

과정명	
09차시	TCP/IP 일반

## <1> TCP/IP 개요

### [1] TCP/IP

- 넓은 의미에서 인터넷에서 사용되는 대표적인 프로토콜의 집합이라 할 수 있음

#### (1) TCP

- 전송계층에서 사용되는 연결 지향형 프로토콜
- 송신한 정보가 수신지에 정확하게 순서대로 도착하였는지 확인해주는 기능을 가지고 있어, 수신 측에서 받은 정보에 오류가 있으면 송신 측에 전달하고 송신 측이 수신 측에 해당 정보를 다시 전송함
- TCP 메시지 헤더에는 오류 발생 시 재전송을 위한 순서 번호, 확인 응답번호 등의 필드가 있으며, 송수신 포트번호에 대한 정보가 존재함

#### (2) IP

- 네트워크 계층에서 사용되는 간단한 오류 검사 기능만 있는 비신뢰성 프로토콜로 패킷이 분실되어도 다시 찾아주지 않음
- 라우터는 IP 주소를 이용해 데이터의 전달 경로를 결정함
- IP 헤더에는 송수신지의 IP 주소, 전체 패킷의 길이, 네트워크 관리나 보안 문제 등과 관련하여 송신 측에서 요청하는 옵션들을 포함하고 있음

### [2] OSI 7 Layer와 TCP/IP 프로토콜

#### (1) OSI 7 Layer

- 자연적으로 만들어진 것이 아닌 국제 표준화 기구인 ISO에서 표준안으로 만든 모델
- 물리 계층, 데이터 링크 계층, 네트워크 계층, 전송 계층, 세션 계층, 표현 계층, 응용 계층의 7층으로 나뉘어져 있음

##### 1) 물리 계층

- Ethernet, RS-232C, 허브, 리피터 등
- 물리적인 매체를 통해 비트 흐름을 전송하기 위한 요구 기능 조정
- 기본적인 물리적인 연결기의 전기적인 명세를 정하고, 네트워크 두 노드를 물리적으로 연결시켜 주는 신호 방식을 다룸

##### 2) 데이터 링크 계층

- MAC, PPP, 브리지, 스위치 등
- 3계층에서 정보를 받아 주소와 제어정보를 헤더와 트레일러에 추가
- 오류 없이 한 장치에서 다른 장치로 프레임 전달

##### 3) 네트워크 계층

- IP, ICMP, IGMP, 라우터 등
- 다중 네트워크 링크에서 패킷을 발신지에서 목적지로 전달

##### 4) 전송 계층

- TCP, UDP, ARP, Gateway 등
- 전체 메시지의 발신지와 목적지 간 제어와 에러 관리
- 패킷들의 전송이 유효한지 확인하고 실패한 패킷은 다시 보내는 등 신뢰성 있는 통신을 보장하며 세그먼트가 포함됨

##### 5) 세션 계층

- SSH, TLS
- 통신 장치 간 상호작용 설정, 유지, 동기화
- 사용자 간의 포트 연결이 유효한지 확인 및 설정

#### 6) 표현 계층

- JPEG, MPEG, SMB, AFP 등
- 운영체제의 한 부분으로 입출력되는 데이터를 하나의 표현 형태로 변환
- 컴퓨터와 사람이 데이터를 서로 이해할 수 있도록 함

