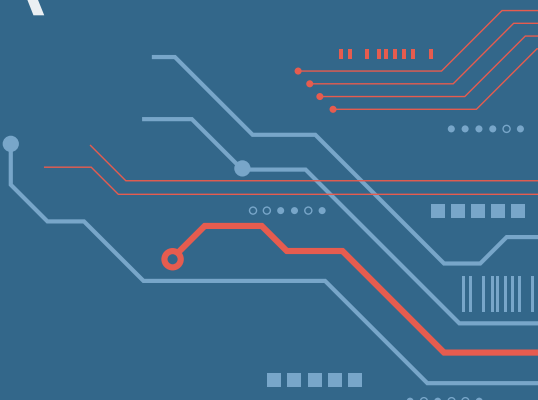


REDES DE DATOS TUIA | FCEIA UNR

Docentes | 1C 2023

Juan Pablo Michelino
Emiliano Pavicich
Andrea León Cavallo
Iván Pellejero
Esteban Toribio

jpmich@fceia.unr.edu.ar
pavicich@fceia.unr.edu.ar
aleoncavallo@gmail.com
ivan.pellejero97@gmail.com
toribio@fceia.unr.edu.ar



06



ETHERNET

6.1. Direcciones MAC.

6.2. Operatoria de un switch.
Tabla MAC. Métodos.

6.3. Dominios de difusión y de
colisión.

6.4. ARP.

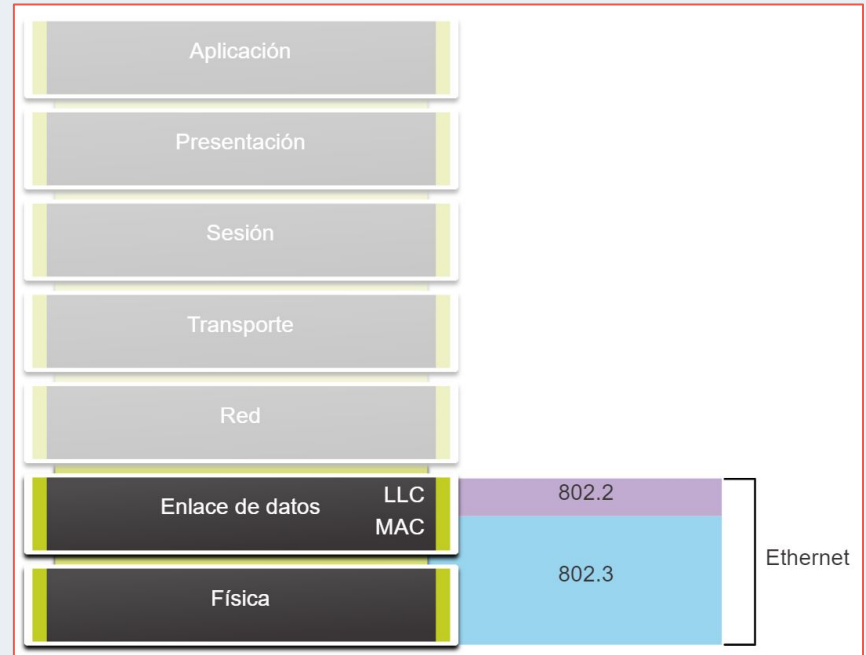
6.5. VLAN. Conceptos. Protocolo
802.1q.



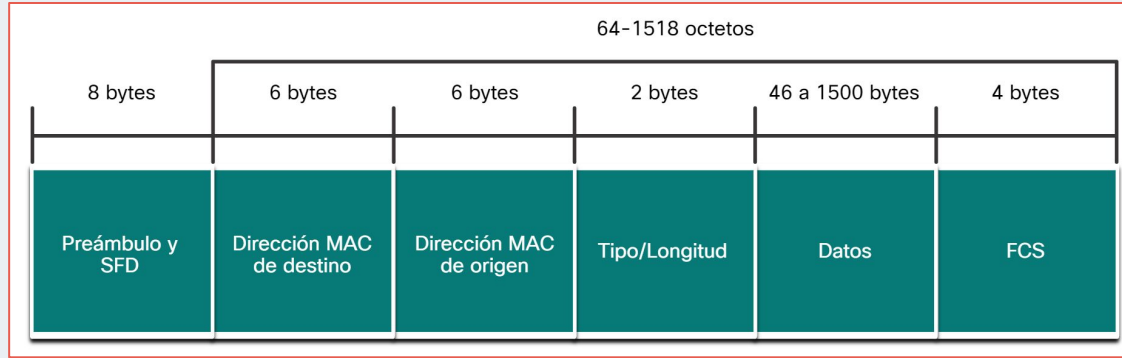
Protocolos Ethernet

Ethernet funciona en la **capa de enlace de datos** y en la **capa física**. Es una familia de tecnologías de red definidas en los estándares IEEE 802.2 y 802.3.

- **Subcapa LLC:** (IEEE 802.2) Coloca información en la trama para identificar qué protocolo de capa de red se utiliza para la trama.
- **Subcapa MAC:** (IEEE 802.3, 802.11 o 802.15) Responsable de la encapsulación de datos y control de acceso a medios, y proporciona direccionamiento de capa de enlace de datos.



Encabezado



Preámbulo: se utiliza para la sincronización; también contiene un delimitador para marcar el final de la información de temporización.

Dirección de destino: dirección MAC de 48 bits para el nodo de destino.

Dirección de origen: dirección MAC de 48 bits para el nodo de origen.

Tipo: valor para indicar qué protocolo de capa superior recibirá los datos una vez que finalice el proceso Ethernet.

Datos o contenido: esto es la PDU, normalmente un paquete IPV4, que se debe transportar a través de los medios.

