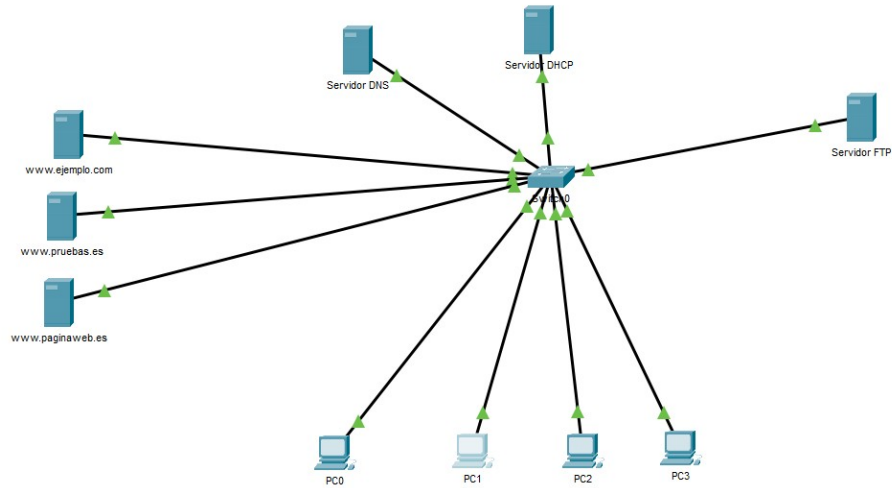


Comprueba desde cualquier PC de la LAN que puedes ver las webs accediendo a su URL desde el navegador.



CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 8: Capa de aplicación

Después de haber añadido todos los servidores (DHCP, DNS, FTP y HTTPS), tu LAN debería haber quedado así:



Adjunta a tu entrega el fichero .pkt obtenido.

Ejercicio 1: Comando ping (Windows) / ping (Linux)

Para probarlo, desde la consola de Windows ("cmd"), teclea `ping` sin parámetros para ver todas las opciones posibles que ofrece el comando. Indica qué comando entero (parámetros incluidos) usarías en Windows para realizar las siguientes acciones (puedes enviar pings de prueba al router o puerta de enlace de tu LAN, a otro equipo de tu misma red o a cualquier equipo externo):

- Enviar sólo 3 pings a un equipo:

```
ping -n 3 8.8.8.8
```

- Enviar pings a un equipo sin parar (hasta que se pulse CTRL+C):

```
ping -t 8.8.8.8
```

- Enviar mensajes de datos de 500 bytes en cada ping:

```
ping -l 500 8.8.8.8
```

- Enviar 5 pings, cada uno de 1000 bytes (combina dos opciones anteriores):

```
ping -n 5 -l 1000 3 8.8.8.8
```

- Enviar pings a un equipo del cual se sabe su IPv6:

```
ping -6 fe80::abcd:1234
```

- Enviarte un ping a ti mismo usando la dirección de loopback (útil para comprobar si tu tarjeta de red funciona correctamente):

```
ping 127.0.0.1
```

- Enviar pings con TTL 24:

```
ping -i 24 8.8.8.8
```

- Enviar pings obligando a que no se fragmenten aunque sea necesario (flag DF=1, ver unidad 6, punto 4 para recordar el uso del flag "Don't Fragment" en la cabecera IPv4):

```
ping -f 8.8.8.8
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Averigua también las siguientes opciones pero en Linux. Para leer los parámetros disponibles en Linux, teclea `man ping`:

- Enviar 5 pings a un equipo: `ping -c 5 www.google.es`
- Esperar 6 segundos entre cada ping enviado: `ping -i 6 www.google.es`
- Enviar 6 pings de 400 bytes cada uno: `ping -c 6 -s 400 www.google.es`
- Enviar 3 pings y mostrar solamente las estadísticas finales:

```
ping -c 3 -q www.google.es
```

Como ves, aunque ping en Windows y Linux realizan la misma función, tienen parámetros diferentes (incluso para usar la misma opción el nombre de parámetro empleado puede ser diferente según el SO).

Internamente, el comando ping usa el protocolo de la capa de red ICMP (Internet Control Message Protocol). La estructura de todo paquete ICMP tiene el siguiente formato:



Para comprobarlo, empleando Wireshark realiza una captura mientras haces varios pings y contesta a las siguientes preguntas:

- ¿Qué n.º aparece en el campo “protocol” de la cabecera IP de cualquier ping? 1

```
Internet Protocol Version 4, Src: 10.5.3.1, Dst: 10.5.3.183
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 428
    Identification: 0x0000 (0)
  Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
```

- ¿Qué n.º aparece en el campo “type” del interior de un ping enviado? 8

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
```

CIPFP Ausiàs March (Valencia)
 1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

- ¿Y en el de un ping recibido? 0

▼ Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)

- ¿Qué filtro usarías en Wireshark para que solo se te mostraran las peticiones de ping? (Puedes usar filtros como icmp.algo==valor)

icmp.type==8

- ¿Y para ver solo las respuestas?

icmp.type==0

Ejercicio 2: Comando ipconfig (Windows) / ip (Linux)

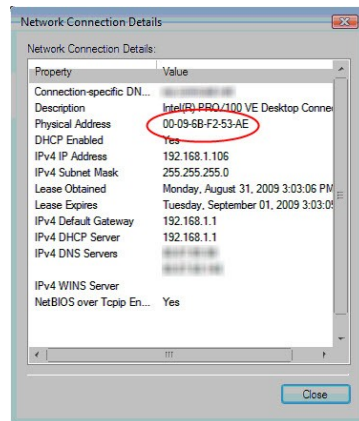
Desde Windows, teclea `ipconfig /all` y rellena la siguiente tabla con los valores de tu conexión real y una breve descripción de cada campo.

