REPASO REDES TEMA 5-7

INTRODUCCIÓN A LA CONFIGURACIÓN DE EQUIPOS

Opciones para laboratorio de pruebas:
- Hardware Real
- GNS3 → Emulador
- Cisco Packet Tracer → Simulador

Command Line Interface (CLI):
Una interfaz de línea de comandos es un mecanismo o una herramienta que permite enviar instrucciones en modo texto a un sistema operativo y visualizar los resultados.

Internetwork Operating System (IOS):
Sistema operativo de routers y switches CISCO.
[IMPORTANTE] Mantener los equipos de red actualizados.

Modos de acceso:
- **Consola:**
  - Se utiliza para configurar el equipo cuando lo compramos.
  - Necesitamos acceso físico al equipo para conectar un cable.
  - Tambien se usa en caso de no recordar la contraseña y querer cambiarla.
- **[Telnet || SSH]:**
  - Ambos se hacen mediante la red IP.
  - Si la red cae **perdemos la gestión.**
  - Es recomendable tener una opción de gestión *fuera de banda* (Out Of Bound (OBB)).

PUERTO Y CABLES DE CONSOLA

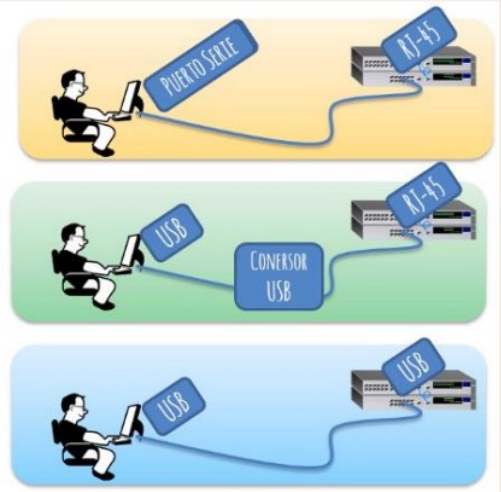
Puertos de un router CISCO
- Puerto de consola
  - Cable azul
- Puertos para SSH o Telnet
  - Cualquier interfaz del router directa o indirectamente conectada nos servirá.

Tipo de comunicación. Telnet y SSH vs Consola
- La comunicación por SSH o Telnet utiliza el protocolo IP.
- La comunicación por Consola NO utiliza el protocolo IP.

Gestión por cable de consola: Conexión
- RJ45
- microUSB

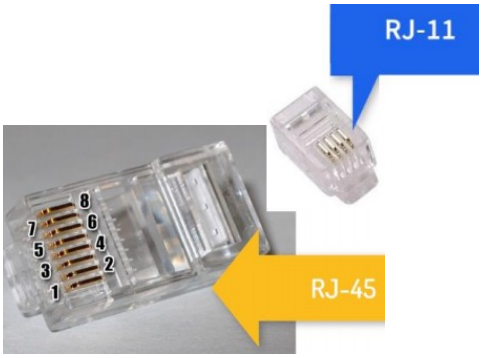
Gestión por cable de consola: Los tres escenarios posibles
- [Nuestro Equipo] – [Equipo de Red]

1. Puerto serie – RJ45
2. Puerto USB – Conversor USB – RJ45
3. Puerto USB – USB



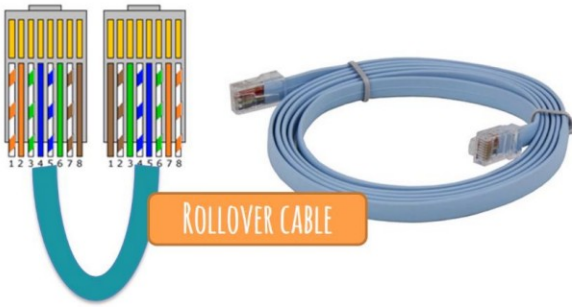
Breve inciso: RJ45

- Tiene 8 pines y 4 pares.
- Otros conectores como el RJ11 tienen menos pines.
- En las redes de datos, el RJ45 usa cables de **cobre.**
- Al tener 8 cables y 8 pines, veremos que hay diferentes tipos de cables en función de cómo conectamos los cables con los pines.



Gestión por cable de consola: El cable RollOver

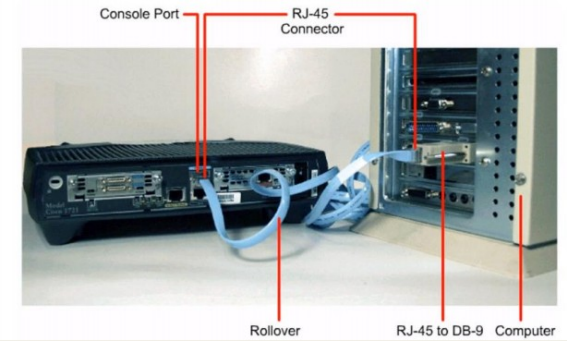
- El nombre viene por el pineado.
- Está totalmente girado el pineado entre un extremo y el otro.