#### 7) 응용 계층

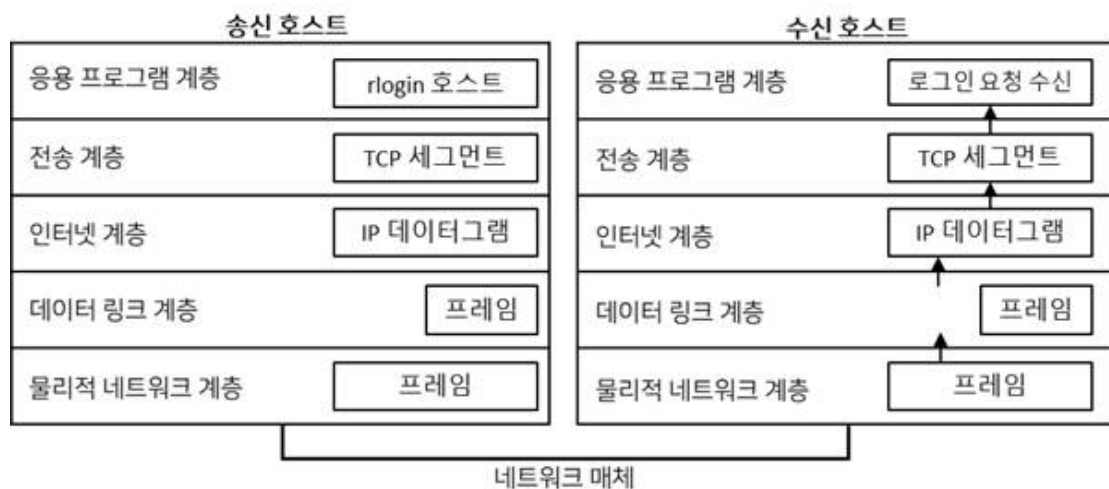
- DHCP, DNS, FTP, HTTP 등
- 사용자 네트워크 자원에 대한 접근 제공
- 네트워크 활동들에 대한 모든 기본적인 인터페이스 제공
- 전형적으로 사용자에게 보이는 유일한 계층

### (2) TCP/IP

- 물리 계층, 데이터 링크 계층, 네트워크 계층, 전송 계층, 응용 계층의 5계층으로 나뉨
- 물리 계층과 데이터 링크 계층에서는 특정 프로토콜을 다루지 않고 OSI에서 지원하는 모든 기술표준을 지원
- 네트워크 계층에서는 데이터 IP, ICMP, ARP, RARP 등을 규정
- 전송 계층에서는 TCP와 UDP 규정
- 응용 계층은 OSI의 응용, 표현, 세션이 묶인 것으로 http, smtp, ftp, telnet 등이 해당됨

#### 1) 통신 원리

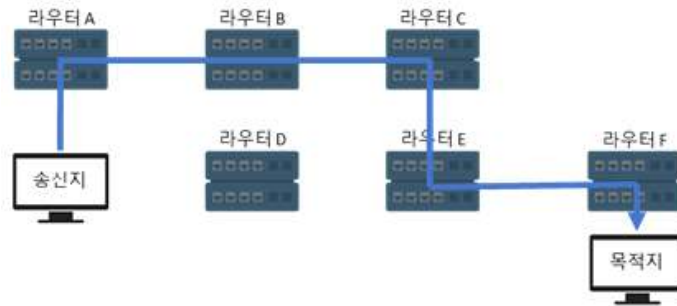
- 송신 측 호스트 응용 프로그램이 보내는 데이터를 수신 측 호스트의 응용 프로그램에 전송하려면 각 프로토콜에서 정의한 제어 정보인 IP 주소, 포트 번호, 오류 체크 코드 등이 필요
- 제어 정보는 위치에 따라 앞쪽의 헤더와 뒤쪽의 트레일러로 나뉨
- 데이터와 제어 정보가 결합된 형태를 패킷이라고 함
- 송신 측 응용 프로그램에서 보낸 데이터는 TCP/IP/이더넷 계층을 지나면서 제어 정보가 붙어 패킷이 생성되고, 수신 측 도착 패킷은 이더넷/TCP/IP 계층을 지나 제어 정보가 제거 되고 응용 프로그램이 데이터를 받게 됨



### [3] 라우터

- 네트워크 간 연결에 사용되는 최적의 전송 경로를 찾아 데이터를 전송하는 장비
- 네트워크 계층 통신을 하는 모든 장치는 라우팅 테이블을 가지고 있음
- 일반 PC도 네트워크 인터페이스가 둘 이상이면 라우터로 구성 가능
- 동작 방식으로는 정적 라우팅과 동적 라우팅이 있음

