Casos prácticos

Redes y aplicaciones telemáticas

Telefónica EDUCACIÓN DIGITAL

Casos prácticos

1 | Diseño de una red

Una empresa quiere crear una red propia con dos tipos diferentes de redes:

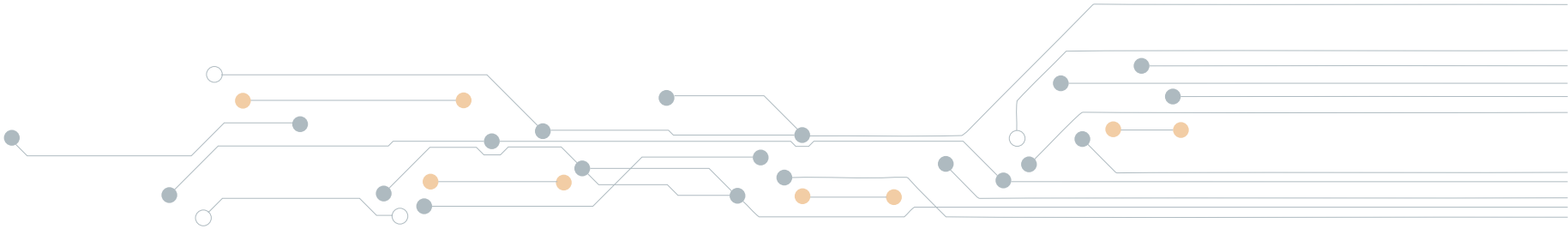
10.0.0.0/8

11.0.0.0/8

A su vez, cada red tiene 3 equipos diferentes. Por ejemplo, 10.0.0.2, 10.0.0.3 y 10.0.0.4 para la red 10.0.0.0/8. Mientras que para la red 11.0.0.0/8, se tiene 11.0.0.2, 11.0.0.3 y 11.0.0.4.

¿Cuántos routers se necesitan para implementar esta red? Haz un diseño óptimo de modo que todos los equipos tengan conectividad con el resto de equipos de otras redes.

NOTA. Se recomienda utilizar un software del estilo Packet Tracer de CISCO para modelar las redes.



1 | Solución

Simplemente, debe ponerse 1 router. Se debe configurar el router con 2 interfaces de red, añadiendo la dirección 10.0.0.1 a la interfaz de red 1, y la dirección 11.0.0.1 a la interfaz de red 2. Además, se deben añadir 2 switches, uno para la red 10.0.0.0/8 y otro para la 11.0.0.0/8. Los 3 equipos de cada red deben estar conectados al switch, por lo que pueden hacerse ping entre ellos. El switch estará conectado al router por su interfaz correspondiente. Al final los equipos de la red 10.0.0.0/8 deben hacer ping con los de la red 11.0.0.0/8

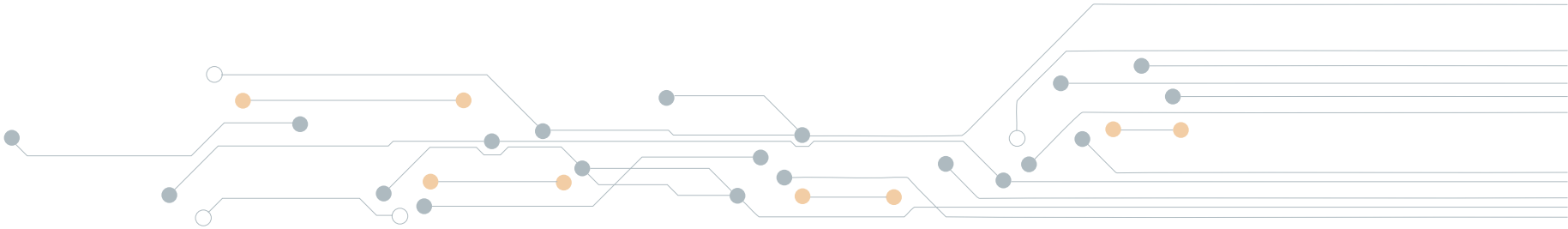
2 | Detección de un ataque ARP Spoofing

En esta práctica estudiaremos la detección y derogación de un ataque ARP Spoofing, mediante dos métodos diferentes:

NOTA. Hay que utilizar una máquina virtual con Windows XP o Windows 7 y una máquina virtual con la distribución de Kali Linux. (Es recomendable utilizar una configuración de red en la máquina virtual de tipo puente o bridge). En primer lugar, llevar a cabo un ataque ARP Spoofing de la máquina Kali Linux (atacante) a la máquina Windows (víctima).

a. Tabla estática. Modifica la entrada del router (suele ser 192.168.1.1, pero podría tener otro valor) en la tabla ARP de tu máquina virtual y conviértela en estática. Prueba MITM y explica qué ocurre.

