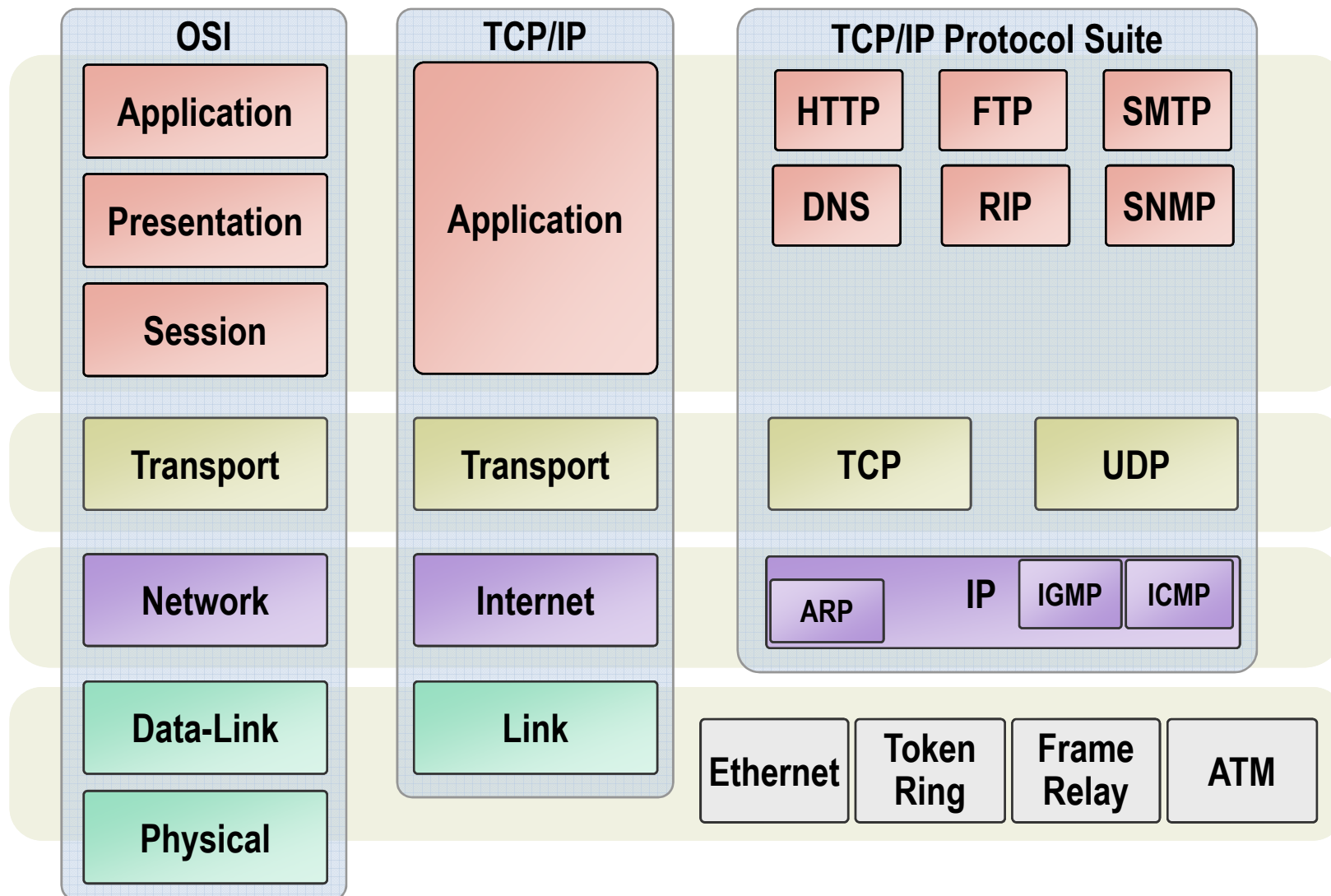




Module 01:

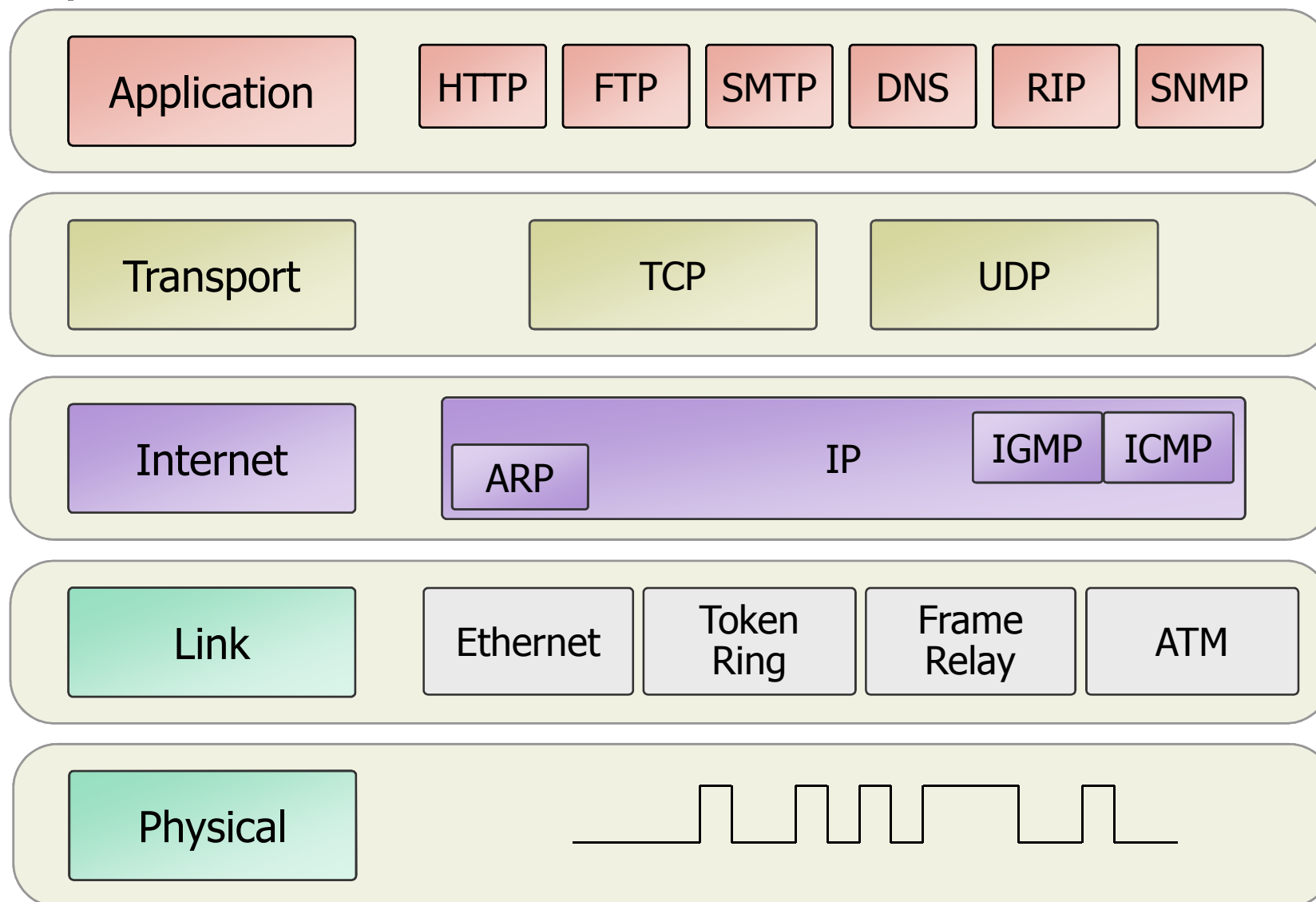
TCP/IP Network

OSI Layer와 TCP/IP Layer 비교



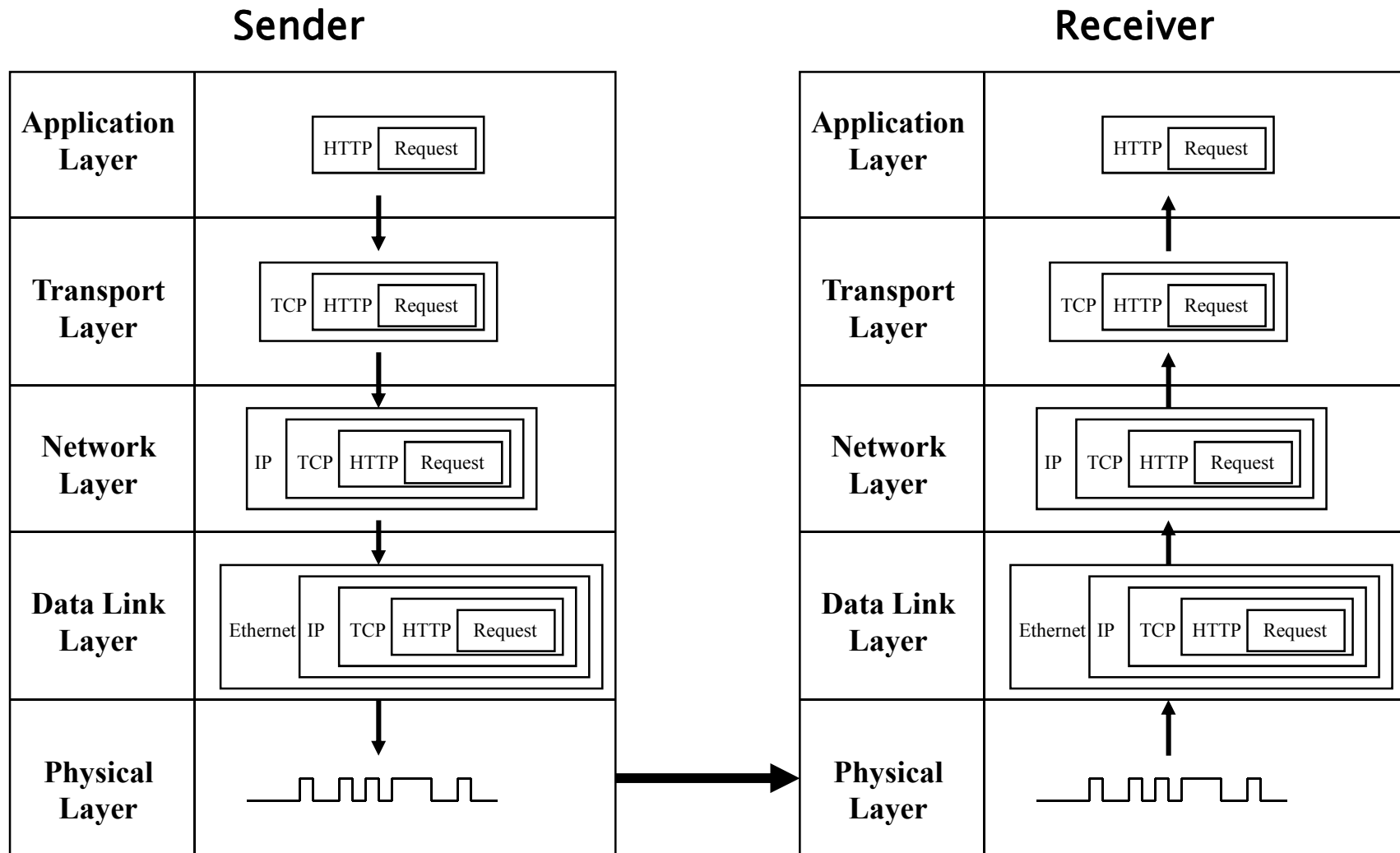


TCP/IP Protocol Suite

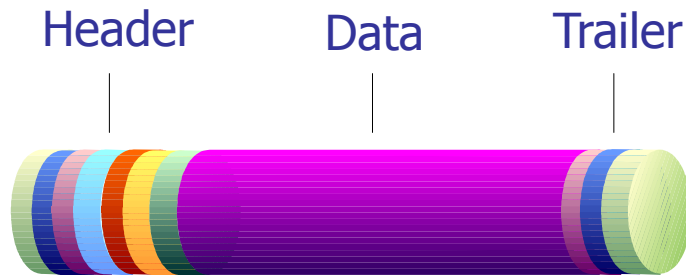




Data Encapsulation 및 De-encapsulaiton



Packet Components



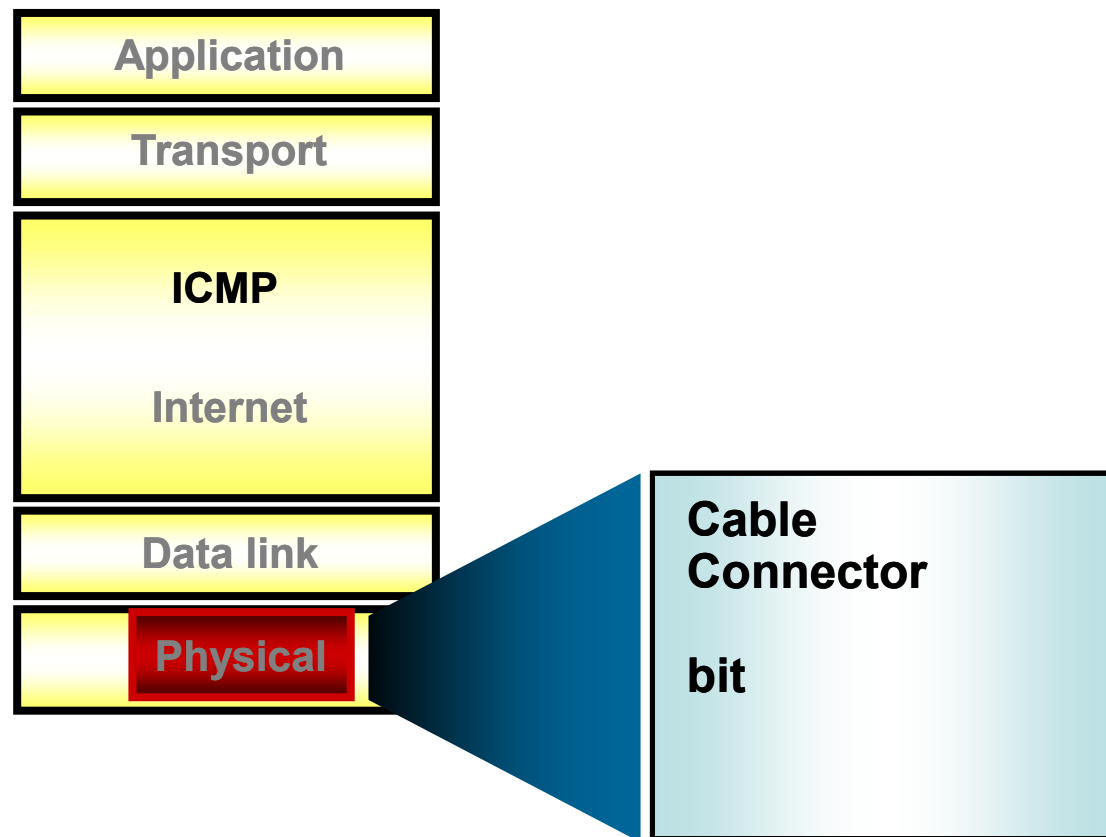
Packet 생성이유?

