네트워크 관리자 입문

한국 지역 정보 개발원

2021.11.10-11.12

강사 소개

서울에서 출생해 인천 대학교(구 인천 전문 대학) 일어과와 경희 사이버 대학교 정보 통신 학과를 졸업하고 한국 외국어 대학교 교육 대학원에서 **전산 교육학 석사**를 취득했다.

약 9년 동안 한국 통신(KT) 등에서 근무하며 다양한 행정 처리와 정보 기술 환경 등을 경험했다. 사무 처리와 관련해 한자 능력 2급 등을 취득했고 정보 기술과 관련해 **정보 처리 산업 기사/정보 보안 산업 기사**와 CCNA/CCNP 등과 같은 자격증을 취득했다. 또한 **교원 2급 자격증과 직업 능력 개발 훈련 교사 3급 자격증** 등을 취득했다.

지난 2004년부터 현재까지 국가 공무원 인재 개발원과 서울시 인재 개발원 등에서 **정보 보안 기사 자격증과 모의 침투 분야 등을 강의 중**이다. 지난 2016년 경찰 인재 개발원(구 경찰 교육원)에서 우수 외래 강사로 감사장을 받았다. 사이버 보안 중 다양한 모의 침투 운영 체제와 사회 공학 등에 특히 관심이 많다.

강의가 없을 때에는 문학•사학•철학 등에 대한 책을 읽거나 국가 정보학 등과 같은 책을 읽는다. 페이스북에서 **모의 침투 연구회(www.facebook.com/groups/metasploits)**와 **사이버 안보 연구회(www.facebook.com/groups/koreancyberwar)** 등을 개설해 활동 중이다.

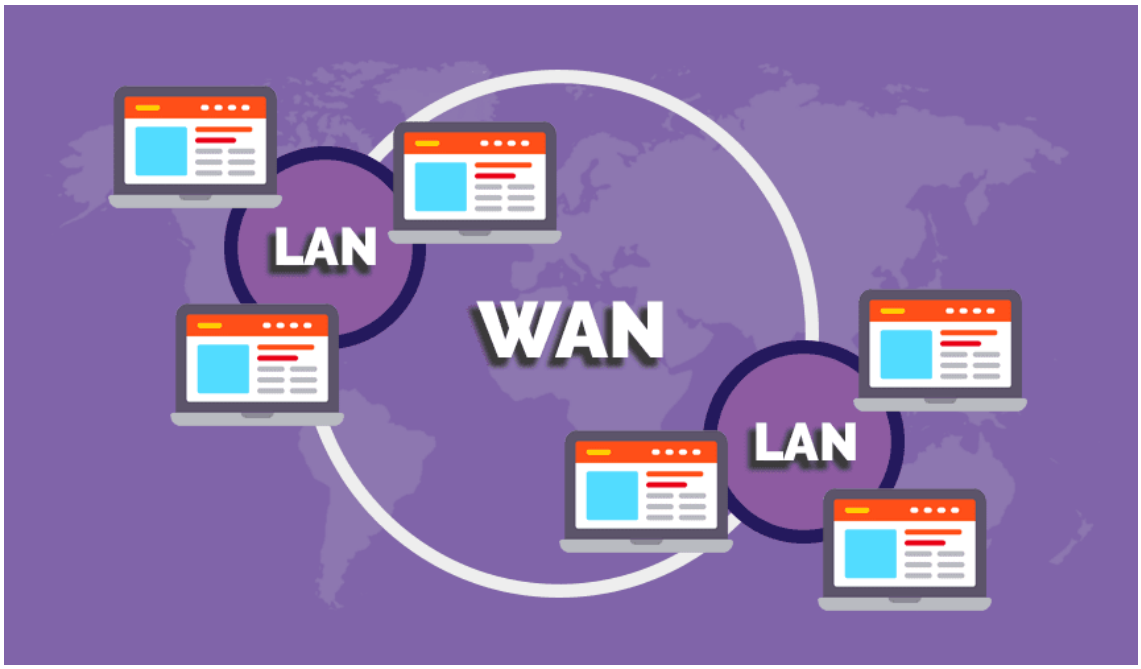
2015년부터 2019년까지 **에이콘 출판사**를 통한 저서로는 **<<해킹 입문자를 위한 TCP/IP 이론과 보안>>•<<칼리 리눅스 입문자를 위한 메타스플로잇 중심의 모의 침투>>•<<백박스 리눅스를 활용한 모의 침투>>•<<해커의 언어 파이썬 3 입문>>•<<소켓 개발 입문자를 위한 백박스 기반의 파이썬 2.7>>** 등이 있고, 공저로는 **<<데비안 리눅스 활용과 보안>>•<<우분투 리눅스 기반의 IDS/IPS 설치와 운영>>•<<모의 침투 입문자를 위한 파이썬 3 활용>>** 등이 있다.

雖不足藏之名山 庶無使墁之醬瓿[비록 명산에 비장할 바는 아니오나 간장 항아리 덮개로는 사용하지 말아 주시옵소서.]

김부식(金富軾)의 <<삼국사기(三國史記)>> 서문 편에서

제1장 TCP/IP 방식을 이해하기 위한 선수 내용

1. LAN 영역과 WAN 영역



(1) LAN 영역

1) MAC 주소에 기반해 내부에서 통신하기 위한 스위칭 공간

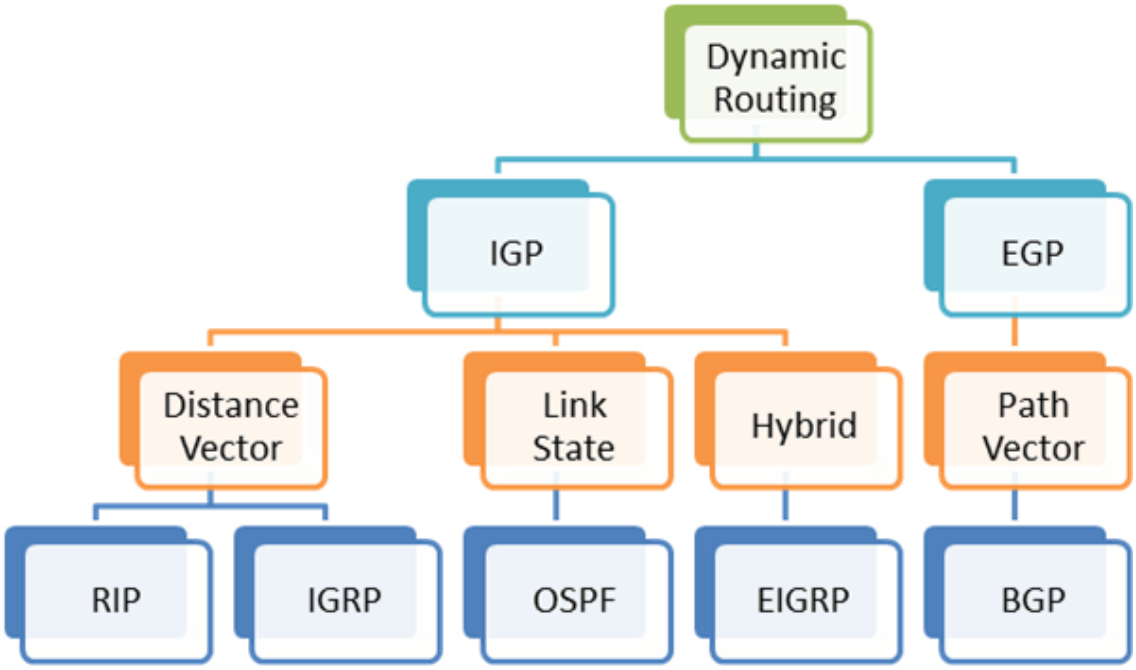
2) 이더넷•토큰 링•FDDI•ATM 등과 같은 프로토콜을 사용

(2) WAN 영역

1) IP 주소에 기반해 외부와 통신하기 위한 라우팅 공간

2) 다시 말해, 라우팅이란 IP 주소에 기반해 자신과 상이한 LAN 영역까지 도달할 수 있는 무수한 경로 중 최상의 경로를 구현하는 기능 또는 기법을 의미