## (1) 정적 라우팅



- 관리자 설정 경로로만 패킷이 지날 수 있도록 설정
- 비교적 환경 변화가 적거나 보안이 중요한 네트워크에서 선호
- 경로 설정이 이루어지지 않아 초기에 관리자가 다양한 라우팅 정보를 분석한 최적의 경로 설정이 가능
- 라우팅 알고리즘을 통한 경로 설정이 이루어지지 않아 라우터의 직접적인 처리 부하 감소
- 네트워크 환경 변화 시 관리자가 새로운 라우팅 정보를 통해 경로를 다시 계산하여 각 라우터에 제공해야 함
- 네트워크 환경 변화에 대한 능동적인 대처가 어려움

## (2) 동적 라우팅

- 라우터가 네트워크 연결 상태를 스스로 파악하여 최적의 경로를 선택해 전송하는 방식
- 네트워크 연결 형태가 변경되어도 자동으로 문제 해결 가능



- 경로 1과 경로 2 중 부하가 걸리지 않는 경로로 데이터 전송
- 문제가 있어 라우터 C가 제대로 작동하지 않는다면 경로 1로만 패킷 전달
- 실시간 경로 설정으로 네트워크 환경 변화에 능동적인 대처 가능
- 라우팅 알고리즘을 통해 자동으로 경로 설정이 이루어져 관리가 쉬움
- 수시로 환경이 변하는 형태의 네트워크에 적합
- 주기적인 라우팅 정보 송수신으로 인한 대역폭 낭비 발생
- 네트워크 환경 변화 시 라우터에 의한 경로 재설정에는 라우터의 처리 부하 증가와 지연을 발생시킴

## <2> TCP/IP 주요 프로토콜

### [1] IP 주소

#### (1) IPv4

- TCP/IP의 가장 기본적인 IP 주소 체계로 대부분의 네트워크에서 사용됨
- 네트워크 주소와 호스트 주소로 구성되며, 네트워크 주소와 호스트 주소는 서브넷 마스크로 구분
- IPv4의 주소 체계는 32비트로 구성되고, 8비트 단위인 옥텟별로 점을 사용하여 구분하며 10진수 형태로 표기됨
- 각 클래스 별로 IP 범위가 있고 클래스 별로 용도를 지정해 사용. IP 클래스는 A, B, C, D, E 클래스로 나누어 네트워크 ID와 호스트 ID를 구분함

1) A 클래스

- 처음 8비트가 네트워크 ID, 나머지 24비트는 호스트 ID
- 네트워크 할당은 128곳에 가능(0~127)

2) B 클래스

- 처음 16비트가 네트워크 ID, 나머지 16비트는 호스트 ID
- 네트워크 할당은 16,384곳에 가능

3) C 클래스

- 처음 24비트가 네트워크 ID, 나머지 8비트는 호스트 ID
- 네트워크 할당은 2,097,152곳에 가능

- 슈퍼네틱팅은 최상단의 라우터에서 해당하는 경로들을 축약하여 보내고자 할 때 여러 네트워크의 공통되는 부분을 정리하여 하나의 커다란 네트워크로 바꾸는 작업을 말함
- 슈퍼네틱팅의 목적으로는 여러 네트워크의 공통되는 부분을 정리하여 하나의 네트워크로 묶기, 여러 라우터를 하나로 요약하여 라우팅 테이블에서 다루어야 할 정보량을 줄여 메모리, CPU 등의 자원 낭비 방지, 네트워크 토폴로지의 급격한 변화의 격리 등이 있음

- 서브네틱팅은 주어진 네트워크 마스크에서 호스트 주소 영역을 네트워크 주소 영역으로 사용하는 것 즉, 하나의 네트워크를 여러 개의 서브 네트워크로 나누는 과정을 말함
- 서브네틱팅은 IP 주소를 효율적으로 사용할 수 있고, 트래픽과 제어의 관리가 가능함

