SENA
TECHNOLOGIES

Network Protocol

< HelloDevice에 적용된 인터넷 프로토콜 >

Sena Technologies, inc.

SENA TECHNOLOGIES

< 목 차 >

SENA TECHNOLOGIES

1. Protocol 이란?

- 두 관련 프로그램간에 교환되는 데이터에 일정한 형태를 규정하는 규칙을 말하며 데이터의 교환을 효율적으로 만드는 기능을 수행한다.
- 데이터 처리 시스템에서는 통신의 복잡성으로 인하여 하나의 프로토콜에서 모든 작업을 수행하는 것은 바람직하지 않다. 그러므로 , 서로 다른 기능을 수행하며, 상호작용을 통하여 사용자에게 서비스를 제공하는 다중의 프로토콜 층 형태로 이루어진 다수의 통신 프로토콜을 사용한다.

1) OSI(Open Systems Interconnect) 참조 모델

- ISO(International Standards Organization)에 의해 발전된 구조모델로 데이터 통신의 구조와 기능을 묘사하는데 자주 사용
- 하나의 일을 수행하기 위해 관련기능 들을 그룹화한 계층화의 개념으로 구성

Layer	설 명
Application	Consists of application programs that use the network
Presentation	Standardizes data presentation to the applications
Session	Manages session between applications
Transport	Provides end -to -end error detection and correction
Network	Manages connections across the network for the upper layers
Data Link	Provides reliable data delivery across the physical link
Physical	Defines the physical characteristics of the network media

표 1) OSI 참조모델

(1) Physical layer

- 데이터 전송 신호를 운반하는데 요구되는 하드웨어의 특성을 정의
- 전압레벨, 인터페이스 핀의 위치와 수 같은 것들이 이층에서 정의된다.
- 예 : RS -232C, V.35

(2) Data link layer

- 신뢰할 수 있는 정보의 전송을 보장하고 전송매체에 연결된 스테이션들에 주소를 지정하는 것

(3) Network layer

- Network를 통한 연결을 관리

- 패킷을 교환노드에 전송하는 방법 등을 통하여 두 스테이션간의 가상경로를 만듬.
- 일반적으로 IP(Internet Protocol)을 TCP/IP의 네트워크층으로 본다.

(4) Transport layer
- 수신측이 전송된 데이터를 그대로 받을 수 있도록 보장한다.
- TCP/IP 의 TCP 및 UDP등이 속한다.

(5) Session layer
- Transport 개체간의 연결에 있어서 메시지의 교환을 제어하는 역할
- 전송방향의 변경, 연결에 대한 인터럽트후 세션의 재시작 등을 관리

(6) Presentation layer
- 데이터를 교환하기 위해 함께 일하는 응용 층들은 어떻게 데이터를 표현할지를 동의해야 한다.
- 표준 데이터 표현루틴을 제공

(7) Application layer
- 사용자가 사용하는 네트워크 프로세서들이 있는 프로토콜 계층
- Telnet, HTTP, 등

2) 프로토콜의 기능
- 통신 양단의 주소지정, 데이터 흐름의 제어 및 신뢰할 수 있는 전송 서비스 제공.
- 에러감시(error detection) : checksums, sequence numbers, acknowledgements,
- 에러제거(error elimination) : retransmission of packets, correction methods
- 주소지정(addressing) : address fields
- 흐름제어(flow control) : receive windows, acknowledge

3) 프로토콜의 형태별 분류
- 연결위주 형과 비연결형으로 나누어진다.
- 연결위주 형은 호출된 개체들이 서로 인식되어지고 몇 가지 형식의 데이터가 교환된 후 연결이 확립되면 데이터가 교환된다. 그리고 서로간의 데이터 교환이 명백하게 이루어졌음을 합의해야 연결이 해제된다.
- 비연결형은 규격에 맞는 데이터를 단순히 전송하기만 하므로 신뢰도가 떨어지나 연결위주 형보다 간단하기 때문에 속도가 빠르다.

2.TCP/IP

1) TCP/IP 프로토콜 구조의 계층

Layer	설 명
Application	Consists of applications and processes that use the network
Host -to -Host Transport	Provides end -to -end data delivery services
Internet	Defines the datagram and handles the routing of data
Network Access	Consists of routines for accessing physical network