Nombre	Valor	¿Para qué sirve?
IPv4	10.3.8.254	Una IP sirve para diferenciar entre conexiones
Máscara	255.255.255.0	Sirve para separar una red en subredes
IPv6	FE80::AA60:407E:2E D0:D83D	Versión 6 de la dirección IP (más grande)
MAC	90:1B:0E:ED:CC:19	Dirección física que identifica una tarjeta de red Ethernet
Puerta de enlace	10.3.8.1	Dirección IP del equipo que proporciona acceso al exterior
IP de los servidores DNS	10.3.8.1	Direcciones IP de los servidores primario y secundario que traducen nombres a IP
¿DHCP activado? (Sí/No)	Sí	Indica si está o no habilitado el reparto automático
IP del servidor DHCP	10.3.8.1	Dirección IP del equipo encargado de repartir configuraciones de red
Fecha y hora de concesión	20/4/23 13:40	Cuándo se otorgó la IP
Fecha y hora de caducidad	20/4/23 21:40	Hasta cuándo se otorgará la IP

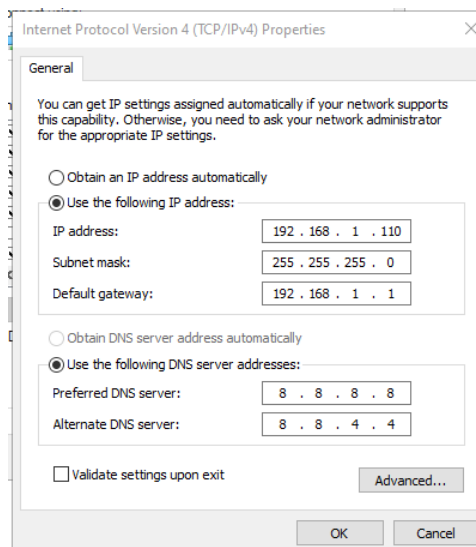
En la tabla anterior, marca en amarillo los campos que son diferentes en otro equipo de tu misma LAN, y en azul los campos que son iguales en todos los equipos de tu misma LAN.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Pega aquí un pantallazo donde aparezcan los mismos datos que al ejecutar `ipconfig` pero de manera gráfica, en alguna sección de Windows, y sin ejecutar comando.



En el caso de que quisiéramos usar una IP estática, ¿cómo lo haríamos? Captura la pantalla que usarías en tu Windows.



Explica para qué sirven los siguientes parámetros de `ipconfig`:

- `ipconfig /release`: libera su IP, avisando al servidor DHCP para que pueda repartirla a otro.
- `ipconfig /renew`: solicita una IP al servidor DHCP.
- `ipconfig /displaydns`: muestra la caché DNS con las parejas de nombres e IP ya resueltos, así como la duración temporal en caché de cada dato.
- `ipconfig /flushdns`: vacía la caché DNS.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Usando el comando `ip` (que poco a poco va sustituyendo al antiguo `ifconfig`) desde el terminal de Linux, asocia cada uno de los siguientes comandos con su definición del listado inferior. Recuerda que puedes usar `man ip` para obtener información sobre todos los parámetros posibles, o mejor aún, probar directamente cada comando en tu equipo y ver los resultados.

Comando	Definición
<code>ip link</code>	A
<code>ip address</code>	I
<code>ip address show enp0s3</code> (siendo <code>enp0s3</code> el nombre de una conexión, también puede ser <code>eth0</code> , etc)	B
<code>ip -s address</code>	L
<code>ip route</code>	G
<code>ip -br link</code> o también <code>ip -br address</code>	E
<code>ip -c link</code>	H
<code>ip -h -s address</code>	J
<code>sudo ip link set enp0s3 down</code> (siendo <code>enp0s3</code> el nombre de una conexión, también puede ser <code>eth0</code> , etc)	K
<code>sudo ip link set enp0s3 up</code> (siendo <code>enp0s3</code> el nombre de una conexión, también puede ser <code>eth0</code> , etc)	C
<code>ip neigh show</code>	M
<code>sudo ip neigh add 192.168.1.17 lladdr 11:22:33:aa:bb:cc dev enp0s3</code>	F
<code>sudo ip neigh del 192.168.1.17 lladdr 11:22:33:aa:bb:cc dev enp0s3</code>	D

Definiciones:

- A) Mostrar el listado con todas las tarjetas de red (reales o virtuales) disponibles en el equipo, y sus MAC
- B) Mostrar la IPv4, máscara y la IPv6 de una conexión concreta
- C) Activar una conexión
- D) Borrar una fila de la tabla ARP
- E) Mostrar información sobre las tarjetas de red o las conexiones IP (mostradas como tabla con columnas)
- F) Añadir una fila a la tabla ARP
- G) Mostrar información sobre el enrutamiento (incluyendo la IP de la puerta de enlace)
- H) Mostrar el listado de las tarjetas de red, usando colores
- I) Mostrar la IPv4, máscara y la IPv6 de todas las tarjetas de red (reales o virtuales) disponibles en el equipo
- J) Mostrar los paquetes recibidos (RX) y transmitidos (TX) usando expresiones con K, M, G, etc
- K) Desactivar una conexión
- L) Mostrar la MTU y los paquetes recibidos (RX) y transmitidos (TX)
- M) Mostrar el contenido de la tabla ARP (similar a `arp -a` en Windows)

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Finalmente, pega aquí un pantallazo de Linux donde aparezca la información de tu conexión (IP, MAC, máscara, DNS, gateway, etc) de manera gráfica, sin ejecutar comando.



Ejercicio 3: Comando netstat (Windows) / ss (Linux)

