MARIA COLLEGE OF ENGINEERING AND TECHNOLOGY, ATTOOR

DEPARTMENT OF INFORMATION TECHNOLOGY

NETWORK PROGRAMMING MANAGEMENT

2 MARKS QUESTIONS & ANSWERS

UNIT-I

TWO MARKS

1. What is a socket?

A socket is a logical endpoint for communication between two hosts on a TCP/IP network. A socket is uniquely identified by three attributes:
- The host's IP address
- The type of service needed. Eg(TCP/UDP)
- The port number

2. State the differences between TCP and UDP.

S.No	TCP	UDP
1	Connection oriented	Connection less
2	Sophisticated	Simple
3	Reliable	Unreliable
4	Byte-Stream Protocol	Datagram Protocol

3. What is Passive open?

The server prepares to accept an incoming connection by calling socket,bind and listen functions. This is called passive open.

4. What is Active open?

The client connects to the server by calling the connect function. It causes the client to send a SYN segment which consists of initial sequence number for the data. This is called Active open.

5. What is Passive close?

The side (client/server) that receives the FIN segments from the other end performs the Passive close.

6. What is Active close?

   The side (client/server) which calls the close function first, is performing Active close.

7. What is half-close?

   The dataflow from the end doing the passive close to the end doing the Active close is called a half-close.

8. What are the three different categories of ports?

   1. The well-known ports (0 to 1023)
   2. The registered ports (1024 to 49151)
   3. The dynamic or private ports (49152 to 65535)

9. What are well-known ports?

   The well-known ports are used to identify well-known services. The port numbers from 0 to 1023 are well-known ports. For example: port 21 is used to identify FTP service, port 80 is used to identify web services.

10. What are registered ports?

   Registered ports are not controlled by IANA. Port numbers from 1024 to 49151 are registered ports. These ports are used according to the convenience of the network community.

11. What are Dynamic/ Private / Ephemeral ports?

   Dynamic ports are short –lived ports. These ports are used only by TCP/UDP client. Port Numbers from 49152 to 65535 are dynamic ports.

12. What is a Reserved port?

   A reserved port is any port less than 1024.These ports can only be assigned to a socket by a super user process.

13. What are Socket Address Structures?

   Socket Address Structure is passed as argument to the socket function. It is used to set the properties of socket such as
   1. Length
   2. Family
   3. port number
   4. IP Address

14. What is host byte order?

The byte ordering followed by a given system can be in two ways: little endian byte order or big endian byte order. This is called host byte order.

15. What is Network byte order?

In a network the sending protocol stack and the receiving protocol stack must agree or the orders in which bytes are transmitted. This is called network byte order. It uses big-endian byte ordering.

16. What is the need of fork system call?

Fork function is used to create a new process. The prototype as follows:
pid_t fork(void);

*returns 0 in child
  Process ID of child in parent
  -1 on error.

17. What are the uses of fork system call?

1. A process makes a copy of itself so that one copy can handle one operation while the other copy does another task.
2. A process wants to execute another program. It calls exec to replace itself with the new program.

18. What is an iterative server?

Iterative server will tie up a server with a single client. We would not be able to serve the multiple numbers of clients simultaneously. It is used for simple, short services.

19. What is a concurrent server?

Concurrent servers service many clients simultaneously using time sharing method or by having different processors. It can be implemented in UNIX by using fork system call.

20. What is the use of getsockname and getpeername function?

getsockname function returns the local protocol adress associated with a socket
getpeername function returns the foreign protocol adress associated with a socket

16 MARKS

1.Explain the TCP/IP layering in detail with neat sketch.
- SAS
- IPv4
- Ipv6
- Generic
- Comparison

2.Explain tne various elementary TCP socket functions.
- Socket()
- Connect()
- Bind()
- Listen()
- Accept()
- Read()
- Write()
- Close()

3.Compare Iterative server and Concurrent server
- Code for iterative server
- Code for concurrent server

4.Explain Byte ordering functions with adress conversion.
- Program to determine host byte order
- Inet_aton,inet_addr,inet_ntoa
- Inet_pton,inet_ntop
- Sock_ntop and related functions

1. What is a signal?

A signal is notifications to a process that an event has occurred.They are also called software interrupts.

2. What is a disposition?

Every signal has some action associated with it. This associated action is called disposition.