3) RIP•OSPF•ISIS•EIGRP 등과 같이 자신의 기준에 따라 최상의 경로를 구하기 위한 라우팅 알고리즘이 필요



4) HDLC•PPP•X.25•프레임 릴레이•ATM 등과 같은 프로토콜을 사용

2. 통신의 개념

(1) 전송

1) 단방향 전송

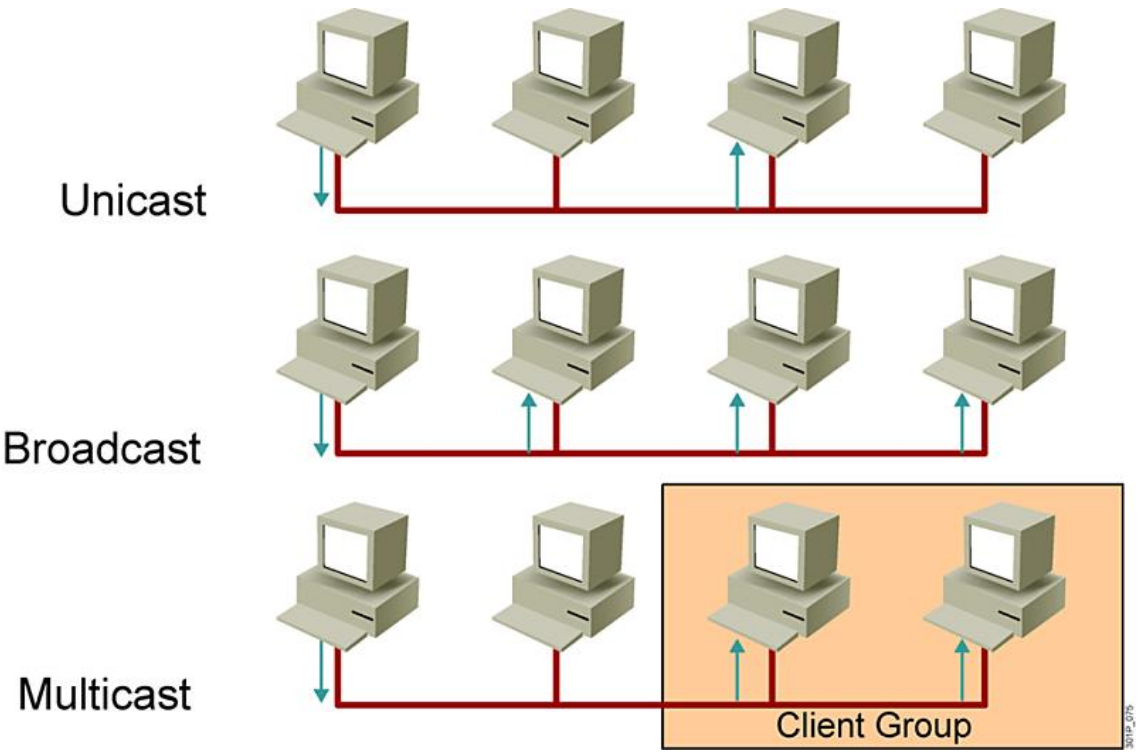
라디오 또는 텔레비전 등

2) 반이중 전송

무전기 또는 허브 장비 등

3) 전이중 전송

전화 또는 스위치 장비 등



4) 유니캐스트 전송

5) 브로드캐스트 전송

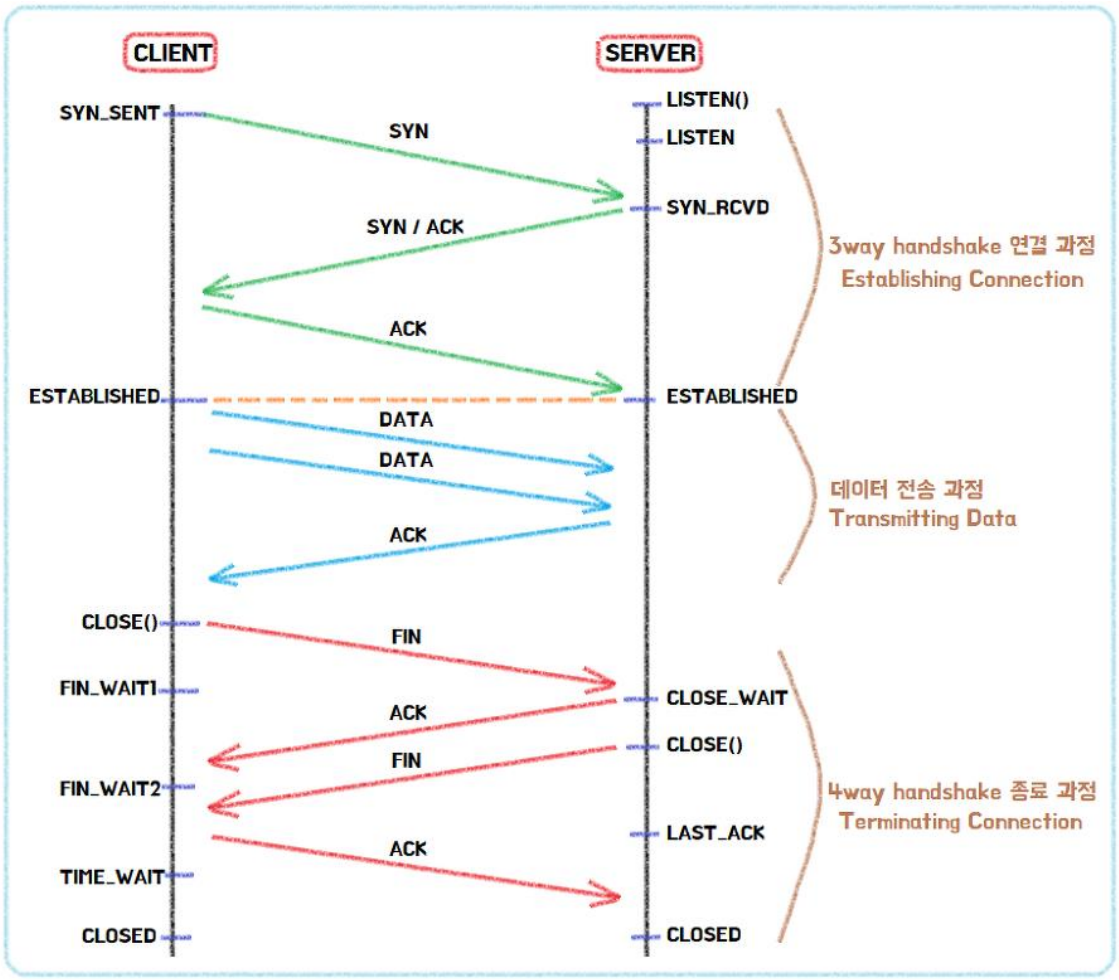
6) 멀티캐스트 전송

(2) 제어

일련의 흐름이기 때문에 기계적으로 분리는 불가능

1) 연결 제어

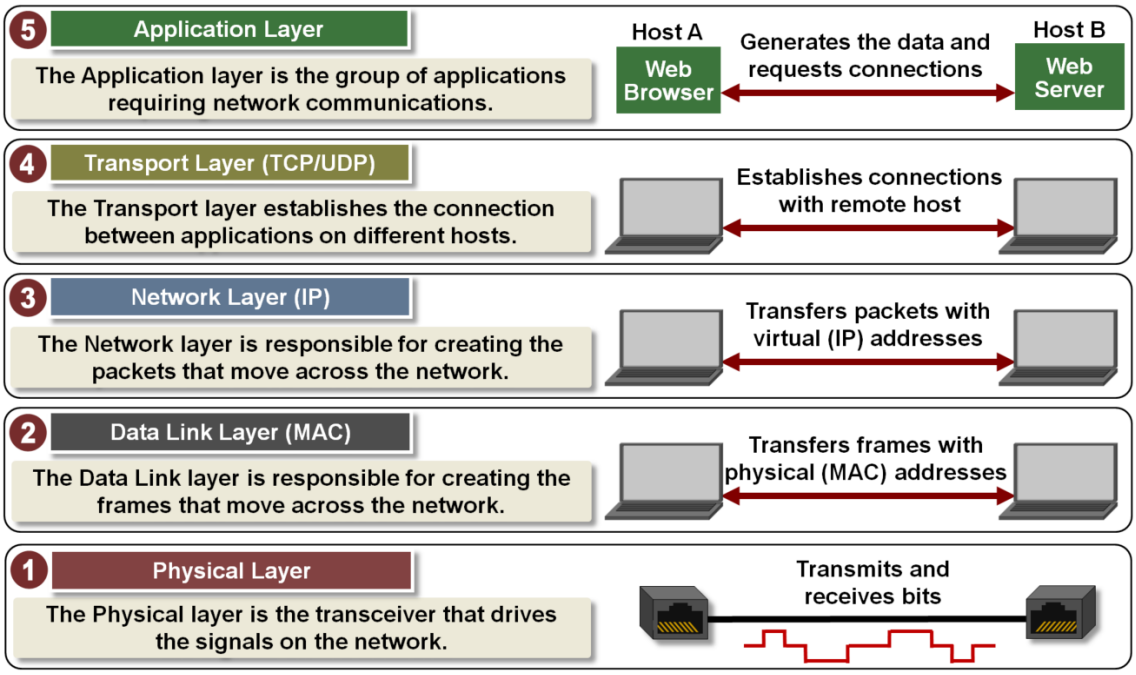
2) 전송 및 흐름 제어


CLIENT
SERVER
SYN_SENT
SYN
LISTEN()
LISTEN
SYN_RCVD
SYN / ACK
ACK
ESTABLISHED
ESTABLISHED
3way handshake 연결 과정
Establishing Connection
DATA
DATA
ACK
데이터 전송 과정
Transmitting Data
CLOSE()
FIN
FIN_WAIT1
CLOSE_WAIT
ACK
CLOSE()
FIN
FIN_WAIT2
4way handshake 종료 과정
Terminating Connection
LAST_ACK
ACK
TIME_WAIT
CLOSED
CLOSED

3) 종료 제어

제2장 TCP/IP 방식의 총론

1. TCP/IP 방식의 개요



(1) 인터넷 표준 프로토콜로서 TCP/IP 방식

1) 빈튼 서프와 밥 칸과 로버트 칸 등이 1973년부터 개발

2) TCP/IP 방식은 단일한 프로토콜을 의미하는 것이 아니라 다양한 프로토콜의 집합체를 의미

(2) 전송 단위의 계층별 종류

편지지	편지 봉투

1) 응용 계층

UDP 페이로드

메시지 단위

2) 전송 계층

UDP 페이로드	UDP 헤더

데이터그램 또는 세그먼트로 단위

3) 네트워크 계층

UDP 페이로드	UDP 헤더	IP 헤더

패킷 단위

4) 데이터 링크 계층

UDP 페이로드	UDP 헤더	IP 헤더	이더넷 헤더

프레임 단위 또는 셀 단위

5) 물리 계층

비트 단위

(3) 인캡슐레이션과 디캡슐레이션 의미

1) 송신 과정에서 일련의 부가 정보를 추가하는 과정을 인캡슐레이션이라 하고 그 역과정을 디캡슐레이션이라고 함

2) 부가 정보와 관련해 주소 정보를 기록하는 부분을 헤더라고 하며 오류 여부를 기록한 부분을 트레일러라고 함

(4) 계층의 의미

1) 통신하기 위한 일련의 과정이나 단계 또는 절차

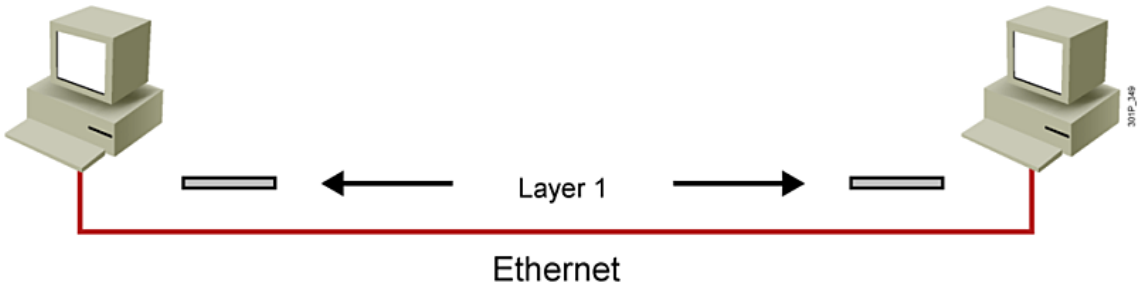
2) 하위 계층으로 내려갈수록 물리적이고 구체적인 속성이 강하고 상위 계층으로 올라갈수록 논리적이고 추상적인 속성이 강함

