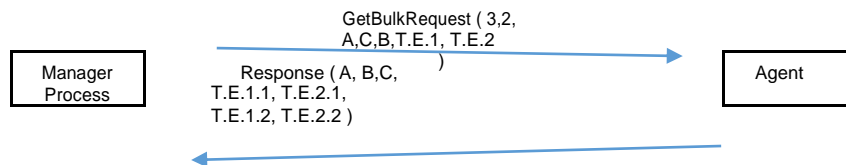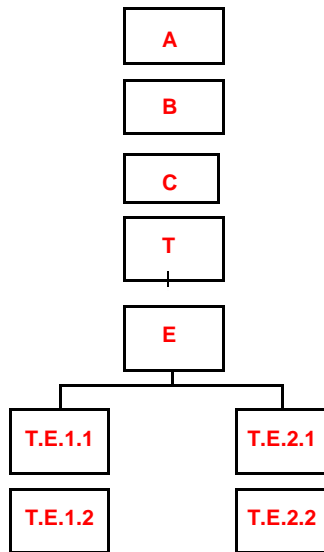## IT 340 – Network Management
Assignment No. 2

Due Date: 5th March, 2016 (Saturday, 11:59 pm)
Total Marks: 10 (Final mark out of 5)

Question No. 1

Apply the Get-Bulk-Request operation for the following MIB. Non-Repeaters is equal to 3 while the max repetitions is equal to 2.   **[2 mark]**

```
                A

                B

                C

                T

                E
          ┌───────────┐
       T.E.1.1      T.E.2.1

       T.E.1.2      T.E.2.2
```

```
                    GetBulkRequest ( 3,2,
                    A,C,B,T.E.1, T.E.2
                            )
  Manager         Response ( A, B,C,              Agent
  Process        T.E.1.1, T.E.2.1,
                 T.E.1.2, T.E.2.2 )
```

Question No. 2

Give two major changes made in SNMP V2 related to minimizing the data exchanged between agents and manager and standardized products.   **[1 mark]**

- Bulk data transfer

- Manager-to-manager message

- Enhancements to SMI: SMIv2
  - Module definitions: MODULE-IDENTITY macro
  - Object definitions: OBJECT-TYPE macro
  - Trap definitions: NOTIFICATION-TYPE macro

- Textual conventions

- Conformance statements

- Row creation and deletion in table

- MIB enhancements

- Transport mappings

Question No. 3
Differentiate between authentication and authorization in SNMPv3   **[2 mark]**

- Authentication verifies user identification
  - Client/server environment
    - Ticket-granting system
    - Authentication server system
    - Cryptographic authentication
  - Messaging environment
    - e-mail
    - e-commerce
- Authorization grants access to information
  - Read, read-write, no access
  - Indefinite period, finite period, one-time use

From Chap 7. (week 5)

Authentication
    • Data integrity:
        HMAC-MD5-96 / HMAC-SHA-96
    • Data origin authentication
        Append to the message a unique Identifier
        associated with authoritative SNMP engine

Authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.

Question No. 4
What are the components of RMON?   **[1 mark]**
RMON Probe Data gatherer: a physical device

Data analyzer: Processor that analyzes data

Question No. 5
What are the advantages of RMON?   **[1 mark]**

Monitors and analyzes locally and relays data; Less load on the network

Needs no direct visibility by NMS; More reliable information

Permits monitoring on a more frequent basis and hence faster fault diagnosis

Increases productivity for administrators

Question No. 6
What is the main difference between network traffic monitoring tools and network status tools?
                                                                   [1 mark]

The network traffic monitoring tools are to check the status of the of the transmission medium. And the network status tools to check the status of the node or the interface.

Question No. 7

Lists four basic network mentoring tools, can help a network's manager to find out the detail of a heavy traffic in his network?   **[1 mark]**

ping, tcpdump, wireshark, multi router traffic grouper (MRTG) etc.

Question No. 8

If one of the server at your network got an attack denial of service (DoS), explain how can the network statistic help you to find the attacker?   **[1 mark]**

By having a statistic for all packets going to that server before it is down, then look for the unusual increase of packets number from a specific source.