

통신 프로토콜 기본

- 1) TCP/IP의 이해
- 2) IPv4 주소체계
- 3) Host to host 통신
- 4) Network to network 통신



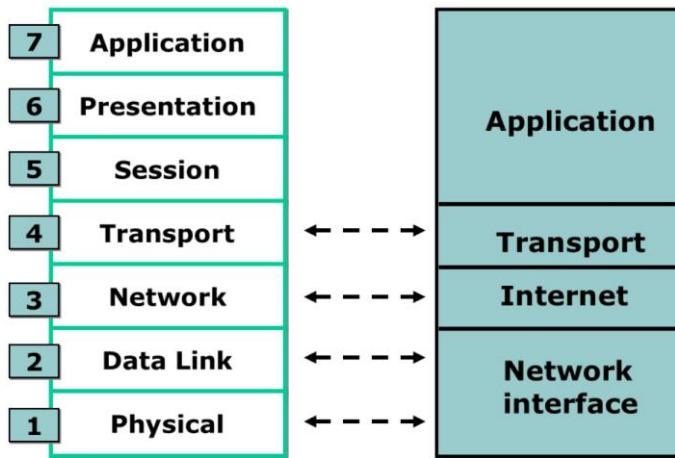
학습목표

- OSI 7layer와 비교하여 TCP/IP의 정의와 그 필요성을 이해합니다.
- IPv4 주소체계와 subnetting을 이해합니다.
- 같은 네트워크 내에 있는 호스트간 통신과정을 이해합니다.
- 다른 네트워크 간 통신과정을 이해합니다.

1. TCP/IP의 이해

3.1 TCP/IP의 이해

● OSI 7 참조모델과 TCP/IP 비교



● TCP/IP (Transmission Control Protocol/Internet Protocol)

- 1960년대 말 미국 국방성이 개발한 ARPANET용의 통신프로토콜로 광역의 상용 패킷교환망이나 최근 폭발적으로 사용하는 인터넷등에 사용됨
- 인터넷 아키텍처 위원회(IAB:Internet Architecture Board)에서 TCP/IP에 관련된 프로토콜이나 오퍼레이션 절차 등을 규정한 RFC(Request For Comments) 사양을 발표하고 있음
- 이 RFC에 대하여 ISO는 1994년 10월 파리에서 IAB하의 IETF와 회의를 갖고 PAS(Public Available Specification, 공개되어 있는 표준)로서 인정할 것을 결정 했음

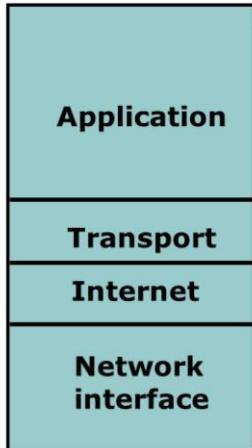
● TCP/IP 프로토콜의 계층구조

- 4 계층으로 구성
- 응용프로세스 계층(application process layer) : 응용 프로세스 간의 정보교환을 담당한다. TCP/IP는 표현계층과 세션계층을 응용계층에서 같이 처리한다.
- 전달계층 (transport layer) : 호스트간의 메시지 단위의 정보교환 및 관리, 프로토콜로는 TCP와 UDP가 있다.
- IP 계층(internet protocol layer) : 통신관련 프로세서간의 네트워크를 통한 패킷 교환

- 네트워크 접속 계층 : 단위 네트워크 내에서의 패킷 및 신호 전송을 담당한다. OSI 물리계층과 본
데이터링크계층을 하나로 취급한다.

3.1 TCP/IP의 이해

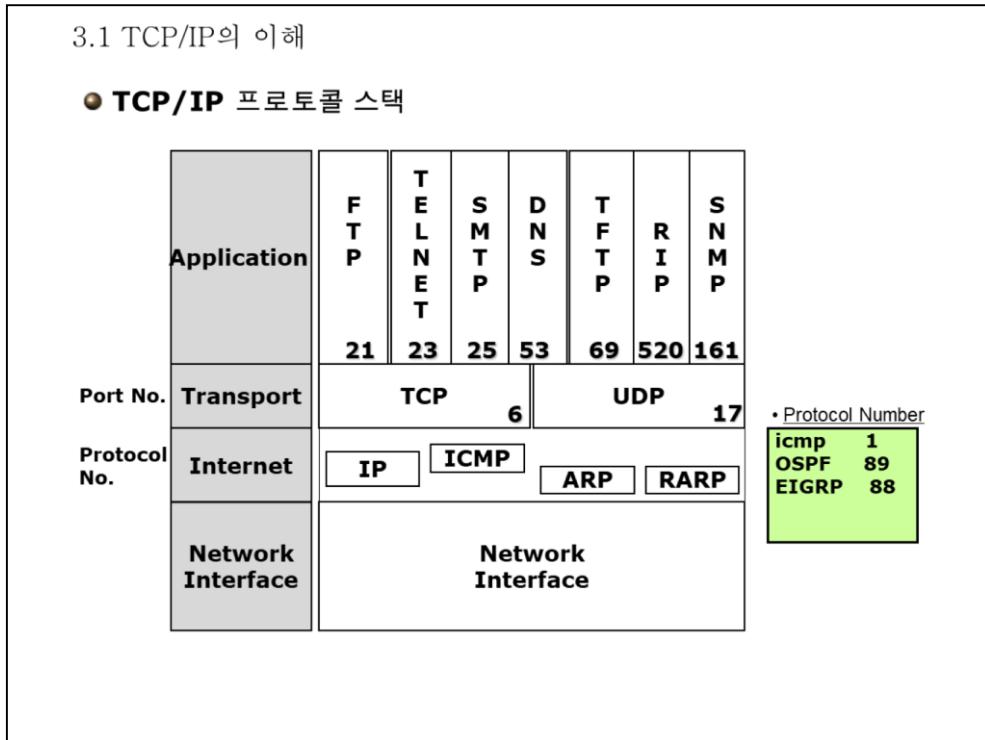
● 응용 계층



- **File Transfer**
 - TFTP/FTP/NFS
- **E-Mail**
 - SMTP
- **Remote Login**
 - Telnet/rlogin
- **Network Management**
 - SNMP
- **Name Management**
 - DNS
- **HTTP**

● TCP/IP의 응용 프로그램은 다음과 같다.

- TFTP(Trivial File Transfer Protocol): UDP를 사용하는 비연결형 파일전송프로토콜로서, 주로 라우터나 스위치등 네트워크 장비의 IOS 이미지를 Upload, Download 할 때 사용된다.
- FTP(File Transfer Protocol): TCP를 사용해서 신뢰성 있고, 연결지향적인 방식으로 파일을 전송하고 수신하는 프로토콜이다.
- Telnet: 원격지에 있는 장비로 표준 터미널 애플레이션 기능을 제공한다. 네트워크 장비에서는 텔넷을 통해 원격지에서 장비(라우터, 스위치)를 설정하도록 한다.
- SMTP(Simple Mail Transfer Protocol): 컴퓨터 네트워크를 통해 전자 메일을 전달하는 프로토콜이다.
- SNMP(Simple Network Management Protocol): 네트워크 장비를 모니터링하고 제어하기 위해 사용하는 프로토콜로 네트워크 장애관리, 장비설정, 통계, 성능 및 보안등을 관리한다.
- DNS(Domain Name Service): 도메인 이름을 논리적인 숫자주소인 IP address로 변환해 주는 일을 담당한다.
- HTTP(Hypertext Transfer Protocol): 웹을 지원하기 위한 프로토콜이다. HTTP는 GET, PUT 같은 프로토콜 기능을 포함해서, 웹서버에게 어떠한 컨텐츠를 요청하고 또는 웹서버로 정보를 보내는 역할을 한다.



- TCP/IP 프로토콜의 전송 계층이 담당하는 일은 사용자의 데이터(전송계층으로 내려온 데이터)를 적절히 분할해서(segment) 보내고, 수신할 때는 다시 조립함으로써 (reassembly) 효과적인 전송이 이루어지도록 한다.
- TCP/IP 프로토콜의 전송계층은 TCP와 UDP 두 가지로 나뉘어 진다. TCP와 UDP 프로토콜은 응용 계층과의 통신을 위해 포트의 개념을 사용한다.
- 하나의 시스템에서 여러 개의 포트를 사용하여, 다양한 응용서비스를 동시에 이용 할 수 있으며, 포트는 2byte 크기로서 1~65535 값을 갖는다.
- 포트번호는 RFC1700에 잘 알려진 포트번호(well-known port number, 1~1023번)가 정의되어 있다. 응용프로그램 개발자가 별도로 사용하려면, RFC1700에 정의되어 있지 않은 포트번호를 사용하면 된다. 255번 이하는 공적인 어플리케이션을 위해 사용하고, 255번에서 1023번 까지는 상용 어플리케이션을 개발하는 회사가 사용한다. 1024번 이상의 포트는 아무나 사용할 수 있다. Client에는 1024 이후의 랜덤한 포트번호가 부여된다.
- Windows system에는 \\Windows\\System32\\Drivers\\etc\\Service 파일에 포트번호가 정의되어 있다.

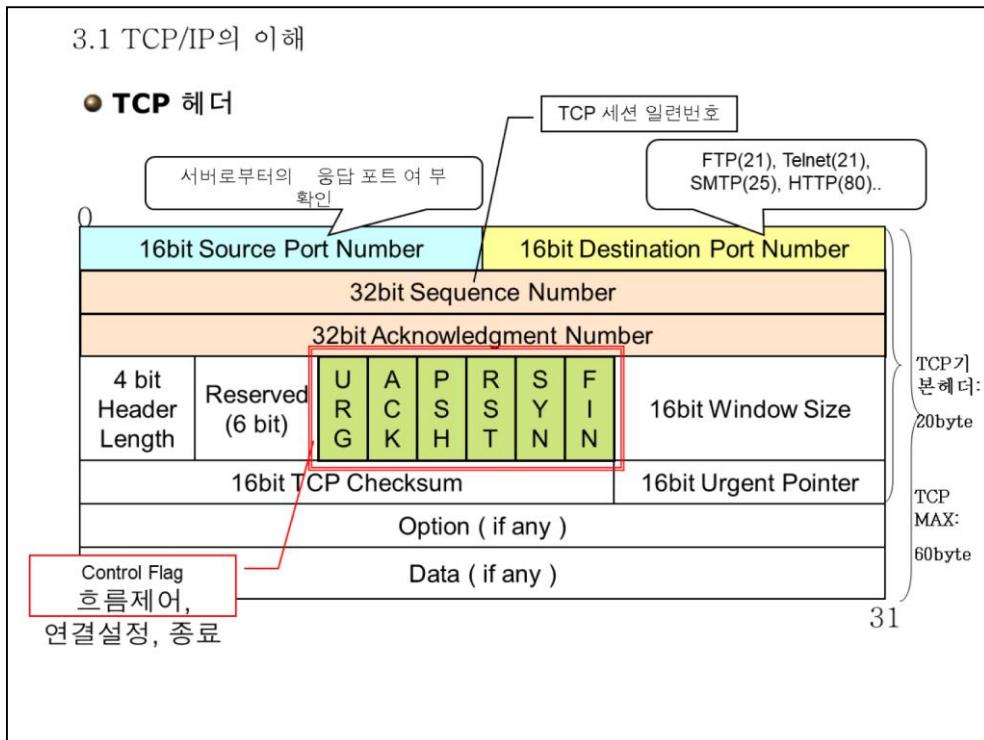
3.1 TCP/IP의 이해

● **TCP 특징**

- 연결 지향 프로토콜
- 예러 검출
- 순서검사(Sequencing)
- 응답(Acknowledgment)
- 흐름 제어(Flow Control)
- 패킷 복구(Packet Recovery)
- Full Duplex 가상회선

● TCP(Transmission Control Protocol)

- 연결지향(connection-oriented)의 신뢰성 있는 프로토콜이다.
- 윈도우를 이용한 흐름제어(flow control)와 순서번호(Sequencing)와 송인번호(Acknowledgment)를 이용한 예러제어를 하게 된다.
- TCP는 ACK를 받지 못한 모든 데이터를 다시 보내게 된다.
- TCP의 장점은 세그먼트의 전달이 보장된다는 것이며, 단점은 연결을 위한 초기 설정 시간이 걸린다는 점이다.
- TCP Segment의 의미: Application의 메시지를 순차적으로 분할하고, 분할된 Data가 전후 상관 관계가 고려되어 있다는 의미에서 Segment라는 용어를 사용하였다.
- TCP는 Full Duplex의 가상회선을 제공하므로 전송회선과 수신회선이 분리되어 있다고 할 수 있다.