3) 상위 계층의 기능에는 하위 계층의 기능을 포함

4) 결론적으로 TCP/IP 방식에 따른 일련의 송신이란 상위 계층에서 하위 계층으로 전환하는 과정이고 논리적 속성이 물리적 속성으로 전환하는 과정이고 일련의 부가 정보를 추가하는 과정

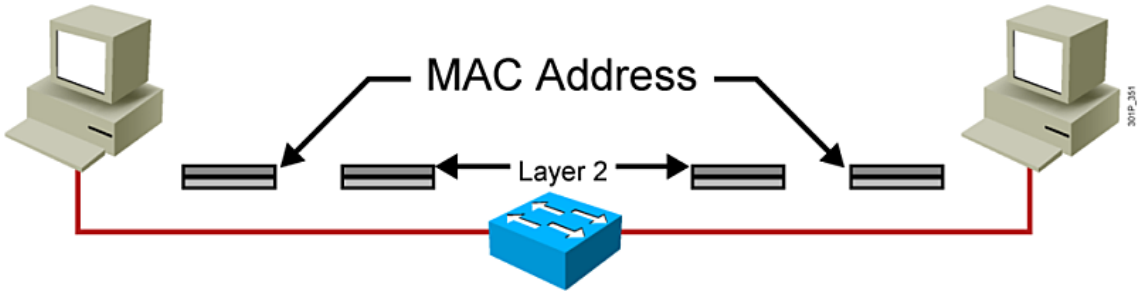
2. TCP/IP 방식에 따른 장비 분류 및 동작 방식

(1) 1계층 장비



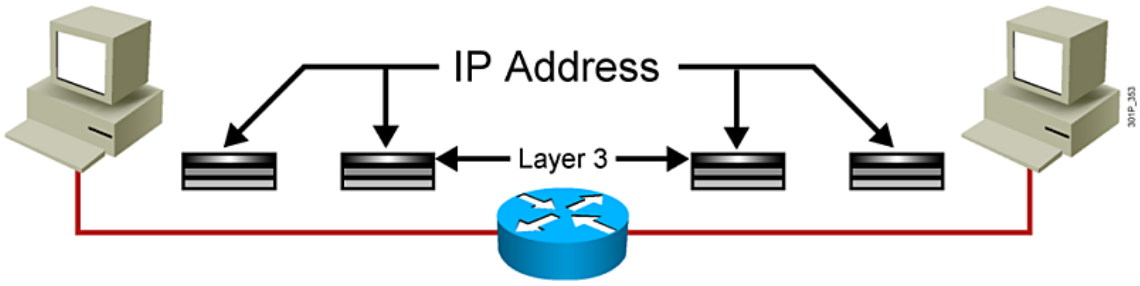
허브 장비와 같이 비트 단위를 처리하는 장치

(2) 2계층 장비



스위치 장비 또는 무선 AP 장비와 같이 프레임 단위를 처리하는 장치

(3) 3계층 장비



라우터 장비와 같이 패킷 단위를 처리하는 장치

제3장 TCP/IP 방식의 응용 계층

1. 응용 계층의 역할

해당 프로토콜에 기반해 실제 정보를 저장한 페이로드를 생성

2. 포트 번호의 개념

서비스	포트 번호	서비스	포트 번호
FTP	TCP 20/21	SSH	TCP 22
TELNET	TCP 23	SMTP	TCP 25
DNS	TCP/UDP 53	DHCP	UDP 67/68
TFTP	UDP 69	HTTP	TCP 80
POP3	TCP 110	NTP	UDP 123
IMAP4	TCP 143	SNMP	UDP 161/162
SSL/TLS	TCP 443	NetBIOS	TCP/UDP 445

(1) 응용 계층에 속하는 프로토콜에 대한 식별 번호

(2) 해당 프로토콜에서 발생한 정보가 흐르는 가상의 통로

(3) IANA 기준에 따른 포트 번호의 종류

1) 0번부터 1,023번까지 잘 알려진 포트 번호

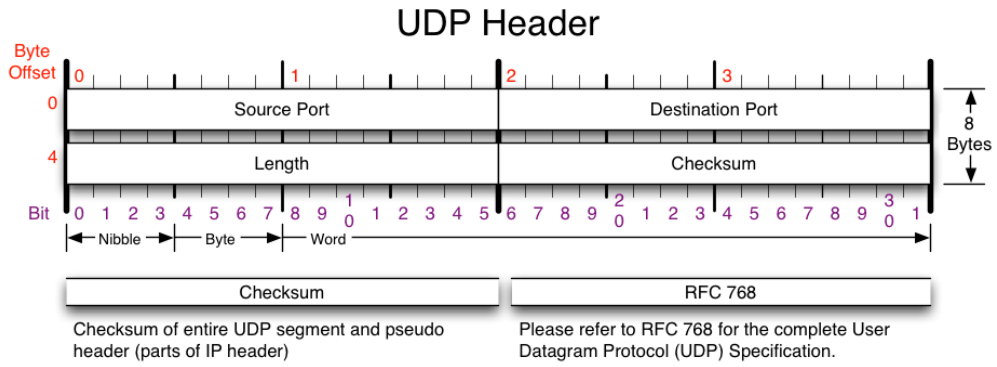
2) 1,024번부터 49,151번까지 등록 포트 번호

3) 49,152번부터 65,535번까지 사설 또는 동적 포트 번호

(4) 출발지 포트 번호는 서비스에 접속할 때마다 운영 체제가 1,024번 이후의 포트 번호를 임의로 할당

제4-1장 TCP/IP 방식의 전송 계층

1. UDP 방식의 특징



(1) 버퍼링 기능이 없는 개념

(2) 단편화가 없는 데이터그램 단위로 전송

(3) 일반적으로 512 바이트 미만의 데이터를 전송

2. TCP 방식의 특징

(1) 버퍼링 기능이 있는 개념

(2) 단편화가 있는 세그먼트 단위로 전송

(3) 일련의 제어 과정

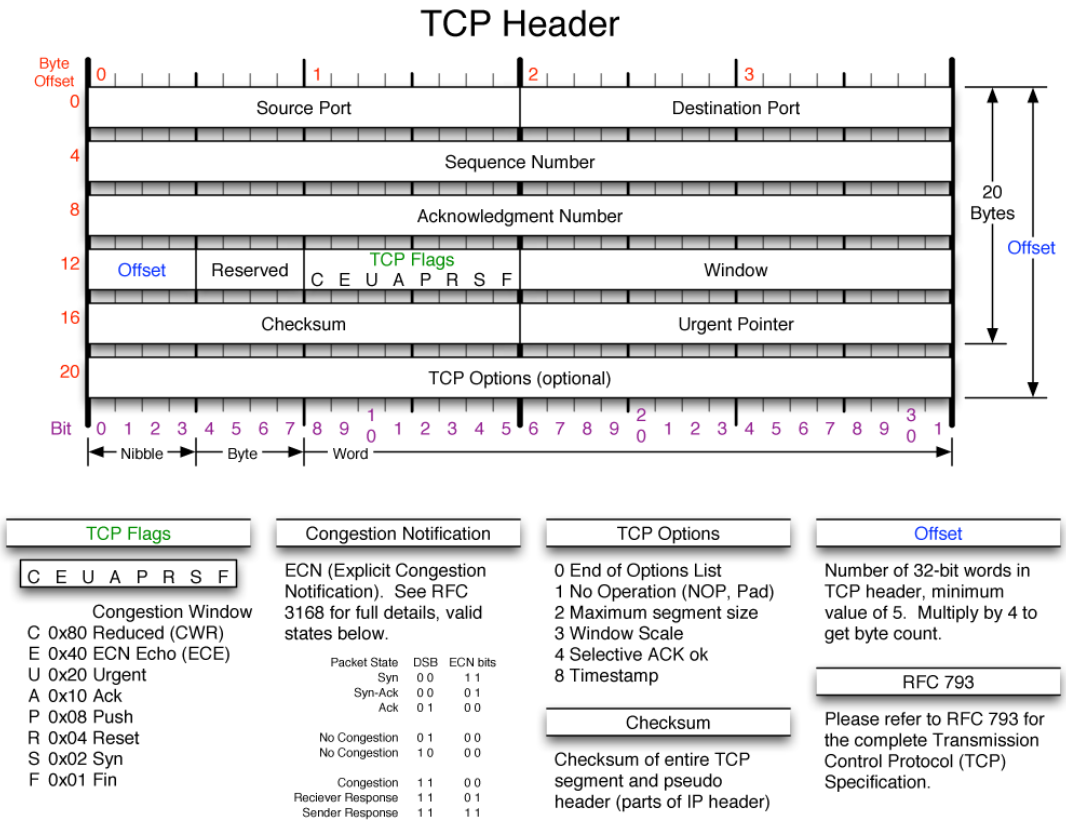
1) 전송 전 3단계 연결 설정 과정

2) 전송 중 오류 발생

송신자는 수신자로부터 ACK 신호를 받아야만 다음 정보를 전송하는데 이를 네글 알고리즘이고 함

3) 흐름 제어

송신자는 수신자의 확인 응답에 따라 전송할 정보의 양을 조절하는데 이를 혼잡 윈도우라고 하며 송신자가 전송할 수 있는 동적인 정보의 양을 슬라이딩 윈도우라고 함



4) 전송 후 3/4단계 연결 종료 과정

(4) 전송 전 3단계 연결 설정 과정과 전송 후 3/4단계 연결 종료 과정은 연속적인 동작

(5) RTO 타이머란 전송 실패한 데이터를 재전송하기 위한 타임아웃

제4-2장 포트 스캔 원리

1. TCP Full Open 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sT

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:37 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.00095s latency).

