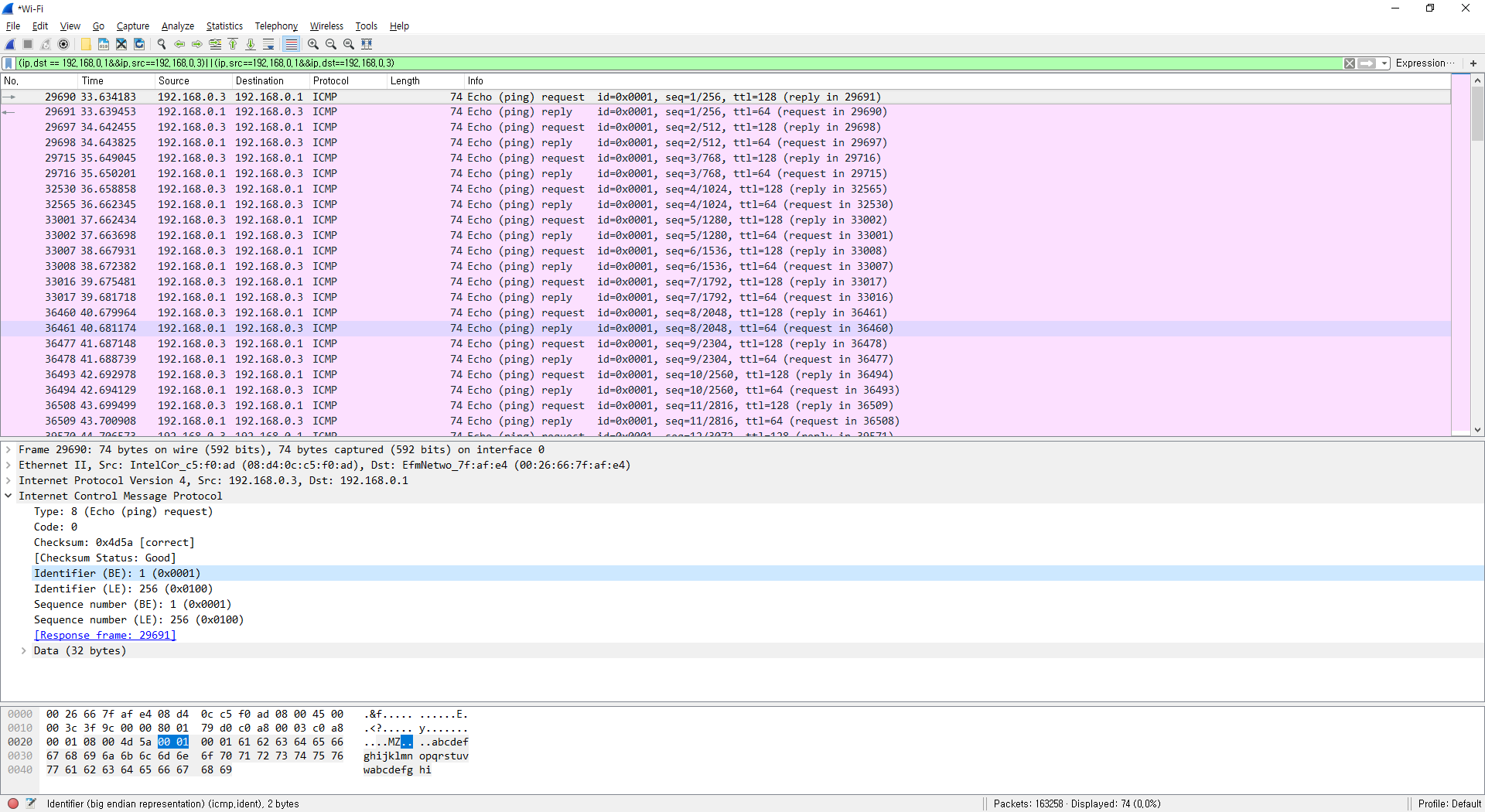
# 와이어샤크 ICMP (핑) 분석 (실전)



