

Redes de Computadores

Práctica 2

Nivel de Enlace

Descripción de la práctica

La práctica consiste en aplicar los conocimientos adquiridos en la asignatura con respecto al Nivel de Enlace en Redes de Área Local. En concreto se pretende que el alumno compruebe el funcionamiento del protocolo ARP, el funcionamiento de los dispositivos de interconexión de nivel 2, y cómo segmentar una red mediante VLANs.

La práctica se realizará en un entorno simulado en el que el alumno creará los escenarios solicitados, configurando los equipos y comprobando su funcionamiento.

En esta práctica se utilizarán *switches*, dispositivos de interconexión de nivel 2. Además se utilizará la funcionalidad de simulación de la herramienta Packet Tracer, muy útil para comprobar cómo trabajan los diferentes elementos de la red.

La configuración de los *switches* se realizará utilizando la interfaz de línea de comandos (CLI) del IOS de Cisco, puesto que los switches son equipamiento real Cisco simulado. Al final de este enunciado se encuentra una descripción de los mandatos IOS necesarios para realizar la práctica, incluyendo nuevas funcionalidades aplicables a esta segunda práctica. Encontrará más información en la [guía de uso](#) y en la [hoja de referencia rápida](#).

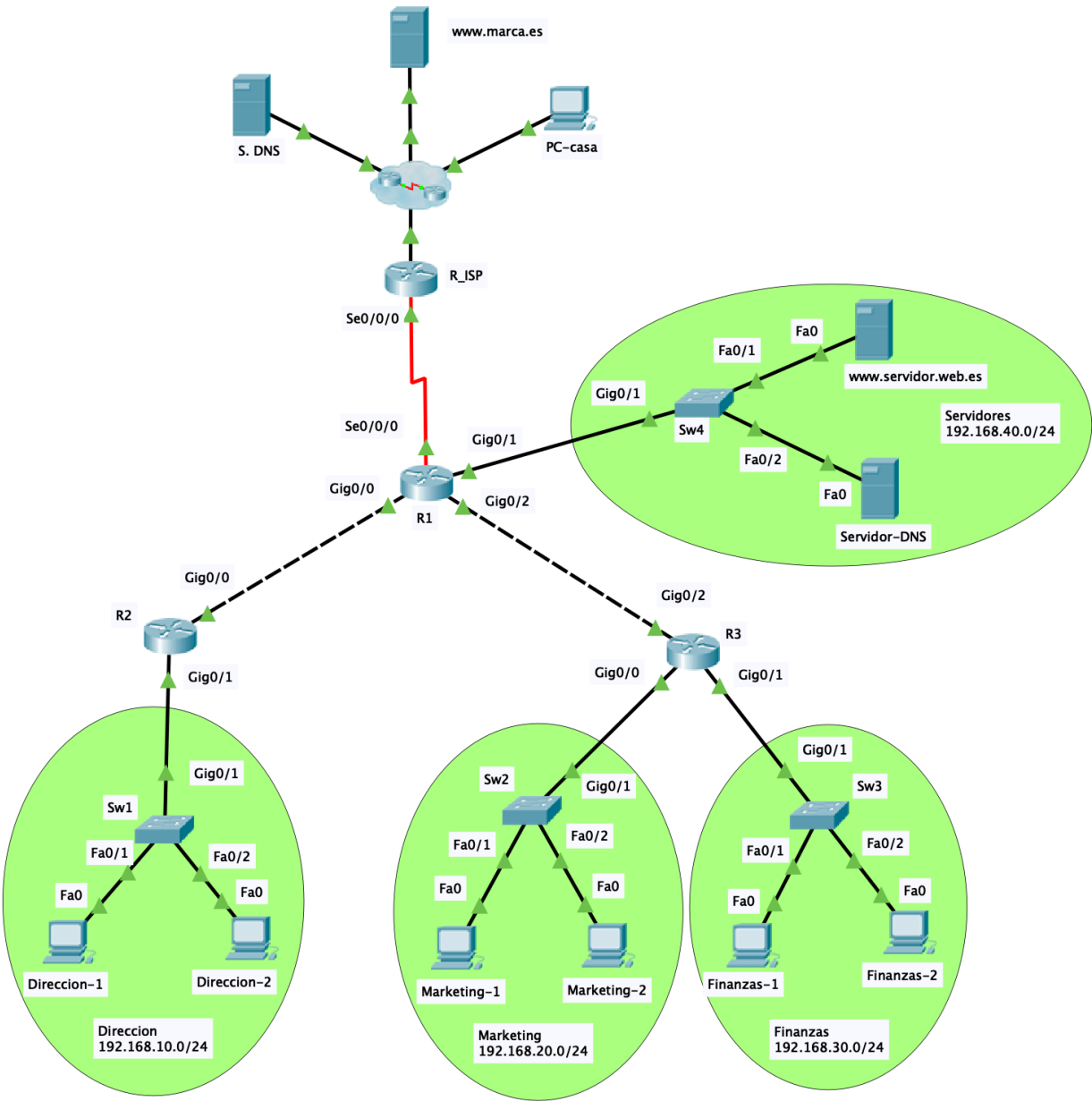
Normas

La práctica se realiza en grupos de dos personas.

Antes de asistir a la primera sesión de laboratorio, los alumnos deberán haber leído y comprendido este enunciado.

Escenario

Una organización dispone de 4 redes internas.



A continuación se muestra el esquema de direccionamiento de las subredes internas de la organización. Los equipos finales y los routers se encuentran configurados para poder interconectarse entre ellos.

