Protocol 이란?

프로토콜이란 통신의 목적을 달성하기 위한 정보의 송신자와 수신자의 사이의 약속을 의미한다.

TCP/IP 프로토콜 이란?

TCP/IP는 패킷 통신 방식의 인터넷 프로토콜인 IP(Internet Protocol)

와 전송 조절 프로토콜인 TCP(Transmission Controll Protocol)로 이루어져 있다.

IP는 패킷 전달 여부를 보증하지 않고, 패킷을 보낸 순서와 받는 순서가

다를 수 있다.

TCP는 IP의 상위 프로토콜로, 데이터의 전달을 보증하고 보낸 순서대로 받게

해준다.

현대의 많은 서비스들이 TCP를 기반으로 한 많은 수의 매플리케이션 프로토콜들이

IP위에서 동작하기 때문에, 묶어서 TCP/IP로 부르기도 한다.

TCP/IP 프로토콜 구조

응용계층->트랜스포트계층->인터넷계층->네트워크 접근 계층

네트워크 접슨 계층

물리적 네트워크를 통한 실제 데이터 송수신을 담당한다.

하드웨어적으로 정의된 물리 주소를 사용해서 통신을 한다.

흔히 사용하는 이더넷(Ethernet)에서는 48비트 MAC address를 사용한다.

인터넷 계층

네트워크 접근 계층의 도움을 받아 데이터를 목적지 호스트까지 전달하는 역할을 한다.

네트워크 접근 계층처럼 주소를 지정하는 방법이 필요한데, 하드웨어적으로 정의된

물리적 주고가 아닌 소프트웨어적으로 정의된 논리적 주소인 IP주소(Internet Protocol)를 사용한다.

IP주소는 통신에 참여하는 호스트를 유일하게 지정하는 방법을 제공하지만, 실제로 통신을

할려면 전송 경로를 결정해야하고 그에 따라 데이터를 전달하는 절차가 필요하다.

이를 라우팅이라 부른다.

즉 IP주소와 라우팅을 이용해서 목적지에 호스트의 데이터가 도달할 수 있게 하는 역할

전송 계층

최종 통신 목적지를 지정하고 오류 없이 데이터를 전송하는 역할을 한다.

여기서 최종 통신 목적지란 호스트가 아닌 호스트에서 실행하고 있는

프로세스(응용 프로그램)이다.

따라서 전송 계층에서 프로세스를 지정하는 일종의 주소를 사용하는데

이 주소를 포트 번호(port number)라 한다.

A호스트의 프로세스와 B호스트의 프로세스가 네트워크상으로

통신을 하기위해서는 포트라는 어떠한 매개체(통로, 주소)가 있어야 한다.

인터넷 계층의 IP는 신뢰성이 없어서 상위 계층의 프로토콜인

전송 계층에서 데이터의 손실 혹은 손상을 검출해 잘못된 데이터가 목적지에

전달되는 일을 방지한다.

그러한 역할을 해주는 전송계층 프로토콜이 TCP이다.

응용 계층

전송 계층을 기반으로 한 다수의 프로토콜과 이 프로트콜을 사용하는 응용 프로그램을 포괄

한다.

소켓(Socket)

소켓은 응용 프로그램에서 TCP/IP를 이용하는 창구 역할을 한다.

응용 프로그램과 소켓 사이의 인터페이스 역할을 하고 있다.

네트워크 응용 프로그램은 소켓을 통하여 통신망으로

데이터를 송수신 하게 된다.

소켓은 응용 프로그램에서 TCP/IP를 이용하는 경우 창구 역할을 하며

응용 프로그램과 소켓 사이의 지점을 소켓 인터페이스라고 한다.

위에서 전송계층에서 프로세스 끼리 통신을 하기 위해서는 포트번호 라는것이

필요한데 그 포트번호는 소켓인터페이스가 할당을 해준다.

Port number

TCP와 UDP가 동작하는 계층에서 제공하는 주소 표현 방식이다.

포트 번호가 필요한 이유는 데이터를 목적지 까지 보내도

어느 서비스에서 이 데이터를 처리해줄지 결정해주기 때문에 포트번호가 필요하다.