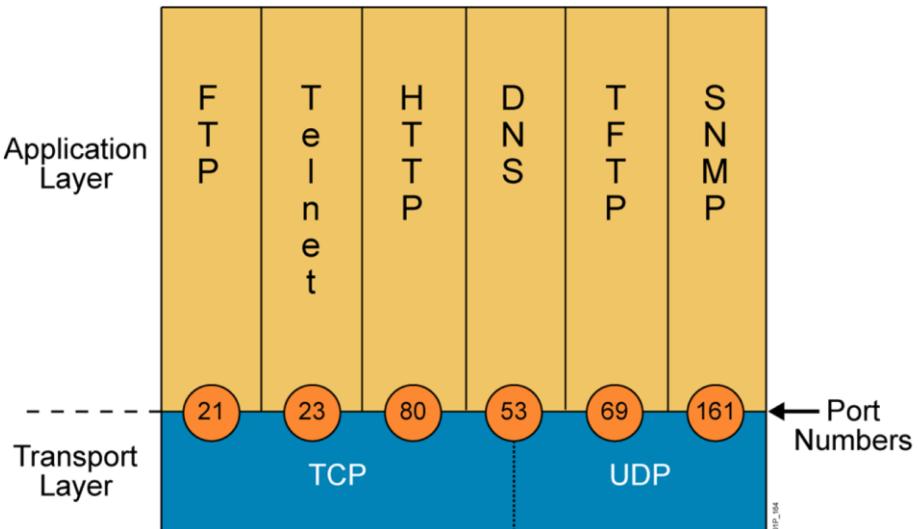


- Source Port : 출발지 Port 번호
- Destination Port : 목적지 Port 번호
- Sequence Number : 데이터가 잘 전송되는지를 보장하기 위해 들어가는 필드로, 전송되는 세그먼트의 순서번호이다.
- Acknowledgment : 통신상대가 발송한 패킷을 받았다는 것을 상대에게 확인해 주는 Number로써 수신한 마지막 Byte 순서번호 + 1을 설정
- Header Length : TCP 헤더의 크기를 나타내는 것으로 32비트(4바이트) 단위이다.
- Reserved : 향후 사용을 위해서 할당된 필드, 현재는 사용하지 않는 필드로 “0”으로 설정되어 있다.
- TCP Header Flag
 - URG : Urgent Pointer가 유효함을 표시
 - ACK : Acknowledgment Number가 유효함을 표시
 - PSH : 수신자는 패킷데이터를 최대한 빨리 응용프로그램에서 전달할 것을 지시
 - RST : 연결을 Reset하도록 지시
 - SYN : 연결의 시작을 나타내기 위해 사용
 - FIN : 연결을 종료하도록 지시
- Window Size : TCP의 호름제어를 위해 양단간의 통신 당사자들은 자신들이 현재 수신할 수 있는 Buffer량을 상대방에게 알려줌. 즉 상대편 장비에게 얼마만큼의 데이터를 보내도 되는지를 알려주는 필드이다.
- TCP Checksum : TCP Header와 Data 필드에 대한 계산된 체크섬으로 에러 여부를 체크한다.
- Urgent Pointer : URG Flag가 On되어 있을 경우에만 유효(전송 Data중 긴급한 Data의

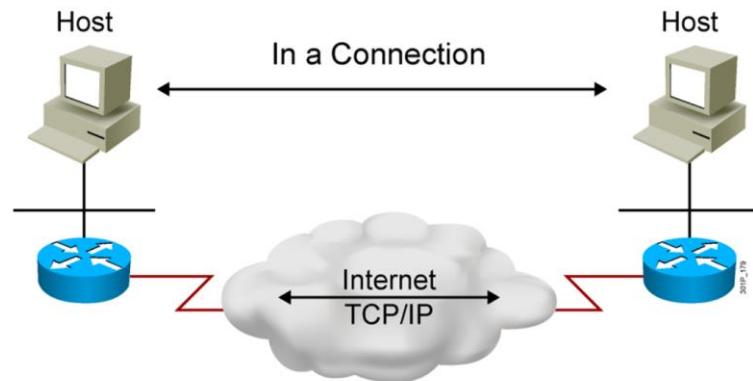
위치 지정)

- Option : 현재 정의되어 있는 옵션으로 최대 TCP 세그먼트 사이즈가 있다.
- 데이터(Data) – TCP 윗단에서 내려온 데이터

3.1 Mapping Layer 4 to Applications

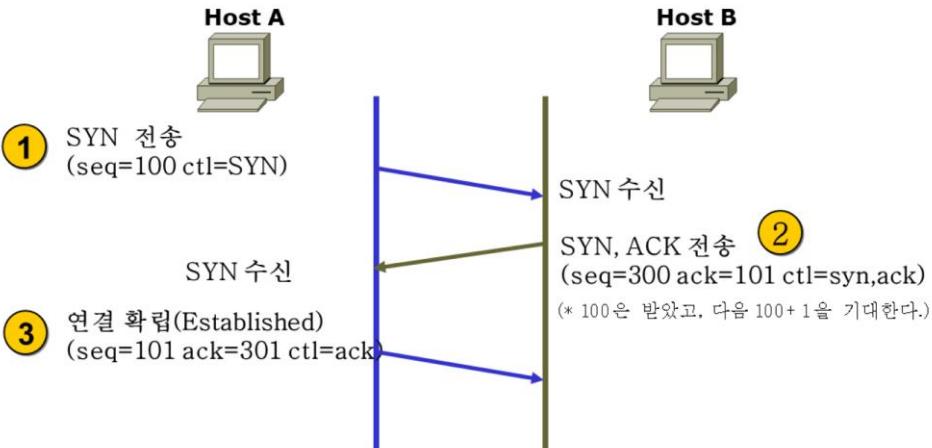


3.1 Establishing a Connection



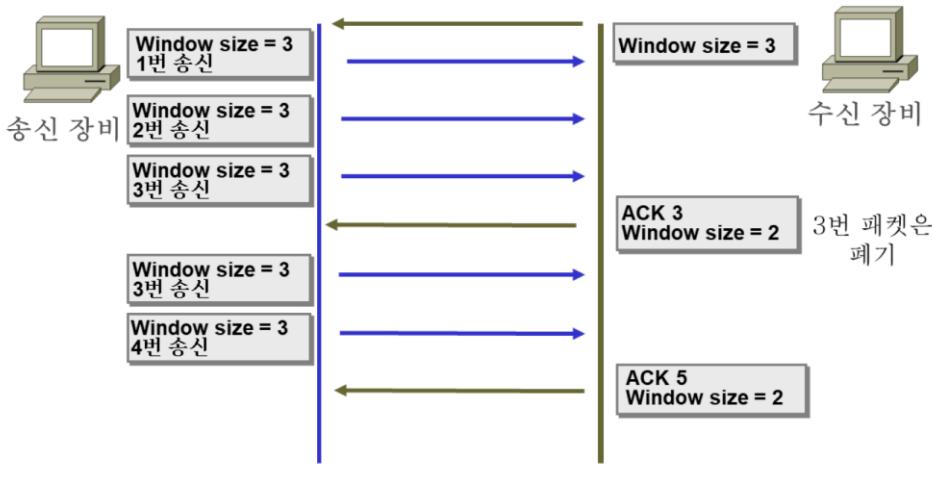
3.1 TCP/IP의 이해

● Three-Way Handshake



- TCP는 가상회선(virtual circuit)을 설정하여 데이터를 전송하고, 전송이 완료된 후에는 회선을 해지하는 절차를 이용한다.
- 가상회선 설정시 통신을 하고자 하는 상대방이 회선설정이 가능한지 확인하는 절차를 3-way Handshake라 한다.
- 3-way Handshake는 syn → ack+ syn → ack 의 다음과 같은 3단계 과정을 거친다.
- Host A에서 B로 임의로 설정한 SYN(순서번호는 100이다)를 보낸다.
- B에서 A로 ACK(100은 받았고, 다음 100+1을 기대한다)을 보낸다. 또한 B에서 A로 SYN(순서번호는 300이다)를 보낸다.
- A에서 B로 ACK(300은 받았고, 300+1을 기대한다)를 보낸다.
- 순서번호(Sequence number)는 보안을 위해 0부터 시작하지 않고 임의의 번호부터 시작된다.

3.1 TCP/IP의 이해

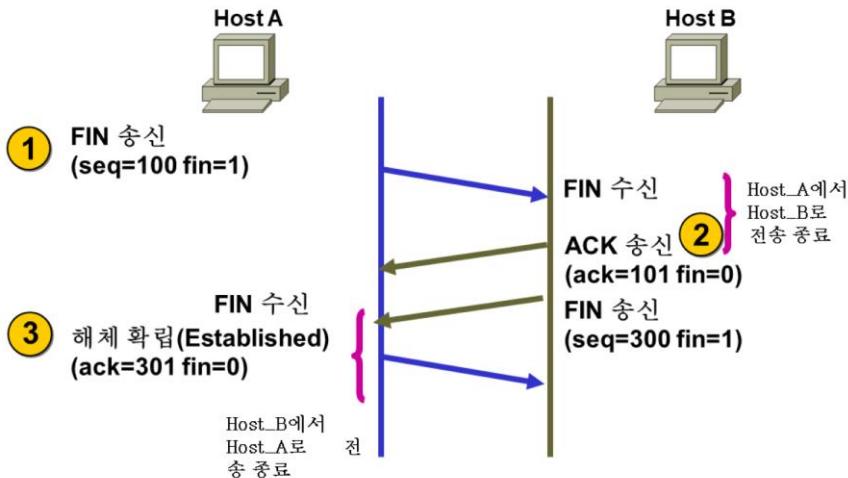
● **TCP Windowing**

Windows Size가 커지면, 훨씬 유연한 통신이 된다.

- 두 시스템간에 데이터가 제대로 전송되기 위해서는 갑작스런 폭주로 인해 반대편 수신측에서 처리할 수 없는 상태에 이르지 않도록 해야 한다.
- 따라서 받는 측에서 내가 얼마나 받을 수 있는지를 계속 알려 주어야 한다. TCP에서는 ACK를 보낼 때 윈도우 사이즈로 받을 수 있는 크기를 알려주고 있으며, 바이트(Bytes)수 단위이다.