- 캐스팅 모드에는 유니캐스트, 멀티캐스트, 브로드캐스트가 있음

1) 유니캐스트

- 단일 인터페이스를 지정
- 맥 주소를 기반으로 상대측 IP 주소를 목적지로 하는 일대일 통신방식

2) 멀티캐스트

- 여러 노드에 속한 인터페이스의 집합을 지정
- 패킷은 주소에 해당하는 모든 인터페이스에 전달

3) 브로드캐스트

- 자신의 호스트가 속해 있는 네트워크 전체를 대상으로 패킷을 전달하는 일대다 통신 방식

- 헤더 구조

필드 이름	내용
Version	IP의 버전 정보. 0x4일 경우 IPv4를 의미함
IHL	IP 헤더의 길이로 필드 값에 4를 곱한 값이 실제 헤더의 바이트 길이
TOS	라우터에서 IP 데이터그램을 처리할 때 우선순위를 정함 기본 값은 0 우선 순위로는 최소 지연, 최대 처리율, 최대 신뢰성, 최소 비용 설정
TL	헤더를 포함한 데이터그램의 전체 길이
Identification	데이터그램이 단편화 될 때 모든 단편에 이 값이 복사되고, 단편화 된 데이터그램이 생성될 때마다 1씩 증가함
Flag	단편화 여부와 단편화된 조각이 첫 번째인지 중간인지 마지막인지 알림 RF : 아직 사용하지 않았으므로 항상 0 DF : 1이면 단편화 되지 않음, 0이면 단편화되었음을 의미 MF : 0이면 마지막 단편이거나 유일한 단편, 1이면 마지막 단편이 아님을 의미
Fragment Offset	기존 데이터그램 안에서 단편의 상대적 위치를 의미
TTL	라우팅 과정에서 라우터를 몇 개 이상 통과하면 해당 패킷을 버릴지 입력

	라우터 하나를 지날 때마다 값이 1씩 줄어들고 0이 되면 버려짐
Protocol	IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 정의함 1 : ICMP 2 : IGMP 6 : TCP 17 : UDP
Header Checksum	패킷 전달 중 발생할 수 있는 오류 검사를 위해 사용하는 것 송신 측에서 체크섬을 계산하여 전송
Source Address	송신측 IP 주소
Destination Address	수신측 IP 주소
Options	해당 패킷에 대한 옵션 사항 입력
Padding	옵션 내용이 입력될 경우 그 값이 32 배수로 데이터가 마무리 되도록 0을 채움
Data	IP 패킷을 통해 전송되는 데이터 부분

## (2) IPv6

- IPv4의 주소 고갈, 클래스 단위 주소 할당 방식으로 인한 주소 낭비의 한계 극복을 위해 개발
- 다양한 서비스의 제공, 라우터 효율성 증가, 보안 기술 향상, 무선 인터넷 지원 등의 기능 제공
- 128비트로 주소 길이를 늘려 IPv4보다 주소 공간을 4배 확장
- 하나의 IP를 활용해 가상 IP를 할당하여 여러 개의 IP처럼 사용 가능
- 브로드캐스트를 대체하기 위한 애니캐스트 전송 방식 등장
- 일부 헤더 삭제, 확장 헤더 도입
- 헤더 포맷은 라우터 부하 감소를 위해 단순화
- MAC 주소와 Prefix를 통해 IP 주소 자동 설정이 가능하여 비용, 시간 감소 및 관리가 편리해짐

- IP 자동설정 방식에는 상태 보존형 자동설정과 상태 비보존형 자동설정 방식이 있음

### 1) 상태 보존형 자동설정

- DHCPv6 서버로부터 주소를 비롯한 모든 네트워크 정보를 얻는 방식
- 주소의 이용 효율성 향상, 보안성 유지
- 복잡한 서버 설치 및 구성과 관리
- 대규모 DB 구축 필요

### 2) 상태 비보존형 자동설정

- LAN 상에서 MAC 주소를 라우터가 제공하는 Prefix와 결합해 고유의 IP 주소를 자동 생성
- 서버가 필요 없음
- 보안 문제 발생 가능

- 주소 체계는 네트워크 ID 64비트와 인터페이스 ID 64비트의 128비트 구성으로 16진수로 표기
- 128 비트 IP 주소는 콜론 두 개 사이에 있는 섹션 4개에서 앞 쪽의 0은 생략이 가능함
- 주소 할당은 네트워크의 규모 및 단말기 수에 따라 순차적으로 할당
- 주소 유형에는 유니캐스트, 멀티캐스트, 애니캐스트가 있음

