3장

유니캐스트 (대부분 통신방식)

- 1:1통신
- 출발지 목적지 1:1 통신

브로드캐스트

- 1:ALL
- 동일 네트워크에 존재하는 모든 호스트가 목적지

멀티캐스트 (IPTV,실시간 방송 등)

- 1:N
- 하나의 출발지에서 다수의 특정 목적지

애니캐스트 (가장 가깝거나 효율적인 서비스 제공 가능 호스트 통신)

- 1:1통신(목적지 동일 그룹 내 1개 호스트)
- 다수의 동일 그룹 중에서 가장 가까운 호스트에서 응답

유니캐스트,애니캐스트 둘다 1:1 통신이지만 통신 가능한 후보자가 다르다.
유니캐스트는 출발지와 목적지가 모두 한 대지만, 애니캐스트는 같은 목적지 주소를 가진 서버가 여러대여서 통신 가능한 다수의 후보군이 있다.
즉, 후보군이 존재한다.

애니케스트 주소?
하나 이상의 네트워크 인터페이스에 할당되는 주소.
해당 주소를 갖는 네트워크 인터페이스 중 가장가까운 네트워크 인터페이스로전달.
유니캐스트 주소 공간내에서 할당되며, 유니캐스트 주소 형식을 동일하게 따라간다.

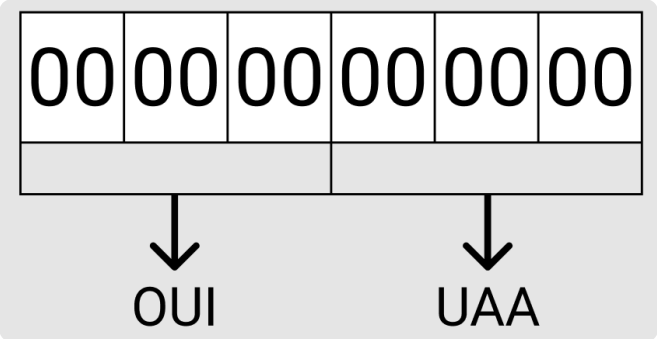
실제 데이터를 전달하려는 출발지가 기준이 아니라 목적지 주소를 기준으로 구분한다.

```
#BUM 트래픽
Broadcast / Unknown Unicast / Multicast
Unknown Unicast
```

Mac 주소 (Media Access Control)
2계층에서 통신을 위해 네트워크 인터페이스에 할당된 고유 식별자.
하드웨어에 고정되어 출하되므로 네트워크 구성 요소마다 다른 주소를 가진다.
제조사 코드 (vendor code) 존재 IEEE가 관리
48비트의 16진수 12자리로 표현된다.

앞 24비트 = OUI (IEEE가 제조사에 할당)

뒤 24비트 = UAA (제조사가 할당)




```
# 유일하지 않을수도 있음.
실수나 의도적으로 발생 가능하지만, 동일 네트워크에서만 중복되지 않으면 된다.
```

```
# MAC 주소 변경
BIA 형태로 NIC에 할당되어있음. ROM형태로 고정되어 있어서 변경은 쉽지않지만, 변경이 가능하긴하
```

MAC 주소동작

NIC가 MAC주소를 가지고 있다가 전기신호가 들어오면 패킷으로 변환하여 내용을 구분 후 MAC 주소 확인한다.

자신의 MAC 주소랑 같으면 보내고 다르면 버린다.

```
# 무차별 모드
다른 목적지를 가진 패킷을 분석하거나 수집해야할 경우, 무차별 모드를 구성한다.
자신의 MAC 주소와 달라도 이를 메로리에 올려서 처리한다.
와이어샤크 사용
```

```
# MAC 주소 여러개
NIC를 여러개 가지면 된다.
```

```
# MAC 주소로 제조사 찾기
OUI는 제조업체를 나타내므로 이를 참고하면 된다. (IEEE에서 확인)
```

IP 주소

3계층에서 논리적 주소인 IP주소 이용

1. 논리 주소이므로 사용자가 변경 가능
2. 네트워크 주소와 호스트 주소로 나누어진다.