1. 네트워크점유현상을 막기 위해
2. 데이터의 오류제어를 빠르게 하기 위해

Ethernet Header	
Destination:	00:50:BF:26:E0:2C
Source:	00:04:76:72:32:B8
Protocol Type:	0x0800 IP
IP Header - Internet Protocol Datagram	
Version:	4
Header Length:	5 (20 bytes)
Type of Service:	%00000000
Precedence:	Routine, Normal Delay, Normal Throughput,
Total Length:	40
Identifier:	54473
Fragmentation Flags:	%010 Do Not Fragment Last Fragment
Fragment Offset:	0 (0 bytes)
Time To Live:	128
Protocol:	6 TCP - Transmission Control Protocol
Header Checksum:	0x0000
Source IP Address:	192.168.100.3 vmdc.koreamoon.net
Dest. IP Address:	219.241.88.110 ksdcd.koreamoon.net
No IP Options	
TCP - Transport Control Protocol	
Source Port:	1926
Destination Port:	20 ftp-data
Sequence Number:	1010157960
Ack Number:	1737408473
Offset:	5 (20 bytes)
Reserved:	%000000
Code:	%010000 Ack
Window:	20440
Checksum:	0x5926 Checksum invalid. Should be:
Urgent Pointer:	0
No TCP Options	
Extra bytes (Padding):	
Data: (6 bytes)	
FCS - Frame Check Sequence	
FCS (Calculated):	0x6572DAAA



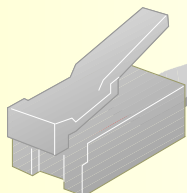
Physical Layer





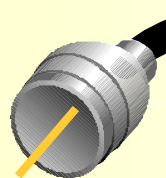
Cable and Connector

Twisted-Pair
10BaseT



Unshielded (UTP)
Shielded (STP)

Coaxial



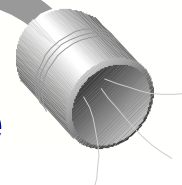
10Base2, 10Base5

ThinNet
ThickNet

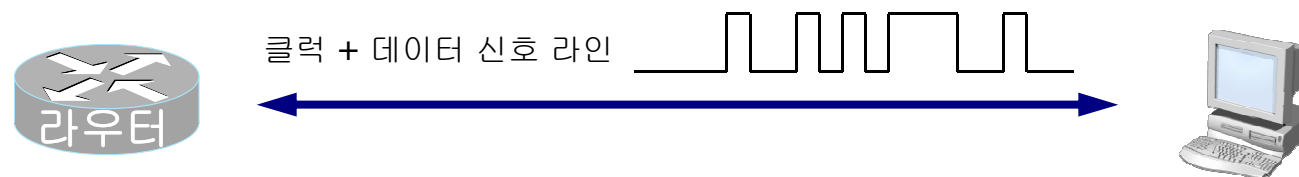
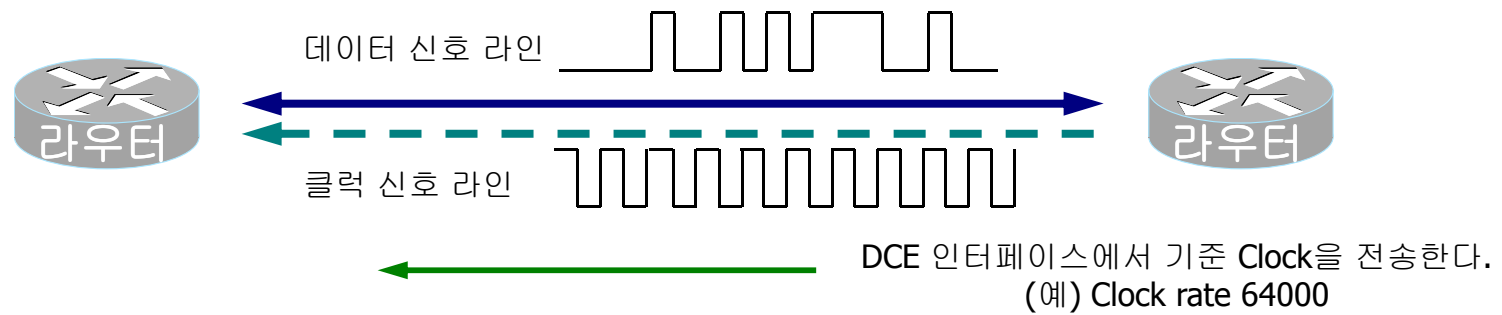
Fiber-Optic

10BaseFx

Multi Mode
Single Mode

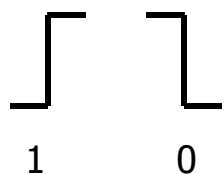
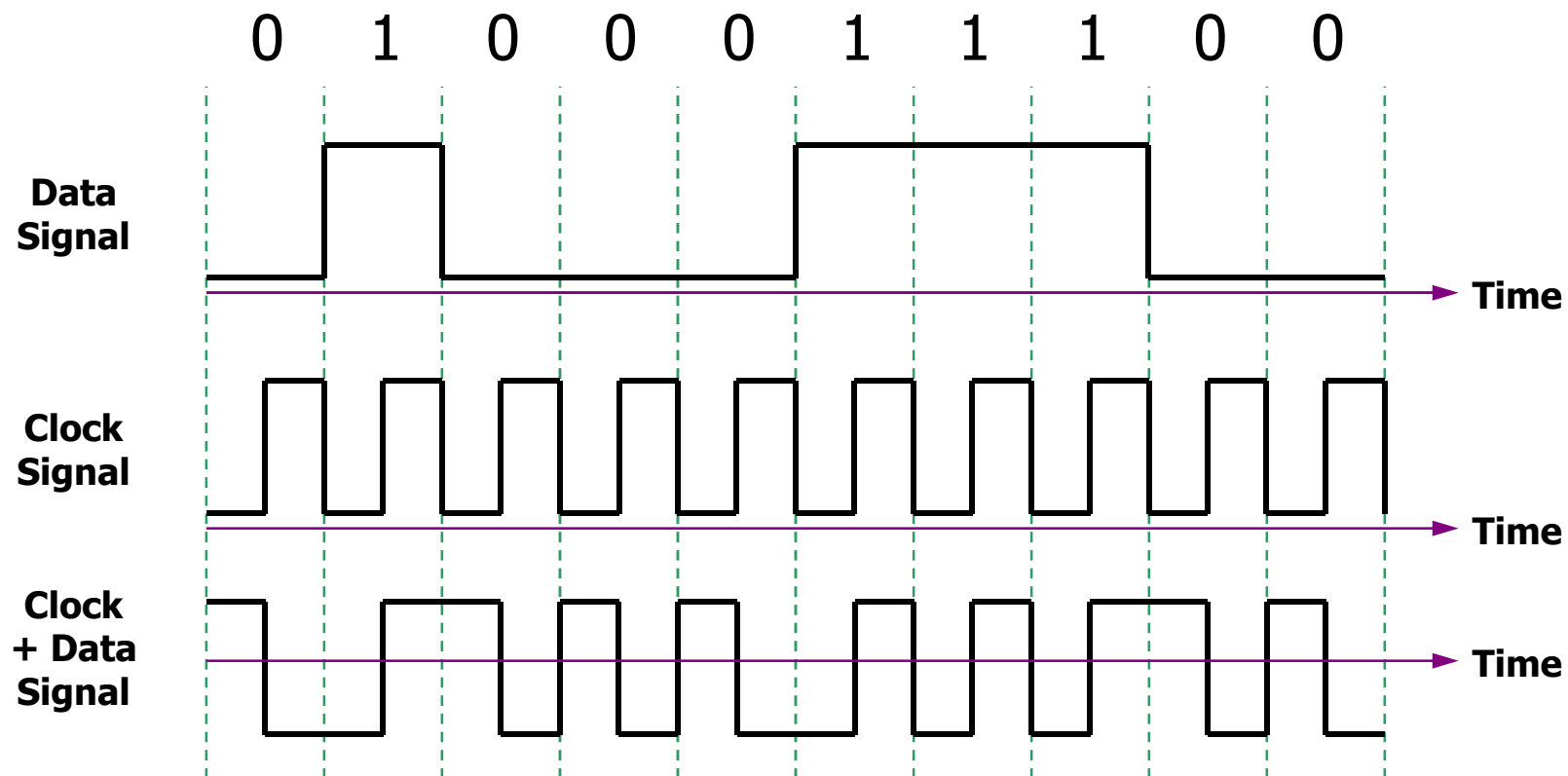


Clock 신호 동기 방법 (0과1 bit를 전달하는 방법)



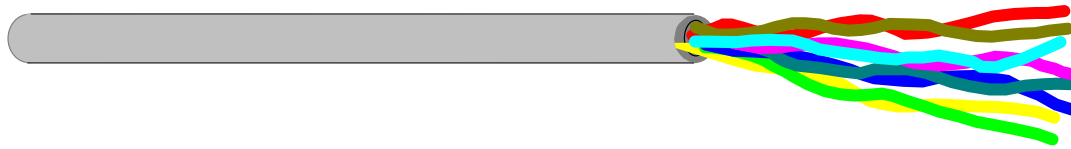


Ethernet (10Mbps) 상의 클럭 신호 와 데이터 신호의 파형

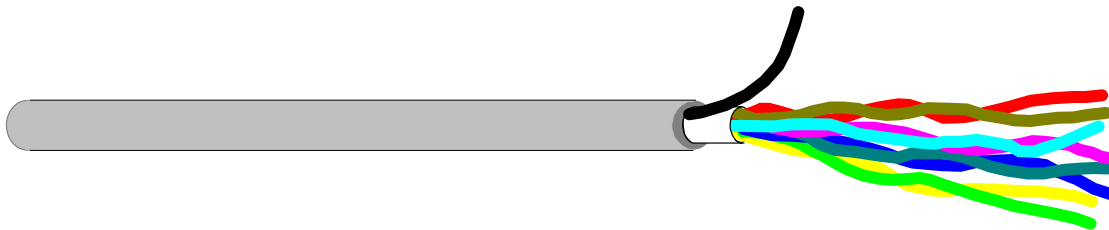


Ethernet(10Mbps)는 맨체스터(Manchester) 인코딩(encoding) 방식을 사용한다. 일정 시점에서 Low에서 High로 변하면 1, High에서 Low로 변하면 0으로 판단하는 신호 항상 주기적으로 변하기 때문에 클럭 신호가 필요 없다. (데이터 신호에 클럭(Clock) 신호가 포함되어 있음.)

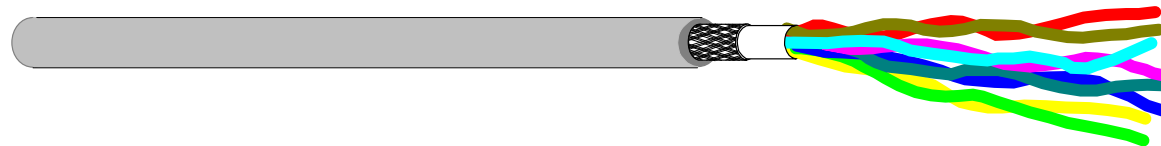
UTP Cable Type




무차폐
UTP



Foil 차폐
FTP

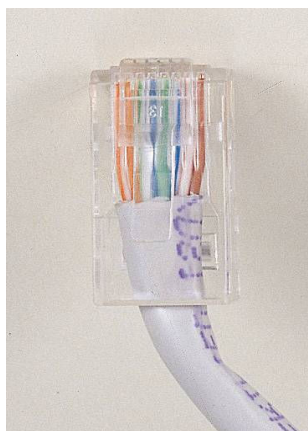


Foil 및 편조 차폐
S-FTP



UTP Cable Category

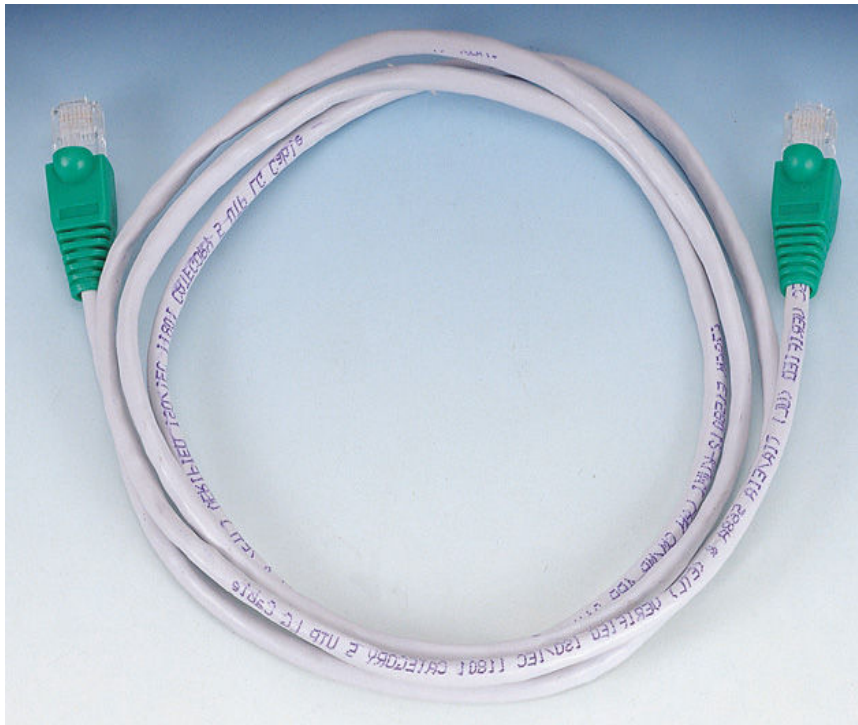
CAT 1	1 Mbps 미만	아날로그 음성 (일반적인 전화 서비스) ISDN BRI 연결용
CAT 2	4 Mbps	주로 IBM의 토큰링 네트워크에 사용
CAT 3	16 Mbps	10BaseT Ethernet 데이터 및 음성 전송
CAT 4	20 Mbps	16 Mbps 토큰링에서 사용 그리 많이 사용되지 않음.
CAT 5	100 Mbps	100 Mbps FastEthernet Network 현재 가장 보편적으로 사용되고 있음.
CAT 6	200MHz ~ 250MHz	1000 Mbps 네트워크를 구성하기 위해 만들어 졌다.



Pin	Wire Pair T is Tip R is Ring
1	Pair 2 T2
2	Pair 2 R2
3	Pair 3 T3
4	Pair 1 R1
5	Pair 1 T1
6	Pair 3 R3
7	Pair 4 T4
8	Pair 4 R4

기본 Network 구축장비

■ LAN Cable – UTP(Unshielded Twisted Pair)



- 명칭 : RJ-45
10/100Base-T
- 전송속도 : 10/100Mbps
- 연결거리 : 100M
- 3대 이상의 PC 연결시
허브 필요



UTP Straight-through Cable

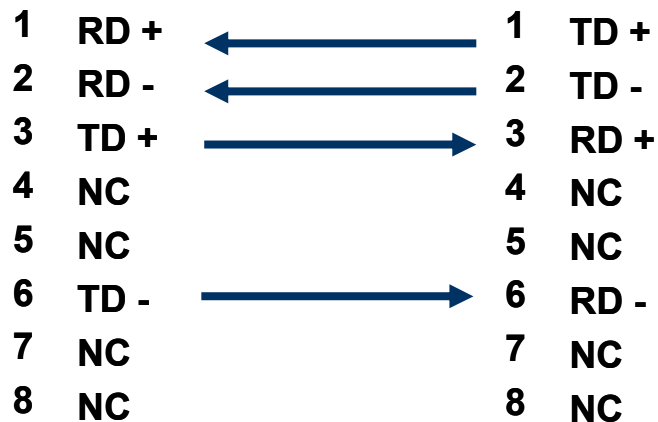
Cable 10BaseT/ 100BaseT Straight-through



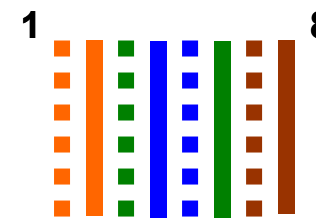
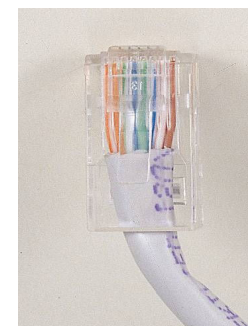
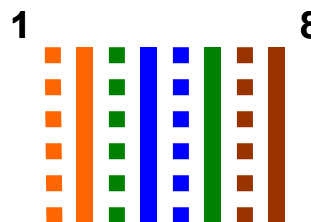
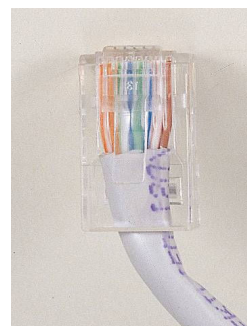
Hub/Switch



Server/Router



Straight-through Cable



케이블 배선을 양끝을
동일하게 배치한다.

