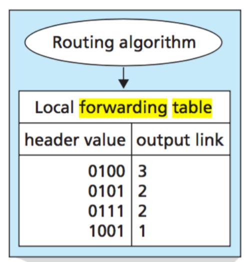
CSCI 4211 16Spring Final Exam Solution

1. When an IP packet arrives a router, how the router decides what is the next router (output link) this packet to be forwarded to? What are the routing table and forwarding table in a router? Please describe the contents of the two tables. What are the differences of the two?

   Solution:
   The router compare the prefix of the input IP address and match the longest prefix of IP address stored in the router. (2')

   Forwarding table: a smaller table generated by routing table. A forwarding table contains only the routes which are chosen by the routing algorithm as preferred routes for packet forwarding. It is often in a compressed or pre-compiled format that is optimized for hardware storage and lookup. (3')



   Routing table:
   Routing table: In computer networking a routing table, is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. (3')

step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

Difference: (2')

a. Forwarding table stores the output link of an IP address within a router, while Routing table stores the routing information of the whole network.
b. Forwarding table is usually smaller than routing table.

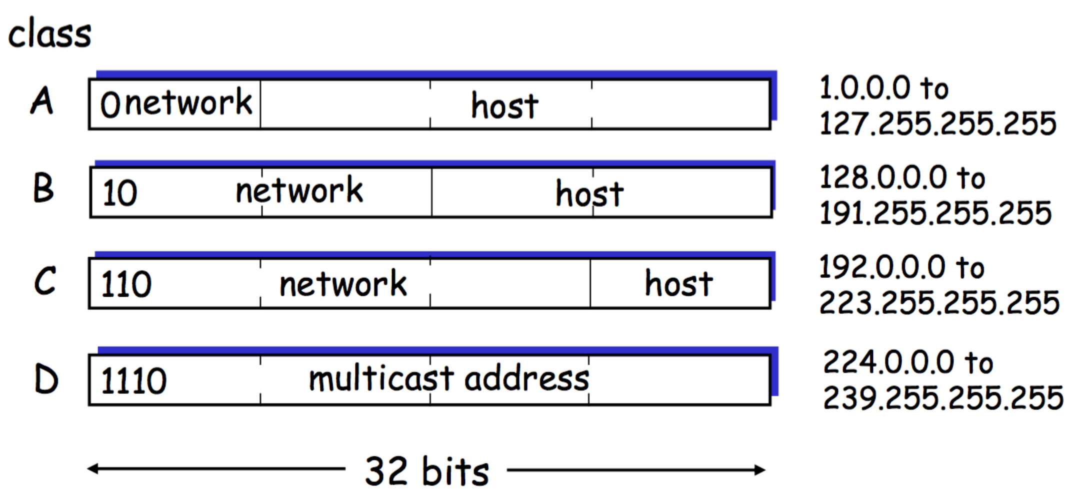
2. OSPF is used for intra-AS routing and is based on link state protocol. Can you describe three advanced features that OSPF has which are not included in the traditional link state routing protocol?

   Solution:
   OSPF (Open Shortest Path First)
   a. Security: all OSPF messages authenticated (to prevent malicious intrusion); TCP connections used
   b. Multiple same-cost paths allowed (only one path in RIP) For each link, multiple cost metrics for different TOS (eg, satellite link cost set “low” for best effort; high for real time)
   c. Integrated uni- and multicast support: Multicast OSPF (MOSPF) uses same topology data base as OSPF
   d. Hierarchical OSPF in large domains.

   Answer 3 of the 4 advantages will have full scores. Lost one will lose 3 points.

3. The original IP addresses are classified into four classes. What are they? If you receive an IP how do you tell which class this IP address belongs to?