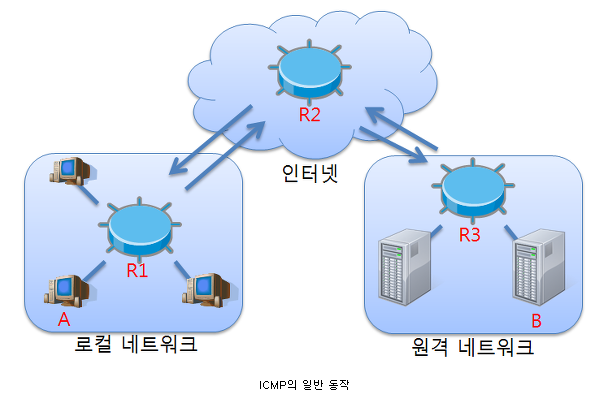
# ICMP < 출처 : <http://blog.daum.net/tlos6733/38> >

* ICMP는 TCP/IP 프로토콜에서 가장 단순한 프로토콜. 대부분의 프로토콜은 네트워크 스택이나 어플리케이션의 동작을 수행하기 위한 종류의 기능을 구현하지만, ICMP는 이름(Internet Control Message Protocol)에서 알 수 있듯이 제어 메시지를 정의하는 프로토콜이다. 그래서 대부분의 ICMP는 IP장비가 다른 장비에게 제어 메시지를 보낼 수 있는 방법을 제공하는 것과 관련이 있다.

(1). ICMP 메시지 전달 서비스

ICMP는 다양한 유형의 정보를 교환할 수 있도록 하는 다양한 메시지 유형을 정의하는 역할. 이들 메시지는 에러를 보고하거나 IP가 원활히 동작할 수 있도록 필요한 여러 중요 정보를 교환하기 위해 생성. ICMP 자체는 서로 다른 ICMP 메시지가 어떻게 쓰이는지를 정의하지는 않음. 즉, 메시지의 실제 용도는 그 메시지를 이용하는 프로토콜에 의해 정의되어 짐. 이러한 방법으로, ICMP는 다른 프로토콜에 간단한 메시지 전달 서비스를 제공한다.

(2). ICMP 일반 동작



ICMP는 일반적으로 IP 메시지 전송에 대한 피드백을 제공하는 데 쓰이며, 이 그림에서 장비 A는 장비 B에 IP 데이터 그램을 송신하고자 한다. 그렇지만 데이터 그램이 R2에 도달했을 때 어떤 문제가 발생하여 데이터 그램이 손실 되었다. 라우터 R2는 ICMP 메시지를 장비 A에게 되돌려 보내어 문제가 발생했다는 사실을 알린다. 이 때 가능하면 장비 A가 그 문제를 고치는 데 필요한 정보까지 같이 보낸다. 라우터 R2는 오직 장비 A로만 ICMP 메시지를 송신할 수 있고, 라우터 R1이나 R3로는 송신할 수 없다.

(3). ICMP 에러보고

ICMP 동작의 한가지 특성은 어떤 에러가 발생하여 ICMP를 통해 그 사실을 알릴 때, 오직 데이터 그램의 최초 출발지로만 알릴 수 있다는 것이다. 사실 이것은 ICMP 동작 방법의 큰 단점입니다. 위의 그림에서는 호스트 A가 호스트 B에게 메시지를 보내는데 라우터 R2에서 데이터 그램의 문제를 탐지했을 때, 라우터 R2는 그 문제가 이전에 메시지를 처리한 라우터 중 하나에서 (예를 들어 라우터R1) 발생했다고 의심할 수 있지만 그 사실을 라우터 R1에게 보고할 수 없다. 즉, 라우터 R2는 ICMP 메시지를 오직 호스트 A로만 보낼 수 있다.