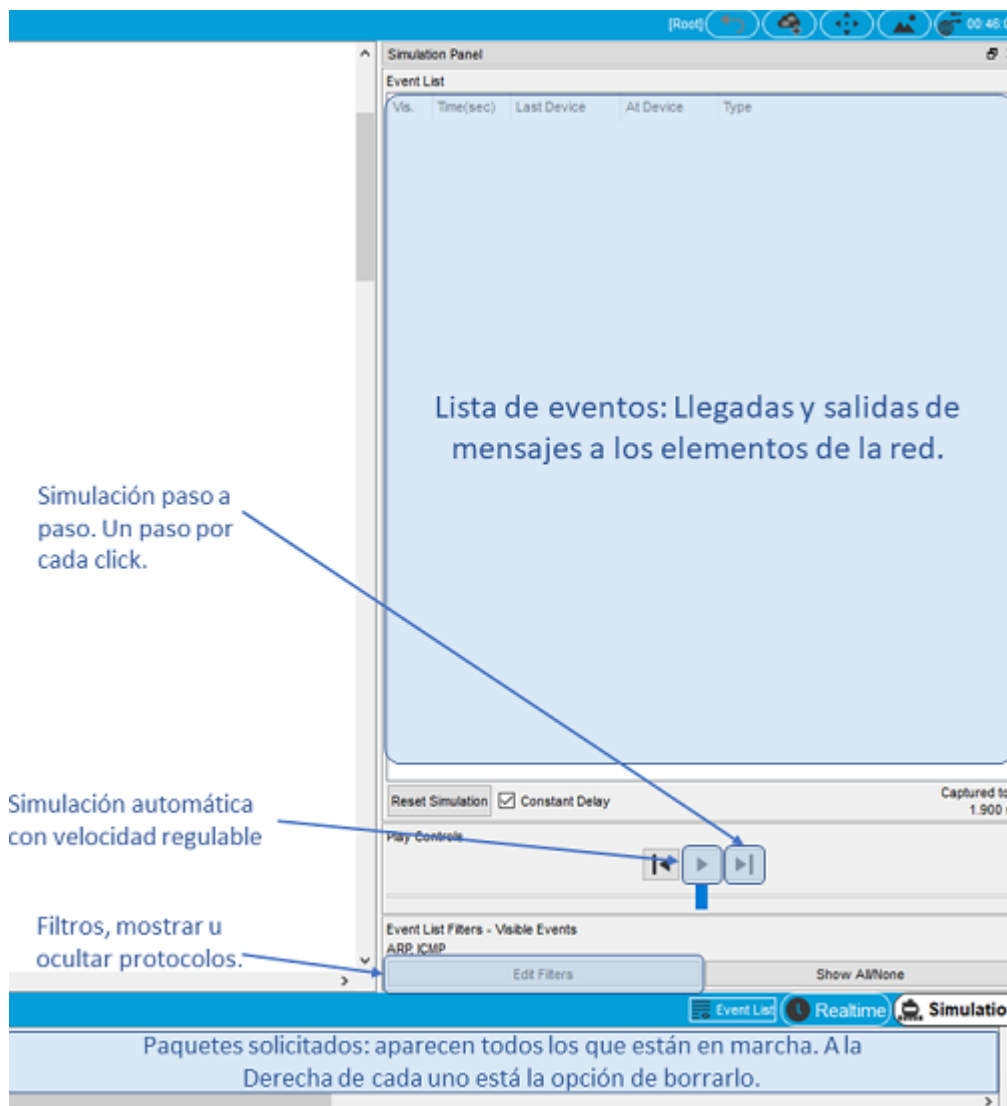
Red	Direcciones
Dirección	192.168.10.0/24
Marketing	192.168.20.0/24
Finanzas	192.168.30.0/24
Servidores	192.168.40.0/24

1. Direcciones IP y direcciones MAC

En este primer escenario se va a analizar el direccionamiento físico (nivel de enlace) y lógico (nivel de red) que se utilizan en las unidades de datos. Se comenzará analizando el funcionamiento del protocolo ARP, que permite traducir direcciones IP en direcciones MAC, observando cómo se propagan las solicitudes ARP y cómo es la respuesta de la máquina correcta. También se comprobará cómo las

direcciones IP de origen y destino identifican a los extremos de la conexión, mientras que las direcciones MAC utilizadas en las tramas de nivel de enlace identifican a los extremos del enlace por el que transitan.

En este escenario se utilizará el modo de simulación de la herramienta Packet Tracer. El modo de simulación permite observar el tránsito de las unidades de datos paso a paso, mostrando los valores de las diferentes cabeceras y la propagación o descarte de las unidades de datos por los elementos de la red. Al iniciar el modo de simulación nos aparece una nueva ventana en la parte derecha de la pantalla que nos permite controlar la simulación:





Antes de arrancar el modo simulación, compruébese que todas las luces están en verde (i.e. no hay ninguna en naranja). Si alguna no está en verde se deberá esperar a que cambie o avanzar el tiempo rápido con el botón **Fast Forward Time (Ctrl+D)**. Una vez arrancado el modo de simulación, se deberán filtrar los protocolos a mostrar. Puesto que se van a analizar mensajes ARP generado mediante peticiones de *ping*, se deberán seleccionar los protocolos ARP e ICMP.

NOTA: Tan sólo los mensajes de los protocolos activados en el modo de simulación serán vistos, aunque los demás seguirán funcionando. Si el alumno genera tráfico pero no llega a ver mensajes, es muy probable que no se esté visualizando el protocolo adecuado.

