24

CONFIDENTIAL

MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION

JANUARY 2016 SEMESTER

SUBJECT CODE	:	INB48103
SUBJECT TITLE	:	NETWORK MANAGEMENT
LEVEL	:	BACHELOR
TIME / DURATION	:	2.00 pm – 4.00 pm (2 HOURS)
DATE	:	19 MAY 2016

INSTRUCTIONS TO CANDIDATES

1. Please read the instructions given in the question paper CAREFULLY.
2. This question paper is printed on both sides of the paper.
3. This paper consists of 5 questions, Answer 4 (FOUR) questions only.
4. Please write your answers on the answer booklet provided.

THERE ARE 7 PAGES OF QUESTIONS, INCLUDING COVER.

SECTION A (Total: 100 marks)

INSTRUCTION: Answer FOUR (4) Questions ONLY
Please use the answer booklet provided.

Question 1

A. Define Management Information Base (MIB)

(2 marks)

B. Define SNMP Trap message

(2 marks)

C. Define User Datagram Protocol (UDP)

(2 marks)

D. With the RMON1 MIB, network managers can collect information from remote network segments for the purposes of troubleshooting and performance monitoring. Describe **THREE (3)** features that RMON1 MIB provides.

(6 marks)

E. You are a network and system administration engineer in a reputable company. You received a trouble ticket pertaining to a complaint of an inaccessibility to internet. Applying your knowledge in scientific method, discuss the trouble shooting process.

(13 marks)

[Total:25 marks]

Question 2

A. SNMP consists of SNMP command, Agent, Manager, MIB, and OID. Discuss the role of each component.

(5 marks)

B. SNMP uses five basic messages (Get, GetNext, GetResponse, Set and Trap) to communicate between the manager and the agent. Show in a diagram of the messages flow between manager and agent then the operation for each basic message listed above.

(10 marks)

C. The SNMP version 1 protocol between manager and element defines only five types of messages. List the FIVE types of message and differentiate the role of each message.

(5 marks)

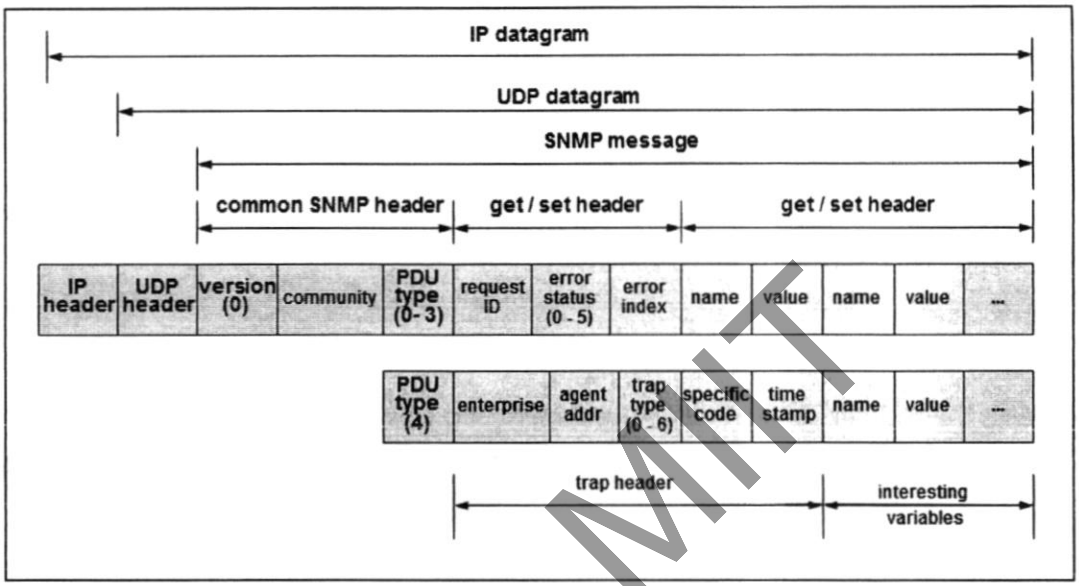

Figure 1

D. You captured a SNMP packet at your gateway router using Wireshark for a traffic analysis. Applying your knowledge in SNMP packet format as shown in Figure 1, interpret the captured SNMP packet based on this information:-

1. PDU type = 2
2. Community = "encryptedPDU: privkey Unknown
3. Error status = 4

(5 marks)

[Total: 25 marks]

Question 3

A. Refer to the SMI object tree in Figure 2. Based on the information, define the object tree with SMI syntax for sysUpTime.