PORT    STATE SERVICE REASON
22/tcp open  ssh     syn-ack
```

(1) 해당 포트가 열린 경우에는 ACK + SYN 응답

(2) 해당 포트가 닫힌 경우에는 ACK + RST 응답

2. TCP Half Open 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:38 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response (0.000057s latency).

PORT    STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
```

(1) 해당 포트가 열린 경우에는 ACK + SYN 응답

(2) 해당 포트가 닫힌 경우에는 ACK + RST 응답

3. FIN 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sF
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:39 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT    STATE           SERVICE REASON
22/tcp open|filtered ssh       no-response
```

(1) SYN 신호를 차단한 방화벽 등을 통과하기 위한 기법

(2) 해당 포트가 열린 경우에는 무응답

(3) 해당 포트가 닫힌 경우에는 ACK + RST 응답

4. X-mas 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sX

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:39 KST
Nmap scan report for localhost (127.0.0.1)
Host is up, received localhost-response.

PORT    STATE           SERVICE REASON
22/tcp open|filtered ssh       no-response
```

(1) SYN 신호를 차단한 방화벽 등을 통과하기 위한 기법

(2) 해당 포트가 열린 경우에는 무응답

(3) 해당 포트가 닫힌 경우에는 ACK + RST 응답

5. Null 스캔 방식

```
root@debian:~# nmap 127.0.0.1 -p 22 --reason -sN

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 10:40 KST
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up, received localhost-response.

PORT     STATE              SERVICE REASON
22/tcp open|filtered ssh        no-response
```

(1) SYN 신호를 차단한 방화벽 등을 통과하기 위한 기법

(2) 해당 포트가 열린 경우에는 무응답

(3) 해당 포트가 닫힌 경우에는 ACK + RST 응답

제5-1장 TCP/IP 방식의 네트워크 계층

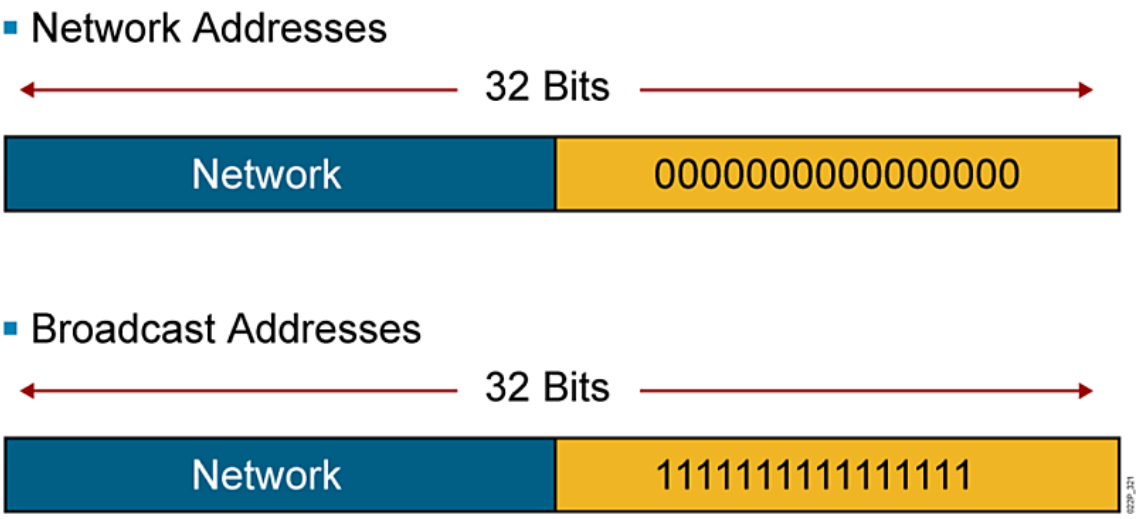
1. IP 주소의 범위

0.0.0.0부터 255.255.255.255까지 총 32 비트

2. IP 주소의 등급

IP Address Class	First Octet Binary Value	First Octet Decimal Value	Possible Number of Hosts
Class A	1-126	00000001 to 01111110*	16,777,214
Class B	128-191	10000000 to 10111111	65,534
Class C	192-223	11000000 to 11011111	254

3. IP 주소의 구성



(1) 네트워크 ID

LAN 영역에 대한 고유한 식별자를 의미하며 등급에 따라 네트워크 ID 범위 결정

(2) 호스트 ID

1) 해당 LAN 영역에 속한 호스트에 대한 고유한 식별자를 의미

2) 호스트 ID에서 모든 비트가 0인 경우를 네트워크 IP 주소라고 하며 모든 비트가 1인 경우를 브로드캐스트 IP 주소라고 함

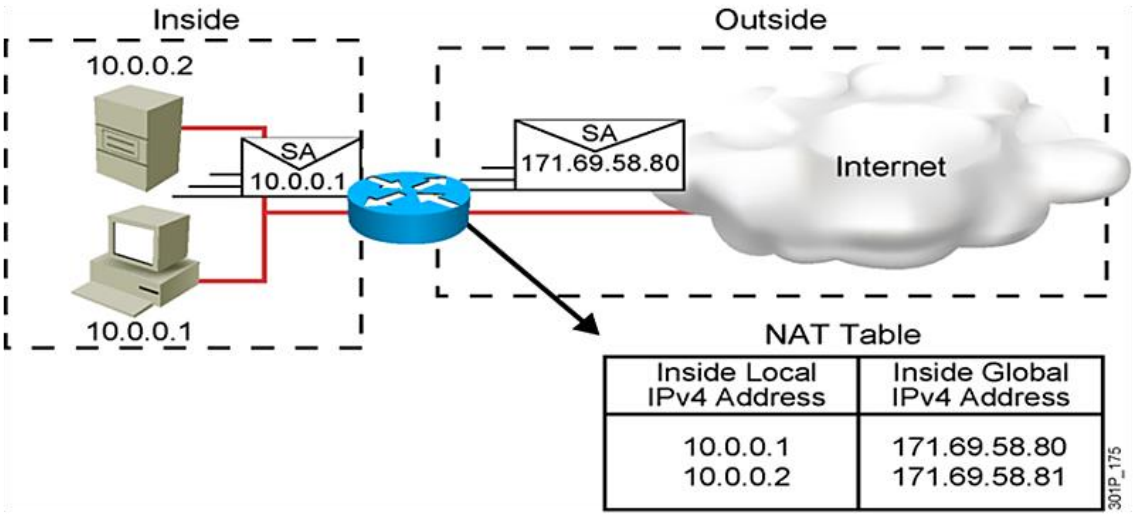
4. 사설 IP 주소 개념

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

LAN 영역 전용 주소로 주소의 고갈을 완화시키고 보안 효과를 얻음

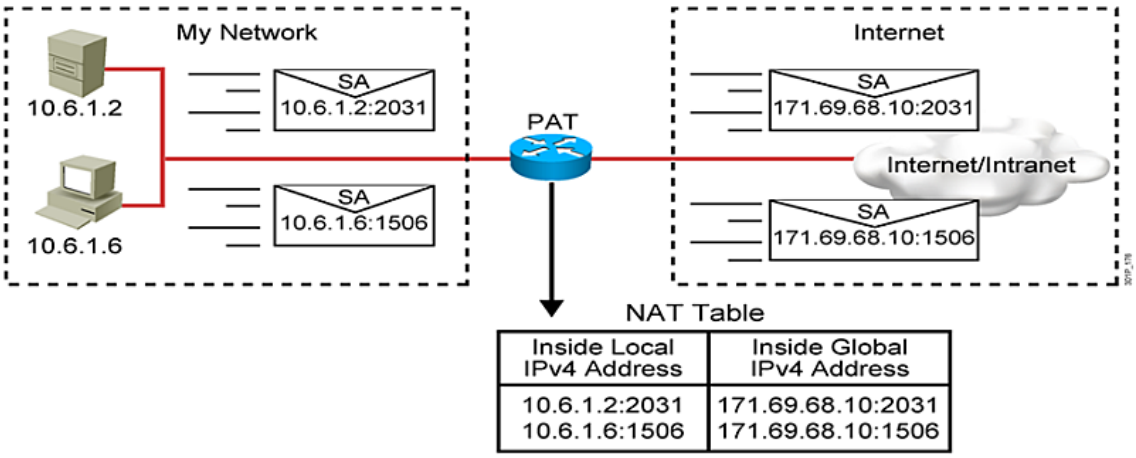
5. IP 주소의 NAT와 PAT 기법

(1) NAT 기법



출발지의 사설 IP 주소를 공인 IP 주소로 변경하는 기법

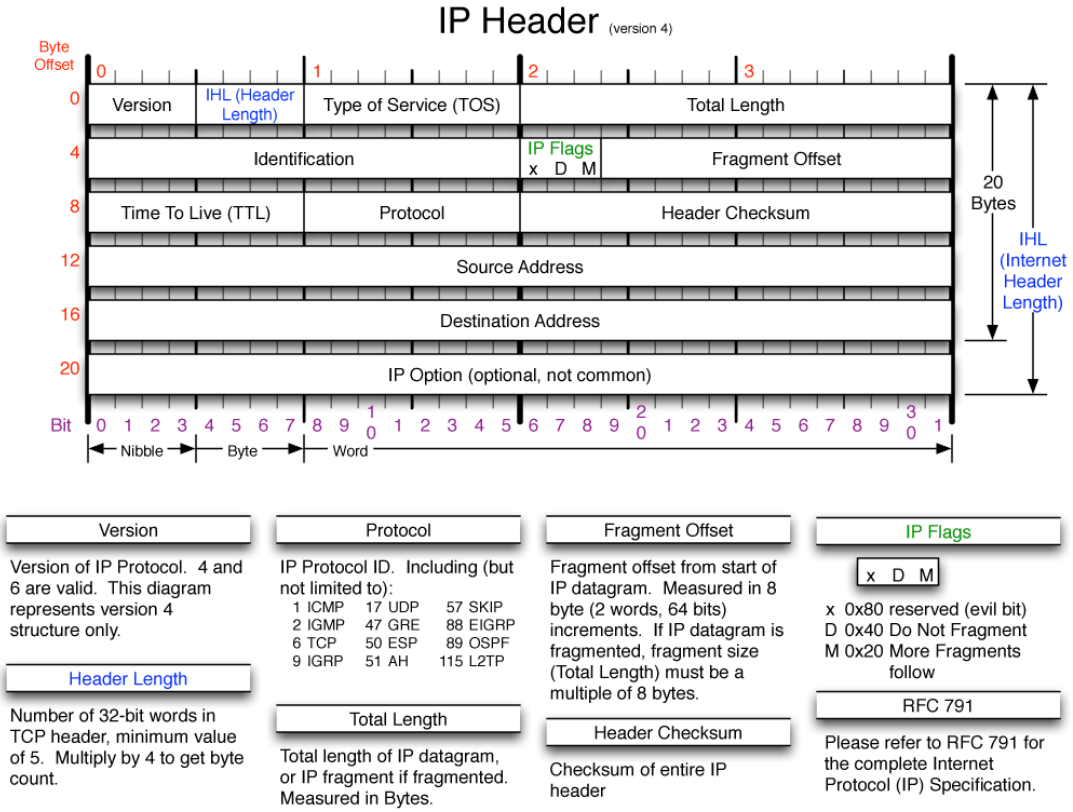
(2) PAT 기법



출발지의 사설 IP 주소를 공인 IP 주소로 변경하고 포트 번호로 구분하는 기법

6. IP 주소의 서브넷 마스크

주어진 IP 주소에서 네트워크 ID와 호스트 ID를 구분하기 위한 식별자



7. IP 주소의 CIDR 기법

제한적인 IP 주소를 C 등급 기준으로 할당하고 라우팅 처리의 부하를 감소할 목적으로 RFC 1519에서 제정

(1) 서브넷

A 또는 B 등급 네트워크 대역을 C 등급 네트워크 대역을 기준으로 할당하는 기법

(2) 수퍼넷

라우터를 대상으로 라우팅 테이블의 크기를 줄이고 플래핑 증상을 방지하며 연속적인 네트워크 대역을 2의 배수에 따라 통합하기 때문에 192.168.10.0/24 대역과 192.168.11.0/24 대역과 192.168.12.0/24 대역과 192.168.13.0/24 대역의 경우에는 192.168.8.0/21 대역와 같이 통합