표 2) TCP/IP 계층구조

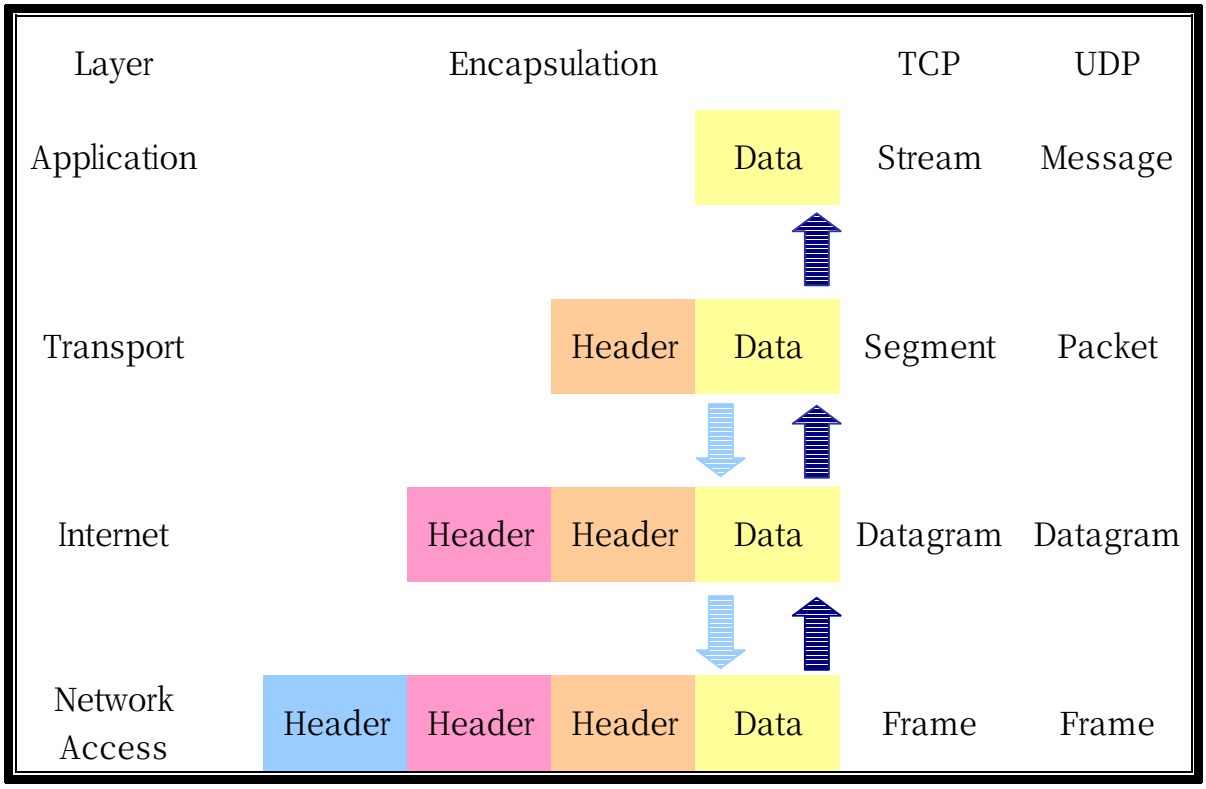

표 3) 데이터 캡슐화, 데이터의 구조

데이터는 네트워크로 보내질 때 스택의 아래로 전송되고, 네트워크로부터 데이터를 받을 때는 스택의 위로 전송된다. 스택의 각각의 층에서 올바른 전송을 위해 제어정보를 추가한다. 이러한 제어 정보를 헤더라고 한다. 각각의 층은 위의 층으로부터 받은 데이터를 정보의 전부로 여기고, 그 정보 앞에 자신의 층의 헤더를 위치시킨다. 각 층마다 전송정보를 추가하는 것을 캡슐화(Encapsulation)라고 한다.

2) Network Access Layer
- 직접적으로 연결된 네트워크상에서 시스템이 다른 장치로 데이터를 전송하는 수단을 제공한다.
- OSI 참조모델 중 하위 세 층(네트워크, 데이터링크, 물리 층)의 역할을 내포하고 있다.
- IP 데이터그램을 네트워크에 의해 전송되는 프레임들 안에 캡슐화 하는 것을 포함한다. 그리고 IP주소를 네트워크에 의해 사용되는 물리적주소에 매핑한다.
- 주소 찾기 프로토콜(ARP) : IP 주소를 이더넷주소에 매핑
3) Internet Layer
- IP(Internet Protocol)는 TCP/IP 네트워크상에서 기본적인 패킷 전송 서비스를 제공한다.
- IP의 위 아래 계층의 모든 프로토콜은 데이터를 전송하기 위해 인터넷 프로토콜을 사용한다.
- 마지막 목적지에 관계없이 들어오고 나가는 모든 TCP/IP데이터는 IP를 통하여 흐른다.
- ICMP(Internet Control Message Protocol)는 TCP/IP를 위해 흐름제어, 에러보고, 정보제공 기능을 수행하는 메시지를 보낸다.
4) Host -to -Host Transport Layer
- Transport layer의 가장 중요한 프로토콜은 전송제어 프로토콜(TCP : Transmission Control Protocol)과 사용자데이터그램 프로토콜(UDP : User Datagram Protocol)이다.
- TCP는 종단간 오류감지 및 교정으로 신뢰성 있는 데이터전송서비스를 제공한다.
- UDP는 작은 오버헤드, 비연결 데이터전송서비스를 제공한다.
- 두 프로토콜 모두 응용 층과 인터넷층사이에서 데이터를 전송한다.
5) Application Layer
- 데이터를 전송하기 위한 트랜스포트 층을 사용하는 모든 프로세서를 포함한다.
- 대부분은 사용자 서비스를 제동하며 새로운 서비스는 항상 이층에 추가되고 있다.
- TELNET(Network Terminal Protocol) : Network상의 원격로그인 제공
- FTP(File Transfer Protocol) : 대화식 파일전송에 사용
- SMTP(Simple Mail Transfer Protocol) : 전자우편을 배달
- 기타 많은 프로토콜이 포함된다.