- 32비트 = IPv4
- 128비트 = IPv4
- “.” 옥탯

192.168.0.1
11000000.10101000.00000000.00000001

네트워크 주소
호스트들을 모은 네트워크를 지칭하는 주소. 네트워크 주소가 동일한 네트워크를 로컬 네트워크라고 한다.
호스트 주소
하나의 네트워크 내에 존재하는 호스트를 구분하기 위한 주소

클래스 개념을 도입
다른 고정된 네트워크 주소체계에 비해 주소를 절약할수 있음.

A클래스
2^8 = 약 250개 네트워크, 한 네트워크 당 2^8 = 약 1600만개 호스트 주소, 네트워크 주소가 앞 8비트 나머지 호스트 주소
B클래스
2^16 = 약 6만 5천개 네트워크, 한 네트워크 당 2^16 = 약 6만5천개 호스트 주소,네트워크 주소가 앞 16비트 나머지 호스트 주소
C클래스
2^24 = 약 1600만개 네트워크, 한 네트워크 당 2^8 = 약 250개 호스트 주소, 네트워크 주소가 앞 24비트 나머지 호스트 주소
D클래스
멀티캐스트
E클래스
예약

쉽게 구분하는법
A클래스 0으로 시작
1.0.0.0 ~ 126.255.255.255 / 127.0.0.0
B클래스 10 으로 시작
128.0.0.0 ~ 191.0.0.0.0
C클래스 110 으로 시작
192.0.0.0 ~ 223.0.0.0
D클래스 1110 으로 시작 / 멀티캐스트.멀티캐스트.멀티캐스트.멀티캐스트
224.0.0.0 ~ 239.0.0.0

사용 가능 호스트 수 계산 방법
네트워크 주소: 172,16.0.0
브로드캐스트 주소: 172.16.255.255
유효 IP 범위: 172.16.0.1 ~ 172.16.255.254

172.16.0.0 → 10101100.00010000.00000000.00000000 ~ 10101100.00010000.11111111.11111111
172.16 까지 네트워크 주소
0.0 은 호스트 주소

2^16 - 2 = 65534
2빼는 이유 = 맨앞 0.0 은 네트워크 주소로, 맨뒤 255.255는 브로드캐스트 주소로 사용

A클래스 = 2^24 - 2
B클래스 = 2^16 - 2
C클래스 = 2^8 - 2

클래스풀 / 클래스리스
클래스 주소 체계가 있으면 클래스풀 (서브넷마스크가 필요없음)

IP부족으로 클래스리스 주소체계가 등장 (낭비되는 IP주소 많음)
단기 대안책: 클래스리스, CIDR
중기 대안책: NAT, 사설 IP주소,
장기 대안책: IPv6

클래스리스 주소 체계
네트워크와 호스트 주소를 나누는 구분자를 사용해야 하는데 이 구분자를 서브넷 마스크라 한다.
2진수 1은 네트워크 주소를 0은 호스트 주소를 표시한다.

네트워크 주소 쉽게 뽑아내는법
& 연산을 한다.

IP 주소 103.9.32.146
서브넷 마스크 주소 255.255.255.0/24

01100111 00001001 00100000 10010010
11111111 11111111 11111111 00000000
01100111 00001001 00100000 00000000 → 103.9.32.0

서브네팅

원래 부여된 클래스의 기준을 무시하고 새로운 네트워크-호스트 구분 기준을 사용자가 정해 원래 클래스풀 보다 더 쪼개서 사용하는것.
부여된 주소를 더 잘라서 사용. (클래스리스의 큰 특징)

IP주소 103.9.32.146
서브넷 255.255.255.192

01100111 00001001 00100000 10/010010
11111111 11111111 11111111 11/000000
&연산
01100111 00001001 00100000 10000000 → 103.9.32.128
2^6 = 64
128~191까지 사용 가능

네트워크 사용자 입장
IP 범위 파악
기본 게이트웨이와 서브넷 마스크 설정이 제대로 되어 잇는지 확인

네트워크 설계자 입장
네트워크 설계 시 네트워크 내에 필요한 단말을 고려한 네트워크 범위 설계
ex) 12곳의 지사 / 최대 12대의 IP / 103.9.32.0/24