소켓을 사용하여 TCP연결설정이 되면 통신 양단의 프로세스가 사용하는 고유 주소는

해당 호스트의 IP주소와 호스트 내부의 포트 번호이다.

인터넷 환경에서 많이 사용하는 네트워크 응용 서비스의 포트번호를

Well-known포트 라고 하는데, 전 세계의 모든 컴퓨터가 동일한 포트 번호를 사용하도록

services파일에 권고되어 있다.

사용자가 연결을 원하는 서버의 호스트IP주소만 클라이언트 프로그램에게

지정하고, 포트 번호는 소켓이 현재 할당되어있지 않고, 1024부터의 번호로 자동할당을

해준다.

ARP

1. IP주소에 대응하는 MAC주소를 알아내는 프로토콜이다.
2. 논리적 주소를 물리적 주소로 변환한다.

ARP 작동과정

1. 송신자는 목적이 IP주소를 지정해 패킷을 송신.
2. IP프로토콜이 ARP프로토콜에게 ARP Request 메시지를 생성하도록

요청

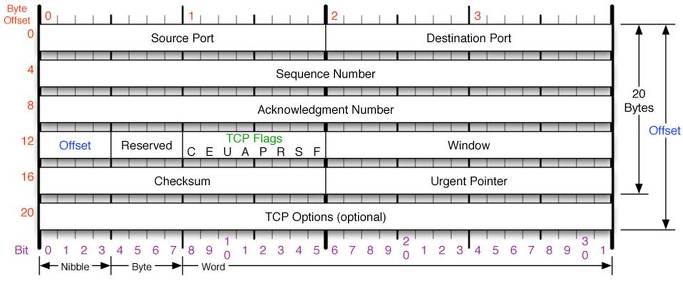
1. 모든 호스트와 라우터는 프레임을 수신 후 자신의 ARP프로토콜에게 전달.
2. 목적지 IP주소가 일치하는 시스템은 자신의 물리주소를 포함하고 있는

ARP Reply메시지를 보냄.

1. 최초 송신측은 지정한 IP주소에 대응하는 물리주소를 획득

\*ARP요청은 브로드캐스트,ARP응답은 유니캐스트

TCP 헤더 구조



Source Port(16bit)

데이터를 생성한 애플리케이션에서 사용되는 포트번호를 나타낸다.

Well-known ports(0~1023):IANA에 의해 배정되고 제어된다.

그 밖의 포트들을 임시포트라 하며 클라이언트들은

임시포트에서 할당받도록 권고되고 있다.

Destication Port(16bit)

목적지 애플리케이션이 사용되는 포트번호 이다.

주로 Well-known port들이 사용된다.

Swquence number 필드(32bit)

전송되는 세그먼트들은 모두 고유한 일련 번호가 부여된다.

네트워크가 불안하여 패킷을 분실,지연 등으로 세그먼트가 순서가

어긋나게 도착 할 수 있기 때문에

Sequence number를 통해서 올바른 순서로 재배열할수있고

분실하거나 손상된 패킷에 대하여 재전송을 요청할 수 있다.

Acknowledgement number 필드(32bit)

1.다음 세그먼트를 수신할 준비가 되었다는 사실을 알린다.

2.모든 데이터가 수신되었다는 것을 나타내는 묵시적인 확인 메시지 역할을 한다.

Header Length필드 (4bit)

헤더의 길이를 32비트 단위로 나타낸다. 최소 필드 값은

5이다. (5 \* 32 = 160bit)

Reserved 필드(6bit)

차후의 사용을 위해서 예약된 6비트 필드이다.

Control Flags 필드(6bit)

6개의 서로 다른 제어 비트 또는 플래그를 나타낸다.

동시에 여러 개의 비트가 1로 설정될 수 있다.

- CWR : Congestion Window Reduced) – 혼잡 윈도우 크기 감소

- ECN : Explicit Congestion Notification) – 혼잡을 알림

- URG(Urgent) : Urgent Pointer 필드가 가리키는 세그먼트 번호까지

긴급 데이터를 포함되어 있다는 것을 뜻한다.

  이 플래그가 설정되지 않았다면 Uregent Pointer 필드는 무시되어야 한다.

- ACK(Acknowledgment) : 확인 응답 메시지

- PSH(Push) : 데이터를 포함한다는 것을 뜻한다.