A continuación se deberá generar tráfico en el sistema, lo cual se puede hacer a través de las interfaces de cada uno de los dispositivos, o a través de las opciones de generar PDU simple o generar PDU compleja del simulador. Para el desarrollo de la práctica **se recomienda generar tráfico tal y como se**

haría con un equipo real. Esto es, utilizar la consola de comandos para mandar pings, o el navegador de los equipos (del simulador) para hacer peticiones HTTP y DNS.

Aunque es preferible que el alumno genere tráfico como si estuviera en un equipo, existe una forma sencilla de generar tráfico mediante el botón de Generar PDU Simple, , que provoca el envío de una solicitud ICMP de echo (*ping*) entre las dos máquinas siguientes en las que se haga click. Una vez hecho esto, aparecerá una nueva entrada en la lista de eventos. En este caso no se selecciona IP de los equipos y, cuando un equipo tiene varias, como un router, el sistema elige una de ellas. Es por esto que se recomienda utilizar la consola de comandos para enviar pings.

Para comprobar la traducción de direcciones IP en direcciones físicas, se va a enviar un *ping* entre dos máquinas que se encuentren en la **misma red**. Vacíe la tabla ARP (siguiente párrafo) y envíe el *ping* al otro elemento, ya sea desde ese *Command Prompt* o a través del botón , todo esto teniendo la simulación activada, para luego ir dándole al botón *capture/forward* e ir avanzando paso a paso. Asegúrese de que tiene una sola petición en la lista de eventos, y de resetear la simulación para poder visualizar más cómodamente los resultados.

Para purgar la tabla ARP los equipos Windows disponen del mandato `arp -d`. Sin embargo, **NO** se recomienda hacerlo de esta forma, puesto que tras ejecutarlo el equipo comunica a todos los demás su dirección IP y MAC a través de un *gratuitous ARP*, que es una solicitud ARP sobre su propia IP, llevando su MAC. Estos mensajes, si bien no tienen efecto, son incómodos en la simulación, y deberían eliminarse antes de generar nuestro propio tráfico. La forma recomendada para borrar la tabla ARP de un PC es **reiniciándolo**. Para ello, se deberá entrar en la pestaña *Physical*, y hacer click en el botón de apagado, y hacer click otra vez para encenderlo.

NOTA: el **reinicio de cualquier equipo se debe hacer en el modo tiempo real**, ya que si se hace en el modo simulación los enlaces entre dispositivos no estarán nunca activos (se quedan en color naranja y nunca llegan a ponerse verde) debido a que el tiempo no avanza.

En la simulación paso a paso, tendrá que hacer click sobre el botón *Capture/Forward*. Con cada pulsación, se avanza un solo paso en la simulación, lo cual se visualiza con mensajes en forma de sobres recorriendo la topología, y con eventos de esos mensajes mostrándose en la lista de eventos. En la lista de eventos, columna *type*, se indica el tipo del evento y el color con el que se representa el sobre correspondiente.

