

SIMON FRASER UNIVERSITY  
SCHOOL OF ENGINEERING SCIENCE

Spring 2013  
ENSC 427: COMMUNICATION NETWORKS

Midterm No. 1(b)  
Wednesday, February 20, 2013

*Duration: 50 minutes. Attempt all problems. Questions may not be equally weighted. Closed book and closed notes. Simple calculators (with no graphing/programming functions) are permitted. PDAs, laptops, and wireless phones are not permitted.*

**Please circle your answers.**

**1. Applications and Layered Architecture:**

Consider the OSI reference model. Application layer is the layer 7 of the OSI model. Select **all** statements that are **correct**:

- (a) Layers 2, 4, and 6 are Data Link, Transport, and Presentation layers, respectively.
- (b) Layers 2, 4, and 5 are Data Link, Session, and Presentation layers, respectively.
- (c) The main role of the Network layer is path determination and one of the roles of the Transport layer is flow control.
- (d) The main role of the Data Link layer is path determination while the main role of the Network layer is physical addressing.
- (e) Data units associated with layers layers 2, 3, and 4 are frames, packets, and segments.
- (f) Data units associated with layers 3, 4, and 5 are frames, packets, and segments, respectively.

**2. Applications and Layered Architecture:**

Select **all** statements that are **correct**:

- (a) IPSec is a Network layer protocol.
- (b) ICMP is a Network layer protocol.
- (c) DNS is an Application layer protocol.
- (d) DHCP is an Application layer protocol.

**3. Applications and Layered Architecture:**

Select **all** statements that are **correct**:

- (a) UDP is not connection-oriented.
- (b) UDP provides the best-effort datagram service.
- (c) TCP datagrams are sent immediately.
- (d) FTP uses only one TCP connection.
- (e) Netstat is a utility used to query a host about its TCP/IP network status.
- (f) Traceroute is a utility used to determine if a host is reachable.

**4. Applications and Layered Architecture:**

Select **all** statements that are **correct**:

- (a) DNS provides conversion between host names and IP addresses.
- (b) Peer-to-Peer applications are unable to connect users directly.
- (c) UDP retransmission is requested if an error is detected.
- (d) Real-time Transport protocol (RTP) runs on top of TCP.
- (e) IP packets are routed according to the host name.

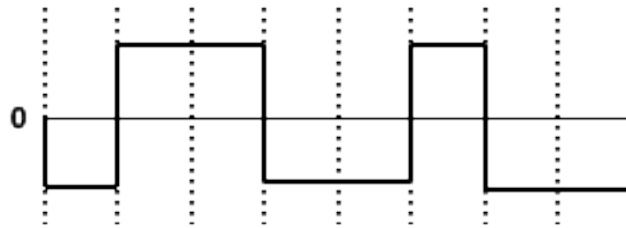
**5. Applications and Layered Architecture:**

Select **all** acronyms that are **not correctly** expanded:

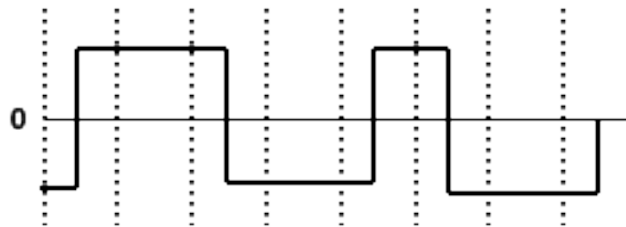
- (a) CRC: Cyclic Redundancy Check
- (b) DNS: Domain Name Server
- (c) DHCP: Dynamic Host Control Protocol
- (d) UDP: User Datagram Protocol
- (e) ICMP: Internet Control Message Protocol
- (f) HTTP: Hyper Text Transport Protocol.

6. **Digital Transmission Fundamentals:**

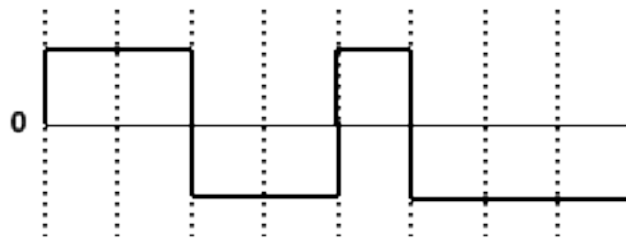
The ASCII code for the character “d” in decimal notation is 100. After converting this decimal number to binary, select the graph that shows character “d” using the Polar NRZ line coding.



