R 8212

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2006.

Seventh Semester

Computer Science and Engineering

CS 431 — NETWORK PROTOCOLS, MANAGEMENT AND SECURITY

Time : Three hours   Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the types of information that should be available for network monitoring?

2. Mention any four functions of configuration management.

3. What is meant by authentication service and proxy service?

4. How can a remote monitor be implemented?

5. Mention any two applications of public key cryptosystems.

6. What are the two types of authentication?

7. Mention any two design goals of firewalls.

8. Mention any two web security threats and counter measures.

9. How does frame relay provide high speed operation?

10. Differentiate between ATM and frame relay.

PART B — (5 × 16 = 80 marks)

11. (a) (i) Draw the frame relay architecture and illustrate the features.   (8)

       (ii) Mention the security enhancements in IPV6.   (8)

Or

(b) (i) Describe ATM architecture and operations. (10)

(ii) Write a note on peer-to-peer secure protocols. (6)

12. (a) Discuss the five types of OSI management functional areas and their features. (16)

Or

(b) Draw the architectural model and elements of a network management system and illustrate. (16)

13. (a) (i) What are extensions proposed in SMP for upgrading SNMP? (8)

(ii) What are the threats that can be handled by SNMPV3? (8)

Or

(b) Describe the architecture of SNMP entity and traditional SNMP manager, as specified in RFC 2271.

14. (a) What are the benefits and applications of IP security? (16)

Or

(b) (i) What are the four types of services provided by firewalls? (8)

(ii) Draw the IPSec authentication header and illustrate the various fields. (8)

15. (a) Discuss the different types of services provided by PGP, algorithms used and their description.

Or

(b) (i) Perform encryption and decryption using RSA algorithm if $p = 11$, $q = 13$, $e = 11$ and $M = 7$. (10)

(ii) Mention the requirements for Kerberos. (6)

———————————————