1. Terminologies of Distributed Systems (24 points)

Briefly explain these terminologies. If they are acronyms, also write what they stand for.

(a) IIOP - Interoperable (Internet) Inter-ORB protocol is a protocol that makes it possible for distributed programs written in different programming languages to communicate over the Internet. IIOP is a critical part of Common Object Request Broker Architecture (CORBA).

(b) ORB - An Object Request Broker (ORB) is the programming that acts as a "broker" between a client request for a service from a distributed object or component and the completion of that request.

(c) Spontaneous Networking - The form of distribution that integrates mobile devices and other devices into a given network.

(d) TLS - Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet.

(e) VPN - A virtual private network (VPN) is a private data network that makes use of the public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

(f) WAP - Wireless Application Protocol is a set of protocols that have been developed specifically for use on wireless portable devices.

2. System Models (20 points)

Consider a communication service used in asynchronous distributed systems. In this service, messages may be lost, delayed, or delivered too faster for the recipient to handle them, but those that are delivered arrive with the correct contents. In addition, checksums apply to both headers and bodies.

(a) Describe the classes of failure exhibited by this service. (8 points)

(b) Classify their failures according to their effect on the properties of validity and integrity. (8 points)

(c) Can this service be described as a reliable communication service? (4 points)

(a) Failures:
- It doesn’t exhibit arbitrary failures because those that are delivered arrive with the correct contents.
- There are Omission failures because of lost messages.
- Because the distributed system in which it is used is asynchronous, it cannot suffer from timing failures.

(b) Properties of validity and integrity:
- Validity is denied by lost messages.
- Checksums apply to both headers and bodies. So integrity is guaranteed.

(c) It cannot be called reliable from the above analysis.
3. Networking and Internetworking (16 points)

A session of applying `ping` and `netstat -rn` on `kirk.cs.twsu.edu` is shown as follows:

```
kirk> ping kirk
PING kirk.cs.twsu.edu (156.26.10.239): 56 data bytes
kirk> netstat -rn
Kernel IP routing table
intersection
Destination Gateway Genmask Flags MSS Window irtt Iface
156.26.10.128 0.0.0.0 255.255.255.128 U 40 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 40 0 0 eth1
0.0.0.0 156.26.10.129 0.0.0.0 UG 40 0 0 eth0
```

(a) How many Ethernet cards does this machine have?
(b) Will an IP datagram destined for 156.26.10.233 be delivered directly, or will be forwarded to a next-hop router? If it will be delivered to a router, identify the one to which it will be delivered.
(c) Will an IP datagram destined for 156.26.10.41 be delivered directly, or will be forwarded to a next-hop router? If it will be delivered to a router, identify the one to which it will be delivered.
(d) Will an IP datagram destined 156.26.1.30 for be delivered directly, or will be forwarded to a next-hop router? If it will be delivered to a router, identify the one to which it will be delivered.

(a) There are two Ethernet cards: `eth0` and `eth1`.
(b) It will be delivered directly.
(c) It will be forwarded to a next-hop router - 156.26.10.129.
(d) It will be forwarded to a next-hop router - 156.26.10.129.

4. Networking and Internetworking (10 points)

(a) What is difference between connection-oriented service and connection-less service? (6 points)
(b) Give an example protocol for which connection-oriented service is appropriate. Also, give an example protocol for connectionless service. (4 points)

(a) A connection-oriented service requires that communication parties set up a link (point-to-point connection) before the service; whereas the connectionless one doesn’t.
(b) Examples for the connection-oriented service are ftp, remote login, talk. Examples for the connectionless service are e-mail, NTP, BOOTP.
5. Interprocess Communication (10 points)
Write socket functions for TCP client-server communication in UNIX.

![Socket Functions Diagram]

6. Operating System Support (20 points)
(a) What are main differences between user-level threads and kernel-level threads? (8 points)
(b) Give two circumstances where user-level thread is better than the kernel-level. (6 points)
(c) Give two circumstances where kernel-level thread is better than the user-level thread. (6 points)

(a) • User-level threads are unknown by the kernel, whereas the kernel is aware of kernel threads.
   • User threads are scheduled by the thread library and the kernel schedules kernel threads.
   • Kernel threads need not be associated with a process whereas every user thread belongs to a process.

(b) • Thread creations are less costly.
   • The thread-scheduling can be customized or changed to suit specific applications.
   • Many more user-level threads can be supported than the kernel could provide.

(c) • The threads can take advantage of a multiprocessor.
   • A thread that takes a page fault won’t block the entire process.
   • Threads within different processes can be scheduled according to a single scheme of relative prioritization.
7. Security (20 points)

Schneier describes the principles of an encryption algorithm are to create confusion and diffusion.

(a) What do confusion and diffusion stand for here? (8 points)
(b) Write a code showing confusion and diffusion. (12 points)

(a) Confusion means to alter a message to make it appear to mean something else. This may still reveal a pattern. So diffusion means to mix up or scramble the contents. This eliminates the patterns.
(b) 
\[ x = y << 4 \text{ xor } y >> 5 + k; \]
\[ y = x << 4 \text{ xor } x >> 5 + k; \]

8. Security (15 points)

(a) What does PGP stand for and its purpose?
(b) Why are asymmetric encryption algorithms usually used for authentication and symmetric encryption algorithms for document secrecy?
(c) Suppose that a firewall blocks all incoming datagrams except for those destined for ports 14, 20, and 21 (telnet and ftp). Can an ftp client inside of the firewall connect to an ftp server outside of the firewall that is listening for ftp requests on the standard port 21? Briefly explain why or why not.

(a) PGP (Pretty Good Privacy) has been developed and distributed with the aim of enabling all computer users to enjoy the level of privacy and integrity afforded by the use of public-key cryptography in their communications.
(b) Asymmetric encryption algorithms provide the public-key which facilitates authentication. In addition, they are usually too slow for document encryption. Symmetric encryption is usually fast enough to use secret key to encrypt document.
(c) Suppose the firewall doesn’t block the outgoing datagrams at port 21, the ftp client can connect to the remote ftp server. But the reply from the server cannot reach the client. So eventually the request will fail.

9. Term Paper (20 points)

(a) What is the topic of your term paper? (4 points)
(b) What are the major goals of your term paper? (8 points)
(c) What is the scope of your term paper? (8 points)

10. RPC, RMI, CORBA Programming (45 points)

Consider an application that implements a remote dictionary. The dictionary offers four operations: count to return the word count, insert to insert a word and its content, delete to delete a word, and lookup to search for a word and return the content of the word.

(a) Use Sun RPC to specify this application.
(b) Use CORBA IDL to specify this application.
(c) Specify this application in a Java RMI interface file.

(a) Sun RPC

```
struct word_content {
    string word<>
    string content<>
};

program RDICTPROG {
    version RDICTVERS {
        int COUNT(void) = 1;
        int INSERT(word_content) = 2;
    }
```
(b) CORBA IDL

```idl
module Dictionary_App {
    interface Remote_Dictionary {
        unsigned long count();
        unsigned long insert(in string word, int string content);
        unsigned long delete(in string word);
        string lookup(in string word);
    }
};
```  

(c) Java RMI interface file

```java
import java.rmi.*;
public interface DictionaryInterface extends Remote {
    public long count() throws RemoteException;
    public long insert(String word, String content) throws RemoteException;
    public long delete(String word) throws RemoteException;
    public String lookup(String word) throws RemoteException;
}
```