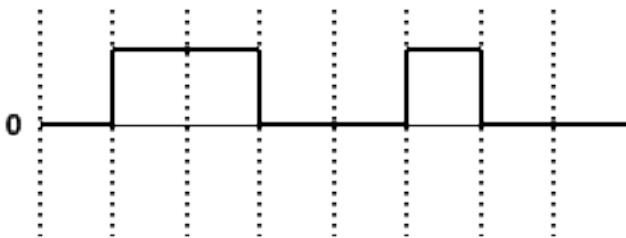
(a)



(b)



(c)

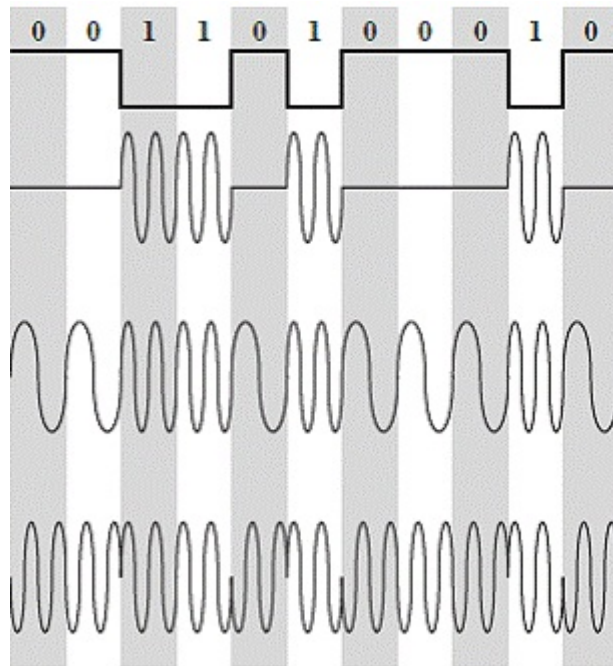


(d)

## 7. Digital Transmission Fundamentals:

Identify the three modulation techniques shown below.

- (a) Amplitude shift keying (top); Quadrature amplitude modulation (middle); Phase shift keying (bottom).
- (b) Amplitude shift keying (top); Frequency shift keying (middle); Phase shift keying (bottom).
- (c) Phase shift keying (top); Amplitude shift keying (middle); Frequency shift keying (bottom).
- (d) Quadrature amplitude modulation (top); Multi-frequency shift keying (middle); Phase shift keying (bottom).
- (e) Frequency shift keying (top); Amplitude shift keying (middle); Dual-tone multi-frequency signalling (bottom).



8. **Case Study: Distributed Denial of Service Attacks:**

Considering the four main components of a distributed denial of service attack (DDoS): real attacker, control master program, attack daemon agents, and the victim. Select **all** statements that are **correct**:

- (a) The control master program sends “execute” messages to the real attacker to notify the attacker that daemons are ready to execute attacks.
- (b) The control master program monitors the attacks and reports to the attacker.
- (c) The control master program communicates with a set of attack daemons.
- (d) The real attacker sends an attack command to the attacker daemon agent.
- (e) The attacker daemon begins the attack on the victim upon reception of an attack command.

9. **Case Study: Distributed Denial of Service (DDoS) Attacks:**

Select **all** statements that are **not correct**:

- (a) Implementation of a Class Based Queuing algorithm requires no additional effort.
- (b) Implementing queuing algorithms in network routers may protect users in case of DDoS attacks.
- (c) Random Early Detection (RED) successfully provides limited bandwidth to legitimate users during a DDoS attack.
- (d) The drawback of the Class Based Queuing algorithm is that it does not guarantee bandwidth requirements under persistent denial of service attacks.
- (e) Filtering routes, disabling IP broadcast, and performing intrusion detection are among the available methods to defend users against attacks.

10. **NS-2 Tutorial:**

Consider the ns-2 code shown in page 6. Select **all** statements that are **correct**:

- (a) The simulated network topology consists of seven nodes.
- (b) Each node is connected to two other nodes.
- (c) The packet size varies throughout the simulation based on the employed protocol.
- (d) The packet transmissions starts when the simulation time reaches 0.005 s.
- (e) User datagram protocol is employed for packet transmission.
- (f) The “*\$ns rtp proto DV*” command selects a dynamic routing model for the simulation.
- (g) There is enough information to calculate the amount of data transferred during the simulation period.
- (h) Node “0” is the traffic source while node “3” is the sink.
- (i) Traces to be used by *nam* are saved in a file called *out.nam*.
- (j) After the simulation ends, the network animator (*nam*) starts automatically and displays the network topology.

```

1 set ns [new Simulator]
2
3 $ns rtproto DV
4
5 set nf [open midterm.nam w]
6 $ns namtrace-all $nf
7
8 proc finish {} {
9     global ns nf
10    $ns flush-trace
11    close $nf
12    exit 0
13 }
14
15 for {set i 0} {$i < 7} {incr i} {
16     set n($i) [$ns node]
17 }
18
19 for {set i 0} {$i < 7} {incr i} {
20     $ns duplex-link $n($i) $n([expr ($i+1)%7]) 1Mb 10ms DropTail
21 }
22
23 set udp0 [new Agent/UDP]
24 $ns attach-agent $n(0) $udp0
25
26 set cbr0 [new Application/Traffic/CBR]
27 $cbr0 set packetSize_ 500
28 $cbr0 set interval_ 0.005
29 $cbr0 attach-agent $udp0
30
31 set null0 [new Agent/Null]
32 $ns attach-agent $n(3) $null0
33
34 $ns connect $udp0 $null0
35
36 $ns at 0.5 "$cbr0 start"
37 $ns rtmodel-at 1.0 down $n(1) $n(2)
38 $ns rtmodel-at 2.0 up $n(1) $n(2)
39 $ns at 4.5 "$cbr0 stop"
40
41 $ns at 5.0 "finish"
42
43 $ns run

```

Code listing 1: The ns-2 code.