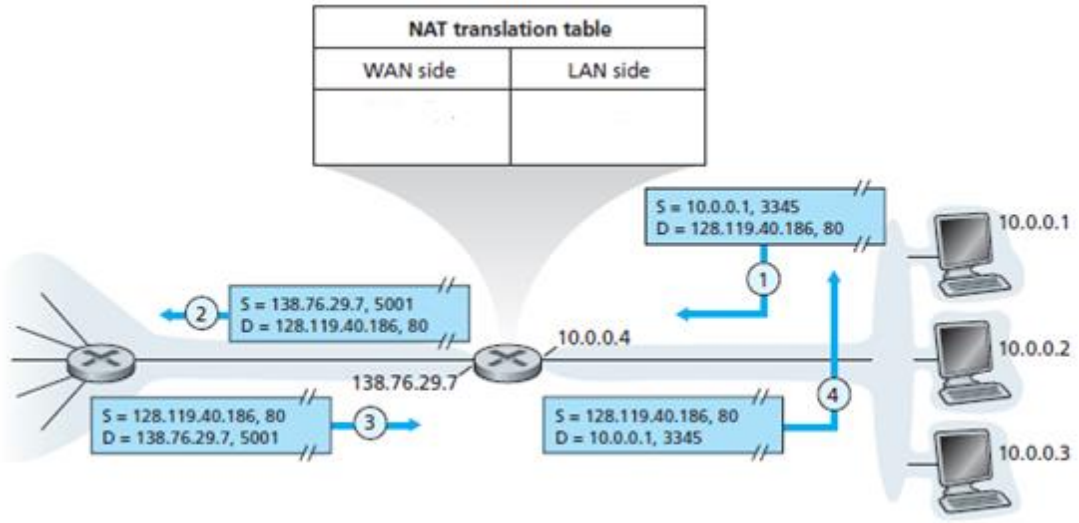
106 博士班資格考
科目：資訊網路
時間：4 小時 (Closed book)

共 10 題，每題 10 分

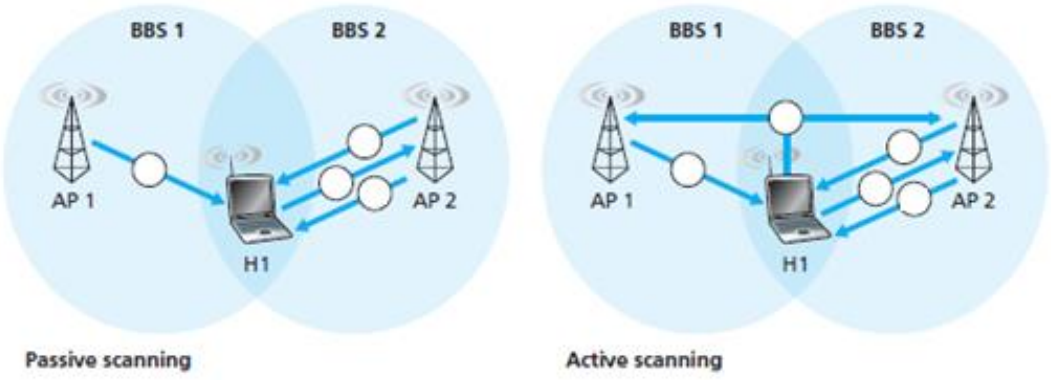
1. 填入下表各種應用(application)之Application-Layer Protocol與Underlying Transport Protocol的內容。

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail		
Remote terminal access		
Web		
File transfer		
Remote file server		
Streaming multimedia		
Internet telephony		
Network management		
Routing protocol		
Name translation		

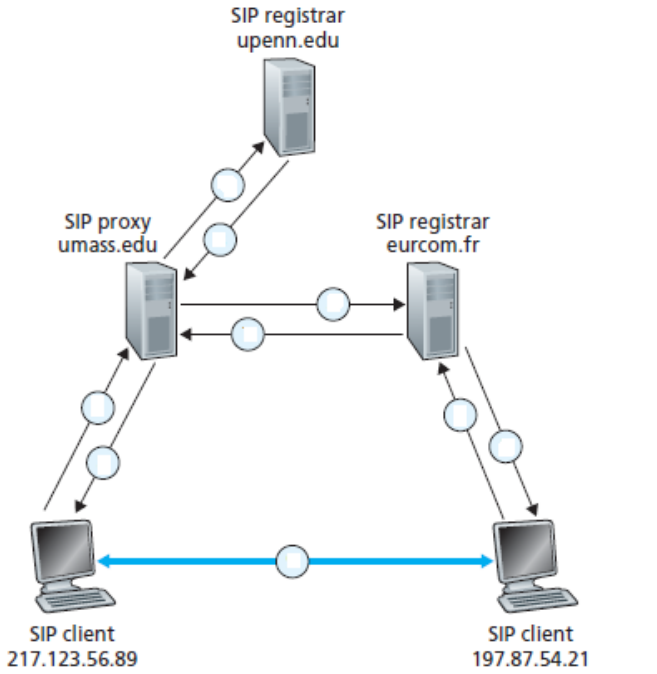
2. 填入下圖NAT translation table的內容。



3. 在下圖圈圈(○)中填入1,2,3...等號碼代表步驟順序，並說明各步驟為何?



4. 在下圖圈圈(○)中填入1,2,3...等號碼代表步驟順序，並說明各步驟為何?



Session initiation, involving SIP proxies and registrars

5. **List six access technologies. Classify each one as home access, enterprise access, or wide-area wireless access.**

6. **a) What is an important difference between a request-response message and a trap message in SNMP?**

   b) What are the seven message types used in SNMP?

7. **Install and compile the Python programs TCPClient and UDPClient on one host and TCPServer and UDPServer on another host.**
   a) Suppose you run TCPClient before you run TCPServer. What happens? Why?
   b) Suppose you run UDPClient before you run UDPServer. What happens? Why?
   c) What happens if you use different port numbers for the client and server sides?

8. a) What are the **virtual local area networks** (**VLANs**) and the 802.1Q-tagged Ethernet VLAN frame?
   b) What are the **Multiprotocol Label Switching (MPLS)** and the MPLS header: Located between link-layer and network-layer?

9. **Consider a subnet with prefix 140.125.90.0/24. Give an example of one IP address (of form xxx.xxx.xxx.xxx) that can be assigned to this network. Suppose a department owns the block of addresses of the form 140.125.83.0/24. Suppose it wants to create four subnets or eight subnets from this block, with each block having the same number of IP addresses. What are the prefixes (of form a.b.c.d/x) for the four subnets or eight subnets?**

10. **a) Using RSA, choose $p = 3$ and $q = 11$, and encode the word "dog" by encrypting each letter separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message.**
    b) Repeat part (a) but now encrypt "dog" as one message m.