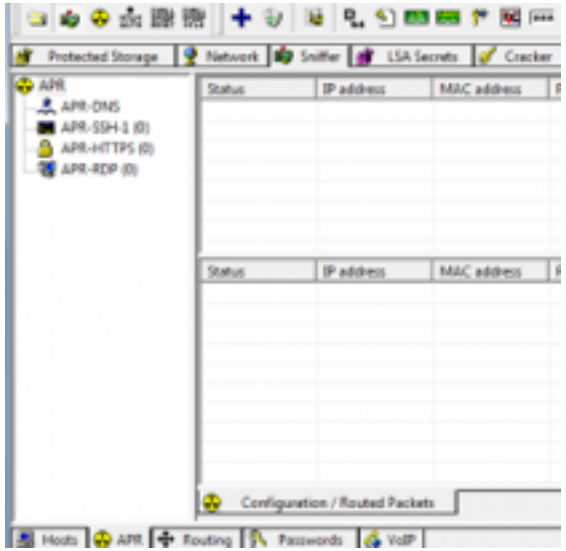
b. Instala XARP y prueba las diferentes configuraciones de la herramienta. Comenta los resultados.



Una vez seleccionadas las direcciones IP, se debe pulsar sobre el tercer botón de la izquierda, el que está al lado del de la tarjeta de red que se pulsó anteriormente. Ambos deben quedar pulsados.

Se puede ver un video resumen en este enlace:

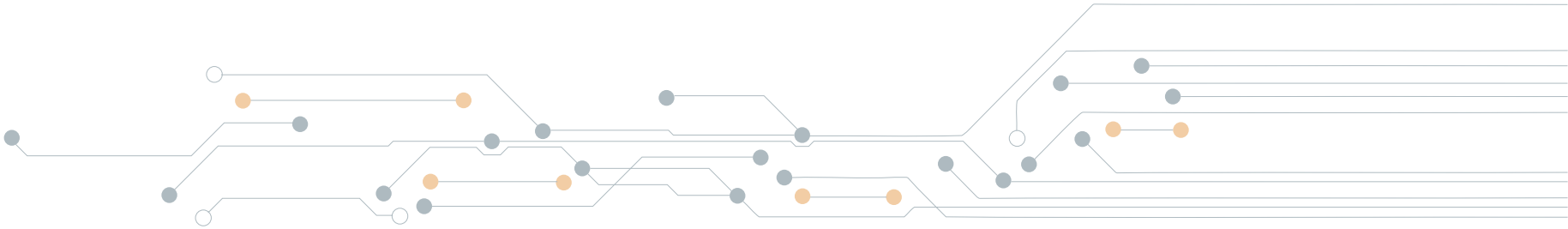
https://www.youtube.com/watch?v=oB0D-m5AVFQ



Los siguientes scripts tienen como objetivo la monitorización de la tabla ARP y avisar al usuario de cuándo se producen cambios en puntos clave:

Script 1

```
#!/bin/bash
if [ $# -ne 1 ]
then
   echo “usage ./mitm.sh <MAC>”
   exit
fi
mac/$1
while true
do
   entradaRouter=$(arp –a | grep 192.168.1.1 | cut –d’ ‘-f4)
   if [ $mac != $entradaRouter]
   then
         echo “Cambio de MAC”
   exit
fi
sleep 2
```