El comando `netstat` (de “network statistics”) de Windows permite ver, entre otras cosas, las conexiones actuales de un equipo. Si lo ejecutamos sin parámetros veremos algo parecido a esto:

```
Administrator: Command Prompt - netstat
Active Connections

Proto Local Address           Foreign Address         State
TCP   127.0.0.1:56304          hlrcv:9001              SYN_SENT
TCP   192.168.10.100:50310     104.20.27.217:https     ESTABLISHED
TCP   192.168.10.100:50312     104.20.27.217:https     ESTABLISHED
TCP   192.168.10.100:52043     40.67.251.132:https     ESTABLISHED
TCP   192.168.10.100:53069     wq-in-f188:5228         ESTABLISHED
TCP   192.168.10.100:55470     relay-033a5347:6568     ESTABLISHED
TCP   192.168.10.100:55839     server-99-86-116-19:https ESTABLISHED
TCP   192.168.10.100:55883     192.0.73.2:https        ESTABLISHED
TCP   192.168.10.100:55961     los02s04-in-f14:https   ESTABLISHED
TCP   192.168.10.100:55962     los02s04-in-f14:https   ESTABLISHED
TCP   192.168.10.100:55978     los02s03-in-f14:https   TIME_WAIT
TCP   192.168.10.100:55980     los02s03-in-f8:https    ESTABLISHED
TCP   192.168.10.100:55989     los02s04-in-f2:https    TIME_WAIT
TCP   192.168.10.100:55990     los02s03-in-f2:https    ESTABLISHED
TCP   192.168.10.100:55991     los02s04-in-f2:https    TIME_WAIT
TCP   192.168.10.100:55992     los02s03-in-f2:https    TIME_WAIT
TCP   192.168.10.100:55995     los02s04-in-f10:https   TIME_WAIT
TCP   192.168.10.100:55996     los02s04-in-f10:https   TIME_WAIT
TCP   192.168.10.100:55999     los02s04-in-f14:https   TIME_WAIT
TCP   192.168.10.100:56000     los02s04-in-f14:https   TIME_WAIT
TCP   192.168.10.100:56001     los02s04-in-f1:https    ESTABLISHED
TCP   192.168.10.100:56013     ec2-52-72-80-38:https   ESTABLISHED
TCP   192.168.10.100:56030     ec2-34-204-157-1:https   ESTABLISHED
TCP   192.168.10.100:56032     ec2-34-204-157-1:https   TIME_WAIT
TCP   192.168.10.100:56037     los02s03-in-f6:https    TIME_WAIT
TCP   192.168.10.100:56038     los02s03-in-f6:https    TIME_WAIT
TCP   192.168.10.100:56054     los02s03-in-f10:https   TIME_WAIT
TCP   192.168.10.100:56055     los02s03-in-f10:https   TIME_WAIT
TCP   192.168.10.100:56056     los02s04-in-f6:https    TIME_WAIT
TCP   192.168.10.100:56057     los02s04-in-f6:https    TIME_WAIT
TCP   192.168.10.100:56060     los02s04-in-f6:https    TIME_WAIT
TCP   192.168.10.100:56068     ec2-52-3-46-228:https   ESTABLISHED
TCP   192.168.10.100:56069     ec2-52-3-46-228:https   TIME_WAIT
```

Cada línea representa una conexión y está formada por cinco datos: IP origen, puerto origen, IP destino, puerto destino y estado de la conexión. Se denomina **socket** al conjunto de IP origen, puerto origen, IP destino y puerto destino. Por ejemplo, el socket

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

formado por 192.168.1.5:23423 y 45.21.231.29:443 representa una conexión desde el puerto 23423 del equipo con dirección IP 192.168.1.5 hasta el puerto 443 (HTTPS) del equipo con dirección IP 45.21.231.29. Esa conexión probablemente representa que desde nuestro equipo (IP privada) se ha contactado con el servidor web del otro equipo, es decir, simplemente representa que desde el equipo se está viendo una página web.

En la salida de `netstat`, las direcciones IP pueden aparecer tanto en formato numérico como en nombre. Del mismo modo, los puertos pueden aparecer como número o como texto ("https" para el puerto 443, etc).

Cada conexión está en un estado concreto, que aparecen en la columna de la derecha (ESTABLISHED, SYN_SENT, TIME_WAIT, etc), que será explicado después.

Comando	Definición
<code>netstat</code>	A
<code>netstat -s</code>	G
<code>netstat -b</code>	D
<code>netstat -e</code>	F
<code>netstat -a</code>	B
<code>netstat -r</code>	I
<code>netstat -p tcp</code>	H
<code>netstat 3</code>	J
<code>netstat -n</code>	C
<code>netstat -n -b -a</code> o también <code>netstat -nba</code>	E

Definiciones:

A: Muestra las conexiones activas del equipo

B: Muestra todas las conexiones del equipo, estén activas o no

C: Muestra las IP y los puertos siempre con números, sin nombres de equipo ni de servicios

D: Muestra, además de las conexiones, el ejecutable asociado a dicha conexión

*E: Muestra **todas** las conexiones con **números** y también el **ejecutable***

F: Muestra estadísticas de envío y recepción, como el n.º de bytes, paquetes, difusiones o errores

G: Muestra estadísticas de todos los protocolos (IPv4, IPv6, ICMP, TCP, UDP)

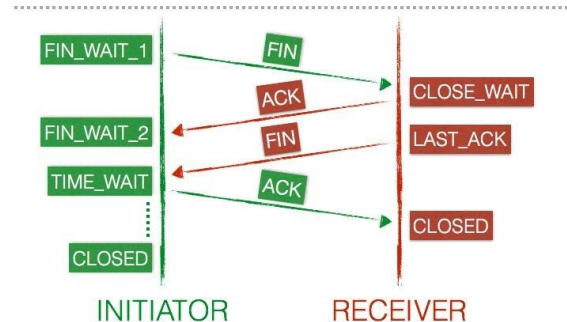
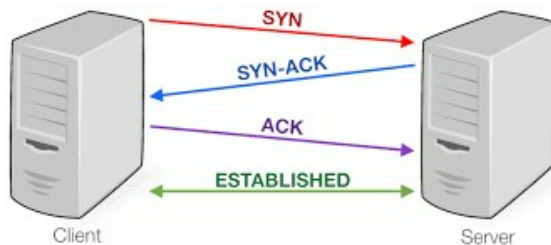
H: Muestra estadísticas según el protocolo de transporte (por ejemplo: TCP)

I: Muestra la tabla de enrutamiento del equipo

J: Muestra las conexiones, y los datos van actualizándose cada 3 segundos

Respecto al estado de una conexión (la columna de la derecha, con valores como ESTABLISHED, etc), es importante que recuerdes primero el proceso de conexión TCP (unidad 6, punto 7). En dicho apartado se explicaban los procesos de establecimiento y finalización de conexión de TCP (fases 1 y 3 del "handshaking", representadas en las siguientes imágenes):

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes



Como ves, los pasos a seguir son:

Fase -1) Conexión cerrada por ambas partes

Fase 0) El servidor está escuchando, a la espera de recibir alguna conexión

Fase 1a) El cliente envía el SYN y está a la espera de recibir el SYN+ACK

Fase 1b) El servidor envía el SYN+ACK y está a la espera de recibir el ACK

Fase 1c) El cliente envía el ACK

Fase 2) Transferencia de datos (conexión establecida)

Fase 3a) El cliente envía el FIN y está a la espera de recibir el FIN+ACK

Fase 3b1) El servidor envía el ACK

Fase 3b2) El servidor envía el FIN y está a la espera de recibir el ACK

Fase 3c) El cliente envía el ACK dando paso a la finalización de la conexión

Fase 4) Conexión finalizada (se vuelve a la fase -1)

Se han marcado en **azul** los pasos que representan un envío por parte del cliente y en **naranja** los pasos asociados al servidor. Como ves, todas estas etapas son necesarias cuando se usa TCP en transporte, ya que para garantizar seguridad, ha de prepararse adecuadamente la conexión.