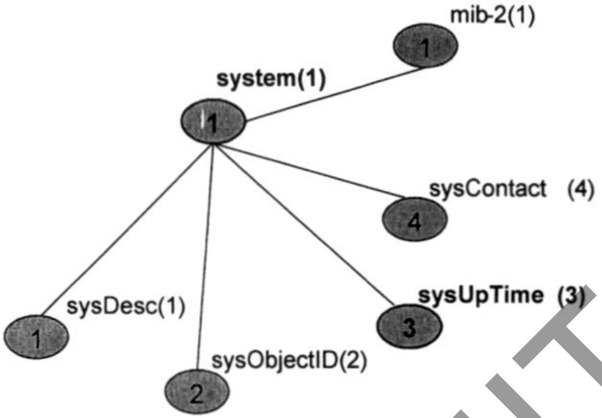

Figure 2

(5 marks)

B. The objects in MIB2 are categorized under 10 different groups: system, interface, address translation, ip, icmp, tcp, udp, egp, transmission, and snmp. Show these groups of mib-2 object in an object identifier tree diagram.

(5 marks)

C. Based on the SMI object tree in Figure 3. Define the SMI syntax

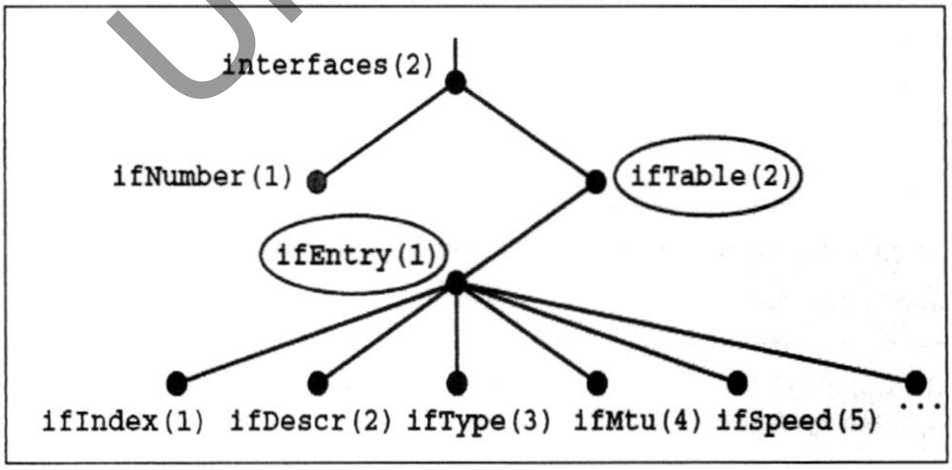

Figure 3

(15 marks)

[Total: 25 marks]

Question 4

A. Refer to Figure 4. Understanding layered model makes it easier to troubleshoot communication problems. SNMP processing indicators can be used to verify the passage of the packet through the UDP layer and the functioning of the Application layer. Based on a single SNMP GET request, discuss the process flow of the complete operation at each respective layer.

