TCP/IP Network

Network Layer

ARP (Address Resolution Protocol)

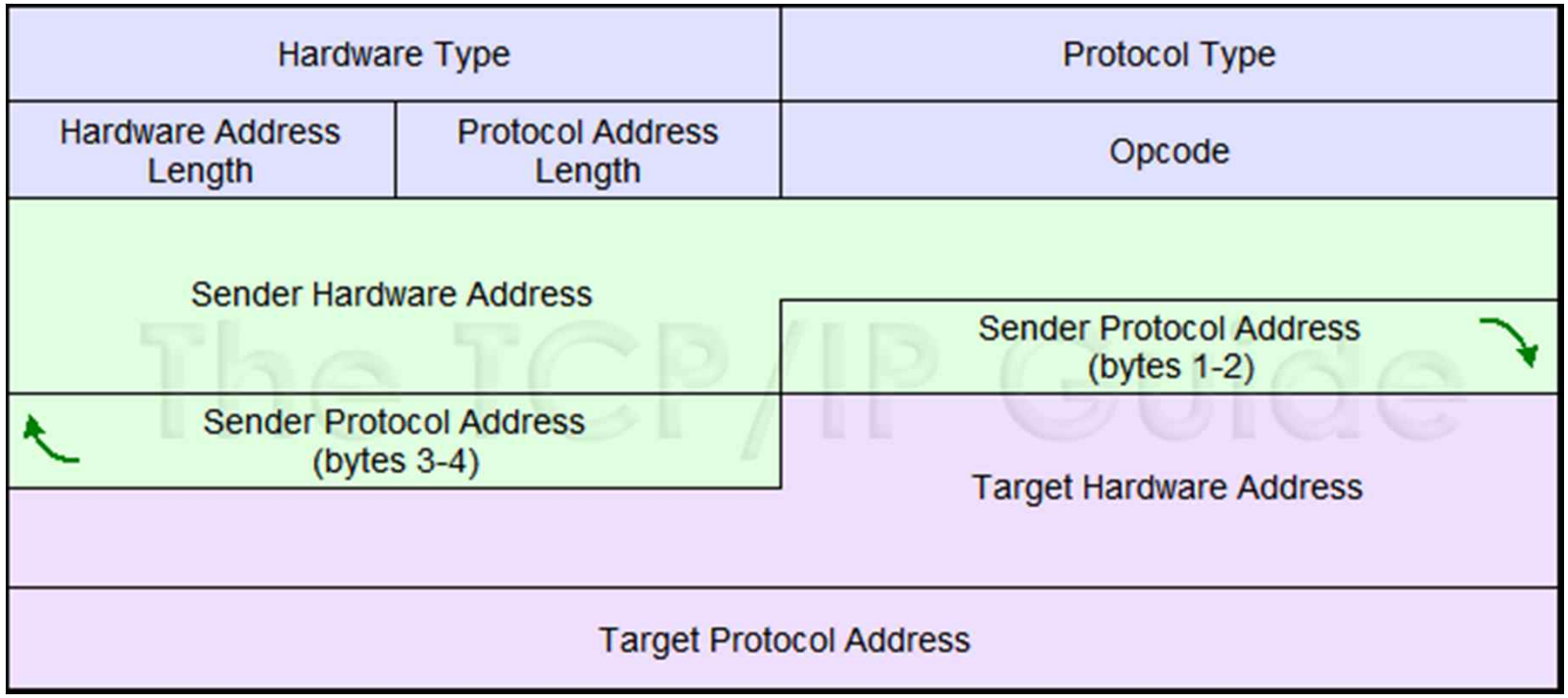
RFC 826

- 네트워크 계층 주소를 데이터 링크 계층 주소로 변환하는 절차
  - IP 주소에 해당하는 데이터 링크 계층 주소를 알아오기 위해 사용
- 동작
  - 로컬 네트워크에 브로드 캐스트 메시지로 ARP 요청 -> 해당 장비 ARP 유니캐스트로 응답

