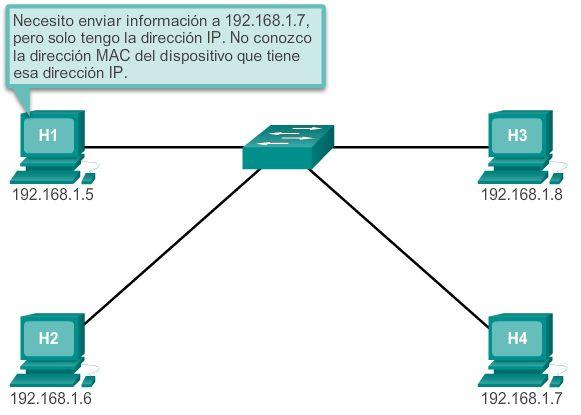
# Introducción a ARP

Cada nodo de una red IP tiene tanto una dirección MAC como una dirección IP. Para enviar datos, el nodo debe utilizar ambas direcciones. El nodo debe utilizar sus propias direcciones MAC e IP en los campos de origen y debe proporcionar una dirección MAC y una dirección IP para el destino. Mientras que una capa OSI superior proporciona la dirección IP del destino, pero el nodo de envío necesita encontrar la dirección MAC del destino para un enlace de Ethernet determinado. Ese es el propósito del protocolo ARP.

El protocolo ARP se basa en determinados tipos de mensajes Ethernet de broadcast y unicast, denominados “solicitudes ARP” y “respuestas ARP”.El protocolo ARP ofrece dos funciones básicas:

 Resolución de direcciones IPv4 a direcciones MAC

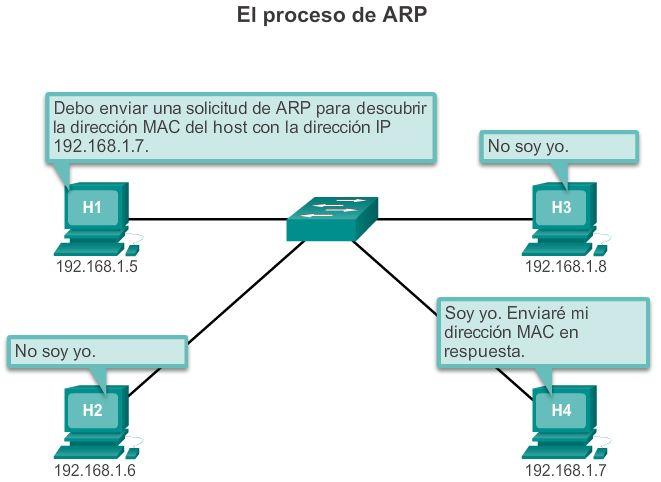
 Mantenimiento de una tabla de las asignaciones



# Funciones del protocolo ARP

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino. Cuando se envía un paquete a la capa de enlace de datos para que se encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de enlace de datos asignada a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

**Mantenimiento de la tabla ARP**

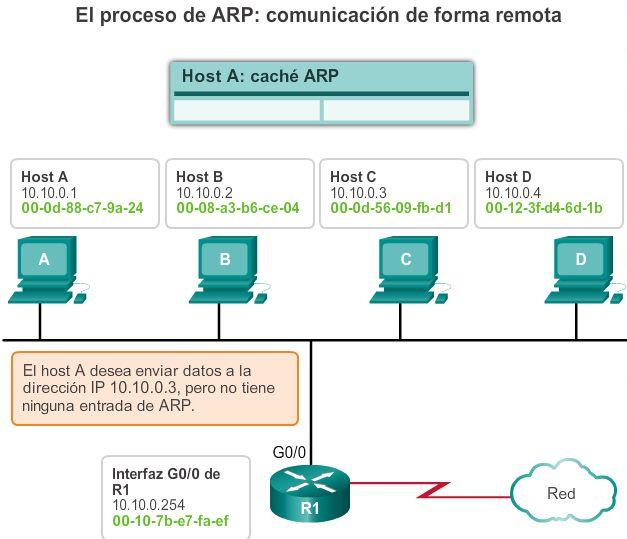
La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones. 