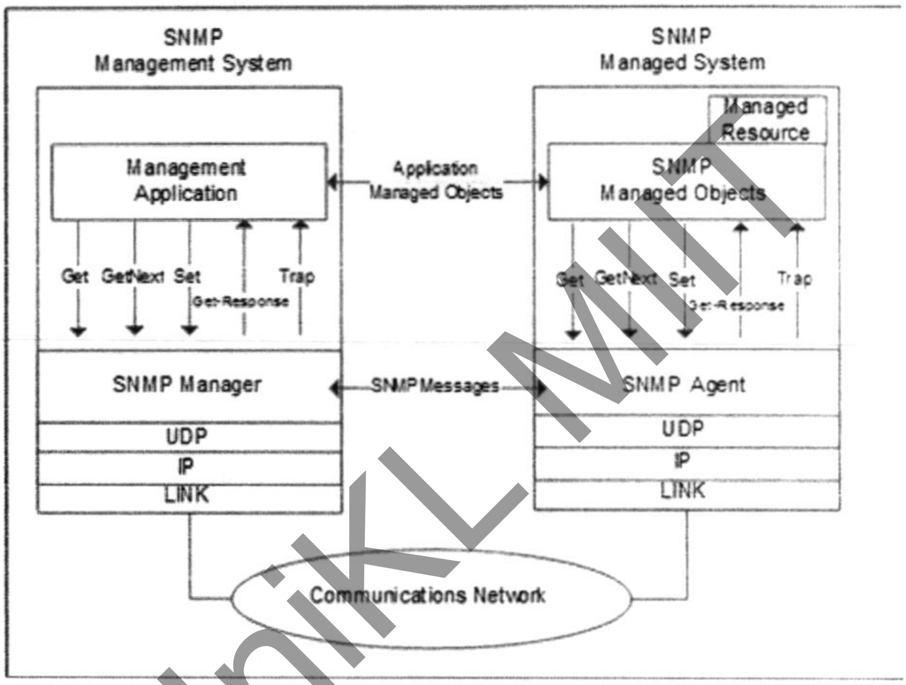

Figure 4: An SNMP message passes through the protocol layers at both the manager and agent

(10 marks)

B. The getbulk command is useful for retrieving a group MIB object at a time. Given the following command:

```
$ ./snmpbulkget -v2c -Cn1 -Cr2 127.0.0.1 -c jb sysDescr sysContact
system.sysName
```

Then, we get a respond of:

```
system.sysDescr.0 = "Centos 7.02 (Build 7601 Multiprocessor Free)"
system.sysContact.0 = "jb@unikl.edu.my"
```

system.sysName.0 = “jb-miit.unikl.edu.my”

Furthermore, we get the following two datagram traces from wireshark (Only UDP and SNMP header are shown). Based on information in figure 5 and figure 6, complete related information indicated in (--A--), (--B--), (--C--), (--D--), (--E--), (--F--), (--G--), (--H--), and (--I--), (--J--), (--K--),(--L--).

```
User Datagram Protocol, Src Port: 34195 (34195), Dst Port: snmp
(161)
    Source port: (--A--) ()
    Destination port: snmp (--B--)
    Length: 63
    Checksum: 0xfe52 (incorrect, should be 0x0c90)
Simple Network Management Protocol
    Version: (--C--) (1)
    Community: (--D--)
    PDU type: (--E--) (5)
    Request Id: 0x0f15c607
    Non-repeaters: 1
    Max repetitions: 2
    Object identifier 1: (--G--) (SNMPv2-MIB::sysDescr)
    Value: NULL
    Object identifier 2: (--I--). (SNMPv2-MIB::sysContact)
    Value: NULL
```

Figure 5: GetBulk datagram

```
User Datagram Protocol, Src Port: snmp (161), Dst Port: 34195
(34195)
    Source port: snmp (161)
    Destination port: 34195 (34195)
    Length: 177
    Checksum: 0xfec4 (incorrect, should be 0x47bb)
Simple Network Management Protocol
    Version: (--C--) (1)
    Community: (--D--)
    PDU type: (--E--) (2)
    Request Id: (--F--)
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: (--G--).0 (SNMPv2-MIB::sysDescr.0)
    Value: STRING: (--H--)
    Object identifier 2: (--I--).0 (SNMPv2-MIB::sysContact.0)
    Value: STRING: (--J--)
    Object identifier 3: (--K--).0 (SNMPv2-MIB::sysName.0)
    Value: STRING: (--L--)
```

Figure 6: GetResponse datagram

(15 marks)

[Total: 25 marks]

Question 5

A. In today's challenging IT / Network environment, it is vital to closely monitor and manage our enterprise network to ensure our network is in peak performance as modern organization relies heavily in computing and communication facilities. Using a NMS (network management software) as an example, answer the following questions:-

i. Discuss the importance of having a good NMS

(3 marks)

ii. Discuss the features that a network management software should have

(3 marks)

iii. Briefly explain the term 'Manager' and 'Agent' from the NMS point of view

(4 marks)

B. The conceptual areas of FCAPS, or Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management were created by the International Organization for Standardization (ISO) to aid in the understanding of the major functions of network management systems. Discuss each of the conceptual areas.

(15 marks)

[Total: 25 marks]

END OF EXAMINATION PAPER