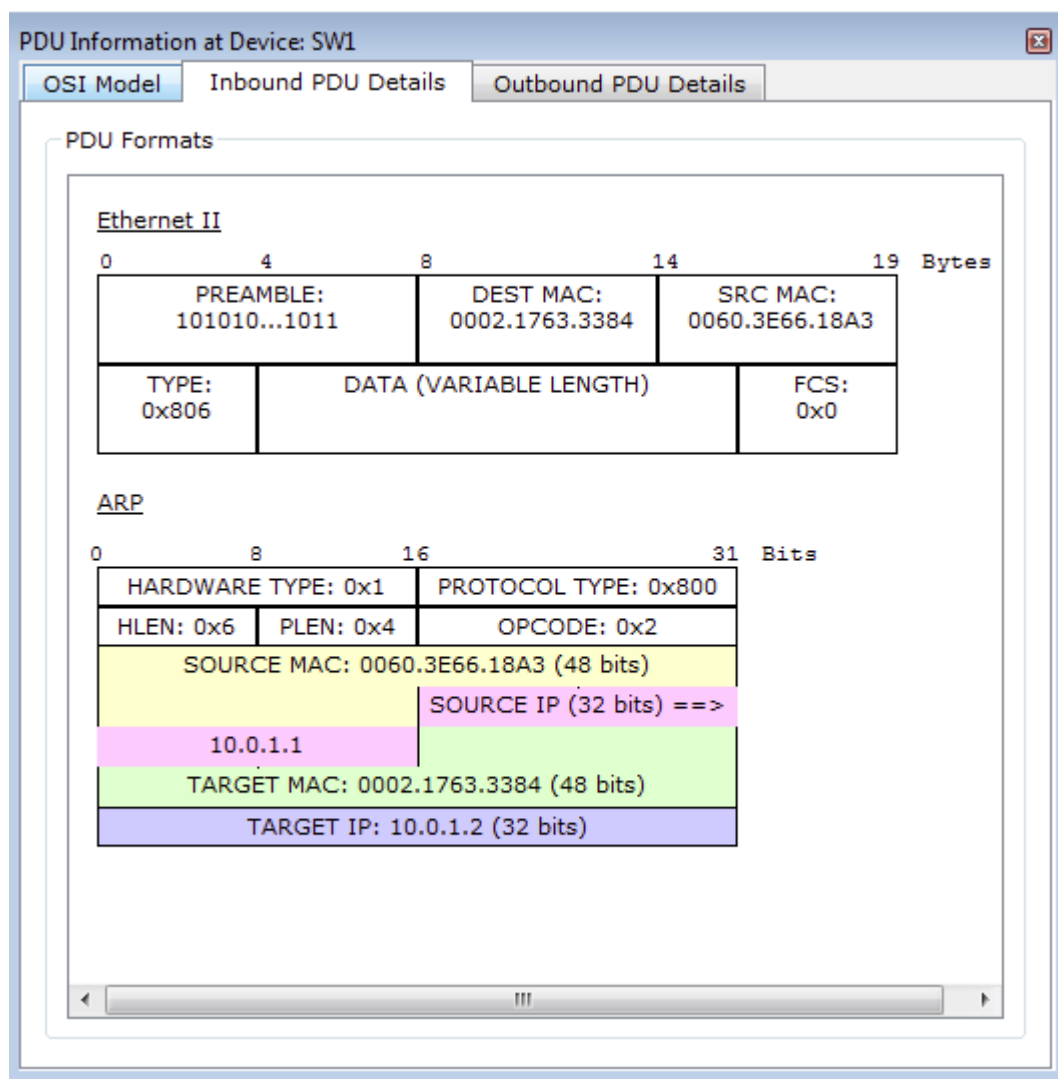
1.1



Partiendo de un equipo con la tabla ARP vacía (recién arrancado), averigüe de qué tipo es el primer mensaje que se envía al hacer un ping a otro. Por ejemplo, haga un ping entre `Marketing-1` y `Marketing-2`. ¿Qué hace el switch con dicho mensaje? ¿Quién responde a dicho mensaje? ¿Qué hacen los demás receptores de ese mensaje cuando les llega?

NOTA: Si purgara la tabla ARP con el mandato `arp -d` (no recomendado), éste envía mensajes *gratuitous ARP*, realizando peticiones ARP que preguntan por su propia MAC. Para evitar que esto nos afecte en la simulación podemos reiniciar la simulación, borrar las tablas ARP, avanzar la simulación hasta que terminen de reenviarse dichos mensajes y entonces, generar el tráfico que queremos comprobar.

Haciendo click en un sobre en la topología se puede obtener información detallada del mismo, apareciendo una ventana como la que se ve a continuación:



En dicha ventana de detalles se puede ver un mensaje a la entrada, y el mismo mensaje a la salida del dispositivo, detallando la estructura y los valores que toma en los diferentes niveles.

1.2

Repita la operación anterior para observar una **petición ARP** y una **respuesta ARP** y trate de responder a las siguientes preguntas:



- Respecto a la cabecera de la trama Ethernet II de la petición ARP ¿A qué dirección va dirigida una petición? ¿Qué máquina la envía? ¿Son las mismas direcciones antes y después de pasar por el switch?
- Compare la petición con la respuesta ARP. Analice qué parámetros cambian entre la petición y la respuesta.
- Muestre la tabla arp (`arp -a`) de la máquina que hizo la solicitud, ¿qué entrada ha aparecido?

Sin borrar ninguna caché ARP, resetee la simulación, borre el mensaje de la lista de mensajes y vuelva a realizar un *ping* entre ambas máquinas. Comprobará cómo ya no se envía el mensaje ARP previo.

1.3

Vamos a comprobar cómo aprende la máquina que **recibe** la petición ARP. Partiremos de una subred en la que ambos equipos (ej: `Marketing-1` y `Marketing-2` tienen sus tablas arp vacías, recién arrancados). Muestre la tabla vacía de `Marketing-2` y, a continuación, realice en modo simulación una petición ICMP de echo (*ping*) desde `Marketing-1` a `Marketing-2`. En el momento en el que `Marketing-2` ha recibido la solicitud acceda a su tabla ARP:



- ¿Qué entrada ha aprendido `Marketing-2`? ¿a qué equipo corresponden esas direcciones?
- ¿De dónde obtiene dichos datos? Muestre el contenido de la **solicitud ARP** y encuentre el/los campos que utiliza `Marketing-2` para obtener dicha información.

1.4

A continuación se va a realizar una petición de *ping* entre dos equipos que se encuentran en **redes diferentes**, separados por un *router*. Debido a que borrar la tabla ARP de un router provoca un aluvión de peticiones ARP, **reinicielo** con `reload` ó cierre y abra nuevamente el fichero `.pkt` tras guardar. Recuerde que el reinicio de equipos siempre se debe ejecutar en modo tiempo real, ya que como el tiempo no avanza en modo simulación, el router nunca termina de arrancar.

Realice el ping entre las dos máquinas que se encuentran en diferente red separadas por un router (Marketing y Finanzas son las únicas de la topología que sirven para este propósito, por ejemplo, haga un ping entre `Marketing-1` y `Finanzas-1`), y observe la petición y la respuesta ARP, como en el apartado anterior:



- ¿Cuál es la dirección IP por la que se consulta? ¿El equipo destino u otro? Trate de razonar los motivos por los que sucede esto.
- Visualice la tabla ARP de los equipos (`arp -a`) y del router (`show arp`). ¿Qué traducción IP/MAC aprende el equipo origen? ¿Qué traducción IP/MAC aprende el equipo destino? ¿Qué traducción(es) IP/MAC aprende el router?
- ¿Llega a conocer en algún momento, el equipo origen, cual es la MAC del equipo destino? Trate de razonar los motivos por los que sucede esto.

1.5

Vuelva a enviar otro mensaje y captúrelo **a su paso por el router**. Observe las diferencias entre los datos mostrados en el mensaje al entrar en el router (*Inbound PDU Details*) y cómo saldrá del router (*Outbound PDU Details*).

NOTA: una petición ARP **no** pasa por un router, por lo tanto no es útil para este propósito. Observe un paquete IP que transporte una petición ICMP o cualquier otra comunicación de nivel de aplicación.