8. IP 주소의 패킷 분할

(1) MTU 개념 및 종류

이더넷 방식은 1500 바이트이고 PPP 방식은 약 300 바이트

(2) IP 플래그 항목의 구성

1) D 비트가 0이면 분할이고 1이면 미분할을 의미

2) M 비트가 1이면 분할의 연속이고 0이면 분할의 종료를 의미

(3) 패킷 분할의 예

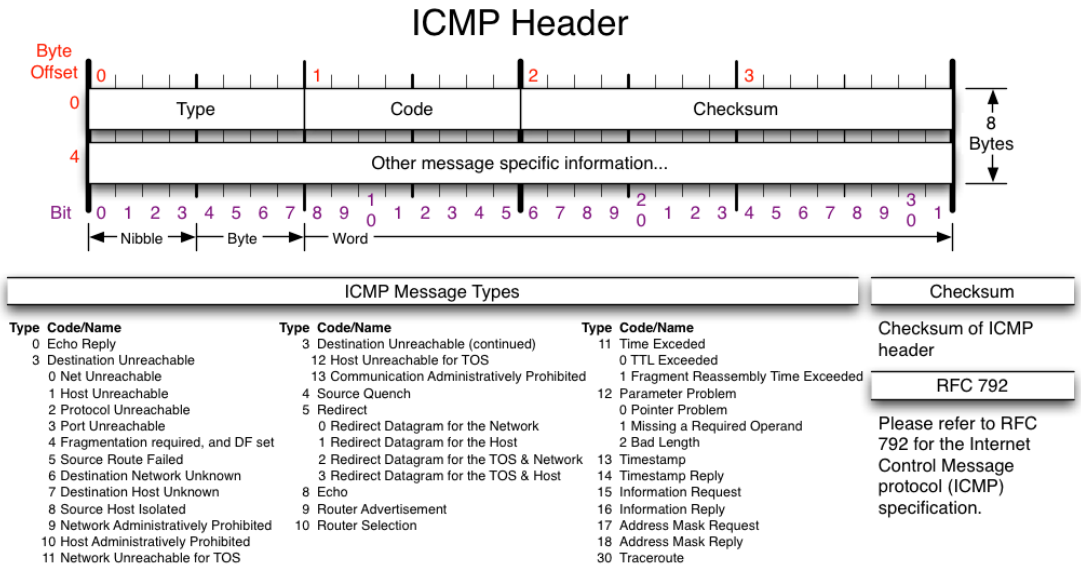
1) 1,500 바이트 패킷의 경우

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
Null	1	Null	Null

2) 6,000 바이트 패킷의 경우

ID 항목	플래그 항목(D 비트)	플래그 항목(M 비트)	플래그먼트 오프셋
1234	0	1	0
1234	0	1	1500
1234	0	1	3000
1234	0	0	4500

제5-2장 ICMP 방식 및 IGMP 방식



1. ICMP 방식의 두 가지 기능

(1) 질의와 응답 기능

(2) 오류 통보 기능

1) 목적지 도달 불가

2) 발신지 억제

혼잡 등이 발생할 경우 라우터 등이 송신자에게 전송 분량이나 속도 등을 줄이라고 알려준다.

3) 시간 초과

4) 매개 변수의 문제

IP 패킷 헤더 항목의 정보가 애매할 경우 라우터 등이 송신자에게 통보

5) 경로 재지정

호스트 자체의 라우팅 테이블에서 목적지로 향하는 라우터를 부적절하게 선택했을 경우 라우터 등이 송신자에게 통보

2. ICMP 방식의 생성 과정

ICMP 페이로드	ICMP 헤더	IP 헤더

무의미한 문자 정보를 생성한 뒤 순서대로 ICMP 패킷 헤더와 IP 패킷 헤더를 부착

3. ICMP 방식에 기반한 ping 명령어와 tracert 명령어

(1) ping 명령어

```
C:₩>ping 8.8.8.8

Ping 8.8.8.8 32바이트 데이터 사용:
8.8.8.8의 응답: 바이트=32 시간=31ms TTL=115
8.8.8.8의 응답: 바이트=32 시간=31ms TTL=115
8.8.8.8의 응답: 바이트=32 시간=31ms TTL=115
8.8.8.8의 응답: 바이트=32 시간=31ms TTL=115

8.8.8.8에 대한 Ping 통계:
패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실), 왕복 시간(밀리초):
최소 = 31ms, 최대 = 31ms, 평균 = 31ms
```

ICMP 방식의 질의 응답 기능에 기반해 구현

(2) tracert 명령어

```
C:₩>tracert 8.8.8.8

최대 30홉 이상의 dns.google [8.8.8.8](으)로 가는 경로 추적:

1    <1 ms    <1 ms    <1 ms  172.30.1.254
```

```
2     1 ms     *        2 ms   220.90.159.254
3     1 ms     1 ms     1 ms   112.188.10.33
4     *        *        *      요청 시간이 만료되었습니다.
5     *        *        *      요청 시간이 만료되었습니다.
6     2 ms     1 ms     2 ms   112.174.70.62
7    29 ms    29 ms    29 ms   72.14.194.106
8    32 ms    31 ms    31 ms   108.170.242.129
9    29 ms    29 ms    29 ms   64.233.175.43
10   31 ms    31 ms    31 ms   dns.google [8.8.8.8]

추적을 완료했습니다.
```

1) 포트 번호 33435번을 사용하는 UDP와 ping 명령어에서 사용하는 TTL 기능을 결합해 구현

2) 경로 추적을 수행할 때마다 라우팅 상황에 따라 다른 경로가 나올 수 있음

3) 일반적으로 윈도우 계열에서는 ICMP 방식을 이용하고 유닉스/리눅스 계열에서는 UDP 방식을 이용

4. IGMP 방식의 기능

그룹 ID로 224.0.0.0부터 239.255.255.255까지 D 등급을 사용

제6장 TCP/IP 방식의 데이터 링크 계층

1. 데이터 링크 계층의 역할

(1) LAN 영역과 WAN 영역에서 사용하는 고유한 프로토콜과 호환성을 보장하기 위한 범용 계층으로 IEEE와 ITU 등에서 관리

(2) 다시 말해, TCP/IP 방식은 데이터 링크 계층을 제외한 나머지 계층만을 IETF에서 관리

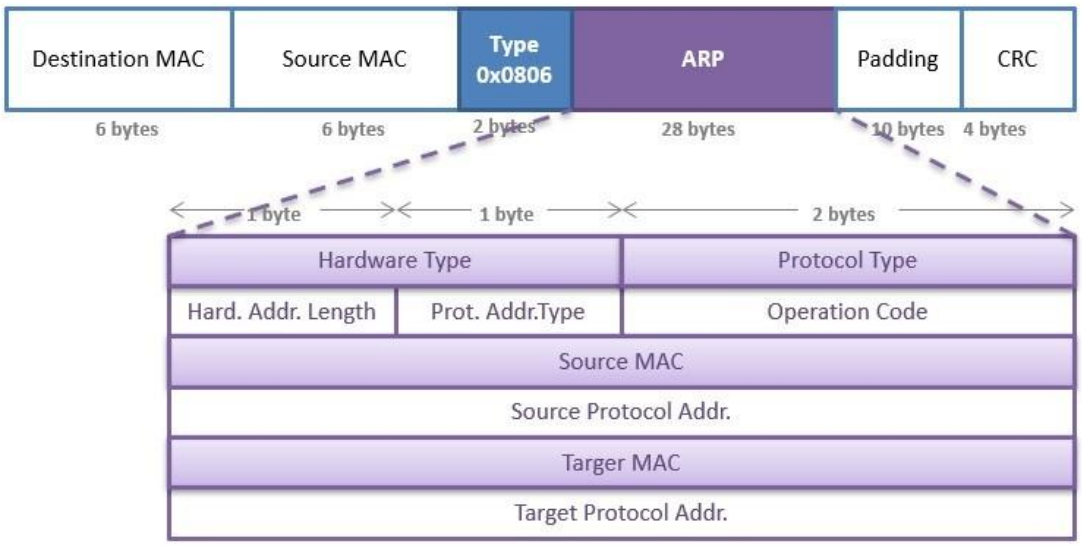
(3) 또한 프레임 헤더가 LAN 영역에 속할 경우에는 MAC 주소가 있지만 WAN 영역에 속할 경우에는 MAC 주소가 없음