Script 2

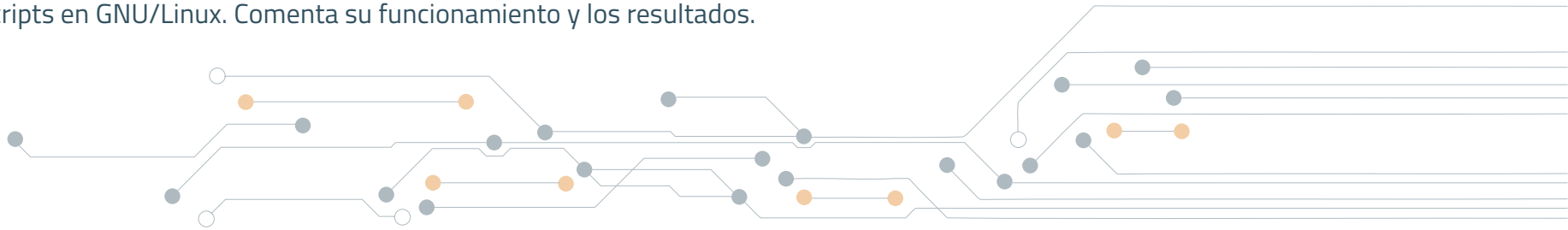
El primer paso es indicar cuándo se produce el cambio de Mac:

```
If [ $mac!= $entradaRouter]
Then
   Echo “La Mac ha cambiado”
Exit
Fi
```

Lo cambiaremos por la siguiente orden:

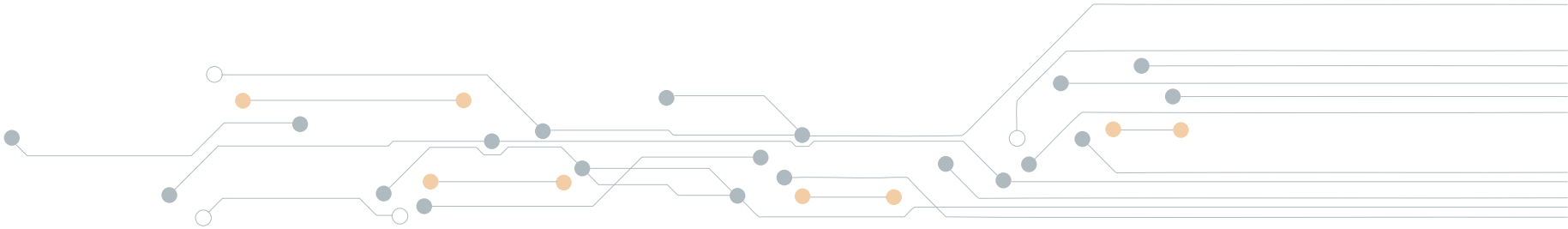
```
If [$mac!= $entradaRouter ]
Then
Echo “La Mac ha cambiado”
Ifconfig <dispositivo de red, ejemplo eth0> down
Exit
fi
done
```

Ejecuta estos scripts en GNU/Linux. Comenta su funcionamiento y los resultados.



3 | Solución

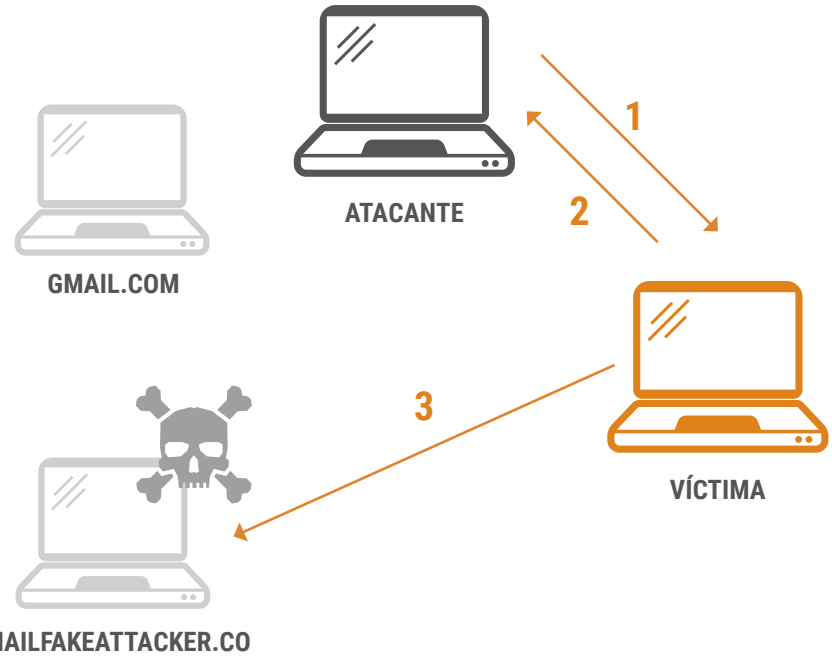
Estos scripts deben ser escritos en bash en el sistema Kali Linux. Abrir un editor de textos y guardar como script1.sh y script2.sh. Se les debe dar permisos con chmod u+x, para que sean ejecutables. El resultado es que se notificará primero la existencia de un ataque ARP Spoofing y con el segundo se tirará abajo la interfaz de red, por lo que se detendrá el ataque.



