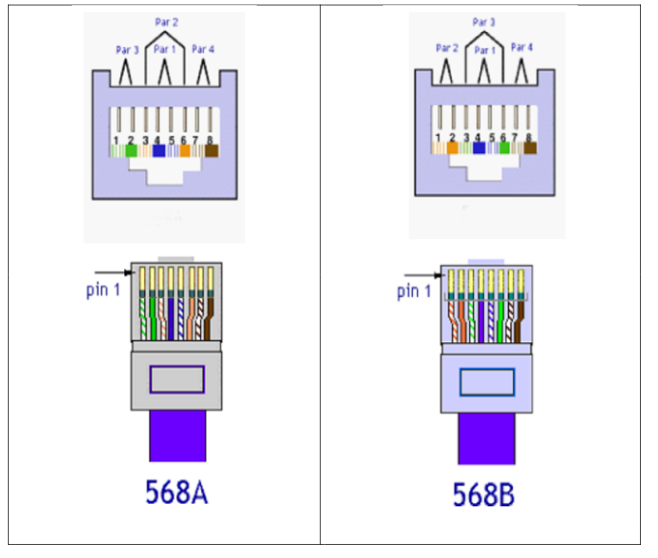
**1. Busca información acerca de las normas TIA 568A y TIA 568B. Haz un breve**

**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**

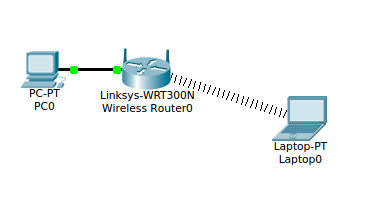
**de WiFi. La configuración de red de los equipos se realizará automáticamente**

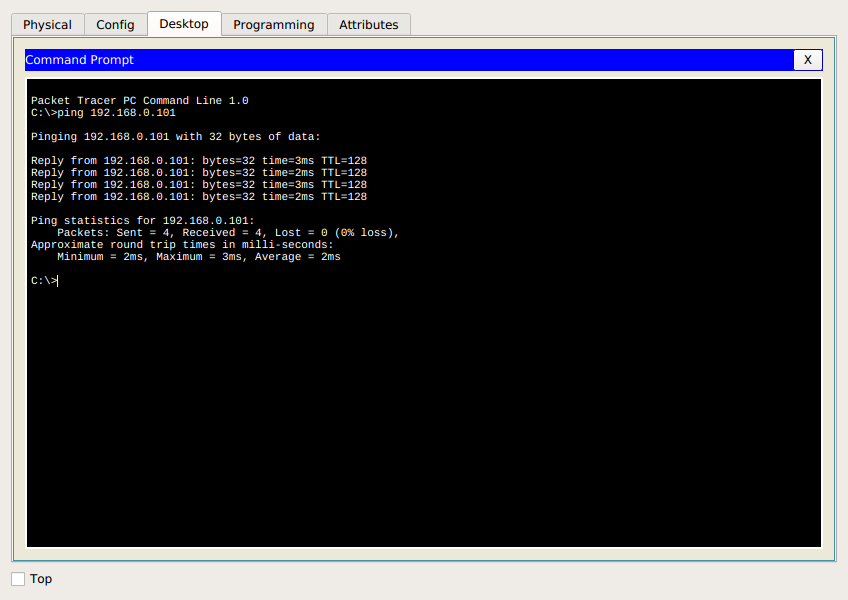
**por DHCP. Indica que configuración de red tienen los equipos y comprueba que**

**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.**

****



**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:** es el nombre de la red local creada, hecho para que sea más fácil conectarse a él sin tener que buscar la IP de la red.

**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 está asignada a un puerto troncal 802.1Q
* 802.1p - (integrado posteriormente en 802.1q) – Tráfico por prioridades
* 802.3 – Estilo de trama Ethernet
* 802.11 – La tecnología de LAN inalámbrica (WLAN), comúnmente denominada “Wi-Fi”
* 802.11s - Estándar de red inalámbrico y una enmienda al protocolo IEEE para las [redes en malla](https://es.wikipedia.org/wiki/Red_inalámbrica_mallada)
* 802.11ac - Estándar de red más reciente utilizado en seguridad inalámbrica.