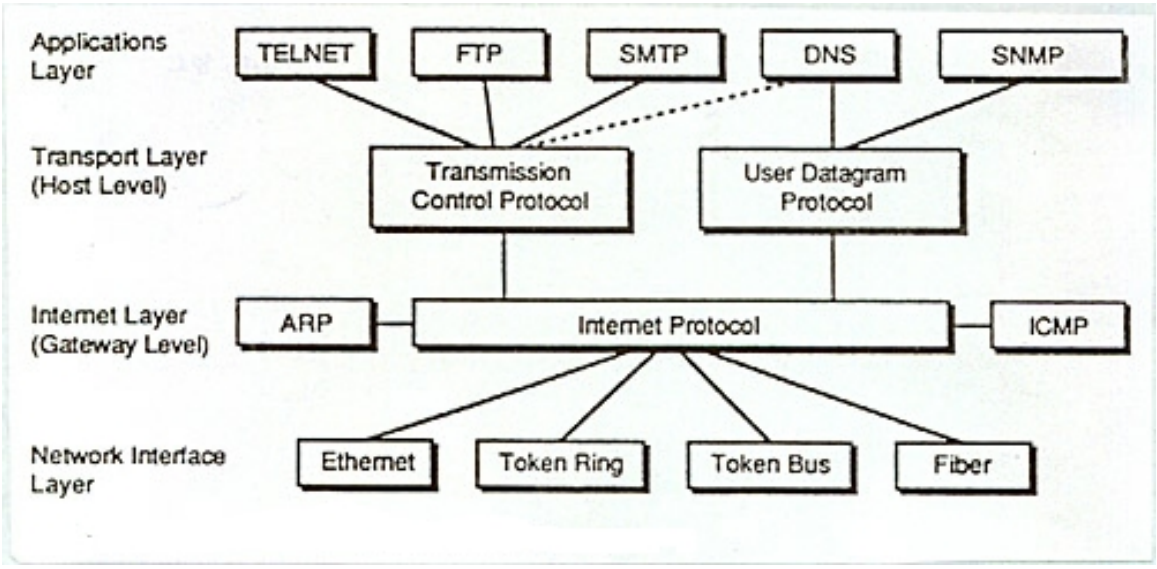

그림 1) Internet Protocol

3. HelloDevice에 적용된 인터넷 프로토콜

	OSI	TCP/IP	HelloDevice 지원				
7	Application	Application	HTTP	DIO,DPRAM,Serial	시스템 설정	BOOTP	DHCP
6	Presentation						
5	Session						
4	Transport	Transport	TCP		UDP		
3	Network	Internet	IP	ICMP	ARP		
2	Data link	Network Access	Ethernet(IEEE802.3)		PPP		
1	Physical layer						

표 4) HelloDevice에 적용된 인터넷 프로토콜

4. Ethernet (IEEE 802.3LAN)

1) 특징

- 일반적으로 DEC, Intel, Xerox사가 1982년에 제안한 표준을 의미하며 CSMA/CD 라고 하는 Access method 사용한다.
- 동축케이블, UTP Cable, 광케이블사용
- 1/10/100Mbps의 Ethernet

2)CSMA/CD(Carrier Sense Multiple Access with Collision Detection)

- 전송미디어(동축케이블)의 캐리어 검출신호를 감시해 전송미디어가 타국에 의해 사용되고 있는가 아닌가를 감지하고 타국이 송신하고 있지않으면 데이터를 송신하고 만약 송신 중에 있으면 송신연기를 실행한다. 그리고 캐리어 검출신호가 없어진 단계에서 최소 프레임간 스페이싱 시간(프레임과 프레임간의 갭 시간:9.6us)후에 데이터 송신을 한다. 또 데이터 송출 중에 데이터의 충돌이 일어나면 일정시간(3.2us)동안 잼 신호(방해신호)를 송출한 후, 난수에 의해 결정되는 대기시간(back-off time)후에 재전송한다.

3) 10 Base-T

- 10 : 10Mbps, 간선의 전송속도
- Base : 베이스밴드방식, 전송방식
- T : Twisted Pair Cable, 전송매체
-기타 : 10Base2, 10Base5, 100BaseT4, 100BaseTX, 10BaseF

4) Ethernet Encapsulation(RFC 894)

Packet

Frame

Ethernet Preamble	Dest. Addr.	Src. Addr.	Type (Len)	Data		FCS
8Byte	6Byte	6Byte	2Byte	46Byte ~ 1500Byte		4Byte
			0x0800	IP Datagram(46 ~ 1500)		
			0x0806	ARP frame(28)	PAD(18)	
			0x0836	RARP frame(28)	PAD(18)	

표 5) Ethernet packet(()내의 단위는 Byte수)

- Ethernet Preamble : 통신 시 동기확립을 위하여 사용함(10101010…11)
- Dest. Addr. : 수신처 어드레스
- Src. Addr. : 발신원 어드레스
- Type,Length : 프로토콜 타입, 데이터의 길이
- Data : 실직적인 데이터(IP Datagram ,ARP등)

- PAD : 데이터가 최소프레임 길이에 도달하지 못할 때 추가하여 조정하는 여분의 비트
- FCS : Frame Checksum Sequence. 프레임 검사
- Packet의 format은 위와 같으며, 이들이 각 단계마다 해당되는 Protocol

5) Station Address(H/W Address)

- 6Byte로 된 Station Address,
- 최초의 2Bit[Group bit, Local Bit]

G	L	7	15	23	31	39	47

항목	설명
G:1 L:1	로컬적으로 관리되는 Multicast Address
G:1 L:0	IEEE에서 관리되는 Multicast Address
G:0 L:1	로컬적으로 관리되는 각 스테이션 어드레스
G:0 L:0	IEEE에서 관리되는 각 스테이션 어드레스

표 6) Station Address 구조

7 Application	Application(TELNET,FTP,HTTP…)		
6 Presentation	Host/Network Byte Order Conversion		SSL
5 Session	RPC		
4 Transmission	TCP		UDP
3 Network	IP	ICMP	ARP
2 Data Link	Ethernet		PPP
1 Physical	Network Hardware		