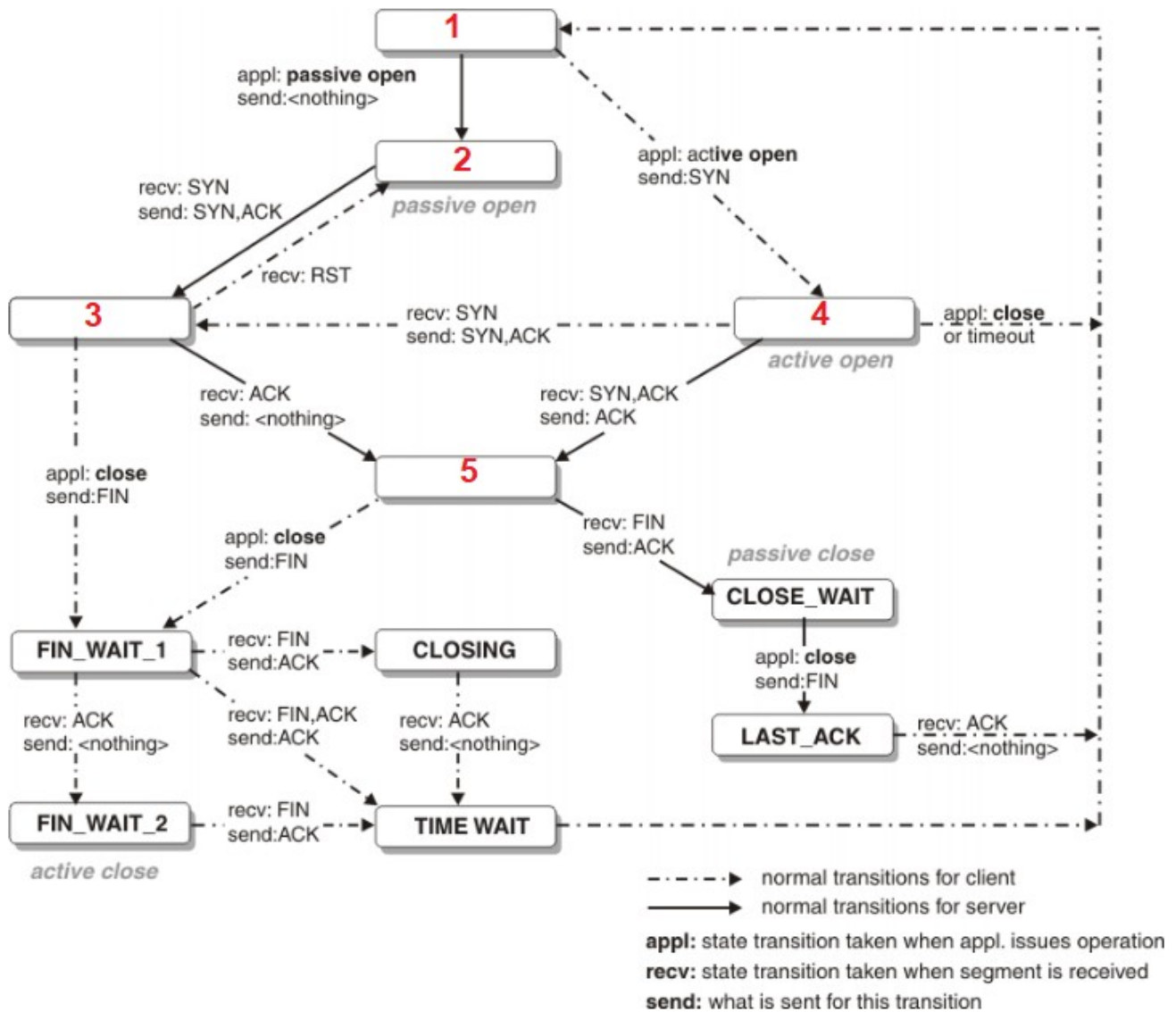
Cada una de las subetapas es un estado posible en `netstat` (ESTABLISHED, etc), según la fase (1, 3, etc) en la que estemos y según el rol (cliente o servidor).

En la siguiente imagen tienes representados todos los estados posibles (en forma de rectángulo), y cómo cambiar de uno a otro (en forma de flecha, siendo continua para los servidores y discontinua si se trata de clientes). El texto encima de cada flecha indica cómo pasar de un estado a otro. Aparecen casi todos los estados, excepto 5.

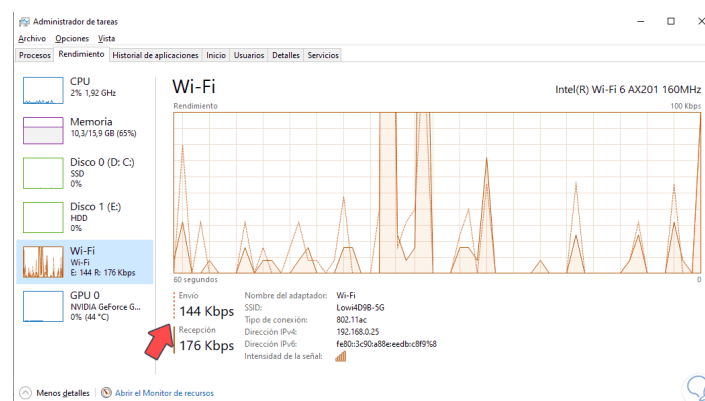
Completa el diagrama asociando los 5 estados que quedan (LISTEN, ESTABLISHED, CLOSED, SYN_RCVD, SYN_SENT) con su correspondiente número:

- 1: CLOSED
- 2: LISTEN
- 3: SYN_RCVD
- 4: SYN_SENT
- 5: ESTABLISHED

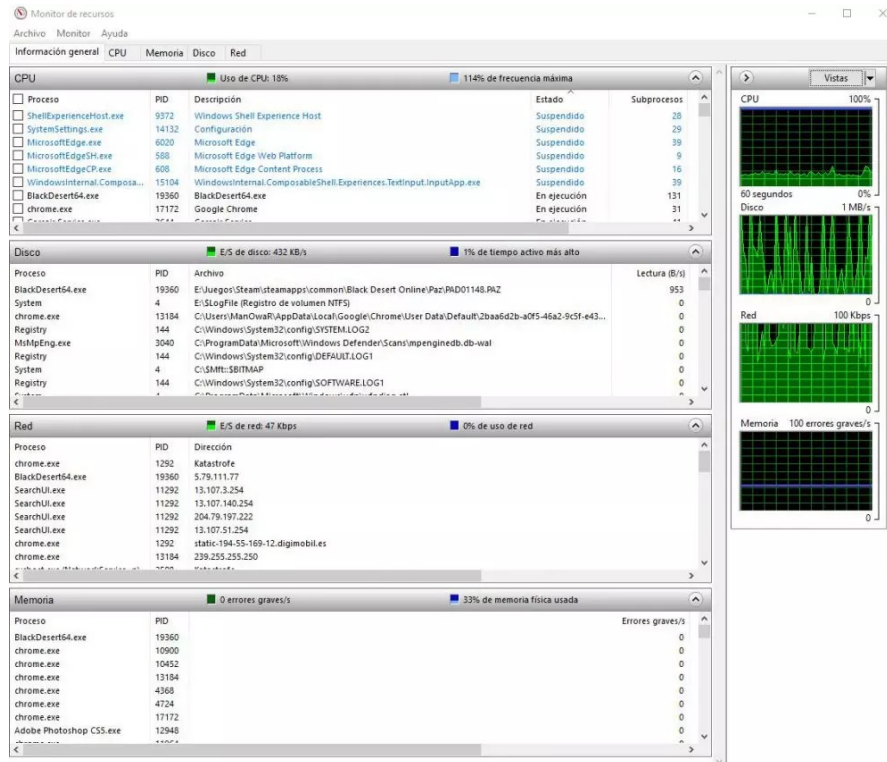
CIPFP Ausiàs March (Valencia)
 1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes



Pega aquí dos pantallazos de tu Windows: el de Rendimiento de tu tarjeta de red y el de Monitor de Recursos de la sección Red.



CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes



Respecto a Linux, el equivalente a `netstat` es el comando `ss` (socket statistics). Ejecuta `ss` en un terminal. Por defecto, se muestran solo los sockets abiertos (o conexiones ya establecidas). Las columnas más importantes son la segunda (“state”), la quinta (“local address:port”) y la sexta (peer address:port), que corresponden al estado, conexión local y conexión remota. Si salen demasiadas líneas de golpe, puedes paginarlas tecleando `ss | more` e ir pulsando la barra espaciadora para pasar de página (esto es aplicable a cualquier comando Linux).

```
bitnami@debian:~$ ss
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
tcp    ESTAB  0      0      * 10749          * 10750
tcp    ESTAB  0      0 /run/systemd/journal/stdout 10750 * 10749
tcp    ESTAB  0      0 /run/systemd/journal/stdout 10644 * 10643
tcp    ESTAB  0      0 /run/systemd/journal/stdout 11046 * 11045
tcp    ESTAB  0      0      * 10643          * 10644
tcp    ESTAB  0      0      * 10923          * 10924
tcp    ESTAB  0      0 /run/systemd/journal/stdout 11067 * 11066
tcp    ESTAB  0      0 /run/systemd/journal/stdout 11209 * 11208
tcp    ESTAB  0      0      * 11208          * 11209
tcp    ESTAB  0      0 /run/systemd/journal/stdout 10924 * 10923
tcp    ESTAB  0      0      * 11045          * 11046
icmp6   UNCONN 0      0      *:::ip6-icmp    *:::
tcp    ESTAB  0      0 [::ffff:10.0.2.15]:mysql [::ffff:10.0.2.21]:64704
tcp    ESTAB  0      0 [::ffff:10.0.2.15]:mysql [::ffff:10.0.2.21]:62253
tcp    ESTAB  0      0 [::ffff:10.0.2.15]:mysql [::ffff:10.0.2.21]:64703
tcp    ESTAB  0      0 [::ffff:10.0.2.15]:mysql [::ffff:10.0.2.21]:62252
bitnami@debian:~$
```

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Teclea cada uno de estos comandos y asocialos con su correspondiente definición.
Puedes ayudarte con `man ss o ss -?`

Comando	Definición
<code>ss</code>	A
<code>ss -t</code>	C
<code>ss -u</code>	L
<code>ss -ua</code>	H
<code>ss -nt</code>	F
<code>ss -ltn</code>	G
<code>ss -lun</code>	B
<code>ss -o state established</code>	J
<code>ss -t4</code>	K
<code>ss -nt dst :443 or dst :80</code>	E
<code>ss -nt dst 20.45.32.21</code>	M
<code>ss -nt dst 20.45.32.21/16</code>	D
<code>ss -nt src 127.0.0.1 sport gt :5000</code>	I

Definiciones:

- A) Muestra las conexiones
- B) Muestra las conexiones UDP que estén a la escucha, usando n.º
- C) Muestra las conexiones TCP
- D) Muestra, usando n.º, las conexiones TCP destinadas a un rango concreto de IP
- E) Muestra, usando n.º, las conexiones TCP destinadas a puertos HTTP o HTTPS
- F) Muestra, usando n.º, las conexiones TCP
- G) Muestra las conexiones TCP que estén a la escucha, usando n.º
- H) Muestra todas las conexiones UDP, en cualquier estado
- I) Muestra, usando n.º, las conexiones TCP que salgan de tu equipo, de un puerto >5000
- J) Muestra las conexiones que estén establecidas
- K) Muestra las conexiones TCP e IPv4
- L) Muestra las conexiones UDP
- M) Muestra, usando n.º, las conexiones TCP destinadas a una IP concreta

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Ejercicio 4: Comando route (Windows) / ip (Linux)