TCP/IP Network

Network Layer

ARP Packet 구조



TCP/IP Network

Network Layer

ARP Packet 구조

- Hardware
  - 요청된 하드웨어 주소 종류를 나타냄
- Protocol
  - 다루고 있는 상위 계층의 프로토콜 정보
- Hardware Address Length
  - 물리매체의 하드웨어 주소의 크기를 바이트 단위로 나타낸다
- Protocol Address Packet
  - 상위 계층의 프로토콜 주소의 크기를 바이트 단위로 나타낸다
- Operation : ARP Packet의 목적을 나타낸다. (요청 또는 응답)
- Sender Hardware Address : ARP Broadcast를 전송하는 시스템의 하드웨어 주소
- Sender Internet Address : ARP Broadcast를 전송하는 시스템의 상위 계층 프로토콜 주소
- Target Hardware Address : ARP Broadcast를 수신하는 시스템의 하드웨어 주소
- Target Internet Address : ARP Broadcast를 수신하는 시스템의 상위 계층 프로토콜 주소

TCP/IP Network

Network Layer

ARP Cache

- 문제점
  - ARP 요청은 broadcast통신을 하기 때문에 지속적인 주소 결정작업은 네트워크 대역폭을 낭비하게 되고, 로컬 네트워크의 모든 장비가 해당 packet를 처리하기 위해서 자원을 소모하게 된다
- 해결
  - Cache Table 생성
    - 하드웨어 주소와 대응하는 IP 주소 집합을 저장하는 DB

- Cache Table에 항목 추가 방법
  - ARP응답을 수신한 시스템은 대상 시스템의 Mac 주소와 IP주소를 ARP table에 저장
  - 수동 입력
    - arp ip-address mac-address
    - arp –s
    - 만료 기간 없이 영구히 캐시에 남아있다
  - 네트워크 세그먼트에서 발생하는 traffic 감시
    - frame을 수신하면 송신지의 IP주소와 Mac주소를 ARP table에 기록

TCP/IP Network

Network Layer

ARP Cache

- Cache 만료 시간
  - 장비 하드웨어 오류나 ip 주소의 변경 또는 장비가 제거 됐을 때, cache정보는 유효하지 않다
  - 시스코 장비 : 4시간
  - 유닉스 : 5분
  - 윈도우 : 20분
- 멀티캐스트 ARP
  - 직접 매핑
  - 그룹 주소의 첫 번째 옥텟을 01-00-5E로 매핑하고 다음 비트에 0을 입력
  - 남은 23비트를 IP 그룹 주소의 23비트 값으로 매핑

TCP/IP Network

Network Layer

ARP Cache 확인

```
C:₩>arp -a
Interface: 211.255.9.138 on Interface 0x1000004
  Internet Address      Physical Address      Type
  211.255.9.130         00-e0-4c-ab-43-ee     dynamic
  211.255.9.254         00-10-7b-38-24-68     dynamic
```

- Static ARP Table 만들기

```
C:₩>arp  –s  211.255.9.254  00-10-7b-38-24-68
C:₩>arp  -a
Interface: 211.255.9.138 on Interface 0x1000004
  Internet Address      Physical Address      Type
  211.255.9.130         00-e0-4c-ab-43-ee     dynamic
  211.255.9.254         00-10-7b-38-24-68     static
```

TCP/IP Network

Network Layer

ARP 동작

RFC 826

- 출발지
  - ARP cache에서 목적지 장비 하드웨어 주소 확인
  - ARP 요청 frame 생성
  - ARP 요청 frame broadcast 전송
- 목적지
  - ARP 요청 프레임 처리
  - ARP 응답 frame 생성
  - ARP 캐시 갱신
  - ARP 응답 프레임 송신
- 출발지
  - ARP 응답 프레임 처리
  - ARP 캐시 갱신

TCP/IP Network

Network Layer

IGMP (Internet Group Management Protocol)

- 멀티캐스트 그룹 관리 프로토콜
  - 데이터 전송 프로토콜이 아니라 네트워크상에 이벤트 또는 변화를 알리는데 사용되는 제어용 프로토콜
  - 멀티캐스트 멤버 가입, 수정, 탈퇴 시에 사용되는 관리 프로토콜.
- Member ship Query
  - 멀티캐스트 라우터는 주기적으로 호스트 그룹들에게 IGMP QUERY MESSAGE를 전송
- Member ship Report
  - 호스트 -> 라우터
- Join
  - 그룹에 가입하고자 하는 요청
- Member continuation
  - 계속해서 해당 그룹에 남기를 원하는 보고
- Leave Report
  - 호스트 -> 라우터