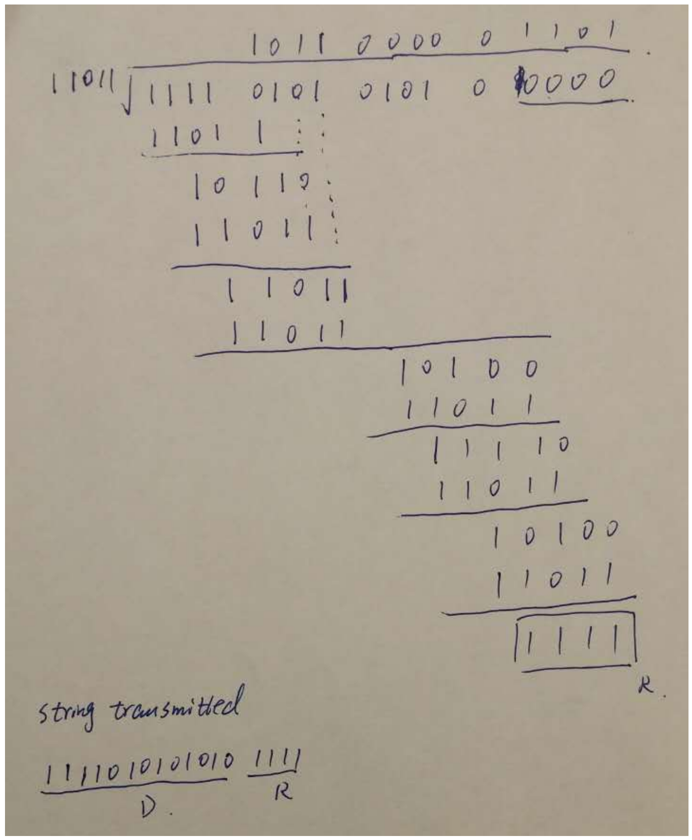
   Solution:
   a. There are 4 classes, A, B, C, and D. (2’). Class A, B, and C use 1 byte, 2bytes, and 3 bytes network address respectively. Class D is reserved for multicast.
   b. # of networks and hosts for each class
      a. A: 126 networks (2^7-2) and 16777214 hosts (2^24-2).
      b. B: 16384 (2^14) Network addresses and 65534 (2^16-2) Host addresses.
      c. C: 2097152 (2^21) Network addresses and 254 (2^8-2) Host addresses
      d. D: In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address
   c. Identify the class of an IP address by comparing the prefix. (4’) as shown in the figure.



Ref: http://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm

4. Given a generator function $g = x^4 + x^3 + x + 1$ and the following message, 1111010101010. Please figure out the bit string that to be transmitted based on CRC. Please show your process.

   Solution:



   Remainder (2'), Data transmitted (2'), Add 4 bits (2'), Process (4')

5. Ethernet is the most popular type of networks today. Please describe the Ethernet protocol in detail.

   Solution:
   Ethernet protocol uses 1-persistent CSMA/CD. (2')

   1-persistent CSMA/CD: （8'） When the transmitting node is ready to transmit, it senses the transmission medium for idle or busy. If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1). In case of a collision, the sender waits for a random period of time and attempts to transmit again unconditionally (i.e. with probability=1)

6. What are the hidden terminal and exposed terminal problems? Describe how CSMA/CA (Collision Avoidance) solves the hidden terminal and exposed terminal problems.

   Solution:
   Hidden terminal: hidden terminals: In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP (2')
   Exposed terminal: exposed node problem occurs when a node (the sender) is prevented from sending packets to other nodes because of a neighboring transmitter. However, there's no interference at the receiver side. (2')

   In order to avoid the hidden terminal problem, the IEEE 802.11 protocol allows a station to use a short **Request to Send (RTS)** control frame and a short **Clear to Send (CTS)** control frame to *reserve* access to the channel. When a sender wants to send a DATA frame, it can first send an RTS frame to the AP, indicating the total time required to transmit the DATA frame and the acknowledgment (ACK) frame. When the AP receives the RTS frame, it responds by broadcasting a CTS frame. This CTS frame serves two purposes: It gives the sender explicit permission to send and also instructs the other stations not to send for the reserved duration. (4')

   To solve the hidden terminal problem, any one receives CTS will not transmit.(1') To solve the exposed terminal problem, node that receive RTS but not CTS can still transmit.(1')

7. Consider IEEE 802.5 token ring. What is a token in 802.5? Can you describe how priority and reservation bits are used? Station X with priority 6 sees station Y with priority 5 passing by, what happen. If another station Z generate packet with priority 7 what happen after X finishes transmitting its current packet?

