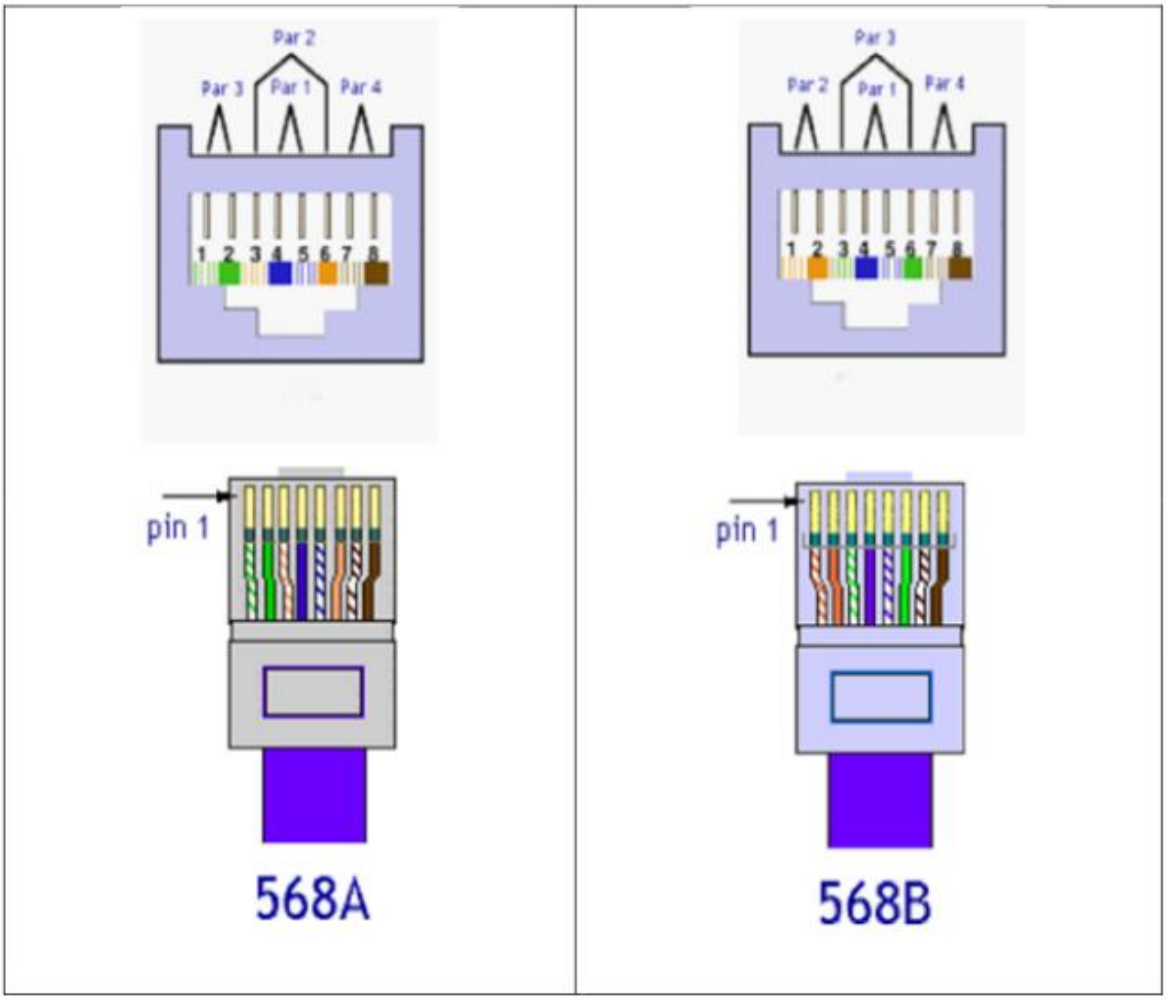
PRÁCTICA 3 .4 - Acceso Físico a la Red

1. Busca información acerca de las normas TIA 568A y TIA 568B. Haz un breve resumen.



Los 568A y 568B intentan definir estándares que permitirán el diseño e implementación de sistemas de cableado.