TCP/IP Network

Network Layer

IGMP (Internet Group Management Protocol)

- Leave group
  - 그룹 탈퇴
- 동일 LAN에 여러 멀티캐스트 라우터가 있으면, IPv4 주소 중 가장 낮은 주소를 갖는 라우터가 Querier역할을 한다.
- IP 프로토콜 필드값은 2, TTL = 1
- IGMP 프로토콜은 LAN내에서만 동작

TCP/IP Network

Network Layer

ICMP (Internet Control Message Protocol)

- 오류 정보나 상태 정보를 송신 측에 전달
- ICMP data는 가변적인 길이를 갖는다
  - ICMP헤더의 기본값은 8bit이며 앞 4bit는 공통으로 사용되고, 뒤의 4bit는 타입에 따라 다르게 사용된다. 그 뒤에 ICMP 데이터 부분은 원본 IP 패킷의 헤더와 데이터 제일 앞의 8byte이상이 오게 된다.
- 언제나 최초의 발신지로 오류 메시지를 전송한다.
- 오류 메시지를 보내는 ICMP 패킷에 대한 오류 메시지는 생성되지 않는다.
- 멀티캐스트 주소를 가진 패킷은 오류메세지가 생성되지 않는다.
- 127.0.0.0 0.0.0.0등 특별히 예약되어있는 주소를 가진 데이터에 대한 오류 메세지는 생성하지 않는다.

TCP/IP Network

Network Layer

ICMP (Internet Control Message Protocol)

- ICMP는 오류보고와 질의 메시지로 나눌 수 있다.
- 에러보고 : 문제 발생 시 에러 메세지 전달
  - 수신처 도달 불가 : 3
  - 발신 제한(발신지 억제) : 4
  - 라우트 변경(재지정) : 5
  - 시간 초과 : 11
  - 파라미터 불량(매개변수 문제) : 12
- 질의 : 한 쌍으로 이뤄져 있으며 특정 정보를 얻기 위해 사용된다.
  - 네트워크 문제 진단
    - type이 질의일 경우에 코드 값은 의미가 없다.
  - 에코 : 0(응답)/8(요청)
    - 고장 진단의 목적, IP의 동작을 검사
  - 타임 스탬프 : 13(요청)/14(응답)
  - 주소 마스크 : 17(요청)/18(응답)
  - 라우트 간청, 광고 : 10(간청)/9(광고)

TCP/IP Network

Network Layer

ICMP Message Type

RFC 792

Type		Message
오류메시지	3	수신처 도달 불가 (Destination Unreachable)
	4	발신제한 (Source Quench)
	5	라우트 변경 (redirect)
	11	시간 초과 (Time Exceeded)
	12	파라미터 불량 (Parameter Problem)
정보제공메시지	0	에코 응답 (Echo Reply)
	8	에코 요청 (Echo Request)
	13	타임 스탬프 요청 (Timestamp Request)
	14	타임 스탬프 응답 (Timestamp reply)
	15	정보 요구 (Information Request)
	16	정보 응답 (Information Reply)
	17	주소 마스크 요구 (Address Mask Request)
	18	주소 마스크 응답 (Address Mask Reply)

Code	Message
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown

http://www.iana.org/assignments/icmp-parameters

- 메시지의 첫 부분은 ICMP 에러 메시지를 나타내며, 메시지의 나머지 부분은 실패한 IP 데이터그램의 헤더와 데이터 첫 8바이트를 포함한다.