Gestión por cable de consola: Adaptador para RollOver

- Cable RollOver + adaptador RJ45 a DB9
  [DB9 = RS232 = Tipo serie]

Ejemplo real de conexión por consola con Rollover

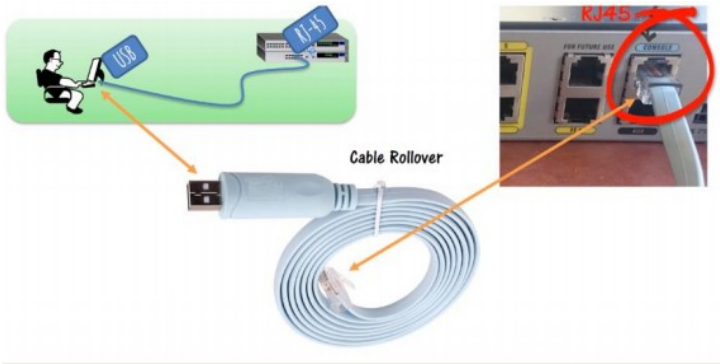


Gestión por cable de consola: RollOver + Adaptador en uno

- Se empezó a utilizar este tipo de cable para simplificar las conexiones.
- Tiene en un extremo un RJ45 y en el otro extremo tiene un DB9.

Gestión por cable de consola: RollOver + adaptador para portatiles actuales

- Cable RollOver + adaptador DB9 a USB



Gestión por cable de consola: RollOver más actualizado

- Cable Rollover (RJ45 a USB)

Gestión por cable de consola: Opción USB

- Cable RollOver (microUSB a USB)

EMULADORES DE TERMINAL

- **Hyperterminal**
- **Putty**
- **Otros (SecureCRT, etc)**

MODOS DE ACCESO SSH Y TELNET

Modo SSH
- Protocolo de capa de aplicación.
- Utiliza la red IP, puerto 22, TCP.
- Encripta la información.

Modo Telnet
- Protocolo de capa de aplicación.
- Utiliza la red IP, puerto 23, TCP.
- No encripta la información.

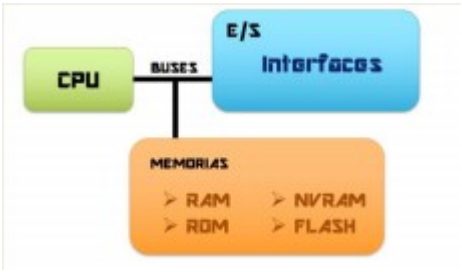
MODOS DE USUARIO DE LA CLI

Introducción a los modos de usuario	**(Prompt)**
• Exex usuario	>
• Exec privilegiado	#
• Configuración global	(config)#

Submodos de Configuración Global

• Interface	(config-**if**)#
• Line	(config-**line**)#
• Router	(config-**router**)#
• VLAN	(config-**vlan**)#
• etc	

TIPOS DE MEMORIA, SECUENCIA DE ARRANQUE Y FICHEROS DE CONFIGURACIÓN



Procesador
- El CPU es el cerebro de la maquina.
- Es quien ejecuta las instrucciones del SO.
- Inicializa el sistema.
- Realiza las funciones de enrutamiento.
- Controla las interfaces de red

Interfaces (entrada/salida)
- Puertos
  - Recibir datos
  - Enviar datos

Memorias
- RAM → Contiene la configuración activa del equipo (running configuration file)
- ROM → Contiene el **Bootstrap**, un programa que inicia el equipo, hace comprobaciones en el hardware y busca el SO en la memoria flash y la carga en la ram.
- NVRAM → Contiene el fichero de configuración de inicio del equipo (startup configuration file)
- FLASH → Permite lectura/escritura, contiene el SO.

Guardar la configuración activa en la configuración de inicio
write memory || copu running-config startup-config

