- **Problem 2** (0 points)

  1. IPv4 must always check the destination addresses on incoming multicast datagrams and discard datagrams if the host is not in the specified multicast group. Explain how the host might receive a multicast destined for a group to which that host is not a member.

     Answer: When the multicast datagram is transmitted on the Ethernet, only the last 23 bits of the IPv4 multicast destination address are mapped to the Ethernet address. However, an IPv4 multicast address has 28 bits and thus multiple IPv4 multicast addresses, say G_1 and G_2, may be mapped to a same Ethernet address. Assume that a host is a member of G_1 but not a member of G_2. Then the host will receive a packet for G_2 in the Ethernet.

  2. The IGMP general query message is used to monitor the memberships in multicast groups. This message may cause a large number of membership report messages. Explain briefly the main techniques used in the IGMP implementation to minimize the overhead of traffic caused by IGMP messages.

     Answer: First, IP multicast addresses are used to deliver IGMP messages. So, a host not in a multicast group will not receive the message for that group.

     Second, in monitoring membership of groups, a multicast router sends one general query to all groups.

     Third, if multiple multicast routers are connected to a same network, only one router (called query router) monitors the membership of all groups (reducing the number of general queries).

     Fourth, multiple membership reports can be sent in one message (IGMPv3). In IGMPv3, a host sets-up a single (interface) timer for the general query from a specific network interface. Once the timer expires, the host sends one message to report the memberships of all groups it belongs to (RFC 3376).

  3. Assume that host H sends a leave report to router R, expressing H leaves multicast group G. What is the destination address in the IPv4 datagram which carries the leave report? What is the address in the address field in the IGMP leave report? Router R sends a group specific query to confirm the leave. What is the destination address in the IPv4 datagram which carries the query? What is the address in the multicast group address field in the query?

     Answer: The destination address in the IPv4 datagram carrying the leave report is the address `224.0.0.2` for the multicast group contains all routers connected to a physic network.

     The address in the address field in the IGMP leave report is the multicast address of the group the host wants to leave.

     The destination address in the IPv4 datagram carrying the query is the multicast address for the group reported in the leave report.

     The address in the multicast group address field in the query is the multicast address for the group reported in the leave report.

4. For the AS in Figure 1, assume that the routing tables for unicast computed by OSPF. Assume that G is a multicast group with members in $N_2, N_4, N_5, N_6.N_7$ and TRPF (Truncated Reverse Path Forwarding) is used by routers to deliver multicast messages. When Router R_5 receives a multicast message P with source N_2 and destination G from interface `eth0`, which interfaces R_5 forwards P to? If P receives P from `eth1`, which interfaces R_5 forwards P to?

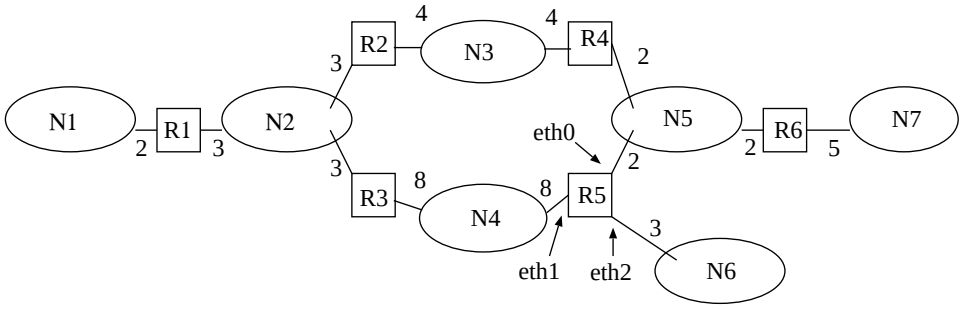

Figure 1: An autonomous system.

Answer: The packet received from `eth0` comes from a shortest path and according to RPF (reverse path forwarding) the packet should be forwarded. Further the packet should be forwarded to `eth2` based on the multicast tree connecting N_2 to N_4, N_5, N_6, N_7.

The packet received from `eth1` does not come from a shortest path and by RPF, the packet should be droped.

5. Main items in an NAT translation table include internal IP addresses, internal port numbers, external IP addresses, external port numbers, NAT port numbers, and payload type. Which items are used to identify a communication session between an NAT box and an internal host? Which items are used to identify a communication session between an external host and an NAT box? Why is the payload type included as a main item in the table?

   Answer: The internal IP address, internal port number, external IP address and external port number are used to identify a communication session between the NAT box and an internal host.

   The external IP address, external port number, the global IP address of the NAT box and the NAT port number are used to identify a communication session between the NAT box and an external host.

   The payload type is used to check if the NAT box needs to perform special works for the communication session.

6. Select an English document (plaintext) of a reasonable length and find the top 5 letters in terms of the high relative frequency in the plaintext. Create the ciphertext of the plaintext by your encryption scheme designed in Problem 1 and find the relative frequencies of the top 5 letters in the ciphertext. Compare the relative frequencies of the 5 letters in the plaintext and ciphertext.

7. DES (Data Encryption Standard) has been widely used as secret key encryption scheme for many years. However, DES has been broken and is no longer considered as very secure. What weakness do you think DES has and how would you improve the security of DES if you are asked to modify it?

   Answer: A major weakness of DES is that the key used for encryption and decryption is too short by the morden computer power. Indeed it is possible to enumerate all DES keys in a practical time with a powerful computing platform.

   One approach to improve the security of DES is use a longer key for encryption and decryption.

8. Explain briefly how public-key and secret-key encryption schemes are combined to make a more efficient encryption scheme.

   Answer: Use a secret-key scheme to encrypt/decrypt data while use a public-key encryption scheme to deliver the key used in the secret scheme.

9. Explain briefly how a public-key encryption scheme is used in digital signature.

   Answer: Assume that A sends a signed document to B. A encrypts the document by A's private key (sign the document) and sends the encrypted document to B. B decrypts the received document by A's public key (verify the sign). To reduce the computation time on the encryption and decryption processes, A can sign a digest of the document and B verifies the sign on the digest: A produces a digest D_A of the document F, encrypts D_A by A's private key, sends B the encrypted D_A and F. B decrypts the received digest to get D_A, creates a digest D_B from F, and compares D_A with D_B. If $D_A = D_B$ then the sign is verified.

10. The PGP protocols use several encryption/decryption keys. Explain the purpose of each key.

    Answer: Assume A sends a message to B via PGP. A uses A's private key to encrypt (sign) (the digest of) the message, uses a secret key K to encrypt the message and the signed (digest of) message, and uses B' public key to encrypt K.

    B uses $B's$ private key to get secret key K, uses K to decrypt the message and the signed (digest of) message, and uses A's public key to decrypt the signed (digest of) message for verifying the signature.