   Solution:
   Token: A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order. (2')

   Priority(2') & Reservation bits (2'): Only stations with a priority equal to or higher than the priority value contained in a token can seize that token. After the token is seized and changed to an information frame, only stations with a priority value higher than that of the transmitting station can reserve the token for the next pass around the network. When the next token is generated, it includes the higher priority of the reserving station. Stations that raise a token's priority level must reinstate the previous priority after their transmission is complete.

   If Station X with priority 6 sees a a data packet with priority 5 passing by, it will change the reservation bit of the data packet to be 6. When the next run starts, a token with priority 6 will generate. (4')

8. What are DIFS and SIFS in IEEE 802.11 protocol? Why and how does the protocol use them?

   Solution:
   DIFS: Distributed Inter-frame Space (2')
   SIFS: Short Inter-frame Spacing (2')

   Stations transmits ACK/DATA when medium is free for time greater than a SIFS/DIFS period. (4') SIFS is shorter than DIFS to give ACK higher priority to transmit. (2')

9. What is the design principle of BGP protocol? Describe how BGP handles the policy based routing. One example of policy-based routing is used in Internet 2. It requires both the organizations of source and destination nodes belong to Internet 2.

   Solution:
   BGP protocol is Border Gateway Protocol (1'). Design principle: Similar to Distance Vector protocol, each Border Gateway broadcast to neighbors (peers) entire path (I.e, sequence of ASs) to destination. In other word, it uses path vector not distance vector to do routing.(3')

   Inter-AS: admin wants control over how its traffic routed, who routes through its net. (3')
   Intra-AS: single admin, so no policy decisions needed. (3')

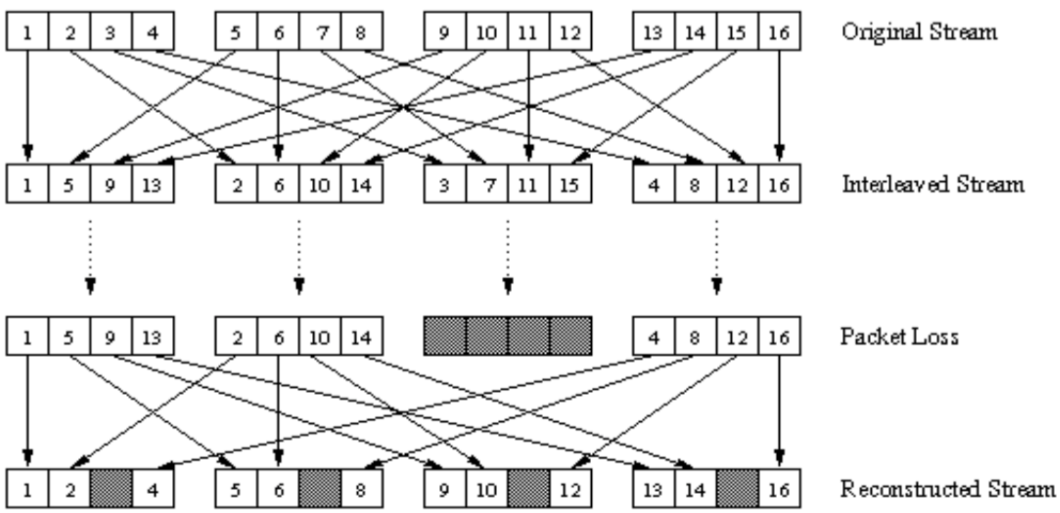
10. A CDMA receiver gets the following chips: (0, 2, -2, 2, 0, 0, -2, 0). Assume the chipping sequence defined as follows:
    A: (-1, 1, -1, -1, -1, -1, 1, -1)
    B: (-1, 1, -1, 1, 1, 1, -1, -1)
    C: (-1, -1, 1, -1, 1, 1, 1, -1)
    D: (-1, -1, -1, 1, 1, -1, 1, 1)
    Which stations are transmitting and what bit was sent b each transmitting station?