UTP Crossover Cable

Cable 10BaseT/ 100BaseT Crossover

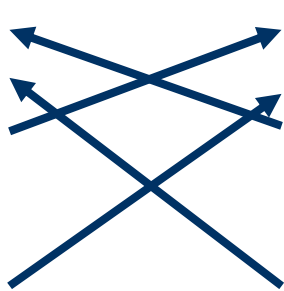


Hub/Switch



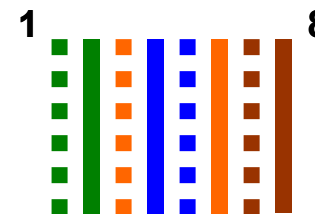
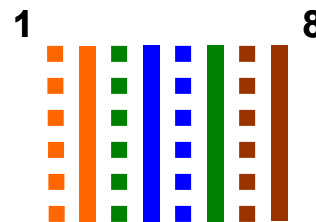
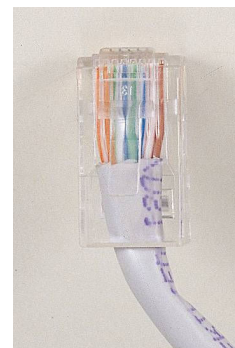
Hub/Switch

Pin	Label
1	RD +
2	RD -
3	TD +
4	NC
5	NC
6	TD -
7	NC
8	NC



Pin	Label
1	RD +
2	RD -
3	TD +
4	NC
5	NC
6	TD -
7	NC
8	NC

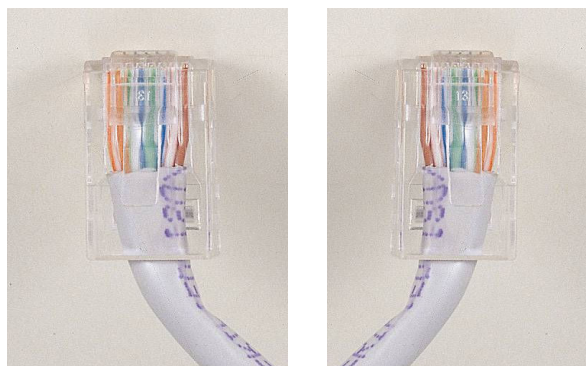
Crossover Cable



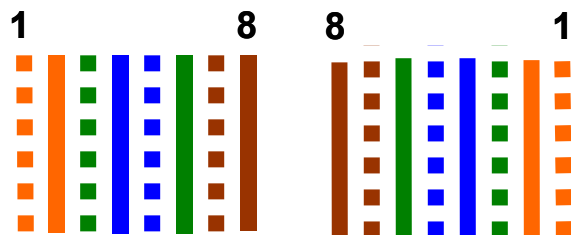
1→3, 2→6 케이블을
크로스 시킨다.



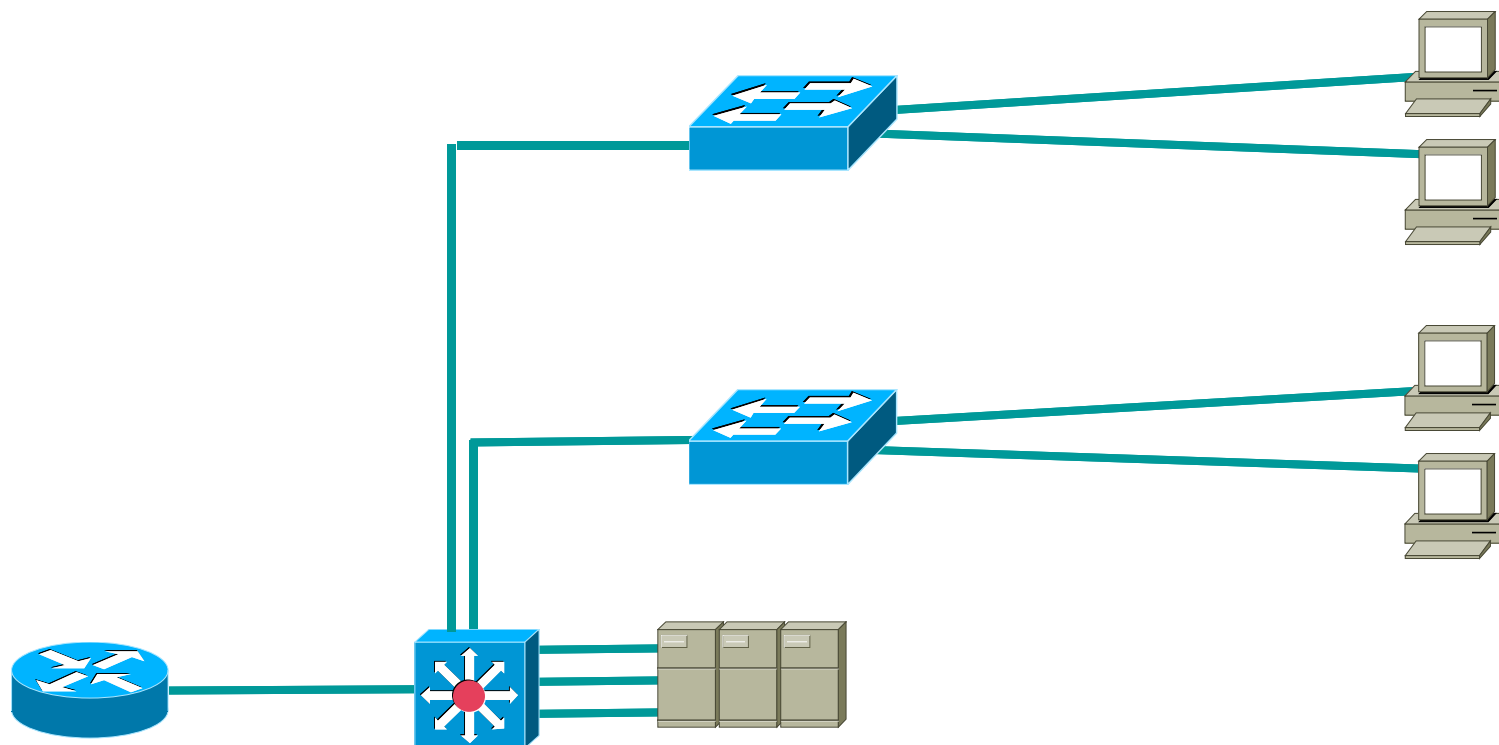
UTP Rollover Cable



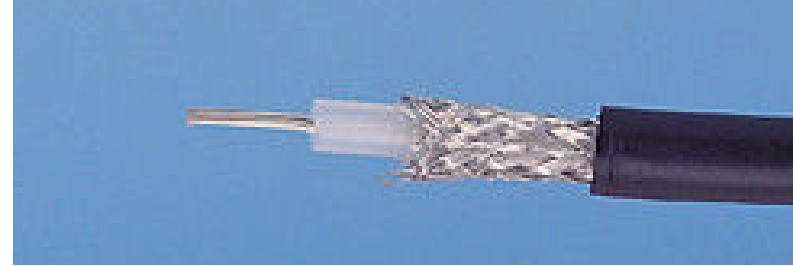
한쪽 케이블을 **Rollover** 시킨다.
Rollover Cable은 라우터나
스위치 관리 콘솔 케이블로
사용된다.



Cabling the Campus



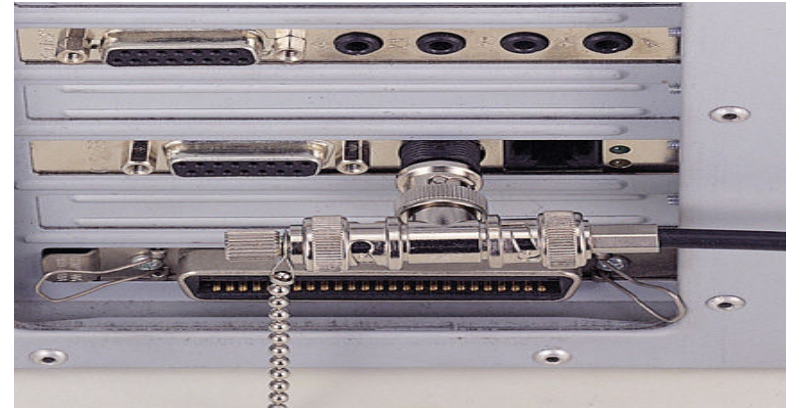
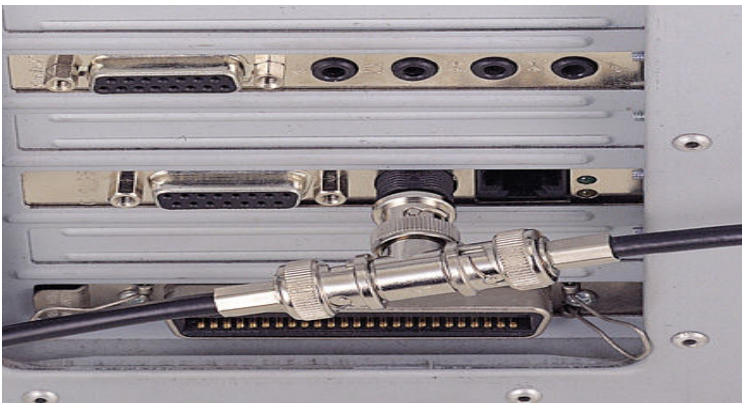
BNC Connector 및 연결형태



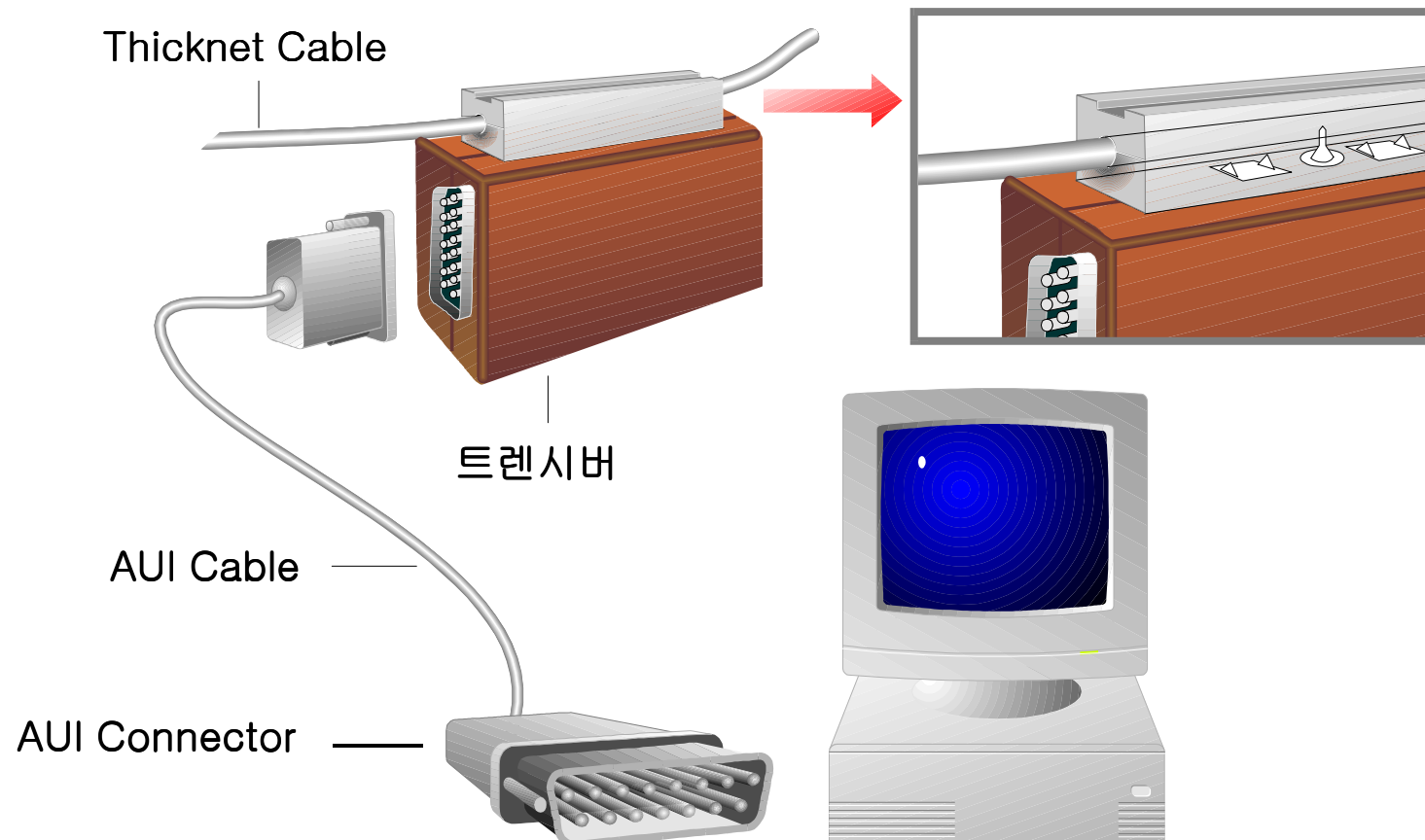
Barrel

T

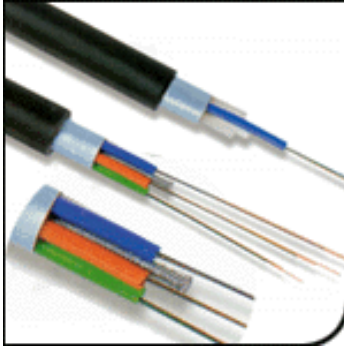
Terminator



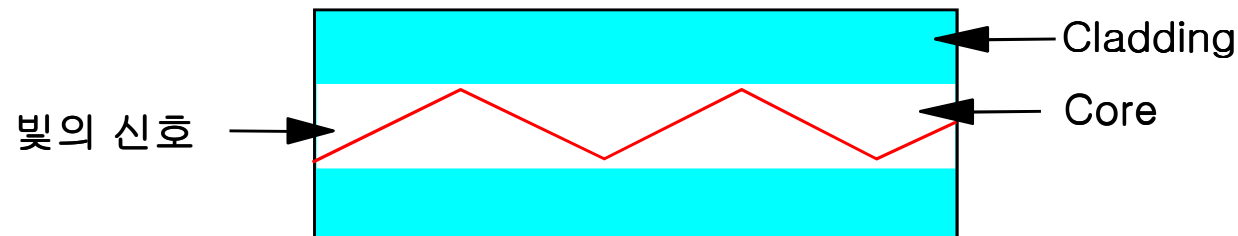
Thicknet Cabling (10Base5)



Fiber Optical

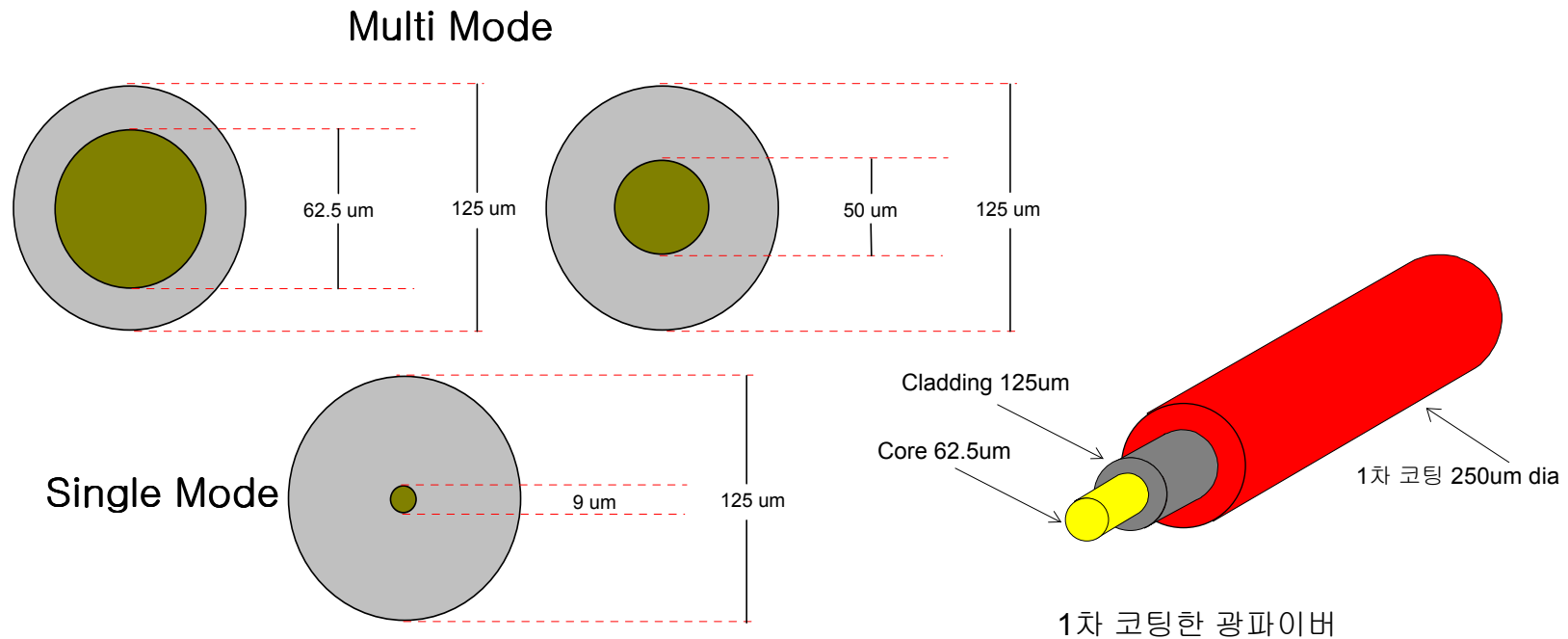


광섬유 케이블은 전기 신호보다 빛을 통해서 데이터를 전송하는 가장 효과적인 전송매체이다. 광섬유 케이블은 아주 높은 대역 용량을 제공하며 빛을 통한 전송을 함으로써 감쇠에 전혀 영향을 받지 않는다. 또한 EMI에 대해서도 전혀 문제가 없을뿐더러 내구성에 대해서도 상당한 신뢰감을 준다. 그러나 설치에 대한 어려움과 고가의 연결장치, 고가의 케이블 가격이 걸림돌로 작용하고 있다.



