Exam.Code:0918
Sub. Code: 6567

2054

B.E. (Computer Science and Engineering)

Sixth Semester

CS-601: Computer Networks and Security

Time allowed: 3 Hours

Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Unit.*

x-x-x

I. Attempt the following:-

a) Contrast the roles of a hub and a bridge in network segmentation and collision domain management.

b) Compare the functions of a stateful firewall and a stateless firewall in network security, considering their inspection methods and policy enforcement.

c) Compare the advantages and disadvantages of wired and wireless LANs, discussing factors such as speed, interference, and mobility.

d) Define the terms "routing" and "switching" in the context of network communication.

e) What is the purpose of a subnet mask in IP networking, and how does it relate to network addressing?

(5x2)

UNIT - I

II. a) Analyze the OSI model in terms of its hierarchical structure and the functions performed at each layer. Evaluate the practical implications of adhering to this model in designing and implementing network protocols. Provide examples illustrating how the OSI model facilitates troubleshooting within network environments.

b) Compare and contrast different categories of networks, including LANs (Local Area Networks), WANs (Wide Area Networks), and MANs (Metropolitan Area Networks), in terms of their scope, geographical coverage, and typical use cases. Evaluate the advantages and disadvantages of each network category and analyze how their characteristics influence network design decisions and infrastructure investments.

(2x5)

III. a) Explain the key differences between IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) in terms of address structure, address space, and features. Evaluate the advantages and disadvantages of IPv4 and IPv6, considering factors such as scalability, security, and support for emerging technologies. Illustrate how the transition from IPv4 to IPv6 addresses the limitations of IPv4 and aligns with the evolving requirements of modern networking infrastructure.

Contd....P/2

b) Compare and contrast Distance Vector Routing and Link State Routing algorithms. Analyze the factors influencing the selection of a routing algorithm in different network environments, including scalability, convergence time, and resource utilization. Evaluate the strengths and weaknesses of both routing algorithms. (2x5)

IV. a) Compare and contrast different flow control mechanisms, such as window-based flow control and rate-based flow control, highlighting their advantages and limitations.

b) Analyze the trade-offs between reliability, latency, and overhead associated with TCP and UDP, considering their suitability for different types of applications and network environments. (2x5)

UNIT - II

V. a) Evaluate the fundamental differences between HTTP and FTP protocol functionalities, including data transfer mechanisms, resource access methods, and error handling. Analyze how HTTP and FTP protocols address distinct requirements for web page retrieval and file transfer, respectively, and discuss their respective roles in supporting efficient data exchange within networked environments.

b) Analyze the hierarchical structure of Domain Name System (DNS) and assess how DNS contributes to the efficiency and reliability of web browsing and other networked applications in modern internet infrastructure. (2x5)

VI. a) Assess how symmetric and public key authentication protocols address the challenges of identity verification, access control, and data integrity in networked environments.

b) Evaluate and compare the role of various security protocols and technologies implemented across different layers in overall network security using suitable real-world examples. (2x5)

VII. a) Compare different protocols used to secure email communication. Discuss the advantages and limitations of each such protocol in terms of interoperability, ease of implementation, and level of security provided.

b) Discuss how IP security addresses common security threats, such as eavesdropping, data tampering, and spoofing attacks using real-life examples. (2x5)

x-x-x