표 7) OSI 참조모델과 Ethernet

5. PPP(Point-TO-Point Protocol)

1) 특징

- Serial links를 통하여 Datagram을 캡슐화 시키는 방법으로 PPP는 PPP Link를 통한 Datagram encapsulation의 기본인 HDLC(High Level Data Link Control) Protocol을 사용한다.
- 데이터링크 층의 프로토콜로서 LCP(Link Control Protocol)을 사용하여 MTU길이의 네고시에이션을 포함한 데이터링크의 확립과 설정 등의 제어를 한다.
- 서로 다른 네트워크층에서의 프로토콜제어를 위해서 NCP(Network control Protocol)가 있어 네트워크의 확립과 설정을 한다.
- 복수의 프로토콜을 지원하고 있고, IP/OSI/IPX등을 동일링크 상에 캡슐화시킬수있다.
- XON/XOFF등을 포함한 제어문자를 투과(Escape)한다.제어문자의 경우 7D를 삽입하고 +20h 한 값을 넣어서 보낸다.(예:0x01 -> 0x7d,0x21)
- 0x7e -> 0x7d, 0x5e , 0x7d -> 0x7d, 0x5d로 변경

2) PPP Frame구성

Flag	Address	Control	Protocol	Data	FCS	Flag
7E	FF	03H	2Byte	0 ~ MTU(1500)	2Byte	7E
			0x0021	Internet Protocol		
			0x8021	IP Control Protocol		
			0xC021	Link Control Protocol		

표 8) PPP Frame

- Flag : Frame의 처음과 끝을 가리킨다.
- Address : Broadcast주소의 표준, PPP는 각개의 Station주소를 할당하지 않는다.(Constant)
- Control : 불연속 Frame에서 User data전송을 부른다.(Constant)
- Protocol : Frame의 정보필드에 캡슐화되어있는 Protocol
- Data : Protocol 의 Datagram, 최대 1500Byte
- FCS : Frame Check Sequence

3) PPP 연결 순서

- LCP에 의한 연결설정 : 양쪽 Peer가 PPP로 접속하게 되면 동시에 양쪽 Peer에서 LCP 접속시도를 하게 된다. 이는 Request 및 그에 따른 Acknowledgment의 절차로 진행된다.
- 위의 과정이 완료하게 되면 Network에 연결하기 위한 설정을 NCP(IPCP)가 하게 된다.
- IPCP에 의해 IP를 할당 받을 수 있다.
- 위의 과정이 종료되면 Data를 교환할 수 있다.
- 모든 데이터 교환 종료 후 LCP에 의해 연결을 종료한다.

7 Application	Application(TELNET,FTP,HTTP…)		
6 Presentation	Host/Network Byte Order Conversion		SSL
5 Session	RPC		
4 Transmission	TCP		UDP
3 Network	IP	ICMP	ARP
2 Data Link	Ethernet		PPP
1 Physical	Network Hardware		

표 9) OSI 참조모델과 PPP

6.IP(Internet Protocol)

1) IP의 특징

- TCP/IP 의 기초를 이루는 프로토콜이다.
- 종점간의 신뢰성 있는 메시지전달이나 흐름제어를 위한 기능을 가지고 있지 않은 비

연결 프로토콜이다.
- 필요 시 패킷을 분할, 단편화 한다.
- 최대 Packet 의 크기는 65,535바이트이다.
- 유한한 Packet수명을 갖는다.

2) IP Frame

<table>
<tr><td colspan="2">0 3 7</td><td>15</td><td colspan="3">18 23</td><td>31</td></tr>
<tr><td>Version</td><td>Length</td><td>Service Type</td><td colspan="4">Packet Length</td></tr>
<tr><td colspan="3">Identification</td><td></td><td>DF</td><td>MF</td><td>Fragment Offset</td></tr>
<tr><td>Time to live</td><td colspan="2">Transport</td><td colspan="4">Header checksum</td></tr>
<tr><td colspan="7">Source Address</td></tr>
<tr><td colspan="7">Destination Address</td></tr>
<tr><td colspan="6">Options</td><td>Padding</td></tr>
</table>

표 10) IP Header

- Version : 현재 IP의 버전표시, 4
- Length : IP Header의 길이
- service Types : 송신한 IP datagram이 요구하는 서비스 품질. 우선도 지정, 지연이 적은 경로의 요구, 전송효율과 높은경로등의 요구
- Packet Length : Protocol Header를 포함한 패킷의 길이(Byte단위)
- Identification : 송신호스트에 의해 생성되는 식별자. 단편들의 연결조각을 식별하기 위해 사용된다.
- Flags : DF(Don't Fragment), MF(More Fragment) 두 비트는 단편화의 경우 패킷의 처리를 제어한다. DF가 세트되면 단편화되지 않는다. MF 비트는 더 이상의 추가적인 서브패킷이 있는지를 나타낸다.
- Fragment offset : MF 비트가 세트되어있다면 이 항목은 패킷에 든 서브 메시지의 전체 메시지의 시작으로부터의 상대적인 위치를 나타낸다. 수신 호스트는 이 항목을 이용하여 원래의 패킷으로 재결합할 수 있다.
- Time to live : 송신 호스트는 패킷이 버려지기까지 얼마나 오랫동안 네트워크상에 존재할 수 있는 지를 확정한다. 이 항목에 사용되는 단위는 초(sec)이며 노드는 이 값을 최소한 1이상 감소할 것을 요구한다. 따라서 일반적으로 이 값은 패킷이 지나갈 수 있는 최대의 노드 수와 같다. 이 값을 설정함으로써 패킷이 네트워크상에서 무한정 회전하는 것을 막을 수 있다. 일반적으로 이 값은 15 ~ 30사이의 값으로 설정한다.
- Transport protocol : IP 데이터필드에 포함하는 IP의 상위 프로토콜을 식별하기 위한 프로토콜 코드. (예 - TCP:6, UDP:17, ICMP:1)
- Header checksum : IP 헤더필드의 에러검출을 위한 checksum