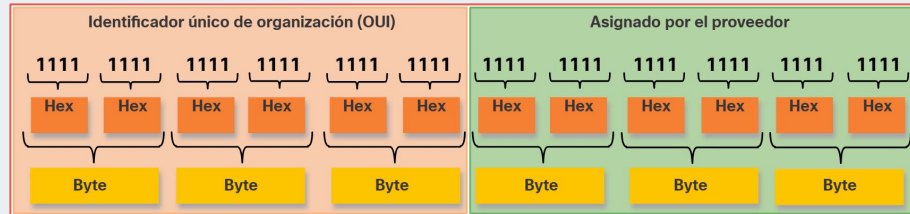
Secuencia de verificación de trama (FCS): un valor utilizado para verificar si hay tramas dañadas.

Direcciones MAC

Una dirección MAC Ethernet es una dirección de 48 bits expresada con 12 dígitos hexadecimales.

Proporciona un método para la identificación del dispositivo en la capa de enlace de datos del modelo OSI.

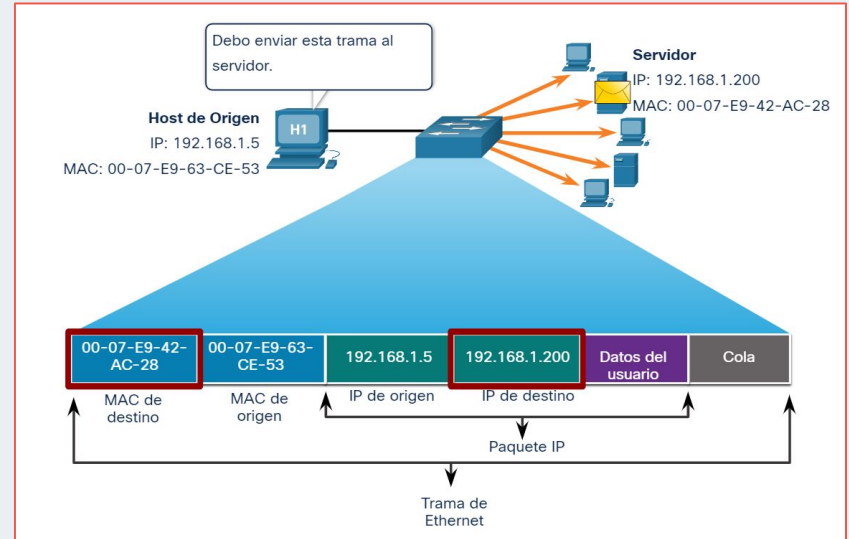
Las direcciones MAC deben ser únicas para el dispositivo Ethernet. Todos los proveedores que venden dispositivos Ethernet deben registrarse con el IEEE para obtener un código hexadecimal único de 6 denominado identificador único de organización (OUI).



MAC de unicast

En Ethernet, se utilizan diferentes direcciones MAC para las comunicaciones de unidifusión, difusión y multidifusión de capa 2.

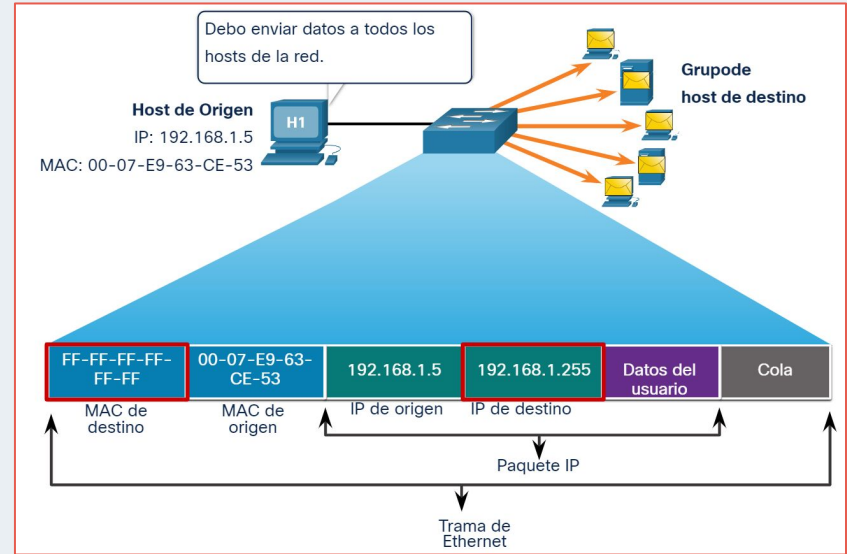
Una dirección MAC de unicast es la dirección única que se utiliza cuando se envía una trama desde un único dispositivo de transmisión a un único dispositivo de destino.



MAC de broadcast

Tiene una dirección MAC de destino de **FF-FF-FF-FF-FF-FF** en hexadecimal. Está inundado todos los puertos del conmutador Ethernet excepto el puerto entrante. No es reenviado por un router.

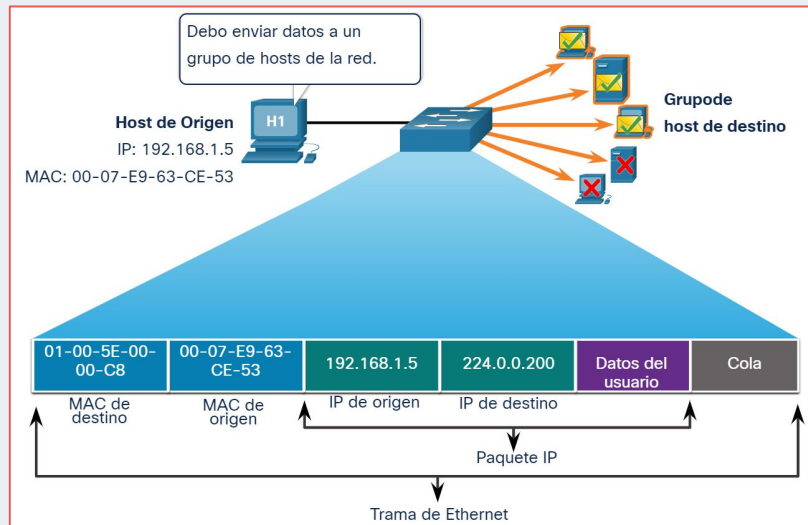
Si los datos encapsulados son un paquete broadcast IPv4, esto significa que el paquete contiene una dirección IPv4 de destino que tiene todos los (1s) en la parte del host. Todos los hosts de esa red local (dominio de difusión) recibirán y procesarán el paquete.