**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.

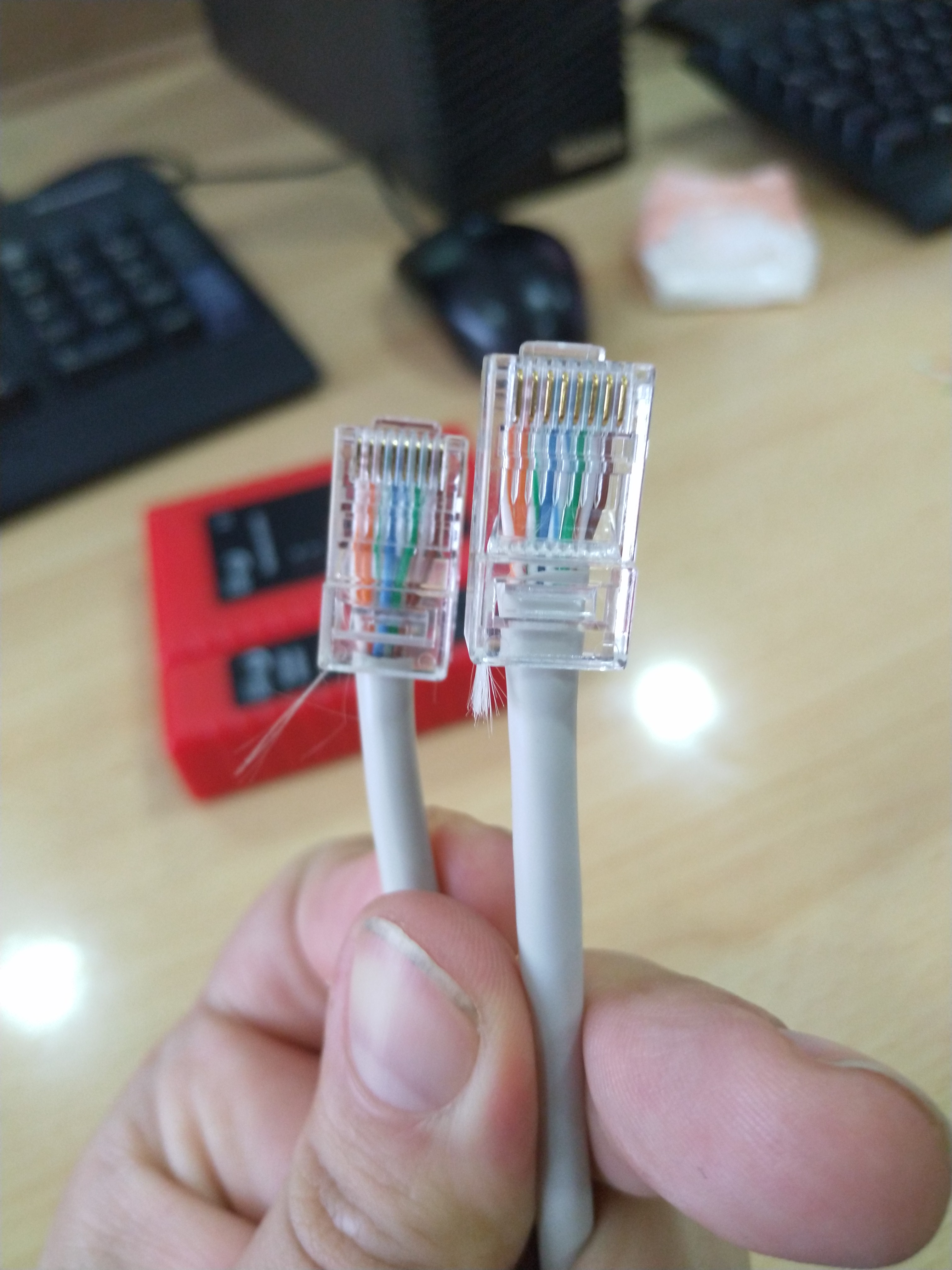


Foto cable directo en TIA 568B.