- RST(Reset) : 수신 거부를 하고자 할때 사용

- SYN(Synchronize) : 가상 회선이 처음 개설될 때 두 시스템의 TCP 소프트웨어는

의미 있는 확인 메시지를 전송하기 위해 일련 번호를서로 동기화해야 한다.

- FIN(Finish) : 작업이 끝나고 가상 회선을 종결하고자 할 때 사용

Window size 필드(16bit)

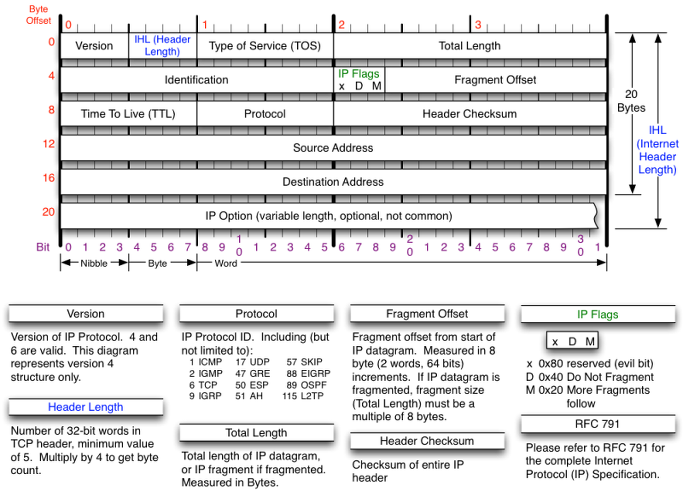
송신 시스템의 가용 버퍼의 크기를 바이트 단위로 나타낸다.

Checksum 필드(16bit)

TCP세그먼트의 내용이 유효한지 검증하고

손상 여부를 검사할수 있다.

IPv4 헤더



Version(4bit)

현재 이 패킷이 v4인지, v6인지를 나타낸다.

ipv4를 뜻하는 0100값이 들어 간다.

Header Length(4bit)

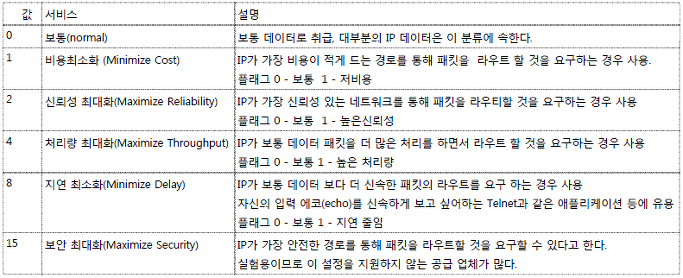
헤더의 길이를 32비트 단위로 나타낸다

대부분의 레더의 길이는 160bit이다

즉 필드값은 5 (5 \* 32 = 160)

Type-of-Service Flags

서비스의 우선 순위를 제공한다.



Total Packet Length(16bit)

전체 ip패킷의 길이,데이터까지 포함한 길이를

바이트 단위로 나타낸다.

Fragmentation Flags(3bit)

처음 1bit는 항상 0으로 설정, 나머지 2비트의 용도는 다음과 같다.

May Fragment : 라우터에 의해 분열되는 여부를 나타낸다.

0 – 분열가능, 1 – 분열 방지

More Fragments: 원레 데이터의 분열된 조각이 더 있는지 여부 판단.

0 – 마지막 조각, 1 – 조각이 더있음

Fragment identifier(16bit)

패킷의 분열이 발생할 경우, 다시 결합할때

데이터의 순서를 구분하기 위해서 사용된다.

Fragment Offset

패킷 재조립시 분할된 패킷간의 순서에 대한 정보.

Time to Live

패킷이 경유할 수 있는 최대 홉 수를 나타낸다.

패킷이 라우터를 하나 통과할때마다 1이 감소하고

0이되면 패킷은 폐기된다.

Protocol

IP Datagram의 몸체에 저장된 상위 계층 프로토콜을 나타낸다.

ICMP: 0x01, TCP: 0x06, UDP: 0x11

Header Checksum

패킷의 오류 발생 여부를 확인하기 위한 필드 이다.

Source address/Destination address

출발지와 목적지를 나타낸다.