Borrando la configuración

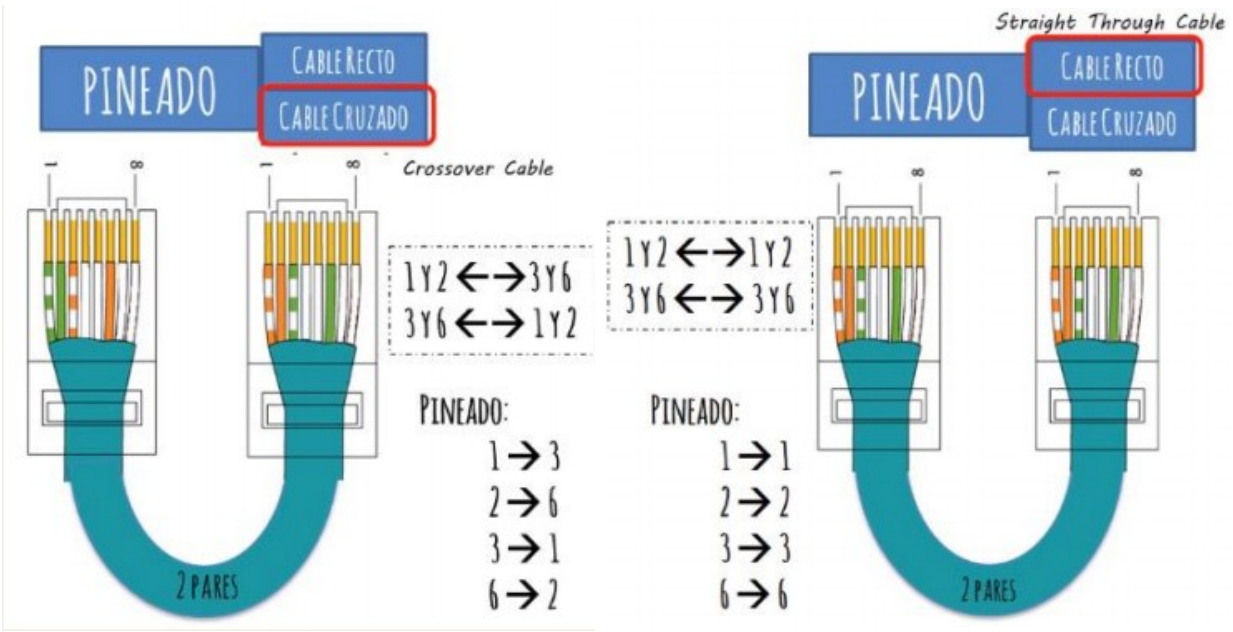
erase startup-config || write erase

PROFUNDIZANDO EN LAS REDES IP

Cableado UTP: Cruzado y Recto

MDI
Transmiten por los pines 1 y 2

MDI-X
Transmiten por los pines 3 y 6



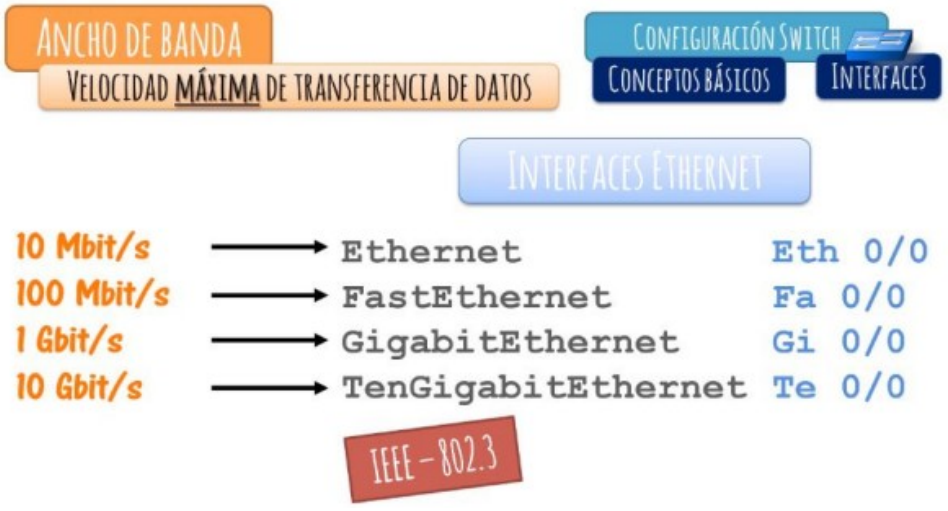
Switches y Hubs

Revisando las tablas de direcciones MAC de los switches

show mac-address-table

clear mac-address-table

Recapitulando conceptos – Ancho de banda (bandwidth)



Recapitulando conceptos – Latencia (delay)

Diferencia entre puerto e interfaz

- **Interfaz** → Representación Software del puerto físico.
- **Puerto** → Hace referencia a la entrada física del equipo.

Configurar DUPLEX y VELOCIDAD

- **AUTO**
- **HALF**
- **FULL**

```
Switch(config-if)#duplex ?
  auto  Enable AUTO duplex configuration
  full  Force full duplex operation
  half  Force half-duplex operation
```

