



Universidad Industrial de Santander Escuela de Sistemas

Redes de Computadoras Seguridad Enlace de Datos

Prof. Gilberto Díaz
gilberto.diaz@uis.edu.co



Envenenamiento ARP

Uno de los ataques más comunes es el ARP spoofing o ARP poisoning. Este se usa para implementar ataques más sofisticados:

- Negación de Servicio (DoS)
- Hombre en el medio (Man in the middle)



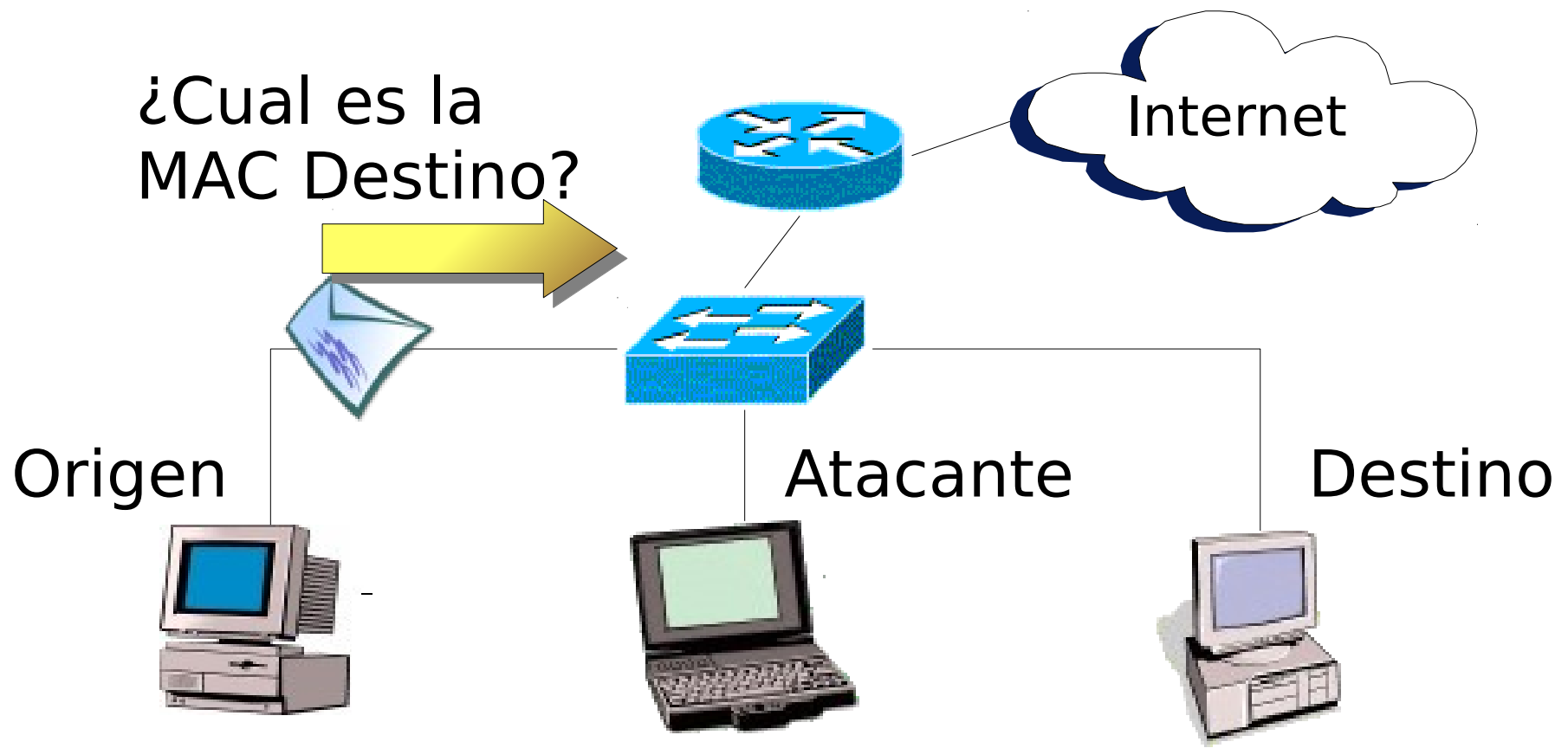
Envenenamiento ARP

El envenenamiento de las tablas ARP se basa en el envío de respuestas fraudulentas para hacer que el tráfico no vaya al nodo destino verdadero sino a otro lado.



