Ex/CSE/PC/B/T/322/2024

Bachelor of Computer Science & Engineering
Third Year, Second Semester Examination

Internet Technologies

Session: 2023-24

Time: 3 Hours Full Marks: 100

Group A (Total Marks: 20) [CO1 and CO2]
[Answer Any Two]

1. A. You are asked to enumerate all the intermediate routers between your machine and a target. What type of ICMP message will be helpful in this regard? Also state how can you achieve this goal.

   B. Under what circumstances does a router or gateway generate an ICMP destination unreachable message? What are the usages of ICMP router solicitation and router advertisement messages?

   C. Consider the resolution of the domain name `www.ugc.gov.in` by a DNS resolver. Assume that no resource records are cached anywhere across the DNS servers. Describe the operation of the iterative query mechanism for resolving the domain name.

$4 + 2 + 4 = 10$

2. A. Consider an instance of TCP's Additive Increase Multiplicative Decrease (AIMD) algorithm where the window size at the start of slow start phase is 1 MSS and the threshold at the start of first transmission is 10 MSS. Assume that a time out occurs during the sixth transmission. Find the congestion window size at the end of tenth transmission.

   B. What is stateful packet filtering? Give one example where it is advantageous.

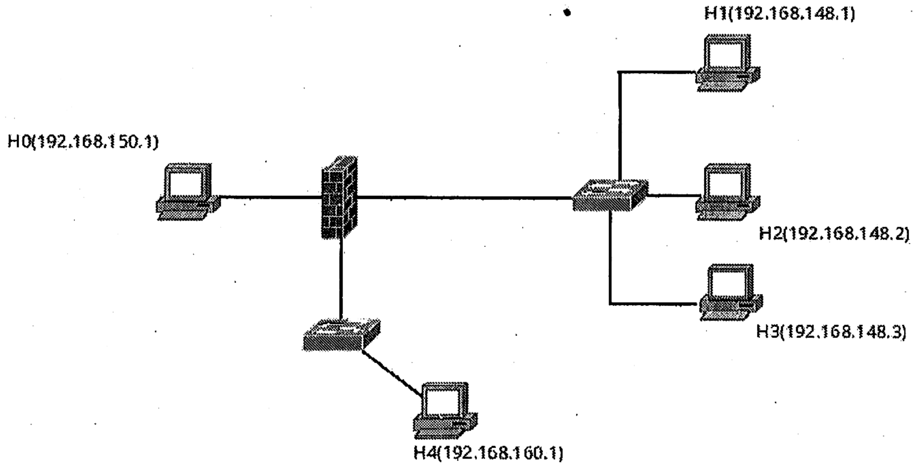
   C. Consider the following network configuration. Generate rules for the packet filtering firewall to implement the following access control policies.

   i. H0 can only access the web service (TCP port 80) at H4.

   ii. Only the web service at H4 can access the database service (TCP port 3306) at H1.

   iii. H2 and H3 can access any UDP services in other networks.

   iv. All other network traffic are blocked.



$4 + 2 + 4 = 10$

[Turn over

3. A. An organization is assigned the block 2000:1110:1287/48. Determine the global unique IPv6 address of an interface in the first subnet (subnet id all 0's), if the Ethernet MAC address of the computer is F5-A9-23-14-7A-D2.

   B. Identify the correct order in which the following actions take place in an interaction between a web browser and a web server.

      i. The web browser requests a webpage using HTTP.
      ii. The web browser establishes a TCP connection with the web server.
      iii. The web server sends the requested webpage using HTTP.
      iv. The web browser resolves the domain name using DNS.

   Provide necessary justifications.

   C. Differentiate between link-local unicast and site-local unicast IPv6 addresses.

   D. How does IPv6 handle fragmentation?

$4 + 2 + 2 + 2 = 10$

Group B (Total Marks: 14) [CO3]
[Answer Any One]

4. A. Explain how the pre master secret is established in SSL handshake protocol using (i) Ephemeral Diffie-Hellman and (ii) Anonymous Diffie-Hellman key exchange algorithms.

   B. Differentiate between SSL session and SSL connection. What are the different parameters associated with these two entities?

   C. Explain how SSL record protocol processes application data before handing it over to TCP.

   D. What is the role of SSL change cipher spec protocol?

$6 + 3 + 3 + 2 = 14$

5. A. Though HTTP is a stateless protocol, user behavior can be tracked. –Justify the comment.

   B. How can HTTP be extended to address the problem of intermittent internet connectivity?

   C. State the limitations of Websocket protocol. State its advantages over HTTP.

$3 + 5 + 6 = 14$

Group C (Total Marks: 30) [CO4]
[Answer Any Two]

6. A. A restaurant deploys a web application for taking online orders. Write a simple chatbot in Node.JS that would communicate the menu with the customers. State the application layer protocols utilized by the application.

   B. Did you utilize Observer/Event Emitter pattern in the code? Justify your answer.

   C. Discuss the role of event demultiplexer in Node.JS. State the design pattern associated with it.

$7 + 4 + 4 = 15$

7. A. Write a Node.js application to push a static advertisement page to the client after the client has connected to the server.

   B. Write the role of object relational mapping in extracting information from the database w.r.t Spring/Express framework. Give suitable code snippets.

   C. Write an echo message service using Express/Spring framework that echos back the input given by the client. Ensure that HTTP protocol is in place.

   D. State the advantages of Spring over Express framework.

$5 + 4 + 4 + 2 = 15$

8. A restaurant deploys a web application for taking online orders. The team plans to provide a list of customized platters for 'home delivery' apart from the 'dine-in' option. Answer the following if the application is developed using the Spring framework.

   A. How can dependency injection be implemented in this application? Clearly show the Controller and associated classes and interfaces.

   B. What is data marshalling? Explain with necessary code snippets.

   C. Differentiate between @*Controller* and @*RestController*.

$8 + 5 + 2 = 15$

Group D (Total Marks: 36) [CO5]
[Answer Any Three]

9. A. What is authorization?

   B. How is user authentication invoked in the request-response workflow by the Spring framework?

   C. A web server hosts a forum. It does not check the comments posted by the users for any security threat. How could this web server pose a security threat to another web application hosted at a different server? Create a solution for the problem utilizing Spring/Express framework.

$2 + 4 + 6 = 12$

10. A. Discuss the authentication service provided by Spring framework when you include $spring - boot - starter - security$ dependency in your code.

   B. Discuss the problem of cross-site request forgery. What is the role of CORS here?

   C. Discuss the notion of 'Data at rest' and 'Data in transition'.

$5 + 5 + 2 = 12$

11. A. State how keys are generated in RSA.

   B. In a secure communication, the RSA public and private keys are chosen as (7, 33) and (3, 33) respectively. Show the encryption of a message `m=2` and the decryption of the corresponding cypher text using these keys.

   C. Explain, why use of public key cryptography is avoided in communications where only confidentiality is required.

   D. Assume you can only use a hash function H and a shared secret S. Show how user A would transmit a message M to user B so that both message authentication and integrity are guaranteed. You should not use any encryption. Provide necessary justifications.

$3 + 3 + 2 + 4 = 12$

12. A. What is a digital certificate? What information does it contain?

   B. What is the role of a certification authority? What is a root certification authority? How does a root certification authority get its own certificate?

   C. During an secure online banking session with bank X, your browser receives a digital certificate of bank X. Explain how does your browser verifies the authenticity of the digital certificate of bank X. Assume that, bank X has obtained its digital certificate from certification authority Y and Y has a self-signed digital certificate.

$3 + 4 + 5 = 12$