4 | DNS Spoofing

En esta práctica realizaremos un DNS Spoofing utilizando Caín. El objetivo es situarnos entre el equipo de la víctima y el DNS interno de la red, como muestra el siguiente esquema:

- El atacante está en medio de la comunicación entre la víctima y el servidor DNS. Cuando la víctima envía una petición DNS al servidor legítimo, ésta es interceptada.
- El atacante reenvía la respuesta DNS falsificada, es decir, la dirección IP que se devuelve a la víctima no corresponde con el dominio legítimo solicitado.
- La víctima se conecta con un sitio malicioso, en vez de conectarse con el sitio web legítimo. La víctima se estará conectando a un sitio web dónde le podrían robar, entre otras cosas, las credenciales.



El atacante actuará como DNS de la víctima por lo que podrá redirigirla hacia donde el atacante desee. Podemos acoplar un servidor web en la propia máquina del atacante y realizar una suplantación de una página web.

Pasos a realizar:

1. Hacer MiTM entre la víctima y el DNS.

2. Definir dónde vamos a redirigir a la víctima.

3. Una vez que hemos hecho esto tenemos el control de la resolución de nombres de la víctima. Piensa qué puedes hacer con dicho control.

4 | Solución

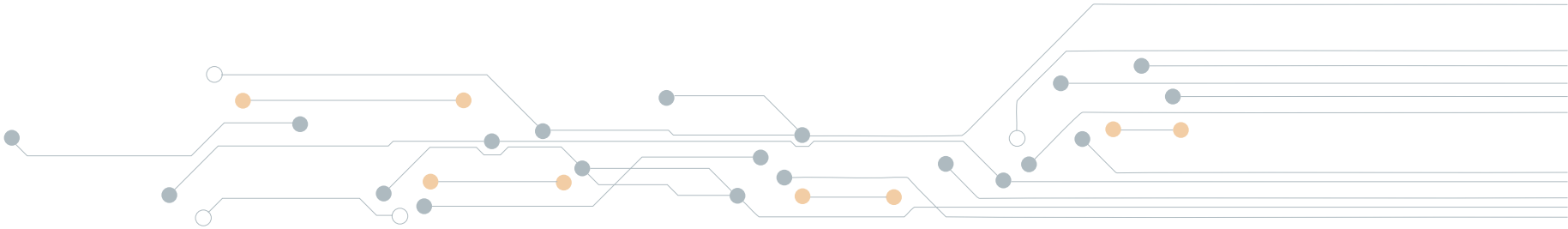
Primero se debe hacer el MiTM a la máquina Windows, desde la máquina Linux, por ejemplo como se ha enseñado anteriormente. Una vez el tráfico esté circulando a través de la máquina Linux, se debe construir un fichero hosts (con un editor de textos). Este fichero se debe utilizar por la herramienta dnsspoof. En este fichero se especificará las direcciones IP acordes a los nombres de dominio que se quieren spoofear. El siguiente fragmento simula el fichero de texto editado:

- <dirección IP máquina Linux> *.<dominio.com>
- <dirección IP máquina Linux> <dominio.com>

Por ejemplo:

192.168.56.102 *.facebook.com

Siendo esa la dirección IP de la máquina Linux y lo otro el dominio a spoofear.