****

**8. Siguiendo los mismos pasos del ejercicio anterior, montar un latiguillo de red**

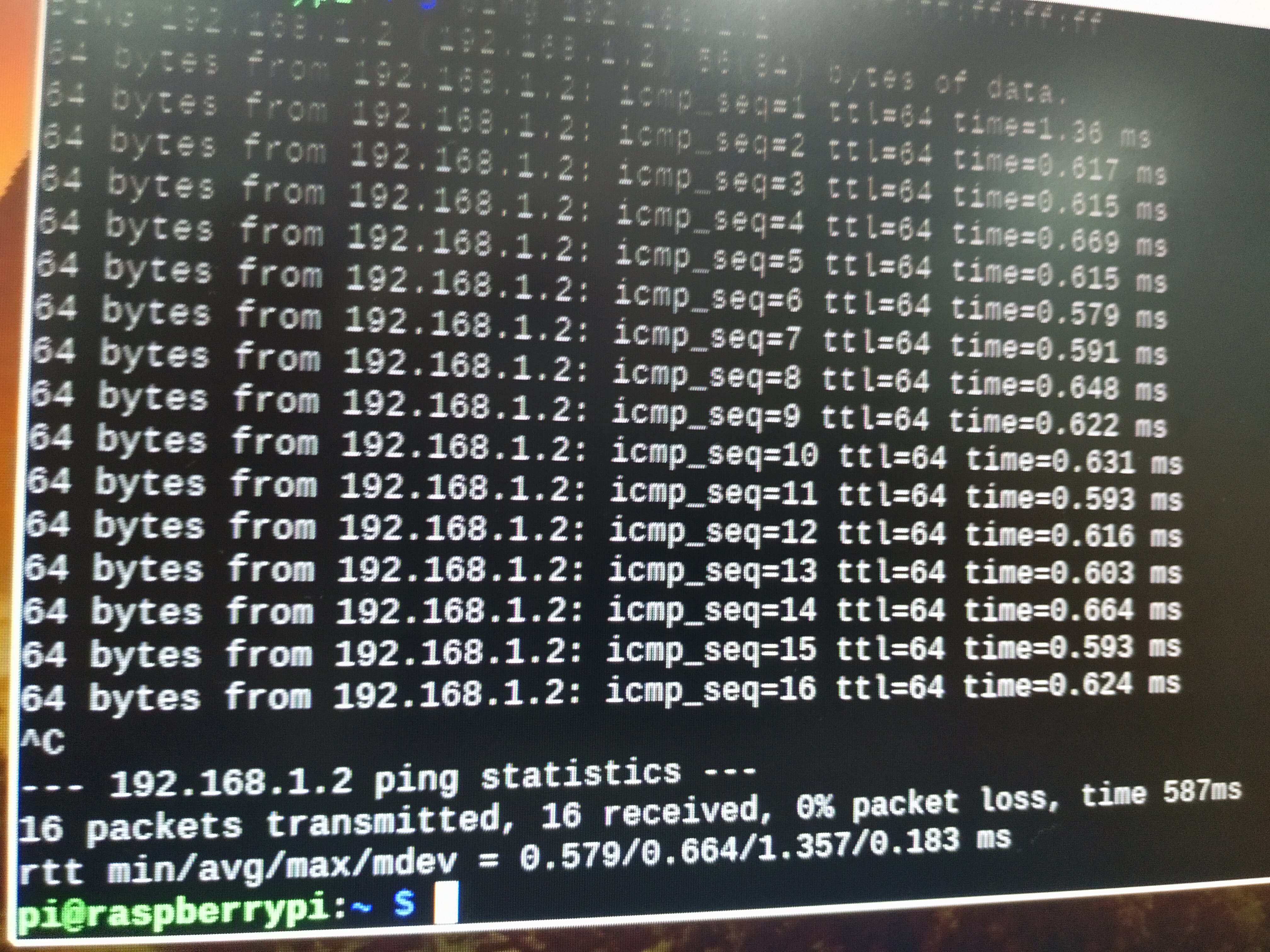
**cruzado y verificar sus conexiones. Conecta directamente 2 hosts con el cable**

**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 adjunta fotos de la instalación.**

**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**: Como máximo 100Mbits/segundo.