Envenenamiento ARP

Cuando se escucha una solicitud de ARP se envía una respuesta falsa.





Envenenamiento ARP

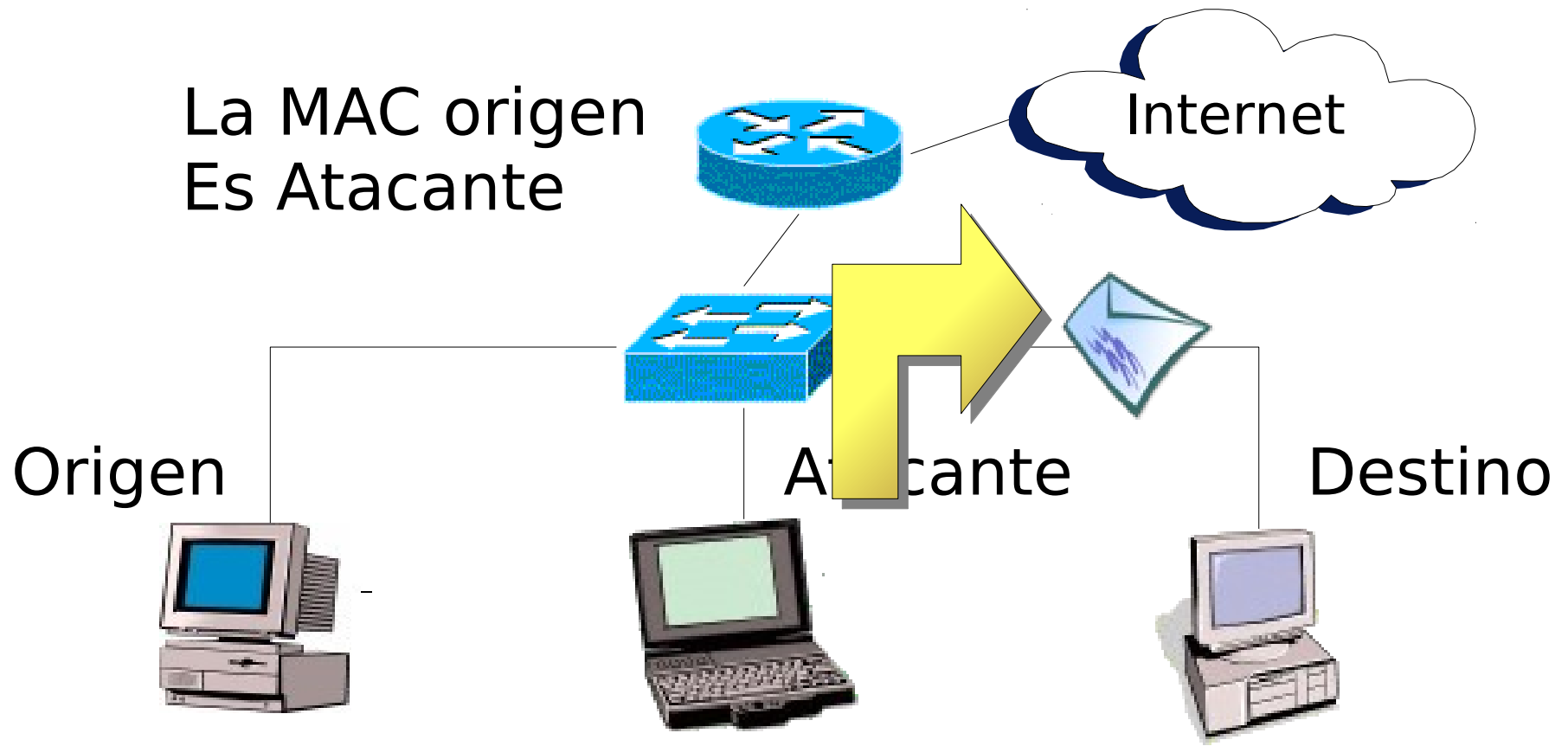
Cuando se escucha una solicitud de ARP se envía una respuesta falsa.





