< 과제 2: pcap 라이브러리 공부 및 샘플 프로그램 해석 >

1. 개요

- 리눅스 상에서 패킷을 잡는 기법에 대하여 공부한다. 구체적으로 pcap library와 관련 테크닉을 공부하고 예제 프로그램을 해석한다. 참고로 본 예제 프로그램은 앞으로 개발할 SimTL의 기초가 되므로 완벽한 이해가 필수적이다.

2. 과제 내용

- 인터넷 자료를 참조하여 pcap library를 공부한다.
- 리눅스에서 pcap library를 사용하여 패킷을 잡아보기" 자료에 있는 프로그램을 해석하고, 중요 테크닉을 공부한다.
  - 프로그램을 해석하여 상세한 순서도(flowchart) (2쪽 이상)를 작성한다.
    - 각 프로토콜에 대한 구조체, ether_header, iph, 등은 앞으로 각 프로토콜 분석 기능 추가시 공부할 것이므로 생략
  - C언어에서 포인터와 함수형 포인터가 뭔지 공부한다.
  - 사용할 수 있는 필터링 기능과 방법에 대해 다음과 같이 공부하고 연습해본다.
    - tcpdump가 무엇인지 알아본다.
    - tcpdump가 지원하는 primitives(패킷 필터링 기능임)을 상세히 공부하고 사용해본다.
- 리눅스에서 pcap library를 사용하여 패킷을 잡아보기" 자료에 있는 프로그램을 리눅스 상에서 수행시켜서 실제 패킷을 잡아본다. (버그가 있으면 해결할 것)

3. 과제 보고

- 반드시 과제보고서 작성 및 제출방법 (홈피 자료 참조)에 따라 작성하여 제출할 것
- 추가적으로 포함시킬 내용
  A. 공부한 내용
  B. 순서도
  C. 프로그램과 수행 결과 예 (수행결과는 화면 캡쳐할 것)
  D. 기타