

# Proxy ARP

From Wikipedia, the free encyclopedia

**Proxy ARP** is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The ARP Proxy is aware of the location of the traffic's destination, and offers its own MAC address as (ostensibly final) destination. The "captured" traffic is then typically routed by the Proxy to the intended destination via another interface or via a tunnel.

The process which results in the node responding with its own MAC address to an ARP request for a different IP address for proxying purposes is sometimes referred to as 'publishing'.

## Uses

Below are some typical uses for proxy ARP:

### Joining a broadcast LAN with serial links (e.g., dialup or VPN connections).

Assume an Ethernet broadcast domain (e.g., a group of stations connected to the same hub or switch (VLAN)) using a certain IPv4 address range (e.g., 192.168.0.0/24, where 192.168.0.1 – 192.168.0.127 are assigned to wired nodes). One or more of the nodes is an access router accepting dialup or VPN connections. The access router gives the dial-up nodes IP addresses in the range 192.168.0.128 – 192.168.0.254; for this example, assume a dial-up node gets IP address 192.168.0.254.

The access router uses Proxy ARP to make the dial-up node present in the subnet without being wired into the Ethernet: the access server 'publishes' its own MAC address for 192.168.0.254. Now, when another node wired into the Ethernet wants to talk to the dial-up node, it will ask on the network for the MAC address of 192.168.0.254 and find the access server's MAC address. It will therefore send its IP packets to the access server, and the access server will know to pass them on to the particular dial-up node. All dial-up nodes therefore appear to the wired Ethernet nodes as if they are wired into the same Ethernet subnet.

### Taking multiple addresses from a LAN

Assume a station (e.g., a server) with an interface (10.0.0.2) connected to a network (10.0.0.0/24). Certain applications may require multiple IP addresses on the server. Provided the addresses have to be from the 10.0.0.0/24 range, the way the problem is solved is through Proxy ARP. Additional addresses (say, 10.0.0.230-10.0.0.240) are aliased to the loopback interface of the server (or assigned to special interfaces, the latter typically being the case with VMware/UML/jails/vservers/other virtual server environments) and 'published' on the 10.0.0.2 interface (although many operating systems allow direct allocation of multiple addresses to one interface, thus eliminating the need for such tricks).

### On a firewall

In this scenario a firewall can be configured with a single IP address. One simple example of a use for this would be placing a firewall in front of a single host or group of hosts on a subnetwork. Example- A network (10.0.0.0/8) has a server which should be protected (10.0.0.20) a proxy-arp firewall can be placed in front of the server. In this way the server is put behind a firewall without making any changes to the network at all.

### Mobile-IP

In case of Mobile-IP the Home Agent uses Proxy ARP in order to receive messages on behalf of the

Mobile Node, so that it can forward the appropriate message to the actual mobile node's address (Care-of address).

### **Transparent subnet gatewaying**

A setup that involves two physical segments sharing the same IP subnet and connected together via a router. This use is documented in RFC 1027.

## **Disadvantages**

Disadvantage of Proxy ARP include scalability (ARP resolution is required for every device routed in this manner) and reliability (no fallback mechanism is present, and masquerading can be confusing in some environments). ARP manipulation techniques, however, are the basis for protocols providing redundancy on broadcast networks (e.g., Ethernet), most notably CARP and Virtual Router Redundancy Protocol.

Proxy ARP can create DoS attacks on networks if misconfigured. For example, a misconfigured router with proxy ARP has the ability to receive packets destined for other hosts (as it gives its own MAC address in response to ARP requests for other hosts/routers), but may not have the ability to correctly forward these packets on to their final destination, thus blackholing the traffic.

Proxy ARP can "hide" device misconfigurations, such as a missing or incorrect default gateway.

## **Further reading**

- RFC 925 – Multi-LAN Address Resolution
- RFC 1027 – Using ARP to Implement Transparent Subnet Gateways
- W. Richard Stevens. The Protocols (TCP/IP Illustrated, Volume 1). Addison-Wesley Professional; 1st edition (December 31, 1993). ISBN 0-201-63346-9

Retrieved from "[https://en.wikipedia.org/w/index.php?title=Proxy\\_ARP&oldid=674542913](https://en.wikipedia.org/w/index.php?title=Proxy_ARP&oldid=674542913)"

Categories: Internet protocols | Internet Standards

- 
- This page was last modified on 4 August 2015, at 16:23.
  - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.