Câu 1: **C**

Địa chỉ nút mạng: 217.65.82.153 ⇔ 11011001.01000001.01010010.10011001

Địa chỉ subnet mask của mạng: 255.255.255.248 ⇔ 11111111.11111111.11111111.11111000

Thực hiện phép toán AND giữa hai địa chỉ trên để tìm địa chỉ vùng mạng ban đầu:

➔ 11011001.01000001.01010010.10011000 ⇔ 217.65.82.152/29

Mỗi vùng mạng có HostID chiếm 3 bit => có 2^3 = 8 host trong mỗi vùng mạng

⇨ Địa chỉ IP của các host trong vùng mạng này lần lượt là : 217.65.82.152, 217.65.82.153, 217.65.82.154,..., 217.65.82.158

Câu 2: **D**

địa chỉ IP 223.112.15.143/21 ⇔ 11011111.01110000.00001111.10001111

Vùng mạng này có NetoworkID chiếm 21 bits, HostID chiếm 11 bits

⇨ Địa chỉ SubnetMask: 11111111.11111111.11111000.00000000

Thực hiện phép toán AND giữa hai địa chỉ trên để tìm địa chỉ vùng mạng ban đầu:

➔ 11011111.01110000.00001000.00000000 ⇔ 223.112.8.0/21

➔ Địa chỉ Broadcast là (phần host toàn bit 1): 11011111.01110000.00001111.11111111 ⇔ 223.112.15.255

Câu 3: **C**

Câu 4:**C**

Địa chỉ IP của vùng mạng là 172.16.10.0/23 ⇔ 10101100.00010000.00001010.00000000

→ vùng mạng này NetworkID chiếm 23 bits, HostID chiếm 9 bits

Địa chỉ broadcast của vùng mạng:

10101100.00010000.00001011.11111111 ⇔ 172.16.11.255

Các địa chỉ IP có thể gán cho các host trong vùng mạng này từ 172.16.10.1 (10101100.00010000.00001010.00000001) → 172.16.11.254 (10101100.00010000.00001011.11111110)

Câu 5: **A**

Áp dụng quy tắc “Longest Matching” → địa chỉ IP khớp nhiều nhất với địa chỉ IP trong interface 0

Câu 6: **B**

Xác định vị lỗi theo quy tắc mã chẵn → lỗi ở hàng 5 cột 4

Câu 7: **B**

Câu 8: **B**

Câu 9: **B**

Câu 10: **D**

Câu 11: **D**

Địa chỉ vùng mạng là 192.168.100.0/24 → 11000000.10101000.01100100.00000000
Vùng mạng này có NetworkID là 24 bits, HostID chiếm 8 bit → mạng lớp C
Chia vùng mạng này thành 8 mạng con → cần mượn HostID 3 bits vì 2^3 =8 mạng con
Số host có tối đa trong mỗi vùng mạng $2^{8-3} - 2$ = 30 host
Subnet Mask mới của vùng mạng con: 11111111.11111111.11111111.11000000

➔ 255.255.255.224

Câu 12: D
Câu 13: D
Netmask: 255.255.240.0 ⇔ 11111111.11111111.11110000.00000000

➔ Phần subnet có 4 bits 1 mượn từ phần HostID
➔ Số vùng mạng con (subnet) có thể có là 2^4 = 16

Câu 14: A
Câu 15: D
Câu 16: D
Câu 17: A
Subnet Mask của mạng con: 255.255.224.0 ⇔ 11111111.11111111.11100000.00000000 và là địa chỉ mạng lớp B

➔ Vùng mạng này có SubnetID chiếm 3 bits

Địa chỉ đầu của vùng mạng (SubnetID): 143.169.64.0/19 ⇔ 10001111.10101001.010 00000.00000000

➔ Địa chỉ broadcast của vùng mạng:10001111.10101001.01011111.11111111 ⇔ 143.169.95.255/19

Câu 18: B
Câu 19: A
Câu 20: D
Các thành phần của HTTP Request

1. Request Method:
   - Đây là phương thức HTTP được sử dụng, chẳng hạn như GET, POST, PUT, DELETE, etc.
   - Nó xác định hành động cần thực hiện với tài nguyên.
2. Request URI:
   - Đây là URI (Uniform Resource Identifier) của tài nguyên được yêu cầu, ví dụ như /index.html hoặc /api/data.
   - Đây là đường dẫn đến tài nguyên trong máy chủ.
3. Request Version:
   - Phiên bản của giao thức HTTP được sử dụng, chẳng hạn như HTTP/1.1 hoặc HTTP/2.0.