El TIA 568B indica que, con el conector RJ-45 presentando la cara plana ha de presentar, de izquierda a derecha los siguientes colores:
Blanco/naranja Naranja Blanco/Verde Azul Blanco/Azul Verde Blanco/Marrón Marrón

2. Explica brevemente qué diferencia hay entre CSMA/CD y CSMA/CA. ¿Dónde se usa cada una?

- **CSMA/CD:** Detecta las colisiones. Se puede utilizar en redes cableadas, pero no en inalámbricas.
- **CSMA/CA:** (acceso múltiple por detección de portadora y prevención de colisiones) Intenta evitar las colisiones. Se utiliza en redes inalámbricas.

3. Explica cuáles son las ventajas e inconvenientes del uso de Wi-Fi frente a Ethernet cableado.

Ventajas:

-Al ser inalámbrica, la red no requiere ninguna estructura de cables.

-Los paquetes de datos se envían más rápido, y sin riesgo de colisión.

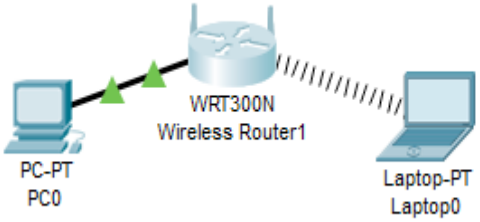
Desventajas:

-Es más caro que el cableado.

-La seguridad es más sensible, ya que hay que configurarla más.

-Tiene peor estabilidad.

4. En el simulador Packet Tracer diseña una red doméstica con un Wireless Router Linksys y 2 equipos uno de sobremesa y un portátil que se conectará a través de WiFi. La configuración de red de los equipos se realizará automáticamente por DHCP. Indica que configuración de red tienen los equipos y comprueba que hay conexión entre ellos con un ping. Visualiza la trama que sale del equipo de sobremesa y compárala con una que salga del portátil. Haz un esquema comparativo de una trama 802.11 con una trama 802.3.




```
C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=16ms TTL=128
Reply from 192.168.0.100: bytes=32 time<1ms TTL=128
Reply from 192.168.0.100: bytes=32 time=7ms TTL=128
Reply from 192.168.0.100: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 8ms
```

PC0:

- IP: 192.168.0.101
- GATEWAY: 192.168.0.1

Laptop0:

- IP: 192.168.0.100
- GATEWAY: 192.168.0.1

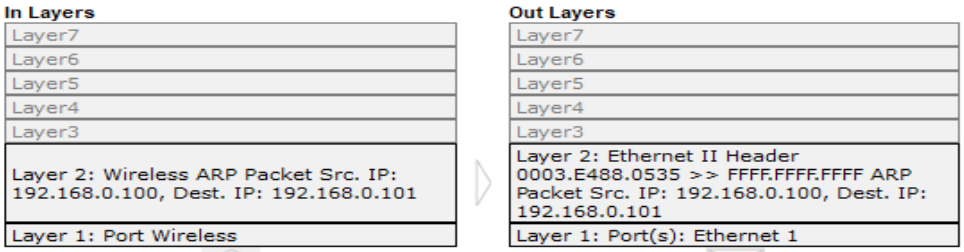
Router0:

- IP: 192.168.0.1

Sale del PC:

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 0030.F28B.ED85 >> 0003.E488.0535 ARP Packet Src. IP: 192.168.0.101, Dest. IP: 192.168.0.100	Layer 2: Wireless ARP Packet Src. IP: 192.168.0.101, Dest. IP: 192.168.0.100
Layer 1: Port Ethernet 1	Layer 1: Port(s): Wireless

Sale del Portatil:



5. Explica los distintos métodos de seguridad que implementan los puntos de acceso WiFi. Configura alguno en el Linksys usado en el ejercicio anterior. ¿Qué es WPS referido a WiFi?