### - 헤더구조

필드 이름	내용
Traffic Class	IP 패킷마다 서로 다른 서비스 요구사항을 구분하기 위한 용도
Flow Label	데이터의 특정한 흐름을 위한 특별한 처리 제공
Payload Length	기본 헤더를 제외한 IP 패킷의 길이 정의
Next Header	확장 헤더의 종류를 표시. IPv4의 프로토콜 번호와 유사한 역할 수행
Hop Limit	IPv4의 TTL 필드와 같은 목적으로 사용

- 기본 헤더의 확장 필드

Routing Header	출발지 호스트가 목적지까지의 라우팅 경로를 지정할 때 사용
Fragment Header	라우터와 라우터 사이의 데이터그램(MTU) 값에 차이가 있을 때 발생
Authentication Header	IP 데이터그램의 보안 지원

(3) 사설 IP 주소

- 공인 IP 주소가 아닌 사적인 용도로 임의 사용되는 IP 주소
- IP 주소 부족을 해결할 수 있고 자유로운 사용이 가능함
- 외부 검색 불가능으로 보안성 증가되고 경제적임
- 주소 할당은 통신망주소변환기 사용

(4) MAC 주소

- 네트워크 세그먼트의 데이터 링크 계층에서 통신을 위한 네트워크 인터페이스에 할당된 고유 식별자
- 48비트로 구성되고 한 칸 당 4bit이며 16진수로 표현. 첫 24비트는 하드웨어 제조업체 고유 ID, 나머지 24비트는 랜 카드의 정보를 담고 있음

[2] TCP와 포트

- TCP의 특징으로는 높은 신뢰성, 가상 회선 연결방식, 연결의 설정과 해제, 데이터 체크섬, 시간 초과와 재전송, 데이터 흐름 제어 등이 있음
- TCP는 패킷을 주고 받기 전에 미리 연결을 맺어 가상 경로를 설정하고, 이 가상 경로를 통해 모든 데이터가 전송됨
- 가상 경로 설정에는 연결을 설정하고 종료하는 두 과정이 필요함
- 연결 설정 과정
  - 1) 1단계(시스템 통신 전)
    - 클라이언트 포트가 Closed인 상태
    - 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태
  - 2) 2단계(클라이언트의 통신 의사 표현)
    - 임의의 포트 번호가 클라이언트 프로그램에 할당
    - 클라이언트의 SYN Sent 상태는 서버 연결을 하고 싶다는 표시
  - 3) 3단계(서버의 클라이언트 요청 수락)
    - 서버가 SYN Received 상태로 전환
    - 클라이언트에게 연결을 해도 좋다는 SYN + ACK 패킷을 보냄
  - 4) 4단계
    - 클라이언트가 연결 요청에 대한 서버 응답을 확인했다는 표시로 ACK 패킷을 서버로 보냄
- UDP는 비연결 지향형 프로토콜로 상대방이 보낸 응답을 확인하지 않고, 송신 시스템이 전송하는 데이터에 대한 목적지 시스템의 확인 절차를 생략함
- UDP는 네트워크에 부하를 주지 않음
- 수신한 데이터의 무결성을 보장받지 못하고 상호 통신이 이루어지지 않아 데이터 일부가 손실되어도 재전송을 요구하지 않는 단점이 있으나 최근에는 네트워크 신뢰도가 매우 높아져 무결성을 보장받지 못해도 효율성 높은 데이터 전송을 위해 많이 사용됨
- 포트 주소는 클라이언트/서버 모델에서 응용 서비스가 통신을 하기 위한 논리적 통로를 말함
- 포트는 데이터를 송수신할 때 프로그램이 사용하는 프로토콜의 일련번호를 표기한 것임