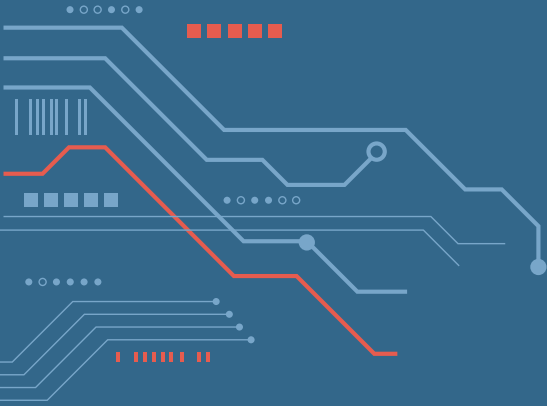


MAC de multicast

Hay una dirección MAC de destino **01-00-5E** cuando los datos encapsulados son un paquete de multidifusión IPv4 y una dirección MAC de destino de **33-33** cuando los datos encapsulados son un paquete de multidifusión IPv6.

Se inundan todos los puertos del conmutador Ethernet excepto el puerto entrante. No es reenviado por un enrutador.





| | | | | | | |

SWITCHING

Switch

Un switch Ethernet de capa 2 usa direcciones MAC de capa 2 para tomar decisiones de reenvío. No tiene conocimiento de los datos (protocolo) que se transportan en la porción de datos de la trama.

El switch toma sus decisiones de reenvío basándose únicamente en las direcciones MAC Ethernet de capa 2. Examina su tabla de direcciones MAC para tomar una decisión sobre a qué puerto re-enviar cada trama que recibe.

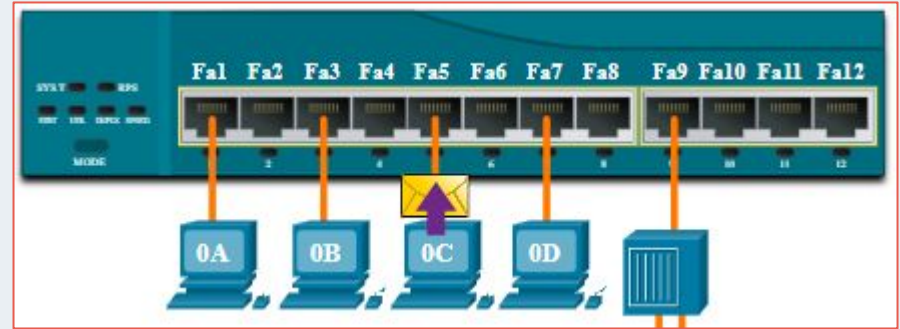
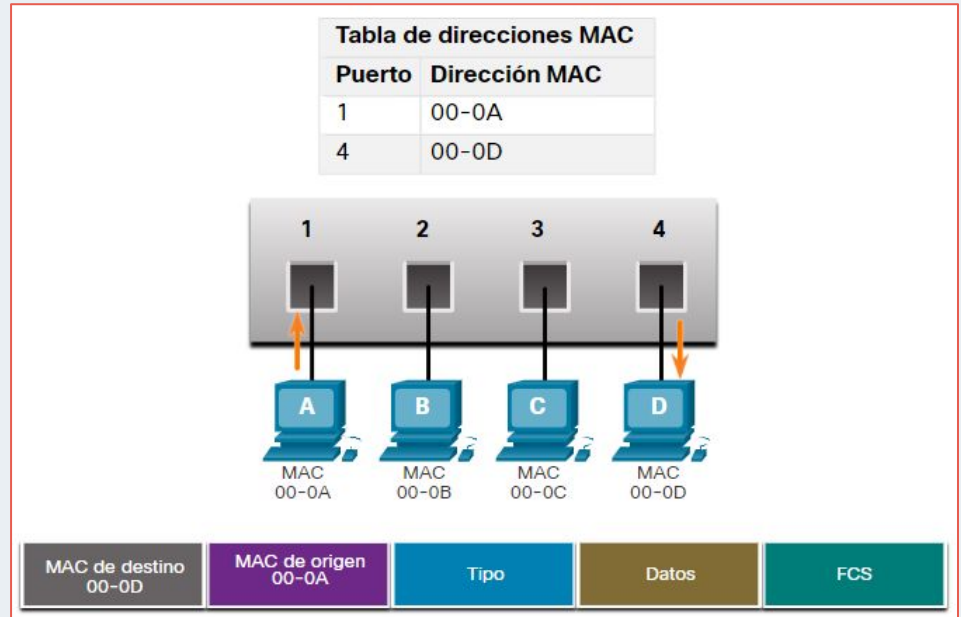


Tabla de direcciones

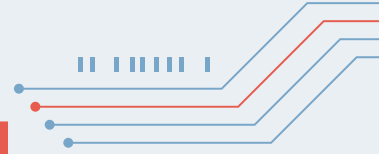
A medida que un switch recibe tramas de diferentes dispositivos, puede completar la tabla de direcciones MAC examinando la dirección MAC de cada trama.

Cuando la tabla de direcciones MAC del switch contiene la dirección MAC de destino, puede filtrar la trama y reenviar un solo puerto.