-WEP (Wired Equivalent Privacy): la encriptación WEP es vulnerable y no se debe utilizar.
•WPA (Wi-Fi Protected Access): Este es básicamente el cifrado estándar WPA o WPA1. Se ha superado y no es seguro.
•WPA2-PSK (TKIP): Se utiliza el estándar WPA2 con cifrado TKIP. Esta opción no es segura, sin embargo, es la mejor opción si se tienen dispositivos antiguos que no soportan una red WPA2-PSK (AES).
•WPA2-PSK (AES): Esta es la opción más segura si no se dispone de WPA3. Utiliza WPA2, con el protocolo de encriptación AES.
•WPA2-Enterprise (WPA2-802.1x): Este modo proporciona la seguridad necesaria para las redes inalámbricas en el mundo empresarial. Ofrece control individualizado y centralizado sobre el acceso a la red Wi-Fi utilizando un servidor RADIUS.
•WPA3: utiliza un cifrado más robusto, con arquitectura de seguridad de 192 bits,pensado para el tratamiento de datos confidenciales. Mayor protección, incluso en aquellos casos en los que el usuario no cuenta con contraseñas robustas. Esto le confiere un mayor grado de protección ante los ataques de fuerza bruta. Procesos de configuración más simplificados, incluso para dispositivos sin pantalla. Se refuerza la protección en redes públicas, cifrando el tráfico entre nuestro dispositivo y el punto de acceso. WPA3 Forward Secrecy, es una característica que evita que un atacante pueda descifrar el tráfico capturado.

WPS: WiFi Protected Setup es la tecnología que abre de manera temporal el punto de acceso a los dispositivos cercanos que compatibles con esta opción. Una vez activado el Botón WPS tu terminal buscará el router al que conectarse sin contraseña. Es más cómodo para el usuario a la hora de conectarse por WiFi, pero a la vez mucho menos seguro.

6. Busca un punto de acceso WiFi en alguna tienda online que soporte 802.1q, 802.3at, 802.11ac, y 802.11s. Explica a que se refiere cada una de esas normas y adjunta una captura de pantalla de las especificaciones del punto de acceso que hayas encontrado.

- 802.1q - Una VLAN nativa que está asignada a un puerto troncal 802.1Q
- 802.11s - Estándar de red inalámbrico y una enmienda al protocolo IEEE para las redes en malla.
- 802.11at – Este estándar, incluye la función PoE, que permite la alimentación de energía a través de la red.
- 802.11ac – opera en la banda de 5Ghz e incorpora varias tecnologías nuevas como el **beamforming**, que aumenta la señal en la dirección de los dispositivos conectados y **MU-MIMO** que permite varias conexiones simultaneas con varios equipos.

Ubiquiti UniFi UAP-AC-PRO Punto de Acceso Doble Banda PoE 2.4 GHz

Velocidad 2.4Ghz: 450Mbps

Velocidad 5Ghz: 1300Mbps

Modo PoE: 802.3af PoE / 802.3at PoE+

Interfaz de Red: 2 x 10/100/1000 Ethernet

Antenas:
- 3 x antenas Dual?Band,
- 2.4 GHz: 3 dBi, 5 GHz: 3 dBi

Wi-Fi Standards: 802.11 a/b/g/n/ac

Seguridad Wireless:
- WEP
- WPA-PSK
- WPA-Enterprise (WPA/WPA2, TKIP/AES)

Ambiente: Interior / Exterior

Dimensiones: ?196.7 x 35 mm

Peso: 350 g

Botones: Reset

Fuente de alimentación:
- 48V, 0.5A PoE Gigabit Adaptador

Consumo máx.: 9W

Power Save Soportado

Certificaciones: CE, FCC, IC

Montaje: Wall/Ceiling (Kits Included)

Temperatura de operación: -10 a 70° C (14 a 158° F)

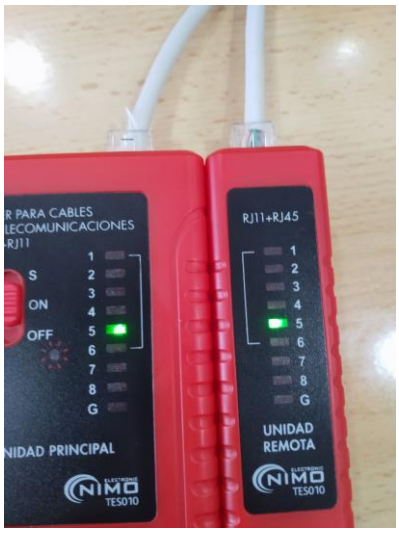
7. Por parejas montar un latiguillo de red directo y verificar sus conexiones. Comprobar el cable con un tester de cables de red ¿cómo indica que el cable es directo y que es correcto?. Adjunta una foto del cable creado donde se visualicen los 2 extremos y otra con la comprobación del tester.