- **AUTO**
- **10 Mbps**
- **100 Mbps**

```
Switch(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

AUTO en ambos casos significa que hará la negociación de forma automática.

Mostrar la configuración de las interfaces

- show interfaces status Muestra todas las interfaces
- show interfaces fastEthernet 0/1 status Muestra una interfaz
- show interfaces fastEthernet 0/1 Muestra toda la config. de una interfaz

PROTOCOLO ICMP Y PING

El protocolo ICMP

- **ICMP** = Internet Control Message Protocol
- Se encuentra dentro de los protocolos de red.
  - Es un protocolo de controlo y notificación de errores.
- Tiene dos funciones principales:
  - Diagnóstico
  - Notificación

Entendiendo mejor ICMP

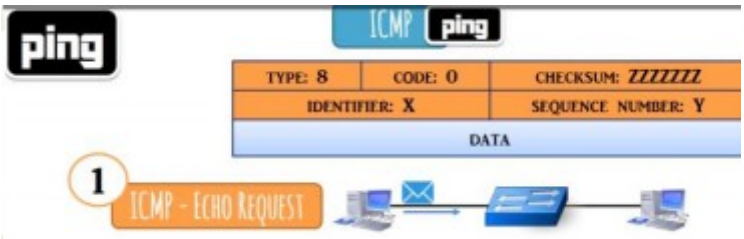
- Funciona sobre el protocolo IP
  - Irá encapsulado DENTRO del protocolo IP
  - La cabecera ICMP estará dentro de los DATOS, que a su vez tendrá una cabecera y unos datos(que son opcionales y podría no haberlos).

La capa de ICMP

Según dónde consultemos, puede que veamos que nos dicen que es un protocolo de la capa de red (considerado un subprotocolo de IP, como un hijo), y en otros sitios que es de la capa de transporte (porque va encapsulado en la capa de red). Aunque hay algo más de consenso en considerarlo de la capa de red.

Entendiendo las cabeceras de ICMP

- Ping utiliza el protocolo ICMP en dos casos diferentes:
  - ICMP – ECHO REQUEST
  - ICMP – ECHO REPLY



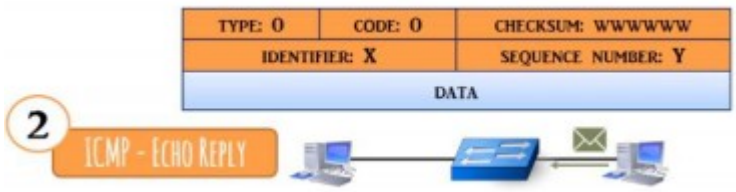
Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench (Deprecated)
5	Redirect
6	Alternate Host Address (Deprecated)
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded

Type 8 — Echo

Registration Procedure(s)
IESG Approval or Standards Action
Reference
[RFC792][RFC2780]
Available Formats
CSV

Codes	Description	Reference
0	No Code	

- El primer valor corresponde al **TYPE:** https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml
- El campo de **CODE**, a grandes rasgos, son subtipos de la cabecera TYPE.
- El **CHECKSUM** es una suma de comprobación para saber si se han alterado los datos.
- Los campos **IDENTIFIER** y **SEQUENCE NUMBER** los asigna el SO.



Type	Name
0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachab
4	Source Quench (Depre
5	Redirect

- **TYPE** y **CODE** 0.
- El **CHECKSUM** tendrá un valor diferente (comprobaciones de integridad).
- Los campos **IDENTIFIER** y **SEQUENCE NUMBER** se mantienen iguales.
- Los **DATA** tambien se mantendrán igual que en la REQUEST.

Mini inciso: STP

- Spanning Tree Protocol, es un protocolo que utilizan los switches para evitar bucles.

EL PROTOCOLO ARP
Protocolo que nos permite conocer la dirección MAC de un equipo a partir de la IP.

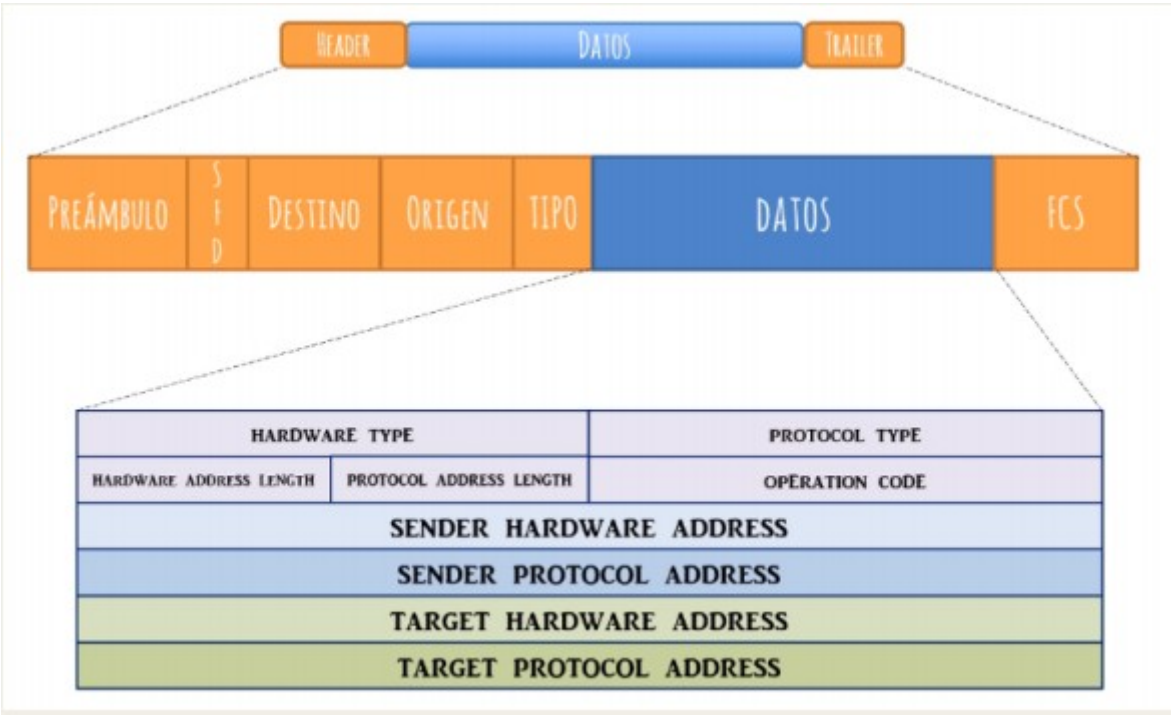
- Protocolo de capa 2
- ARP lanza una trama con MAC destinto: FFFF.FFFF.FFFF (broadcast)
- La trama contendrá una pregunta del tipo:
  - ¿Quien tiene la MAC de la IP 192.168.0.10?
- La respuesta del destino será tipo Unicast.
- Cuando la respuesta llega al PC origen, este aprenderá la MAC en la tabla ARP.

Analisis de cabeceras ARP

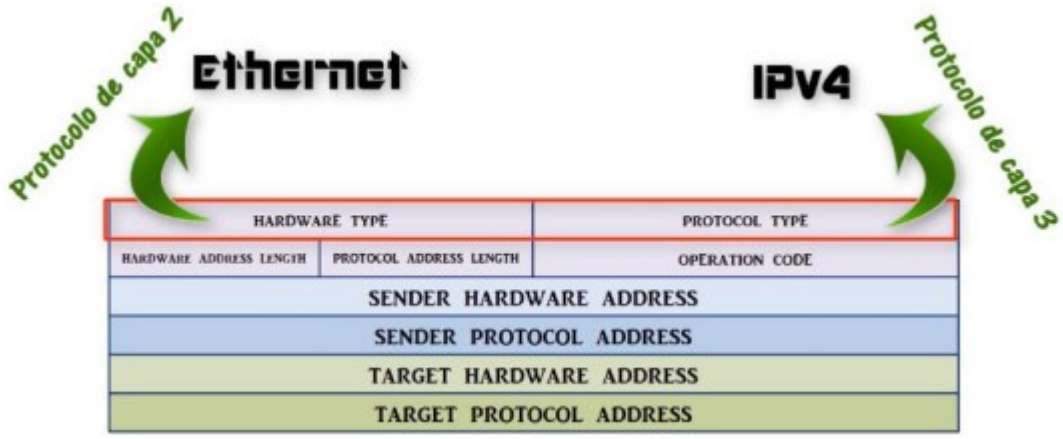
- En la petición ARP el origen será el PC que la envía y el destino será el Broadcast.
- En la respuesta ARP el origen será el equipo que lo envía y el destino el equipo que debe recibir la trama.

- En el campo Tipo, para una petición ARP veremos la identificación hexadecimal **0x0806**.

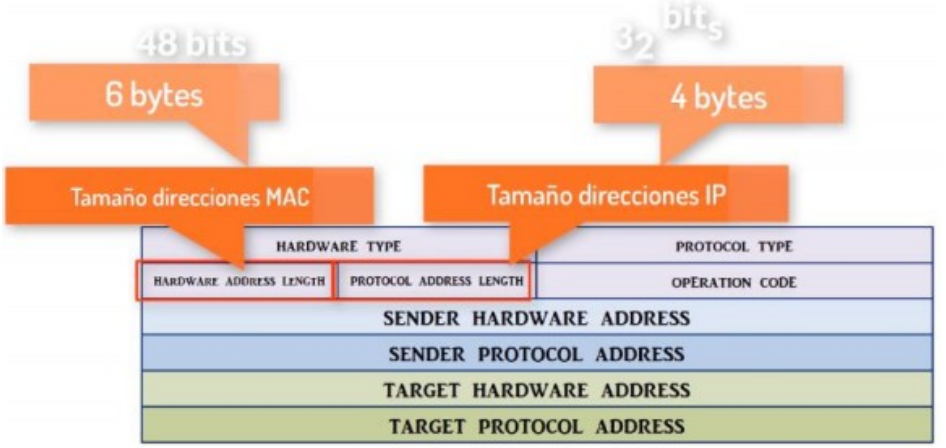
- La información contenida en el protocolo ARP irá en el campo de datos.



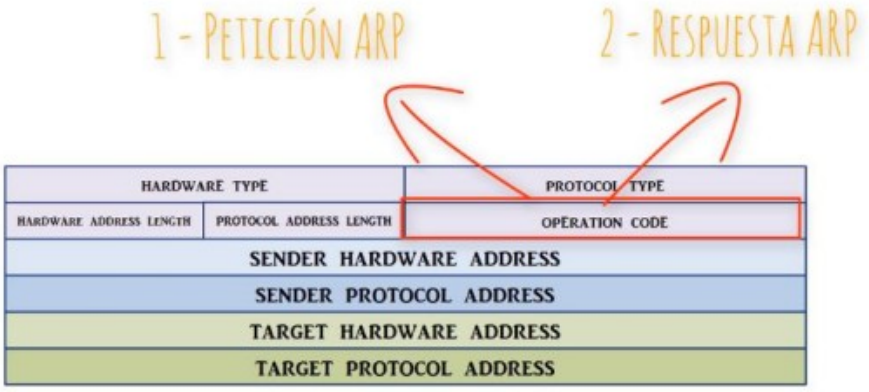
- El campo **HARDWARE TYPE** y **PROTOCOL TYPE** sirven para decir que tipo de direcciones se van a mapear.
- **HARDWARE TYPE** es donde irá el protocolo de capa 2.
- **PROTOCOL TYPE** irá el protocolo de capa 3.
- Estos campos contienen **códigos** (1 para hardware y 0x0800 para IPv4).



