Computer Networks: Homework #3

Due on April 20, 2018 at 11.59pm

Prof. Raquel Hill

Akash B. Sheth

Problem 1

IP Subnetting

1. Consider a subnet with prefix 128.119.30.128/26. Give an example of one IP address (of the form xxx.xxx.xxx.xxx) that can be assigned to this network.
2. Suppose an ISP owns the block of addresses of the form 128.119.40.64/26, and the ISP want to create four 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?

Solution

Part A
We are given subnet mask of 26. Therefore, the masked bits are as follows:

11111111.11111111.11111111.11000000

Using this, we know that the network id is 128.119.30.128 and the broadcast address is 128.119.30.191. Thus, usable range of IPs is 128.119.30.129 to 128.119.30.190. We can assign any IP from the range. One such IP is 128.119.30.170.

Part B
Block of address owned by ISP: 128.119.40.64/26
We find that the range of IPs blocked by the ISP is 128.119.40.64 to 128.119.40.127.
We want to divide this block of IP addresses into 4 blocks containing same number of IP addresses. 4 is a power of 2 –> (2^2). Therefore total number of subnet mask bits will be 26+2 = 28.
Thus, 4 subnets are as given below.

1. 128.119.40.64/28, Range: 128.119.40.64 to 128.119.40.79
2. 128.119.40.80/28, Range: 128.119.40.80 to 128.119.40.95
3. 128.119.40.96/28, Range: 128.119.40.96 to 128.119.40.111
4. 128.119.40.112/28, Range: 128.119.40.112 to 128.119.40.127

Problem 2

Assume that you are interested in detecting the number of hosts behind a NAT. You observe that the IP layer stamps an identification number sequentially on each IP packet. The identification of the first IP packet generated by a host is a random number, and the identification numbers of the subsequent IP packets are sequentially assigned.

(a) Based on this observation, and assuming you can sniff all packets sent by the NAT to the outside, outline a simple technique that detects the number of unique hosts behind a NAT. Justify your answer.
(b) If the identification numbers are not sequentially assigned, but randomly assigned, would your technique work? Justify your answer.

Solution:

Part A
Assumption: We can sniff all packets sent by the NAT to the internet.
Observation: Starting IP packet by a particular host has a randomly generated identification number but subsequent packets are sequentially assigned.

Based on this observation and assumption, we can make clusters of packets and then count of the clusters will give us the unique hosts behind a NAT.

Example:
If a host starts with identification number 1300, then subsequent packets can be 1301 to 1320. Another host can start with identification number 1629, then subsequent packets can be 1630 to 1649, and so on.

Part B
Since our technique of clustering is based on the sequentially assigned packets and not on randomly assigned packets, the technique will fail for randomly assigned packets as there will be no base for clustering.

Problem 3

Routing

1. What is BGP High Jacking? Explain how a network prefix can be highjacked. If no authentication methods are used, does advertising a prefix cause a BGP peer to accept the new advertisement?
2. Explain the fundamental difference between link state and distance vector routing algorithms. Your explanation should discuss the centralized or distributed nature of the algorithm(s).

Solution

Part A

When the internet traffic is sent off course intentionally or unintentionally, it is called BGP hijacking (Prefix hijacking). It means that a group of IP addresses are compromised by corrupting the routing table maintained using the Border Gateway Protocol.
Network hijacking is carried out by configuring router to advertise prefixes which are not assigned to it.
As there is no way of authenticating the advertisement, a BGP peer will accept the new advertisement.

Part B

The fundamental difference between the link state and distance vector routing algorithm is that the link state algorithm maintains the complete view of the network including cost of all the links at all the routers and that is why it is also called centralized algorithm whereas the distance vector routing algorithm maintains the view only of its physically connected neighbours and that is why it is also called decentralized routing algorithm.

Problem 4

Suppose nodes A and B are on the same 10 Mbps broadcast channel, and the propagation delay between the two nodes in 245 bit times. Suppose A and B send Ethernet frames at the same time, the frames collide, and then A and B choose different values of K in the CSMA/CD algorithm. Assuming no other nodes are active, can the re-transmissions from A and B collide? When answering this question, suppose A and B begin transmission at t=0 bit times. They both detect collisions at t=245 bit times. Suppose K_A=0 and K_B=1. At what time does B schedule its re-transmission? At what time does A begin transmission? (Note: The nodes must wait for an idle channel after returning to Step 2 see protocol.) At what time does As signal reach B? Does B refrain from transmitting at its scheduled time?

Solution

Assumptions:

1. The jam signal is transmitted when the collision takes place for 48 bit times
2. Idle channel time = 96 bit times.

Time	Event
0	Node A and B, both start transmitting
245	Collision takes place
245 + 48 = 293	Jam signal transmission complete
245 + 293 = 538	Node B's last bit arrives at A; Now A detects an idle channel
538 + 96 = 634	A starts transmitting
293 + 512 = 805	Now B returns to Step 2 and must detect idle channel
634 + 245 = 879	Now A's last bit reaches B

Here, re-transmission from Node A and Node B do not collide because B waits to re-transmit till the time A's re-transmitted bit reaches B.