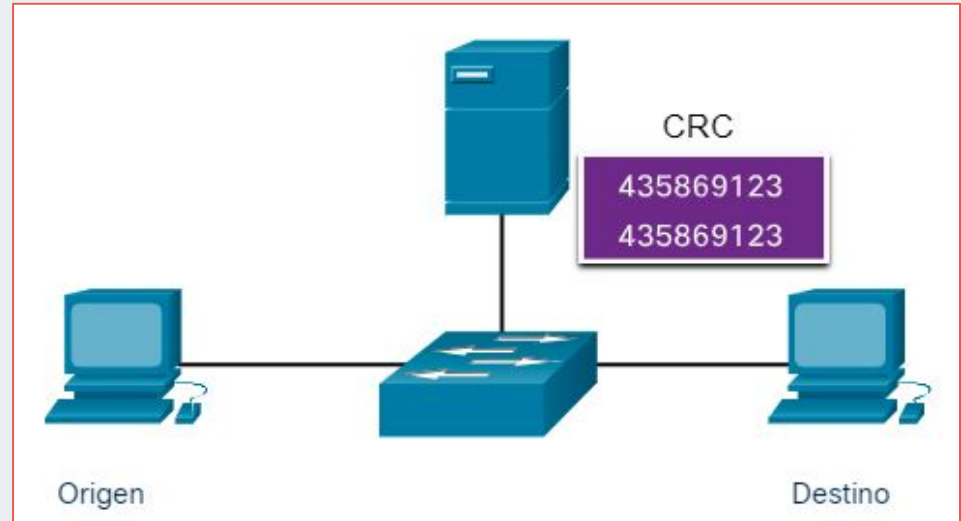
Si la dirección MAC de destino no está en la tabla, el switch reenvía la trama por todos los puertos, excepto el de entrada.



Reenvío por almacenamiento y envío



Este método de reenvío de trama **recibe la trama completa y calcula el CRC**. La CRC utiliza una fórmula matemática basada en la cantidad de bits (números uno) de la trama para determinar si esta tiene algún error. **Si la CRC es válida, el switch busca la dirección de destino, que determina la interfaz de salida.** Luego, la trama se reenvía desde el puerto correcto.



Reenvío por método de corte

- En este tipo de switching, el switch **actúa sobre los datos apenas los recibe**, incluso si la transmisión aún no se completó.
- El switch almacena la cantidad suficiente de trama como para leer la dirección MAC de destino para que pueda determinar a qué puerto debe reenviar los datos. La dirección MAC de destino se encuentra en los primeros 6 bytes de la trama después del preámbulo.
- El switch busca la dirección MAC de destino en la tabla de switching, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado.
- El switch **no lleva a cabo ninguna verificación de errores** en la trama.

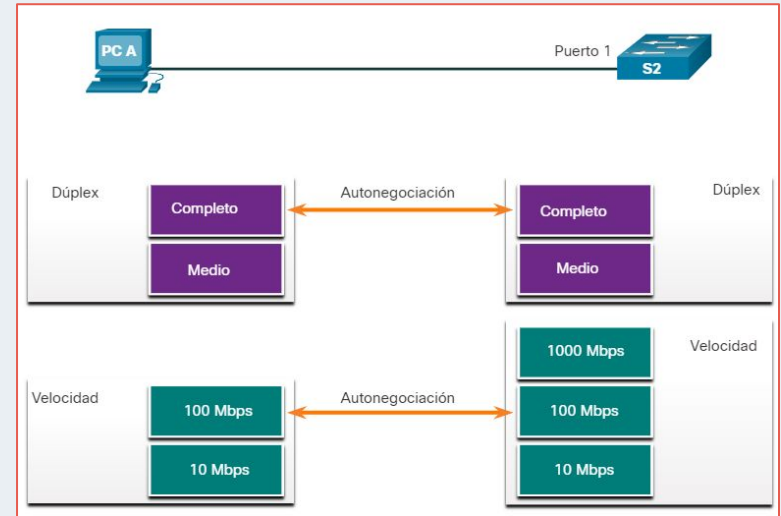


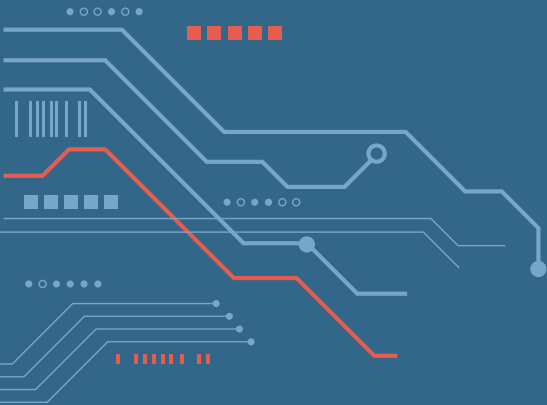
Configuración de dúplex y velocidad

Es fundamental que los parámetros de **dúplex** y de **ancho de banda** coincidan entre el puerto de switch y los dispositivos conectados, como una computadora u otro switch.

Se utilizan dos tipos de parámetros dúplex para las comunicaciones en una red Ethernet:

- **Dúplex completo** - Ambos extremos de la conexión pueden enviar y recibir datos simultáneamente.
- **Semidúplex** - Solo uno de los extremos de la conexión puede enviar datos por vez.





| | | | | | | |

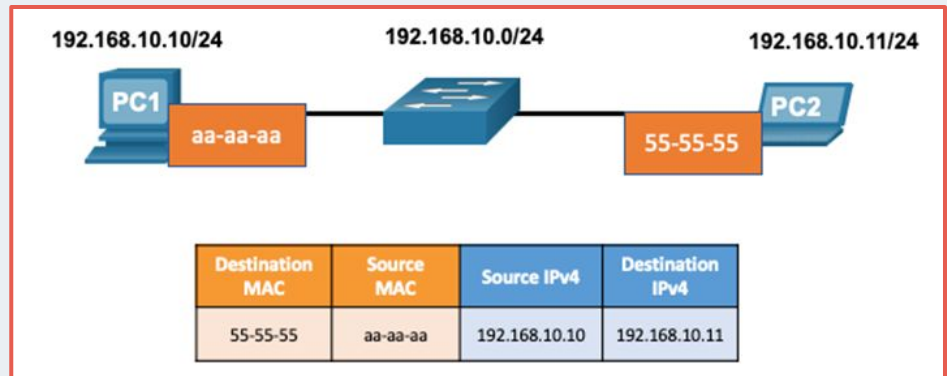
ARP

MAC e IP: Destino en la misma red

Hay dos direcciones principales asignadas a un dispositivo en una LAN Ethernet:

- **Dirección física de capa 2 (Dirección MAC):** Se utiliza para comunicaciones de NIC (Network Interface Card) a otra NIC en la misma red Ethernet.
- **Dirección lógica de capa 3 (Dirección IP):** Se utiliza para enviar el paquete desde el dispositivo de origen al dispositivo de destino.