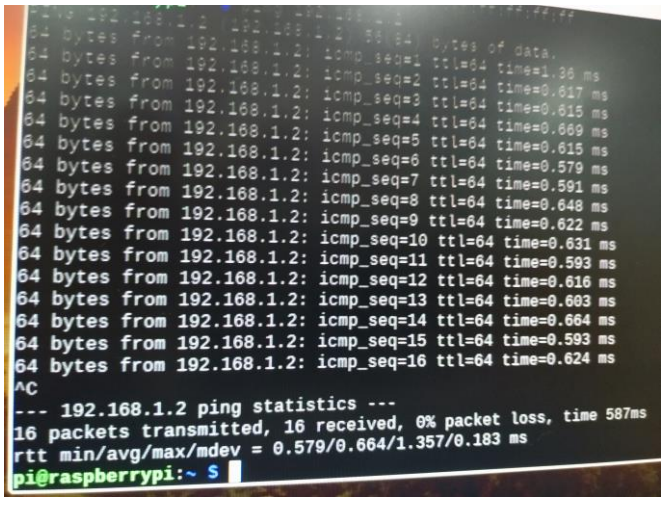
En el tester tienen que coincidir las luces de un lado con el otro en todos los leds, del uno al 8.

8. Siguiendo los mismos pasos del ejercicio anterior, montar un latiguillo de red cruzado y verificar sus conexiones. Conecta directamente 2 hosts con el cable cruzado, configura un equipo con la IP "192.168.1.1" y el otro equipo con la IP "192.168.1.2", comprueba con un ping que hay conectividad entre los dos equipos.

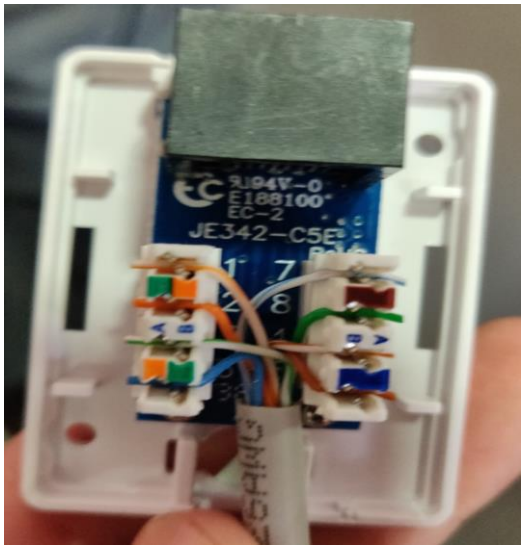
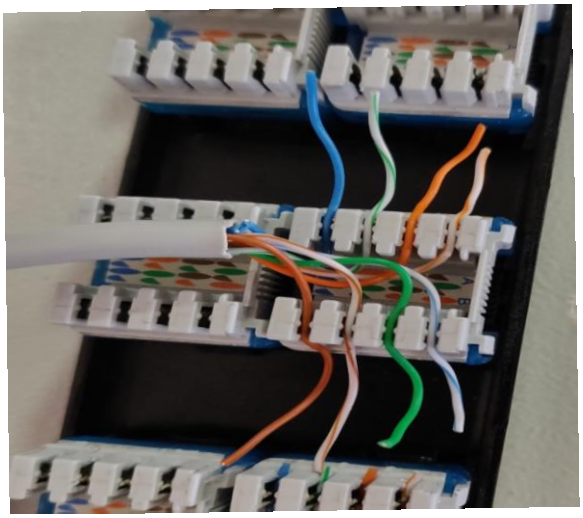
Cables creados y ping probados por Axel y Kevin.

Prueba de conexión y ping.