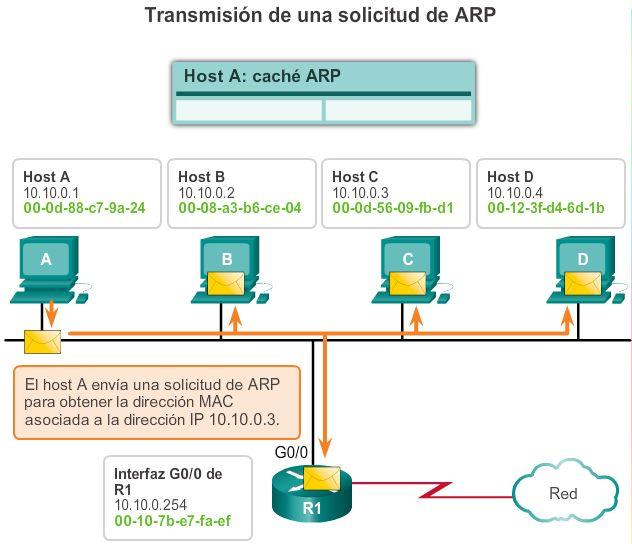
# Funcionamiento del ARP

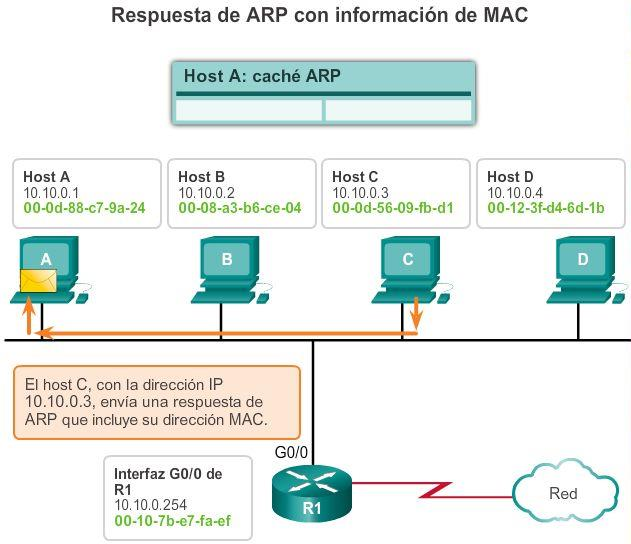
**¿Qué hace un nodo cuando debe crear una trama y la caché ARP no contiene una asignación de una dirección IP hacia una dirección MAC de destino?** Genera una solicitud de ARP. Cuando el ARP recibe una solicitud para mapear una dirección IPv4 a una dirección MAC, busca el mapa almacenado en su tabla ARP. Si no encuentra la entrada, la encapsulación del paquete IPv4 no se realiza y los procesos de Capa 2 notifican al ARP que necesita un mapa. Los procesos ARP envían entonces un paquete de solicitud de ARP para descubrir la dirección MAC del dispositivo de destino de la red local. Si un dispositivo que recibe la solicitud tiene la dirección IP de destino, responde con una respuesta de ARP. Se crea un mapa en la tabla ARP. Los paquetes para esa dirección IPv4 pueden ahora encapsularse en tramas.

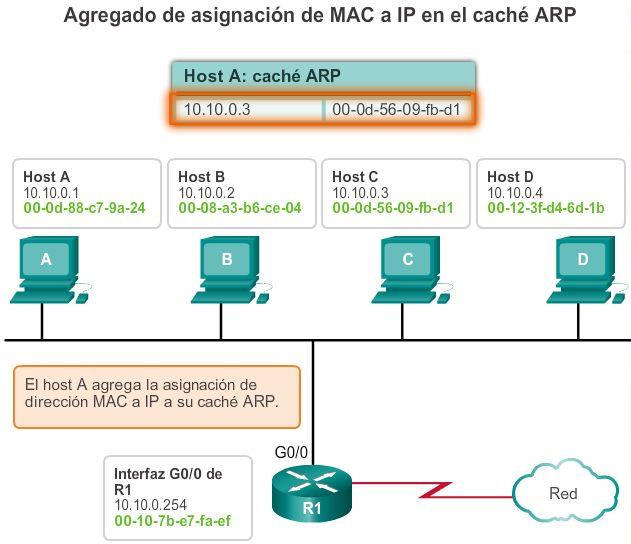
Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no puede crearse una trama. Esta falla de encapsulación se informa a las capas superiores del dispositivo.

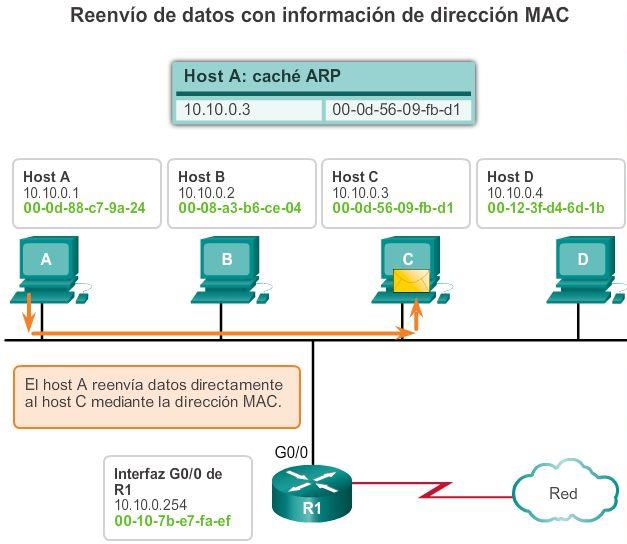
Si el dispositivo es un dispositivo intermediario, como, por ejemplo, un router, las capas superiores pueden optar por responder al host de origen con un error en un paquete ICMPv4.