3.1 TCP/IP의 이해

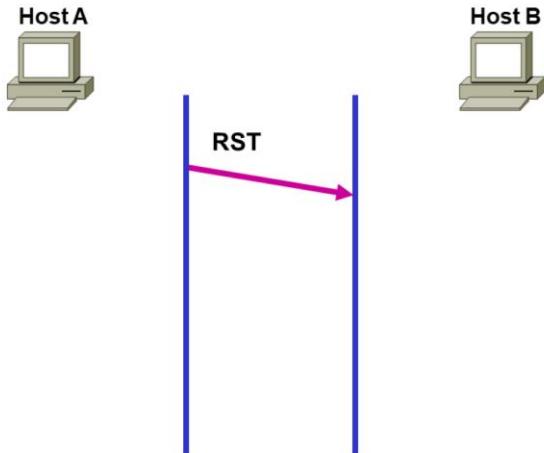
● 연결 해체 단계(정상종료)



- TCP는 데이터 전송이 완료된 후에는 회선을 해지하는 절차를 이용한다.
- TCP는 Full Duplex의 가성회선을 제공하므로 전송회선과 수신회선이 분리되어 있다고 할 수 있으며, 각각의 회선이 FIN요청에 의해 별도 해지 될수있다.
- Host A는 전송 할 데이터를 모두 전송 하였으면 HostB로 FIN segment를 전송한다.(회선해지요청)
- HostB는 FIN segment를 수신하면 ACK(seq+1)로 회선 해지 요청을 수신했음을 알린다. 이렇게 되면 HostA에서 HostB로 전송은 종료되었음을 의미한다. .(회선해지응답)
- 아직 HostB에서 HostA로의 통신은 가능한 상태이다. 이와 같이 절반 방향만 종료된 상태를 Half Close라 한다.
- HostB에서 필요한 데이터 전송을 완료한 후 회선을 종료해도 되면 회선 해지 요청(FIN)을 보낸다.(회선해지요청)
- HostA가 ACK를 HostB로 전송하면 가상회선 연결이 종료된다. (확인응답)

3.1 TCP/IP의 이해

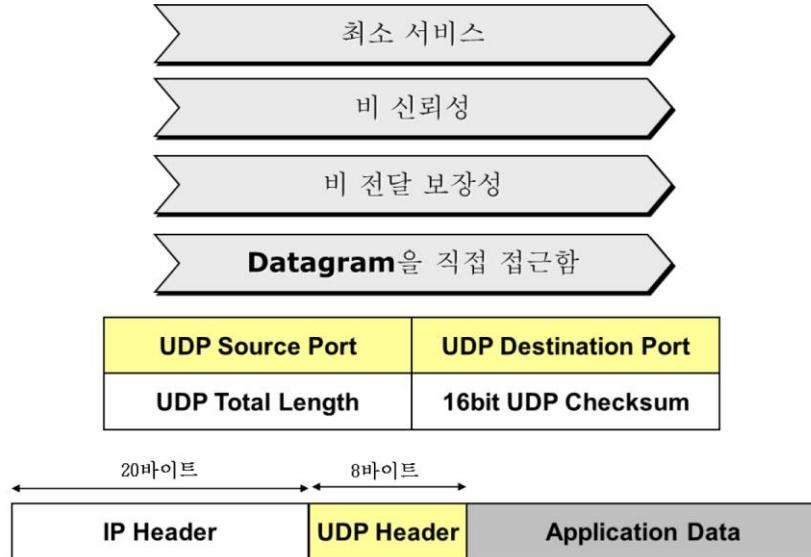
● 연결 해체 단계



- TCP 회선 해지는 FIN요청에 의한 정상 종료와 RST 메시지에 의한 비정상적인 중단해제가 있다.
- FIN는 큐에 대기하고 있는 데이터를 모두 전송한 후에 종료하므로 데이터의 손실이 없다.
- HostA 나 HostB 중 오류나 긴급한 문제로 TCP Session을 종료해야 할 경우 Reset segment를 생성하여 상대편에 전송하면 회선종료 절차를 준수하지 않고 즉시 회선을 해지한다.
- Reset이 발생하는 경우는 존재하지 않는 포트에 대한 연결을 요구, 연결요구가 도착할 때에 목적지 포트상에 프로세스가 대기하고 있지 않는 경우 등이다.

3.1 TCP/IP의 이해

- **UDP 특징 및 헤더**



- UDP는 비연결성 서비스로 데이터 전달의 보장이 안 되는 비신뢰성 프로토콜이지만, 어플리케이션 프로토콜에 오버헤드가 적고 간단하게 구현될 수 있는 전송서비스를 제공한다.
- UDP는 일반적으로 브로드캐스트, 멀티캐스트를 집중적으로 이용하는 어플리케이션 또는 탐색과 질의에 빠른 응답을 요구하는 어플리케이션에 사용된다.
- UDP의 전송 단위를 Datagram이라 하며, 데이터 크기가 간단하여 전송 단위 (datagram) 별로 전송하는 것을 의미한다.

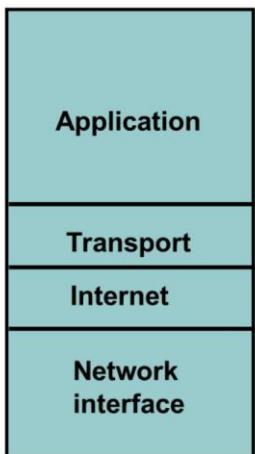
3.1 TCP/IP의 이해

▣ TCP와 UDP 비교

TCP	UDP
Connection oriented	Connectionless
Sequencing 지원	Sequencing 지원하지 않음
Error control을 한다	Error control 하지 않음
Flow control을 한다	Flow control 하지 않음
Unicast 전송	Unicast, Multicast, Broadcast 전송
Full duplex	Half duplex
데이터 전송	실시간 Traffic 전송 (VoIP, Multimedia 등)

- TCP와 UDP는 가장 근본적으로 Connection-Oriented된 프로토콜인가 Connectionless 프로토콜인가의 차이를 지닌다.
- TCP는 두 사용자 시스템간의 통신에서 에러 제어, 흐름 제어, 데이터 순서 보장, 데이터 손실 및 중복 해결을 수행하지만 UDP는 두 사용자 시스템간의 통신에서 단순한 전송을 수행할 뿐 데이터 순서도 보장하지 못하며 데이터 손실 및 중복을 해결하지 못한다.
- UDP의 경우, 오늘날 Network Infrastructure가 발전하면서 등장한 새로운 Service인 VoIP와 Video Streaming Service에 적합하다.

3.1 TCP/IP의 이해

● **Internet** 계층

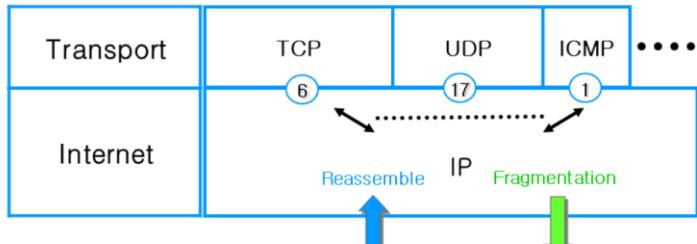
- **Internet Protocol (IP)**
- **Internet Control Message Protocol (ICMP)**
- **Address Resolution Protocol (ARP)**
- **Reverse Address Resolution Protocol (RARP)**

- 인터넷 계층에서 하는 주된 일은 네트워크가 물리적으로 어떻게 만들어지든 간에 발신자 네트워크에서 목적지 네트워크로 데이터를 전송한다.
- 인터넷 계층의 프로토콜은 IP(Internet Protocol), ICMP(Internet Control Message Protocol), ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol), DHCP(Dynamic Host Configuration Protocol) 등이 있다.

3.1 TCP/IP의 이해

▣ IP 특징

- IP : Internet Protocol



- 논리적 주소인 IP Address 사용
- IP Address를 이용 경로 관리
- 최적의 경로 선택
- Packet 전송
- Best-Effort Delivery
 - 신뢰성 보장 못 함

- IP는 IP Address 기반으로 Network이나 Host를 인지하며 목적지 주소지로 Packet 전송을 담당하고 있다.
- 목적지 주소가 없는 경우에는 무조건 해당 Packet을 Discard 한다.
- IP는 TCP나 UDP와 같이 상위 Layer의 Protocol로부터 Data를 받아서 Packet 단위로 전송 한다.
- Layer2로 보낼 때는 커다란 Packet을 작은 단위의 Frame으로 분할(Fragmentation)하여 전송하며, Frame의 크기는 Layer2 Protocol의 종류에 따라 다르다.
- 반대로 Layer2로부터 받은 Frame을 재조립(Reassemble)하여 Layer 4로 보내 준다. 이때 Layer4의 어떤 Protocol에게 보낼 것인지를 구분하기 위해 Protocol ID가 사용된다.

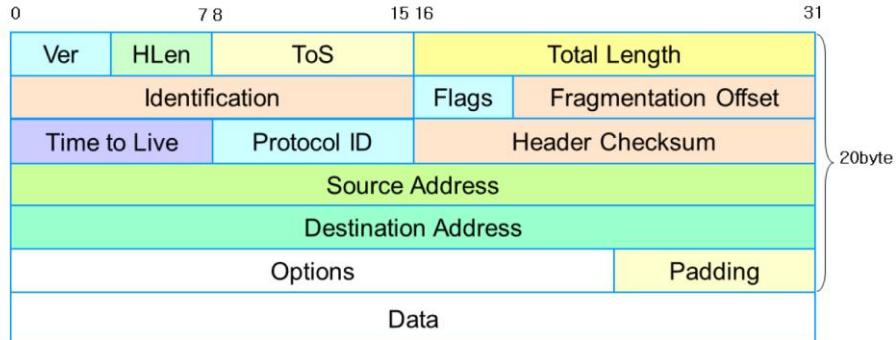
참조 사이트 <http://www.iana.org/assignments/protocol-numbers>

● IP 데이터그램의 처리

- 한 메시지가 여러 개의 패킷으로 나뉘어졌기 때문에, 각 패킷은 필요한 경우 서로 다른 경로를 통해 보내어질 수도 있으며, 패킷들은 원래 보낸 순서와는 다른 순서로 도착될 수도 있음
- IP는 단지 패킷 배달만 할 뿐이며, 순서가 흐트러진 패킷들을 올바르게 재정렬하는 것은 상위 프로토콜인 TCP가 처리함

3.1 TCP/IP의 이해

▣ IP Header



- VER (Version) : IP protocol version (IPv4, IPv6)
- HLEN (Header Length) : 32비트 단위의 헤더길이를 표시한다. 데이터그램의 헤더는 60 바이트까지 가능하다. 대부분의 IP 헤더의 길이는 20바이트이며, 이 필드의 값은 거의 항상 5다. ($5 \times 32 = 160$ 비트, 또는 20바이트)
- Service Type : 우선순위(3bit)와 서비스유형(4bit)의 서브필드로 구성되며, 현재 버전-Version 4에서는 보통 우선순위는 사용되지 않는다. QoS (Quality of Service)에서 사용
- TOTAL LENGTH : IP Header와 데이터 길이의 합계이며 16bit로 표현되므로 IP Packet의 최대길이는 65,536 바이트까지 가능하다.
- Fragmentation Identifier : 데이터그램의 식별자이다.
- Fragmentation Flags : Fragment된 패킷인지, Fragment된 경우 마지막 Fragment 인지를 표시한다.
- Fragment Offset : Fragment된 패킷인 경우, 원래 패킷에서의 위치를 표시한다.
- TIME TO LIVE (TTL) : 데이터그램의 수명을 나타낸다. 라우터를 경유 시 1씩 감소한다.
- PROTOCOL Identifier : IP가 전송하는 프로토콜을 명시한다.(TCP=6, UDP=17, ICMP=1)
- Header Checksum : IP Header의 체크섬 값을 저장한다. 경유지 및 도착지에서 헤더의 체크섬을 재계산하여 일치하지 않으면 데이터그램을 폐기한다.
- SOURCE IP ADDRESS : 보내는 노드의 32-bit IP address
- DESTINATION ADDRESS : 받는 노드의 32-bit IP address
- IP OPTIONS : 특별한 IP 추가 Option을 설정할 수 있으나, 대부분의 경우 사용하지 않는다. 최대 40Byte까지 가능하므로 IP Header의 크기는 최대 60Byte에 이를 수 있다.
- PADDING : Option이 추가되는 경우, IP Header가 32bit 단위로 끝날 수 있도록 채우는 부분이다.
- IPv4의 기본 헤더는 20Byte이며, 12개의 필드로 구성되어 있다.