1. 하나의 네트워크에 12개 IP 할당
2. 2^4= 16 단위로 배정
3. 16개 IP 가진 네트워크 12개를 확보하면 된다. (남는 2개는 보류)

```
사설 아이피 대역을 사용하여 충분한 IP 대역을 사용하는게 좋다.
공인 IP = 수 제한 , 사설 IP = 회사내부에서만 사용(제한x)
최대한 같은 크기의 네트워크를 할당하고, 10진수로 표현해도 쉽게 이해할 수 있는 C클래스단위 24
```

공인IP
 전 세계에서 유일해야 하는 식별자로 쓰는 IP주소
사설IP
 인터넷에 연결하지 않고 개인적으로 네트워크를 구성해서 쓰는 IP주소
인터넷에 접속하지 않거나 NAT을 사용하면 사설IP주소를 사용한다.
사설IP를 사용하면 IP를 변환해주는 NAT장비를 통해 공인 IP로 변경하여 인터넷 접속이 가능하다.
가정에서의 공유기 = NAT 장비 역할

다른 기관에서 사용중인 공인 IP를 회사 내부에서 사용하면 해당 IP로 접근이 불가능하므로 피해야한다.

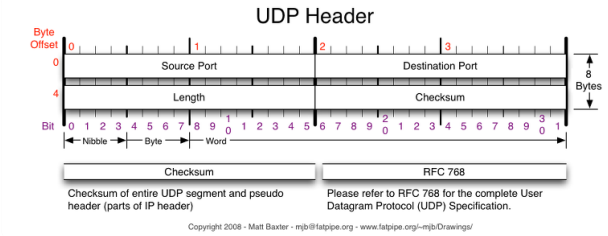
#Bogon IP
IANA가 여러가지 목적으로 예약해놓아 공인IP로 할당하지 않는 주소를 Bogan IP라고 한다.

TCP/UDP
4계층은 목적지 단말 안에서 동작하는 여러 애플리케이션 프로세스— 중 통신해야 할 목적지 프로세스를 정확히 찾아가고 패킷 순서가 뒤바뀌지 않도록 잘 조합해 원래 데이터를 잘 만들어내기 위함.
인캡슐레이션/디캡슐레이션 과정에서 추가되는 헤더 정보

1. 각 계층에서 정의하는 정보
2. 상위 프로토콜 지시자 정보

2계층은 이더타입, 3계층은 프로토콜 번호,4계층은 포트 번호가 상위 프로토콜 지시자
패킷을 잘 분할하고 조립하기 위해서 seq 번호와 Ack 번호를 사용한다.

TCP 헤더			
Souce Port (16bit)			Destination Port (16bit)
Sequence Number (32bit)			
THL (4bit)	Reserved (6bit)	Code Bits (6bit)	Window size (16bit)
Checksum (16bit)			Urgent Pointer (16bit)
Option (0~40 byte)			

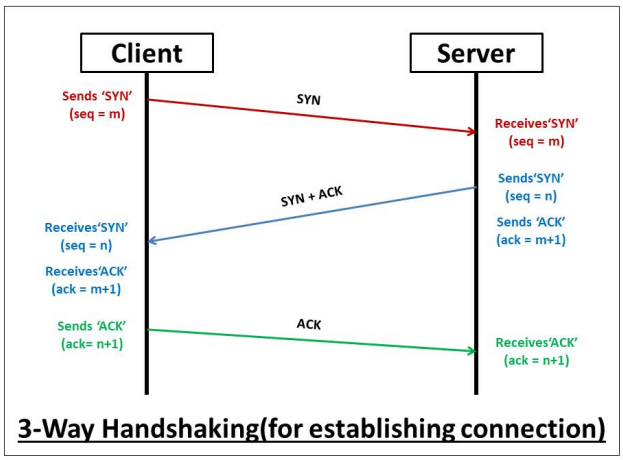


TCP/IP 프로토콜 스택에서 4계층의 상위 프로토콜 지시자는 포트 번호이다.
TCP/IP에서는 클라이언트-서버 방식으로 서비스 제공한다.
2계층,3계층은 상위 프로토콜 지시자는 출발지와 도착지를 구분하지 않지만, 4계층 프로토콜 지시자인 포트 번호는 출발지와 목적지를 구분해 처리해야 한다.