3. What is the use of 'sigprocmask'function?

The 'sigprocmask'function is used to selectively block and unblock a set of signals.

4. List the Posix signal semantics.

1. Signal handler once installed remain forever.
2. When a signal handler is executing the signal being delivered is blocked.
3. If a signed is generated one or more times while it is blocked, it is delivered only one time after it is unblocked.
4. It is possible to selectively block and unblock a set of signals using the 'sigprocmask'function.

5. What is a Zombie process?

A Zombies process is one that has completed its execution but still has an entry in the process table, allowing the process that started it to read its exit status.

6. What is the difference between wait and waitpid function?

Wait – If a process calls wait ( ) and if it has one or more children that are executing, then wait blocks until the first of the existing children terminate.
Waitpid – Waitpid gives us more control over which process to wait for. The pid arguments specifies the process ID that we want to wait for.

7. What are the two phases of an input operation?

The two phases of an input operation:
1. Waiting for the data to be ready.
2. Copying the data from the kernel to the process.

8. What are the difference between signal driven I/O model and asynchronous I/O model?

Signal driven I/O model	Asynchronous I/O model

Kernel notifies when an I/O operation is initiated.	Kernel notifies when an I/O operation is complete.
Signal is generated before the data copy.	Signal is not generated until the data has been copied to application buffer.
Synchronous I/O operation	Asynchronous I/O operation

9. Under what condition a socket is ready for reading?

     1. The number of bytes of data in the socket receive buffer is greater than or equal to the current size of low water mark for the socket receive buffer.

     2. The read-half of the connection is closed.

     3. The socket is a listening socket and the number of completed connection is nonzero.

     4. A socket error is pending.

10. Under what condition a socket is ready for writing?

     1. The number of bytes of available space in the socket send buffer is greater than or equal to the current size of low water mark for the socket.

     2. The write-half of the connection is closed.

     3. A socket error is pending.

11. Differentiate 'shutdown'&& 'close'?

Shutdown	Close
We can initiate connection termination without the reference count.	Connection termination is initiated only if reference count reaches zero.
It is possible to terminate the connection is three ways: *Reading side *Writing side *Both sides	It is only possible to terminate the connections on both sides of data transfer.

12. What is Denial of service attacks?

     When a server is handling multiple clients there is a possibility that the server can block in a function call related to a single client. It can hang the server and deny service to all other clients. This is called a Denial of service attack.

13. What is the use of 'pselect'function?

     pselect function is the same as select function but it increases the time precision from microseconds to nanoseconds. Also it takes a new argument that enables us to avoid race conditions when signals are being caught.

14.What is the use of SIGCHILD signal?

The SIGCHILD signal is sent by the kernel whenever a process terminates,to the parent of the terminating process

15.What is the use of FIN signal?
When the client terminates the connection,it sends the FIN signal to the server and then closes the connection.

16. What is the use of SIGPIPE signal?
When a process writes to a socket that has received RST,the SIGPIPE signal is sent to the process.The default action of this signal is to terminate the process so the process must catch the signal to avoid being involuntarily terminated.

16 MARKS

1.Write a TCP socket program to implement Echo server/Echo client
- TCP echo server code
- Str_echo function
- TCP echo client
- Str_cli function

2.Explain in detail the different I/O Multiplexing models.
- Blocking I/O
- Nonblocking I/O
- I/O Multiplexing
- Signal driven I/O
- Asynchronous I/O

3.Explain Posix signal handling.
- Signal function
- Code for signal function
- Posix signal semantics
- Handling SIGCHILD Signals
- Handling Zombies

UNIT-3
TWO MARKS

1. What is the use of getsockopt function?

The getsockopt function is used to get the values of socket options that was set already. The prototype of getsockopt as follows

getsockopt (sockfd, level, optname ,*optval,*optlen);

2. What is the use of setsockopt function?

The setsockopt function is used to set the values for the socket options .The prototype of setsockopt as follows

setsockopt (sockfd,level,optname ,*optval,optlen);

    *level specifies code (general socket code or protocol specific code).

   *Optname is the option name such as Broadcast, Debug etc.

   *Optval is the value of the optname.

   *Optlen is the length of the option.

3. What is pending error?

When an error occurs on a socket, the kernel sets a variable named so_error to one of standard values. This is called pending error.