- Detalle las diferencias encontradas entre las direcciones del nivel de enlace y las direcciones del nivel de red utilizadas. ¿Cuales cambian a su paso por el router? ¿Cual es el motivo?
- Observe un mensaje **al pasar por un switch** y repita la operación ¿Qué direcciones cambian a su paso por un switch? ¿Cual es el motivo?

1.6

En modo simulación, habilitando los protocolos DNS y HTTP, realice una petición HTTP desde el navegador web de un equipo de la red de finanzas hacia `www.servidor.web.es`. Avance la simulación hasta que se resuelva la petición ARP y observe, **al pasar por el primer router**, la petición DNS ó HTTP (la segunda vez ya no debería ver la petición DNS porque el navegador habrá guardado la traducción en su caché, no obstante, algunas versiones del simulador no simulan esto correctamente y por cada petición se realiza una petición DNS).



- ¿Qué direcciones IP origen y destino lleva la petición? ¿A qué equipos corresponden? ¿Cambian al pasar por el router?
- ¿Qué direcciones MAC origen y destino lleva la petición? ¿A qué equipos corresponden? ¿Cambian al pasar por el router?

Además, observe en cualquier parte del recorrido tanto la petición **DNS** como la respuesta HTTP (puede hacer la petición desde un equipo que no conozca aún la traducción `www.servidor.web.es - 192.168.40.2`). Observe los detalles de todos los protocolos en ambos casos y responda a la siguientes preguntas:



- Para un mensaje **DNS**
 - ¿Qué protocolo es encapsulado en la trama de enlace? ¿En qué campo se identifica?
 - ¿Qué protocolo es encapsulado en el paquete del nivel de red? ¿En qué campo se identifica?
- Para un mensaje **HTTP**
 - ¿Qué protocolo es encapsulado en la trama de enlace? ¿En qué campo se identifica?
 - ¿Qué protocolo es encapsulado en el paquete del nivel de red? ¿En qué campo se identifica?

2. Funcionamiento de un switch

Los switches reenvían las tramas que reciben en función de la dirección MAC destino de las mismas. Para ello, construyen una tabla de direcciones MAC que les permite saber sobre qué puerto deben reenviar una trama. El aprendizaje es automático, y se realiza observando las tramas que van conmutando. Si el switch desconoce dónde se encuentra la máquina destino, reenvía la trama por todos los puertos salvo por el que la recibió.

Para comprobar dicho comportamiento vamos a crear un escenario favorable. Dado que cualquier envío (por ejemplo, un *ping*) nos puede provocar un envío previo de ARP que se difunde por todos los puertos, vamos a realizar un *ping* entre dos máquinas, por ejemplo los servidores, y a continuación vamos a borrar la tabla de direcciones MAC del switch implicado con:

```
Switch# clear mac-address-table
```


A partir de este momento, vamos a enviar un *ping* paso a paso. El equipo origen ya conoce la dirección MAC del equipo destino, evitando que se envíe un mensaje ARP previo. Deténgase cuando el switch haya recibido la petición de *ping*.



- Muestre la tabla de direcciones MAC del switch con `show mac-address-table`. ¿Qué dirección acaba de aprender el switch? ¿A qué equipo corresponde dicha dirección?
- Muestre la cabecera del mensaje recibido tal y como aparece en la pestaña *Inbound PDU Details* ¿Qué campo de la cabecera Ethernet II del mensaje recibido ha utilizado el switch para aprender?
- ¿Qué dirección destino tiene la trama que va a encaminar? ¿Sabe el switch dónde se encuentra dicha máquina? ¿Qué hará en switch si no lo sabe?

Avance en la simulación comprobando cómo el switch envía la petición por inundación. Avance hasta que el switch recibe la respuesta ICMP, mirando su tabla de conmutación antes y después de que la respuesta le llegue.



- ¿Cuál es la MAC destino de dicha trama? ¿Conoce el switch el puerto al que tiene conectada dicha máquina? ¿Qué hará el switch en este caso? Compruebe su afirmación.
- ¿Ha aprendido algo más el switch al procesar la respuesta?

3. VLANS

La organización se ha dado cuenta de lo rígido que resulta su esquema de direccionamiento, el cual le impide que la gente de marketing, finanzas o dirección puedan colocarse en cualquier lugar de la organización y tengan que estar confinados en cierto bloque o departamento. Aun así desea aislar las diferentes redes por seguridad. Para cumplir sus requisitos, la organización ha decidido eliminar los routers internos, (manteniendo sólo uno que le da salida a Internet) y construir una única red física formada por switches con soporte para VLANs.

La organización va a crear 4 VLANs diferentes, en las cuales utilizará el siguiente esquema de direccionamiento:

Nombre VLAN	Direcciones	Identificador de VLAN
Dirección	192.168.10.0/24	10
Marketing	192.168.20.0/24	20
Finanzas	192.168.30.0/24	30
Servidores	192.168.40.0/24	40

Esas direcciones son las que ya utilizan los equipos de la topología en el fichero `.pkt` descargado, por lo que los cambios a realizar se centran en la infraestructura de red.

Partiendo de la topología actual, se deberán eliminar los routers (excepto R1), y conectar los switches existentes utilizando cable cruzado (el que se muestra con color negro discontinuo). La topología resultante será la siguiente:


```
SW1(config-if)# switchport access vlan <VLAN-id>
```

- Si se desea asignar más de un puerto a la vez, se puede utilizar la sintaxis para asignar rangos (atentos a la palabra **range**):

```
SW1(config)# interface range Fa x/y-z
```

```
SW1(config-range-if)# switchport mode access
```

```
SW1(config-range-if)# switchport access vlan <VLAN-id>
```

3. Los puertos que interconectan *switches* han de configurarse como puertos etiquetados (también conocidos como troncales o *trunk*), en los que las tramas viajarán etiquetadas con la etiqueta correspondiente. En todos esos puertos es necesario realizar lo siguiente:

```
SW1(config)# interface Fa X/Y
```

```
SW1(config-if)# switchport mode trunk
```

- Tenga en cuenta que los enlaces troncales hay que definirlos como tal **en sus dos extremos**.

