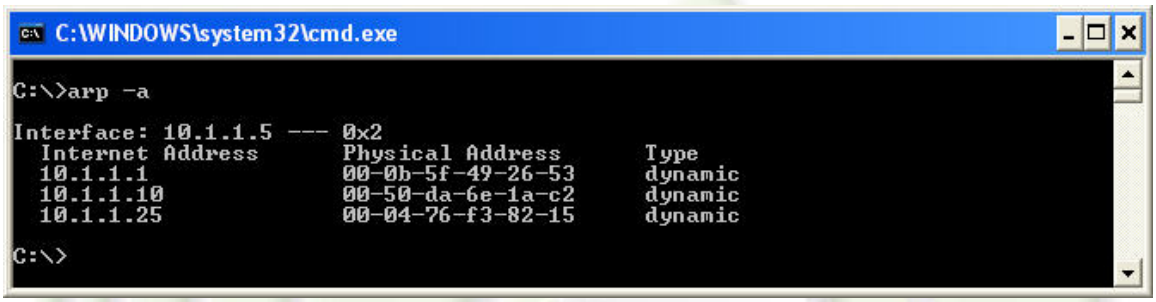
2.1.1

ADDRESS RESOLUTION PROTOCOL

(ARP)

USING MICROSOFT WINDOWS



Laboratory Overview

Objective

At the end of this lab students will be able to use the arp.exe TCP/IP utility to view and modify the ARP cache.

Information for Laboratory

A. Students will utilize the arp.exe Windows TCP/IP utility

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Instructor Preparation

Before class, the instructor or a lab assistant will ensure that each student has access to a Windows based computer with Network connectivity and TCP/IP installed and working.

Estimated Completion Time

30 Minutes

Address Resolution Protocol (ARP)

In the most basic definition, ARP is used to translate hardware (MAC) addresses to Internet Protocol (IP) addresses over Ethernet.

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IP version 4, to map IP network addresses to the hardware addresses used by a data link protocol. Address Resolution Protocol operates below the network layer as a part of the interface between the OSI network and OSI Data link layers.

The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.

An Ethernet network uses hardware addresses to identify the source and destination of each frame sent on the Ethernet. The hardware address is also known as the Medium Access Control (MAC) address. Each computer network interface card is allocated a globally unique 6 byte (48 bit) MAC address when the factory manufactures the card (stored in a PROM). This is the normal MAC source address used by an interface. A computer sends all packets which it creates with its own hardware MAC source address, and receives all packets which match the same hardware address in the destination field or one (or more) pre-selected broadcast/multicast addresses.

The Ethernet address is a data-link layer address and is dependent on the interface card which is used. IP operates at the network layer and is not concerned with the data-link addresses of individual nodes which are to be used. The address resolution protocol (ARP) is therefore used to translate

between the two types of address. The ARP client and server processes operate on all computers using IP over Ethernet.

The processes are normally implemented as part of the software driver that drives the network interface card.

There are four types of arp messages that may be sent by the arp protocol. The types of message are:

1. ARP request
2. ARP reply
3. RARP request (Reverse ARP)
4. RARP reply (Reverse ARP)

To reduce the number of address resolution requests, a client normally caches resolved addresses for a short period of time. The ARP cache is of a finite size, and would become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow without check. The ARP cache is therefore periodically flushed of all entries. This deletes unused entries and frees space in the cache. It also removes any unsuccessful attempts to contact computers which are not currently running.

Example of the use of the Address Resolution Protocol (arp)

Let's say computer A is trying to contact computer B on the same LAN via the "ping" program. It is assumed that no previous IP datagrams have been sent or received form this computer, and therefore ARP must first be used to identify the MAC address of the remote computer.

The ARP request message…

"WHO IS X.X.X.X TELL Y.Y.Y.Y"

Where computer B's IP address is X.X.X.X and computer A's IP address is Y.Y.Y.Y. The ARP request message is sent using the Ethernet broadcast address. Since it is broadcast, it is

received by all systems on the same LAN. This ensures that the target of the query is in fact connected to the network. Only this system responds. The other systems on the LAN discard the packet silently.