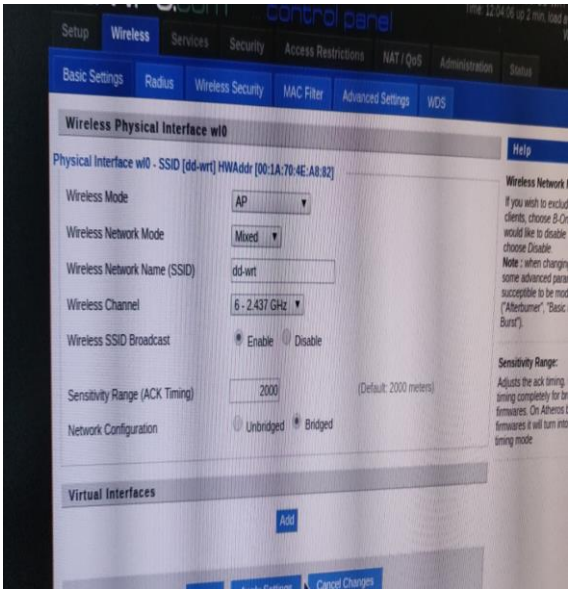


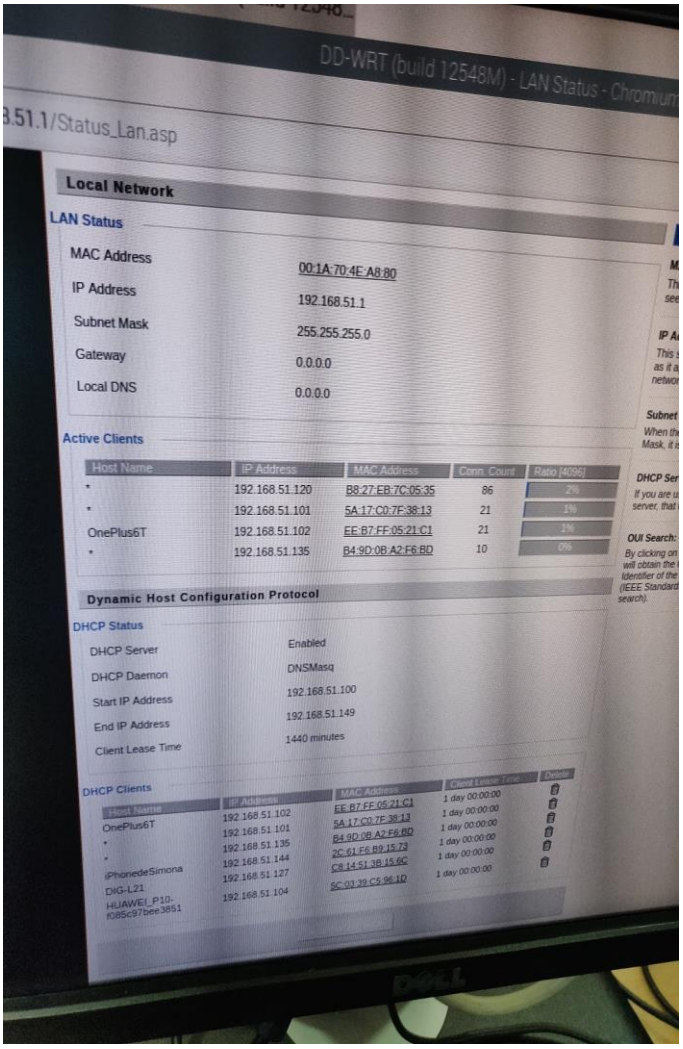


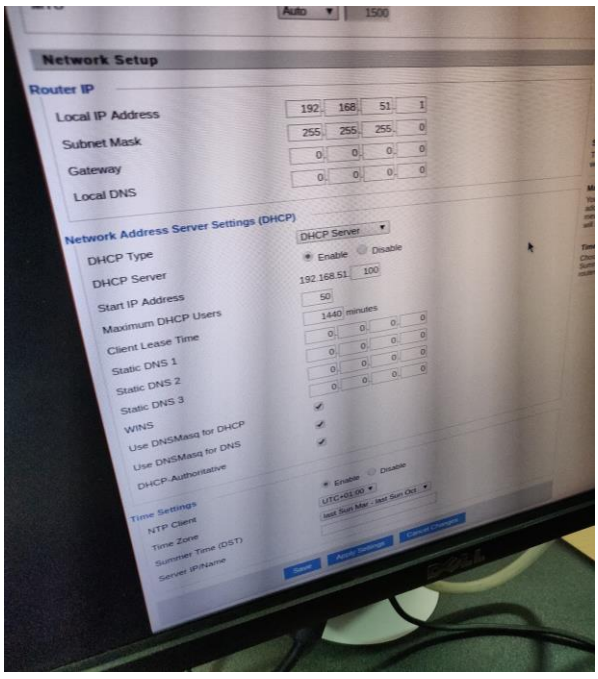
9. Con los latiguillos directos creados, monta una red con los compañeros de tu fila para al menos 2 hosts. La red deberá tener, si hay disponibilidad, una roseta conectada al patch panel de un rack, un switch (al que podemos conectar directamente el resto de equipos), un router y conexión WiFi. Los equipos obtendrán por DHCP una IP de la red "192.168.5X.0/24", siendo X el número de tu fila. Comprueba con un ping que tienes acceso a los hosts conectados, que puedes unir un móvil a la red y que puedes navegar por Internet. Indica todas las configuraciones realizadas y adjuntas fotos de la instalación.