- Nó xác định phiên bản giao thức mà cả client và server đang sử dụng để giao tiếp.

4. Accept:
   - Đây là một trường tiêu đề mà client gửi để chỉ định loại nội dung (MIME types) mà nó có thể xử lý, ví dụ: text/html, application/json.
   - Server sẽ sử dụng thông tin này để trả về nội dung phù hợp nhất với yêu cầu của client.
5. Accept-Language:
   - Trường này xác định ngôn ngữ ưu tiên của client, ví dụ: en-US, fr, vi.
   - Server có thể sử dụng ngôn ngữ này để trả về nội dung bằng ngôn ngữ tương ứng nếu có sẵn.
6. Upgrade-Insecure-Requests:
   - Thông báo cho server rằng client chấp nhận nâng cấp các yêu cầu HTTP từ http lên https.
   - Giá trị thường là 1 nếu client yêu cầu nâng cấp, ví dụ: Upgrade-Insecure-Requests: 1.
7. User-Agent:
   - Trường này chứa thông tin về phần mềm client (trình duyệt hoặc ứng dụng) đang gửi yêu cầu, ví dụ: Mozilla/5.0....
   - Thông tin này có thể bao gồm loại trình duyệt, hệ điều hành và phiên bản phần mềm.
8. Accept-Encoding:
   - Định rõ kiểu mã hóa mà client hỗ trợ, như gzip, deflate.
   - Server có thể nén nội dung trước khi gửi về cho client dựa vào các mã hóa được hỗ trợ.
9. Host:
   - Địa chỉ tên miền hoặc địa chỉ IP của server mà client đang gửi yêu cầu.
   - Trường này đặc biệt quan trọng khi có nhiều trang web được lưu trữ trên cùng một server.
10. Connection:
    - Xác định xem kết nối sẽ được giữ mở (keep-alive) hay đóng sau khi hoàn tất yêu cầu (close).
11. Authorization:
    - Thông tin xác thực của client, thường chứa mã hóa Base64 của tên người dùng và mật khẩu.
    - Được dùng trong các kết nối yêu cầu xác thực (Authentication).
12. Credentials:
    - Chi tiết xác thực của client (thường đi cùng với trường Authorization).
    - Được sử dụng để kiểm tra quyền truy cập.
13. Full Request URI:

- Đây là URI đầy đủ của tài nguyên được yêu cầu, bao gồm cả giao thức và tên miền, ví dụ: https://www.example.com/index.html.

14. [HTTP Request 1/1]:
    - Cho biết đây là yêu cầu HTTP đầu tiên và duy nhất trong gói tin này.
    - Con số này sẽ thay đổi nếu có nhiều yêu cầu HTTP trong cùng một kết nối TCP.
15. Respond in frame: [Số Frame]:
    - Tham chiếu đến frame chứa phản hồi HTTP từ server.
    - Bạn có thể nhấp vào số frame trong Wireshark để di chuyển đến frame phản hồi tương ứng.

Câu 21: C

Câu 22: C

mạng lớp C với Subnet Mask là 255.255.255.192 ⇔ 11111111.11111111.11111111.11000000

➔ SubnetID chiếm 2 bit → có 2^2 =4 mạng con và số host tối đa trong mỗi mạng con là 2^{8-2} -2= 62

Câu 23: A

Câu 24: C

Câu 25: A

Câu 26: B

Để xác định gói tin nào sẽ được chuyển tiếp đến mạng A, ta cần kiểm tra xem địa chỉ đích của gói tin có nằm trong phạm vi địa chỉ của mạng A hay không

Mạng A có subnet mask 255.255.248.0 ⇔ 11111111.11111111.11111000.00000000

➔ Các địa chỉ IP trong Mạng A có NetworkID chiếm 16 bits, HostID chiếm 11 bits, SubnetID chiếm 5 bits

➔ Số host tối đa trong mạng A là 2^{32-21}-2=2046

Mạng A bắt đầu với địa chỉ IP là SubnetID 205.16.32.0 ⇔ 11001101.00010000.00100000.00000000