Envenenamiento ARP

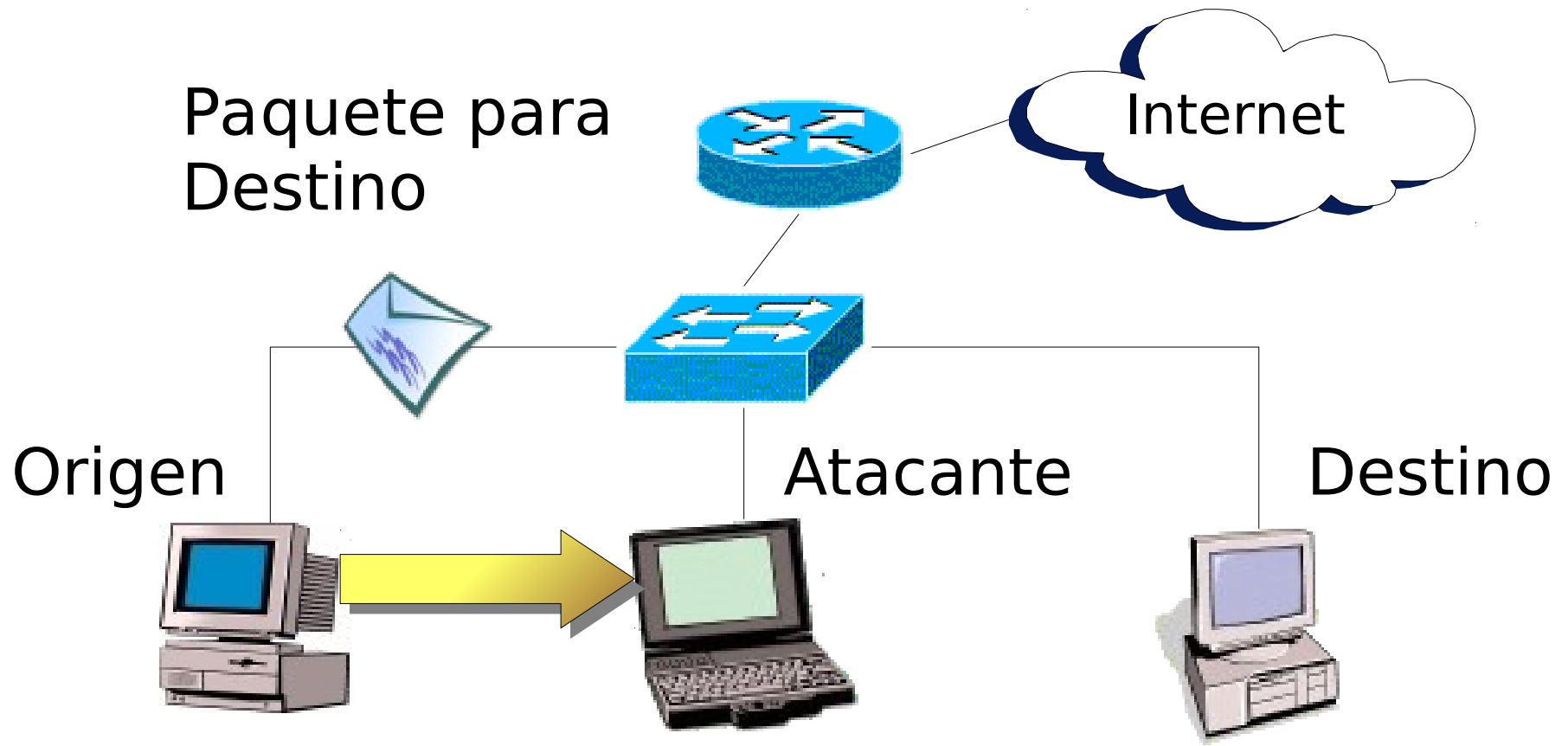
Cuando se escucha una solicitud de ARP se envía una respuesta falsa.