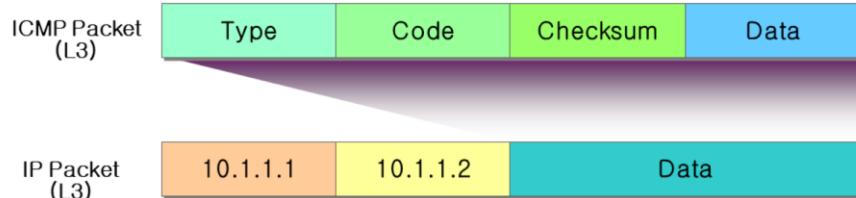
3.1 TCP/IP의 이해

▣ ICMP

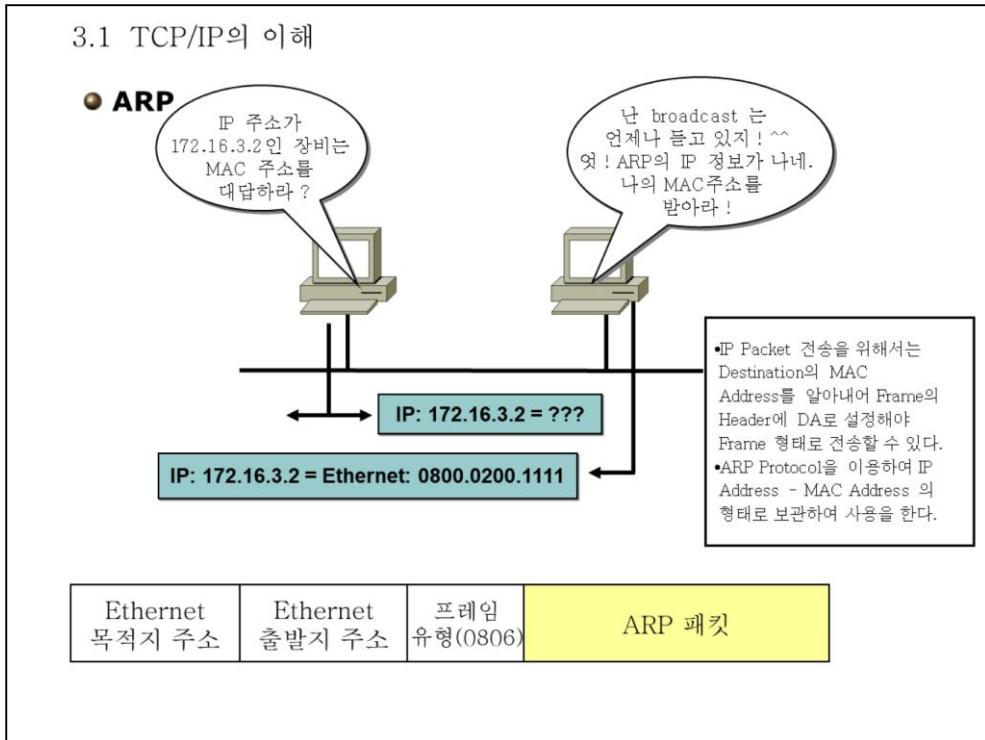
- ICMP : Internet Control Message Protocol
- 오류 보고 (Error 발생 시 처리에 관한 IP의 단점 보완)

▣ ICMP Service

- Echo Request and Reply (Ping Command)
- Destination Unreachable
- ICMP Redirect
- Time Exceed



- IP 계층의 일부이며, ICMP Message는 IP Packet으로 만들어진 다음 전달된다.
- IP Datagram을 전달하는데 발생하는 에러 혹은 특별한 상황에 대한 정보를 주고 받는다.
- 에러 메시지와 정보관련 메시지로 구성되어 있다.
- 정보 관련 메시지
 - Echo Request/Reply
 - echo request 메시지는 특정 호스트의 ICMP 프로세서에 보내진다.
 - 그리고 ICMP 프로세서는 반드시 echo reply 메시지로 응답해야 한다.
- 에러 메시지
 - Destination Unreachable
 - 라우터가 최종 목적지로 데이터그램을 전달할 수 없을 때
 - network unreachable, host unreachable, port unreachable
 - Redirect
 - 데이터그램이 잘못된 라우터로 전달되었을 때 해당 라우터는 데이터그램을 잘못 보낸 호스트에게 올바른 경로 정보를 전달해 준다. 이후 호스트는 라우팅 테이블을 갱신하고 정상적인 경로로 데이터그램을 전송한다.
 - Time Exceeded
 - 데이터그램의 Time To Live(TTL) 값이 0이 되었을 때, 해당 데이터그램의 송신자에게 보내는 메시지
 - traceroute는 icmp time-exceeded 메시지를 이용한다.



● ARP (Address Resolution Protocol)

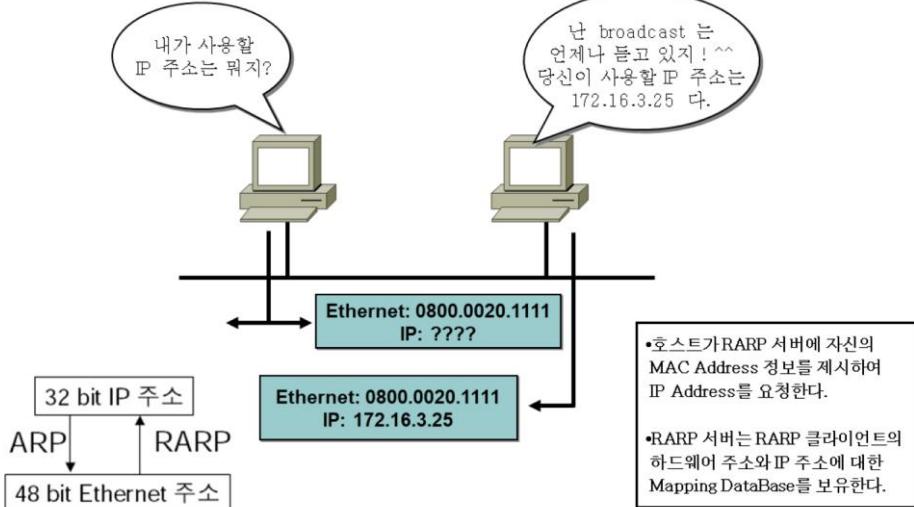
- IP 주소로부터 해당하는 하드웨어 주소를 찾는다
- ARP 프로토콜의 동작은 같은 서브넷 내에서만 유효하다.
- 이더넷 프레임에 실려서(캡슐화되어) 전달된다.
- ARP는 두 가지 메시지 ARP Request, ARP Reply를 사용한다.

● ARP Cache

- 호스트는 ARP Cache 테이블에 Address Binding 정보를 저장한다.
- 테이블은 “하드웨어주소-IP주소”쌍으로 구성된다.
- 목적지의 하드웨어 주소가 필요할 경우에 먼저 ARP Cache를 찾아보고 없으면 ARP request를 이용하여 목적지 하드웨어주소를 알아낸다.
- Cache 정보는 참조될 때마다 Refresh되며, 일정 시간 동안 참조되지 않는 정보는 자동 소멸된다.

3.1 TCP/IP의 이해

● RARP



● RARP(Reverse Address Resolution Protocol)

- 하드웨어 주소를 가지고 자신의 IP Address를 얻는 방법
- RARP request, RARP reply

● RARP는 DHCP로 설정된 호스트(DHCP Client)가 부팅과 함께 IP Address를 얻을 때 사용된다.

2장 IPv4 주소체계

3.2 IPv4 주소체계

	Example			
A IP address is a 32-bit binary number	10101100000100001000000000010001			
For readability, the 32-bit binary number can be divided into four 8-bit octets	10101100	00010000	10000000	00010001
Each octet (or byte) can be converted to decimal	172	16	128	17
The address can be written in dotted decimal notation	172.	16.	128.	17

- IP 주소는 32 bit 로 이루어진다
- 32 bit는 4개의 octet로 나누어 표현 된다
- 각 octet(1 byte)는 십진수로 표현된다
- 각 십진수는 점을 통해 구분되어 진다(Dotted-decimal notation)

● IP 주소 관리 조직

- IANA(Internet Assigned Numbers Authority) : IP 주소, AS#, 최상위 도메인등을 관리하는 단체이다
- NIDA : 인터넷 진흥원으로 국내의 IP주소와 도메인 이름 할당한다.

● 숫자와 점을 이용한 표현 (Dotted-decimal notation)

- IP 주소는 32 bit 로 이루어진다 : 10101100000100001000000000010001
- 32 bit는 4개의 octet로 나누어 표현 된다 : 10101100 00010000 10000000 00010001
- 각 octet(1 byte)는 십진수로 표현된다 : 172 16 128 17
- 각 십진수는 점을 통해 구분되어 진다(Dotted-decimal notation) : 172.16.128.17

3.2 IPv4 주소체계

A B C ... Easy as 1 2 3

Class A ... First 1 bit fixed  Host . Host . Host

Class B ... First 2 bits fixed  Network . Host . Host

Class C ... First 3 bits fixed  Network . Network . Host

- 첫 번째 octet을 기준으로 Class 가 구분된다.

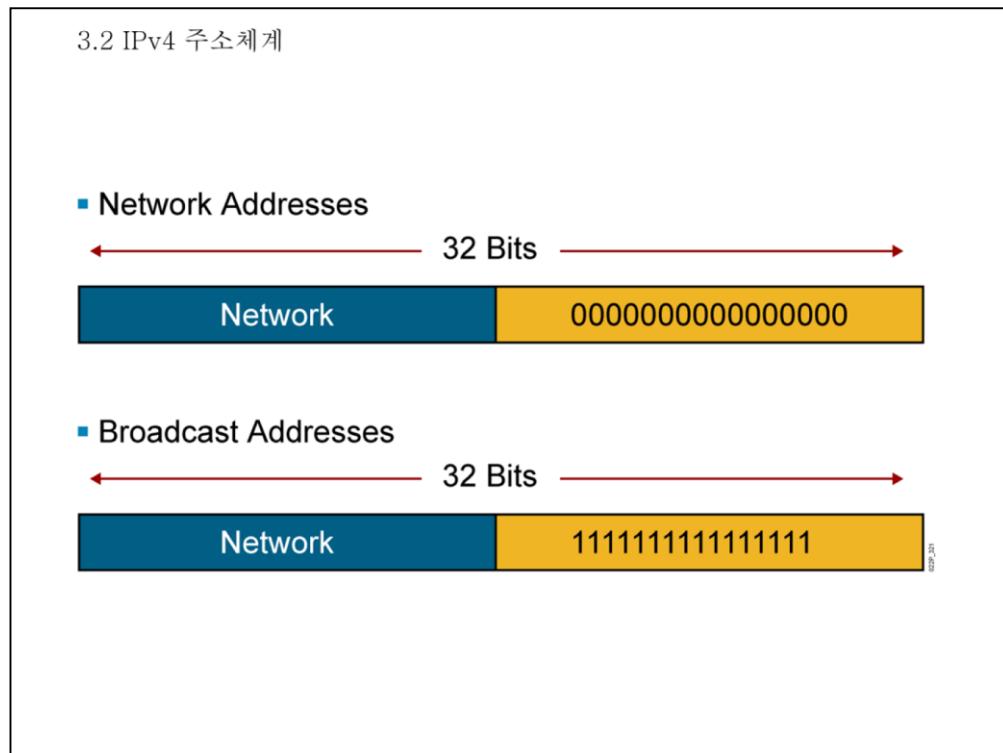
● IP 주소 Class 구분

- 호스트수면에서 다양한 규모의 네트워크를 지원하기 IP address space를 Class A, B, C 세 개의 클래스로 나눔
 - Class D는 multicast groups을 위해 사용되며, 이때 Network과 Host 주소로 구분되지 않는다.
 - Class E 영역은 오직 연구용으로만 예약되어 있다.
- A Class는 N.H.H.H로 default subnet mask는 255.0.0.0이다. (N=Network, H=Host)
- A Class 주소 중 127 (01111111)은 Loopback 테스트(local host)를 위해 예약되어 있기 때문에 네트워크 주소로는 할당되지 못한다.
- B Class는 N.N.H.H로 default subnet mask는 255.255.0.0
- C Class는 N.N.N.H로 default subnet mask는 255.255.255.0

3.2 IPv4 주소체계

IP Address Class	First Octet Binary Value	First Octet Decimal Value	Possible Number of Hosts
Class A	1-126	<u>0</u> 0000001 to <u>0</u> 1111110*	16,777,214
Class B	128-191	<u>1</u> 0000000 to <u>1</u> 0111111	65,534
Class C	192-223	<u>11</u> 000000 to <u>11</u> 011111	254

*A class의 127 (01111111) 네트워크는 loopback test를 목적으로 예약되어 있다.