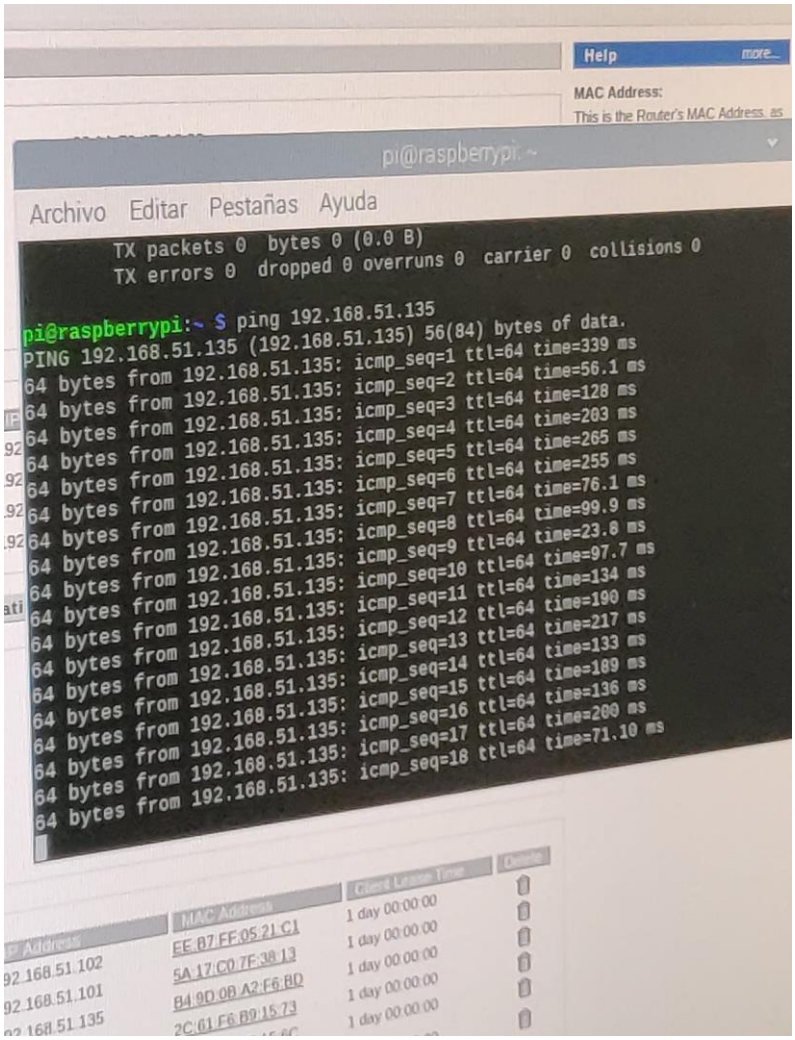
Roseta	
	

Configuración Router



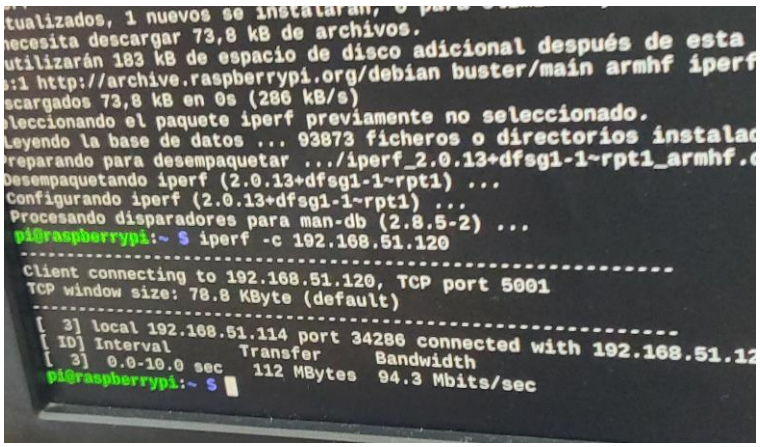

DD-WRT (build 12548M) - LAN Status - Chromium
3.51.1/Status_Lan.asp
Local Network
LAN Status
MAC Address 00:1A:70:4E:A8:80
IP Address 192.168.51.1
Subnet Mask 255.255.255.0
Gateway 0.0.0.0
Local DNS 0.0.0.0
Active Clients
Host Name | IP Address | MAC Address | Conn. Count | Ratio [4096]
* 192.168.51.120 B8:27:EB:7C:05:35 86 2%
* 192.168.51.101 5A:17:C0:7F:38:13 21 1%
OnePlus6T 192.168.51.102 EE:B7:FF:05:21:C1 21 1%
* 192.168.51.135 B4:9D:0B:A2:F6:BD 10 0%
Dynamic Host Configuration Protocol
DHCP Status
DHCP Server Enabled
DHCP Daemon DNSMasq
Start IP Address 192.168.51.100
End IP Address 192.168.51.149
Client Lease Time 1440 minutes
DHCP Clients
Host Name | IP Address | MAC Address | Client Lease Time | Delete
OnePlus6T 192.168.51.102 EE:B7:FF:05:21:C1 1 day 00:00:00
* 192.168.51.101 5A:17:C0:7F:38:13 1 day 00:00:00
* 192.168.51.135 B4:9D:0B:A2:F6:BD 1 day 00:00:00
iPhonedeSimona 192.168.51.144 2C:61:F6:B9:15:73 1 day 00:00:00
DIG-L21 192.168.51.127 C8:14:51:3B:15:6C 1 day 00:00:00
HUAWEI_P10-f085c97bee3651 192.168.51.104 5C:03:39:C5:96:1D 1 day 00:00:00


Auto
1500