Envenenamiento ARP

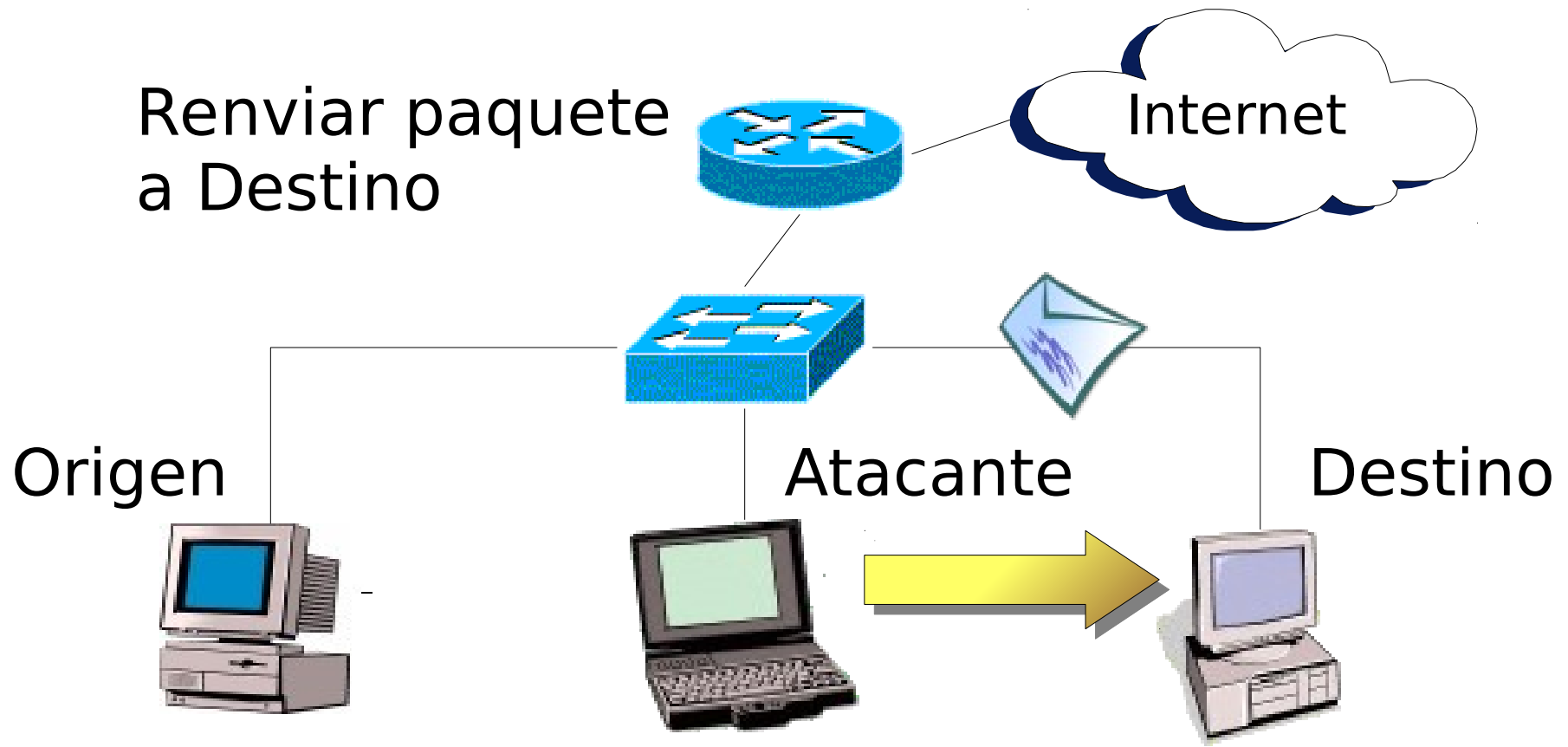
Cuando se escucha una solicitud de ARP se envía una respuesta falsa.