2. ARP 방식의 기능과 구조

(1) ARP 방식의 기능

상대방 IP 주소에 기반해 자기가 속한 LAN 영역에서 상대방 MAC 주소를 구하는 기능을 수행

(2) ARP 헤더의 구조



1) 하드웨어 유형

해당 LAN 영역에서 사용하는 프로토콜의 유형을 정의

2) 프로토콜 유형

TCP/IP 네트워크 계층에서 사용하는 프로토콜의 유형을 정의

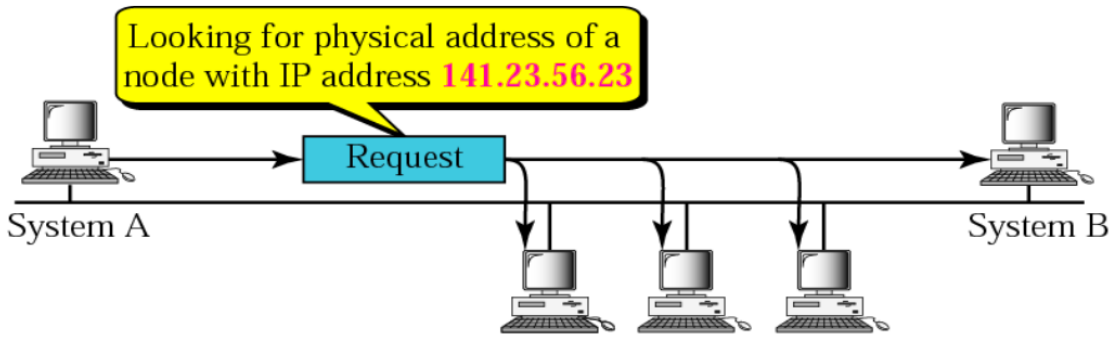
3) 하드웨어 주소 길이

4) 프로토콜 주소 길이

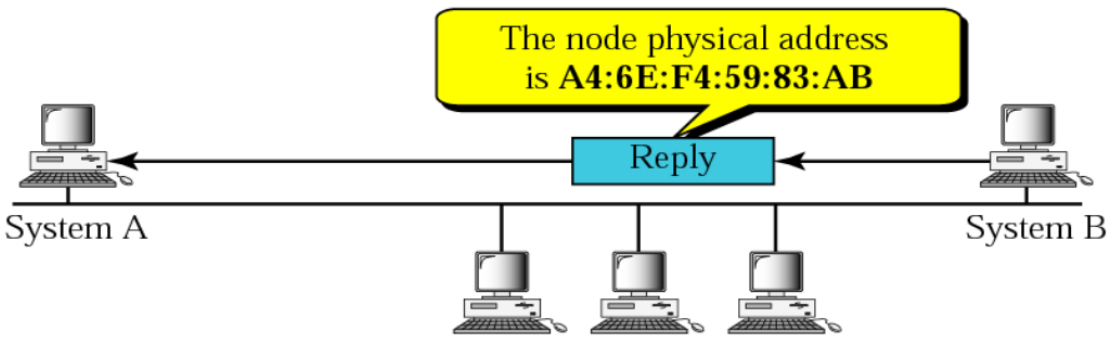
5) 동작 코드

1은 요청이고 2는 응답

3. ARP 방식의 동작 순서



a. ARP request is broadcast



b. ARP reply is unicast

(1) 송신자는 목적지 IP 주소에 대응하는 목적지 MAC 주소를 구하기 위해 라우터를 포함한 동일한 LAN 영역에 속한 모든 호스트를 대상으로 브로드캐스트 방식에 따라 ARP 요청

(2) 수신자는 자신의 MAC 주소를 유니캐스트 방식으로 ARP 응답

```
# cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.10.1     0x1         0x2         00:50:56:c0:00:08     *        eth0
192.168.10.220   0x1         0x2         00:0c:29:c8:66:0d     *        eth0
192.168.10.2     0x1         0x2         00:50:56:ec:c3:ba     *        eth0
```