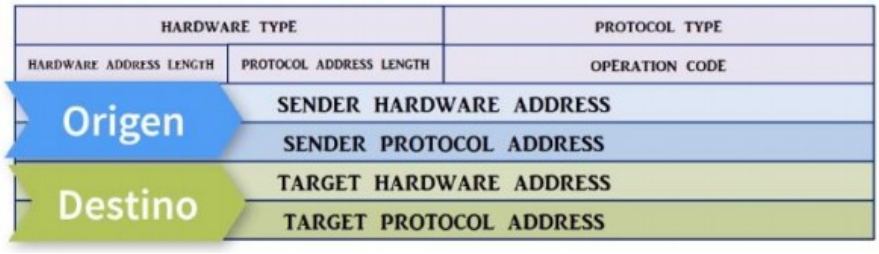
- Los siguientes campos hacen referencia al tamaño de las direcciones MAC e IP.
- Dirección MAC – 6 bytes
- Dirección IP – 4 bytes



- El campo **OPERATION CODE** solo puede tener dos valores:
  - Petición ARP – **1**
  - Respuesta ARP – **2**



- Por ultimo encontramos los campos más importantes:
  - MAC e IP de origen (SENDER)
  - MAC e IP de destino (TARGET)



Otros tipos de ARP

- **ARP tradicional** → El que hemos visto en clase y el más utilizado.
- **Reverse ARP (RARP)** → Para conocer la IP sabiendo solo la MAC.
- **Proxy ARP** → Para que un router responda las solicitudes ARP de otros hosts.
- **Gratuitous ARP** → Para conocer las MAC de todos los equipos de la red.
- **ARP Probe y ARP Announcement** → Se utilizan en procesos de detección de direcciones duplicadas.

INTRODUCCIÓN A WIRESHARK

¿Qué es Wireshark?

- Es un programa que se utiliza para capturar tráfico de red y posteriormente poder analizarlo.
- Es un programa gratuito y es software libre multiplataforma.

¿Cuál es su función?

- Podremos analizar la información a lo largo de sus capas.
- Resulta útil en el día a día de los técnicos de red cuando la red no esté funcionando como debería y queramos analizar qué está pasando con el tráfico.

Usos de Wireshark

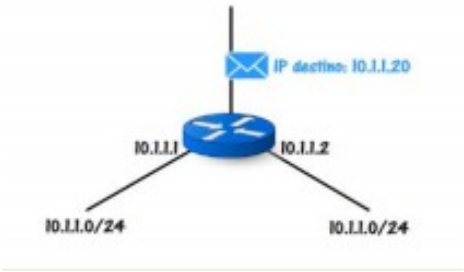
1. Analisis de tráfico para resolución de problemas. [TROUBLESHOOTING]
2. Testeo de las aplicaciones de red que hagan los desarrolladores.
3. Aprendizaje y entendimiento de las redes telemáticas.

¿Cómo lo usaremos?

- Nosotros lo usaremos para capturar el tráfico que entra y sale de nuestra interfaz de red.
- En un entorno de trabajo normalmente se trabaja con port mirroring, que consiste en conectarnos a un puerto de red del equipo que queramos analizar su funcionamiento, y configurarlo para que se reenvíe todo por este (además de a donde deba ir).
  - Port Mirroring = Puerto espejo