- Source Address : 송신한 곳의 IP Address
- Destination Address : 수신한 곳의 IP Address
- Option : IP 데이터그램 전송 시에 라우터등에 의뢰하는 처리를 지시한다. 경로기록, 고정경과에 의한 전송, 보안, 통과시각의 기록등
- Padding : 옵션영역을 사용하는 경우 IP헤더필드가 32 비트의 정수배가 되도록 삽입하는 부분

3) IP Address의 Class

	0	8	16	24	영 역
Class A	0 Net ID	Host ID			1.0.0.1 ~ 126.255.255.254
Class B	1 0 Network ID		Host ID		128.0.0.1 ~ 191.255.255.254
Class C	1 1 0 Network ID			Host ID	192.0.0.1 ~ 223.255.255.254
Class D	1 1 1 0 Multicast Address				
Class E	1 1 1 1 미래를 위한 예약				

표 11)IP Address의 Class

- IP Address의 할당은 nic에서 관리한다(network Information Center)
- 네트워크에 연결된 모든 호스트는 고유한 주소를 가져야 한다.
- Network ID는 컴퓨터가 포함되어 있는 네트워크를 정의하고 Host ID는 이 네트워크 내의 특정 컴퓨터를 나타낸다.
- Host ID 가 모두 0인 경우는 네트워크 자체를 나타내고 모두 1인 경우는 브로드캐스트 어드레스용이므로 사용할 수 없다.
- Class A의 Network ID 127은 특수한 목적(루프 백 주소)으로 예약되어 있으므로 통상의 네트워크 Address로 사용할 수 없다.

4) Subnet Mask

- IP Address중 Host ID부분을 복수의 보다 작은 네트워크로 분할할 수 있다. 이렇게 하면 호스트 ID로써 사용되고 있던 어드레스 값도 네트워크 ID부분으로 편이할 수 있기 때문에 보다 많은 네트워크를 수용할 수 있게 된다.
- Subnet화를 위해 32bit IP Address의 Network ID와 host ID를 구분할 수 있도록 설정하는 값
- Class A : 255.0.0.0, Class B : 255.255.0.0, Class C : 255.255.255.0
- Public IP Address : 외부의 네트워크에 IP레벨에서 액세스하는 호스트

- Private IP Address : 네트워크 외부로의 액세스를 하지 않고 자신의 네트워크내에 만으로 폐쇄된 호스트, 외부의 네트워크에 액세스하는 일이 있지만 한정된 서비스(전자우편,FTP,NEWS,Rlogin)만을 사용하는 호스트에 사용
- SubNet의 구성으로 부족한 IP Address의 효율적 활용이 가능하다.

5) IP Routing

- Routing Table을 검색하여 호스트와 목적지가 직접 연결되어 있거나(같은서브넷) 공유된 네트워크(같은 네트워크 그룹)일 경우 목적지로 직접 전송하거나 next-hop 라우터로 데이터그램을 전송한다.
- 그렇지 않은 경우 데이터그램을 Default 라우터로 보낸 후 라우터가 목적지로 직접 전송하게 된다.
- 만일 위와 같이 전혀 일치하는 항목이 없다면 데이터그램을 폐기하고 "Host Unreachable" 또는 "Network unreachable" 메시지가 Application에 반송된다.

6) 단편화(Fragmentation)

- 어떠한 유형의 네트워크를 통해서라도 패킷을 전송하기 위해서 IP는 각각의 네트워크에서 데이터그램의 크기를 조절할 수 있는 기능을 제공한다.
- 단편화는 각 네트워크내의 각 노드의 IP가 수신한 패킷을 다음 노드나 호스트로 전송하기 위해 이 패킷을 분할하는 것을 말하며 모든 목적지 호스트는 단편화된 메시지를 재합성할 수 있어야 한다.

7. ICMP(Internet Control Message Protocol)

- TCP/IP를 위해 제어,에러보고,정보제공 기능을 수행하는 메시지를 보낸다.

1) ICMP Header

0	7	15	31
Type	Code	Checksum	
Miscellaneous			
Data(IP protocol Header, 8byte test Data)			

표 12) ICMP Header

- Type : ICMP 메시지의 타입
- Code : 위에서 지정한 타입에 속하는 하위기능을 지시하는 코드
- Checksum : 완전한 ICMP 메시지의 Checksum
- Miscellaneous : 순서번호나, 인터넷주소 등을 담기 위한 항목
- IP protocol Header : Error가 발생한 IP 데이터그램의 헤더와 그 안에 있는 데이터의 첫 8Byte

2) ICMP 패킷의 타입

타입	기능	타입	기능
0	Echo reply	3	Destination Unreachable
4	Source quench	5	Redirect
8	Echo request	11	Time exceeded for a datagram
12	Parameter problem on a datagram	13	Time stamp request
14	Time stamp reply		

표 13) ICMP 패킷의 타입

(1) Destination unreachable : 다음과 같은 메시지 운반
- Network, Host, Protocol 또는 Port를 찾을 수 없음
- 단편화가 필요하나 DF비트가 설정되어 있음

(2) Source quench
- Gateway가 메시지를 임시 저장할 용량을 가지고 있지 않은 경우 Gateway는 해당 Host에 메시지 보냄
- 전송 Host는 반드시 뒤에 이어지는 메시지의 전송속도를 낮추어야 한다.