- 다음과 같은 2가지 경우는 예약되어 있는 주소로 어떤 경우라도 호스트에게 할당되어질 수 없다.

- 호스트 부분으로 사용되어지는 bit가 모두 다 0으로 표시되어 지는 경우 Network을 대표하는 번호로 예약되어 있기 때문에 일반 호스트에게 할당할 수 없다.

- 호스트 부분으로 사용되어지는 bit가 모두 다 1으로 표시되어 지는 경우 해당 Network의 모든 호스트를 나타내는 broadcast 주소로 예약되어 있기 때문에 일반 호스트에게 할당할 수 없다.

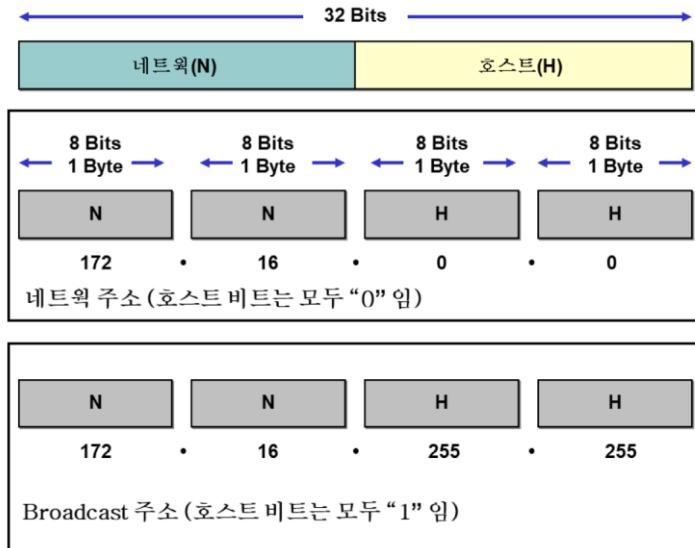
3.2 IPv4 주소체계

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

- 다음과 같이 사설 IP로 예약되어 있는 주소들은 공인망(인터넷망)에서 사용할 수 없다.
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
- 일반적으로 IPV4 Address의 고갈 및 보안에 대한 고려를 이유로 내부망에는 비공인(private) 주소를 사용한다.
- 사설 IP의 사용은 공인 IP Address 확보의 어려움을 해결할 수 있으며, 외부의 공인 주소 영역과 직접 통신이 이루어 질 수 없다는 측면에서 내부망을 보호하는 보안 문제에 대응할 수 있고, 내부 네트워크 구성 및 관리의 유연성을 확보할 수 있다.
- IETF RFC 1918에서 권고하는 사설 주소로 사용할 수 있는 영역이 정의되어 있다.
- 내부망에 있는 사용자는 NAT(Network Address Translation)기능을 이용하여 공인 Address로 변환 후 인터넷에 접속할 수 있다.

3.2 IPv4 주소체계

● 기본 네트워크/Broadcast 주소



● 각 클래스별 Default Subnet Mask

- 기본적으로 각 클래스별로 A Class는 처음 1Byte, B Class는 2Byte, C Class는 3Byte까지가 네트워크 영역이 됨
- Default Subnet Mask를 사용시 라우터는 Subnet Mask 부분이 2진수로 1인 부분까지를 네트워크로 인식함
- A Class는 N.H.H.H로 default subnet mask는 255.0.0.0
- B Class는 N.N.H.H로 default subnet mask는 255.255.0.0
- C Class는 N.N.N.H로 default subnet mask는 255.255.255.0

- 각 클래스에서 호스트 주소에는 모든 bit를 0 또는 1로 설정할 수 없다.
- 이것은 각 Bits가 all-0's이면 this network을 의미하고, all-1's이면 broadcast address를 의미하기 때문이며, 고로 각 클래스 별로 host에 할당할 수 없는 Address가 2개씩 존재하게 된다.
 - 예를 들어 B-class 네트워크에서 172.16.0.0은 호스트 비트가 모두 '0'으로 네트워크 주소이며, 172.16.255.255는 호스트 비트가 모두 '1'로 브로드캐스트 주소이다. 이 두 주소는 host 주소로 사용할 수 없다.

3.2 IPv4 주소체계

● 서브넷 마스크의 Octet 값

128	64	32	16	8	4	2	1	=	
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

- IP 주소에서는 2진수 값과 같은 십진수 값이 사용된다.
- 예 : 11111111 = 255

- 서브넷 개념은 라우팅을 위해서는 필수적이고 라우터에 대한 환경 설정을 조작하거나 주소가 어떻게 나누어져 있는지를 알기 위해서 필요함



○ Address(주소)

- 네트워크에 있는 호스트의 인터페이스에 할당되는 유일한 식별값
- 호스트가 여러 개의 인터페이스를 가진다면 그 각각은 유일한 주소를 가져야 함

○ Subnet(서브넷)

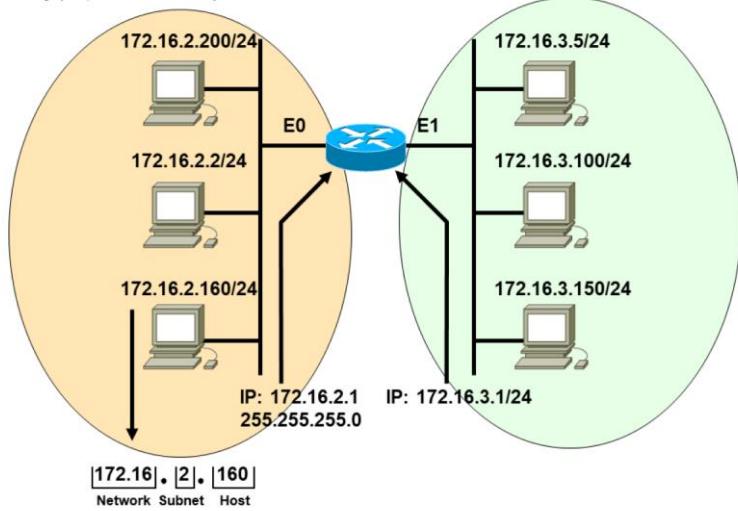
- 원래 호스트를 위해 남겨진 부분 중 네트워크으로 사용하기 위해 나누어진 네트워크의 연장부분

○ Subnet Mask(서브넷마스크)

- 주소에 관계된 서브넷 부분과 호스트 부분에 대한 32bit 조합이며 이를 통해 Subnet 부분의 네트워크 부분을 알 수 있음

3.2 IPv4 주소체계

- 서브넷 주소의 계획

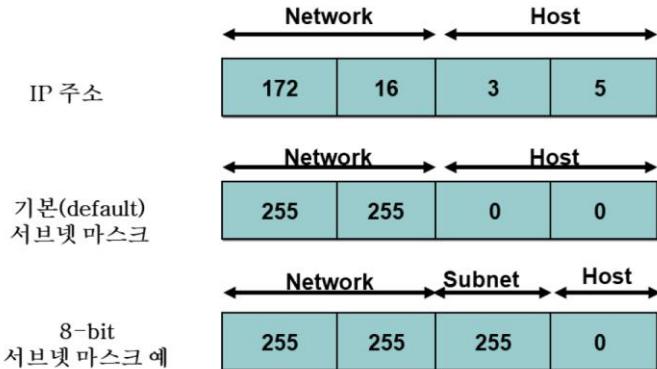


- IP: 172.16.2.1 255.255.255.0 = 172.16.2.1/24(prefix 표기)와 동일 의미
- 서브넷은 라우터의 인터페이스 기준으로 분리된 네트워크로 구성한다.

- 서브넷은 라우터의 인터페이스 기준으로 분리된 네트워크로 구성한다.
- Layer3 스위치에서는 vlan마다 분리된 네트워크로 구성한다.
- IP 주소: 172.16.2.1 subnetmask: 255.255.255.0과 동일한 의미의 prefix 표기로 172.16.2.1/24(네트워크의 bit수)로 표기한다.

3.2 IPv4 주소체계

● B class subnetting

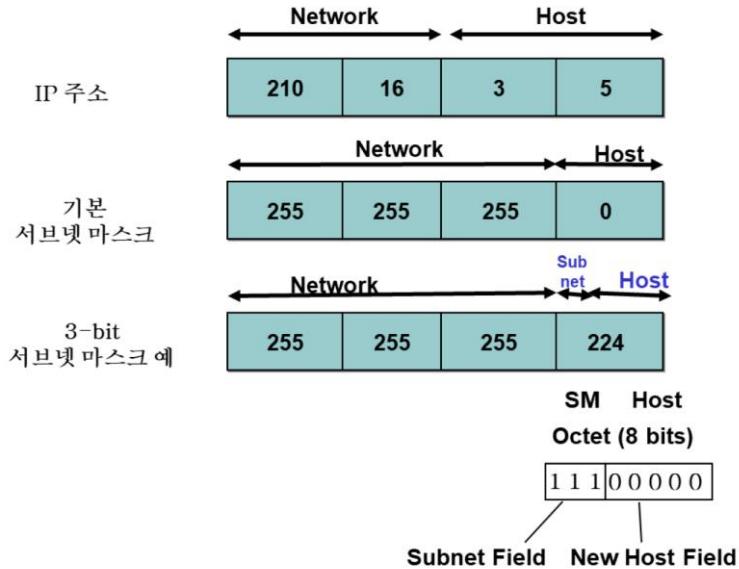


- 서브넷 마스크를 위한 비트의 확장 시 호스트 비트는 높은 순서 비트 (high-order bit)부터 시작된다.

- B Class Address 172.16.3.5와 172.16.4.5를 Default Subnet Mask 적용 시에는 동일한 172.16 네트워크이지만 8-Bit Subnet Mask를 적용하면 172.16.3.0 네트워크와 172.16.4.0 네트워크로 다른 네트워크가 된다.
- Subnet Mask의 십진수를 이진수로 바꿨을 때 Bit의 값이 2진수로 1인 Bit 영역이 네트워크 Address 영역이 되며 나머지 부분이 Host Address 영역이 된다.
- Default Subnet Mask 적용 시 172.16.0.0 네트워크 Address이며 3.5는 Host Address가 된다.
- 8-Bit Subnet Mask(255.255.255.0) 적용 시 172.16.3.0 네트워크 Address이며 5가 Host Address가 된다.