광섬유의 단면을 살펴보면 두 부분으로 나누며, 중심부를 코어(Core), 외곽을 클래드(Clad)이라고 한다. 빛이 광섬유를 통과하여 나갈 때에, 클래드는 거울과 같은 역할을 수행하여 빛을 반사한다. 이 반사된 빛은 다시 코아 속을 통과하고 다시 클래드로 가서 반사된다. 이러한 과정이 반복됨으로써 빛이 광섬유를 통하여 전송되는 것이다. 이때, 빛이 클래드 밖으로 나올 수 없게 광섬유가 만들어져 있다.

광섬유의 유형 및 구조

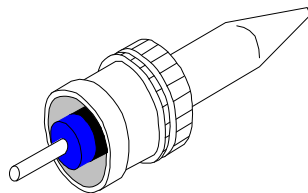


단일모드(Single mode) 케이블 : 단일 빛 경로를 통한 전송을 허용하며 일반적으로 레이저 신호가 사용된다. 특히 중앙 Core는 너무 좁아(일반적으로 10미크론 이하) 단일 경로를 통한 전송만이 가능하기 때문에 가장 큰 정밀도를 갖는다. 따라서 멀티모드에 비해 가격이 비싸다. 이론상으로는 50Gbps의 전송속도까지 가능하다.

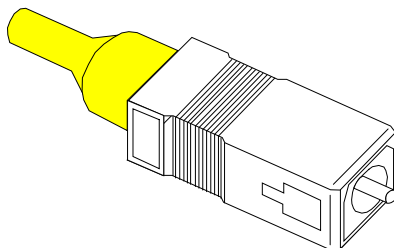
멀티모드(Multi mode) 케이블 : 이 케이블은 중앙 Core의 너비가 넓기 때문에 빛이 Core를 따라 다중의 경로로 전송이 가능하다



광 파이버 커넥터



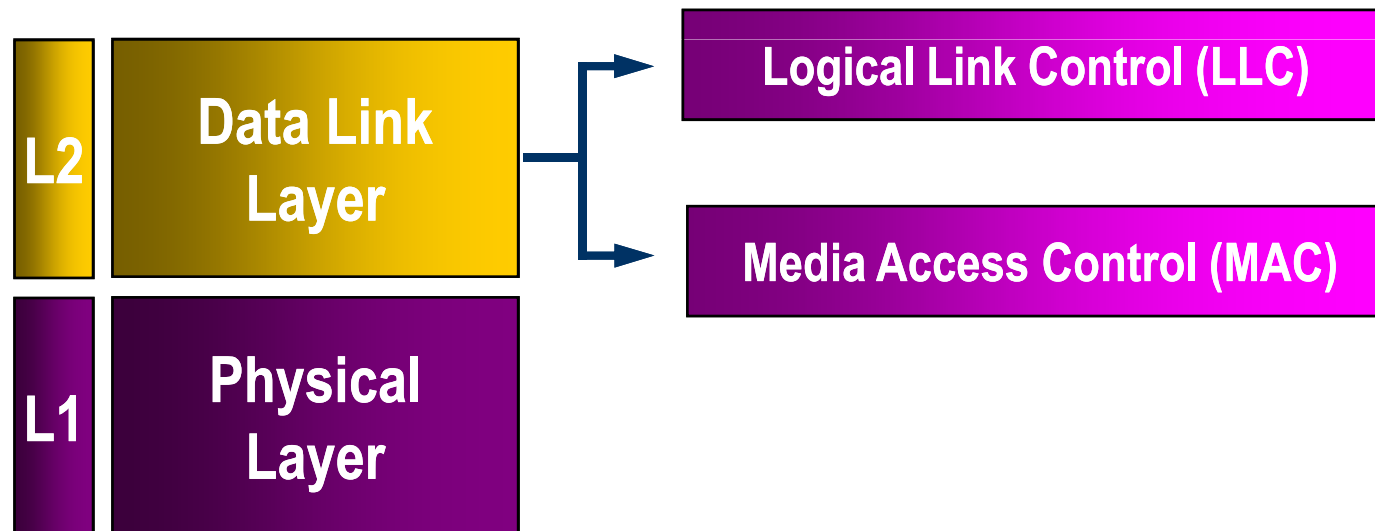
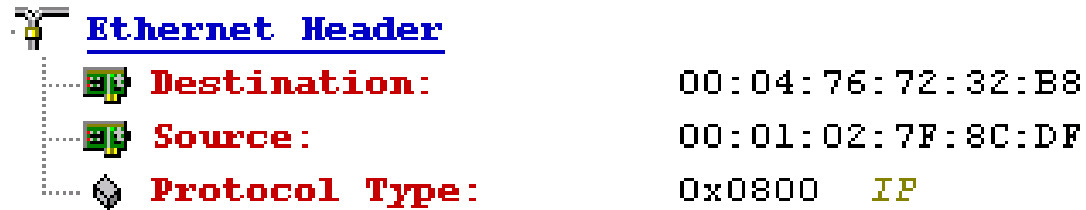
데이터 통신에서 가장 일반적인 커넥터는 ST 커넥터이다.



ISO 11801에는 SC 커넥터가 규정됨.



Ethernet Frame Format





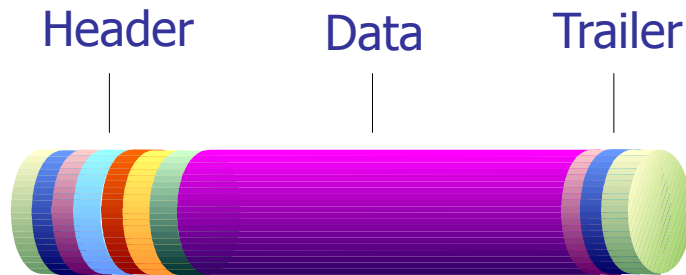
EUI-48 and EUI-64

- EUI-48 (48-bit Extended Unique Identifier)
 - 00-0E-35-05-80-6F
 - 상위 24bit는 Company ID (제조 회사에 할당된 주소임.)
 - 하위 24bit는 Extension ID (제조번호에 해당함.)
 - 하나의 OUI는 $2^{24} = 16,777,216$ 개 MAC 사용.
- EUI-64 (64-bit Extended Unique Identifier)
 - 00-0E-35-FF-FE-05-80-6F
 - 상위 24bit는 Company ID 이다. (제조회사)
 - 하위 40bit는 Extension ID 이다. (제조번호)
 - 하나의 OUI는 $2^{40} = 1,099,511,627,776$ 개 MAC 사용.

Company ID 확인 사이트

<http://standard.ieee.org/regauth/oui/index.shtml>

Packet Components



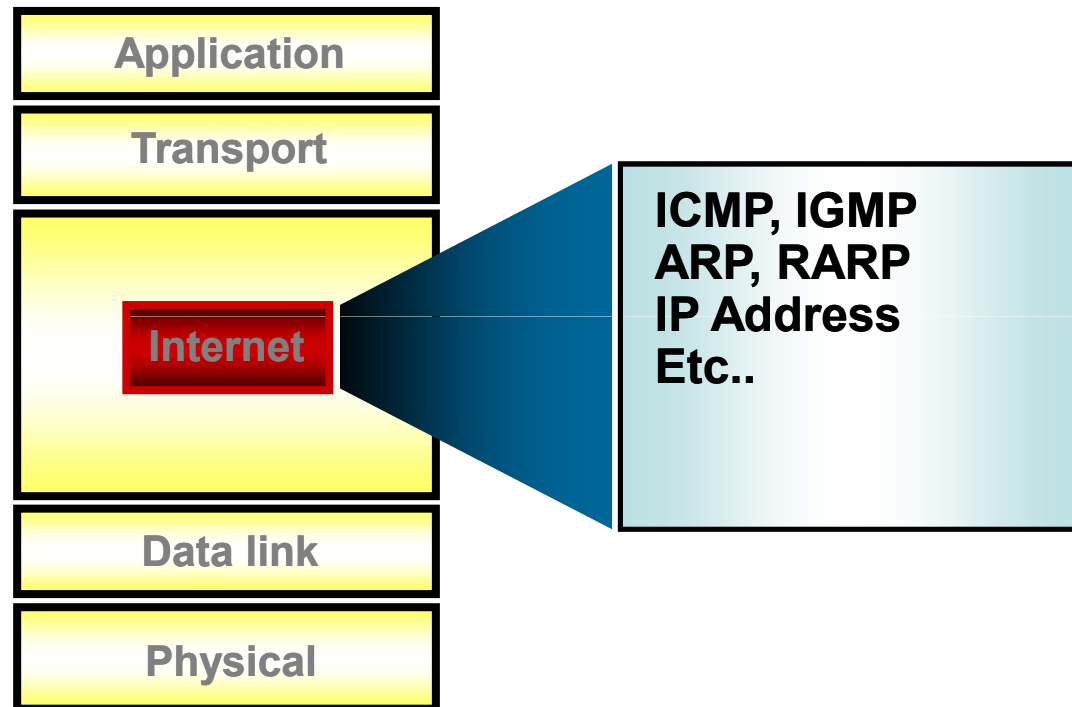
Packet 생성이유?


1. 네트워크점유현상을 막기 위해
2. 데이터의 오류제어를 빠르게 하기 위해

Ethernet Header	
Destination:	00:50:BF:26:E0:2C
Source:	00:04:76:72:32:B8
Protocol Type:	0x0800 IP
IP Header - Internet Protocol Datagram	
Version:	4
Header Length:	5 (20 bytes)
Type of Service:	%00000000
Precedence: Routine, Normal Delay, Normal Throughput,	
Total Length:	40
Identifier:	54473
Fragmentation Flags:	%010 Do Not Fragment Last Fragment
Fragment Offset:	0 (0 bytes)
Time To Live:	128
Protocol:	6 TCP - Transmission Control Protocol
Header Checksum:	0x0000
Source IP Address:	192.168.100.3 vmdc.koreamoon.net
Dest. IP Address:	219.241.88.110 ksdc.koreamoon.net
No IP Options	
TCP - Transport Control Protocol	
Source Port:	1926
Destination Port:	20 ftp-data
Sequence Number:	1010157960
Ack Number:	1737408473
Offset:	5 (20 bytes)
Reserved:	%000000
Code:	%010000 Ack
Window:	20440
Checksum:	0x5926 Checksum invalid. Should be:
Urgent Pointer:	0
No TCP Options	
Extra bytes (Padding):	
Data: (6 bytes)	
FCS - Frame Check Sequence	
FCS (Calculated):	0x6572DAAA



Internet Layer







IPv4 Header

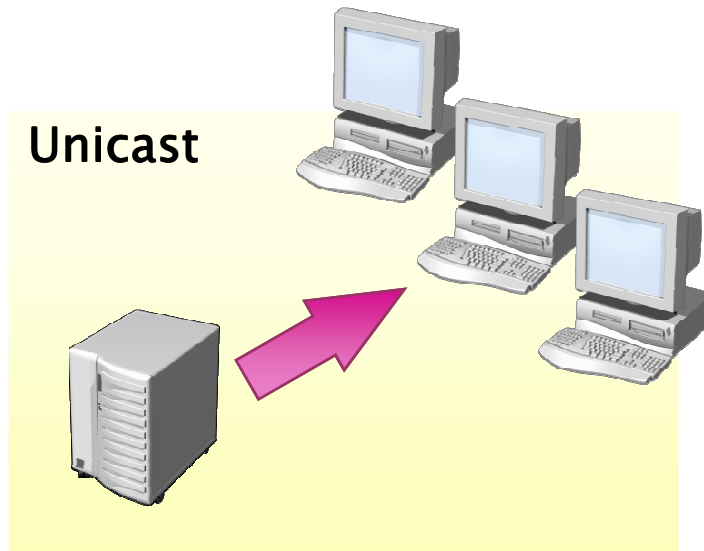


IP Header - Internet Protocol Datagram

◆	Version:	4
◆	Header Length:	5 (20 bytes)
◆	Type of Service:	%00000000
◆		<i>Precedence: Routine, Normal Delay, Normal Throughput,</i>
◆	Total Length:	48
◆	Identifier:	9768
◆	Fragmentation Flags:	%010 <i>Do Not Fragment Last Fragment</i>
◆	Fragment Offset:	0 (0 bytes)
◆	Time To Live:	128
◆	Protocol:	6 <i>TCP - Transmission Control Protocol</i>
◆	Header Checksum:	0x0000
◆	 Source IP Address:	211.255.9.138
◆	 Dest. IP Address:	211.255.9.207
◆	No IP Options	

Type of Data Transmissions (Unicast)

Segment	D-IP : 192.168.1.5 S-IP : 192.168.1.8	D-MAC : 0050.BF1C.82D3 S-MAC : 0050.DC34.32CA
---------	--	--



A Host가 B Host에게 Data를 전달하는 가장 일반적인 방법이다.

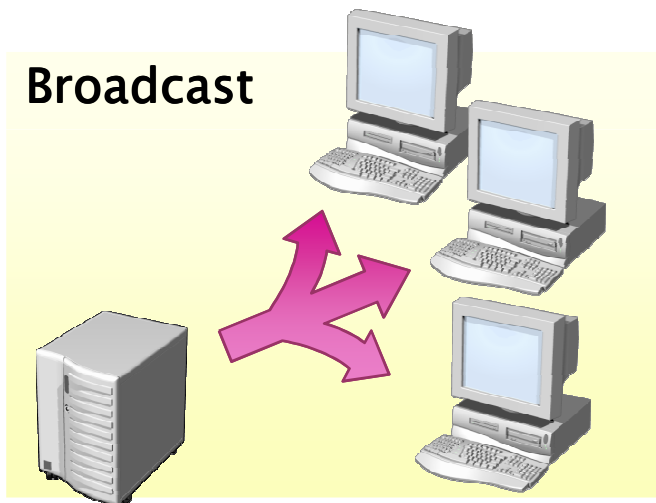
Source Address와 Destination Address를 명시하여 해당하는 장비만이 데이터를 처리하는 방법이다.

동일한 정보를 많은 호스트에 전달시에는 비 효율적인 방법일수 있다.

Host to Host 전달을 기반으로 하므로 다른 Host에 부하는 주지 않는다.

Type of Data Transmissions (Broadcast)

Segment	D-IP : 255.255.255.255 S-IP : 192.168.1.8	D-MAC : FFFF.FFFF.FFFF S-MAC : 0050.DC34.32CA
---------	--	--



단일 Host가 Segment에 모든 호스트를 대상으로 Data를 전달시 사용된다.

목적지 주소를 각 주소에 예약된 **Broadcast Address**를 입력하여 전달한다. 모든 호스트는 이 메시지를 수신한다.

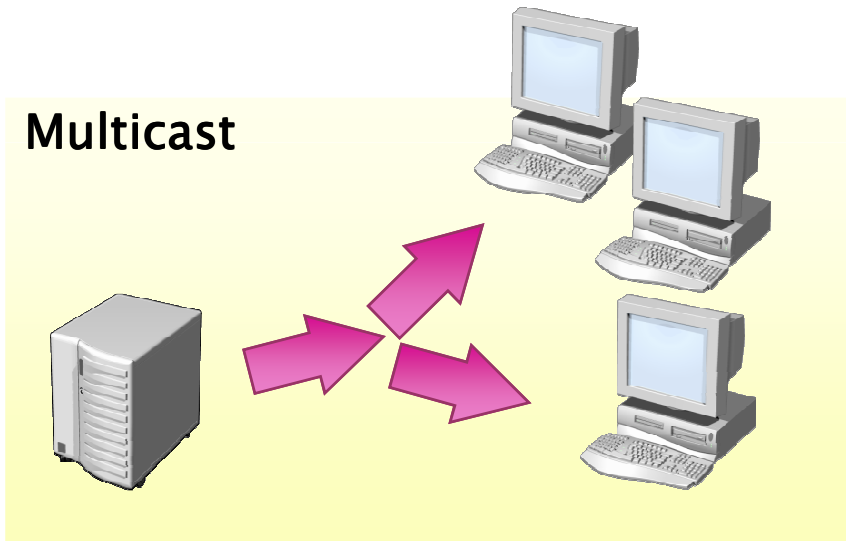
동일한 정보를 한번에 모든 호스트에게 전달하는 장점을 갖는다.