(3) Redirect
- IP 패킷의 전송경로 상에 불필요한 우회전송이 발생하는 경우 이 메시지를 전송한다.
- ICMP 패킷에 다음번 Gateway의 주소를 담고있으므로 전송개체의 경로 표에 기록된다.

(4) Echo reply and Echo request
- Echo request가 한 컴퓨터에 전송되면 결과로서 Echo reply를 보낸다.
- 지연시간의 측정이나 작업준비의 확인 등의 기능을 구현하는데 사용한다.

(5) Time exceed
- TTL(Time To Live)이 종료됨에 따라 무시되는 메시지나 단편 재합성 타이머가 종료한 메시지를 전송하는 개체에게 전달

(6) Parameter problem
- 잘못된 프로토콜 헤더 항목을 가진 IP 데이터그램의 전송개체에게 그 패킷이 무시되었음을 알림

8.ARP(Address Resolution Protocol)

(1) 특징
- IP주소에서 Ethernet주소와 같은 물리적인 하드웨어 주소로의 변환
- ARP 요구와 응답으로 이루어져 있으며 ARP요구는 네트워크에 연결된 모든 호스트에 Broadcast한다.
- 이 요구에 있는 IP주소를 소유하고 있는 기계는 이 ARP요구에 응답하여 자신의 하

드웨어 주소를 담고있는 ARP 응답을 보낸다.

(2) ARP 패킷 형식

0	8	16	24 31
Hardware Type		Protocol Type	
H/W Addr. Length	Pro. Addr.Length	Operation	
Sender Hardware Address(Byte0 -3)			
Sender Hardware Address(Byte4 -5)		Sender IP Address(Byte0 -1)	
Sender IP Address(Byte2 -3)		Target Hardware Address(Byte0 -1)	
Target Hardware Address(Byte2 -5)			
Target IP Address(Byte0 -3)			

표 14) ARP 패킷형식

- Hardware Type : Ethernet 1
- Protocol Type : ARP request(1), ARP response(2), RARP request(3), RARP response(4),

(3) ARP 캐시

- 운영체제에서는 ARP요구 후 응답이 들어오면 그 내용을 ARP 캐시에 저장하고 일정 시간이 지나면 캐시에서 내용을 삭제한다.

(4) ARP 명령

- C:\ > arp a (ARP 캐시의 내용을 본다)
- C:\ > arp d 192.168.1.25 (ARP 캐시의 내용에서 192.168.1.25를 삭제)

(5) RARP

- ARP와는 반대로 H/W Address로 IP Address를 찾는 프로토콜
- ARP와 패킷 형식은 같고 Protocol Type만 다르다.

9.TCP(Transmission Control Protocol)

1) 특징

- 트랜스포트 층의 프로토콜이다.
- TCP의 주된 작업은 네트워크를 통한 신뢰할 수 있는 데이터의 전송이다.
- 연결형 바이트 스트림 프로토콜이다.

2) 전송방식

- TCP는 재전송을 위하여 긍정적수신인식(PAR, Positive Acknowledgement with Re-transmission)방식을 사용한다.
- 이것은 원격시스템으로부터 데이터를 성공적으로 도착했다는 메시지를 받지 않으면 데이터를 재전송한다.

- TCP의 데이터 유닛을 세그먼트라고 한다. 각 세그먼트는 수신자가 데이터가 손상되지 않은 것을 검증하는 Checksum을 가진다.
- 수신자는 송신자로부터 데이터를 받은 후 Checksum을 이용하여 데이터에 손상이 없으면 긍정적수신인식을 보낸다. 만약 데이터 세그먼트가 손상되었다면 수신자는 이 세그먼트를 폐기한다.
- 송신자는 적정 시간이 지난 후 긍정적수신인식이 도착하지 않으면 세그먼트를 재전송한다.

3) TCP Segment 형식

<table>
<tr><td colspan="2">0</td><td colspan="2">8</td><td colspan="2">16</td><td colspan="2">24 31</td></tr>
<tr><td colspan="4">Source Port</td><td colspan="4">Destination Port</td></tr>
<tr><td colspan="8">Sequence Number</td></tr>
<tr><td colspan="8">Acknowledgment Number</td></tr>
<tr><td>offset</td><td colspan="2">Reserved</td><td>Flags</td><td colspan="4">Windows Size</td></tr>
<tr><td colspan="4">Checksum</td><td colspan="4">Urgent pointer</td></tr>
<tr><td colspan="6">Options</td><td colspan="2">Padding</td></tr>
<tr><td colspan="8">Data</td></tr>
</table>

표 15) TCP Segment 형식

(1) Source & Destination Port : 각각 16bit크기의 이 두 항목은 가상회선의 양끝의 종점을 지정한다.

(2) Sequence & Acknowledge Number : 각 32bit크기를 가지며 이 두 항목은 각 데이터가 연결이 설정되어 있는 동안 교환되는 데이터의 전체 흐름에서 어느 위치에 해당하는지를 나타낸다. Sequence Number는 송신방향에서의 순서를 나타내고 acknowledge number는 수신되는 바이트의 순서에 적용된다.