Envenenamiento ARP

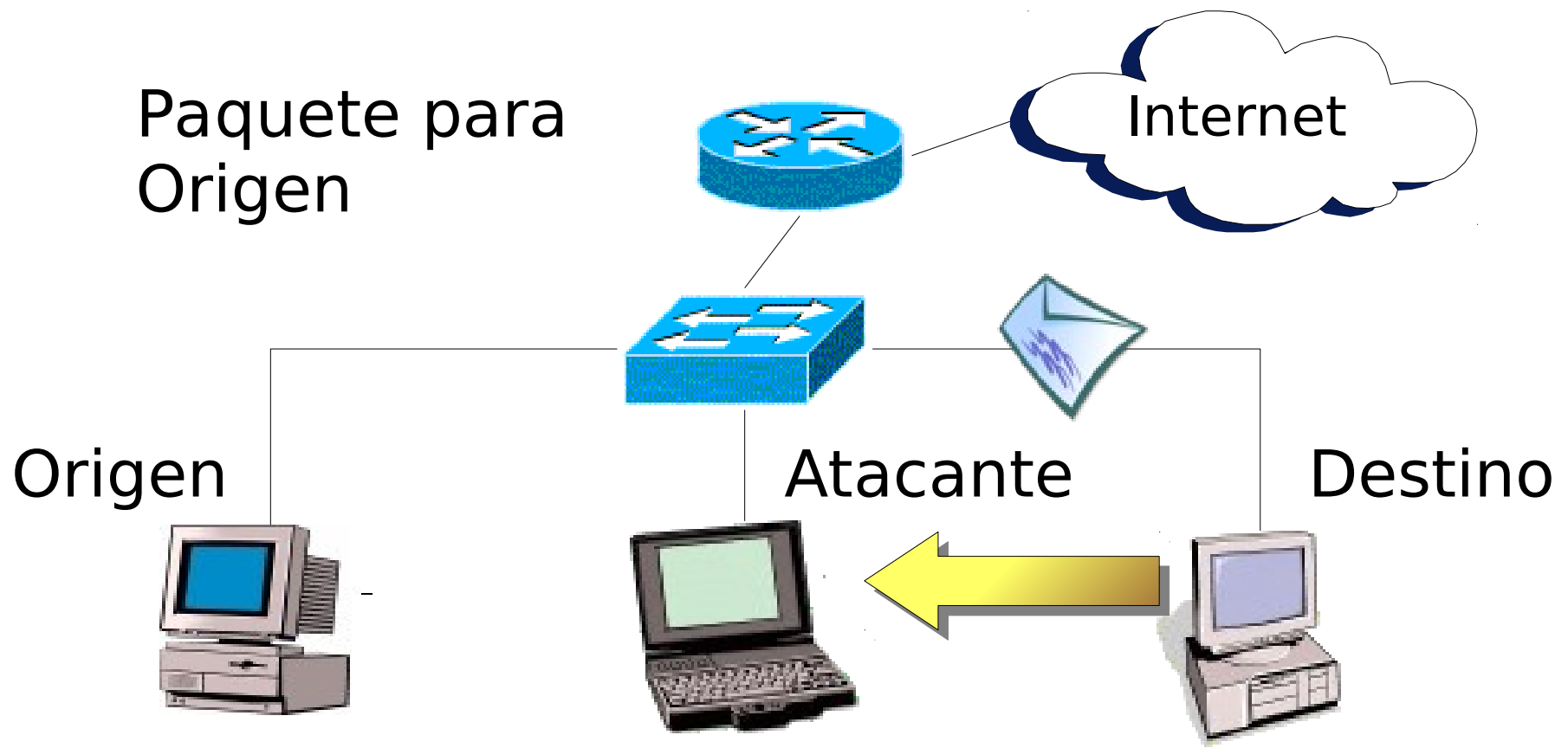
Cuando se escucha una solicitud de ARP se envía una respuesta falsa.