¿Por qué un router no puede tener la misma red en dos interfaces distintas?
– Porque pondríamos al router en una situación imposible de resolver.

- Imaginad el escenario de la derecha, donde tenemos a un router con dos interfaces con la misma red.
- En cada interfaz, el router tendría una IP diferente.
- ¿Pero qué pasaría si llega un paquete para la dirección 10.1.1.20? ¿Por dónde lo envía? El router no podrá determinar la interfaz por para reenviar.
- Un router nunca nos va a permitir configurar dos interfaces para la misma red. (nos dará error).



FRAME REWRITE – Reescritura de frame

¿Qué vamos a ver?

- En esta sección vamos a terminar nuestra imagen mental en cuanto al modo en el que se realiza una comunicación IP entre dos equipos.
- Nos falta en todos este proceso una pieza clave, que se llama FRAME REWRITE
- Hasta ahora, solo se ha producido frame rewrite en la última práctica, e indicamos que lo íbamos a explicar en esta.
- Vamos a entender cómo irá cambiando el paquete y la trama a lo largo de todo el trayecto de envío por la red, pasando de router a router hasta llegar al destino.

Resumen

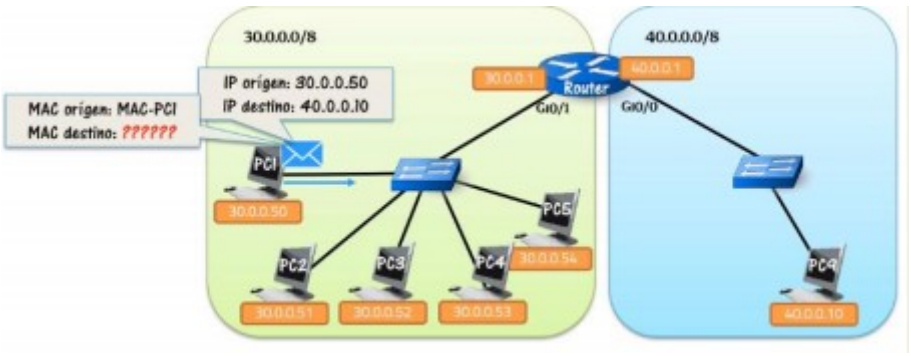
- Hemos visto que a nivel de capa 2 han ido cambiando las direcciones MAC de origen y destino.
- Pero a nivel de capa 3 se han mantenido iguales.
- Normalmente se dice que la capa 2 se encarga del hop-to-hop delivery, es decir, de la entrega salto a salto.
- Para el nivel 3 se dice que encarga de la end-to-end delivery, es decir, la entrega extremo a extremo.

Recordando qué pasaba en una misma red

- A nivel de capa 3:
  - Se crea el paquete a enviar, y en las direcciones se pondrán la IP de destino y la IP de origen.
    - Destino IP PC4
    - Origen IP PC1
- A nivel de capa 2:
  - Se encapsula la información en una trama, que en su cabecera tendrá también las direcciones MAC de origen (MAC PC1) y destino (MAC PC4).