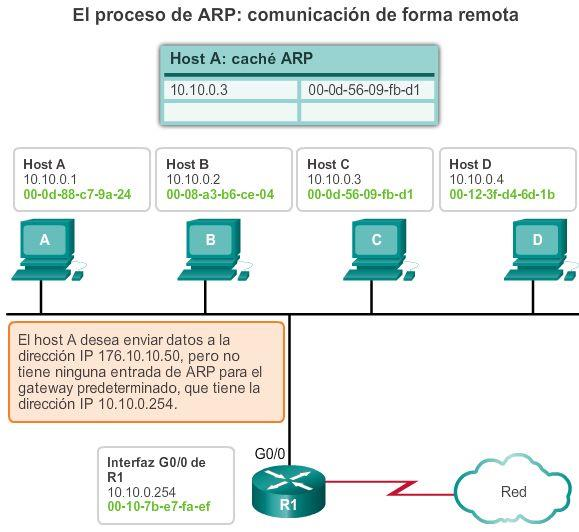
# Función del protocolo ARP en la comunicación remota

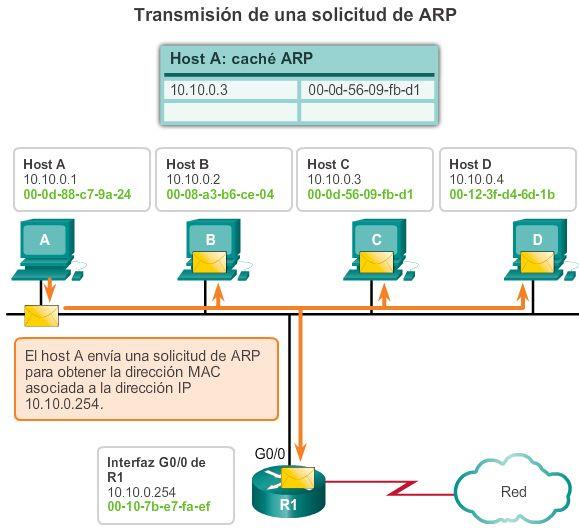
Todas las tramas deben enviarse a un nodo de un segmento de red local. Si el host IPv4 de destino se encuentra en la red local, la trama utilizará la dirección MAC de este dispositivo como la dirección MAC de destino.

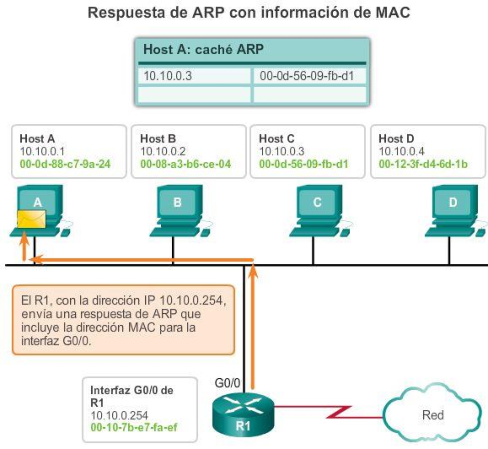
Si el host IPv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del router que es el gateway o el siguiente salto que se utiliza para llegar a dicho destino. El nodo de origen utilizará la dirección MAC del gateway como dirección de destino para las tramas que contengan un paquete IPv4 dirigido a hosts que se encuentren en otras redes.

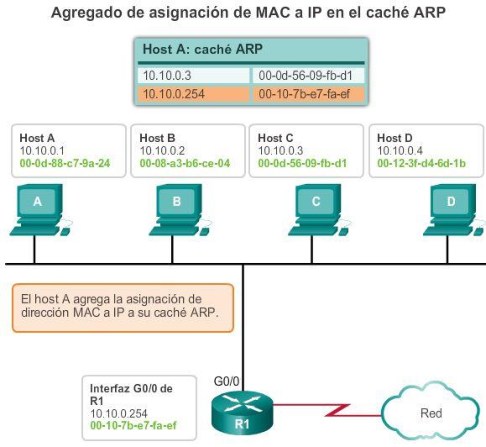
En caso de que la entrada de gateway no se encuentre en la tabla, el proceso de ARP normal enviará una