3.2 IPv4 주소체계

● C class subnetting



- Class C 주소 = 24 bits는 네트워크 영역, 8 bit는 호스트 영역으로 3bit 가 서브네트워크를 위해 호스트 영역으로 확장되어 있다.
- 기본 subnet mask에 3bit subnetting을 2진수로 표기하면 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 이며,
- 이를 dotted-decimal notation 표현으로 나타내면 서브넷마스크 = 255.255.255.224 이 된다.

3.2 IPv4 주소체계

● C class Host/Subnet 테이블

클래스B #bits	마스크	사용가능한 서브넷수 ($2^n - 2$)	사용가능한 호스트수 ($2^n - 2$)
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

- 서브넷과 호스트에 영역에 모든 0과 1은 제외된다.
- $2n - 2 = \text{Subnet 수}$, $2n - 2 = \text{Host 수}$
- 시스코는 ip subnet-zero 명령 지정 시 subnet 수 = 2^n , Host 수 = $2^n - 2$

- C Class Address에 대하여 8-Bit Subnet Mask 적용 시 위와 같은 서브넷과 호스트 수가 결정된다.
- 실 적용 환경의 네트워크와 호스트 요구 수량과 향후 요구 수량 등을 고려하여 적절히 선택하여 설계하여야 한다.
- C-class의 6bits 255.255.255.252(=30)는 peer-to-peer WAN 구간에 주로 사용된다.
- 252는 이진수로 11111100이며, 사용 가능한 서브넷 수는 62개($2^6 - 2 = 62$), 한 서브넷 당 사용 가능한 호스트 수는 2개($2^2 - 2 = 2$) 이는 주로 장비 연결 구간에 사용된다. => 주로 WAN 구간에 사용된다.

3.2 IPv4 주소체계

● **subnetting** 예제 1

얼마의 bit가 호스트 영역으로 확장되어야 하나?

(ip subnet-zero 설정 사용)

- 네트웍 주소: 202.168.57.0
- 필요한 서브넷 : 3 개
- 서브넷당 호스트 수: 55개

- 요구 사항을 충족하는 서브넷을 위해 2 비트가 확장된다.
- $202.168.57.0/24 \Rightarrow 202.168.57.0/26$
 - 2 서브넷 비트: $2^2 = 4$ 서브넷
 - 호스트를 위해 6비트가 사용: $2^6 - 2 = 62$ 서브넷당 호스트 수
- Class C 기본 마스크 11111111 11111111 11111111 00000000
- 수정된 서브넷 마스크 11111111 11111111 11111111 11000000
- 요구된 서브넷 마스크를 십진수와 점으로 표현 = 255.255.255.192



3.2 IPv4 주소체계

- $202.168.57.0/24 \Rightarrow 202.168.57.0/26$
- Subnet mask: 11111111 11111111 11111111 11000000 = 255.255.255.192

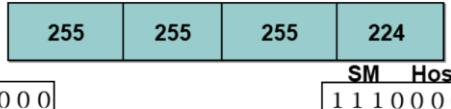
Subnets 2진표기 (2^n)	이용될 수 있는 Subnets 수 (10진표기)	서브넷당 사용가능한 호스트 범위 ($2^n - 2$)
00000000	202.168.57.0/26	202.168.57.1 – 62
01000000	202.168.57.64/26	202.168.57.65 – 126
10000000	202.168.57.128/26	202.168.57.129 – 190
11000000	202.168.57.192/26	202.168.57.193 – 254



3.2 IPv4 주소체계

210.16.3.0

3-bit
서브넷 마스크



Subnet 경
우의 수

000	0 0 0 0 0 = 0	=> 210.16.3.0 /27	서브넷 네트워크로서 사용하지 않음
001	0 0 0 0 0 = 32	=> 210.16.3.32/27	
010	0 0 0 0 0 = 64	=> 210.16.3.64/27	
011	0 0 0 0 0 = 96	=> 210.16.3.96/27	
100	0 0 0 0 0 = 128	=> 210.16.3.128/27	
101	0 0 0 0 0 = 160	=> 210.16.3.160/27	
110	0 0 0 0 0 = 192	=> 210.16.3.192/27	Subnet 브로드캐스트로서 사용하지 않음
111	0 0 0 0 0 = 224	=> 210.16.3.224/27	

210.16.3.32
서비넷의
host 수

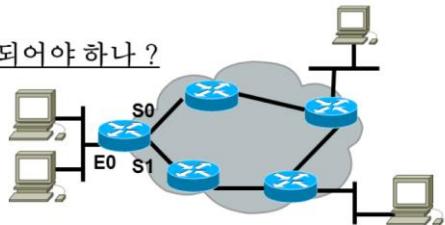
001	0 0 0 0 0 = 32	=> 210.16.3.32/27	서브넷 네트워크를 의미하므로 할당하지 않음
001	0 0 0 0 1 = 33	=> 210.16.3.33/27	
001	0 0 0 1 0 = 34	=> 210.16.3.34/27	
001	0 0 0 1 1 = 35	=> 210.16.3.35/27	
001	0 0 1 0 0 = 36	=> 210.16.3.36/27	
001	...		
001	1 1 1 1 0 = 62	=> 210.16.3.62/27	Subnet의 브로드캐스트 이므로 할당하지 않음
001	1 1 1 1 1 = 63	=> 210.16.3.63/27	

- 시스코에서는 Ip subnet-zero 기능을 이용하면 subnet 210.16.3.0/27 과 210.16.3.224/27 을 subnet으로 사용 가능하도록 지원한다.
- Cisco IOS version 12.0 이상에서는 ip subnet-zero 가 기본으로 설정되어 있다.

3.2 IPv4 주소체계

● **subnetting** 예제 2

얼마의 bit가 호스트 영역으로 확장되어야 하나?
(ip subnet-zero 설정 사용)



- 네트워크 주소: 202.168.57.0
- 필요한 서브넷: 8 개
- 서브넷당 호스트 수: 30개

- 요구 사항을 충족하는 서브넷을 위해 3 비트가 확장된다.
- 202.168.57.0/24 => 202.168.57.0/27
 - 3 서브넷 비트: $2^3 = 8$ 서브넷
 - 호스트를 위해 5비트가 사용: $2^5 - 2 = 30$ 서브넷당 호스트 수
- Class C 기본 마스크 11111111 11111111 11111111 00000000
- 수정된 서브넷 마스크 11111111 11111111 11111111 11100000
- 요구된 서브넷 마스크를 십진수와 점으로 표현 = 255.255.255.224



3.2 IPv4 주소체계

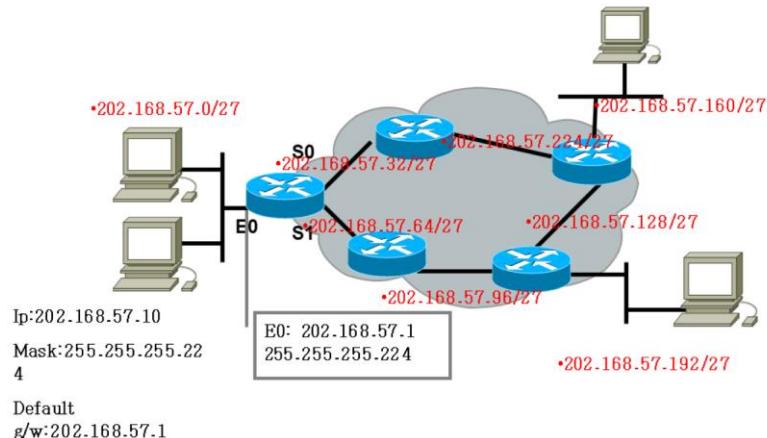
- 202.168.57.0/24 => 202.168.57.0/27
- Subnet mask: 11111111 11111111 11111111 11100000 = 255.255.255.224

Subnets 2진 표기 (2^n)	이용 가능한 Subnets (10진 표기)	서브넷당 사용 가능한 호스트 범위 ($2^n - 2$)
00000000	202.168.57.0/27	202.168.57.1 – 30
00100000	202.168.57.32/27	202.168.57.33 – 62
01000000	202.168.57.64/27	202.168.57.65 – 94
01100000	202.168.57.96/27	202.168.57.97 – 126
10000000	202.168.57.128/27	202.168.57.129 – 158
10100000	202.168.57.160/27	202.168.57.161 – 190
11000000	202.168.57.192/27	202.168.57.193 – 222
11100000	202.168.57.224/27	202.168.57.225 – 254



3.2 IPv4 주소체계

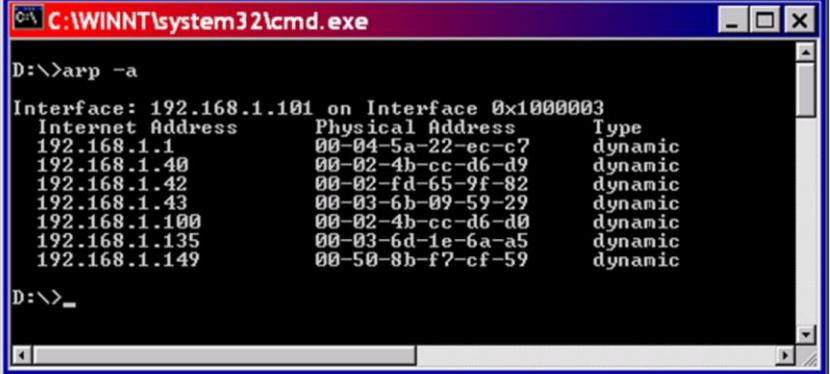
● IP 주소 배치(FLSM)



- FLSM(Fixed Length Subnet Mask) : 서브넷팅된 네트워크의 subnetmask 길이가 고정된 크기로 동일하다.

3장 Host to host 통신

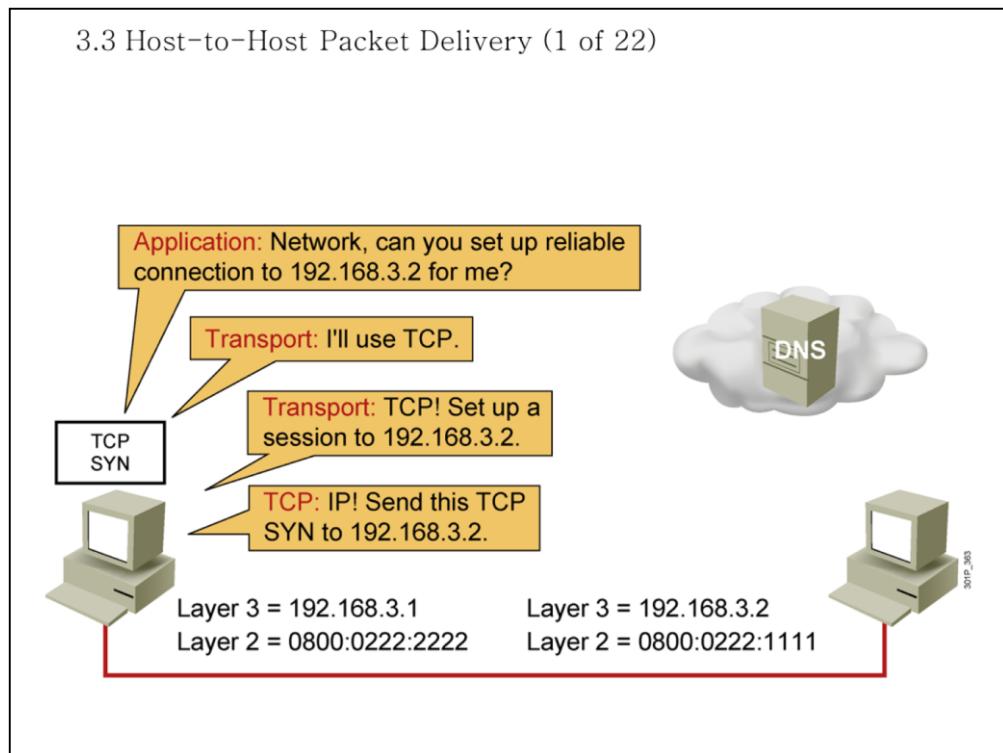
3.3 ARP Table



The screenshot shows a Windows command prompt window titled 'C:\WINNT\system32\cmd.exe'. The command 'arp -a' is entered, displaying the ARP table for interface 192.168.1.101. The table lists various IP addresses and their corresponding MAC addresses and types.