- Cuando llegue la información, el PC4 verá que la dirección MAC de destino es la suya, así que aceptará la trama, la desencapsulará y pasará la información a la capa 3, que verá que la IP destino es la suya, y aceptará el paquete.

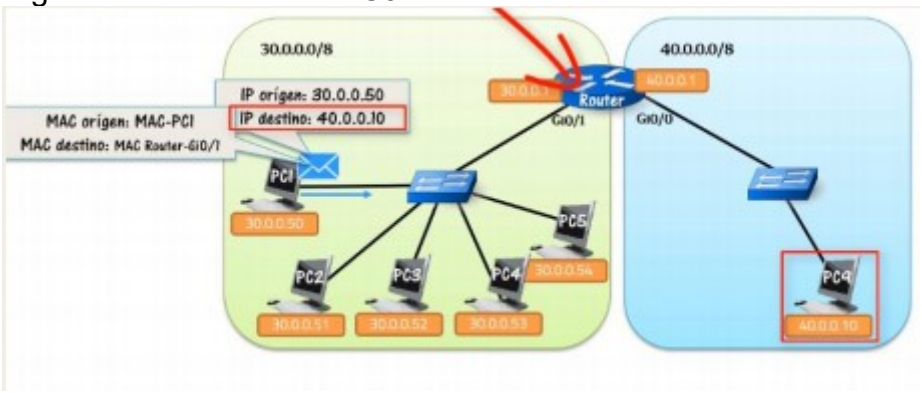
Envío en diferentes redes IP

- Si el PC1 quiere enviar algo al PC9…
- A nivel de capa 3 sigue igual que en el anterior ejemplo.
- Pero a nivel de capa 2, como MAC origen pondrá la MAC PC1, ¿pero qué pondrá como MAC destino?

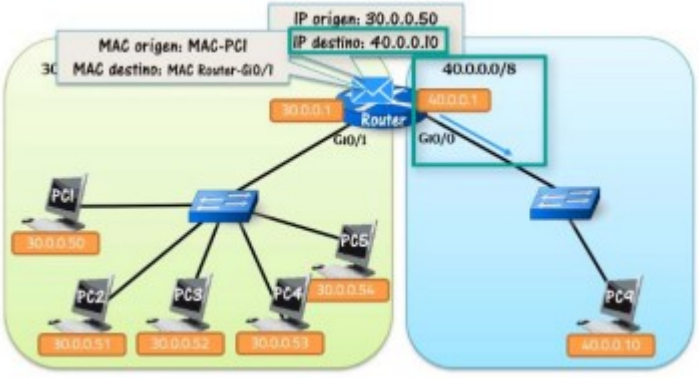


- No podrá poner la MAC del PC9, porque si hace esto, cuando se realice el envío por la misma red, la MAC no coincidirá con ningún equipo y todos la descartarán.
- Vamos a pensar en otra cosa. Si queremos llegar a la IP del PC9, en el paquete pondremos la IP del PC 9, ¿Verdad?
  - Pero si ponemos esa IP en la cabecera del paquete IP, ¿cómo se va a enviar al router para que lo lleve hasta allí?
  - Y si ponemos como IP destino en la cabecera la del router, ¿cómo vamos a llevarlo luego al PC9?
- ¿Aquí hay algo que se nos escapa

- Lo que pasará es que el PC1 pondrá como MAC destino la MAC del router (para la interfaz que se encuentra en esa red).
- La IP seguirá siendo la IP del PC9.



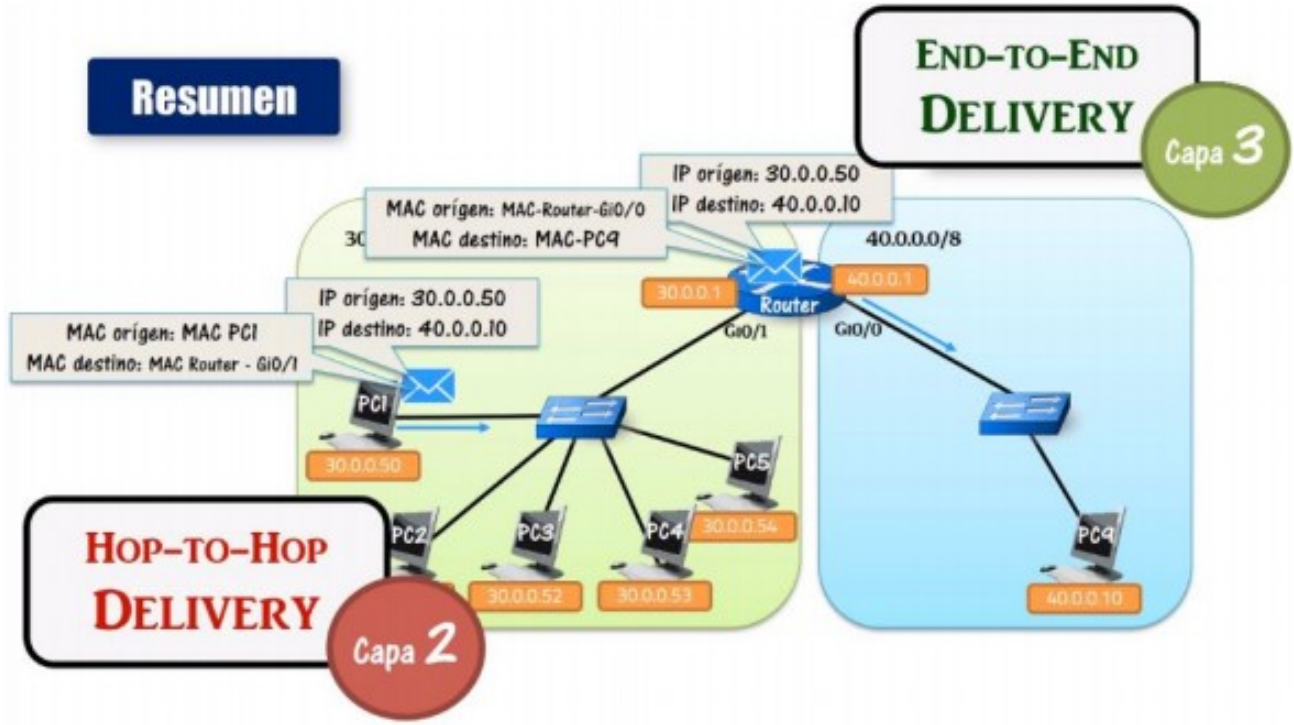
- El router desencapsulará la trama dado que iba dirigida a él.
- Y cuando llegue al nivel 3, comprobará que la IP destino no es la suya, y por tanto, tiene que hacer su función → El routing
  - Así que mirará su tabla de rutas para ver hacia dónde reenviar el paquete.
  - Lo hará por GI0/0



- Cuando el router vaya a reenviar el paquete por GI0/0 para que llegue a PC9…
- Las IP origen y destino se mantienen. ¿Pero qué aparecerá en los campos de direcciones MAC origen y destino?

- Como MAC destino pondrá la del PC9, porque ahora sí vamos a poder llegar hasta él.
- Como dirección MAC origen, va a ser la del router (en esa interfaz GI0/0)

RESUMEN



OTRO EJEMPLO