

# Wireshark NAT lab quiz (optional) [Limited to 3 Attempts] Results for Vandit Jyotindra Gajjar

❗ Correct answers will be available May 8 at 17:30 - Jun 19 at 17:00.

Score for this attempt: **14** out of 14

Submitted May 6 at 14:51

This attempt took 17 minutes.

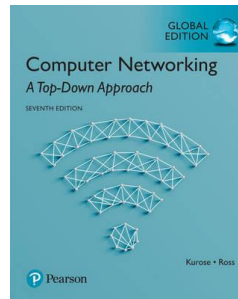
## Question 1

1 / 1 pts

Wireshark Lab: NAT v7.0

Adapted from Supplement to  
*Computer Networking: A Top-Down  
Approach*, 7<sup>th</sup> ed., J.F. Kurose and  
K.W. Ross

*"Tell me and I forget. Show me and I  
remember. Involve me and I  
understand."* Chinese proverb



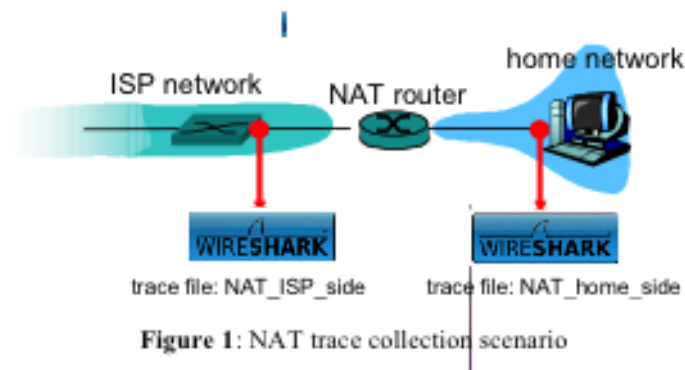
© 2005-2012, J.F Kurose and K.W.  
Ross, All Rights Reserved

In this lab, we'll investigate the behavior of the NAT protocol. This lab will be different from our other

Wireshark labs, where we've captured a trace file at a single Wireshark measurement point. Because we're interested in capturing packets at both the input and output sides of the NAT device, we'll need to capture packets at *two* locations. Also, because many students don't have easy access to a NAT device or to two computers on which to take Wireshark measurements, this isn't a lab that is easily done "live" by a student. Therefore in this lab, you will use Wireshark trace files that we've captured for you. Before beginning this lab, you'll probably want to review the material on NAT section 4.3.4 in the text[1]. The basic idea behind NAT is that you can re-use [private IP addresses](https://en.wikipedia.org/wiki/Private_network#Private_IPv4_address_spaces)

([https://en.wikipedia.org/wiki/Private\\_network#Private\\_IPv4\\_address\\_spaces](https://en.wikipedia.org/wiki/Private_network#Private_IPv4_address_spaces)) behind the NAT router and these addresses will never be sent out onto the network, but are instead 'translated' by the NAT router to use a public IP address. Several private addresses can be mapped to a single public address and are differentiated by port number. The NAT router builds a table that allows the packets to be translated from their external to their internal addresses. NAT replaces private address/port with the public address/port as packets are sent onto the Internet and when responses are received, NAT looks up the address and port in the table and replaces the public address/port with the private address/port.

### 1. NAT Measurement Scenario



In this lab, we'll capture packets from a simple web request from a client PC in a home network to a [www.google.com](https://www.google.com) server. Within the home network, the home network router provides a NAT service, as discussed in Chapter 4. Figure 1 shows our Wireshark trace-collection scenario. As in our other Wireshark labs, we collect a Wireshark trace on the client PC in our home network. This file is called NAT\_home\_side[2]. Because we are also interested in the packets being sent by the NAT router into


the ISP, we'll collect a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in Figure 1. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT\_ISP\_side.

Open the NAT\_home\_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file.

Looking at the NAT\_Home\_Side trace, what is the IP address of the client in the HTTP GET request?

---

[1] References to figures and sections are for the 7<sup>th</sup> edition of our text, *Computer Networks, A Top-down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.

[2] Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>  (<http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>) and extract the files need for this lab.

192.168.1.100

Correct.

## Question 2

1 / 1 pts

Is this address a public or private IP address?

☐ public☒ private**Question 3****4 / 4 pts**

In the HTTP GET at time 7.109267. The source IP address of this request is  . The destination IP addresses is  . The TCP source port is  and the destination port is

**Answer 1:****Answer 2:****Answer 3:****Answer 4:**

**Question 4**

1 / 1 pts

At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267?

**Question 5**

1 / 1 pts

The IP source and destination and ports in the SYN packet are the same as those in the HTTP GET?

☒ True☐ False**Question 6**

1 / 1 pts

In the following we'll focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (NAT\_ISP\_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

Open the NAT\_ISP\_side. *Note that the time stamps in this file and in NAT\_home\_side are not synchronized since the packet captures at the two locations shown in Figure 1 were not started simultaneously.* (Indeed, you should discover that the timestamps of a packet captured at the ISP link is actually less than the timestamp of the packet captured at the client PC).

Comparing the NAT\_Home\_Side and the NAT\_ISP\_Side of the HTTP GET request, which of the fields are **different**, after the packet has passed through the NAT router?

---

☒ TTL (time to live)

---

☐ version

---

☐ header length

---

☐ flags

---

☐ destination port number

---

☒ source IP address

---

☐ destination IP address

---

☐ source port number

☒ checksum

### Question 7

1 / 1 pts

The source address in the HTTP GET request sent from the NAT router is (choose all that apply):

- ☒ a public (routable) IP address
- ☐ a private (non routable) IP address
- ☐ a class B address
- ☒ a class A address
- ☐ a class C or CIDR address

### Question 8

4 / 4 pts

Using your answers to this lab, fill in the NAT translation table entries for HTTP connection studied in the lab.

## NAT translation table

LAN side		WAN side	
IP:	192.168.1.100	:PORT:	IP: 71.192.34.104 :PORT:
	4335		4335

---

**Answer 1:**192.168.1.100

---

**Answer 2:**4335

---

**Answer 3:**71.192.34.104

---

**Answer 4:**

4335

Quiz Score: **14** out of 14