연결이 설정되면 TCP연결에 참여하는 양 종점은 초기 Sequence Number를 설정하는데 이 값은 해당패킷이 네트워크상에 남아있는 동안(IP Time to live)에는 반복되지 않는다. 이 값들은 연결 설정 시 교환되며 승인된다. 데이터 전송 시 송신 개체는 Sequence Number를 앞서 송신한 바이트의 수만큼 증가시키며 Acknowledge Number는 수신개체가 얼마만큼의 데이터를 정확하게 수신하였는지 표시한다.

(3) Data offset : TCP Header의 크기를 나타낸다. 데이터영역의 시작을 판단하는데 사용된다.

(4) Flags : TCP에서의 특정작업을 유발한다.

- URG : Urgent 항목의 포인터가 유효함
- ACK : Acknowledgement number 유효함
- PSH : 해당 세그먼트의 데이터는 응용프로그램에 전달되어야 한다. 이 세그먼트에 대한 Acknowledgement는 현재 Acknowledgement Number까지의 모든 데이터가 수신개체에 도달했음을 알려준다.

- RST : 연결을 재설정하거나 유효하지 않은 세그먼트에 대한 응답으로 사용
- SYN : 연결설정요구를 나타내며 반드시 승인되어야 한다.
- FIN : 한쪽 끝에서 유발되는 연결의 종료와 일정방향으로의 데이터 흐름의 끝을 나타낸다. 반드시 승인되어야 한다.

(5) Window Size
- 이 항목은 수신개체가 해당 연결에 할당된 버퍼로 받아들일 수 있는 데이터의 바이트 수를 나타낸다. 목적지 TCP는 데이터의 흐름을 제어하기 위해 이 항목을 사용한다.

(6) Checksum : 16bit 배타적 논리합에 의한 데이터 체크코드
(7)Urgent pointer : 긴급데이터의 스트림 상의 종료바이트의 위치를 나타낸다.
(8) Option : 최대 세그먼트 길이 등의 옵션을 지정

4) Port Number
- Port Number는 트랜스포트 레벨에서의 주소지정을 위하여 사용된다.
- 포트 번호는 16bit 크기를 가지므로 이론적으로 65,535개의 서로 다른 TCP 연결을 동시에 가질 수 있다.
- UDP도 Port Number를 사용하며 TCP와는 각각의 주소공간을 가지므로 같은 Port Number라도 동일하지 않다.
- 유용한 Port Number는 호스트에 따라 제한된다.
- Server의 포트 번호는 고정되나 Client의 Port Number는 Server가 특별한 Port Number를 지정하지 않는 한 관계없다.
- 일반적으로 알려진 Port Number : FTP(23,TCP),TFTP(69,UDP)..

5) TCP 의 연결(Three -way handshake)
- 호스트 A에서 SYN 플래그를 가진 세그먼트를 호스트 B에 보냄으로써 연결을 시작한다
- 이 세그먼트는 호스트 B에 호스트 A가 연결 설정을 원한다는 것을 알리며 이 세그먼트의 시작번호에서 어떠한 순서번호를 사용할 지 알려준다.
- 호스트 B는 수신인식(ACK)와 SYN비트 집합을 가진 세그먼트를 가지고 호스트 A에 응답하며 호스트 B가 어떤 순서번호를 가지고 시작할 지를 호스트 A에 알린다.
- 호스트 A는 호스트 B의 세그먼트를 인식하는 세그먼트를 보내고 실제 데이터를 전송한다.

6) TCP 연결의 종료
- 연결을 종료하기 위해 송신할 데이터 없음(FIN) 비트를 포함한 세그먼트를 가지고 Three -way handshake를 교환한다.

10. UDP(User Datagram Protocol)

1) UDP의 특징
- 신뢰성이 결여된 비연결형 프로토콜이다.

- 매우 간단한 형식의 프로토콜이다.
- 최선의 전송을 제공한다.
- 데이터의 에러감지를 위해 Checksum을 실행한다.
- Broadcast를 지원한다.

2) UDP Header

16bit Source port Number	16bit Destination Port Number
16bit UDP Length	16bit UDP Checksum
DATA	

표 16) UDP Header

- Source & Destination Port Number : 16bit로 TCP처럼 트랜스포트 층의 사용자 참조로 사용
- Length : Protocol Header를 포함한 전체 데이터그램의 길이
- Checksum : 데이터, 프로토콜 헤더, 등을 포함하는 Checksum

3) Checksum의 생성 : 가상 헤더를 만들어 Checksum계산

0	8	16	24 31
Source IP Address			
Destination IP Address			
Zero	Protocol	UDP Length	
16bit Source port Number		16bit Destination Port Number	
16bit UDP Length		16bit UDP Checksum	
DATA			Padding

표 17) 가상 헤더

3) 브로드캐스팅
- 어떤 호스트에서 케이블상의 모든 호스트에 프레임전송
- 목적지 IP Address 255.255.255.255
- UDP에 적용됨

4) 멀티캐스팅
- 멀티캐스트 그룹에 속한 호스트에 전송

11. BOOTP(Bootstrap Protocol)

1) 특징
- 디스크 장치가 없는 시스템의 초기 가동 시에 자신의 IP주소를 얻기 위해 RARP의 대용으로 개발된 프로토콜
- IP주소이상의 많은 정보 전달가능
- Router를 통과해 전송이 가능

2) BOOTP 패킷

0	8	16	24 31
Opcode	H/W Type	H/W Addr. Len.	Hop Count
Transaction ID			
Number of seconds		Flags	
Client IP Address(4byte)			
Your IP Address(4byte)			
Server IP Address(4byte)			
Gateway IP Address(4byte)			
Client H/W Address(16Byte)			
Server Host name(64Byte)			
Boot Filename(128Byte)			
Vendor Specific info(64Byte)			

표 18) BOOTP 패킷

- Opcode : Bootrequest(1), BootReply(2)
- H/W Type : Ethernet(1), IEEE 802.(6)..