    Solution:
    Chip * A / 8 = 0 -> not transmitting (2')
    Chip * B / 8 = 1 -> transmitting 1 (2')
    Chip * C / 8 = -1 -> transmitting 0 (2')
    Chip * D / 8 = 0 -> not transmitting (2')
    Calculation process (2')

11. In voice over IP, how often a digitalized voice data is transmitted over IP network and what is the size of a packet? Since voice data is very delay sensitive, it is hard to transmit a packet if a packet is lost. Can you describe the interleaving mechanism used to remedy the loss of a packet situation?

Solution:

a. A digitalized voice data is transmitted every 20ms. (2')
b. The size of a packet is 160 Bytes. (2')
c. (6')



12. Describe Weighted Fair Queueing (WFQ) Scheme as shown below. What are the major issues that WFQ can help to solve?

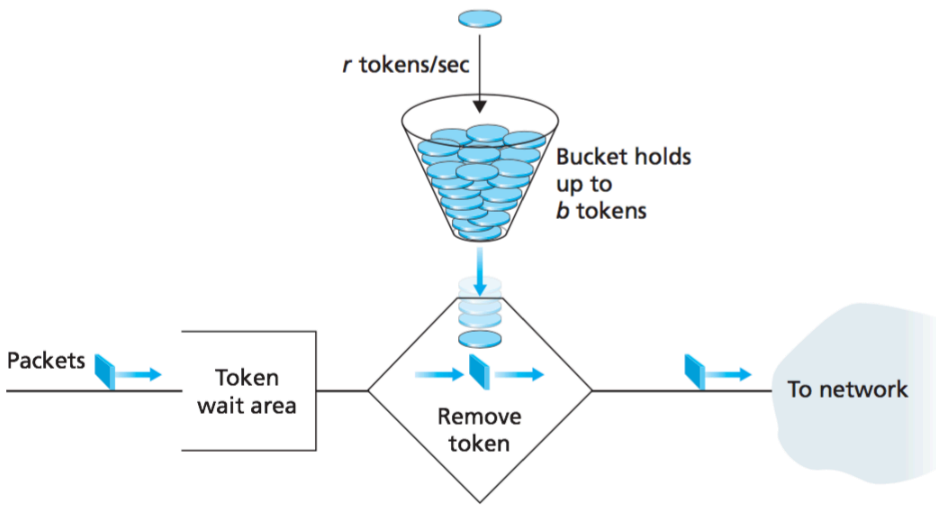
Solution:
Weighted fair queueing (WFQ) is a data packet scheduling algorithm used by network schedulers. It is a generalization of fair queue by considering the class of data packets (2').

As in round robin scheduling, a WFQ scheduler will serve classes in a circular manner—first serving class 1, then serving class 2, then serving class 3, and then (assuming there are three classes) repeating the service pattern. WFQ is also a work-conserving queuing discipline and thus will immediately move on to the next class in the service sequence when it finds an empty class queue. (4')

But Weighted Fair Queuing is a generalized Round Robin in which an attempt is made to provide a class with a differentiated amount of service over a given period of time (4')

13. What is the leaking bucket scheme? How it can be used to police packet flow?

Solution:



A leaky bucket consists of a bucket that can hold up to b tokens. (1') Tokens are added to this bucket as follows. New tokens, which may potentially be added to the bucket, are always being generated at a rate of r tokens per second. (1') (We assume here for simplicity that the unit of time is a second.) If the bucket is filled with less than b tokens when a token is generated,(1') the newly generated token is added to the bucket; (1') otherwise the newly generated token is ignored, and the token bucket remains full with b tokens. (1')

Let us now consider how the leaky bucket can be used to police a packet flow. Suppose that before a packet is transmitted into the network, it must first remove a token from the token bucket. If the token bucket is empty, the packet must wait for a token. (An alternative is for the packet to be dropped, although we will not consider that option here.) Let us now consider how this behavior polices a traffic flow. Because there can be at most b tokens in the bucket, the maximum burst size for a leaky-bucket- policed flow is b packets.(2') Furthermore, because the token generation rate is r, the maximum number of packets that can enter the network of any interval of time of length t is rt + b. (2')Thus, the token-generation rate, r, serves to limit the long-term average rate at which packets can enter the network (1')