Envenenamiento ARP

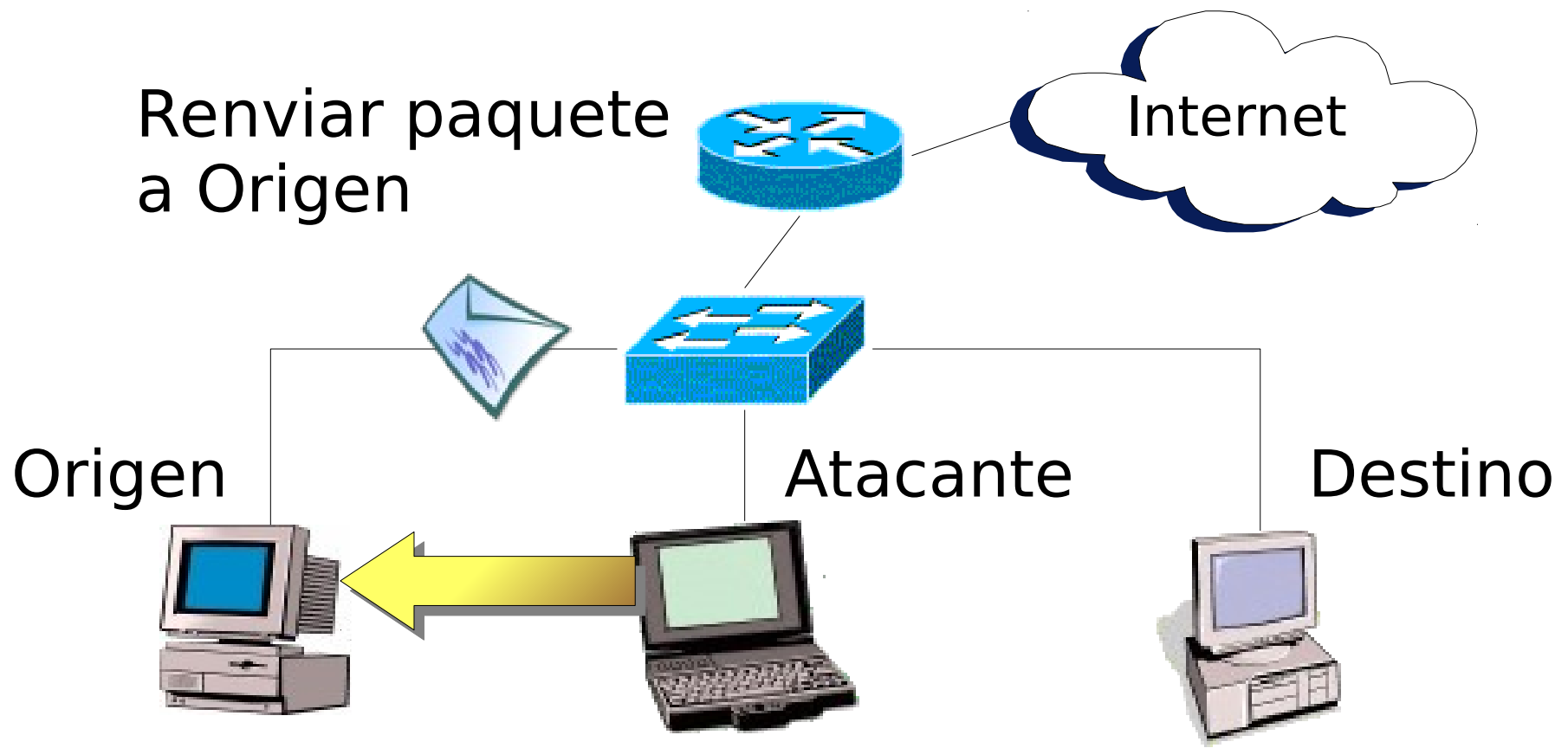
Cuando se escucha una solicitud de ARP se envía una respuesta falsa.





Envenenamiento ARP

Cuando se escucha una solicitud de ARP se envía una respuesta falsa.



- Utilizar direcciones MAC fijas de los hosts más importantes de la red local (servidores, enrutadores, etc) a través del archivo

/etc/ethers

- Asignar MAC fijas a cada puerto de los switches
- Instalar herramientas de detección de ataques