3) 동작방식

- Client의 BOOTP Request에 대한 Server의 Reply로 설정된다.
- Server는 UDP .67, Client 는 68번 을 사용한다.

12. DHCP(Dynamic Host Configuration Protocol)

1) 특징

- UDP상의 프로토콜로 네트워크내의 시스템의 IP Address를 일원 관리하기 위한 방법을 제공한다.
- BOOTP와 포맷이나 프로토콜이 거의 같다.

2) BOOTP와 다른점

- 사용기한이 정해진 어드레스 설정이다
- IP Address를 위한 모든 파라미터 제공
- DHCP 메시지 타입을 지정

3) DHCP 패킷

0	8	16	24 31
Opcode	H/W Type	H/W Addr. Len.	Hop Count
Transaction ID			
Number of seconds		Flags	
Client IP Address(4byte)			

Your IP Address(4byte)
Server IP Address(4byte)
Gateway IP Address(4byte)
Client H/W Address(16Byte)
Server Host name(64Byte)
Boot Filename(128Byte)
Option

표 19) DHCP 패킷

- Option : DHCP의 메시지타입 지정, lease time등 설정(RFC1533)

4) IP Address 할당방법

- 자동할당(Automatic Allocation) : 영구적인 IP 할당
- 동적할당(Dynamic Allocation) : 사용기간 한정 IP 할당

(사용기간 4byte길이의 초 단위, 0xFFFFFFFF인 경우 무기한)

- 수동할당(Manual Allocation) : 네트워크 관리자가 IP Address할당

5) DHCP IP 결정방법

- 클라이언트가 DHCPDISCOVER 메시지를 브로드캐스트하면 DHCP 서버는 요구된 구성정보를 DHCPOFFER메시지로 통지한다.
- 클라이언트는 서버의 ID나 희망 정보 값을 실어 DHCPREQUEST메시지를 브로드캐스트하면 선택된 서버는 그 IP Address가 비워있을때(DHCPDISCOVER의 처리인 경우), 나 그 IP Address가 타당하며 비어있을때(DHCPREQUEST일 때)에는 DHCPACK(긍정응답), 그 외의 경우에는 DHCPNAK(부정응답)을 되돌려보낸다.
- 클라이언트가 DHCPACK를 받아 정합성을 체크 한 후 이상이 없으면 시스템구성을 시행하지만 문제가 생기면 DHCPDECLINE 메시지를 보내 다시 한번 처음부터 시작된다.(DHCPNAK인 경우도 다시 시작)
- 서버의 응답이 DHCPACK 나 DHCPNAK가 아닌 경우에는 DHCPREQUEST를 재전송한다.
- 클라이언트가 IP Address 사용기간 전에 사용을 끝내는 경우 DHCPRELEASE 메시지를 보내 해방시킨다.

13. HTTP(Hyper Text Transfer Protocol)

1) 특징

- WWW(World Wide WEB)이라 불리는 인터넷의 Application 레벨 프로토콜이다.
- 프로토콜 그 자체와 그 프로토콜상에서 보내지는 데이터 형식을 독립시킬 수 있다.
- 사용자 에이전트는 일반적으로 브라우저(Browser)라 불리운다.

2) 송수신 체계

- HTTP 는 Request와 Response라는 단순한 체계로 이루어져 있다.

- 클라이언트는 서버와 연결을 확립하고 , request method, URI, Protocol Version, 등을 서버에 Request를 보낸다.
- 서버는 메시지의 Protocol version, Status code, Status Line을 회신 한다. 마지막 메시지에 서버정보, 엔티티메타정보, 보디 컨텐츠 포함한다.

3) HTTP 메시지 Type

HTTP-message	Simple-Request	Method SP Full-Request-URI CRLF
	Simple-Response	Entity-Body
	Full-Request	Request-Line *(General-Header | Request-Header | Entity-Header) CRLF [Entity-Body]
	Full-Response	Status-Line *(General-Header | Request-Header | Entity-Header) CRLF [Entity-Body]

표 20) HTTP Protocol

- Simple-Request를 받으면 Simple-Response를 반환
- Method : Request-URI로 지정되는 리소스에 대해 실행되는 방법
  (GET,HEAD,POST 등)
- Request-URI(uniform Resource Identifier) : URL(장소) 또는 URN(이름)
- Request-Line : Method SP Request-URI SP HTTP-Version CRLF
- Status-Line : HTTP-Version Sp Status-Code Sp Reason-Phrase CRLF

14. 기타 프로토콜

1) SMTP : Simple Mail Transfer Protocol - Mail을 전송하는 프로토콜
2) FTP : File Transper Protocol - 파일을 전송하는 표준 프로토콜
3) IGMP : Internet Group Management Protocol Multicasting을 위한 Host와 Router을 위해 사용된다.
4) SNMP : Simple Network management Protocol 인터넷 관리 운영
5) SLIP : Serial Line Internet Protocol Dial-up 사용자가 네트워크를 사용하도록 하는 프로토콜.
6) NNTP : Network News Transfer Protocol