많은 **Broadcast**는 호스트에 성능저하를 가져온다.

Type of Data Transmissions (Multicast)

Segment	D-IP : 224.2.138.2 S-IP : 192.168.1.8	D-MAC : 0100.5E02.8A02 S-MAC : 0050.DC34.32CA
---------	--	--

Multicast



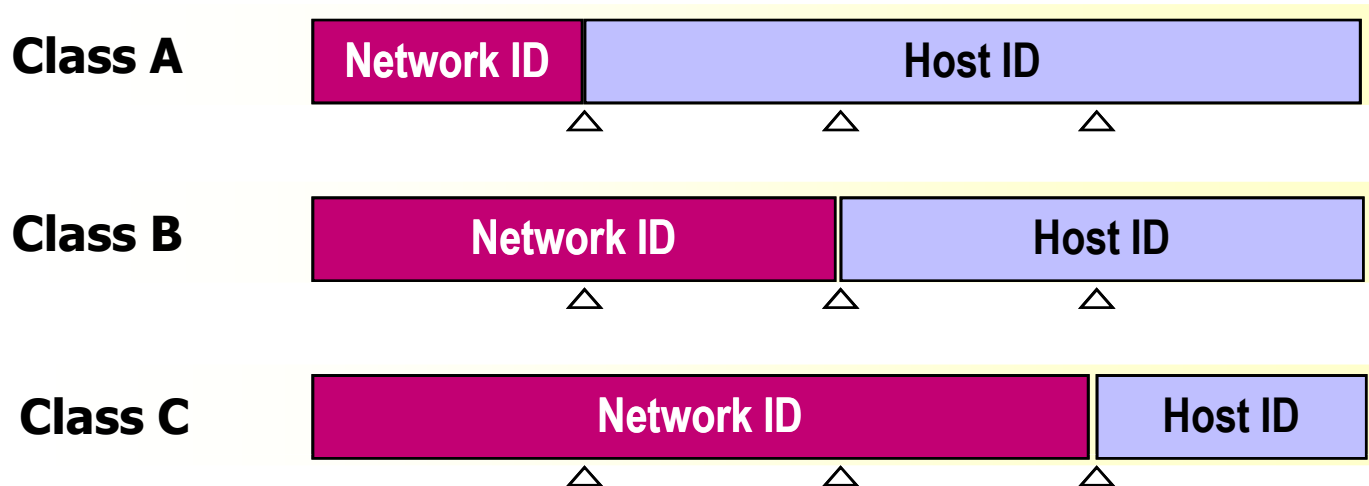
단일 Host가 예약된 주소 (Multicast Address)

목적지 주소를 각 주소에 예약된 Broadcast Address를 입력하여 전달한다. 모든 호스트는 이 메시지를 수신한다.

동일한 정보를 한번에 모든 호스트에게 전달하는 장점을 갖는다.

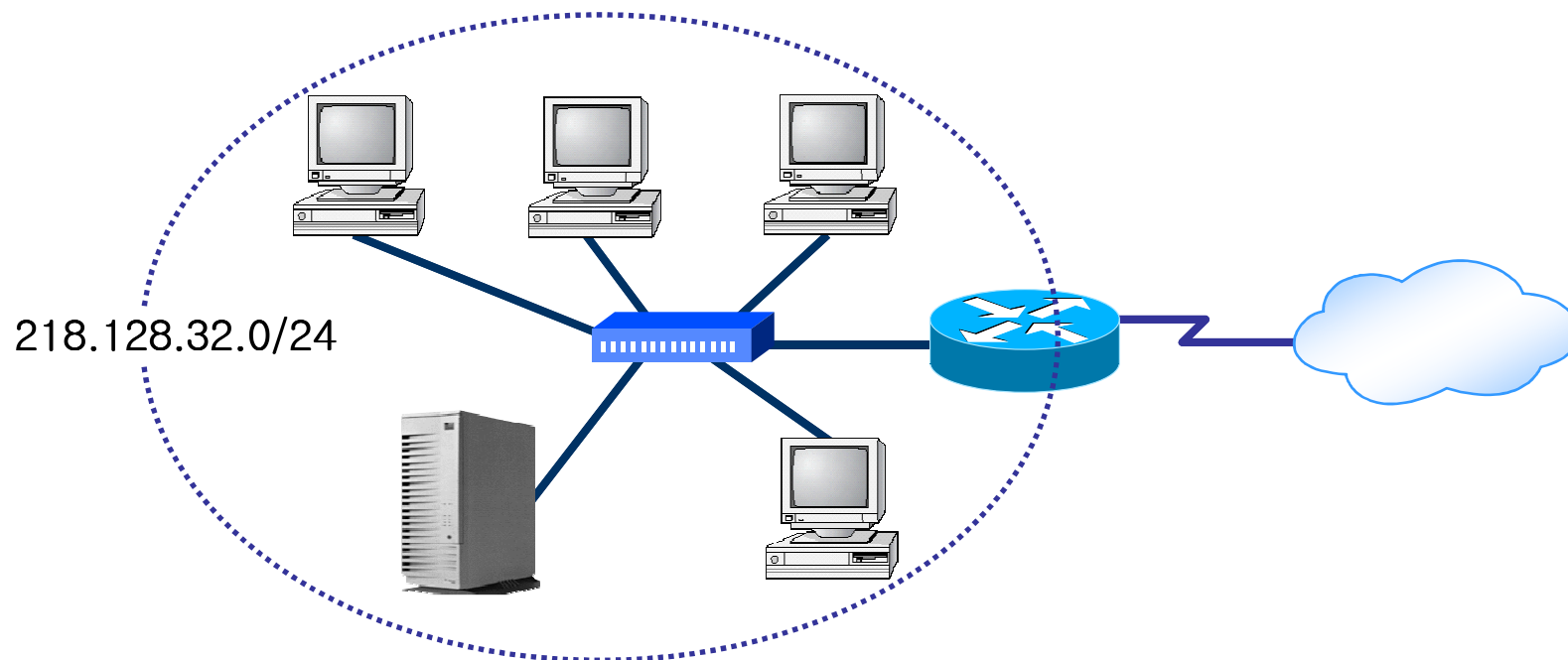
많은 Broadcast는 호스트에 성능저하를 가져온다.

IP Address Classes (사용 가능한 IP)



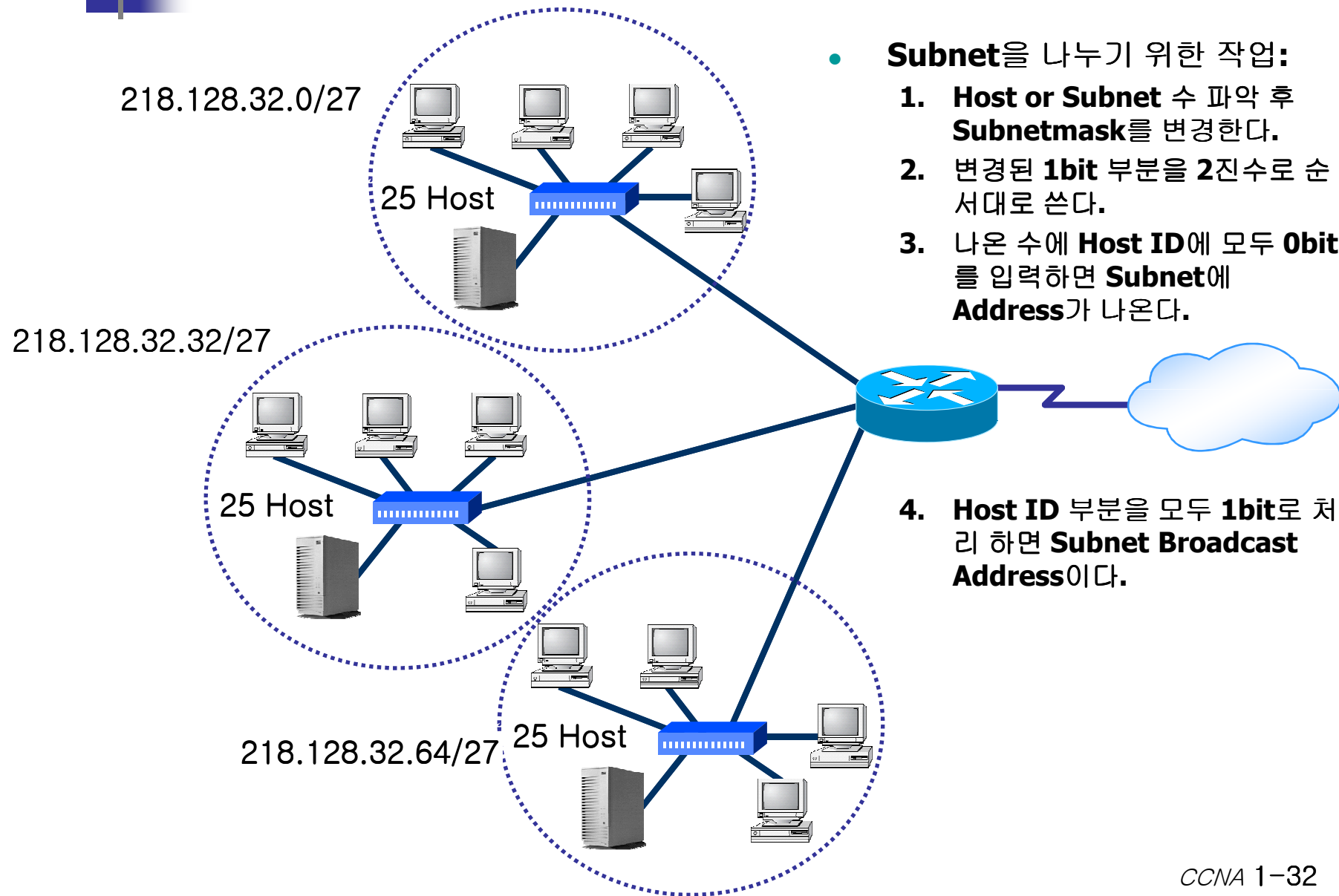
- **IPv4 Address**는 **32bit** 이며 **8bit**씩 **4**개의 옥텟으로 구분하여 **10**진수로 표기한다.
- **A Class?**
 - **8bit**를 **Network ID**로 **24bit**를 **Host ID**로 배포되는 주소이며 **128**개의 **Network**에 하나의 **Network**당 **2²⁴**개의 **Host**를 설치 할 수 있는 네트워크 주소이다.
- **B Class?**
 - **16bit**를 **Network ID**로 **16bit**를 **Host ID**로 배포되는 주소이며 총 **16384**개의 **Network**에 네트워크 당 **Host**는 **2¹⁶**개의 **Host**를 설치할 수 있는 네트워크 주소 이다.
- **C Class?**
 - **24bit**를 **Network ID**로 **8bit**를 **Host ID**로 배포되는 주소이며 네트워크 당 **256**개의 **Host**를 설치 할 수 있는 네트워크 주소이다.

Subnetting 이란?



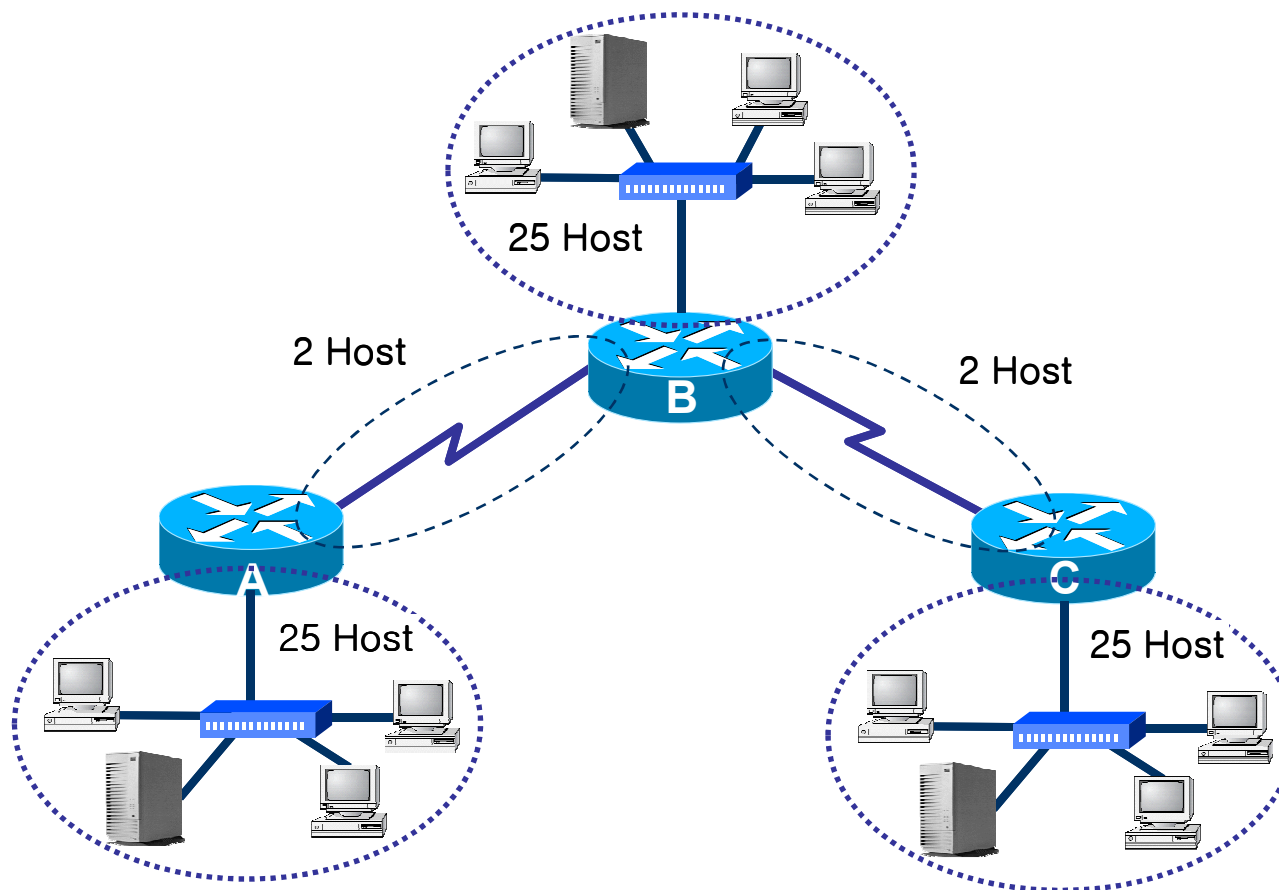
- **Broadcast Domain**에 많은 호스트가 연결된 경우 호스트에 발생한 **Broadcast traffic**이 모든 호스트에 전달되어 많은 **Broadcast Traffic**이 발생하며 하나의 **Broadcast Domain**에서는 보안이 취약하기 때문에 **Firewall**이나 **ACL**과 같은 정책을 구현하기 위해서는 **Network Segment**를 나누는 것이 효율적이다.
- **ISP**업체에서는 회선을 임대한 기업들에 **IP**를 할당하기 위하여 **Subnetting**을 한 후에 **IP**를 할당하여 주소를 절약한다.

