**CS3506 Lab 2: Worksheet**

**Part 1: ICMP and Ping**

1. What is the IP address of the source host? What is the IP address of the destination host (UCC web server)? Confirm that the destination address is for the UCC webserver by running the command line network utility nslookup, i.e “nslookup [www.ucc.ie](http://www.ucc.ie)”.

The source IP address is likely a local address assigned to your machine. If it starts with 192.168, it indicates a private IP range used in local networks. The destination IP address shown in the ping output is 143.239.20.1, which is the IP address of www.ucc.ie.

1. What is the significance to the fact the source has an address starting with 192.168? Check out this IETF document on Address Allocation for Private Internets: <https://datatracker.ietf.org/doc/html/rfc1918>

Can you conclude anything about the subnet of the source relative to that of the UCC subnet?

An IP address starting with 192.168 indicates that the source is part of a private IP range as defined by RFC 1918. This means that the source is behind a router or firewall and is likely using Network Address Translation (NAT) to connect to external networks.

The UCC server's IP address (143.239.20.1) is a public IP, which means it is accessible over the internet. The private IP range used by the source is different from the public IP subnet of UCC, indicating that the source is on a local network separate from the UCC subnet.

1. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP (Internet Control Message Protocol) operates at the network layer (Layer 3 of the OSI model), whereas ports are associated with transport layer protocols like TCP and UDP (Layer 4). Since ICMP is used for network diagnostics and not for data transport like TCP/UDP, it does not require port numbers. Instead, it uses types and codes to indicate different functions (e.g., echo request, echo reply).

1. Referring to one of the ICMP requests and matching replies, how does the source know if a request or reply has been lost?

When a ping request is sent, the source expects to receive a corresponding reply for each request. If a reply is not received within a certain timeout period, the source concludes that the packet was lost. The ping output will show the statistics for transmitted and received packets, allowing you to identify any packet loss. Additionally, sequence numbers in ICMP packets help match requests to their corresponding replies, making it easier to detect missing responses.

**Part 2: ARP and Ethernet**

1. What is the IP address of the host sending the ping?

143.239.72.118

You can determine the IP address of the host sending the ping by examining the ARP requests in the packet capture (e.g., using Wireshark). Look for the "Who has [destination IP]? Tell [source IP]" format in the ARP request, where the source IP is the IP address of the host sending the ping

1. What is the message number of the ARP request for csfiler? How many bytes are the MAC addresses in the Ethernet frame containing the ARP request message?

73 - The Ethernet frame containing the ARP request will have two MAC addresses: the source MAC address (VMware\_f5:de:ba) and the broadcast destination MAC address (ff:ff:ff:ff:ff:ff for ARP requests).

MAC addresses in Ethernet frames are 6 bytes (48 bits) each, so the total number of bytes for the source and destination MAC addresses in the Ethernet frame would be 12 bytes (6 bytes each).

1. Why does the ARP request have a broadcast destination MAC address while the ARP reply has a unicast destination?

An ARP request is sent as a broadcast because the sender does not know the MAC address of the destination IP and needs all devices on the network to receive the request to identify the owner of the IP address. The ARP reply, however, is sent as a unicast directly to the requesting host, since the sender of the ARP reply knows the MAC address of the host that made the request.

1. What the switch will do when receiving ARP request packet? What would a router do if it received an ARP?

A switch will broadcast the ARP request to all ports except the one it received it from, because switches operate at Layer 2 (Data Link Layer) and forward broadcast frames to all devices in the same local network.

A router will not forward the ARP broadcast to other networks. Routers operate at Layer 3 (Network Layer) and do not forward broadcasts between different network segments.

1. Why are there so many ARP requests in the trace and only the single ARP reply?

When the ARP cache is cleared, the host does not know the MAC address of the target (csfiler). As a result, it will issue an ARP request to resolve the MAC address for the target IP.

After the initial ARP request, the target will respond with an ARP reply, which associates its MAC address with the IP address.

Once the ARP reply is received, the host caches this information, and further ARP requests are unnecessary for subsequent packets during this session, which explains why there’s only one ARP reply.