(3) 송신자는 ARP 캐시 테이블에 해당 목적지 MAC 주소를 등록시킨 뒤 유니캐스트 방식으로 실제 정보를 수신자에게 전송

제7장 TCP/IP 방식에 따른 완전한 전송 과정

1. UDP 방식에 따른 전송 과정

(1) UDP 속성에 따라 응용 계층에서 전송할 메시지 생성

(2) UDP 데이터그램 헤더와 IP 패킷 헤더 생성

(3) ARP 캐시 테이블에 목적지 MAC 주소 검색

(4) 브로드캐스트 방식에 따라 ARP 요청 전송

(5) 스위치 장비에서 플러딩 동작에 의해 ARP 패킷 통과

(6) 목적지에 ARP 패킷 도달

(7) 유니캐스트 방식에 따라 ARP 응답 전송

(8) 스위치 장비에서 포워딩 동작에 의해 ARP 패킷 통과

(9) ARP 캐시 테이블에 목적지 MAC 주소 저장

(10) 버퍼에 저장 중인 패킷 단위로부터 프레임 단위를 완성한 뒤 비트 단위로 전송

2. TCP 방식에 따른 전송 과정

(1) TCP 속성에 따라 응용 계층에서 전송할 메시지 생성

(2) 전송 계층에서 TCP SYN 세그먼트 헤더와 IP 패킷 헤더 생성

(3) 네트워크 계층에서 프레임 헤더 작성을 위한 ARP 패킷 생성

(4) 브로드캐스트 방식에 따라 ARP 요청 전송

(5) 목적지에 ARP 패킷 도달

(6) 유니캐스트 방식에 따라 ARP 응답 전송

(7) ARP 응답 처리

(8) ARP 캐시 테이블에 목적지 MAC 주소 저장

(9) 버퍼에 저장 중인 패킷 단위로부터 프레임 단위를 완성 후 SYN 신호를 전송

(10) SYN 신호의 수신

(11) ACK/SYN 신호의 송신

(12) ACK/SYN 신호의 수신

(13) ACK 신호의 송신

(14) TCP 방식에 따른 송수신자간의 연결 성립

(15) 버퍼에 저장 중인 메시지 단위로부터 순차적으로 비트 단위로 전환한 뒤 전송 개시

(16) 목적지에서 비트 단위 수신 후 순차적으로 메시지 단위로 전환

(17) 전송 계층에서 송신자에게 ACK 응답 발생

제8장 LAN 영역의 개념적 이해

1. LAN 영역의 개념적 정의

(1) MAC 주소에 기반한 내부 통신

(2) 동일한 네트워크 ID 공유

(3) 단일한 ARP 브로드캐스트 영역을 형성

2. OSI 방식에 따른 LAN 영역

(1) 논리 회선 제어 부계층

OSI 방식의 네트워크 계층과 데이터 링크 계층의 중간 매체로서 랜 카드의 장치 드라이버에 해당

(2) 매체 접근 제어 부계층

1) 전송 단위 프레임 생성

2) 장치 식별 주소 제공

3) LAN 범위의 전송 제어

(3) 물리 계층

1) 매체 전송 담당

2) 인코딩 및 디코딩 수행

3) 다양한 토폴로지 제공

3. 이더넷의 시작

미국의 로버트 멧칼프가 1969년 무선 통신을 구현하기 위해 설계한 알로하넷 방식에서 기

원

4. 이더넷의 발전

(1) 초기 이더넷

1) 버스 토폴로지 기반

2) 매체로 10 BASE 2 또는 10 BASE 5와 같은 동축 선로 사용

3) CSMA/CD 방식 사용

(2) 구식 이더넷

1) IEEE 802.3 제정

2) 매체로 10 BASE T와 같은 UTP 회선 사용

3) 허브를 통해 물리적 스타 토폴로지와 논리적 버스 토폴로지 구현

(3) 고속 이더넷

1) IEEE 802.3u 제정

2) 스위치를 통해 물리적 스타 토폴로지와 논리적 점대점 구축

(4) 기가비트 이더넷

1) IEEE 802.3z 제정

2) 매체로 IEEE 802.3ab 방식의 1000 BASE-T 및 1000 BASE-SX와 1000 BASE-LX 같은 광 섬유 사용

(5) 10 기가비트 이더넷

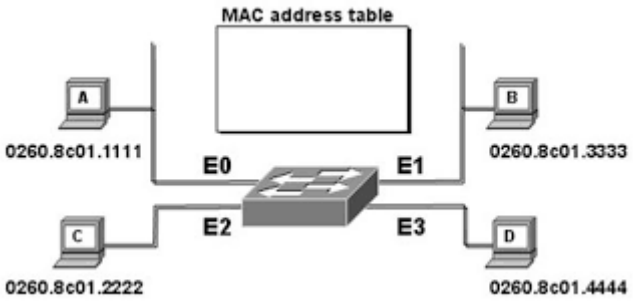
1) IEEE 802.3ae 제정

2) 광 섬유 전용 및 CSMA/CD 방식 제거

(6) 100 기가비트 이더넷

IEEE 802.3ba 제정

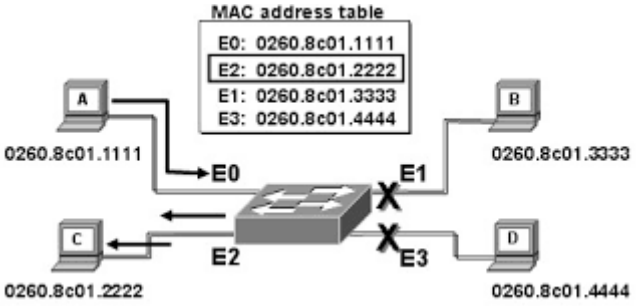
5. 스위칭 동작 과정



(1) 송신자의 주소를 등록하고 목적지의 주소를 검색하는 러닝 기능 수행

(2) 목적지의 주소가 없을 경우 입력 포트를 제외한 모든 포트를 대상으로 플러딩 기능 수행

(3) 목적지의 주소가 있을 경우 블럭킹과 포워딩 기능을 동시에 수행



(4) 일정 시간 동안 해당 주소에서 통신이 없는 경우 에이징 기능을 수행

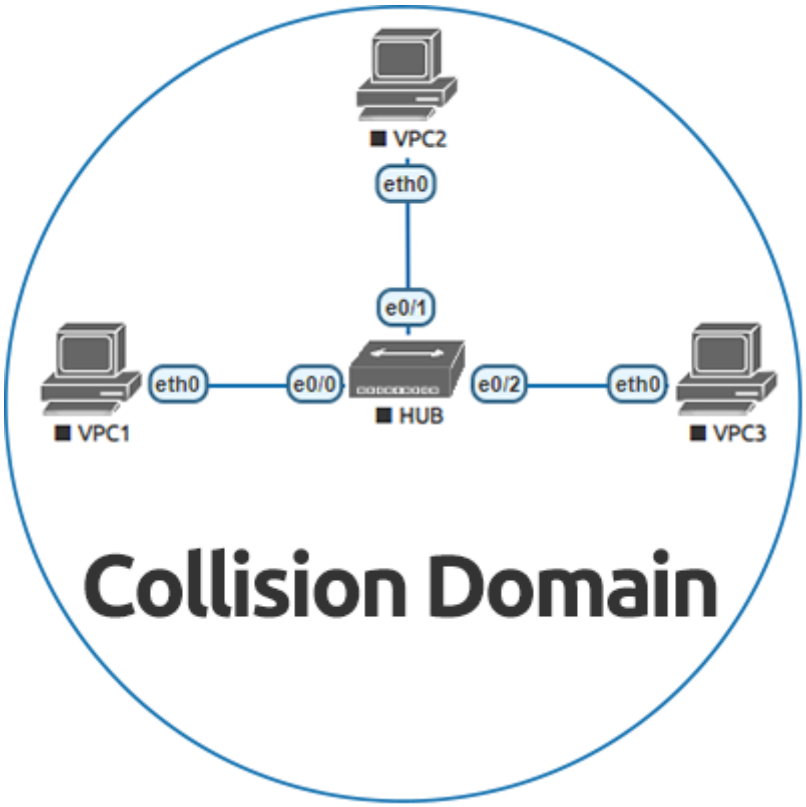
(5) 허브와 스위치 연결시 문제

1) 허브의 반이중 방식과 스위치의 전이중 방식 사이에서 충돌이 발생해 전체적인 속도 저하가 발생

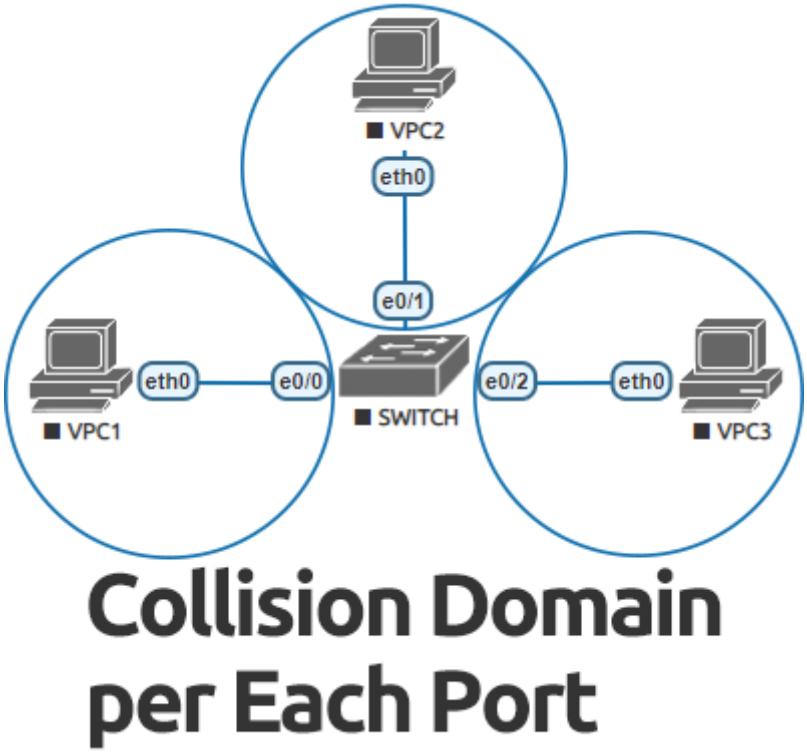
2) 스위치에 불필요한 주소 누적 및 이에 따른 플러딩 동작 발생 가능성