Subnet 구조

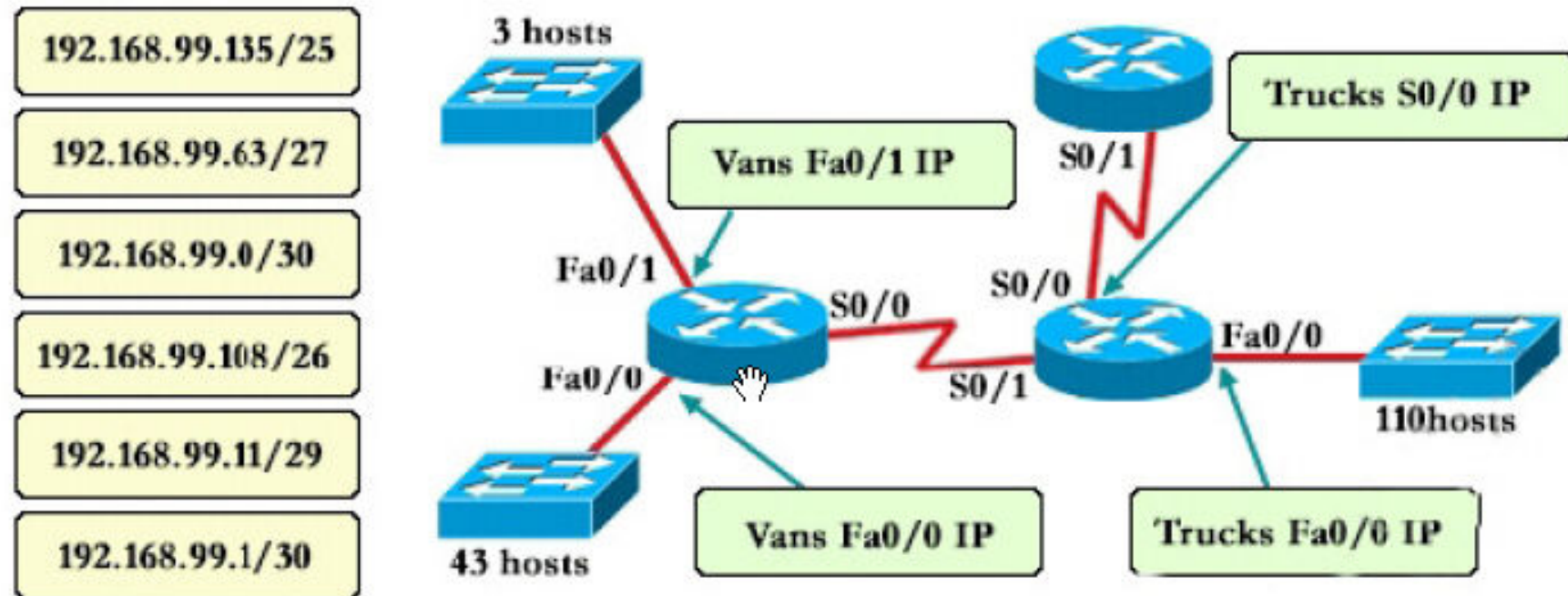


VLSM?

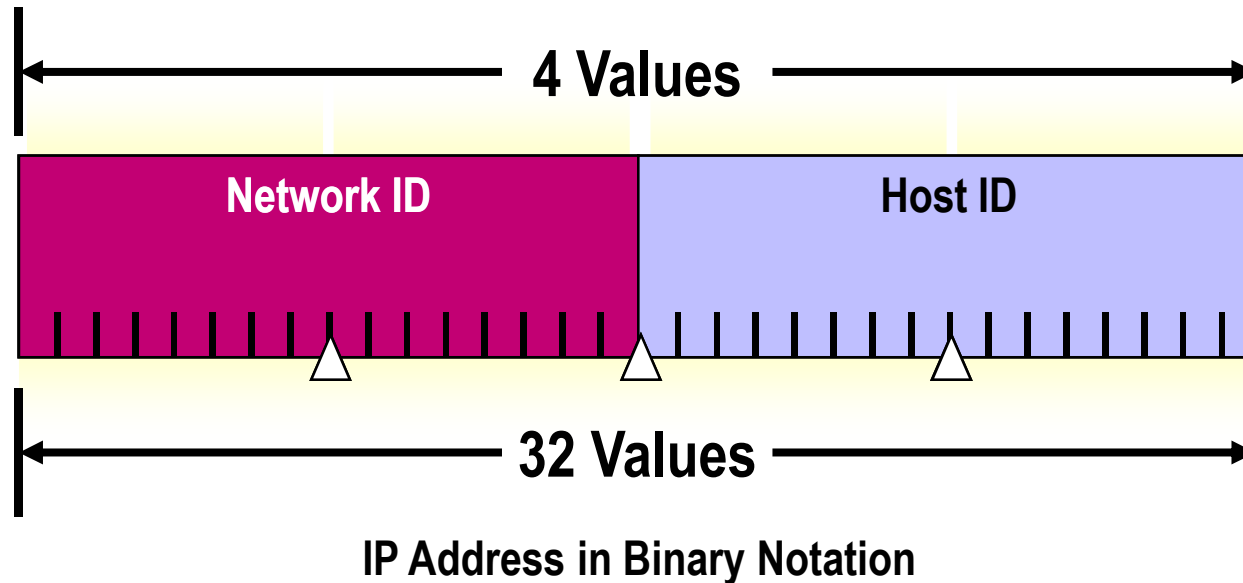
VLSM variable-length subnet mask(가변 길이 서브넷 마스크)의 약어. 서로 다른 서브넷에서 동일한 네트워크 번호로 다른 서브넷 마스크를 지정할 수 있는 특성. VLASM은 가용 주소 공간을 최적화하는데 도움이 된다.



VLSM Example



Defining CIDR



00001010 11011001 01111011 00000111

- **CIDR (Classless Inter-network Domain Routing)**이란 주소 재할당 개념이다. 기존 **Class**기반 주소에서 **Class**를 제외하고 **32bit** 전체 **bit**에 대해 **Network**과 **Host**를 재 설정한 주소 구조이다. 기존 **Class** 기반 주소에 비해 주소 손실을 줄여 주고, **Router**에는 구조화된 주소 할당으로 인해 **Routing Table**을 줄여 **packet Delay**를 줄인다.



IP Header Format



IP Header - Internet Protocol Datagram

◆	Version:	4
◆	Header Length:	5 (20 bytes)
◆	Type of Service:	%00000000
◆		<i>Precedence: Routine, Normal Delay, Normal Throughput,</i>
◆	Total Length:	48
◆	Identifier:	9768
◆	Fragmentation Flags:	%010 Do Not Fragment Last Fragment
◆	Fragment Offset:	0 (0 bytes)
◆	Time To Live:	128
◆	Protocol:	6 TCP - Transmission Control Protocol
◆	Header Checksum:	0x0000
◆	Source IP Address:	211.255.9.138
◆	Dest. IP Address:	211.255.9.207
◆	No IP Options	



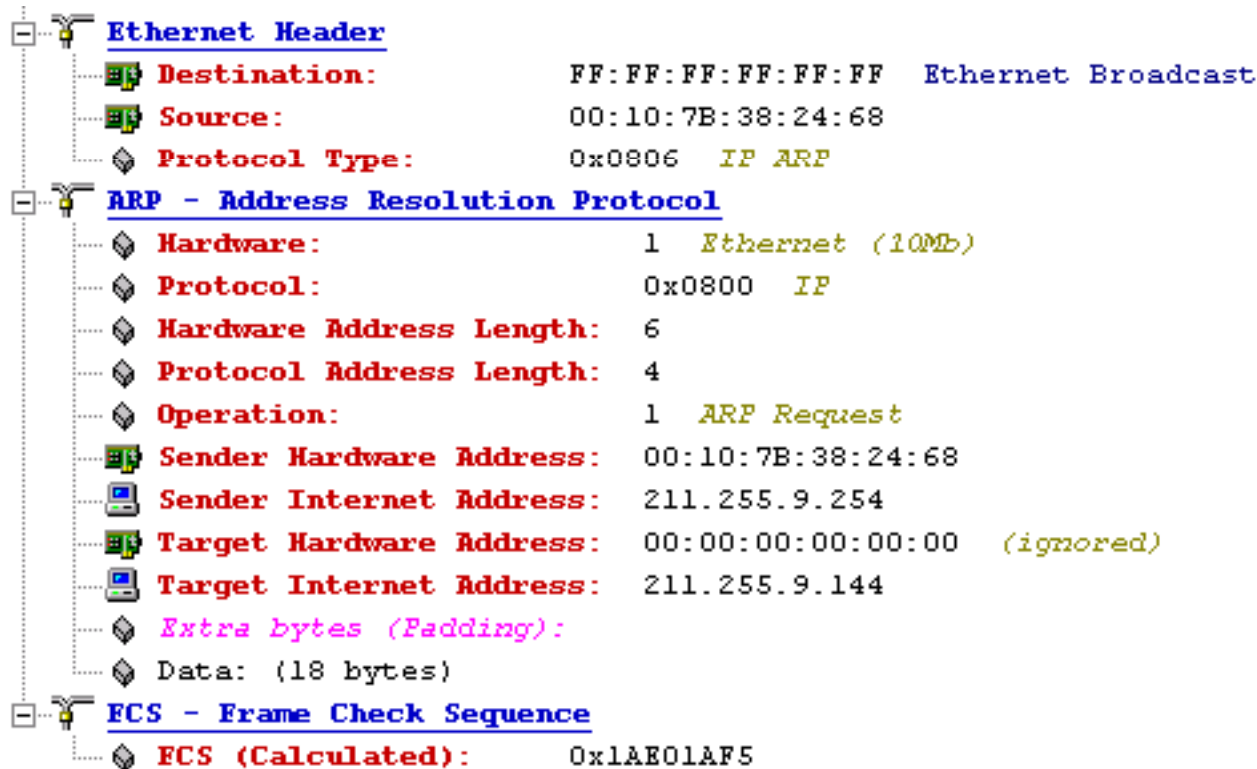
IP Header 설명

필드명	비트	역할
Version	4	IP Protocol Version 정보 현재 인터넷에서 사용되는 Version은 v4 이다.
Header Length	4	IP Header의 길이를 32비트 단위로 나타낸다. (Default 5) $5 \times 32 = 160\text{bit} = 20\text{Byte}$
Type-of-Service Flags	8	Internet의 Application, Host, 그리고 Router에 우선순위 서비스를 제공한다. 이 필드를 설정하여 Datagram의 처리순서를 빠르게 할 수 있다.
Total Packet Length	16	헤더와 몸체를 포함한 전체 IP Packet의 길이를 바이트 단위로 나타낸다.
Fragment Identifier	16	분열이 발생한 경우 조각을 다시 결합하는 일을 돕기 위한 조각들이 속한 원래의 Datagram을 나타낸다.
Fragmentation Flags	3	현재의 분열상태의 단서 제공 3Bit중 마지막2Bit만 사용 (첫번째 Bit는 예비용 두번째 Bit는 분열허용여부 (0 : 허용 1 : 허용 안됨) 세번째 Bit는 현재의 조각이 마지막인지 여부 표시 마지막 인 경우 0 더 있으면 1로 표기한다.
Fragmentation Offset	13	8바이트의 오프셋으로 조각에 저장된 원래 Datagram의 바이트 범위를 나타낸다.
Time-to-Live	8	Datagram이 전달 불가능한 것으로 판단되어 소멸되기 이전에 Datagram이 이동할 수 있는 단계의 수를 나타낸다.
Protocol Identifier	8	IP Datagram의 몸체에 저장된 상위 계층 프로토콜을 나타낸다.
Header Checksum	16	IP 헤더의 Checksum을 저장한다.
Source IP Address	32	Datagram을 전송한 원래 컴퓨터의 32비트의 IP Address이다.
Destination IP Address	32	Datagram 수신할 최종목적지의 32비트 IP Address이다.
Option	가변	IP가 Type-of-Service를 통해 우선순위 서비스를 제공하는 것처럼 Option 필드를 사용하여 특별한 처리 옵션을 추가로 정의할 수 있다.
Padding	가변	IP 헤더의 길이는 32비트 단위여야 한다. 헤더에 옵션이 추가되면 헤더는 32비트로 나눠 떨어지도록 부족분이 채워져야 한다.

주소변환 프로토콜 (ARP)

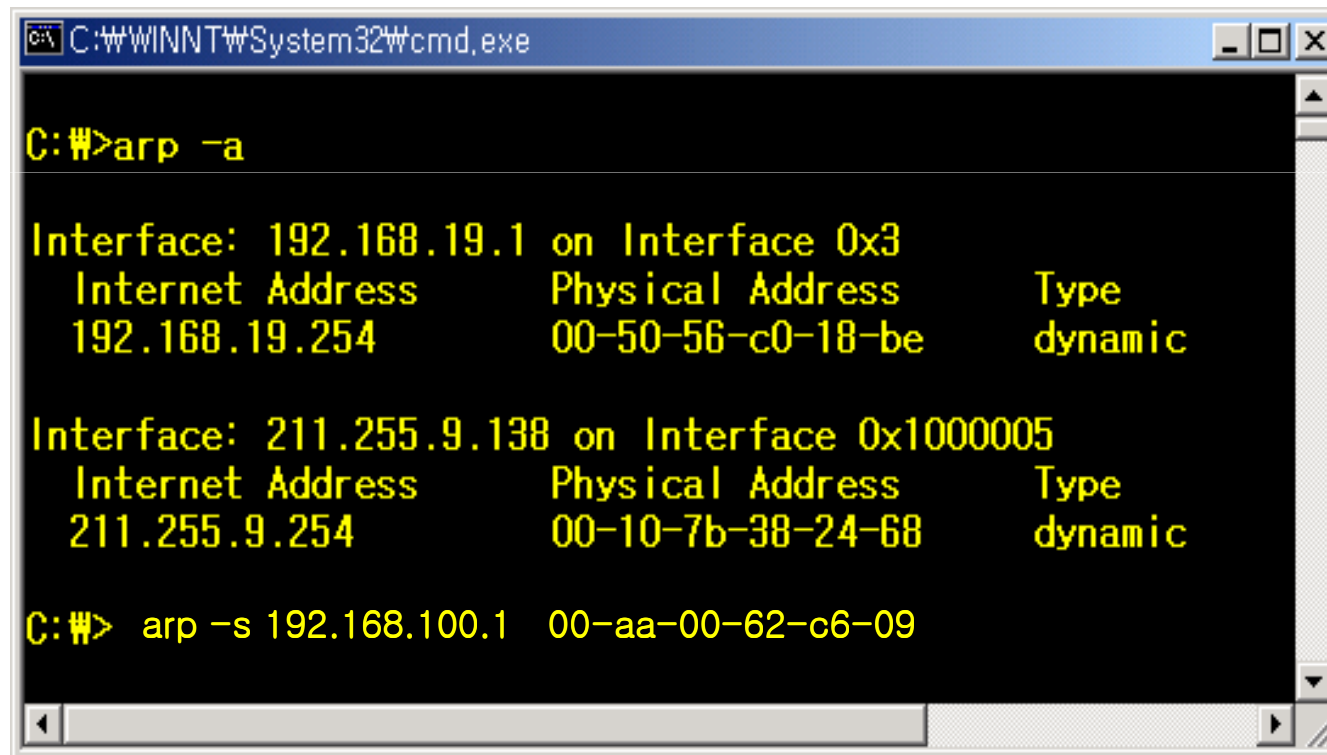
같은 네트워크 세그먼트에 있는 두 IP장비가 통신하는 경우에는 그 네트워크에서 이용하는 특정 매체에 적합하게 정의된 하위 계층 프로토콜과 주소 지정 (Addressing)메커니즘을 사용한다.

예를 들어, 이더넷 장비는 통신할 때 이더넷에 특화된 주소를 사용한다. 반면 프레임릴레이는 프레임릴레이에 특화된 주소를 사용한다. IP 시스템이 통신하기 위해서는 먼저 로컬 장비가 속한 네트워크에 연결된 다른 장비들의 하드웨어 주소를 확인해야 한다. 주소 변환 프로토콜 (ARP, Address Resolution Protocol)은 이런 서비스를 제공한다.