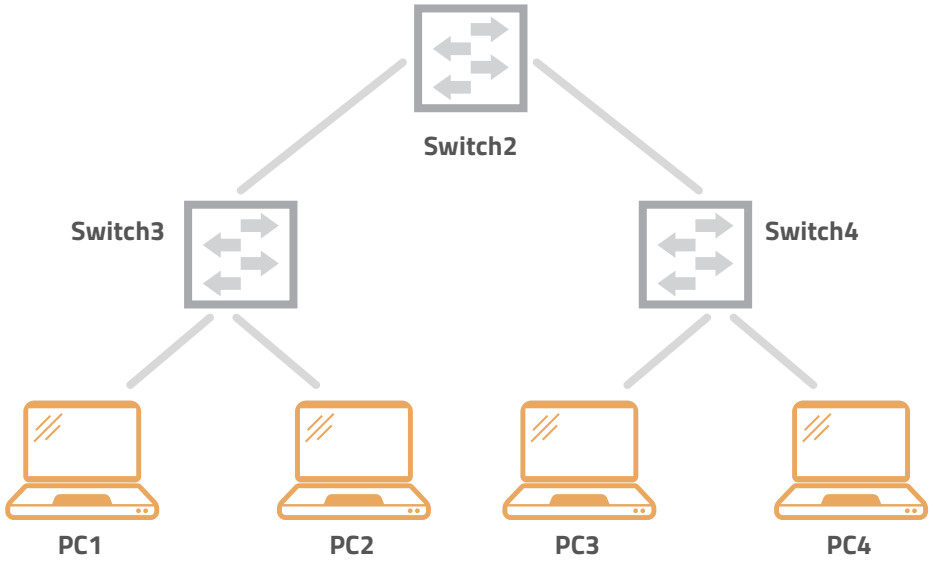


```
root@kali:~# dnsspoof -i eth0 -f hosts.txt
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.57]
192.168.0.56.1055 > 8.8.8.8.53:  681+ A? estaticosak1.tuenti.com
192.168.0.56.1055 > 8.8.8.8.53:  681+ A? estaticosak1.tuenti.com
192.168.0.56.1055 > 8.8.8.8.53:  1272+ A? www.tuenti.com
192.168.0.56.1055 > 8.8.8.8.53:  1272+ A? www.tuenti.com
```

Desde la máquina Windows se podría hacer un ipconfig /displaydns (desde un cmd.exe) y se vería que se está resolviendo el dominio a una dirección IP de la máquina Linux realmente. Desde el navegador no se aprecia, y puede provocar la aparición de un ataque de phishing.

5 | VLAN

En esta práctica estudiaremos el concepto de VLAN, estudiando el siguiente escenario:



El objetivo es crear 2 VLAN, aislando a los dos conjuntos de PCs.

Prueba 1

En la primera prueba aislaremos a PC1 y PC2 de PC3 y PC4. Como por defecto la VLAN1 está creada crearemos una segunda VLAN. Para ello configuraremos el switch 4 para que los puertos de PC3 y PC4 se conecten a VLAN 2. En el switch 3 no hay que realizar ninguna configuración.

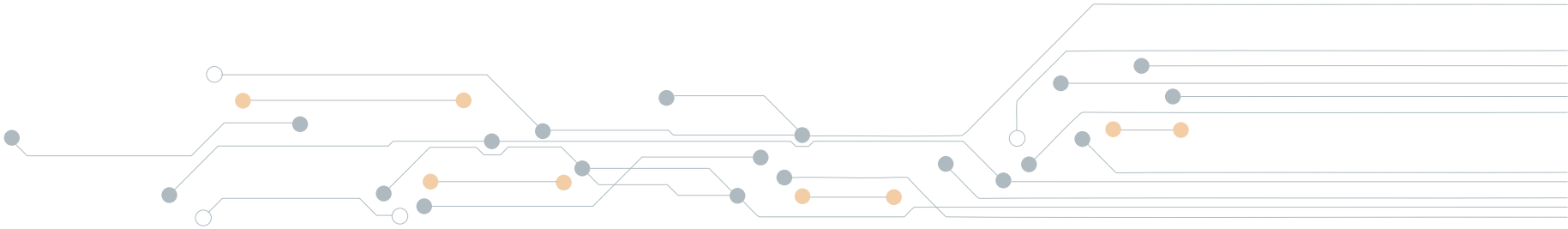
Comprueba que todo funciona como debe. ¿Qué forma tienes de comprobarlo?

