

# ARP Injection Overview



Revision 1.1

## ARP Defined

Address Resolution Protocol (ARP) is a protocol to handle conversions from a host's network layer address to its hardware address.<sup>1</sup> In other words, ARP enables devices to discover the connection between a host's IP address and its MAC address. This method of automatic discovery allows communication between hosts on the same network, hosts on different networks, and communication through devices such as firewalls, bridges, and access servers.

ARP works by sending out a broadcast message, called ARP request, which is normally answered by the owner of the address with a unicast ARP reply message.

## Gratuitous ARP Request Defined

Gratuitous ARP Request (also known as "ARP announcement") is a type of request that is unsolicited, and is normally not intended to cause a reply. While Gratuitous ARP Requests can serve many purposes,<sup>2,3</sup> the most prominent use of such a request is for a host to announce its existence in the network. For further information, please see the section titled "Additional Information."

## The ARP Injection Technique

One of the main reasons ARP is important in wireless network security is that, in some situations, it can be used to force the generation of packets with new WEP Initialization Vectors (IV). Capturing these packets and replaying them can be used to efficiently decipher the WEP key of a WLAN.

ARP messages are interesting for three reasons: ARP requests elicit ARP replies; ARP requests are of fixed, known size; and ARP requests are small, thus they are able to be transmitted in large quantity.

Fixed packet size is important as packets of a fixed size are easy to identify without the need to decrypt them. This unique property can be used to identify ARP requests even on a network for which it doesn't have a decryption key.

Once an ARP request is identified on the target network, it is then replayed many times per second. For a normal ARP request, this elicits an ARP reply from the target for every ARP request, with the benefit that every ARP reply carries a new WEP Initialization Vector. Because of this, transmitting ARP requests can be very useful for coaxing the target network into generating the wireless traffic necessary for an attack. For this reason, this technique is the most effective way used by well-known tools like Cain & Abel and aircrack-ng to speed up the retrieval of a network's WEP key.

---

<sup>1</sup> RFC 826 - Address Resolution Protocol, a.k.a. STD 37

<sup>2</sup> Wireshark Gratuitous ARP - [wiki.wireshark.org/Gratuitous\\_ARP](http://wiki.wireshark.org/Gratuitous_ARP)

<sup>3</sup> How to Disable the Gratuitous ARP Function - [support.microsoft.com/kb/219374](http://support.microsoft.com/kb/219374)

## Why Injecting ARP Requests Might Not Generate Unique IVs

If the replayed request is a Gratuitous ARP Request, normally the request will not elicit any response. Tools like Cain & Abel or aircrack-ng, however, are unable to discern normal ARP requests from Gratuitous ARP Requests as they are the same size. Because the target network traffic is encrypted, there is no method of packet identification other than size. Thus, it is possible to discern ARP packets from those that are unlikely to be ARP packets, but it's not possible to discern normal ARP requests from Gratuitous ARP Requests.

The result is that, in some cases, Cain & Abel or aircrack-ng will see something that looks like an ARP packet and start replaying it, but this will generate no responses (and, therefore, no Unique IVs).

### Additional Information

- [Wireshark Wiki](http://wiki.wireshark.org/Gratuitous_ARP) - [wiki.wireshark.org/Gratuitous\\_ARP](http://wiki.wireshark.org/Gratuitous_ARP)
  - A good overview of Gratuitous ARP with examples
- [RFC 826](http://tools.ietf.org/html/rfc826) - [tools.ietf.org/html/rfc826](http://tools.ietf.org/html/rfc826)
  - The official specification
- [Header Format](http://www.networksorcery.com/enp/protocol/arp.htm) - [www.networksorcery.com/enp/protocol/arp.htm](http://www.networksorcery.com/enp/protocol/arp.htm)
  - Map of the ARP protocol
- [Wikipedia](http://en.wikipedia.org/wiki/Address_Resolution_Protocol) - [en.wikipedia.org/wiki/Address\\_Resolution\\_Protocol](http://en.wikipedia.org/wiki/Address_Resolution_Protocol)
  - General overview of ARP