Network Setup
Router IP
Local IP Address 192.168.51.1
Subnet Mask 255.255.255.0
Gateway 0.0.0.0
Local DNS 0.0.0.0
Network Address Server Settings (DHCP)
DHCP Type DHCP Server
DHCP Server Enable Disable
Start IP Address 192.168.51.100
Maximum DHCP Users 50
Client Lease Time 1440 minutes
Static DNS 1 0.0.0.0
Static DNS 2 0.0.0.0
Static DNS 3 0.0.0.0
WINS
Use DNSMasq for DHCP
Use DNSMasq for DNS
DHCP-Authoritative
Time Settings
NTP Client Enable Disable
Time Zone UTC+03:00
Summer Time (DST) last Sun Mar - last Sun Oct
Server IP/Name
Save
Apply Settings
Cancel Changes



10. ¿Cuál es el ancho de banda teórico entre 2 equipos del ejercicio anterior? Realiza una prueba de rendimiento. Instala en 2 equipos iperf "sudo apt install iperf", en un equipo ejecuta "iperf -s" y en el otro equipo "iperf -c IP_equipo1". Explica los resultados obtenidos.

Teórico: 100Mbits/s. **Real:** 94'3Mbits/s



El ordenador que ejecuta **iperf -s** hace de "servidor", y el que ejecuta **iperf -c 192.168.51.120** hace de "cliente". El cliente establece la conexión con el servidor, y le envía un paquete de 112MB. En base a lo que tarda en llegar, se calcula el ancho de banda real entre los dos equipos, en este caso 94,3Mb/s.