The target system computer B, receives the request, processes it, and forms an ARP response,

"X.X.X.X is hh:hh:hh:hh:hh:hh"

Where hh:hh:hh:hh:hh:hh is the Ethernet (MAC) source address of computer B, itself. This packet is send unicast to the address of the computer sending the query (in this case Y.Y.Y.Y). Since the original request also included the hardware address (MAC source address) of the requesting computer, this is already known, and doesn't require another ARP message to find this out. After Computer A receives the response, it processes it and caches the IP address with the corresponding MAC address. IP datagrams from the network layer, with destination IP addresses may now be encapsulated in Ethernet frames, moved down to the physical layer where its put on the wire and received by the destination node with the correct Ethernet address.

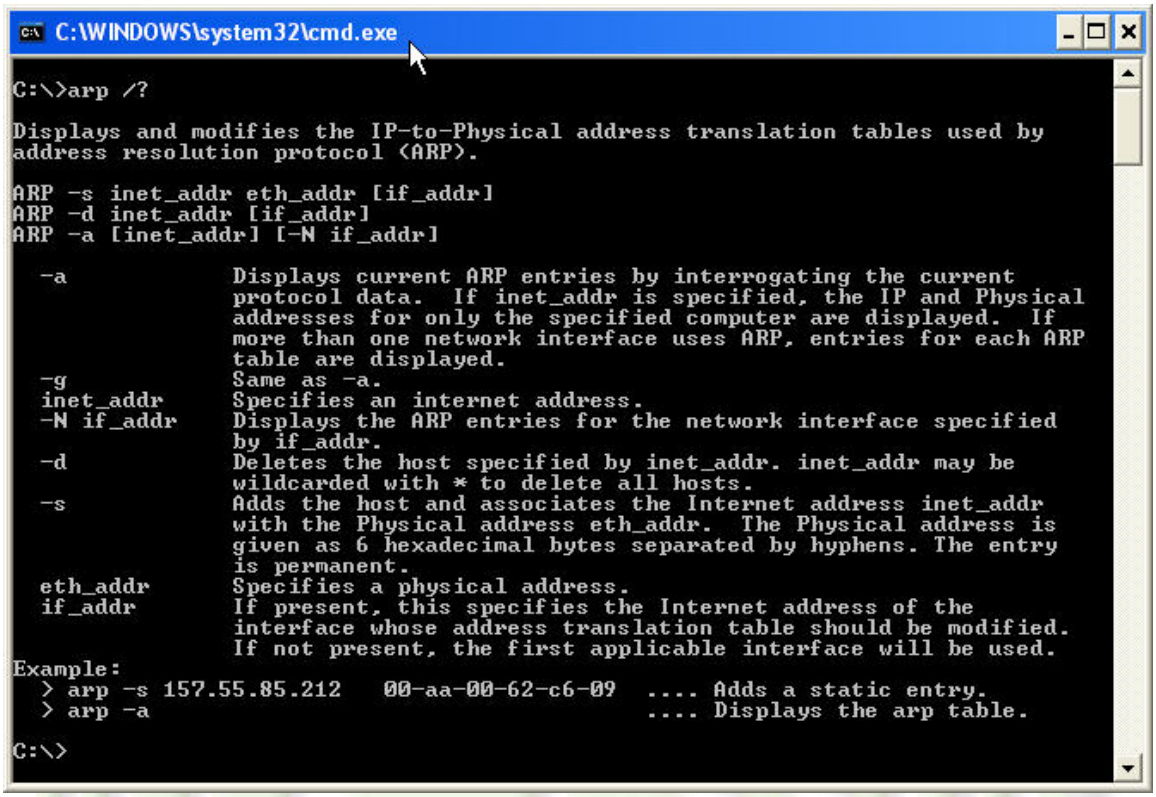
ARP Commands via Windows TCP/IP Utilities arp.exe

All TCP/IP enabled devices connected via Ethernet have loaded, and use Address Resolution Protocol. Most computer operating systems such as windows and unix have command line utilities such as arp.exe. In this lab, The Microsoft Windows operating system will be used to explore the features of ARP using arp.exe

Step 1: ARP /?