El puerto del switch Sw4 que interconecta con el router R1 también tendrá que declararse como *trunk*.

En este punto ya debería funcionar la interconexión entre las máquinas dentro de **la misma VLAN**, independientemente de su localización. Compruebe dicha conectividad entre máquinas que se encuentran conectadas al mismo *switch* de acceso. A continuación, instale una nueva máquina en una ubicación física diferente (por ejemplo, una máquina de Marketing junto a las máquinas de Finanzas (deberás conectarla en un puerto asignado a la VLAN de Marketing), y compruebe la conectividad con dicha máquina desde las demás de su VLAN.



- ¿Funcionará la comunicación entre equipos de diferente VLAN? Compruébelo
- Revise el parámetro **gateway** de la configuración de los PCs. ¿tiene alguien asignada esa dirección?

3.1

Una vez probada la conectividad, vamos a comprobar el funcionamiento de la separación de una red física en múltiples redes virtuales VLAN. Borre la tabla ARP de un equipo que actuará como emisor (**arp -d**), e ingrese en modo simulación. Active el filtrado de ARP y de ICMP, y envíe un ping entre dos máquinas de la misma VLAN (la máquina origen es aquella a la que hemos borrado la tabla ARP).



- Avanzando paso a paso en la simulación, ¿Qué equipos reciben la solicitud **broadcast** de ARP? ¿Llega a todos los *switches*? ¿Y a todos los equipos finales?
- ¿Llega dicha solicitud a equipos de diferente VLAN?

3.2

Finalmente se procederá a configurar el router **R1** para que encamine entre las diferentes redes virtuales. Para ello se va a utilizar la configuración *router on a stick*, que utiliza un único puerto de un router con tantas sub-interfaces virtuales como VLANs se deseen interconectar.

1. En la interfaz del router conectada a un switch (el puerto del *switch* al que se conecta ha de estar marcado como *trunk*), se crearán tantas subinterfaces como VLANs se deseen interconectar. Para crear una subinterfaz virtual y asociarle dirección IP y VLAN hay que hacer lo siguiente:

```
R1(config)# interface Gig x/y.z
```

```
R1(config-subif)# encapsulation dot1Q <VLAN-id>
```

```
R1(config-subif)# ip address <dir_IP> <máscara>
```

```
R1(config-subif)# ip nat inside
```

- La subinterfaz se crea añadiendo un número extra (**z**) tras un punto al final del identificador de la subinterfaz. Así, si queremos crear una subinterfaz de la interfaz Fa0/1, crearemos la subinterfaz **Fa0/1.3**. Ese identificador **no tiene por qué** coincidir con el identificador de VLAN, pero suele hacerse así por claridad.
 - El comando **ip nat inside** es necesario para que NAT siga funcionando, y los equipos de las VLANs tengan acceso a Internet.
 - Cada sub-interfaz recibe una dirección IP del rango que se utilice en dicha VLAN. Como las VLANs se comportan como redes separadas, cada una tendrá su propia dirección de red y máscara. El router crea entradas de conexión directa en la tabla de rutas para acceder a cada una de las VLANs.

> * Atendiendo a la configuración de los equipos de la red, y evitando

- Antes de configurar las IPs en las sub-interfaces se recomienda eliminar la dirección IP de las interfaces utilizadas hasta el momento, porque pueden colisionar con las que se asignarán, especialmente Gigabit0/2. Para ello, y tras entrar en el modo de configuración de una interfaz, se deberá introducir el mandato **no ip address**.
- Tras crear las sub-interfaces, es a la interfaz **física** a la que se le indica que permanezca activada (las sub-interfaces no requieren del comando **no shutdown**):

```
R1(config)# interface fa x/y
```

```
R1(config-if)# no shutdown
```

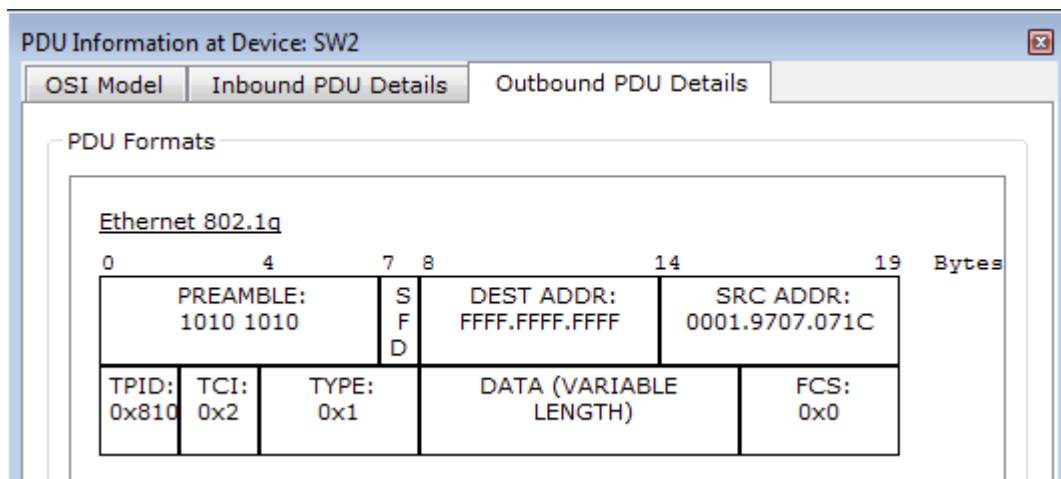
Compruebe ahora la conectividad entre máquinas de diferente VLAN.