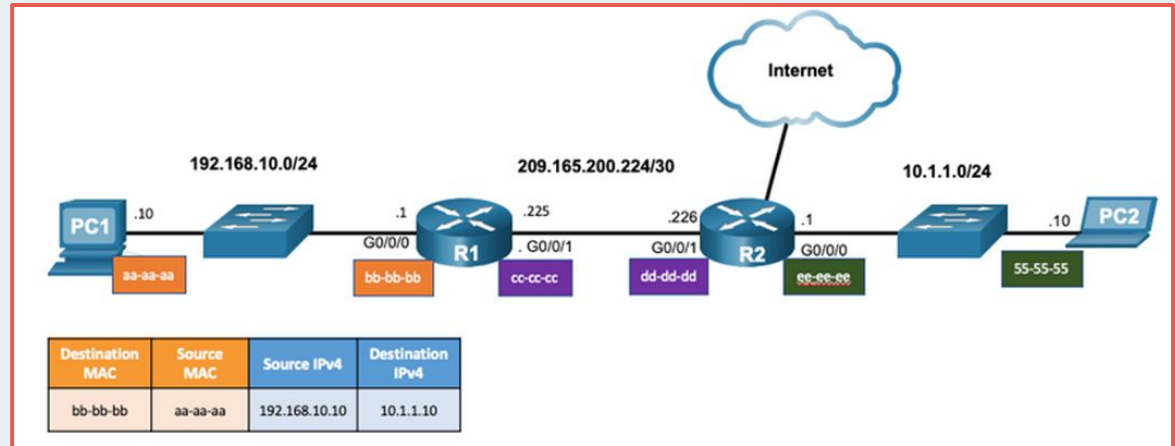
Las direcciones de capa 2 se utilizan para entregar tramas desde una NIC a otra NIC en la misma red. Si una dirección IP de destino está en la misma red, la dirección MAC de destino será la del dispositivo de destino.



MAC e IP: Destino en red remota

Cuando la dirección IP de destino está en una red remota, la dirección MAC de destino es la de la puerta de enlace predeterminada.

- IPv4 utiliza **ARP** para asociar la dirección IPv4 de un dispositivo con la dirección MAC de la NIC del dispositivo.
- IPv6 utiliza **ICMPv6** para asociar la dirección IPv6 de un dispositivo con la dirección MAC de la NIC del dispositivo.

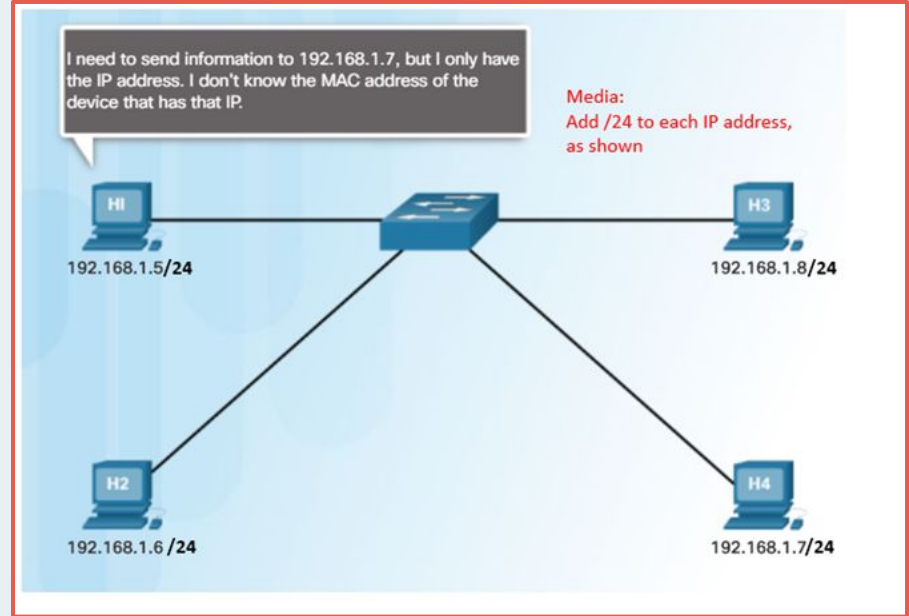


Address Resolution Protocol

Un dispositivo utiliza ARP para determinar la dirección MAC de destino de un dispositivo local cuando conoce su dirección IPv4.

ARP proporciona dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantenimiento de una tabla ARP de asignaciones de direcciones IPv4 a MAC



Funciones

Para enviar una trama, un dispositivo buscará en su tabla ARP una dirección IPv4 de destino y una dirección MAC correspondiente.

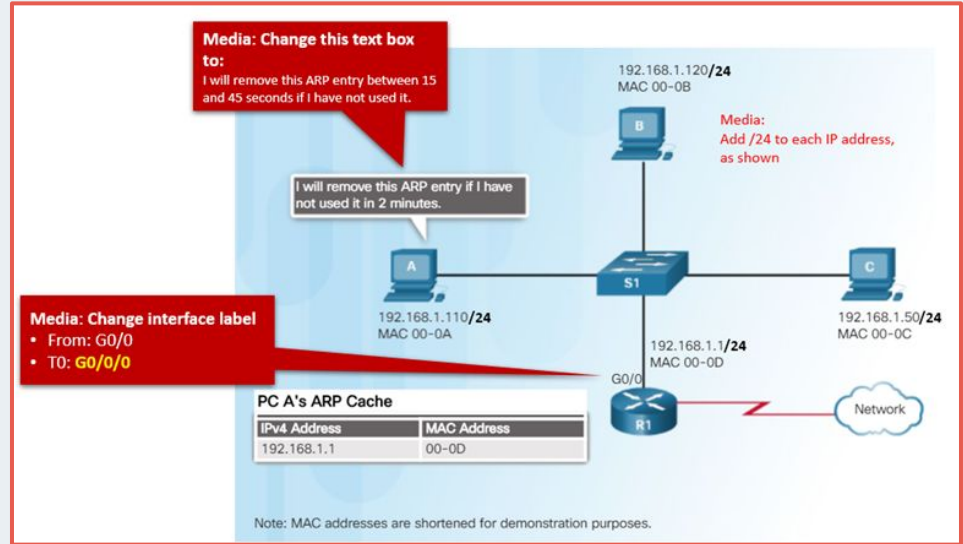
- Si la dirección IPv4 de destino del paquete está en la misma red, el dispositivo buscará en la tabla ARP la dirección IPv4 de destino.
- Si la dirección IPv4 de destino está en una red diferente, el dispositivo buscará en la tabla ARP la dirección IPv4 de la puerta de enlace predeterminada.
- Si el dispositivo localiza la dirección IPv4, se utiliza la dirección MAC correspondiente como la dirección MAC de destino de la trama.
- Si no se encuentra una entrada en la tabla ARP, el dispositivo envía una solicitud ARP.

