# 네트워크 분석에 대한 정의

* 네트워크 트래픽을 살펴보고, 분석하는 것.
* 다음은 와이어샤크를 사용해 수행될 수 있는 분석 작업의 목록이다.
* l 네트워크상에서 최상위 전달 의뢰자Talker 찾기
* l 사용 중인 프로토콜과 애플리케이션 식별하기
* l 연결된 모든 네트워크 트래픽과 애플리케이션에 평균 초당 패킷율과 초당 바
* 이트율 결정하기
* l 통신 중인 모든 호스트 나열하기
* l 데이터 전송 애플리케이션에 의해 사용되는 패킷의 길이 알기
* l 가장 일반적인 연결 문제들 바로 알기
* l 느린 처리로 인한 클라이언트 요청들 사이에 생기는 지연 관찰하기
* l 잘못 구성된 호스트 위치 알아내기
* l 파일 전송이 느려지는 호스트와 네트워크 폭주 탐지하기
* l 비동기 트래픽 우선순위 식별하기
* l 웹사이트로 보내지는 속도를 시험하기 위한 HTIP 흐름을 그래프로 나타내기
* l 네트워크상에서 특이한 스캐닝 트래픽 식별하기
* l 클라이언트와 서버 오류를 나타내는 HTTP 오류 응답 빨리 식별하기
* l 클라이연트， 서벼와 광범위한 오류를 나타나는 VoIP 오류 응답 빨리 식별하기
* l 트래픽의 동작을 비교하기 위한 그래프 생성하기
* l 애플리케이션 처리량을 그래프로 그리고， 전체 링크 트래픽 화변 비교하기
* l 암호화하지 않은 트래픽 애플리케이션 식별하기
* l 네트워크 트래픽에서 다양한 네트워크 문제의 영향을 알기 위해 VoIP 통신의
* 재생하기
* I 수동적인 운영체제와 애플리케이션 사용 탐지 수행하기
* l 네트워크에서 특이한 프로토콜과 인식할 수 없는 포트 번호 사용 관찰하기
* I 네트워크에서 호스트와 애플라케이션의 시작 프로세스 검사하기
* l 평균 서비스 응답 시간SRT. Service Response Time과 용납할 수 없는 SRT 식별하기
* l 주기적인 패킷 생성 애플리케이션과 프로토콜의 간격을 그래프로 그리기

# 스위치

* 스위치에 패킷이 도착하면 스위치는 패킷 내의 체크섬(Checksum)을 확인하고, 패킷의 체크섬이 틀리면 그 패킷은 ‘불량’으로 간주해 폐기합니다. 체크섬에 문제가 없으면 스위치는 패킷의 목적지 MAC 주소를 검사하고, 목적지 MAC 주소를 이용해 스위치의 어느 포트가 호스트에 연결되어있는지를 결정하기 위해 MAC 주소 테이블을 참조합니다. MAC 주소 테이블에 대상 MAC 주소가 없다면 스위치는 응답을 통해 대상 MAC 주소를 찾기 위해 모든 포트로 패킷을 전송한다. 그후, 스위치가 자신의 테이블에 있는 해당 MAC 주소를 가졌다면 스위치는 그 패킷을 해당 포트로 전달한다. 브로드캐스트는 스위치의 모든 포트로 전달된다. 다르게 설정되어 있다면 멀티캐스트도 스위치의 모든 포트로 전달됩니다.

# 라우팅

* 라우터는 IP 헤더 내의 IP 주소를 기반으로 패킷을 전달한다. 라우터의 MAC 주소로 패킷을 보낼 때 라우터는 패킷이 유효한지 확인하기 위해 체크섬을 검사하고, 체크섬이 정확하지 않으면 패킷을 폐기한다. 체크섬이 정확하면 라우터는 MAC 헤더(이더넷 헤더와 같은)를 제거하고 TTL(Time to Live)내의 값과 패킷의 목적지를 식별하기 위해 IP 헤더를 검사한다. 패킷이 너무 오래된 것이면(TTL 값이 1이면), 라우터는 패킷을 폐기하고, 송신자에게 ICMP TTL 초과 메시지를 전송한다. 그 후, 라우터는 목적지 IP 네트워크를 결정하기 위해 라우팅 테이블을 참조한다. 라우터가 대상 네트워크에 직접 연결되어 있다면 라우터는 패킷을 보낼 수 있다. 라우터는 IP 헤더의 TTL 값을 감소시키고, 패킷을 전달하기 전에 새로운 MAC 헤더를 생성해 적용한다. 대상 네트워크가 로컬 네트워크에 연결되어 있지 않으면 라우터는 패킷을 라우팅 테이블을 참조할 때 알게 된 다음 홉 라우터로 전송한다. 라우터는 주소 지정 정보를 기반으로, 패킷을 허용하거나 차단하는 규칙을 포함할 수 있다. 대부분의 라우터는 방화벽 기능을 제공하고 또 다른 특징을 기반으로 트래픽을 차단하거나 허용할 수 있다.

# 방화벽

* 방화벽(Firewall)은 규칙을 기반으로 트래픽을 검사해 통신을 허용하거나 차단하기 위해 만들어 졌다. 예를 들어 방화벽이 외부의 호스트에서 내부 서버의 21번 포트로 향하는 모든 TCP 연결을 차단할 수 있다. 기본적으로 방화벽은 OSI 3 계층인 네트워크 계층에서 동작한다. 이런 측면에서 방화벽은 네트워크 트래픽을 처리할 때 라우터처럼 동작한다. 방화벽은 방화벽 규칙에 의해 차단되지 않는 트래픽만 전달한다. 방화벽은 패킷을 전달하기 전 패킷 앞에 새로운 MAC 헤더를 추가한다. 또한 방화벽이 네트워크 주소 변환(NAT, Network Address Translation)이나 프록시 기능 같은 추가 기능을 제공한다면 패킷에 변화가 발생한다. NAT 시스템은 클라이언트 사설 IP 주소를 숨길 때 사용되며, 기본 NAT 시스템은 패킷의 발신지와 목적지 IP 주소를 간단히 변경하고, 회신 시 트래픽을 제대로 전달하기 위해 테이블에서 연결 관계를 추적한다. 또한 포트 주소 변환(PAT, Port Address Translation) 시스템을 포트 정보를 변경해 단일 아웃바운드 주소를 사용할 때 다중 내부 연결들을 역다중화하는 방법으로 사용한다. 또한 프록시 서버도 트래픽에 영향을 미친다. 표준 방화벽을 사용할 때 보이는 통신과 달리 클라이언트는 프록시 서버에 연결하고, 프록시 서버는 대상과 다른 연결을 한다. 이런 통신을 트러블슈팅할 때 검사하려면 두 연결을 완전히 분리해야한다.