4. What is half-open connection?

If the client host crashes, the server process will never knew about it. The server will continually wait for input that can never arrive. This is called a half open connection.

5. What is a pipe?

TCP connection between two end points is called a pipe .

Eg:TCP connection pipe with a capacity of 8 segments.

Data 8		Data7		Data6		Data5	
	Ack1		Ack2		Ack3		ack4

6. What is the bandwidth-delay product?

The capacity of the pipe is called the bandwidth-delay product. It is the product of bandwidth and Round TripTime.

Bandwidth-delay product= bandwidth*RTT Bytes

7. What is the receive low-water mark?
The receive low-water mark is the amount of data that must be in the socket receive buffer for 'select' function to return 'readable'. The default value us one for both TCP and UDP sockets.

8. What is the send low-water mark?
The send low-water mark is the amount of available space that must exist in the socket send buffer for 'select' function to return 'writeable'.The default value for TCP socket is 2048.

9. What is the purpose of the Nagle algorithm?
The purpose of the Nagle algorithm is to reduce the number of small packets on a MAN.

10. What is Nagle algorithm?
The algorithm states that if a given connection has outstanding data, then no small packets will be send on the connection until the existing data is acknowledged.

11. What is an outstanding data?
An outstanding data is an data that is send by aTCP, and for which it is currently awaiting an acknowledgement.

12. What is a small packet?
A small packet is any packets smaller than MSS(Maximum segment size).

13. Mention some application built with UDP
1. DNS –Domain Name System
2. NFS-Network File System
3. SNMP-Simple Network Management Protocol

14. Distinguish between connected UDP Socket and Unconnected UDP Socket

Unconnected UDP Socket	Connected UDP Socket
1. Default UDP socket created when we create a socket in UDP. 2.We use 'send to' function to send any data 3. We use 'recvfrom' to receive data. 4. We should specify destination IP address and port number for the above function. 5. Asynchronous errors are not returned in UDPsockets.	Created as a result of calling 'connect' on a UDP socket. We use 'write to' function to send any data

1. Discuss about IP socket option and ICMP socket options in detail with suitable examples
2. Briefly discuss about DNS with an example.
3. Describe about the different socket options for Internet operation and control
4. Explain the purpose and usage of UDP sockets and their different functions.

UNIT 4
TWO MARKS

1. Compare IPv4 and IPv6

	IPv4	Ipv6
Address length	32 bits	128 bits
Fragmentation	Hosts and routers	Hosts only
Check sum in header	Yes	No
DNS name queries	Uses A records	Uses AAAA records
Qos support	Small extent	Better extent

Address structure	Struct sockaddr-in
	{
	Sa_family_t sin family
	in_port _t sin _port
	struct in_addr sin_addr
	}
		Struct sockaddr_in6
		{
		Sa_family_t in6_family
		Int_port_t sin6_port
		Uint32_t sin6_flowinfo
		Structin6_addr sin6_addr
		Unit32_t sin6_scope_id"
		}

2. List out the benefits of IPv6.
   - Address depletion solved
   - International misallocation solved
   - End-to-End communication restored
   - Scoped address & address selection possible
   - More efficient forwarding and fast routing
   - Built –in security and mobility

3. What are the rules of Dual-stack host in dealing with listening socket?

A listening IPv4 socket can accept incoming connections from IPv4 clients. If a server has a IPv6 listening socket which has wild card address, then the socket can accept incoming connections from either IPv4 or IPv6.

4. Give note on IPv6_ADDRFROM option.

IPv6_ADDRFORM provide socket transformation between IPv4 and IPv6, enabling sockets to be passed between IPv4 and IPv6 applications. Applications already developed using IPv4 will have no knowledge of this socket option; this implies that all IPv4/IPv6 socket transformation should only be performed by IPv6 applications.

5. What are the disadvantage of using fork () function?

- Fork is expensive. Memory is copied from the parent to the child, all descriptors are duplicated in the child
- IPC is required to pass information between the parent and child after the fork. Passing information from the parent to the child before the fork is easy, since the child starts   with a copy of the parent's data space and copy of all the parents descriptors .But returning information from the child to the parent takes more work.