Dada esta tabla de enrutamiento capturada en un equipo:

```

IPo4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.18.6.1        10.18.6.211      10
10.18.6.0                  255.255.255.0    On-link          10.18.6.211      266
10.18.6.211                255.255.255.255  On-link          10.18.6.211      266
10.18.6.255                255.255.255.255  On-link          10.18.6.211      266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          10.18.6.211      266
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          10.18.6.211      266
  
```

- ¿Cuál es la IP del equipo que posee esta tabla? 10.18.6.211
- ¿Cuál es la puerta de enlace del equipo? 10.18.6.1
- Indica qué fila (primera, segunda, etc) de la tabla representa la siguiente información:
 - “Los paquetes de difusión global o broadcast son aceptados por la tarjeta de red” Fila 11
 - “Los paquetes destinados a 127.0.0.1 son aceptados por la tarjeta de red” Fila 6
 - “Los paquetes destinados a cualquier IP que empiece por 127 son aceptados por la tarjeta de red” Fila 5
 - “Los paquetes destinados a 10.18.6.211 son aceptados por la tarjeta de red” Fila 3
 - “Los paquetes destinados a la dirección de difusión de la LAN son aceptados por la tarjeta de red” Fila 4
 - “Los paquetes que no encajen con ninguna de las otras filas serán enviados a la puerta de enlace” Fila 1

Completa esta tabla de enrutamiento, correspondiente a un equipo con IP 192.168.0.1, sin subnetting y con puerta de enlace 192.168.0.254:

Destino de red	Máscara	Puerta de enlace	Interface
0.0.0.0	0.0.0.0	192.168.0.254	192.168.0.1
192.168.0.255	255.255.255.255	On-Link	192.168.0.1
192.168.0.1	255.255.255.255	On-Link	192.168.0.1
127.0.0.0	255.0.0.0	On-Link	127.0.0.1
127.0.0.1	255.255.255.255	On-Link	127.0.0.1
255.255.255.255	255.255.255.255	On-Link	127.0.0.1
255.255.255.255	255.255.255.255	On-Link	192.168.0.1

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Pega aquí un pantallazo de la tabla de encaminamiento de tu equipo.

```
Command Prompt

=====
Interface List
7...02 00 54 74 68 72 .....EasyTether Network Adapter
15...0a 00 27 00 00 0f .....VirtualBox Host-Only Ethernet Adapter #2
6...9e b6 d0 e1 69 3f .....Microsoft Wi-Fi Direct Virtual Adapter
9...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
12...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
2...9c b6 d0 e1 69 3f .....Killer Wireless-n/a/ac 1535 Wireless Network Adapter
23...9c b6 d0 e1 69 40 .....Bluetooth Device (Personal Area Network) #2
1.....Software Loopback Interface 1
14...00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.254    192.168.1.75     35
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
192.168.1.0                255.255.255.0    On-link          192.168.1.75     291
192.168.1.75              255.255.255.255  On-link          192.168.1.75     291
192.168.1.255              255.255.255.255  On-link          192.168.1.75     291
192.168.44.0               255.255.255.0    On-link          192.168.44.1     291
192.168.44.1              255.255.255.255  On-link          192.168.44.1     291
192.168.44.255            255.255.255.255  On-link          192.168.44.1     291
192.168.56.0               255.255.255.0    On-link          192.168.56.1     281
192.168.56.1              255.255.255.255  On-link          192.168.56.1     281
-- More --
```

Ahora vamos a cambiar un poco tu tabla de encaminamiento (necesitarás privilegios de administrador). Teclea `route` sin parámetros para ver los ejemplos de cómo añadir y eliminar filas a una tabla.

- Elimina la fila “default” (la primera, con 0.0.0.0) de tu tabla. ¿Qué comando has tecleado? `route add a.a.a.a mask b.b.b.b c.c.c.c`, siendo a.a.a.a la red destino, b.b.b.b la máscara y c.c.c.c el siguiente salto.

Imprime de nuevo la tabla y comprueba que ha desaparecido la fila. ¿Tienes acceso a Internet? ¿Por qué? Pese a borrar la fila, puede que la fila se regenere instantes después automáticamente por lo que no se notaría una pérdida de la conexión.

- Lo más probable es que la fila “default” se añada automáticamente al cabo de unos instantes, ya que es fundamental para poder tener acceso al exterior. Si no se añadiera, ¿qué comando teclearías para hacerlo? `route del a.a.a.a mask b.b.b.b c.c.c.c`, siendo a.a.a.a la red destino, b.b.b.b la máscara y c.c.c.c el siguiente salto.

Si te equivocas o sigues sin tener acceso a la red, la tabla de enrutamiento se genera automáticamente cada vez que reinicias el equipo.

- ¿Qué fila de la tabla borrarías si no quisieras responder pings destinados a tu equipo? La que va destinada a mí, es decir, aquella en la que aparece mi IP

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

- Si elimináramos las filas que tienen 255.255.255.255 en la primera columna, ¿podrías enviar peticiones ARP? Sí ¿Y responder a peticiones ARP de otros? No

Desde Linux:

- Pega un pantallazo de tu tabla de encaminamiento (comando `ip route`)

```
mascunyand@sp-pc02:~/Escritorio$ ip route
default via 10.2.3.1 dev enp2s0 proto dhcp metric 100
10.2.3.0/24 dev enp2s0 proto kernel scope link src 10.2.3.12 metric 100
169.254.0.0/16 dev enp2s0 scope link metric 1000
mascunyand@sp-pc02:~/Escritorio$
```

- Busca con qué parámetros borrarías la fila “default”

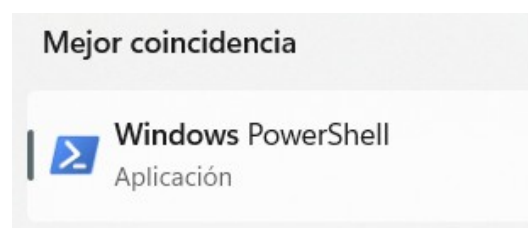
```
sudo ip route del x.x.x.x/24 via y.y.y.y dev enp0s3
```

- Busca con qué parámetros añadirías una fila

```
sudo ip route add x.x.x.x via y.y.y.y dev enp0s3
```

Ejercicio 5: Windows PowerShell

El “Símbolo del sistema” de Windows (comando “cmd”) se lleva usando tradicionalmente en Windows desde hace décadas, y aunque es completamente funcional, las últimas versiones del SO proporcionan un shell mucho más potente y avanzado (por ejemplo, para autocompletar comandos y rutas con el tabulador). Puedes acceder a él buscando “Windows PowerShell” entre los programas de tu equipo.



CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

En el siguiente ejercicio deberás teclear cada uno de los comandos desde PowerShell y, observando el resultado devuelto, indicar qué comando de los vistos en los ejercicios anteriores sería el equivalente.

Comando Windows PowerShell	Comando cmd/Símbolo del sistema
Get-NetAdapter	g)
Get-NetIPConfiguration	e)
Test-NetConnection www.google.es	a)
Test-NetConnection www.google.es -TraceRoute	c)
Get-NetTCPConnection	d)
Get-NetRoute	f)
Get-DnsClientCache	h)
Clear-DnsClientCache	b)

Los comandos del Símbolo del Sistema son:

- a) ping www.google.es
- b) ipconfig /flushdns
- c) tracert www.google.es
- d) netstat -na
- e) ipconfig /all
- f) route print
- g) ipconfig
- h) ipconfig /displaydns

Ejercicio 6: Comparativa comandos de red Windows/Linux

Dada la siguiente tabla, completa con el comando Windows o Linux equivalente (incluyendo parámetros):

Windows	Linux
ping -n 5 www.google.es	ping -c 5 www.google.es
ping -n 6 -l 300 192.168.0.1	ping -c 6 -s 300 192.168.0.1
arp -a	ip neigh show
ipconfig /all	ip address
netstat -n -p tcp	ss -nt
route print	ip route

Ejercicio 7: Resolución de errores en una LAN (I)

Dadas las siguientes situaciones, indica una posible causa y una posible solución para cada caso. Si hay múltiples causas de error, solo será necesario que indiques una.

a) Envías pings a equipos del exterior usando su nombre y no funcionan, pero si envías pings con la IP sí que funcionan

Causa:

El servidor DNS no funciona

Solución:

Usar otro

b) Envías pings a www.google.es y no funcionan pero si envías pings a www.bing.es o cualquier otro nombre, sí que funcionan

Causa:

Google no responde pings, no hay problema en mi LAN

Solución:

Ninguna, no falla mi red

c) Envías pings a otro equipo de tu LAN y sí que funcionan pero al enviar cualquier ping al exterior no funciona

Causa:

Posible error en el equipo que hace de puerta de enlace (suele ser el router)

Solución:

Verificar el correcto funcionamiento de la puerta de enlace y comprobar también que el servidor DHCP reparte la puerta de enlace correcta a los clientes

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

d) Envías pings a otro equipo de tu LAN situado en la misma sala y sí que funcionan, pero al enviar cualquier ping a otro equipo de la LAN situado fuera de tu sala, no funciona. Tampoco funcionan pings al exterior.

Causa:

Posible error en el cable entre el switch y el exterior de la sala, o posibles errores en la tabla de encaminamiento de los equipos

Solución:

Verificar y comprobar los cables entre switches, modificar las tablas de encamamiento para que sean correctas en el caso de que estuvieran mal

e) Envías pings a cualquier equipo de tu LAN o del exterior y sí que funcionan, excepto al enviar ping a un equipo concreto situado en la misma sala que el tuyo.

Causa:

Error en el equipo destino (o no responde pings)

Solución:

Verificar el equipo destino, su tarjeta de red y el cable que lo une al switch

f) No funciona ningún ping enviado por tu equipo. El resto de equipos de tu LAN sí funcionan bien y tienen acceso

Causa:

Error en mi equipo

Solución:

Comprobar tarjeta de red del equipo y también el cable que une mi equipo con el switch

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

g) No funciona ningún ping enviado por tu equipo y el resto de equipos de tu LAN tampoco funcionan bien

Causa:

Error general en la red

Solución:

Verificar el servidor DHCP y la puerta de enlace (sus tarjetas, cables y switches a los que están conectados)

Ejercicio 8: Resolución de errores en una LAN (II)

Veamos solamente algunas de las numerosas secciones que tiene esta herramienta:

- ***All nodes managed by NPM:*** Aquí aparece un listado de TODOS los dispositivos de la LAN, clasificados por su fabricante (Cisco, IBM,...) o el tipo de SO (Windows, Linux,...). Haz clic en "Manage nodes" para ver todos los nodos o dispositivos conectados. Luego haz clic en "Windows". Verás una tabla con cuatro columnas.

¿Qué indica cada una de las cuatro columnas?

Nombre del equipo, IP, versión de IP, estado

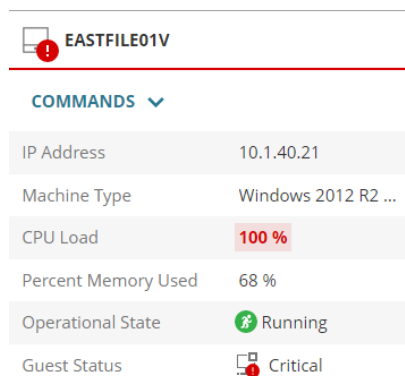
Cada dispositivo está clasificado con un color (rojo, amarillo, verde). ¿Qué indican los colores?

Rojo: error, amarillo: advertencia, verde: OK

Si dejas el ratón quieto unos instantes sobre un equipo (sin hacer clic en él), verás información adicional como el tiempo _medio_ de respuesta, la _carga_ de la CPU o el porcentaje de _memoria_ usada.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Pega aquí un pantallazo donde se vea un equipo que tenga una carga de CPU extremadamente alta.



EASTFILE01V	
COMMANDS ▾	
IP Address	10.1.40.21
Machine Type	Windows 2012 R2 ...
CPU Load	100 %
Percent Memory Used	68 %
Operational State	Running
Guest Status	Critical

Vuelve a la pantalla principal haciendo clic en My Dashboards, Network, NPM Summary.

- **MPLS network:** Aquí aparece un esquema de los diferentes routers de la red y cómo están organizados. Haz clic en “View Mode”.

En cada router aparece el estado actual (rojo o verde) de tres características. ¿Cuáles?