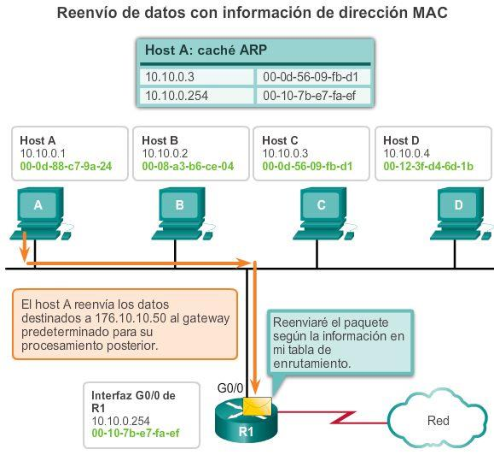
solicitud de ARP para recuperar la dirección MAC asociada con la dirección IP de la interfaz del router.









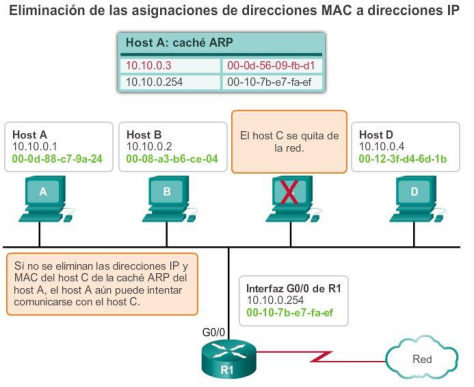


# Eliminación de entradas de una tabla ARP

Para cada dispositivo, un temporizador de caché ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y su sistema operativo. Por ejemplo: algunos sistemas operativos de Windows almacenan las entradas de caché ARP por 2minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

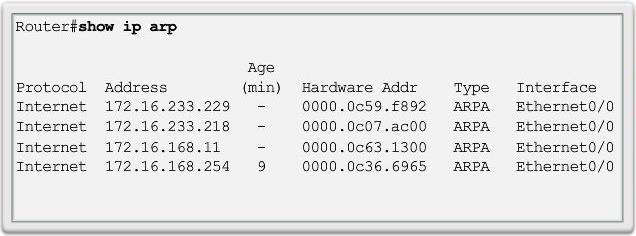
También pueden utilizarse comandos para eliminar manualmente todas o algunas de las entradas de la tabla ARP. Después de eliminar una entrada, el proceso para enviar una solicitud de ARP y recibir una respuesta de ARP debe ocurrir nuevamente para ingresar la asignación en la tabla ARP.

Cada dispositivo tiene un comando específico del sistema operativo para eliminar el contenido de la caché ARP.

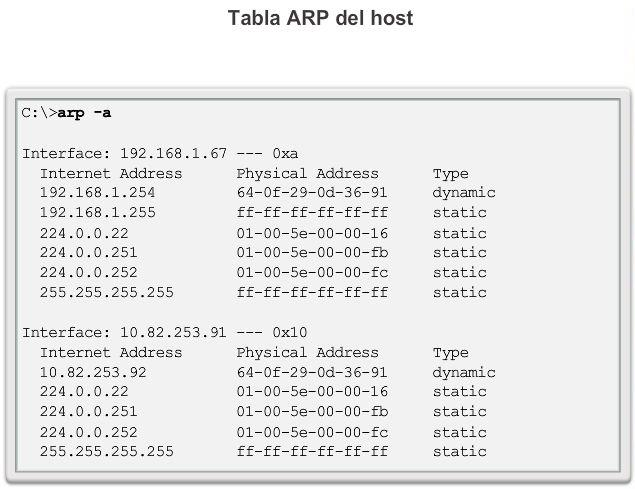


# Tablas ARP en dispositivos de red

En un router Cisco, se utiliza el comando show ip arp para mostrar la tabla ARP



En una PC con Windows 7, se utiliza el comando arp -a para mostrar la tabla ARP.



# Cómo puede ocasionar problemas el protocolo ARP

**Sobrecarga en los medios**

Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de broadcast. En una red comercial típica, estos broadcasts tendrían probablemente un impacto mínimo en el rendimiento de la red. Sin embargo, si un gran número de dispositivos se encendiera y todos comenzaran a acceder a los servicios de la red al mismo tiempo, podría haber una disminución del rendimiento durante un período de tiempo breve.

**Seguridad**

En algunos casos, el uso del ARP puede ocasionar un riesgo potencial de seguridad. La suplantación o el envenenamiento ARP es una técnica que utiliza un atacante para introducir una asociación de direcciones MAC incorrecta en una red emitiendo respuestas ARP falsas. El individuo falsifica la dirección MAC de un dispositivo y de esta manera las tramas pueden enviarse a la dirección equivocada.