1. You will notice quite a few MDNS protocol messages in the trace. What does MDNS do?

MDNS (Multicast DNS) is used for name resolution in local networks without needing a central DNS server. It enables devices to discover each other and resolve hostnames to IP addresses using multicast queries. It's commonly used in home or small office networks, especially with devices like printers or smart devices.

1. Notice also some HSRP messages; these are for Cisco’s Hot Standby Router Protocol. What does this protocol do? What is the Virtual address that it advertises for the first-hop router? Why does the message include an MD5 authentication field? What are the actual IP addresses of the two routers?

What does HSRP do?

* HSRP (Hot Standby Router Protocol) provides redundancy for IP networks by allowing multiple routers to work together as a single virtual router. This ensures that if the primary router fails, a backup router can take over without disrupting the network. HSRP helps maintain network availability and continuous access to resources.

What is the Virtual address that it advertises for the first-hop router?

* In the screenshot, the HSRP messages are sent to the multicast address 224.0.0.2, which is used for HSRP communication. The actual virtual IP address that HSRP advertises would be configured on the routers, but this is not shown directly in the capture. Typically, the virtual IP is a shared address that hosts on the network use as their default gateway.

Why does the message include an MD5 authentication field?

* MD5 authentication is used to secure the HSRP communication between routers. It helps ensure that the HSRP messages are coming from a legitimate source and have not been tampered with. This prevents unauthorized devices from sending false HSRP messages that could disrupt the network's routing.

What are the actual IP addresses of the two routers?

* The IP addresses shown are 143.239.75.253 and 143.239.75.252. These represent two routers participating in the HSRP group, with one in the "Active" state and the other in the "Standby" state.

1. If you want to ping a device outside your network (e.g., www.google.com) and your ARP table is empty (e.g., machine has just started your device), what would be the first ARP message sent from your machine asking for? How does it make this decision?

The first ARP message would be asking for the MAC address of the default gateway (router). This is because the device needs to send packets to the gateway to reach external networks. The gateway is responsible for forwarding traffic from the local network to destinations outside the network. If the gateway's MAC address is not in the ARP table, the device will send an ARP request to find it.

1. What is the 48-bit Ethernet address of your computer (either your own computer or the lab PC)? Use *ifconfig* command in Linux/UNIX or *ipconfig /all* in windows to know information about your machine interfaces. On Linux the default interface name for Ethernet is usually *eth0* and for WiFi is *wlan0.* On a Mac the default Ethernet/WiFi is usually *en0*.

00:24:81:c7:d6:14

If you see two interfaces showing up as enp0s0 types, it likely means you have two different network interfaces (possibly one for Ethernet and one for another connection type, like a secondary network card). Here’s how to determine which one to use:

1. Check for an IP Address:
   * If only one of the interfaces has an IP address assigned (under the inet field), that is the active interface.
2. Look for the Connection Status:
   * You can check if the interface is up and running. The line will include UP,BROADCAST,RUNNING if the interface is active.
3. Determine by Connection Type:
   * If you’re using a wired Ethernet connection, the active interface will likely be the primary enp0s0.
   * If one is connected to a specific network (e.g., a virtual machine network or a secondary wired connection), you might see different IPs or subnet configurations.
4. Go to http://www.macvendorlookup.com and look up the manufacturer of your computer’s Ethernet interface and write it down.

MAC Address Details

**Company**

Hewlett Packard

**Address**

20555 State Highway 249  
Houston TX 77070  
US

**Range**

00:24:81:00:00:00 - 00:24:81:FF:FF:FF

**Type/Database**

MA-L | MAC Address Block Large | OUI

1. How many Ethernet addresses can a company create when owning a single OUI?

An OUI (Organizationally Unique Identifier) is the first 24 bits (3 bytes) of a MAC address, which are assigned to a company. The remaining 24 bits of the MAC address can be used by the company to create unique addresses.

Since 24 bits are available for the company to assign, the total number of Ethernet addresses that can be created with a single OUI is:

224=16,777,2162^{24} = 16,777,216224=16,777,216

Therefore, a company can create 16,777,216 unique Ethernet addresses using a single OUI.