Internet Address	Physical Address	Type
192.168.1.1	00-04-5a-22-ec-c7	dynamic
192.168.1.40	00-02-4b-cc-d6-d9	dynamic
192.168.1.42	00-02-fd-65-9f-82	dynamic
192.168.1.43	00-03-6b-09-59-29	dynamic
192.168.1.100	00-02-4b-cc-d6-d0	dynamic
192.168.1.135	00-03-6d-1e-6a-a5	dynamic
192.168.1.149	00-50-8b-f7-cf-59	dynamic

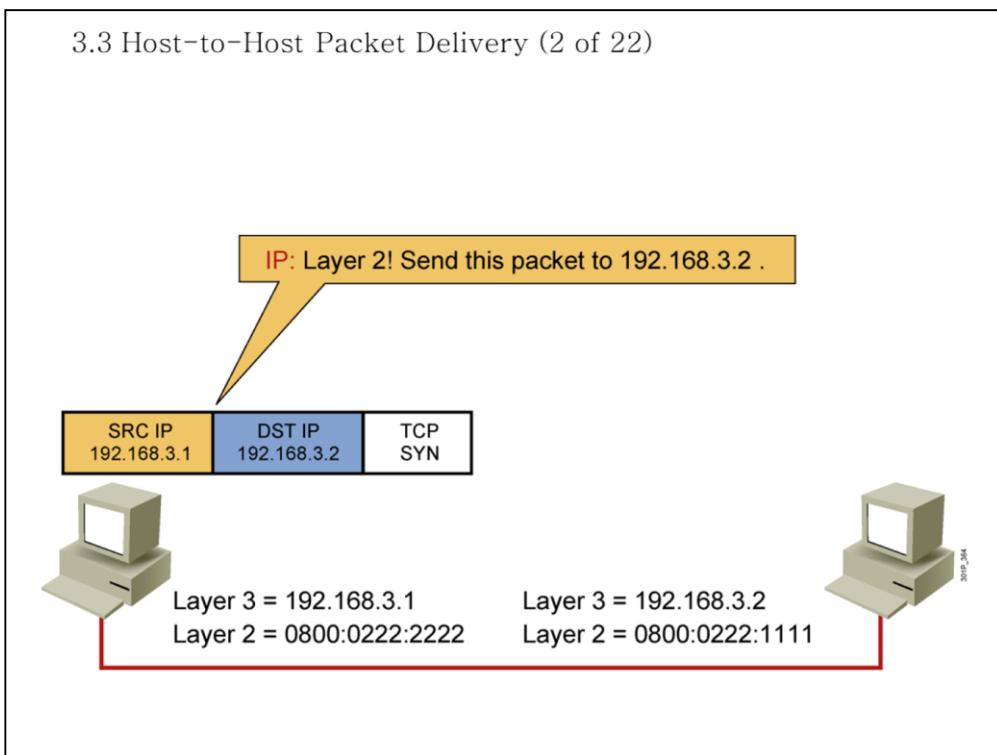
3.3 Host-to-Host Packet Delivery (1 of 22)



● Lesson Aim

- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (2 of 22)



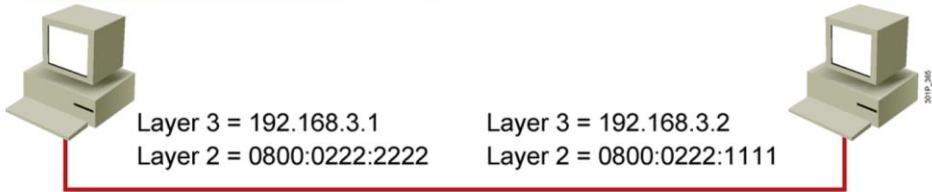
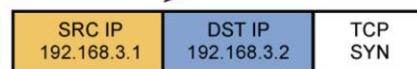
- Lesson Aim

- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (3 of 22)

Layer 2: ARP, do you have a mapping for 192.168.3.2?

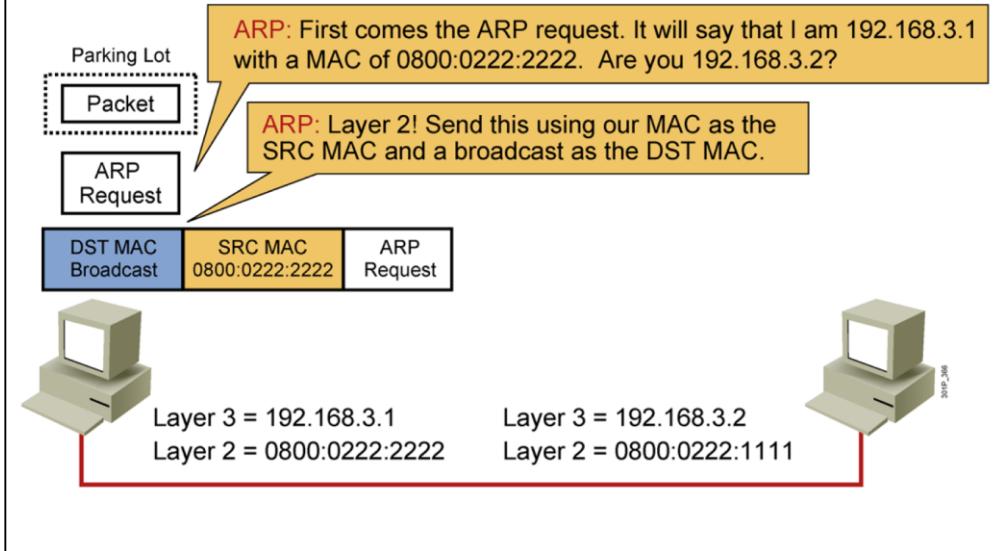
ARP: Is 192.168.3.2 in my ARP table? No, I guess Layer 2 will have to put the packet in the parking lot until I do an ARP.



● Lesson Aim

- <Enter lesson aim here.>

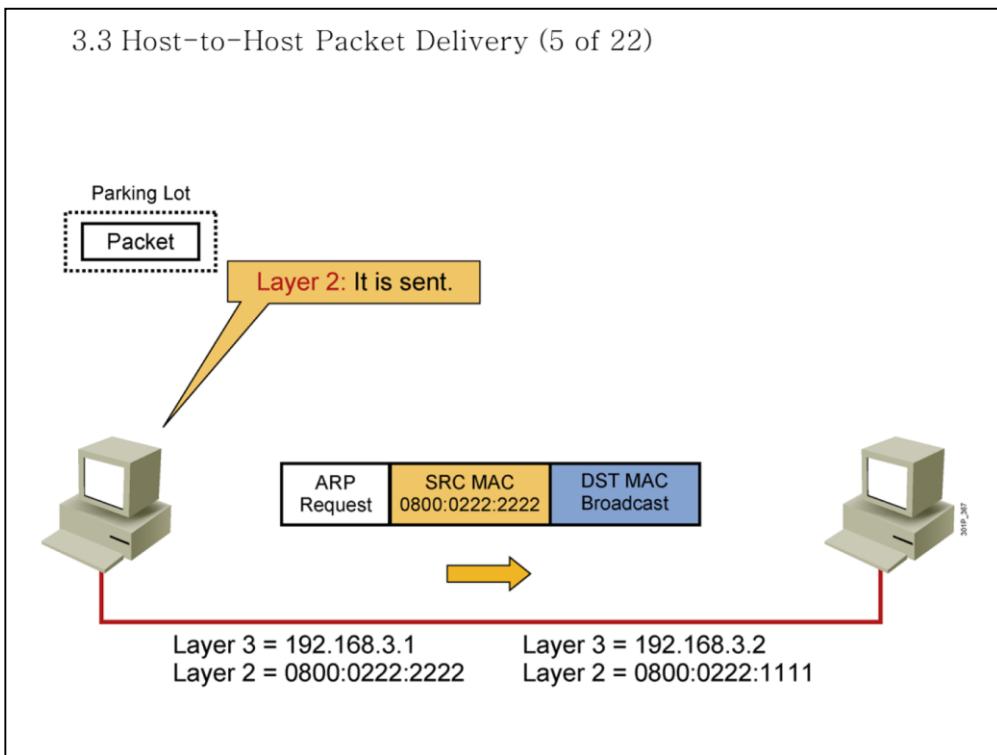
3.3 Host-to-Host Packet Delivery (4 of 22)



● Lesson Aim

- <Enter lesson aim here.>

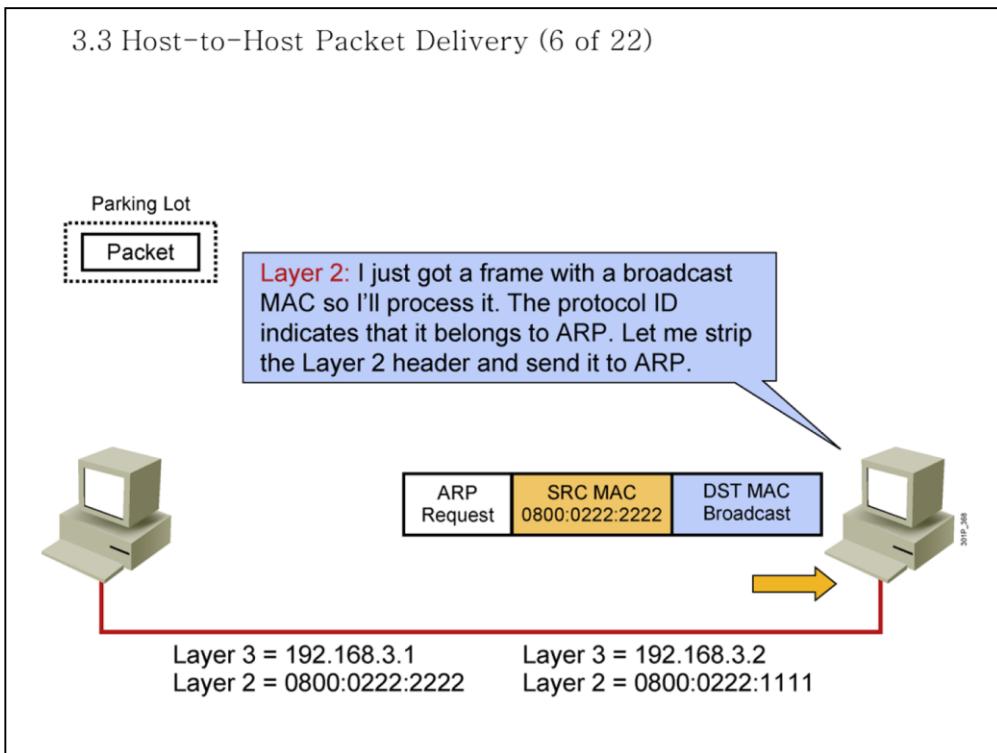
3.3 Host-to-Host Packet Delivery (5 of 22)