Địa chỉ broadcast mạng A là: 11001101.00010000.00100111.11111111 ⇔ 205.16.39.255 → chỉ có địa chỉ 205.16.37.44 thuộc mạng này

Câu 27: B

Câu 28: A

sự tắc nghẽn do nhận được 3 ACKs trùng khi tại round đó cwnd bị giảm giá trị đi một nửa so với cwnd trước đó (theo cơ chế Fast Retransmit)→ tại round thứ 26

Câu 29: B

Ban đầu ssthresh = 8, tại round 22 xảy ra sự kiện timeout (cwnd=1) nên ssthresh= cwnd(22)/2 = 26/2=13

Câu 30: D

Ở giai đoạn slow start-> cwnd sẽ tăng theo cấp số nhân (x2)

Câu 31: D

Do mạng chuyển mạch gói "store-and-forward" yêu cầu truyền tải toàn bộ gói tin qua router trước khi gửi tiếp gói tin đi, thời gian để bit đầu tiên của gói tin từ máy A đến máy B sẽ là:

$$T = \frac{L}{R} = \frac{8 * 10^6\ (bits)}{10 * 10^6\ (bps)} = 0.8s = 800ms$$

Câu 32: C

Câu 33: B

Câu 34: A

Câu 35: C

Lớp A: Địa chỉ IP có phần đầu từ 0 đến 127. (tức là 0.0.0.0 đến 127.255.255.255)
Lớp B: Địa chỉ IP có phần đầu từ 128 đến 191. (tức là 128.0.0.0 đến 191.255.255.255)
Lớp C: Địa chỉ IP có phần đầu từ 192 đến 223. (tức là 192.0.0.0 đến 223.255.255.255)

➔ Địa chỉ 10.1.1.1 thuộc lớp A.

Câu 36: B

A. 101000100010

1. Thực hiện phép chia nhị phân: 10011101000100110÷10011.
2. Kết quả phần dư là: **0** (không có lỗi).

B. 101000100010

1. Thực hiện phép chia nhị phân: 101000100010÷10011101000100010 \div 10011101000100010÷10011.
2. Kết quả phần dư là: **101** (có lỗi).

C. 101000100011

1. Thực hiện phép chia nhị phân: 101000100011÷10011101000100011 \div 10011101000100011÷10011.
2. Kết quả phần dư là: **11** (có lỗi).

D. 101000100111

1. Thực hiện phép chia nhị phân: 101000100111÷10011101000100111 \div 10011101000100111÷10011.
2. Kết quả phần dư là: **0** (không có lỗi).

Kết luận:

Dữ liệu nhận **A (101000100110)** và **D (101000100111)** không có lỗi vì phần dư sau phép chia là 0.

Câu 37: C

Câu 38: C

Câu 39: B

Câu 40: C

1. Địa chỉ trong dải riêng (Private Addresses):
    - 192.168.0.0 - 192.168.255.255 (Lớp C) là một dải địa chỉ riêng, không được phép sử dụng trên Internet mà chỉ được sử dụng trong các mạng nội bộ.
2. Địa chỉ loopback:
    - 127.0.0.0 - 127.255.255.255 là dải địa chỉ dành cho loopback, nghĩa là các địa chỉ này chỉ dùng để giao tiếp trong máy tính, không thể sử dụng trên mạng Internet.

Phân tích các địa chỉ trong câu hỏi:

- A. 192.168.98.20: Thuộc dải địa chỉ riêng 192.168.x.x, nên không thể sử dụng trên mạng Internet.
- B. 126.0.0.1: Thuộc dải Lớp A, từ 1.0.0.0 đến 127.255.255.255, nhưng 127.0.0.0 - 127.255.255.255 là dải loopback, không thể dùng trên mạng Internet. Dù vậy, 126.0.0.1 vẫn có thể được sử dụng trên Internet vì nó nằm ngoài dải loopback.
- C. 201.134.1.2: Đây là một địa chỉ IP hợp lệ trong dải công cộng, có thể dùng trên mạng Internet.
- D. Tất cả các câu trên: Không phải tất cả các địa chỉ đều không thể dùng trên mạng Internet, vì 126.0.0.1 và 201.134.1.2 có thể sử dụng được.