TCP
4계층의 특징을 대부분 포함
세션을 안전하게 연결
데이터 분할 및 패킷 전송 확인
전송크기(window Size) 고려

패킷을 잘 분할하고 잘 조합하도록 패킷에 순서를 주고 응답 번호를 부여한다.
순서 부여 = 시퀀스 번호

응답 번호 = ACK 번호



윈도 사이즈와 슬라이딩 윈도

패킷이 잘 전송되었는지 별도의 패킷을 받는 행위 자체가 통신 시간을 늘리고 거리가 늘어나면 응답시간이 늘어난다.

패킷을 하나만 보내는게 아니라 많은 패킷을 한꺼번에 보내고 응답을 1개만 받는식으로 효율성을 증가시킨다.

네트워크 상태가 안좋아하지면 패킷 유실의 위험이 있으므로 윈도 사이즈를 조절한다.

한 번에 데이터를 받을 수 있는 데이터 크기 = 윈도우 사이즈

네트워크 상황에 따라 이 윈도사이즈를 조절하는것 = 슬라이딩 윈도

TCP헤더 윈도 사이즈로 표현 가능한 최대 크기 2^16 이지만 현대 사회에서는 너무 작은 크기임.

윈도 사이즈를 64K보다 대폭 늘려 통신하는데 tCP헤더는 변경 불가하므로 헤더 사이즈를 늘리자않고 뒤의 숫자를 무시하는 방법으로 윈도우 사이즈를 증가시켜 통신한다.

TCP 데이터에 유실 발생하면 윈도 사이즈를 절반으로 떨어뜨리고 정상적인 통신이 되는 경우 서서히 하나씩 늘린다.

네트워크경합이 발생해서 패킷드롭이 생기면 작아진 윈도 사이즈로 통신속도가 느려질수 있다.

경합을 피하기위해 회선속도를 증가시키거나, 버퍼가 큰 네트워크 장비를 사용하여 해결한다.

3방향 핸드쉐이크

TCP에서는 통신을 하기 전, 사전 연결작업을 진행한다. (일방적으로 보내서 목적지에서 정상적으로처리 못하는 상황 방지)

TCP에서 3번의 패킷을 주고받으면서 통신을 준비한다.

1. 서버는 LISTEN 상태
2. 클라이언트에서 SYN 패킷 전송 SYN-SENT 상태
3. 서버에서 Syn을 받음. SYN-RECEIVE 상태
4. 서버에서 Syn,Ack 응답
5. 클라이언트에선 이 응답을 받고 ESTABLISHED 상태
6. ESTABLISHED 상태는 연결이 성공적으로 완료됨을 나타냄.

기존 통신과 새로운 통신을 구분하기 위해 헤더에 Flag값을 넣어서 통신한다.

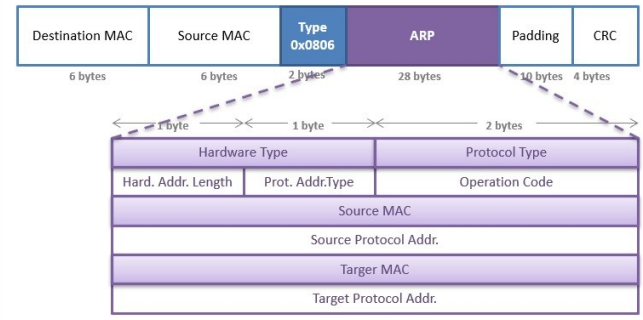
TCP 플래그

SYN	연결 시작 용도로 사용 SYN 플래그에 1 표시
ACK	ACK 번호가 유효하면 1로 표시해서 보낸다. 초기 SYN이 아닌 모든 패킷은 기존 메세지에 대한 응답이므로 ACK 플래그가 1로 표기된다.
FIN	연결 종료 시 1로 표시된다. 데이터 전송을 마친 후 정상적으로 양방향 종료 시 사용된다.
RST	연결 종료 시 1로 표시된다. 연결 강제 종료를 위해 연결을 일방적으로 끊을때 사용된다.
URG	긴급 데이터인 경우 1로 표시
PSH	서버 측에서 전송할 데이터가 없거나 데이터를 버퍼링 없이 응용 프로그램으로 즉시 전달할 것을 지시할때 사용한다.