Temperatura, ventiladores y batería.

Las líneas que unen dispositivos están etiquetadas con dos números en cada extremo. ¿Qué indican esos datos?

Velocidad del enlace y porcentaje de uso

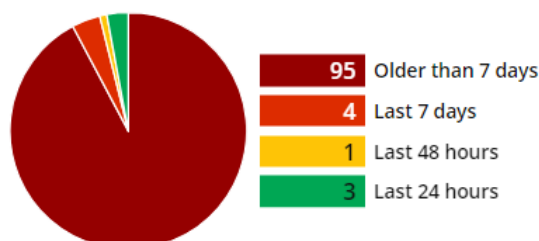
Finalmente, ve a My Dashboards, Network Configuration, Config Summary.

- **Config Summary:** Pega un pantallazo para cada apartado donde se vea claramente la respuesta a cada pregunta:

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

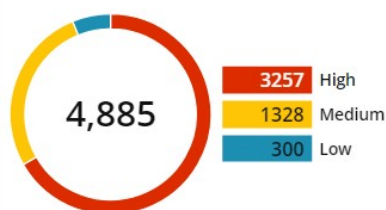
¿Cuántos dispositivos hicieron copia de seguridad (backup) de su configuración hace más de 7 días?

Last config backup date



¿Cuántas vulnerabilidades del firmware son catalogadas como altas?

Firmware vulnerabilities



Listado donde aparezca cuándo expira el soporte técnico para cada dispositivo.

End of Support

Display Name	Expiration Date
EASTADDC01v	2023-04-30T13:45:20.12
EASTFILE01v	2023-07-04T13:45:20.12
EASTROOTCA	2023-06-20T13:45:20.12

Para terminar con SolarWinds, busca en sus numerosos menús, escoge dos secciones adicionales que no hayan sido mencionadas y te parezcan interesantes, y explica para qué crees que sirven, junto a un pantallazo de cada una.

Ejercicio 9: Resolución de errores en una LAN (III)

A continuación verás dos listados, uno con problemas y otro con posibles soluciones. Asocia en la hoja final los problemas con la solución más adecuada para cada caso. Las soluciones propuestas son orientativas y genéricas.

Problemas

1. La tarjeta de red no funciona. Sus LEDs aparecen siempre apagados, incluso probando con otro cable de repuesto.
2. La conexión de un PC va demasiado lenta. La tarjeta de red es Fast Ethernet. El equipo no parece tener ningún otro problema.
3. El router tiene funcionalidad limitada y problemas de estabilidad. Se detectan también incompatibilidades entre el router y algunos dispositivos.
4. Un PC no se conecta a la red, pese a que en días anteriores sí que lo hacía correctamente. El resto de equipos funcionan con normalidad.
5. Un portátil (conexión inalámbrica) va demasiado lento al acceder a la red.
6. En un servidor aparece el mensaje "Conflicto de direcciones"
7. Un equipo con IP dinámica, al que antes siempre se le asignaba la misma IP dinámica sin problema, recibe una IP del rango 169.x.x.x desde hace unos días. Recientemente se sustituyó su tarjeta de red por otra más potente y desde entonces no tiene conexión. Los LEDs de la tarjeta y del switch se iluminan correctamente.
8. Toda la red en general va lenta.
9. A determinadas horas y solo en determinadas zonas de la LAN, la red va lenta.
10. De repente, ningún equipo recibe IP dinámica.
11. El antivirus de un equipo alerta de una posible infección

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Soluciones

- a) Reemplazar la tarjeta de red por otra idéntica.
- b) El administrador recientemente cambió la IP estática de un equipo, y esa IP está dentro del rango de direcciones a repartir por el servidor DHCP. Hay que modificar la IP estática que se cambió, o excluirla del rango a repartir.
- c) Comprobar si ambos extremos del cable están bien conectados y verificar si el cable no está dañado. Sustituirlo, de ser así.
- d) Comprobar mediante un analizador de tráfico que los usuarios no están viendo contenido no permitido que posiblemente sature la red (por ejemplo, streaming o continuas descargas de gran tamaño). Estudiar el rendimiento de los servidores de manera individualizada. Comprobar el estado general de los switches.
- e) Actualizar la tarjeta de red sustituyéndola por una Gigabit Ethernet. Estudiar el rendimiento general del equipo si persistiera el problema.
- f) Confinar todos los archivos sospechosos y dejarlos en cuarentena. Aislar el equipo para que no intercambie datos con el resto. Desinfectar el equipo. Registrar los posibles envíos de datos llevados a cabo por el usuario del equipo (posible compartición de pendrives o de archivos infectados). Estudiar el uso de los puertos del equipo en busca de un virus que intente propagarse por la red. Obtener el ejecutable asociado a la infección y eliminarlo (de la RAM, del disco y de su posible carga al iniciar el equipo). Restaurar la copia de seguridad más reciente del equipo para evitar una mayor pérdida de datos y dejarlo en un estado correcto. Analizar el resto de la red por si hubiera posibles infecciones adicionales.
- g) Intentar acercar el portátil al router inalámbrico o punto de acceso. Analizar el uso de los canales y elegir un canal más libre. Comprobar la compatibilidad entre los estándares soportados por la tarjeta de red inalámbrica y el router o punto de acceso. Estudiar el rendimiento general del portátil.
- h) El firewall de la red (situado también en el servidor DHCP) avisa de que su log ha desbordado el disco duro interno. Limpiar o eliminar el log y reiniciar el servidor.
- i) Actualizar el firmware del router por una versión más reciente.
- j) Realizar la nueva reserva asociada con la MAC adecuada en el servidor DHCP.
- k) Usar un analizador del tráfico para comprobar si hay equipos que tal vez envían demasiado tráfico por difusión en esas zonas de la red. Estudiar la posibilidad de usar VLAN o subnetting para disminuir la difusión. Reiniciar los switches de las zonas afectadas.

CIPFP Ausiàs March (Valencia)
1º de SMR (Sistemas Microinformáticos y Redes). Modalidad semipresencial
Módulo: Redes Locales
Actividades Unidad 9: Protección, vigilancia y soporte de redes

Problema	Solución
1	a
2	e
3	i
4	c
5	g
6	b
7	j
8	d
9	k
10	h
11	f