Operating Systems and Networks
Assignment 8

1 ARP: Hands-on

In this exercise you will use Wireshark to examine the ARP protocol in more detail. You will ping the IP address 8.8.8.8 and analyze the exchanged messages.

(1) MAC addresses are stored in an ARP cache to avoid successive ARP requests. In order to ensure that ARP messages will be exchanged, you have to clear the ARP cache. Use the man page of the `arp` command to find out how to delete ARP cache entries. Verify that the table is empty using e.g., `arp -nv` on Linux. What is the approximate lifetime of an ARP cache entry?

(2) Open Wireshark and start capturing incoming and outgoing traffic. Use the `ping` command to send ICMP echo requests to the IP address 8.8.8.8. Locate the ARP messages exchanged (you can use appropriate display filters) and note the Ethernet and IP source and destination addresses. To which entities do these addresses belong and why? **Hint:** Use the command `ip route show` on the Linux command line to check the local routing table. After running ping, check the ARP table entries with the `arp` command. Use the results to help explain you answer.

2 Traceroute: Hands-on

(1) Use the traceroute utility (tracert on Windows) to trace the route from your system to the following universities in other countries. For each traceroute output, find the transoceanic link(s) noting the 2 endpoints' (of the longest hop) IP addresses and the delay between them.

  a) www.mit.edu (Boston, USA)

  b) www.ubc.ca (Vancouver, Canada)

  c) www.u-tokyo.ac.jp (Tokyo, Japan)

  d) ucl.ac.uk (London, UK)

3 ICMP

ICMP is usually listed as a layer 3 (network layer) protocol. As data gets sent to lower layers, each underlying layer adds its own header. Note, however, that ICMP messages use an IP (another layer 3 protocol) header to encapsulate their data. Could ICMP be better classified as a layer 4 (transport) protocol? Justify your answer. Hint: the beginning of RFC 792 (`https://tools.ietf.org/html/rfc792`) may provide clues.

4 NAT and Private Address Space

RFC 1918 "Address Allocation for Private Internets" (`https://tools.ietf.org/html/rfc1918`) specifies 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as private addresses suitable for unrestricted private internal use. Many home networks use the 192.168.1.0/24 address space and use NAT to a single public address.

(1) Could 172.28.2.35/24 be used as the address space for an internal network? Explain your answer.

(2) Could 10.255.255.0/24 be used as the address space for an internal network? Explain your answer.

(3) Assume a technically illiterate user configures 8.8.8.0/24 as the internal address space on his/her home router. Assume that NAT is used at the router, and there is a public interface on that router with IP address 19.33.93.140. Briefly explain what happens if a user at a system with IP 8.8.8.2 attempts to establish a network connection with a system on the Internet at IP address 8.8.8.8 (Google public DNS). Can the two systems communicate? Why? Why not?

5 Longest Prefix Match 1

The following is a forwarding table at router R. Suppose packets with the following destination IP addresses arrive at router R. Determine the next hop. Give only one answer for each destination, using longest prefix matching.

Destination Network	Next Hop
139.179.200.0/23	R1
139.179.128.0/18	R2
139.179.120.0/20	R3
139.179.220.0/21	R4
139.179.0.0/16	R5

(a) 139.179.60.10   (b) 139.179.226.40   (c) 139.179.124.55   (d) 139.179.220.180

6 Longest Prefix Match 2

Without using longest prefix matching, a forwarding table looks like the one below on the left. If we use longest prefix matching, we can combine a few entries. Fill in the reduced table on the right.

Prefix	Outgoing Interface
128.128.0.0/9	eth0
128.160.0.0/11	eth1
128.176.0.0/12	eth0
128.192.0.0/10	eth0
default	eth2

Prefix	Outgoing Interface
default	eth2