國立雲林科技大學資訊管理系

113 學年度第 1 學期博士班資格考 (Ph.D. Qualify Exam)

考試科目 (Subject)：資訊網路 (Computer Networking)

時數與方式 (Hour and type)：四小時 (4 hours)

Close book, 不可使用計算器 (Calculators not allowed)

**Part 1**: 60 points (Optional Questions: Answer 3 out of 4, 20 points each; if you answer more than 3 questions, only the first 3 answered questions will be graded.)

1. You have recently purchased a new wireless router to integrate with your existing cable modem for home networking. Your Internet Service Provider (ISP) employs a dynamic IP address assignment system, wherein only a single public IPv4 address is allocated to your external interface (the router's WAN port). Within your home network, five devices (all computers) connect wirelessly to this router, utilizing the IEEE 802.11 (Wi-Fi) protocol.
   a. How are IP addresses managed for the five internal devices within your home network? Discuss the mechanisms and protocols involved in distributing addresses to internal devices. What specific address types are used, and how does the addressing scheme ensure proper communication both within the local network and with external internet resources?
   b. Does the wireless router employ Network Address Translation (NAT)? If so, explain in detail how NAT is used to manage multiple internal devices behind a single public IP address.
   c. Examine the security implications of using NAT in this home network scenario. What risks might arise from this configuration, and what protective measures can be implemented to mitigate potential vulnerabilities associated with NAT? Does NAT provide any level of inherent security, particularly against unsolicited inbound traffic? How might advanced techniques like stateful packet inspection or port forwarding play a role in conjunction with NAT in this environment?

2. Given the wide variety of protocols in modern networking, different application-layer protocols serve specialized roles in facilitating communication and resource exchange across networks. Consider four foundational protocols: HTTP, FTP, SMTP, and DNS.
   a. Provide a comprehensive breakdown of its purpose, typical usage scenarios, and the processes involved in its functioning (e.g., connection establishment, request/response cycle, command/response interaction).
   b. Examine the underlying transport layer protocols (TCP/UDP) utilized by each of these protocols and explain the implications of these choices for reliability,

performance, and data flow control.

c. Assess the error detection, correction, and recovery mechanisms of each protocol. What strategies are used to ensure data integrity and delivery, and how do these protocols handle packet loss, retransmission, and timeouts? Discuss the role of handshaking, acknowledgments, and retries in maintaining reliability.
d. Explore the inherent security vulnerabilities in each protocol (e.g., plaintext transmission in FTP and SMTP). Consider the role of modern security enhancements such as HTTPS, SFTP, SMTPS, and DNSSEC. How does each protocol balance security concerns with performance overhead in securing data transmission and authentication?

3. As multimedia data transmission over the Internet becomes increasingly prevalent, several challenges arise due to the diverse requirements of different media types and the limitations of network infrastructure.
   a. Compare different technologies and protocols designed for multimedia streaming and real-time data transport over the Internet, including RTP (Real-time Transport Protocol), RTSP (Real-time Streaming Protocol), HTTP-based streaming (e.g., HLS, DASH), and WebRTC.
   b. How do these technologies handle critical factors like latency, packet loss, synchronization, and adaptive bitrate streaming? What strategies do they employ to maintain smooth playback and minimize buffering under varying network conditions?
   c. In what scenarios would you choose RTP/RTSP over HTTP-based streaming (or vice versa)? Provide a detailed comparison of their strengths and weaknesses in specific application domains, such as live video conferencing, on-demand video streaming, and interactive multimedia applications.

4. Describe the principles and mechanisms of IP addressing, including the concepts of subnetting and supernetting. How does CIDR (Classless Inter-Domain Routing) improve the efficiency and flexibility of IP address allocation compared to the traditional classful addressing system?

**Part 2**: 40 points (Optional Questions: Answer 4 out of 6, 10 points each; if you answer more than 4 questions, only the first 4 answered questions will be graded.)

5. Suppose nodes A, B, and C are connected to the same broadcast LAN (e.g., Ethernet). If node A sends a large number of IP datagrams to node B, with each Ethernet frame addressed to B's MAC address, will node C's network adapter process these frames? Will C's network layer handle the IP datagrams? How would your answer change if A sends the frames using the MAC broadcast address?

6. Discuss the key features and operational methods of the 802.11 wireless network protocol. What is mobility management, and how is it implemented in mobile networks?

7. Explain the Internet's five-layer protocol stack. What are the primary functions and protocols associated with each layer?

8. What are the key differences between TCP and UDP? In what situations would you choose to use TCP over UDP and vice versa?

9. Explain the ARP protocol and its role between the network layer and the data link layer. What are the basic concepts and operational methods of Ethernet?

10. Explain common network attack types (such as DDoS attacks and phishing attacks) and corresponding defense measures. What is Public Key Infrastructure (PKI), and how does it secure network communications?