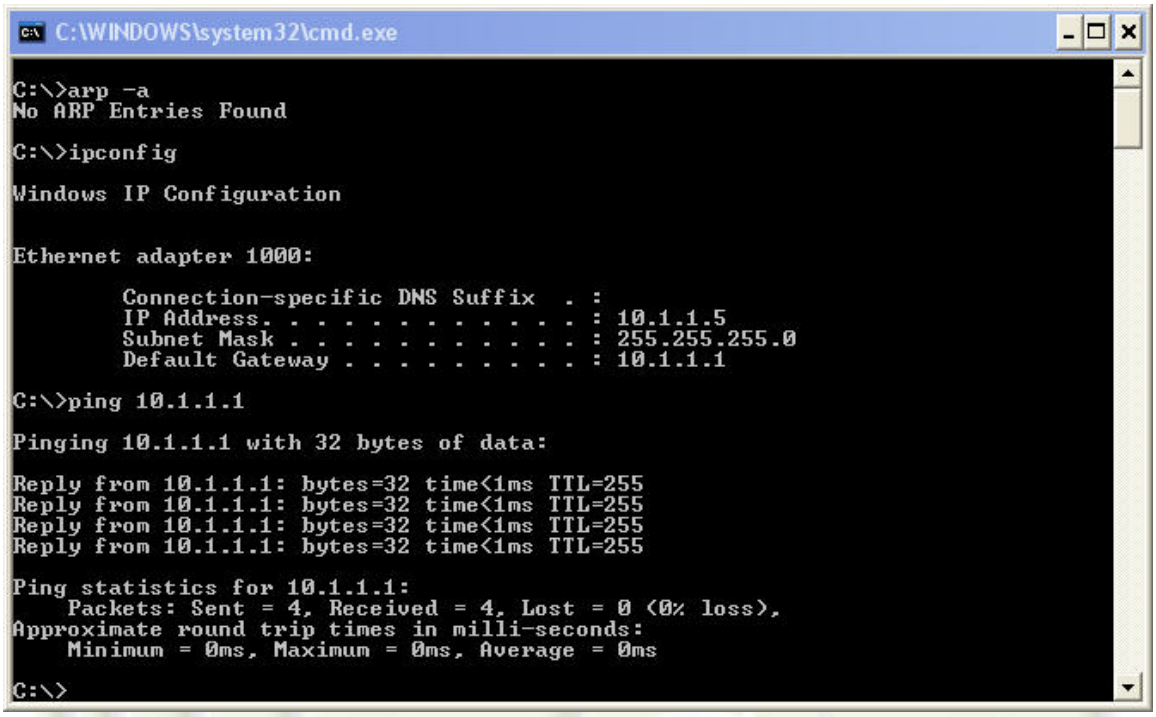
Open a command prompt from the START, Run, cmd and click OK. At the C:\> prompt type ‘arp /?’ and press enter.

The following will show you all the command line interface options for arp.exe



Step 2: ARP –a

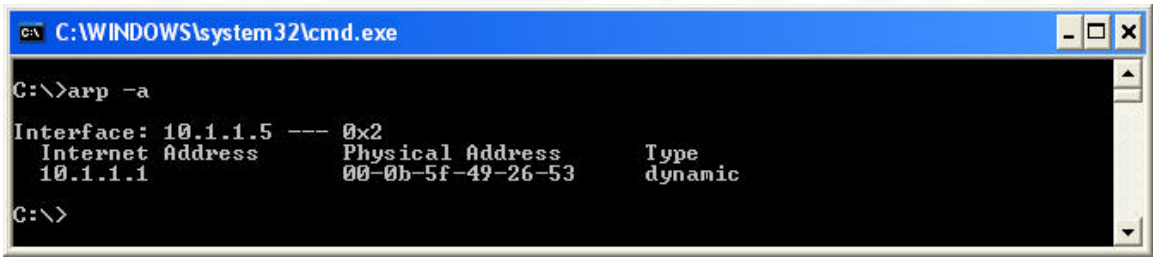
At the command prompt, type ‘arp –a’ to display your current ARP cache



You may not have any entries in your arp cache, as above. At the prompt type 'ipconfig' to check your IP configuration.