- En modo simulación, realice un *ping* entre dos máquinas de diferente VLAN conectadas al **mismo switch de acceso**. Compruebe el camino seguido por los datagramas que contiene el mensaje ICMP.

3.3

Cuando una trama es enviada entre *switches*, se le añade una etiqueta 802.1Q, que se refleja en el modo simulación como un campo hexadecimal denominado **TCI**:



Observe la etiqueta que se añade en un ping de una máquina de Dirección hacia una máquina de Marketing

- ¿Qué dispositivo añade la etiqueta?
- ¿En algún momento cambia la etiqueta asignada a esa trama? ¿Quién la cambia y por qué?
- ¿Qué dispositivo elimina la etiqueta?
- ¿Los dispositivos finales (PCs) ven en algún momento las etiquetas?

3.4

Una persona del departamento de Finanzas, con un PC asignado es reasignado a otro departamento y pasa a formar parte de la plantilla de Marketing. Sin embargo no desea modificar su puesto de trabajo.



- ¿Qué cambios son necesarios en la configuración de su PC para que siga utilizando su ordenador pero se conecte a la red de Marketing? Apunte TODOS los cambios que se han de realizar
- Compruebe su afirmación realizando los cambios necesarios a un equipo de Finanzas que se ha de conectar a la red de Marketing.

3.5

Ahora que existe libertad para colocar los PCs de cada red, mueva los PCs por los diferentes switches de la organización (sin realizar cambios de configuración en los equipos). Conecte equipos de dirección en otros switches, por ejemplo.



- ¿Qué cambios deberá realizar en la infraestructura para que el equipo se conecte de forma correcta en su nueva ubicación, a su antigua VLAN?

3.6

Activando el modo simulación para visualizar los mensajes ICMP, realice una petición ping entre dos equipos de diferente VLAN conectados al mismo switch de acceso.



- ¿Qué camino cree que seguirá dicho paquete?
- Compruébelo con el modo simulación
- ¿Pueden los dispositivos de nivel 2 (switches) cambiar una trama de una VLAN a otra?

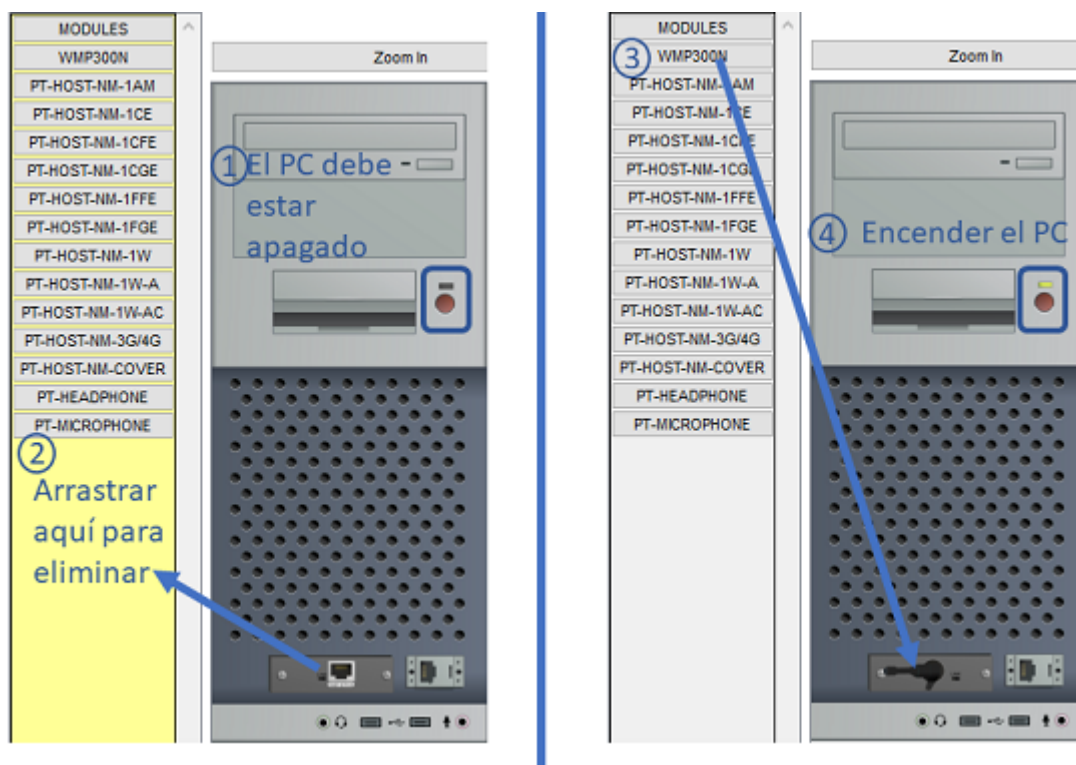
4. Ofrecer conexiones Wi-Fi en red aislada (Opcional)

La organización desea ofrecer conectividad Wi-Fi a sus empleados. Pero por motivos de seguridad desea mantener las comunicaciones Wi-Fi en una red diferente, interconectada a través del router, donde puede poner un *firewall* para filtrar las comunicaciones.

Diseñe e implemente una solución que le permita poner varios puntos de acceso en **diferentes localizaciones** de la organización, de forma que los dispositivos inalámbricos se interconectan entre ellos **en el mismo dominio de difusión**. Interconecte la red con las demás redes a través del router central.