UDP
데이터 통신은 데이터 전송의 신뢰성이 핵심이다.
UDP는 데이터 전송을 보장하지 않는 프로토콜이므로 제한된 용도로만 사용된다.
음성데이터나 실시간 스트리밍 같이 시간에 민감한 프로토콜이나 애플리케이션을 사용하는 경우나 사내 방송, 증권 시세 데이터 전송에 사용되는 멀티캐스트처럼 단방향으로 다수의 단말과 통신해 응답을 받기 어려운 환경에 주로 사용된다.
대부분 음성, 동영상과 같이 청각,시각적으로 응답시간에 민감한 경우
중간에 데이터가 몇개 유실되는게 재전송을 위해 멈추는것보다 낫다.
UDP는 TCP처럼 연결 확립 절차가 없지만 인터럽트를 거는 용도로 첫데이터를 리소스 확보를 위해 사용하고 유실한다.

```
TCP를 사용하는 경우도 있음. 대신 초~수분 동영상을 미리 받아놓고 캐시에 저장해서 재생한다.
```

ARP
2계층 MAC 주소는 NIC에 종속적인 주소이고 3계층 IP는 DHCP를 이용해 자동 할당받거나 하여 사용된다.
실제 통신은 IP주소를 이용해 일어난다. MAC 주소는 상대방 주소를 자동으로 알아내 통신한다. 상대방의 MAC주소를 알아내기 위해 사용되는 프로토콜이 ARP



MAC 주소와 IP주소를 연계시키기 위해 사용되는 프로토콜

TCP/IP 프로토콜 스택 외에도 TCP-이더넷 프로토콜과 같이 3계층 논리적 주소와 2계층 물리적 주소 사이에 관계가 없는 프로토콜에서 ARP 프로토콜과 같은 매커니즘을 사용해 물리적 주소와 논리적 주소를 연결한다.
상대방의 MAC주소를 알아내려면 ARP 브로드캐스트를 수행해서 네트워크 전체에서 상대방의 MAC주소를 알아내야 한다.

패킷을 보낼때마다 ARP브로드 캐스트를 하면 효율성이 떨어지므로, 메모리에 이 정보를 저장하여 재사용한다.
ARP작업은 CPU에서 직접 처리한다. → 부하가 크다.
ARP 테이블 저장기간을 일반 피시보다 길게 설정, ARP요청을 필터링하거나 천천히 처리하여 해결.

ARP 동작
ARP 패킷 필드 중 중요 4개 필드

1. 송신자 하드웨어 MAC 주소
2. 송신자 IP 프로토콜 주소
3. 대상자 MAC 주소
4. 대상자 IP 프로토콜 주소 4개 필드

A에서 B로 ping을 보낼때 상대방 MAC주소를 모르기 때문에 ARP요청을 브로드캐스트하고, ARP 패킷을 네트워크에 브로드캐스트할때 자신의 MAC주소를 출발지로,도착지는 브로드캐스트로 채운다.
MAC과 IP주소는 자기 자신 주소로, 대상자 IP주소는 10.1.1.2를 대상자 MAC주소는 00-00-00-00-00-00으로 채운다.
서버 B에서 대상자가 자신이므로 ARP요청을 처리한다. 이때 송신자와 수신자 위치가 바뀐다. A의 정보를 포함해 자신의 정보를 다시 채운후 응답한다.
서버 A는 응답받은 정보를 통해 ARP테이블을 갱신한다.

ARP 요청 - 브로드캐스트
ARP 응답 - 유니캐스트

GARP
Gratuitous ARP, 대상자 Ip 필드에 자신의 IP주소를 채워서 ARP 요청을 보낸다.

