Address Resolution Protocol (ARP)

Updated: January 21, 2005


Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a required TCP/IP standard defined in RFC 826, "Address Resolution Protocol (ARP)." ARP resolves IP addresses used by TCP/IP-based software to media access control addresses used by LAN hardware. ARP provides the following protocol services to hosts located on the same physical network:

- Media access control addresses are obtained by using a network broadcast request in the form of the question "What is the media access control address for a device that is configured with the enclosed IP address?"

- When an ARP request is answered, both the sender of the ARP reply and the original ARP requester record each other's IP address and media access control address as an entry in a local table called the ARP cache for future reference.

Hardware addressing

Hardware built for use on LANs must contain a unique address programmed into the device by the manufacturer. For Ethernet and Token Ring LAN hardware, this address is known as a media access control address.

Each media access control address identifies the device within its own physical network with a 6-byte number programmed into read-only memory (ROM) on each physical hardware device, such as a network adapter. Media access control addresses are typically displayed in hexadecimal (for example, 00-AA-00-3F-89-4A).

Authority and registration of media access control addresses are overseen by the Institute of Electrical and Electronics Engineers (IEEE). Currently, the IEEE registers and assigns unique numbers for the first three bytes of the media access control address to individual manufacturers. Each manufacturer can then assign the last three bytes of the media access control address to individual network adapters.

How ARP resolves media access control addresses for local traffic

The following illustration shows how ARP resolves IP addresses to hardware addresses for hosts on the same local network.

In this example, two TCP/IP hosts, Host A and B, are both located on the same physical network. Host A is assigned the IP address of 10.0.0.99 and Host B is assigned the IP address of 10.0.0.100.

When Host A tries to communicate with Host B, the following steps resolve Host B's software-assigned address (10.0.0.100) to Host B's hardware-assigned media access control address:

1. Based on the contents of the routing table on Host A, IP determines that the forwarding IP address to be used to reach Host B is 10.0.0.100. Host A then checks its own local ARP cache for a matching hardware address for Host B.

2. If Host A finds no mapping in the cache, it broadcasts an ARP request frame to all hosts on the local network with the question "What is the hardware address for 10.0.0.100?" Both hardware and software addresses for the source, Host A, are included in the ARP request.

   Each host on the local network receives the ARP request and checks for a match to its own IP address. If a host does not find a match, it discards the ARP request.

3. Host B determines that the IP address in the ARP request matches its own IP address and adds a hardware/software address mapping for Host A to its local ARP cache.

4. Host B sends an ARP reply message containing its hardware address directly back to Host A.

5. When Host A receives the ARP reply message from Host B, it updates its ARP cache with a hardware/software address mapping for Host B.

Once the media access control address for Host B has been determined, Host A can send IP traffic to Host B by addressing it to Host B's media access control address.

How ARP resolves media access control addresses for remote traffic

ARP is also used to forward IP datagrams to local routers for destinations that are not on the local network. In this situation, ARP resolves the media access control address of a router interface on the local network.

The following illustration shows how ARP resolves IP addresses to hardware addresses for two hosts on different physical networks connected by a common router.

In this example, Host A is assigned an IP address of 10.0.0.99 and Host B uses an IP address of 192.168.0.99. Router interface 1 is on the same physical network as Host A and uses the IP address 10.0.0.1. Router interface 2 is on the same physical network as Host B and uses the IP address 192.168.0.1.

When Host A tries to communicate with Host B, the following steps resolve Router interface 1’s software-assigned address (10.0.0.1) to its hardware-assigned media access control address:

1. Based on the contents of the routing table on Host A, IP determines that the forwarding IP address to be used to reach host B is 10.0.0.1, the IP address of its default gateway. Host A then checks its own local ARP cache for a matching hardware address for 10.0.0.1.

2. If Host A finds no mapping in the cache, it broadcasts an ARP request frame to all hosts on the local network with the question “What is the hardware address for 10.0.0.1?” Both hardware and software addresses for the source, Host A, are included in the ARP request.

   Each host on the local network receives the ARP request and checks for a match to its own IP address. If a host does not find a match, it discards the ARP request.

3. The router determines that the IP address in the ARP request matches its own IP address and adds a hardware/software address mapping for Host A to its local ARP cache.

4. The router then sends an ARP reply message containing its hardware address directly back to Host A.

5. When Host A receives the ARP reply message from the router, it updates its ARP cache with a hardware/software address mapping for 10.0.0.1.

Once the media access control address for Router interface 1 has been determined, Host A can send IP traffic to Router interface 1 by addressing it to the Router interface 1 media access control address. The router then forwards the traffic to Host B through the same ARP process as discussed in this section.

The ARP cache

To minimize the number of broadcasts, ARP maintains a cache of IP address-to-media access control address mappings for future use. The ARP cache can contain both dynamic and static entries. Dynamic entries are added and removed automatically over time. Static entries remain in the cache until the computer is restarted.

Each dynamic ARP cache entry has a potential lifetime of 10 minutes. New entries added to the cache are timestamped. If an entry is not reused within 2 minutes of being added, it expires and is removed from the ARP cache. If an entry is used, it receives two more minutes of lifetime. If an entry keeps getting used, it receives an additional two minutes of lifetime up to a maximum lifetime of 10 minutes.

You can view the ARP cache by using the `arp` command. To view the ARP cache, type `arpSa` at a command prompt. To view `arp` command-line options, type `arpJa` at a command prompt.

**Note**

- There is a separate ARP cache for each network adapter.