C:\Users\Hans\AppData\Local\Microsoft\Windows\INetCacheContent.Word\ICMP Ipv4 2.png

이러한 제한은 IP 동작 방식 때문에 생겼다. IP 데이터 그램 포맷에 있는 주소 필드는 오직 최초 출발지 주소(Src)와 최종 목적지(Dst) 밖에 없기 때문이다. 라우터R2가 라우터R1 으로부터 데이터 그램을 받았을 때 그 데이터 그램 안에 들어 있는 것은 오직 장비 A의 주소(Src)다. 그래서 라우터R3는 문제 보고를 장비 A로만 송신해야 하며 장비 A는 그 보고를 어떻게 해야 할지 결정해야 한다. 장비 A는 사용하는 경로를 바꿀 수도 있고 관리자가 라우터 R1이 문제를 해결하는 데 사용할 수 있는 에러 보고서를 생성할 수도 있다.

(4). ICMP 메시지 생성과 처리

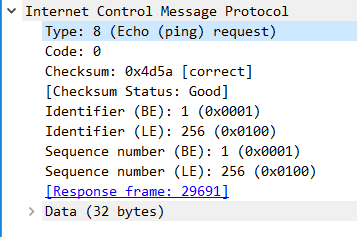
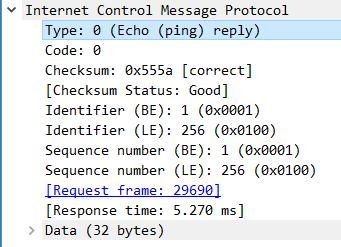
ICMP는 IP의 보조적인 프로토콜이기 때문에 IP의 자원을 너무 많이 소모하지 않고 IP의 기능을 도와야 한다. 여기서 IP의 자원은 대역폭이다. ICMP 메시지는 중요하지만, 네트워크 운영 중 발생하는 부하의 일부로 간주되어야 한다. ICMP 메시지는 사용자 데이터를 담고 있지 않기 때문에 ICMP로 인한 대역폭 낭비는 장비 전체 대역폭의 극히 일부분이다. 그래서 꼭 필요한 경우에만 ICMP 메시지를 보내고, ICMP 메시지가 생성되는 상황을 신중히 제어해야 한다.

(5). ICMP 트래픽 분석

‘일반’ ICMP 트래픽을 주관하는 네트워크로 정의하기는 어렵다. 일부 네트워크 IT 사의 직원은 연결을 수행하기 위해 ping을 사용하는 반면에 다른 회사들은 ICMP 에코 요청과 응답을 제한한다.

1). 기본 ICMP 트래픽

Ping 요청을 해보았을 때, ‘정상 ICMP 트래픽’일 경우, ICMP 기반 ping에서 에코 요청에 대해 ICMP 유형 8을 사용하며, 에코 응답에는 ICMP 유형 0을 사용되어집니다.

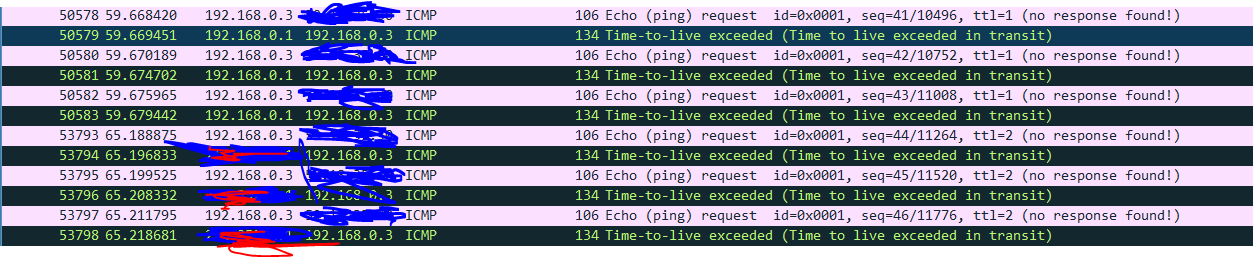


2). Traceout

ICMP 기반, TCP 기반, IDE 기반의 3가지 다른 traceroute가 있다. ICMP 기반 traceroute는 IMCP 에코 요청을 사용하며, IP 헤더에 Time to Live (TTL)값을 수정한다. 경로를 따라 라우터에 도착한 패킷처럼 들어오는 TTL 값은 검사가 되었다. 들어오는 TTL 값이 1이면 라우터는 ICMP 시간초과(Time to Live 초과 – 유형5, 코드0)에 대한 응답을 한다. 이는 라우터의 IP 주소를 발견할 수 있게 한다.

