Computer Networking (COMP2322)
Class Project Part Two

Rocky K. C. Chang

Please answer the two questions below for the second part of the project. The first question is written. The second question is based on the actual experimentation. Please assemble the IP network in Figure 2 and answer those questions with evidence from Wireshark captures. You may set up a Linux machine for the router.

1) (On paper) Consider an IP network in Figure 1 in which two IP subnets (subnets 1 and 2) have been configured. In each host's routing table, there are two main routing entries: one to its own subnet and the other one to its default router. $H1$ uses `123.123.2.10` for its default route, whereas $H2$ uses `123.123.1.10` for its default route.

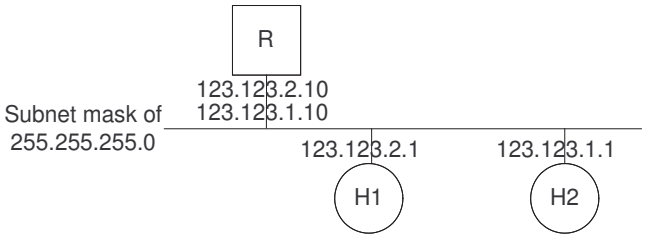


Fig. 1. A network of two IP hosts and two IP routers.

   a) If $H1$ sends an IP packet to $H2$, how is the packet forwarded to the destination?
   b) If $H1$ sends an IP broadcast packet to its own IP subnet using `123.123.2.255`, will the packet be received by the IP layer of $H2$? Explain your answer.
   c) In (a), is there an ICMP redirect message sent out by a router? Explain your answer.

2) (On experiments) To verify the answers to question 2 of assignment 2, we configured the hosts $H1$ (`Ibm_b3:f0:cf`) and $H2$ (`Ibm_16:8b:06`) with different subnet addresses, and the hosts communicated with each other through router R (`Tp-LinkT_c9:41:05`), as depicted in Figure 2. Their configurations and forwarding tables were:

   - R (`eth1.0`): `123.123.1.10`; (`eth1.1`): `123.123.2.10`; MAC Addr: `00:21:27:C9:41:05`
   - $H1$ (`eth0`): `123.123.2.1/24`; gateway `123.123.2.10`; MAC Addr: `00:11:25:B3:F0:CF`
   - $H2$ (`eth0`): `123.123.1.1/24`; gateway `123.123.1.10`; MAC Addr: `00:11:25:16:8B:06`.

$H1$'s routing table:

Destination	Gateway	Net mask	Interface
`123.123.2.0`	`123.123.2.1`	`255.255.255.0`	`eth0`
`0.0.0.0`	`123.123.2.10`	`0.0.0.0`	`eth0`

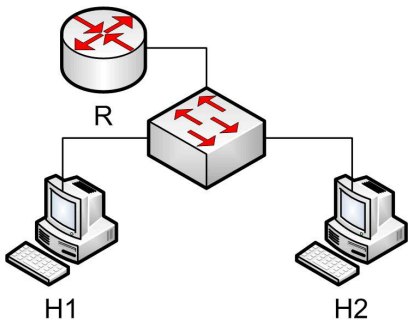


Fig. 2. Router R connected to hosts $H1$ and $H2$ through a switch.

$H2$'s routing table:

Destination	Gateway	Net mask	Interface
`123.123.1.0`	`123.123.1.1`	`255.255.255.0`	`eth0`
`0.0.0.0`	`123.123.1.10`	`0.0.0.0`	`eth0`

R's routing table:

Destination	Gateway	Net mask	Interface
`123.123.2.0`	`123.123.2.10`	`255.255.255.0`	`eth1`
`123.123.1.0`	`123.123.1.10`	`255.255.255.0`	`eth1`

Moreover, their ARP caches were initially empty. Then $H1$ sent ping requests (ICMP echo requests) to $H2$. The following list records what actually happened.