6. What are the shared information by all threads within a process?

All treads within a process share the following:
- Process instructions
- Most data
- Open files
- Signal handlers and signal dispositions'
- Current working directory
- User and group IDs

7. What are the information each thread possess?

Each thread has its own

- Thread ID
- Set of registers, including program counter and stack pointer
- Stack
- err no
- Signal mask
- Priority

8. What are the basic functions related to threads?

- pthread _ create() Function
- pthread_ join(0Function
- pthread_ self Function
- pthread_ detach Function
- pthread_ exit Function

9. How threads are created?

When a program is started by exec a single thread is created, called the initial thread or main thread. Additional threads are created by pthread_ create.
pthread_ create.
#include<pthread.H>
int pthread_create(pthread_t *tid,cons pthread_attr_t *attr,void*(*func)(void *),void *arg);
Returns:0 if ok, positive Exxx value on error
Each thread within a process is identified by a thread ID, whose data type is thread_t(often an unsigned int).On successful creation of a new thread , its ID is returned through the pointer tid .

11. What are the attributes of treads?

Each tread has following attributes
- Its priority
- Its initial stack size
- Whether it should be a daemon thread or not

12. Give a note on pthread_ join() function

#include<pthread.h>
int pthread_join(ptread_t tid, void **status);

The pthread_ join() function shall suspend execution of the calling thread until tid terminates, unless the target tid has already terminated. On return from a successful pthread_ join() call with a non-NULL status argument, the value passed to thread_ exit() by the terminating thread shall be made available in the location referenced by status.

13. How threads are terminated?

There are two ways for a thread to terminate

- The function that starts the thread can return. Since this function must be declared as returning a void pointer that return value is the exit status of the thread.
- If the main function of the process returns or if any thread calls exit, the process terminates.

14. What is the benefit of multithreaded code?

- Improve application responsiveness
- Use multiprocessors more efficiently
- Improve program structure
- Use fewer system resources

15. What do you mean by Threaded server?

The threaded server is probably the simplest "real" server type. A server program almost always needs to handle more than one connection at a time. The reason is since each connection gets its own thread, each thread can use simple blocking I/O on the socket. Each thread handles its connection more or less identically to the way the basic server handles each connection.

16. What are the features provides by the raw socket?

Raw sockets provides by the features not provided by the normal TCP and UDP sockets:
- Raw sockets let us read and write ICMPv4, IGMPv4, and ICMPv6 packets.
- With a raw socket , a process can read and write IPv4 datagrams with an IPv4 protocol field that is not processed by the kernel .Most kernels only process datagrams containing values of 1 (ICMP), 2 (IGMP), 6 (TCP) and (UDP)
- With a raw socket, a process can build its own IPv4 header using the IP_HDRINCL socket option.

17. How raw socket is created.

The socket function creates a raw socket when the second argument is SOCK_RAW.The third argument is normally nonzero.
For example, to create an IPv4 raw socket we would write
int sockfd;
sockfd=socket(AF_INET,SOCK_RAW,protocol);

where protocol is one of the constants, IPPROTO_xxx, defined by including the <netinet/in.h> header, such as IPPROTO_ICMP.Only the super user can create a raw socket.This prevents normal users from writing their own IP datagrams to the network.

18. Write short note on raw socket output.

Output on a raw socket is governed by following rules:
- Normal output is performed by calling send to or send massage and specifying the destination IP address. Write. Write, or send can also called if the socket has been connected.
- If the IP_HDRINCL option is not set the starting address of the data for the kernel to send specifies the first byte following the IP header because the kernel will build the IP header and pretend it to the data from the process. The kernel sets the protocol field of the IPv4 header that it build to the third argument from the call to socket.

19. What is the use of ping program?

   Ping program lets us to test whether another host is reachable in the computer network.

20. What is the disadvantage of threads?

   All threads within a process share the same global memory. This makes the sharing of information easy between the threads, but along with this simplicity comes the problem of synchronization

16 MARKS

1. Elaborate about raw sockets creation,input and output
2. Explain how a TCP echo server using threads is created and also give their advantages
3. Explain trace route program with suitable example
4. Explain Ping program with suitable example

UNIT 5
TWO MARKS

1. What is the purpose of management station in network management?

   Management station serves as the interface for the network manager to work on the network management system.

2. What are the elements present in Management Station?

   • Management applications for data analysis, fault recovery and so on.

   • An interface to monitor and control the network.

   • Capability to transfer the network manager's requirements into the actual monitoring and control of remote elements in the network.