ARP Cache

ARP 요청을 보냈던 시스템은 ARP응답을 수신하면 질의 대상 시스템의 하드웨어 주소와 IP주소를 로컬 캐시(Cache)에 저장한다. 시스템에서 다음 번 데이터를 보낼 때 로컬 캐시를 검사하여 엔트리를 찾으면 그것을 사용함으로써 또 다른 요청을 브로드캐스트 할 필요가 없어짐으로 로컬 트래픽을 줄일 수 있다. 응답하는 시스템도 동일하게 로컬 Cache에 ARP정보를 저장한다.



```
C:\WINNT\System32\cmd.exe

C:\>arp -a

Interface: 192.168.19.1 on Interface 0x3
  Internet Address      Physical Address      Type
  192.168.19.254        00-50-56-c0-18-be    dynamic

Interface: 211.255.9.138 on Interface 0x1000005
  Internet Address      Physical Address      Type
  211.255.9.254         00-10-7b-38-24-68    dynamic

C:\> arp -s 192.168.100.1 00-aa-00-62-c6-09
```



ARP Cache 및 Static ARP Table

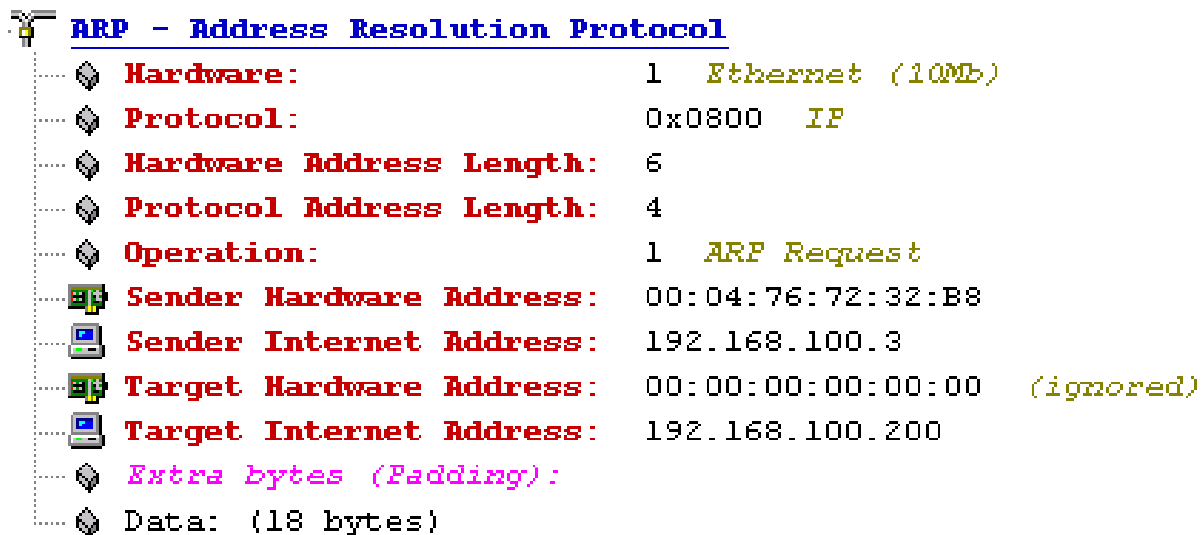
ARP Cache 확인하기

```
C:\W>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 정보 만들기

```
C:\W>arp -s 211.255.9.254 00-10-7b-38-24-68  
C:\W>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
```


ARP Packet 구조



The image shows a Wireshark packet capture details pane for an ARP Request. The title is 'ARP - Address Resolution Protocol'. The list of fields includes Hardware, Protocol, Hardware Address Length, Protocol Address Length, Operation, Sender Hardware Address, Sender Internet Address, Target Hardware Address, Target Internet Address, Extra bytes (Padding), and Data. Each field has a small icon to its left and a value to its right. The values are: Hardware: 1 Ethernet (10Mb), Protocol: 0x0800 IP, Hardware Address Length: 6, Protocol Address Length: 4, Operation: 1 ARP Request, Sender Hardware Address: 00:04:76:72:32:B8, Sender Internet Address: 192.168.100.3, Target Hardware Address: 00:00:00:00:00:00 (ignored), Target Internet Address: 192.168.100.200, Extra bytes (Padding):, and Data: (18 bytes).

ARP - Address Resolution Protocol	
Hardware:	1 Ethernet (10Mb)
Protocol:	0x0800 IP
Hardware Address Length:	6
Protocol Address Length:	4
Operation:	1 ARP Request
Sender Hardware Address:	00:04:76:72:32:B8
Sender Internet Address:	192.168.100.3
Target Hardware Address:	00:00:00:00:00:00 (ignored)
Target Internet Address:	192.168.100.200
Extra bytes (Padding):	
Data:	(18 bytes)

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 Length : 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



Operation Code & Hardware Type

Number Operation Code (op)

-
- | | |
|---|-----------------|
| 1 | REQUEST |
| 2 | REPLY |
| 3 | request Reverse |
| 4 | reply Reverse |
| 8 | InARP-Request |
| 9 | InARP-Reply |

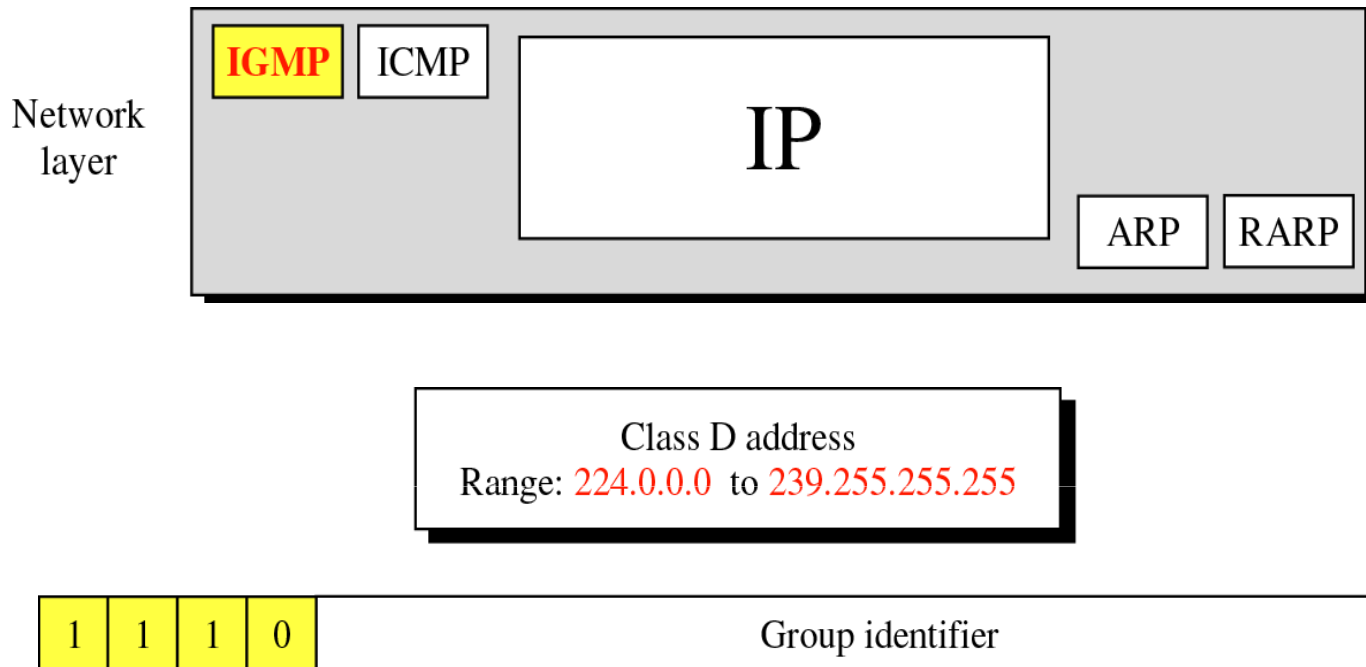
Number Hardware Type (hrd)

-
- | | |
|----|--------------------------------------|
| 1 | Ethernet (10Mb) |
| 4 | Proton ProNET Token Ring |
| 6 | IEEE 802 Networks |
| 7 | ARCNET |
| 11 | LocalTalk |
| 15 | Frame Relay |
| 17 | HDLC |
| 19 | Asynchronous Transmission Mode (ATM) |
| 20 | Serial Line |
| 24 | IEEE 1394.1995 |
| 31 | IPsec tunnel |

참고 사이트

<http://www.iana.org/assignments/arp-parameters>

IGMP (Internet Group Management Protocol)



시스템이 다른 호스트와 통신하는 방법은 일반적으로 **Unicast** 와 **Broadcast** 두 가지 방법이 있다. 또 다른 방법으로는 그룹주소를 사용해서 **Packet**을 보내는 **Multicast** 가 있다. **Multicast**는 그룹 주소를 감시하고 있는 호스트만이 데이터를 수신하며, 다른 네트워크 장비는 그것을 무시한다. 이런 방식은 **Broadcast**의 제한을 피해 한 호스트에서 여러 개의 목적지로 동시에 데이터를 보내야 하는 응용 프로그램에 유용하다.

ICMP에 대해서

IP는 신뢰성을 보장하지 않는다. 따라서 네트워크 장애나 중계 라우터 등의 에러에 대처 할 수 없다. 이런 경우 수신측에서 송신측으로 데이터의 사고에 대한 내용을 전달할 필요가 있다. ICMP는 이와 같은 오류 정보를 발견 송신측에 메시지를 전달하는 기능을 한다.

ICMP - Internet Control Messages Protocol

```


..... ICMP Type:           8  Echo Request
..... Code:             0
..... Checksum:        0x9EF3
..... Identifier:      0x0200
..... Sequence Number: 0x2700
..... Extra bytes (Padding):
..... Data: (124 bytes)
  
```

타입	메시지
0	에코 응답 (Echo Reply)
3	수신처 도달 불가능 (Destination Unreachable)
4	발신 제한 (Source Quench)
5	라우트 변경 (redirect)
8	에코 요구 (Echo Request)
11	시간 초과 (Time Exceeded)
12	파라미터 불량 (Parameter Problem)

타입	메시지
13	타임스탬프 요구 (Timestamp Request)
14	타임스탬프 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)

ICMP Error Message

ICMP 에러 메시지를 읽는 가장 쉬운 방법은 메시지를 다룰 수 있는 크기로 나누는 것이다. 메시지의 첫 부분은 항상 보고되는 측정 ICMP 에러 메시지를 나타내며, 메시지의 나머지 부분은 실패한 IP 데이터그램의 헤더와 데이터 첫 8바이트를 포함한다.

 ICMP - Internet Control Messages Protocol

- ◆ **ICMP Type:** 3 *Destination Unreachable*
- ◆ **Code:** 3 *Port Unreachable*
- ◆ **Checksum:** 0xFF68
- ◆ **Unused (must be zero):** 0x00000000
- ◆
- ◆ *Header of packet that caused error follows.*

Type

0 Echo Reply

3 **Destination Unreachable**

Codes

0 Net Unreachable

1 Host Unreachable

2 Protocol Unreachable

3 **Port Unreachable**

5 Source Route Failed

6 Destination Network Unknown

7 Destination Host Unknown

ICMP Type & Code

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

ICMP Utility Ping

가장 보편적으로 ICMP를 사용하는 도구는 Ping 이다. Ping 도구는 ICMP Echo Request 메시지를 전송하여 목적지시스템 으로부터 ICMP Echo Reply 메시지로 응답을 받는데 걸린 시간을 측정함으로써 네트워크 연결을 검사할 수 있다.

```
C:\WINNT\System32\cmd.exe

C:\W>ping 192.168.100.200

Pinging 192.168.100.200 with 32 bytes of data:

Reply from 192.168.100.200: bytes=32 time<10ms TTL=128
Reply from 192.168.100.200: bytes=32 time<10ms TTL=128
Reply from 192.168.100.200: bytes=32 time<10ms TTL=128
Reply from 192.168.100.200: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.100.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\W>
```

Unix (Traceroute) Windows (Tracert) 를 사용하여 네트워크 라우터를 확인하는 방법이다. 이 방법은 IP Header에 TTL 값을 1씩 증가시켜 Time Exceeded ICMP 오류 메시지를 통해 라우팅 경로를 점검 할 수 있다.

```
ICMP - Internet Control Messages Protocol
  ICMP Type: 8 Echo Request
  Code: 0
  Checksum: 0x0F5C
  Identifier: 0x0200
  Sequence Number: 0x3C00
  Extra bytes (Padding):
  Data: (32 bytes)
```

```
ICMP - Internet Control Messages Protocol
  ICMP Type: 0 Echo Reply
  Code: 0
  Checksum: 0x175C
  Identifier: 0x0200
  Sequence Number: 0x3C00
  Extra bytes (Padding):
  Data: (32 bytes)
```

```
C:\WINNT\System32\cmd.exe

C:\W>tracert 192.168.1.2

Tracing route to CLUSTER01 [192.168.1.2]
over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  app-srv.koreamoon.net [192.168.100.200]
  2  <10 ms  <10 ms  <10 ms  CLUSTER01 [192.168.1.2]

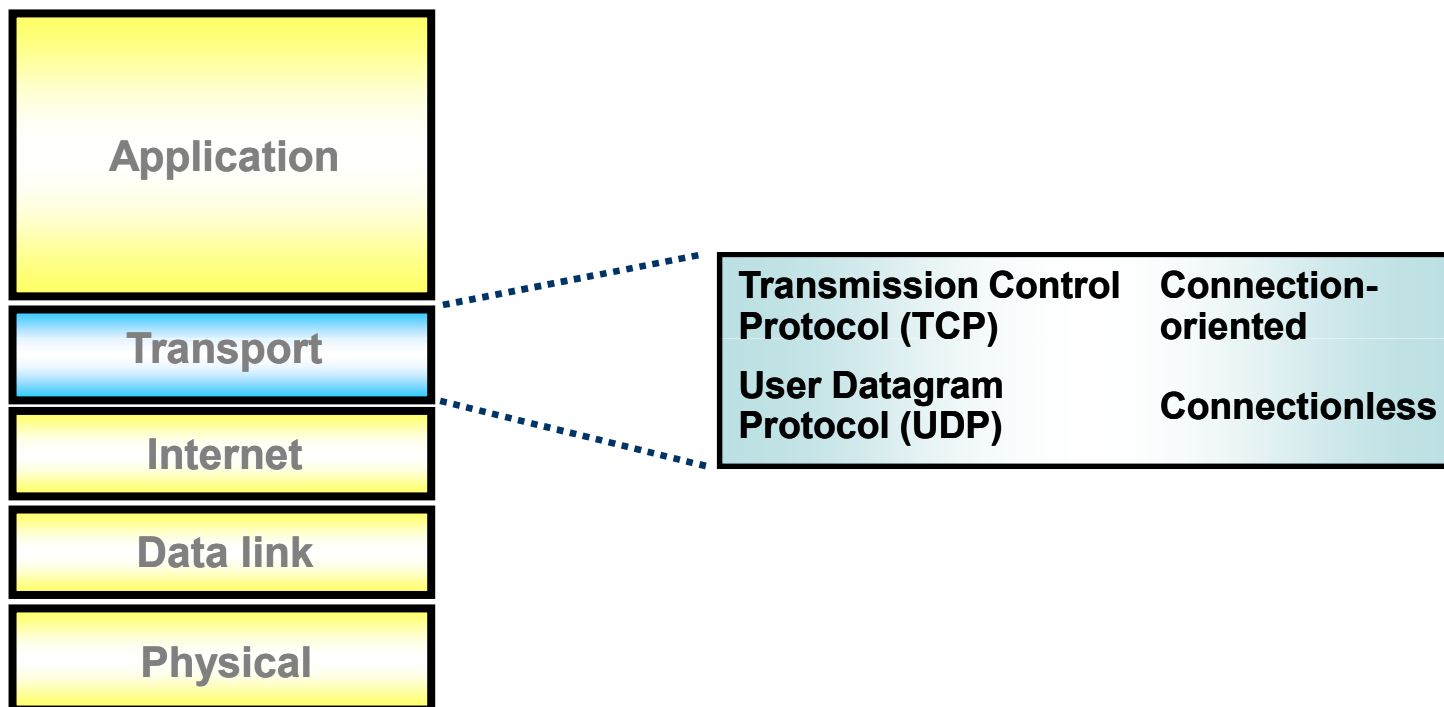
Trace complete.