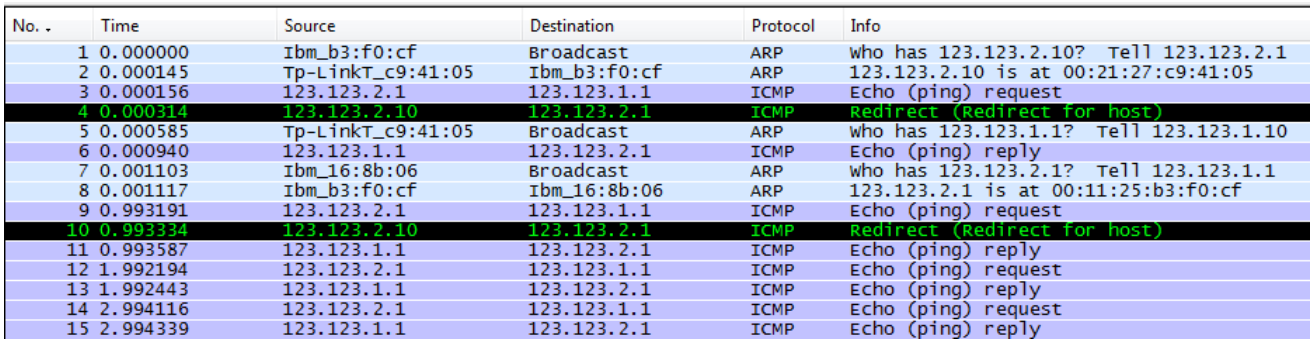
- $H1$ broadcasted an ARP request for the MAC addr of `123.123.2.10`.
- R replied the ARP request with its MAC addr (`00:21:27:C9:41:05`).
- $H1$ sent out a ping request to $H2$ (`123.123.1.1`).
- R received the ping request, sent an ICMP Redirect message to $H1$, and forwarded the ping request to $H2$.
- $H2$ replied the ping request by sending an ICMP echo reply to R. Similar to before, R sent an ICMP Redirect message to $H2$.
- $H2$ broadcasted an ARP request for the MAC address of `123.123.2.1`, and $H1$ replied.
- $H1$ sent a second ping request to $H2$ via R, and ICMP Redirect messages were again issued by R to $H1$ and $H2$.
- Starting from the third ping request and on, $H1$ and $H2$ were able to exchange ping requests and replies directly, without going through R.

Figure 3 shows the Wireshark capture at $H1$ with the promiscuous mode off (i.e., captures only packets destined to $H1$ and sent by $H1$). Note that since this trace was captured at $H1$, it does not contain the communication between R and $H2$.

Given the information above, answer the questions below with succinct explanation.

a) What is the destination MAC address in the frame of packet 3 in the Wireshark trace?

b) What is the value in the "Gateway address" field in the ICMP Redirect message (i.e., packets 4 and



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Ibm_b3:f0:cf	Broadcast	ARP	Who has 123.123.2.10? Tell 123.123.2.1
2	0.000145	Tp-LinkT_c9:41:05	Ibm_b3:f0:cf	ARP	123.123.2.10 is at 00:21:27:c9:41:05
3	0.000156	123.123.2.1	123.123.1.1	ICMP	Echo (ping) request
4	0.000314	123.123.2.10	123.123.2.1	ICMP	Redirect (Redirect for host)
5	0.000585	Tp-LinkT_c9:41:05	Broadcast	ARP	Who has 123.123.1.1? Tell 123.123.1.10
6	0.000940	123.123.1.1	123.123.2.1	ICMP	Echo (ping) reply
7	0.001103	Ibm_16:8b:06	Broadcast	ARP	Who has 123.123.2.1? Tell 123.123.1.1
8	0.001117	Ibm_b3:f0:cf	Ibm_16:8b:06	ARP	123.123.2.1 is at 00:11:25:b3:f0:cf
9	0.993191	123.123.2.1	123.123.1.1	ICMP	Echo (ping) request
10	0.993334	123.123.2.10	123.123.2.1	ICMP	Redirect (Redirect for host)
11	0.993587	123.123.1.1	123.123.2.1	ICMP	Echo (ping) reply
12	1.992194	123.123.2.1	123.123.1.1	ICMP	Echo (ping) request
13	1.992443	123.123.1.1	123.123.2.1	ICMP	Echo (ping) reply
14	2.994116	123.123.2.1	123.123.1.1	ICMP	Echo (ping) request
15	2.994339	123.123.1.1	123.123.2.1	ICMP	Echo (ping) reply

Fig. 3. A partial Wireshark capture of the packets when $H1$ pings $H2$ at $H1$ with the promiscuous mode off.

10 in the Wireshark trace)?

c) How many ICMP header(s) is (are) included in the IP packet that carries the ICMP Redirect message?

d) The Wireshark at $H1$ could capture R's ARP requests for $H2$'s MAC address but not the ARP reply. What is the reason for that?

e) $H1$ could send ping requests directly to $H2$ without first sending out an ARP request for $H2$'s MAC address. What is the reason for that?

f) If we examine the Wireshark trace captured at R with the promiscuous mode off, which packets in Figure 3 that will *not* show up in the trace?

g) If we examine the Wireshark trace captured at $H2$ with the promiscuous mode off, which packets in Figure 3 that will *not* show up in the trace?

h) Are the ICMP headers of packets 3 and 12 in Figure 3 identical?

i) If the router's two interfaces `eth1.0` and `eth1.1` are now configured with two separate physical interfaces each of which is connected directly to a host, will R still send the ICMP Redirect messages? Note that the routing tables remain the same.