자신의 IP주소와 MAC주소를 알릴 목적으로 사용
목적지 MAC주소는 브로드캐스트 MAC주소를 사용한다.

5. IP 주소 충돌 방지
   자신에게 할당된 IP가 다른곳에서 사용되고 있지않은지 GARP를 통해 확인
6. 상대방의 ARP 테이블 갱신
   가상 MAC주소를 사용하지 않는 데이터베이스 HA솔루션에서 주로 사용한다.
   액티브-스탠바이 구조
7. HA용도 고가용성 클러스터링,FHRP(VRRP,HSRP)
   실제 MAC주소를 사용하지 않는 가상 MAC주소를 사용하는 클러스터링.
   네트워크에 있는 스위치장비의 MAC 테이블 갱신이 목적이다.
   가상 MAC주소를 쓰면 ARP 테이블 갱신할 필요가 없다.
   클러스터링 중간에 스위치의 MAC 테이블은 마스터가 변경되었을 때 가상 MAC주소의 위치를 적절히 찾아가도록 업데이트 해야 하므로,마스터가 변경되는 시점에 MAC주소 변경이 필요하다.
   역할이 변경되면 GARP를 전송하고 스위치에서 MAC주소에 대한 포트정보를 새로 변경하여 MAC테이블을 갱신한다.

```
#FHRP (First Hop Redundancy)
VRRP,HSRP 디폴트 게이트웨이에서 장애가 발생한 경우, 해당 네트워크에 속한 단말이 외부 네트워크
두대의 디폴트 게이트웨이가 한대처럼 동작해 한대에 문제가 생겨도 계속 지속 서비스가능
```

RARP
Reverse ARP, GARP와 같은 프로토콜 구조지만 목적이 다르다.
RARP는 IP주소가 정해져 있지 않은 단말이 IP할당을 요청할때 사용한다.
나 자신의 MAC주소는 알지만 IP주소는 모를때 사용한다.
현재는 DHCP, BOOTP로 사용하지 않음.

서브넷과 게이트웨이
원격지 네트워크 통신과 같은 네트워크 통신은 서로 장비나 동작방식이 다르다.
원격지 네트워크 통신에 사용하는 장비 = 게이트웨이(3계층 스위치)

게이트웨이
원격 네트워크 통신은 네트워크를 넘어 전달되지 못하기 때문에 장비의 도움을 받는다.
게이트웨이에 대한 정보를 PC에 입력한다 = 기본 게이트웨이

ARP 브로드캐스트는 원격지 네트워크로 보낼수 없다.
기본 게이트웨이 역할은 3계층 장비 수행

통신할때 가장 먼저 동일 LAN인지, 서로 다른 네트워크인지 확인해야한다.

이때 서브넷마스크를 사용한다.

```
# Proxy ARP
ARP를 대행해주는 기능
기본 게이트웨이에 프록시 ARP가 설정되어 있으면, 원격지 통신이라도 로컬에 ARP 브로드캐스트를
```

2계층 통신 vs 3계층 통신
2계층 통신 = 레이어 2통신 = 로컬 네트워크 통신
3계층 통신 = 레이어 3통신 = 원격지 네트워크 통신

로컬 네트워크 통신은 2계층까지만 정보를 확인해서 전송한다.
ARP 요청을 보낼 때 직접 브로드캐스트를 이용하므로 L2통신이라 한다.

원격지 네트워크 통신은 3계층까지 정보를 확인해서 전송한다. L3 통신

구분은 출발지와 도착지가 같은 네트워크에 속해있는지 아닌지에 따라 나누어진다.

같은 네트워크(로컬 네트워크)
직접적으로 통신한다. 상대방의 MAC주소를 알아내기 위해 ARP브로드캐스트를 이용하고 상대방의 MAC주소를 알아내자마자 패킷이 캡슐화되어 통신 시작
MAC주소가 IP 주소와 같다.

외부 네트워크
ARP 요청을 기본 게이트웨이의 IP주소로 요청한다.
MAC 주소와 IP주소가 다르다.
도착지 IP는 실제 도착지이며, 도착지 MAC주소는 디폴트 게이트웨이의 MAC주소가 사용된다.