Next, ping your Default Gateway as above,
'ping x.x.x.x' where x.x.x.x is the IP address of your gateway, and press enter.

If the ping was successful, the computer has used ARP to find the hardware address of the IP address you pinged, and you can now recheck you ARP cache for the entry as below.



Print this screen off, and save to a Word Document. You will add to this document in a later step.

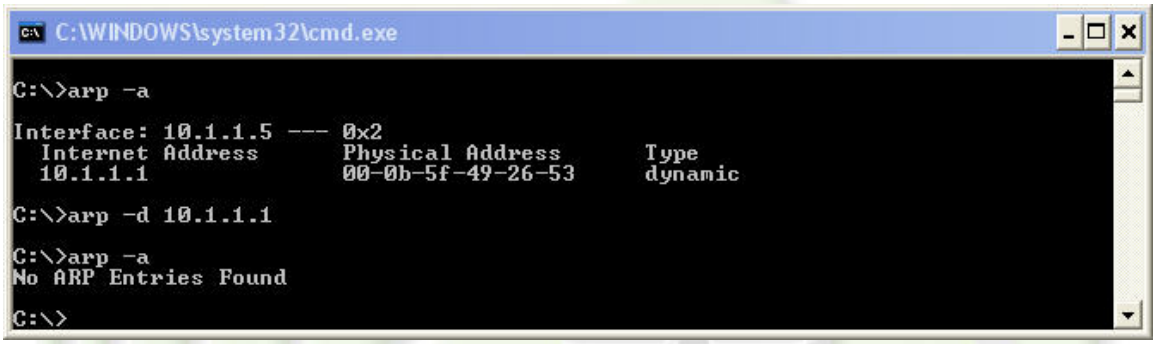
Step 3: arp –d

You can delete entries in the cache by waiting for the cache to expire, or by using arp –d.

Check your arp cache with the arp –a command to verify atleast one entry.

Delete the arp entry by typing ‘arp –d x.x.x.x where x.x.x.x is the IP address for the arp entry you wish to delete.

Check you ARP cache again by issuing the arp –a command, verify that the entry was in fact deleted from the cache.



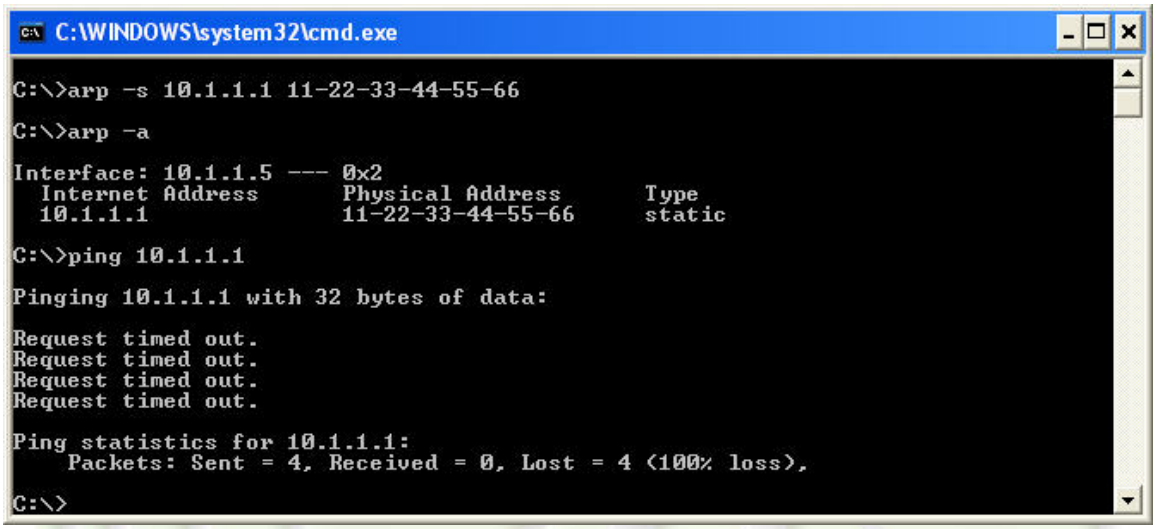
Step 4: arp –s

You can also add static entries to the arp cache manually with the arp –s command. From the command prompt issue the following command to add a static arp entry…

‘arp –s X.X.X.X 11-22-33-44-55-66’ where X.X.X.X is the IP address of your default gateway.