Funcionamiento

1. Una **solicitud** de ARP es un broadcast de capa 2. Contiene la dirección IP del host de destino y la dirección MAC de broadcast: FF:FF:FF:FF:FF:FF.
2. Todos los nodos en la LAN Ethernet reciben y examinan el contenido. El nodo cuya dirección IP coincide con la dirección IP en la solicitud responde. La respuesta es una trama de unicast que incluye la dirección MAC que corresponde a la dirección IP en la solicitud. Esta respuesta se utiliza para crear una entrada nueva en la tabla ARP del nodo de envío.
3. Las entradas en la tabla ARP tienen una **marca de hora**.

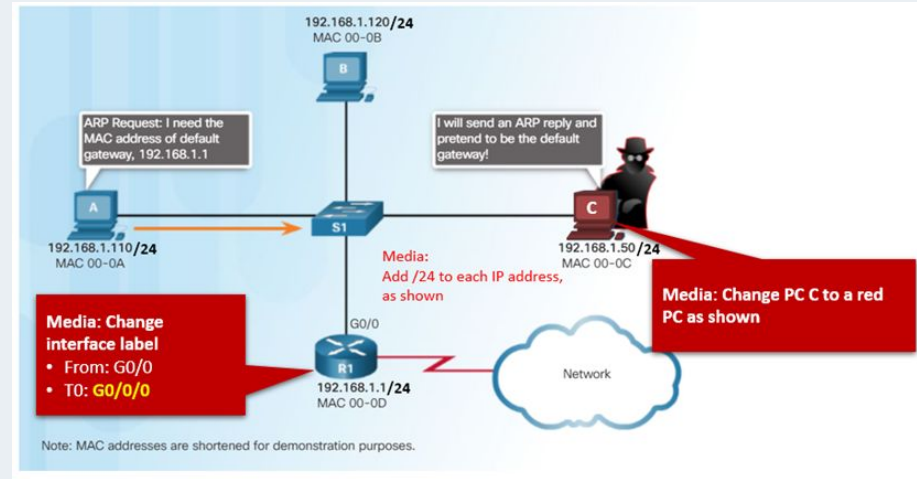
Eliminación entradas en tabla ARP

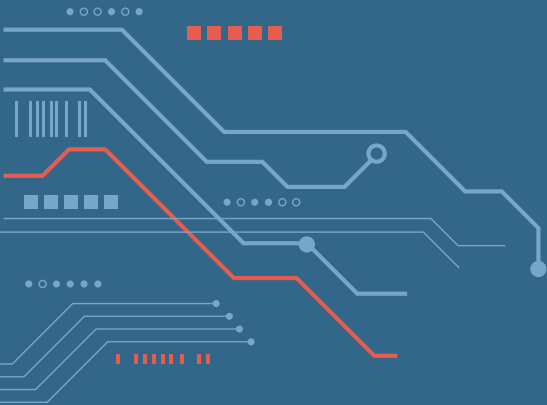
- Las entradas no son permanentes, se eliminan cuando un temporizador de caché ARP caduca después de un período de tiempo especificado.
- La duración del temporizador de caché ARP difiere según el sistema operativo.
- Las entradas también pueden ser eliminadas manualmente por el administrador.



Problemas ARP: Broadcasting y spoofing

- Las solicitudes ARP son recibidas y procesadas por cada dispositivo de la red local. Las emisiones ARP excesivas pueden causar reducción en el rendimiento.
- Las respuestas ARP pueden ser suplantadas por un actor malintencionado para realizar un ataque de envenenamiento ARP.
- Los switches empresarial incluyen técnicas de mitigación contra ataques ARP.



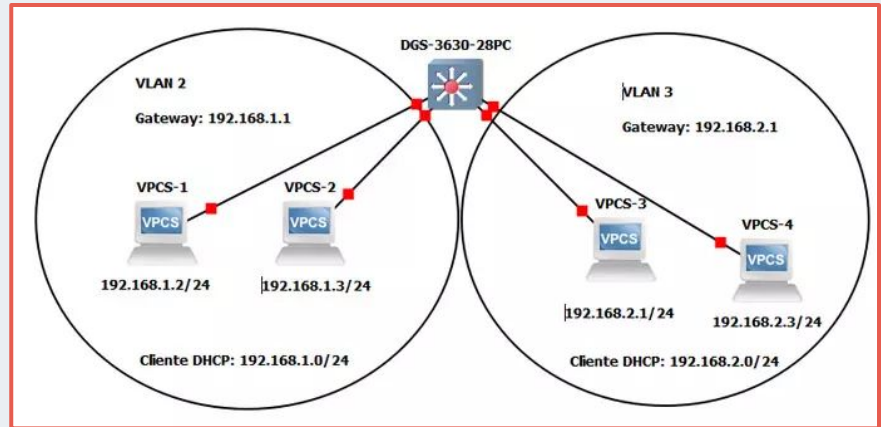


| | | | | | | |

VLAN

Virtual LAN

- VLAN es una tecnología de redes que permite crear redes lógicas independientes dentro de la misma red física.
- El objetivo de las VLAN es segmentar adecuadamente la red y usar cada subred de una forma diferente.
- Es una tecnología soportada tanto por routers como switches.