TCP/IP Network

Network Layer

ICMP Error Code

- Type 3 : 목적지 도달 불가의 경우 코드 값 – 목적지 도달 불가의 이유
  - 0 : 네트워크에 도달 불가
    - 하드웨어 고장등의 이유로 목적지 네트워크에 도달 못한다.(알고는 있지만 현재 시점에서 도달하지 못한다.)
  - 1 : 호스트에 도달 불가
    - 하드웨어 고장 등의 이유로 목적지에 도달 못한다.(알고는 있지만 현재 시점에서 도달하지 못한다.)
  - 2 : 프로토콜 도달 불가
    - 해당 목적지까지 도착은 했지만 데이터를 전달해야 할 서비스 프로토콜이 동작하지 않고 있어서 전달하지 못한다.
  - 3 : 포트 도달 불가
    - 해당 목적지까지 도착은 했지만 데이터가 프로세스로 전송되어야 할 포트가 막혀있어서 전달하지 못한다.
  - 4 : 단편화 불가
    - 단편화가 필요하지만 IP헤더의 DF가 1로 설정되어서 단편화가 일어나지 않아서 데이터를 전달하지 못한다.

TCP/IP Network

Network Layer

ICMP Error Code

- 5 : 발신지 경로 실패 – 발신지에서 라우팅을 하지 못한다.
- 6 : 목적지 네트워크를 알 수 없다. – 목적지 네트워크의 경로를 알 지 못한다,
- 7 : 목적지 호스트를 알 수 없다. : 호스트의 위치를 알 지 못한다.
- 8 : 발신지 호스트 고립
- 9 : 목적지 네트워크와 통신이 관리상 이유로 금지
- 10 : 목적지 호스트와의 통신이 관리상의 이유로 금지
- 13 : 관리자가 필터를 설치해서 호스트에 도달할 수 없다.

• Code 2,3번은 목적지 호스트에 의해서만 생성될 수 있고, 나머지는 라우터에 의해서 생성된다.

• Type 4 : 발신지 억제 코드 값
  - 혼잡 발생으로 인한 데이터 폐기를 발신지에 알리고, 흐름제어 기능을 수행한다.

• Type 11 : 시간 경과
  - TTL값이 만료 될 경우
  - 최종 목적지가 정해진 시간 안에 쪼개진 단편을 모두 받지 못한 경우 이미 받은 단편들을 폐기하고 원래의 발신지로 시간 경과 메시지를 보낸다.

TCP/IP Network

Network Layer

ICMP Utility - Ping

- Ping
  - icmp를 사용하여 호스트들 사이에서의 IP 연결성을 테스트한다.
  - 지정된 호스트가 icmp 에코 요청을 받게 되면 icmp 에코 응답으로 응답한다.
  - 응답이 타임아웃 이내의 시간에 도착하지 않으면 응답을 받지 못하였음을 알려주는 메시지를 제공한다.
  - 요청을 발송한 후에 핑은 성공률과 평균 왕복 시간 등의 정보를 요약해서 출력한다.
- 로컬 핑(127.0.0.1)
  - 응답이 네트워크 계층으로 부터 온다. IP가 호스트에 적절하게 설정되어 있음을 테스트 하기 위함. 주소, 마스크, 게이트웨이 등이나 하부 계층의 상태에 대해서는 알수 없다.
- 게이트웨이 핑
  - 호스트가 로컬 네트워크 내에서 정상적으로 동작하고 있음을 테스트.
- 원거리 호스트 핑
  - 로컬 호스트가 인터네트워크를 통하여 통신할 수 있는지를 테스트 하기 위함

TCP/IP Network

Network Layer

ICMP Utility - Traceroute

- 연결된 두 호스트 사이간의 경로를 관찰하기 위하여 사용되는 경로 추적 유틸리티.
- 목적지로 TTL값이 1인 패킷을 3개 전송. TTL값을 1씩 증가 시키면서 목적지에 도착할 때 까지 패킷 발송.
- TTL
  - 패킷이 거치는 홉의 최대수를 제한한다. 1씩 감소 하다 0이 되면 패킷을 폐기하고 ICMP 시간 초과 메시지를 보낸다
- 왕복시간(RTT)
  - 패킷이 원격 호스트에 도착할 때 까지 걸린 시간과 그 호스트로부터 응답이 되돌아오는데 걸리는 시간의 합.
- *는 손실된 패킷을 표시
- 경로를 따라 성공적으로 도착한 홉의 목록을 생성한다.
- 데이터가 수신지에 도착하면 경로 안의 모든 라우터의 인터페이스 목록이 나열된다. 수신지로 가는 도중에 실해하면, 경로상에서 응답한 마지막 라우터의 주소를 얻을 수 있다