Como puntos de acceso utilice los puntos de acceso genéricos denominados **AccessPoint-PT-N**, no hace falta configurarle contraseña, sólo el SSID deseado.

- Se recomienda no utilizar el mismo SSID en todos los puntos de acceso, puesto que un equipo inalámbrico tiende a conectarse a un punto de acceso que no tiene por qué ser el más cercano (de hecho suele ocurrir lo contrario).
- Como equipos para conectarse a ellos se deberán añadir PCs (sobremesa o portátil), y además, deberá instalarles una tarjeta inalámbrica. Para ello, en el modo de configuración **Physical**, apáguelo, arrastre su componente Ethernet hacia la lista de módulos disponibles para eliminar la tarjeta de red Ethernet, y arrastre en ese hueco el componente **Linksys-WPC300N**, que es una tarjeta inalámbrica.



- A continuación, en el equipo/s añadidos/s, iremos a **Desktop>PC Wireless** y buscaremos la red Wi-Fi con el SSID que hayamos creado.
- La configuración IP de los portátiles conectados deberá hacerse de forma manual.



- ¿Qué direcciones ha decidido utilizar para estos dispositivos?
- ¿Qué cambios habría que hacer en los dispositivos de red?

Abra de nuevo el modo de simulación, realice una petición entre un dispositivo inalámbrico y un dispositivo conectado a la misma VLAN (inalámbrico o Ethernet, como el router). Preste atención a las cabeceras de nivel 2 de la trama inalámbrica



- ¿A quién pertenecen dichas direcciones?
- ¿Cuales de ellas utiliza el Punto de Acceso para construir la trama Ethernet que envía al switch?

4.1 DHCP

La organización se ha dado cuenta que es bastante ineficiente que cada persona que se quiera conectar por Wi-Fi tenga que configurar de forma estática su dispositivo. Para solucionarlo se va a instalar un servidor DHCP para que los equipos obtengan su configuración de red de forma automática al conectarse por Wi-Fi.

Para ello seleccionamos en *End Devices* un servidor genérico. Debemos configurarlo de igual forma que configuramos cualquier equipo final, teniendo en cuenta que queremos que de servicio en el mismo dominio de difusión que los dispositivos wireless.



- ¿A qué switch debemos conectar el servidor?
- ¿Debemos configurar algo en el switch al que lo conectemos?

Para activar el servicio DHCP deberemos irnos a la pestaña *Services > DHCP* y activarlo (*on*). Añadiremos un nuevo pool de direcciones con el nombre que queramos. Los parámetros de configuración del pool serán los mismos que usabamos cuando configurabamos un equipo wireless de forma estática en el anterior apartado (i.e. default gateway, servidor DNS, dirección de inicio del rango y máscara). Adicionalmente deberemos indicar el número máximo de usuarios que queremos permitir en la red wireless.

Para comprobar que todo funciona correctamente, cambie la configuración de uno de los portátiles de estática a DHCP y espere hasta recibir la configuración u obtener un error.



- ¿Que parámetros de configuración recibe el equipo por DHCP?

Para examinar como funciona el protocolo DHCP usaremos el modo simulación. En este modo, cambie la configuración de otro portatil de estática a DHCP para generar una petición DHCP (filtre los protocolos para solo ver el protocolo DHCP).



El equipo inicialmente genera un mensaje de tipo DHCPDISCOVER:

- ¿Qué dirección IP destino tiene dicho mensaje? ¿A qué equipos llegará dicho mensaje?

Cuando el servidor DHCP recibe el mensaje avance la simulación hasta que el servidor genere un mensaje de respuesta de tipo DHCPOFFER. Compare el mensaje de entrada (DHCPDISCOVER) y de salida (DHCPOFFER) del servidor.

- ¿Qué información añade el servidor? ¿A qué se corresponde esta información?
- ¿Que dirección destino tiene dicho mensaje?

Cuando el equipo recibe el mensaje DHCP OFFER, genera un mensaje DHCP REQUEST el cual sirve para que el equipo comunique al servidor que acepta la configuración enviada previamente.

Avance la simulación hasta que el servidor DHCP genere un mensaje de tipo DHCP ACK confirmando la recepción del DHCP REQUEST del equipo y viendo como finalmente el equipo obtiene su configuración.

Anexos

Anexo 1. Guía de uso de la interfaz IOS de Cisco. VLAN

Mostrar la tabla ARP de un router

```
Router# show ip arp
```

Ver o eliminar la tabla de conmutación MAC en un switch

```
Switch# show mac-address-table  
Switch# clear mac-address-table
```

Creación y asignación de VLANs en un switch

Para crear VLANs en un switch utilizaremos

```
SW1(config)# vlan <VLAN-id>  
SW1(config-vlan)# name <Nombre>
```

La forma de asignar un puerto a una VLAN es:

```
SW1(config)# interface Fa x/y  
SW1(config-if)# switchport mode access  
SW1(config-if)# switchport access vlan <VLAN-id>
```


Si se desea asignar más de un puerto a la vez, se puede utilizar la sintaxis para asignar rangos (el guión en la primera orden va entre espacios):

```
SW1(config)# interface range Fa x/y - z
SW1(config-range-if)# switchport mode access
SW1(config-range-if)# switchport access vlan <VLAN-id>
```

Para configurar un puerto de un switch como *trunk*:

```
SW1(config)# interface Fa X/Y
SW1(config-if)# switchport mode trunk
```

Para mostrar el estado de los puertos asociados a VLANs y *trunk*:

```
SW1# show vlan [brief]
SW1# show interface trunk
```