Beneficios

- **Seguridad:** No se permite a las VLANs intercambiar tráfico, es necesario ascender a nivel de red con un router.
- **Segmentación:** Nos permite segmentar todos los equipos en diferentes subredes y a cada una asignarle una VLAN diferente.
- **Flexibilidad:** Podremos colocar a los diferentes equipos en una subred o en otra de manera fácil y rápida y tener unas políticas de comunicación donde permitimos o denegamos el tráfico.
- **Optimización de la red:** Contención del broadcast en dominios más pequeños en redes donde el tráfico consiste en un alto porcentaje de transmisiones y multidifusiones.

Beneficios

- **Administración de aplicaciones y proyectos simples:**
 - Permiten asociar lógicamente a los diferentes usuarios en base a etiquetas, puertos del switch, a su dirección MAC o dependiendo de la autenticación que hayan realizado.
 - Pueden existir en un solo switch asignando a cada puerto el acceso a una determinada VLAN o en varios switches interconectados a través de los enlaces troncales.

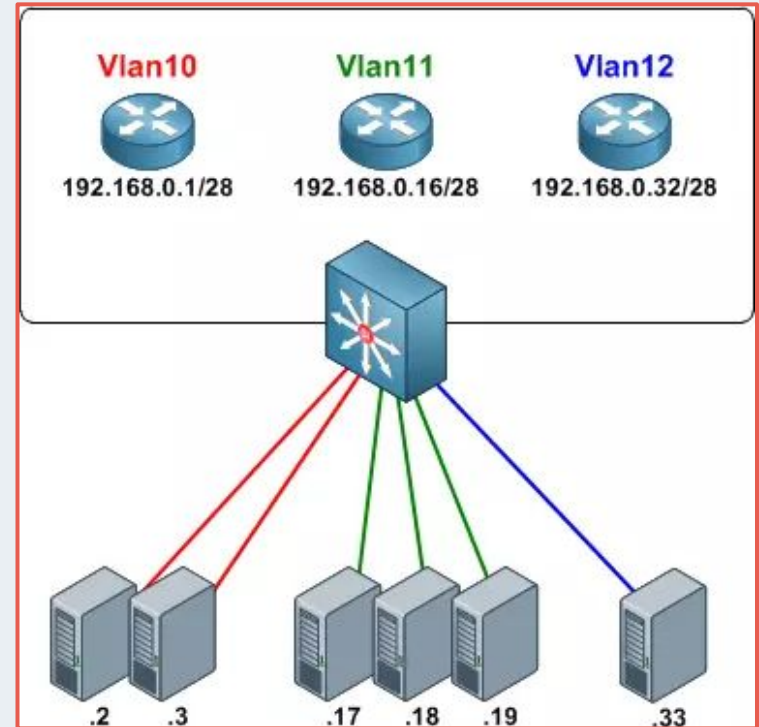
Desventajas

Administración compleja: Puede suponer el mismo o incluso más trabajo y costo que las redes LAN.

Aislamiento: Si la red es muy grande, cabe la posibilidad de que sean necesarios varios router para poder comunicarse sin problema, por lo cual aumentaría el coste de instalación.

Usos de las VLANs

Las VLAN nos va a permitir segmentar la red local en varias subredes más pequeñas enfocadas específicamente a una tarea en cuestión, además, podremos proporcionar seguridad porque las VLAN entre ellas no se podrán comunicar.



Tipos de VLANs

Las diferentes VLANs que existen son las basadas en el estándar **IEEE 802.1Q**:

- Tagging basado en etiquetas.
- Basadas en puerto.
- Basadas en MAC.
- VXLAN

Éstas se configuran en los Access Point y en los switches.

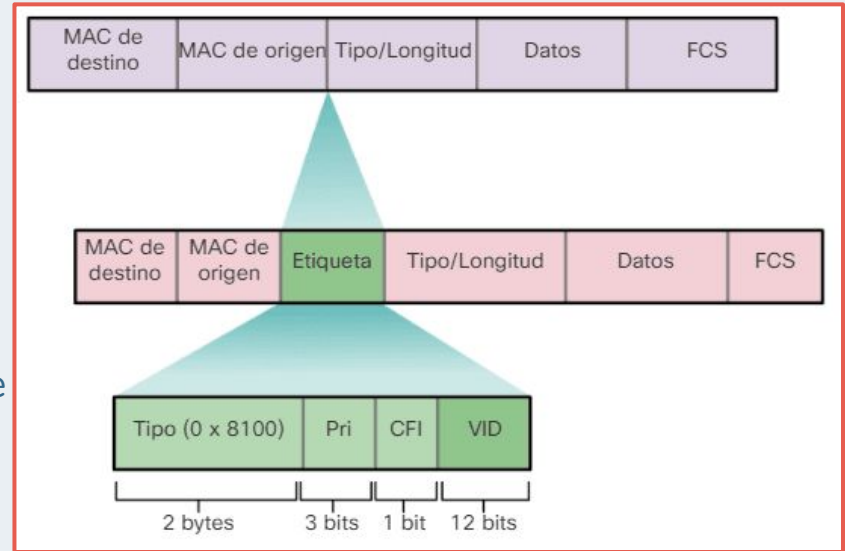
Tipos de VLAN

802.1Q VLAN Tagging

Es el tipo de VLAN más utilizada, hace uso del estándar **IEEE 802.1Q** para etiquetas o quitar la etiqueta a las VLANs.

Añade 4 bytes al encabezado y cambia el *EtherType* valor **0x8100** para señalar que se ha cambiado el formato de la trama.

Dentro de un switch podremos configurar los diferentes puertos como **tagged** o **untagged**.