C:\W>
```



Transport Layer

TCP/IP





UDP (User Datagram Protocol)

IP 네트워크에서 응용프로그램들은 서로 통신하기 위해서 TCP 나 UDP 표준전송 프로토콜을 사용한다. 그 중에서 UDP 는 작고 신뢰성이 없지만 오버헤드가 적어서 빠른 전송 서비스를 제공하는 사용자 Datagram Protocol이다.

UDP - User Datagram Protocol	
Source Port:	52891
Destination Port:	39213
Length:	276
Checksum:	0x2047
UDP Data Area:	
Data:	(268 bytes)

Well Known UDP Port

포트	설명
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS Name Service (WINS)
161	Simple Network Management Protocol (SNMP)

Source Port & Destination Port : 송.수신측 호스트의 포트번호를 나타낸다.

Length : UDP 패킷의 옥텟 단위 길이. 이 길이는 UDP 헤더와 그 데이터를 포함한다.

길이 필드의 최소 값은 8 이며 0 크기의 데이터 필드를 나타낸다.

Checksum : UDP 헤더 데이터를 포함한 세그먼트 전체에 대하여 계산한 값이다. 에러체크에 사용된다.

일반적으로 대부분의 응용프로그램들은 사용하지 않는다.

UDP Data Area : UDP 메시지의 Data 부분

TCP (Transmission Control Protocol)

TCP - Transport Control Protocol

- ◆ **Source Port:** 21 ftp
- ◆ **Destination Port:** 1093 proofd
- ◆ **Sequence Number:** 2117515078
- ◆ **Ack Number:** 769789660
- ◆ **Offset:** 5 (20 bytes)
- ◆ **Reserved:** %000000
- ◆ **Code:** %011000 Ack
- ◆ **Window:** 5840
- ◆ **Checksum:** 0x18A1
- ◆ **Urgent Pointer:** 0
- ◆ **No TCP Options**

Code (제어 플래그)

표 1-1

URG	수신자가 이미 흐르고 있는 옥텟을 처리하는 것을 기다리지 않고 대역을 벗어나 데이터를 보내기 위해 사용된다. (Telnet에서 인터럽트형 명령전송시 사용)
ACK	수신 통지 번호가 유효하다는 것을 나타낸다.
PSH	TCP가 즉시 이 메시지를 상위 계층 프로세스에 즉시 전달 할 수 있게 해준다.
RST	복구되지 않는 오류로 인해 가상 회로를 리셋하기 위해 사용된다.
SYN	가상 회로 연결의 시작을 나타낸다. SYN = 1 ACK = 0 연결 패킷 (연결요청) SYN = 1 ACK = 1 연결 수신 통지 (연결 요청 응답) SYN = 0 ACK = 1 데이터 또는 ACK 패킷
FIN	연결을 종료하기 위해 사용됨.



TCP Header 설명

Source Port & Destination Port : 송수신측 호스트의 포트번호를 나타낸다.

Sequence Number : 후술하는 SYN 플래그가 1인 경우에는 초기 순서 번호를 나타낸다. SYN이 0인 경우에는 세그먼트의 순서번호를 나타낸다.

Ack Number : 수신자에 의 예상되는 다음 바이트의 순서 번호를 나타낸다. TCP 수신 통지는 누적된다.

Offset : TCP 헤더의 32비트 워드 번호이다. 이 필드는 TCP 옵션 필드의 길이가 변할 수 있으므로 필요하다.

Code : 표 1-1 참고

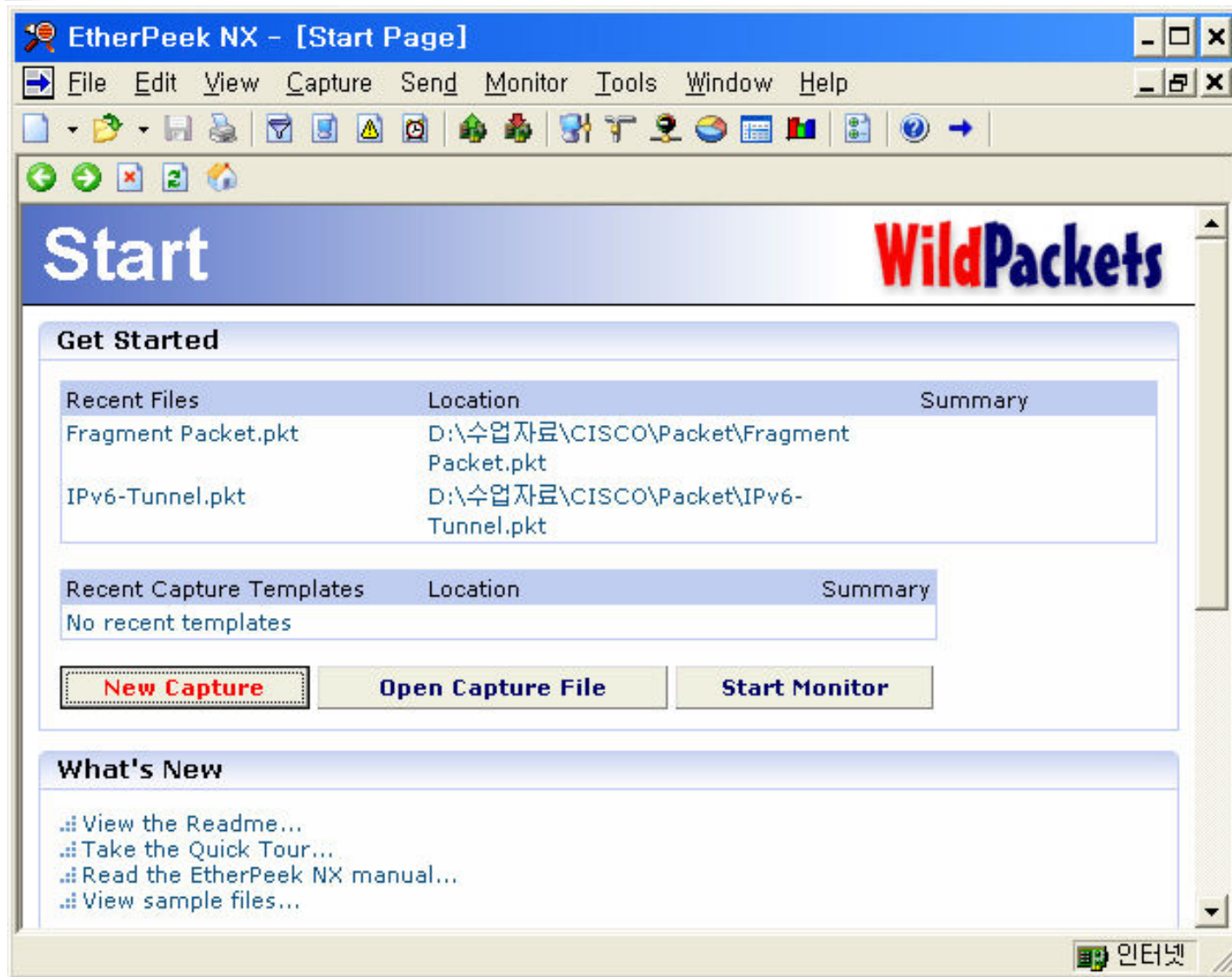
Window : 수신측이 받을 수 있는 데이터 사이즈를 수신측에서 송신측으로 전송하는 값

Checksum : TCP 헤더 데이터를 포함한 세그먼트 전체에 대하여 계산한 값이다. 에러 체크에 사용된다.

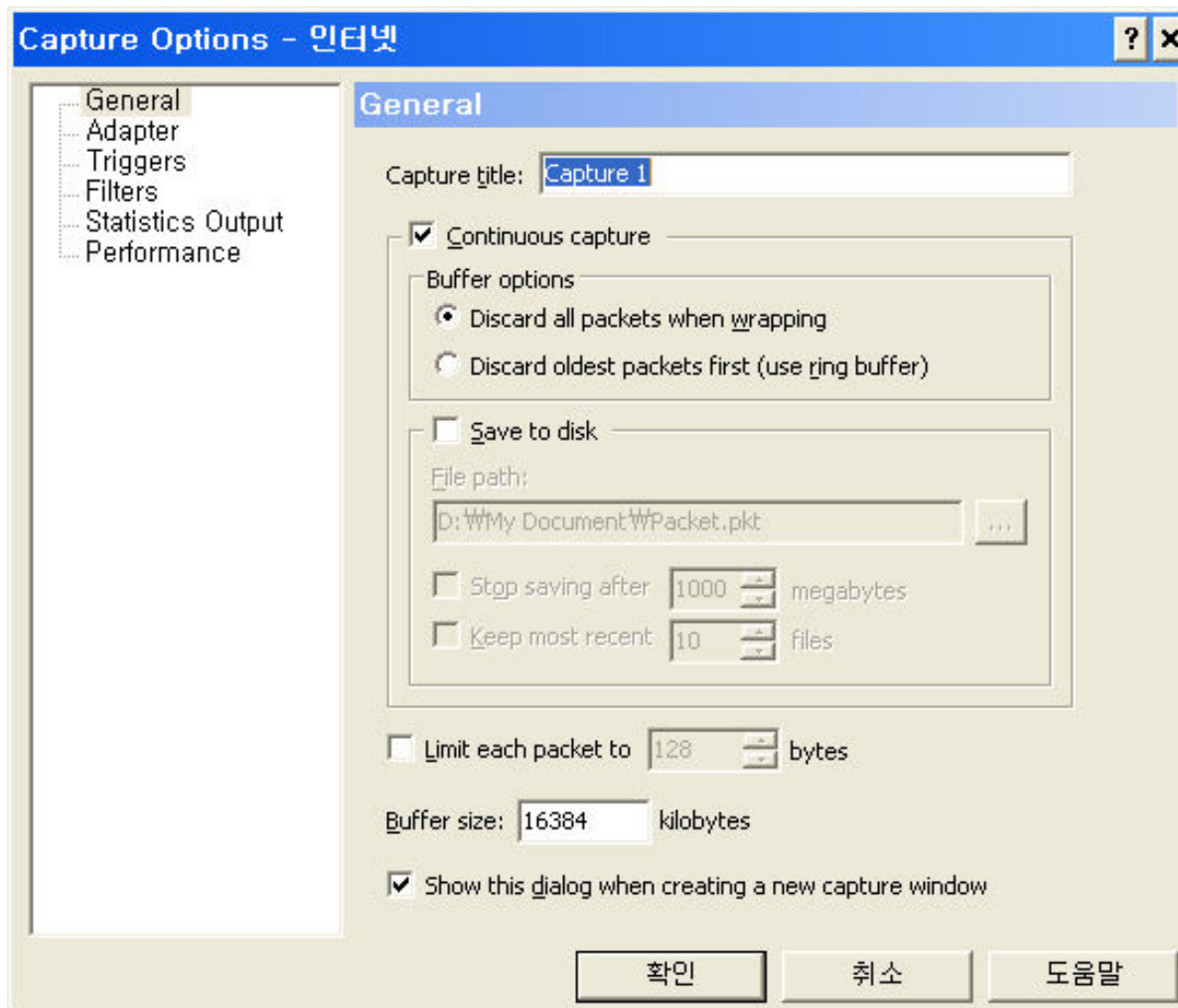
Urgent Pointer : 긴급히 처리해야 할 필요가 있는 데이터의 마지막 바이트의 위치를 나타낸다.

Option : 연결이 구성되는 동안 협상할 최대 Segment 크기(MSS) 옵션을 정의한다.

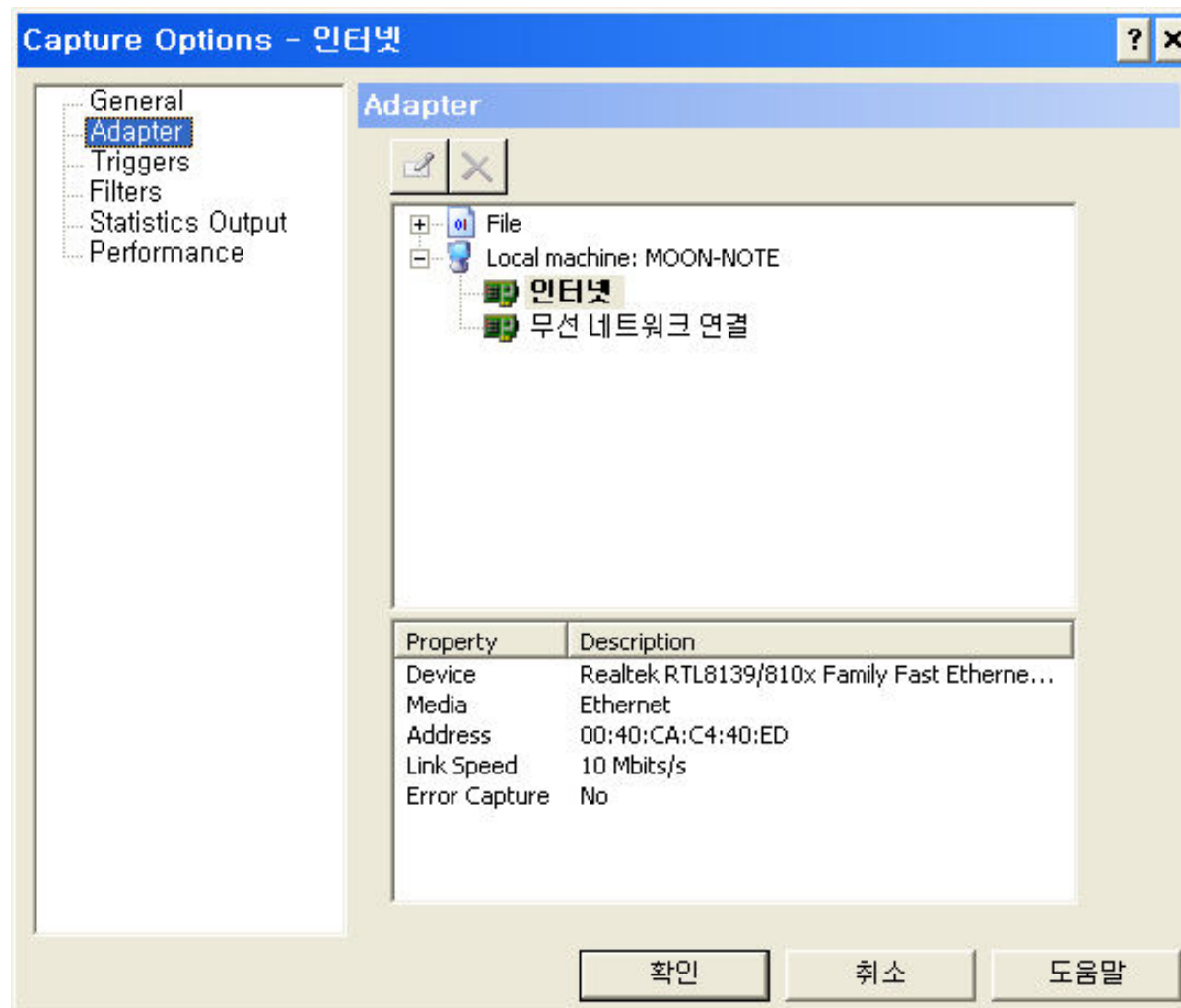
Etherpeek Packet Analyzer



Etherpeek 설정 - General



Etherpeek 설정 - Adapter



Packet Capture Start

EtherPeek NX - [Capture 1]

File Edit View Capture Send Monitor Tools Window Help

Packets received: 255 Memory usage: 1%
Packets filtered: 255 Filter state: ← Accept all packets Stop Capture

Packet	Source	Destination	Flags	Size	Absolute Time	Protocol
240	IP-192.168.1.30	IP-168.126.63.1		80	10:49:56.859274	DNS
241	IP-192.168.1.30	IP-168.126.63.1		80	10:49:57.859169	DNS
242	IP-192.168.1.30	IP-168.126.63.1		77	10:49:58.745982	DNS
243	IP-192.168.1.30	IP-168.126.63.1		80	10:49:59.859541	DNS
244	IP-192.168.1.30	IP-222.122.50.242		64	10:50:00.390147	HTTP
245	IP-192.168.1.30	IP-219.255.135...		64	10:50:00.390944	HTTP
246	IP-192.168.1.30	IP-219.255.135...		64	10:50:00.391171	HTTP
247	IP-192.168.1.30	IP-222.122.16.94		64	10:50:00.395862	HTTP
248	IP-192.168.1.30	IP-220.73.156.144		64	10:50:00.396227	HTTP
249	IP-220.73.156.144	IP-192.168.1.30		64	10:50:00.400255	HTTP
250	IP-192.168.1.30	IP-220.73.156.144		64	10:50:00.400316	HTTP
251	IP-222.122.16.94	IP-192.168.1.30		64	10:50:00.400644	HTTP
252	IP-192.168.1.30	IP-222.122.16.94		64	10:50:00.400674	HTTP
253	IP-192.168.1.30	IP-222.122.50.242		64	10:50:00.624221	HTTP
254	IP-192.168.1.30	IP-168.126.63.1		77	10:50:02.746746	DNS
255	IP-192.168.1.30	IP-168.126.63.1		80	10:50:03.860300	DNS

Packets Nodes Protocols Summary Graphs Expert Log Peer Map Filters

Capturing 무선 네트워크 연결 Packets: 255 Duration: 0:00:37
For Help, press F1 인터넷



LAB : Network Analyzer를 이용한 packet 캡처하기

- Network Monitor 설치하기
- ARP, ICMP 패킷 캡처하기