

1. (20%) 802.11 WEP
 - a. Why is 802.11 WEP (with RC4) vulnerable to attacks? Please described as detailed as you can.
 - b. If the initial vector (IV) is encrypted during transmission, can the WEP approach work against attacks? Why or Why not?

2. (20%) Multimedia Networking Applications:
 - a. How should the Internet evolve to better support multimedia? Please elaborate on the three kinds of the solution philosophy, i.e., (i) integrated services philosophy, (ii) differentiated services philosophy, and (iii) laissez-faire.
 - b. Why do we need client buffering for multimedia networking applications? Please draw a figure for explanation.

3. (20%) Circuit switching vs. packet switching
 - a. What advantage does a circuit-switched network have over a packet-switched network?
 - b. Given a 1Gbps link, users are generating data at a rate of 100kbps when busy, but are busy generating data only with probability $p=0.1$. Consider packet switching and a user population of M users. Give a formula (in terms of p , M , N) for the probability that more than N users are sending data.

4. (20%) Domain Name System (DNS)
 - a. Why not implementing a centralized database for domain name system?
 - b. Bob accesses the Internet at home via a dynamic IP maintained by HiNet. If Bob would like to install a web server at home with the domain name "bobhome.idv.tw". Please elaborate on how Bob registers and activates the domain name. Note that the provider of "idv.tw" is "TWNIC", and the authoritative DNS server is "ns1.twnic.net.tw".

5. (10%) TCP slow start and TCP futures
 - a. Describe the basic operation of TCP slow start. What are the main advantages of TCP slow start that have made it a success in Internet?
 - b. Why are new versions of TCP for high-speed transmission needed?

6. (10%) Compare inter-AS routing protocol with intra-AS routing protocols in the Internet.