<http://blog.naver.com/PostView.nhn?blogId=shj1126zzang&logNo=220058972700&parentCategoryNo=&categoryNo=30&viewDate=&isShowPopularPosts=true&from=search>

% 위의 URL은 CMD의 tracert 사용법 및, 원리를 나타낸 것이다.

즉, tranceoute (windows : tracert)는 현재 자신의 위치에서 (예, google.com)까지 패킷을 링크 1회 이동시키고 죽이면서(TTL 값을 수정) 어디까지 갔는지에 대한 정보를 받아오고, 그 이후에 2회, 3회, … 계속 반복 수행하여 최종 목적지 까지 순서대로 어디를 거쳐서 갔는지 그리고 최종 목적지까지 몇 개의 홈을 지나서 도착 했는지를 추적하는 명령어이다. 

3). TTL (Time To Live)

TTL은 IP 패킷 내에 있는 값으로서, 그 패킷이 네트워크 안에 너무 오래 있어서 버려져야 하는지의 여부를 라우터에게 알려준다. 패킷들은, 여러 가지 이유로 적당한 시간 내에 지정한 장소에 배달되지 못하는 수가 있다. 예를 들어, 부정확한 라우팅 테이블의 결합은 패킷을 끝없이 순환하게 만들 수도 있다. 일정한 시간이 지나면 그 패킷을 버리고, 재전송할 것인지를 결정하도록 그 사실을 발신인에게 알릴 수 있게 하기 위한 해결책으로 TTL이 사용된다. TTL의 초기치는 시스템에 의해 대개 8비트 길이의 패킷 헤더에 설정된다. TTL에 관한 원래의 아이디어는, 일정 시간 동안을 초 단위로 지정함으로써 그 시간이 지나면 패킷을 버리도록 하기 위한 것이다. 각 라우터는 TTL 필드로부터 적어도 하나의 숫자를 빼도록 되어 있으며, 그 계산은 대개 패킷이 버려지기 전에 허용되는 라우터 개수를 의미하는데 사용된다. 패킷을 받는 각 라우터는 TTL 필드 내의 값에서 1을 뺀다. 그 값이 0이 되었을 때, 라우터는 그것을 감지하여 그 패킷을 버리고 ICMP 메시지를 발신지 호스트로 보낸다.

Ping과 traceroute 유틸리티는 둘다 특정 호스트 컴퓨터에 접근을 시도하거나 그 호스트까지의 경로를 추적할 때 TTL 값을 사용한다.

Traceroute는 수신 경로에 따라 이어지는 각 라우터에 의해 그 패킷이 버려지도록 하기 위해, 의도적으로 낮은 TTL 값을 이용하여 패킷을 보낸다.

즉, 패킷을 보내고 패킷이 버려졌다는 ICMP 메시지를 돌려받기 전까지의 시간은, 이어지는 각각의 홉 이동시간을 계산하는데 사용된다.

멀티캐스팅 IP 프로토콜을 사용하면, TTL 값은 패킷이 전달되어야 하는 범위나 구역을 가리킨다.

% TTL

0 – 같은 호스트로 제한

1 – 같은 서브넷으로 제한

32 – 같은 사이트로 제한

64 – 같은 지역으로 제한

128 – 같은 대륙으로 제한

255 – 제한이 없다

Ping 명령어 사용 시 TTL(Time To Live) 값을 확인할 수 있는데, 이 때 나오는 TTL 값은 운영체제 마다 기본 TTL 값이 달라서 운영체제를 추측할 수도 있다. 윈도우 경우에는 TTL 디폴트 값이 128이므로, TTL 이 120번대 값이 나오면 윈도우 서버라는 것을 추측할 수 있다.

<http://mindnet.tistory.com/entry/ICMP-Ping-ttl-%EA%B0%92%EC%9D%84-%ED%86%B5%ED%95%B4-%EC%9A%B4%EC%98%81%EC%B2%B4%EC%A0%9C-%ED%99%95%EC%9D%B8>

위의 URL은 TTL에 따라 나오는 운영체제를 알 수 있다.