5 | Solución

Para la prueba 1:

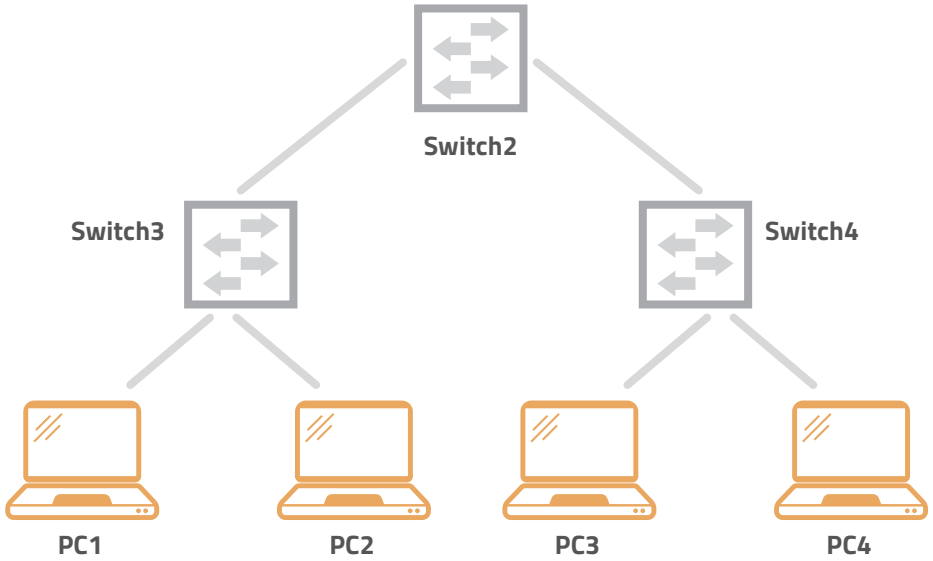
- Para crear una VLAN, acceder a la consola del switch:
  - Enable
  - Configure terminal
  - Vlan database
  - Vlan 2 name prueba
  - Exit
  - Interface <puerto en el que el PC3 está conectado>
  - Switchport Access vlan 2
  - Interface <puerto en el que el PC4 está conectado>
  - Switchport Access vlan 2

- Comprobar que PC3 y PC4 se ven, pero no se ven con PC1 y PC2



6 | VLAN II

En esta práctica estudiaremos el concepto de VLAN, estudiando el siguiente escenario:



En la segunda prueba deseamos que PC1 pueda verse con PC3, pero no con el resto. PC2 sólo podrá verse con PC4.

Ayuda

Config terminal

No shutdown

Interface fastethernet <número puerto>

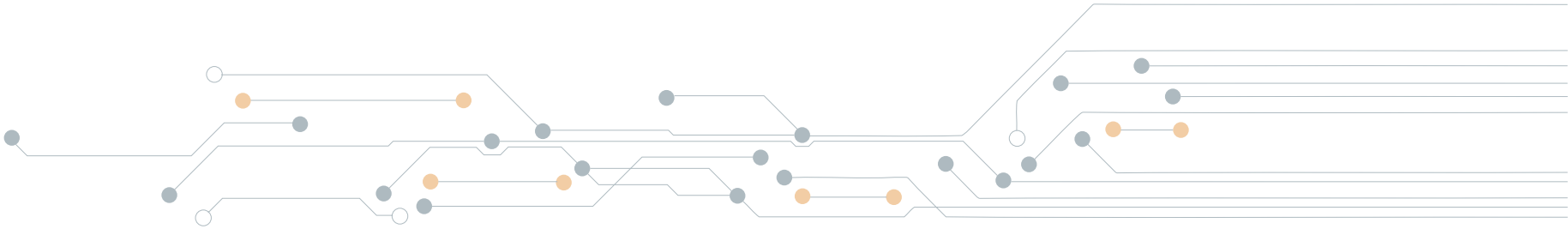
Ip address <ip><máscara red>

Vlan < número> #Para crear vlanes

Show

Show vlan

Switchport Access vlan <número vlan>



6 | Solución

Para la prueba 2:

Aquí simplemente hay que cambiar la VLAN de los puertos del switch a los que se conectan los PC. PC1 y PC3 en VLAN1, y PC2 y PC4 en VLAN2, por ejemplo. Además, hay que añadir entre el puerto que conecta el switch 1 y el switch 2 lo que se llama un puerto de trunk (es decir, que puede pasar tráfico de cualquier VLAN). También, hay que añadir entre el puerto del switch 2 y el 4 la misma configuración un puerto de trunk.

Switch(config)#interface <puerto en el que está conectado con el otro switch>

Switch(config-if)#switchport mode trunk

Telefónica EDUCACIÓN DIGITAL