6. 충돌 영역 관점에서 허브와 스위치의 비교

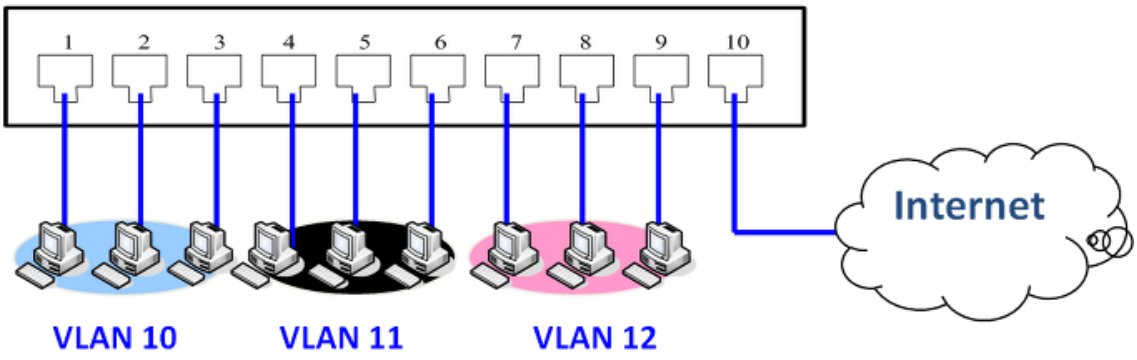
(1) 허브 한 대가 단일 충돌 영역을 생성



(2) 스위치 포트 한 개가 단일 충돌 영역을 생성



7. 가상 LAN



(1) 등장 배경

ARP 브로드캐스트 등에 따른 과부하 문제와 보안 문제 등을 해결하기 위해 등장

(2) 구현 방법

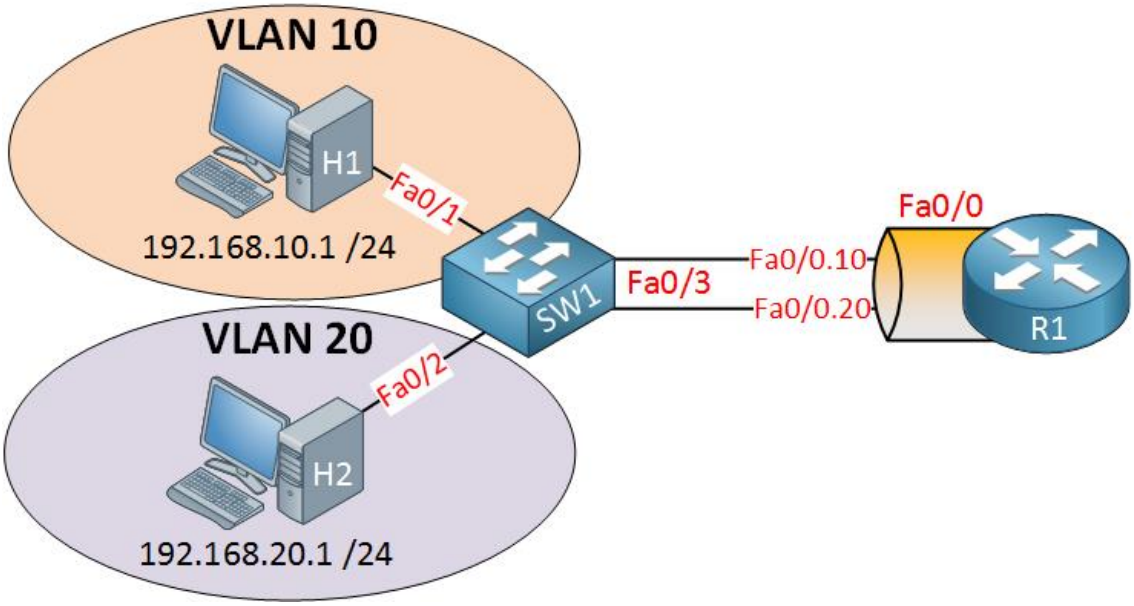
1) 논리적 방식

단일 IP 주소 대역을 서브넷 대역으로 분리

2) 물리적 방식

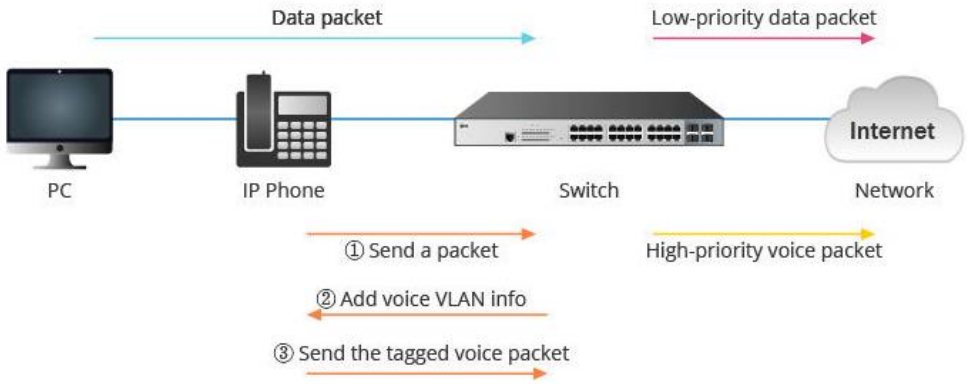
일반적으로 스위치 장비의 포트에 기반해 ARP 브로드캐스트 영역을 분리

(3) 상이한 VLAN 사이의 통신 구현



L3 스위칭 또는 VLAN 라우팅

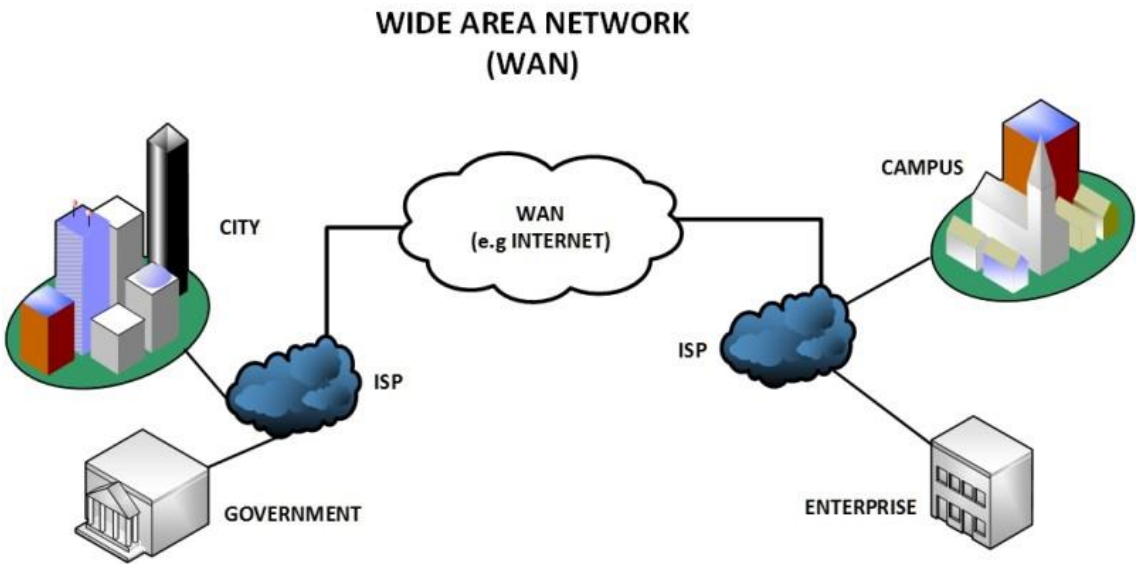
(4) 음성 VLAN



물리적으로 IP 전화기와 PC를 스위치의 한 포트에 연결하지만 논리적으로는 서로 상이한 VLAN으로 구성

제9장 WAN 영역의 개념적 이해

1. WAN 영역의 개념적 정의



IP 주소에 기반한 외부 사이의 통신 영역

2. WAN 영역의 구성

(1) WAN 영역의 계층 구조

(2) DTE와 DCE를 연결하는 회선의 종류

(3) 전통적인 WAN 영역의 구성

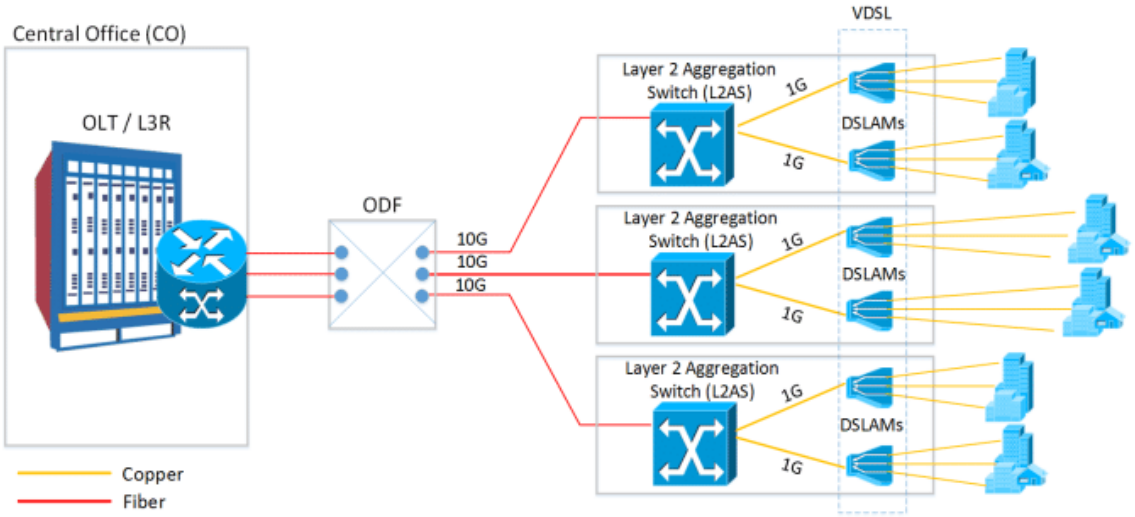
3. OSI 방식의 1계층에 따른 WAN 종류

(1) 전용 회선 방식

(2) 회선 교환 방식

(3) 가상 회선 방식

(4) 메트로 이더넷 방식

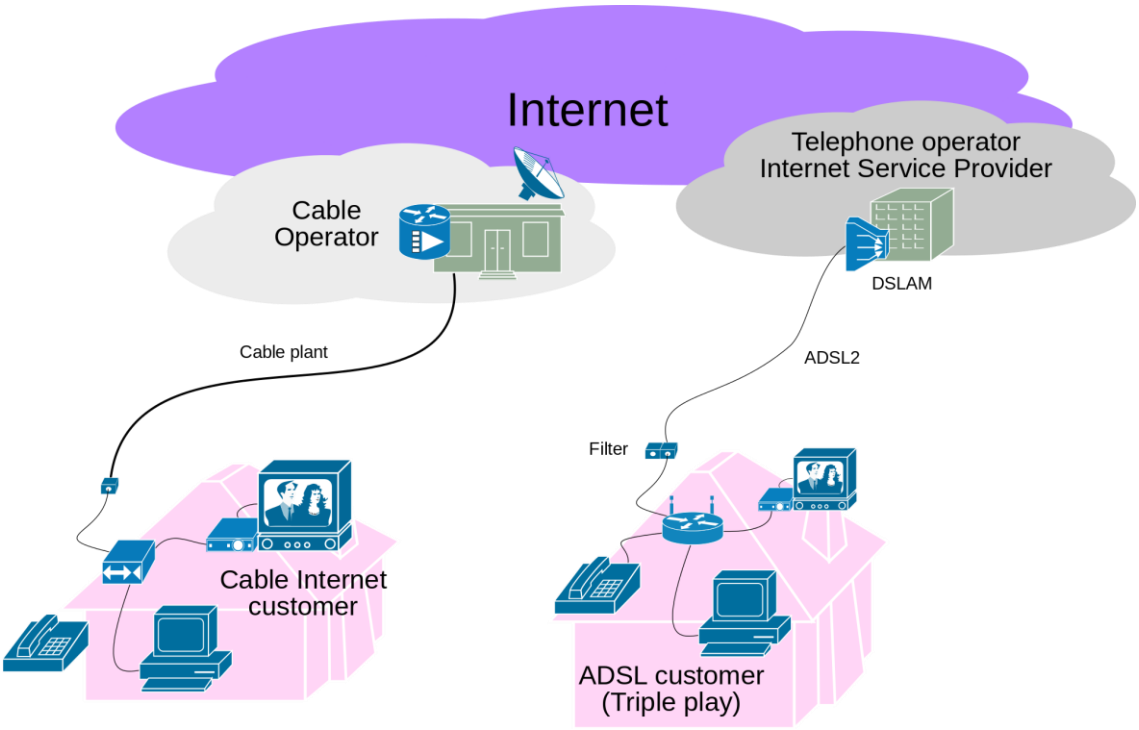


1) LAN 영역에서뿐만 아니라 WAN 영역까지 이더넷 방식을 확장한 기술

2) 광 섬유를 이용해 최대 100Km까지 적용 가능

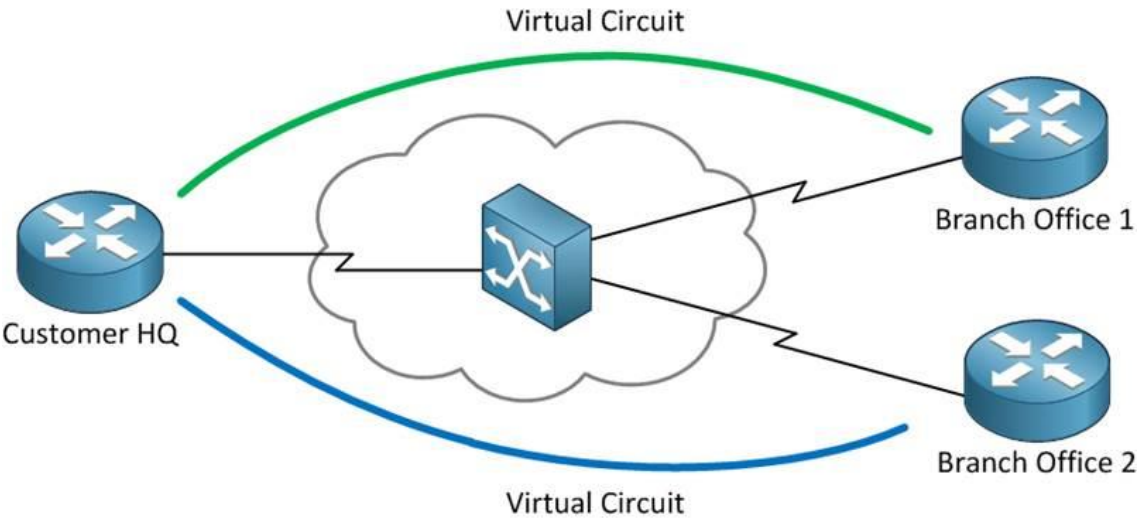
3) 오직 점대점 기능만을 지원하는 IEEE 802.3ae에서만 구현

(5) 브로드밴드 방식



서비스 제공 업체에서 라우터와 스위치 등을 설치한 뒤 가입자로 하여금 방송망이나 통신망 등을 이용해 인터넷에 접속할 수 있도록 하는 기법

4. OSI 방식의 2계층에 따른 WAN 종류



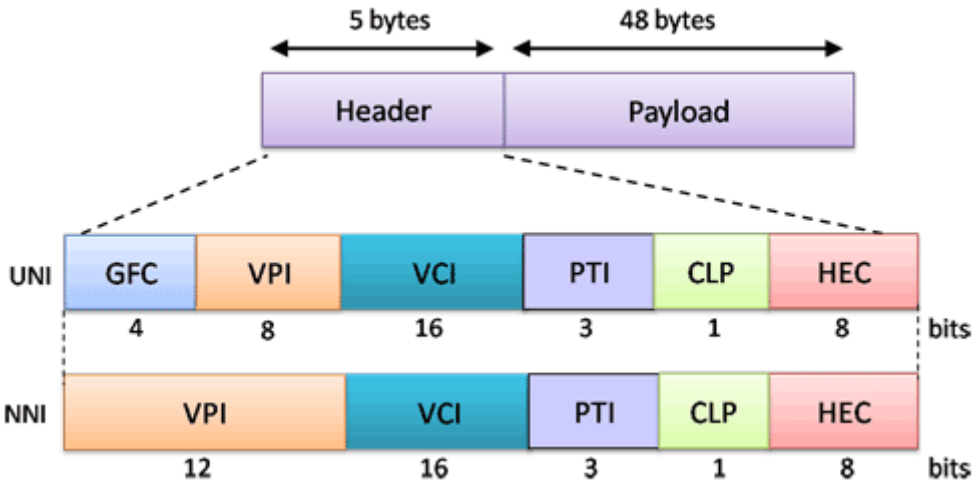
(1) X.25 방식

가상 회선 기능을 제공

(2) 프레임 릴레이 방식

가상 회선 기능을 제공

(3) ATM 방식



1) 가상 회선 기능을 제공

2) 셀이란 일정한 길이의 프레임 단위을 의미

(4) HDLC 방식

(5) PPP 방식

인증과 압축 기능을 제공

(6) PPPoE 방식

인증 기능을 내장한 PPP 헤더에 이더넷 헤더를 추가하는 일종의 터널링 방식