UNIVERSITI SAINS MALAYSIA

Second Semester Examination
Academic Session 2004/2005

March 2005

CST314 – Network and Security Management

Duration : 2 hours

INSTRUCTIONS TO CANDIDATE:

- Please ensure that this examination paper contains **SIX** questions in **THREE** printed pages before you start the examination.

- Answer **ALL** questions.

ENGLISH VERSION OF THE QUESTION PAPER

1.   SNMP is a protocol for TCP/IP based network management.

   (a)   List and describe briefly the **four (4)** components of SNMP.

   (b)   Describe how the SNMP protocol works.

   (c)   Explain succinctly the difference between the database of a network management system and its MIB. How do you implement each in a network management system?

(15/100)

2.   The OSI Model determines five application category of user-oriented network management system.

   (a)   List and describe briefly those **five (5)** application categories.

   (b)   You are establishing a small company (less than 40 staff). Give an example of each of the five application categories that you would implement in your network management system.

   (c)   Consider a network of multivendor components. Hubs are made by 3COM and are managed by 3COM Supervisor NMS (Network Management System). Routers are made by Cisco and are managed by CiscoWorks NMS. The entire network is managed by a general-purpose NMS such as HP OpenView Network Node Manager. Draw a three-tier management network that performs configuration and fault management. Explain the rational for your configuration.

(15/100)

3.   Imagine that you are working for a company that has decided to move from an SNMP-based management system to a web-based management system. You are asked to prepare a proposal on the two approaches, WBEM or JMX. The proposal consists of the following.

   (a)   Steps needed to be done for this migration

   (b)   Diagram of the architecture of the proposed system.

(20/100)

4. The School of Computer Science wishes to block a few IPs from being accessed by users from outside its network.

    (a) What is the network edge device that should be used to achieve this?

    (b) Can this device be used to close off certain ports of the network from access by users from the outside?

    (c) Give a brief explanation why someone would want to close off ports from being accessed from the outside.

    (15/100)

5. (a) A router is one of the two devices that hackers use to redirect IP addresses. What is the name of the second device?

    (b) Provide a brief description of the IPSec protocol used in IPv6.

    (20/100)

6. (a) What service is provided by port 22? Provide a short explanation about that service.

    (b) Which port is used for Email services (SMTP)?

    (c) State the main differences between a NAT and a Proxy.

    (15/100)

- oooOooo -