Verify the entry with the arp –a command. Once you have verified the manually added 11-22-33-44-55-66 MAC address for the IP of your default gateway, send a test ping to your default gateway ‘ping X.X.X.X’

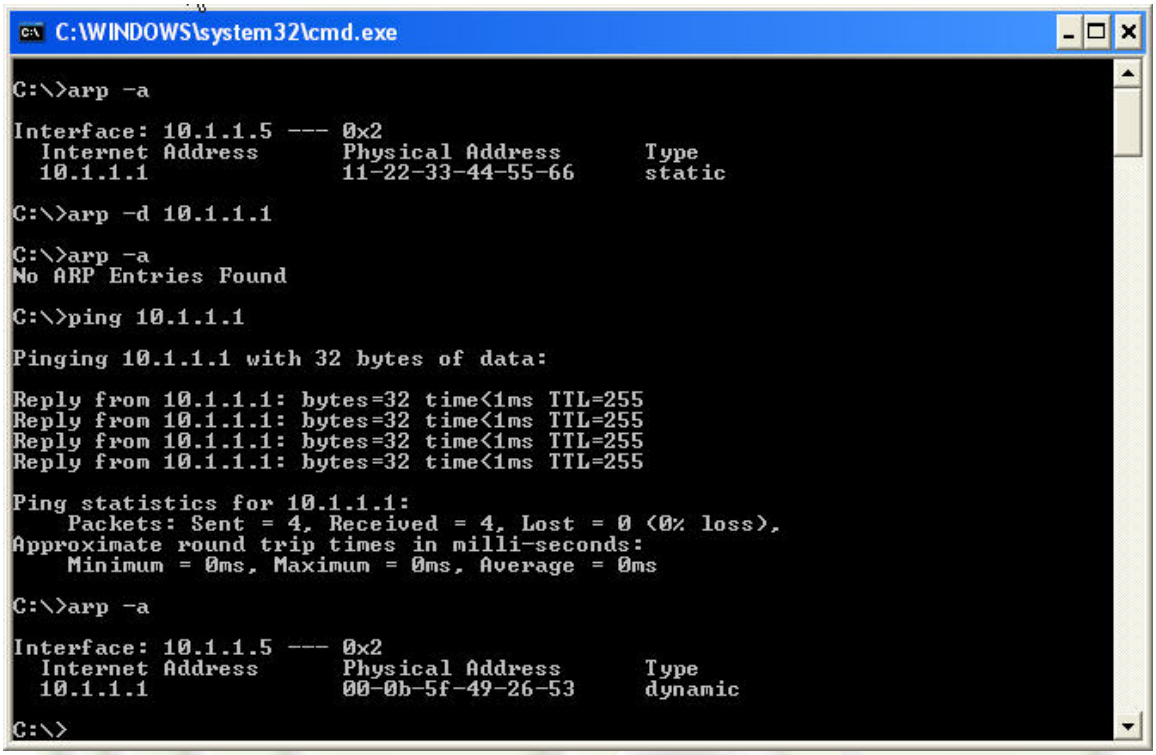
Since the hardware address for the IP is now incorrect, the ping will fail, the Ethernet Frame is being generated with the wrong MAC address for the destination, and your default gateway is disregarding the frame.



Print this screen off, save to your same Word Document and print off for your instructor. Make sure you put your name within the document.

As below, delete the entry for the 11-22-33-44-55-66 MAC address, and verify the arp cache with the arp –a command. The entry should be gone now, ping your default gateway again.

This time, with no entries in the cache, arp will lookup the correct hardware address instead of using the wrong one you manually entered, and the ping will be successful. Check your arp cache again for the correct Physical Address of the default gateway.



Analysis:

1) How/why could ARP be a security threat/issue?
2) Some companies document every MAC address within their network. Why would they do this?
3) Why is it important that you should understand how arp works in an TCP/IP network?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Research the Address Resolution Protocol RFC online at http://www.faqs.org/rfcs/rfc826.html

Appendix:

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).