Tipos de VLAN

802.1Q VLAN Tagging

- **VLAN tagged:** En las tramas Ethernet se incorpora el tag del VLAN ID. Éste tipo de VLANs son entendidas por todos los switches, por los Access Point WiFi y los routers.
- **VLAN untagged:** En las tramas Ethernet se retira el tag del VLAN ID. Principalmente se utilizan de cara a los equipos finales como ordenadores, portátiles, impresoras, cámaras IP y otro tipo de dispositivos.

Tipos de VLAN

802.1Q VLAN Tagging

Los switches permiten configurar los puertos físicos de diferentes formas:

- **Acceso:** Son los puertos donde conectaremos los PC, impresoras, smartphones y los equipos finales, este puerto de acceso tendrá configurada una VLAN como *untagged*.
- **Troncal o trunk:** Lleva una o varias VLANs de un equipo capa 2 a otro capa 2. Aceptan los paquetes *tagged* que se le configuren sin modificarlos.
- **Dynamic:** Dependiendo del tipo de paquete que reciba el switch, se pondrá como access o como trunk. Por seguridad, no es recomendable ésta configuración.

Tipos de VLAN

VLAN basadas en puerto

También conocida como *Port Switching* se trata de la más extendida y utilizada por switches de gama muy baja. Cada puerto se asigna a una VLAN y los usuarios que estén conectados a ese puerto pertenecen a la VLAN asignada. Los usuarios dentro de una misma VLAN poseen visibilidad los unos sobre los otros, aunque no a las redes locales virtuales vecinas.

Tipos de VLAN

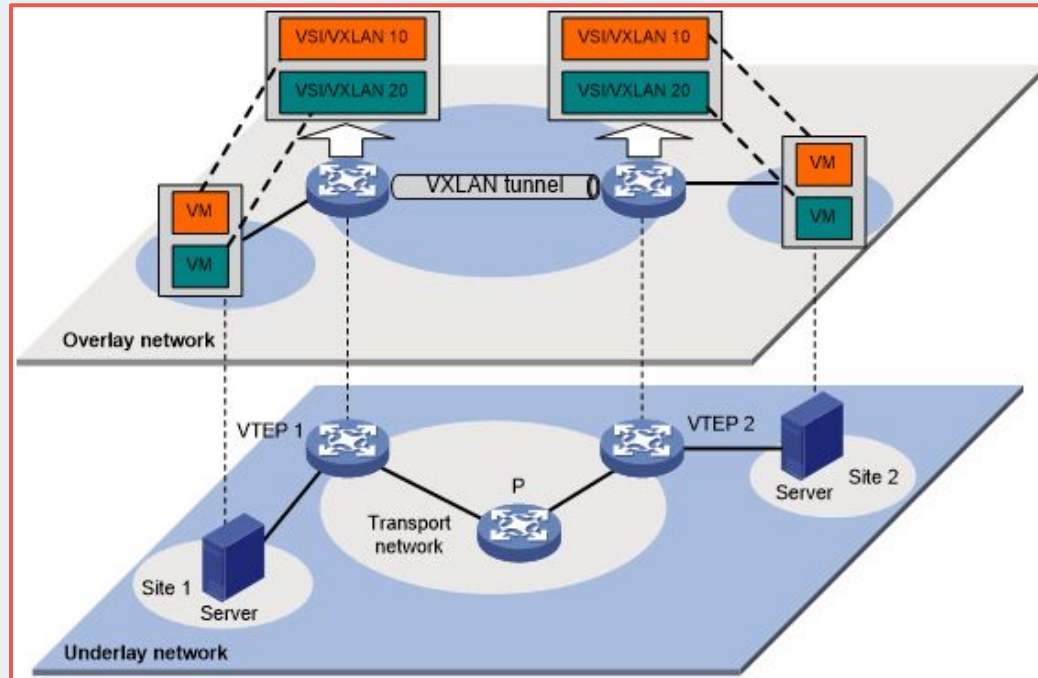
VLAN basadas en MAC

Cada dirección MAC se asigna a una VLAN. Permite movilidad sin necesidad de que se tengan que aplicar cambios en la configuración del switch o del router, pero se necesita cargar las MACs de todos los dispositivos.

Solamente los switches de gama más alta permiten VLAN basada en MAC.

Tipos de VLAN

VXLAN

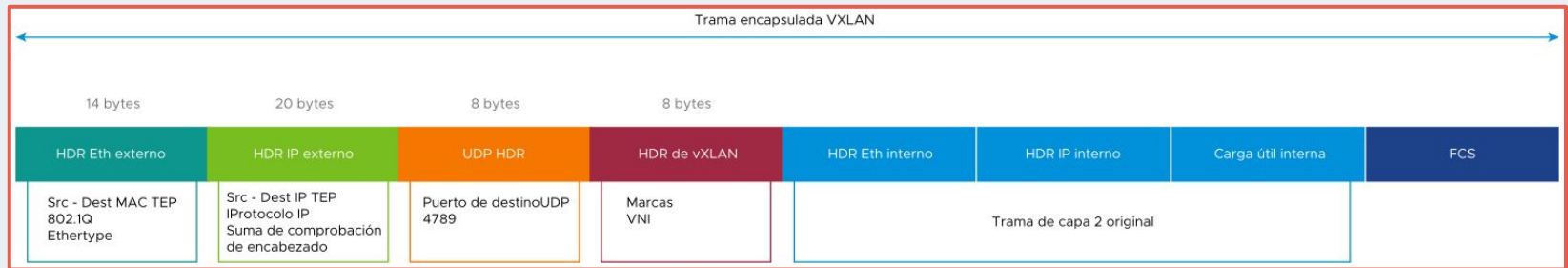


Tipos de VLAN

VXLAN

Se las conoce como VLAN Extendida. Superpone redes de capa 2, en una infraestructura de capa 3, encapsulando tramas de capa 2 en paquetes UDP.

Se identifica mediante un identificador único de 24 bits denominado VXLAN Network Identifier (VNI).



RECURSOS BIBLIOGRÁFICOS

- Cisco NetAcad Introduction to Networks:
 - Módulo 7: “Switching Ethernet”
 - Módulo 9: “Resolución de dirección”

<https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/>