- 포트 번호는 각각의 네트워크 메시지가 해당하는 특정 프로세스를 인식하기 위한 방법으로, 접속 요청을 하는 포트는 1,024 이상의 번호로 지정되며, 접속 요청을 받는 측의 포트는 1,024 이하로 지정됨

### [3] 그 밖의 주요 프로토콜

#### (1) ARP

- IP 주소를 물리적 주소로 대응시키기 위해 사용되는 프로토콜
- 여러가지 컴퓨터 시스템에서 번지 지정의 차이를 해결하기 위한 규약으로 MAC 주소를 알려줄 것을 전체 네트워크에 요청하는 패킷인 ARP Request 패킷과 MAC 주소를 상대방에게 응답하는 패킷인 ARP Replay 패킷으로 구성

- 프록시 ARP는 라우터 등과 같은 장비 안에서 ARP 요구에 응답하는 기술을 말함

##### 1) Proxy ARP 1

- 라우터가 종단 노드를 대신해 요청한 호스트로 ARP 응답을 전송하는 ARP 프로토콜의 변이형
- 저속 WAN 링크에서 대역폭 사용을 줄이는데 도움

##### 2) Proxy ARP 2

- 하나의 호스트가 다른 호스트의 ARP 요청에 응답하기 위한 기술
- 라우터는 자신의 정체를 숨기고, 패킷을 실제 목적지로 라우팅하기 위한 역할 수행
- 서브넷이 좀 더 좋은 해결 방안으로 여겨지고 있음

#### (2) RARP

- 시스템의 시작 또는 IP 주소 설정과 같은 특별한 요청이 있을 경우 동작
- RARP Server와 RARP Client의 두 가지 형태로 구성

##### 1) RARP Server

- MAC 주소, IP 주소에 관한 정보 소유
- RARP 클라이언트 요청을 수신하면 응답으로 RARP 클라이언트가 어떤 IP 주소를 사용해야 하는지 알려줌

##### 2) RARP Client

- TAP/IP 프로토콜이 동작할 때 RARP 프로토콜을 동작시켜 RARP 서버로부터 IP주소를 할당 받음
- 서버로부터 실시간으로 운영체제를 메모리에 다운받아 동작시키는 디스크가 없는 클라이언트

#### (3) ICMP

- TCP/IP를 이용하여 두 호스트 간의 통신을 담당하는 프로토콜
- 두 호스트가 통신 시 여러 가지 에러, 경고 상태를 서로 알려줄 때와 상대 호스트의 통신 가능 유무를 확인하는데 사용

#### (4) PPP

- OSI 7계층 중에서 2계층인 데이터 링크 계층에서 사용되는 특정 프로토콜들의 집합. 즉, 두 양단 간에 통신을 하도록 도와주는 프로토콜을 말함
- 두 양단 사이의 링크에 커넥션 개설, 유지, 관리, 시험 및 종료하는 등의 역할 수행
- 링크를 통해 3계층인 네트워크 계층의 프로토콜들을 다중화하여 복합적으로 전송하고 데이터그램을 캡슐화 하는 등의 일을 함

#### (5) RIP

- UDP/IP 상에서 동작하는 라우팅 프로토콜

- 패킷이 목적 네트워크 주소에 도착할 때까지의 최단 경로 결정
- 목적 네트워크 주소, 다음 홉 IP 주소, 목적 네트워크까지의 홉수 등의 정보는 라우터 내의 라우팅 데이터베이스에 기록되어 라우터끼리 정기적으로 정보를 교환하며, 그 중 유효한 경로를 추출한 테이블을 라우팅 테이블이라고 함
- 전송 프로토콜로 UDP를 사용하며 포트번호 520으로 할당됨
- 소규모 네트워크 상에서 효율적이고 비교적 간단한 구성으로 표준 라우팅 프로토콜이기 때문에 모든 제조사의 라우터에서 지원하는 프로토콜로 호환성이 좋음
- 홉수가 16 이상이면 네트워크를 찾지 못해 데이터를 보내지 못하기 때문에 대규모 네트워크에서의 사용은 한계가 존재하며, 속도나 거리 지연들을 고려하지 않아 최적 경로 산정에 비효율적임