   • A database of information extracted from the MIBs of all the managed entities in the network.

3. What is managed device?

   A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this   information available to NMSs using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.

4. Define MIB

The MIB is a collection of access points at the agent for the management station. A management station performs the monitoring function by retrieving the value of MIB objects.

5. What are the key capabilities of SNMP?

- Get: enables the management station to retrieve the value of objects at the agent.
- Set: enables the management station to set the value of objects at the agent.
- Trap: enables an agent to notify the management station of significant events.

6. Define Trap directed polling

At initialization time, a management station can p[olla ii of the agents it knows for some key information. Once this baseline is established the management station refrains from polling. Instead, each agent is responsible for notifying the management station of any unusual event. These events are communicated in SNMP messages known as traps. At this point, the management station may direct polls to the agent reporting the event and perhaps to some nearby agents in order to diagnose any problem and to gain more specific information about the exception condition.

7. Define proxies.

To accommodate devices that do not implement SNMP, the concept of proxy was developed. In this scheme agent acts as a proxy for one or more other devices; that is , the SNMP agent acts on behalf of the proxies devices. The management station sends queries concerning a device to its proxy agent. The proxy agent converts each query into the management protocol that the device is using, When the agent receives a reply to a query, it passes that reply back top the management station. Similarly, if an event notification of some sort from the device is transmitted to the proxy, the proxy sends that onto the management station in the form of a trap message.

8. What are the objectives of MIB?

- The object or objects used to represent a particular resource must be same at each system.
- A common scheme for representation must be used to support interoperability.

9. Define MIB structure

All managed objects in the SNMP environment are arranged in a hierarchical or tree structure. The leaf objects of the tree are the actual managed objects, each of which

represents some resource, activity, or related information that is to be managed. The tree structure itself defines a grouping of objects into logically related sets.

10. How are we to define objects?

- There are two ways in which a managed object can be defined
- Define a new type called Object and every in the MIB would be of this type.
- Use a macro to define a set of related types used to define managed objects.

11. State the levels of definitions for macros.

- Macro definition: defines the legal macro instances; specifies the syntax of a set of related types.
- Macro instance: an instance generated from a specific macro definition by supplying arguments for the parameters on the macro definition; specifies a particular type.
- Macro instance value: represents a specific entity with a specifies value

12. Mention the goals of SNMP.
- The SNMP explicitly minimizes the number and complexity of management functions realized by the management agent itself.
- The functional paradigm for monitoring and control be sufficiently extensible to accommodate additional, possibly unanticipated aspects of network operation and management.
- The architecture is, as much as possible, independent of the architecture and mechanisms of particular hosts or particular gateways.

13. State the practical issues of SNMPv1 protocol

- Differences in SNMP support by vendors of bridges and routers
- Objects not supported
- Selection of a network management station
- Polling Frequency
- Limitations of SNMP

14.State the goals of RMON

- Off-line operation
- Proactive monitoring
- Problem detection and reporting
- Value added data
- Multiple managers

15. State the advantages of SNMPv2

Adds and enhances some protocol operations, like Trap operation. Defines two new operations namely; Get Bulk and Inform.

16. What are the applications of SNMPv3?

- Command generator application
- Command responder application
- Notification originator application
- Proxy forwarder application

17. What are the key concepts of SNMPv2 SMI?

- Object definitions
- Conceptual tables
- Notification definitions
- Information modules

18. What data's are present in the TCP connection table?

The data are present in the TcmCP connection table State; delete TCB, Local address, Local port, Remote address and Remote port

19. State the key enhancements in SNMPv2

Macro used to define object types has been expanded to include several new data types. New convention has been provided for creating and deleting conceptual rows in a table. SNMPv2 MIB contains basic traffic information about the operation of the SNMPv2 protocol and also other information related to the configuration of an SNMPv2 manager or agent. Two new PDUs included are: Get Bulk Request enables the manager to receive large blocks of data efficiently; Inform Request enables one manager to send trap type of information to another.

20. State the types of access to the management information

- Manager-agent request-response
- Manager-manager request-response
- Agent-manager unconfirmed

16 MARKS

1. Explain the architecture of SNMPv3 with neat diagram
2. Explain in detail RMON
3. Explain MIB
4. Compare SNMPv2 & SNMPv3