● Lesson Aim

- <Enter lesson aim here.>

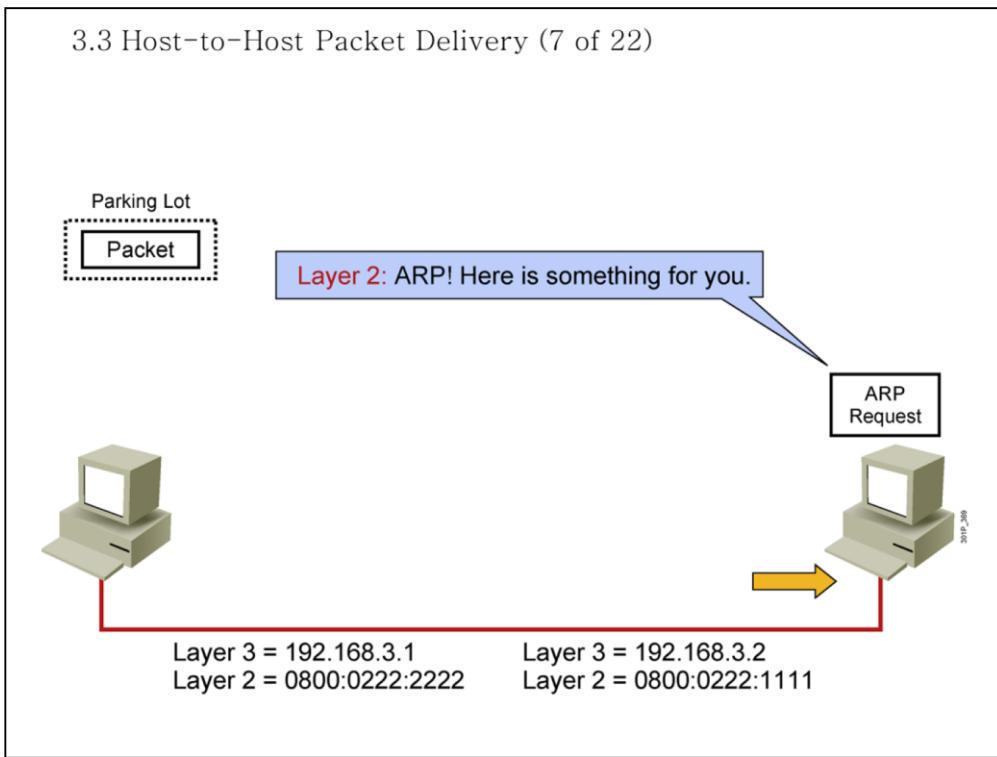
3.3 Host-to-Host Packet Delivery (6 of 22)



● Lesson Aim

- <Enter lesson aim here.>

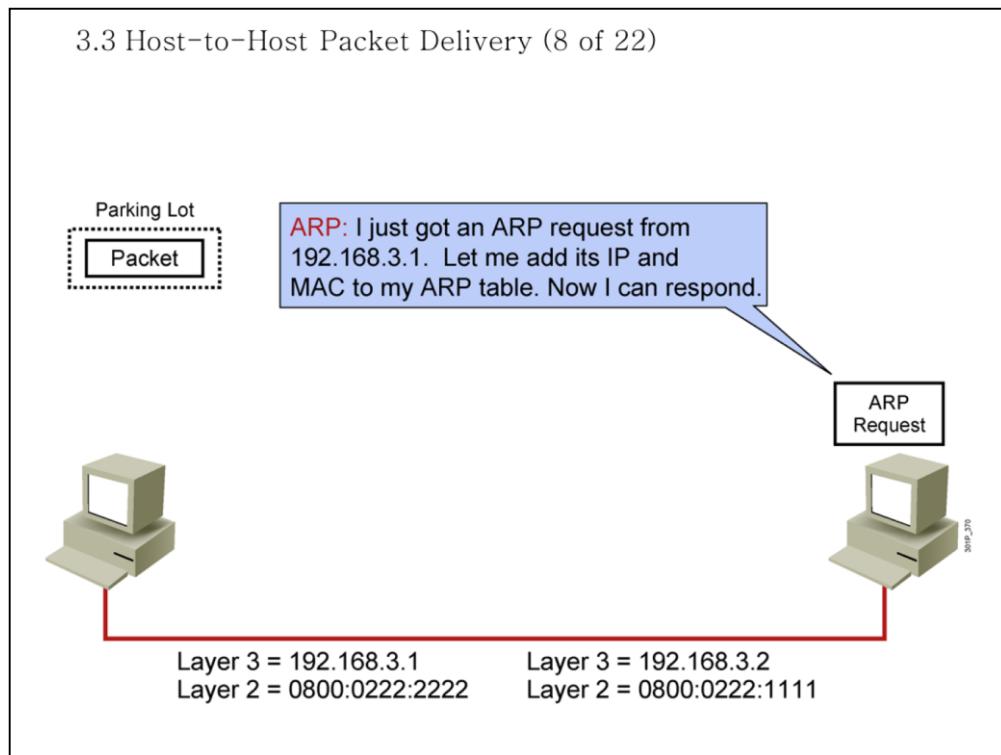
3.3 Host-to-Host Packet Delivery (7 of 22)



- Lesson Aim

- <Enter lesson aim here.>

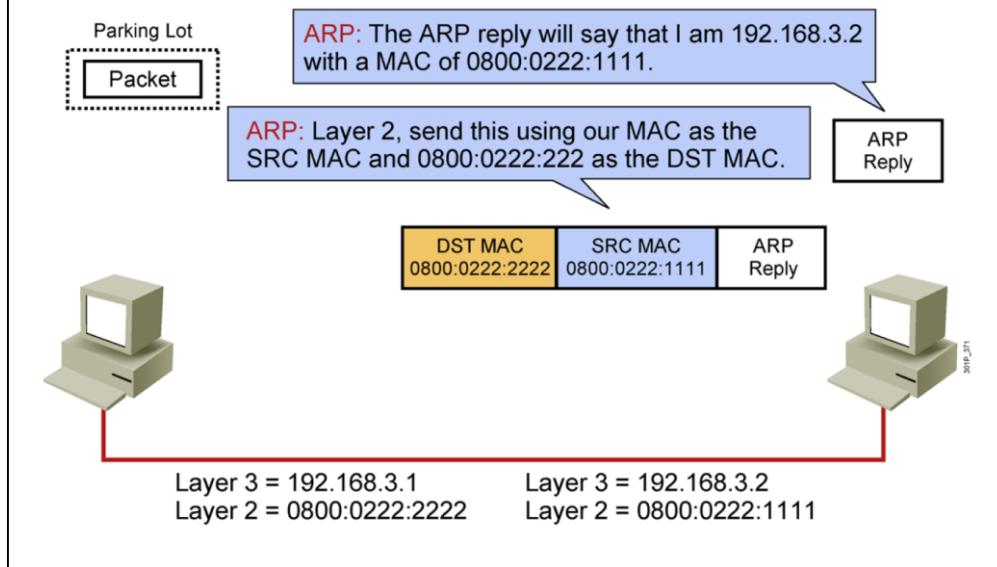
3.3 Host-to-Host Packet Delivery (8 of 22)



- Lesson Aim

- <Enter lesson aim here.>

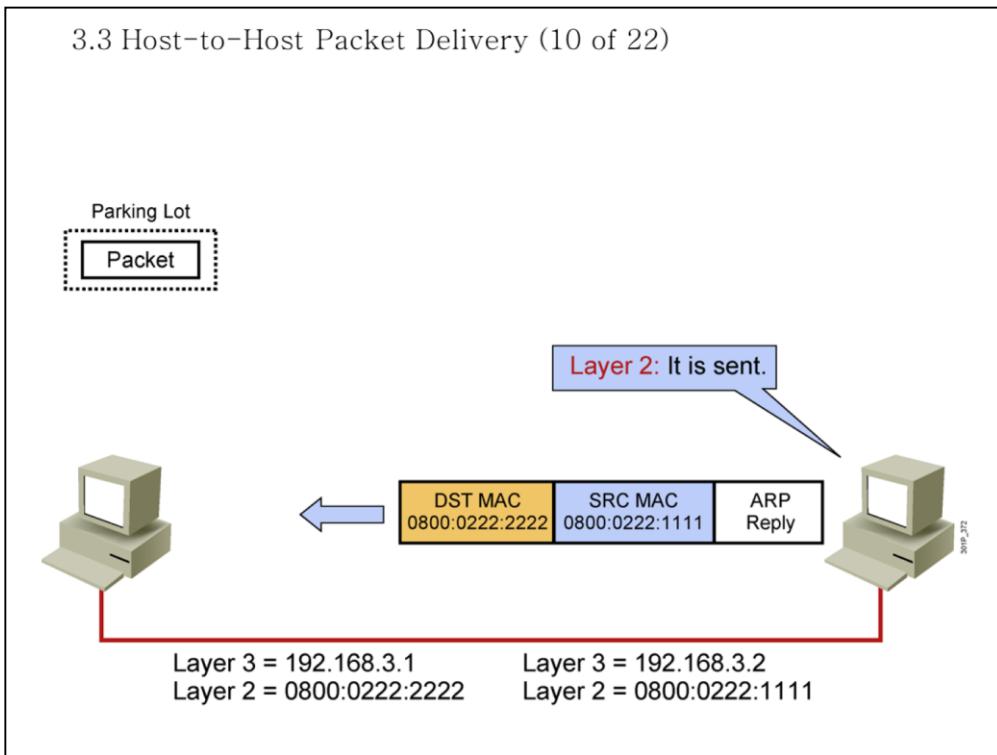
3.3 Host-to-Host Packet Delivery (9 of 22)



- Lesson Aim

- <Enter lesson aim here.>

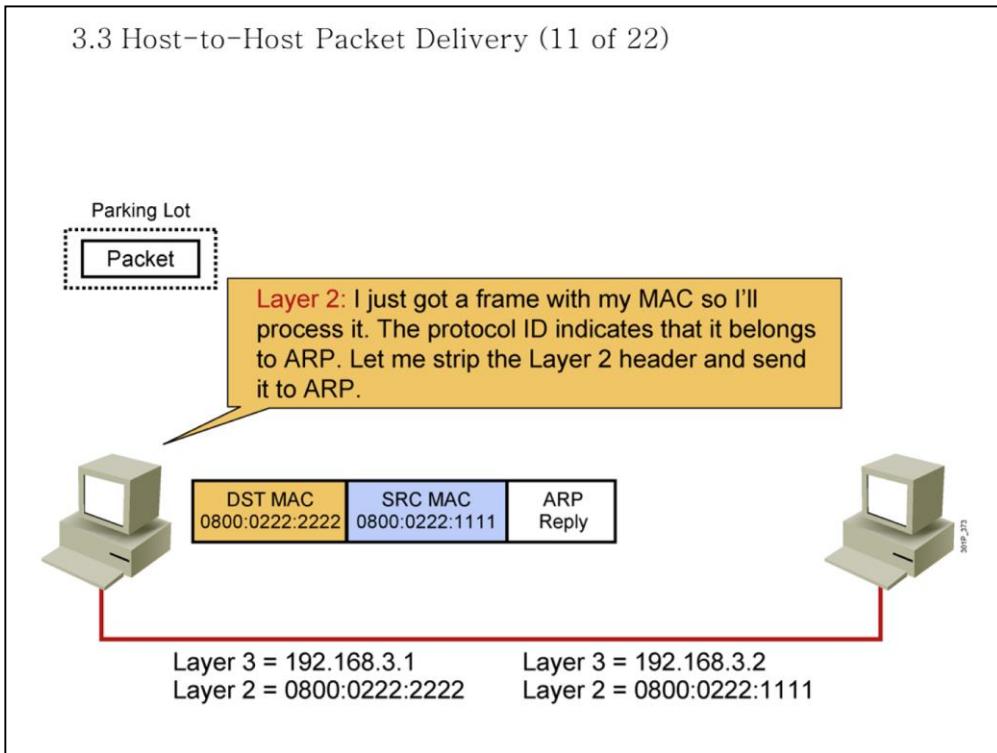
3.3 Host-to-Host Packet Delivery (10 of 22)



● Lesson Aim

- <Enter lesson aim here.>

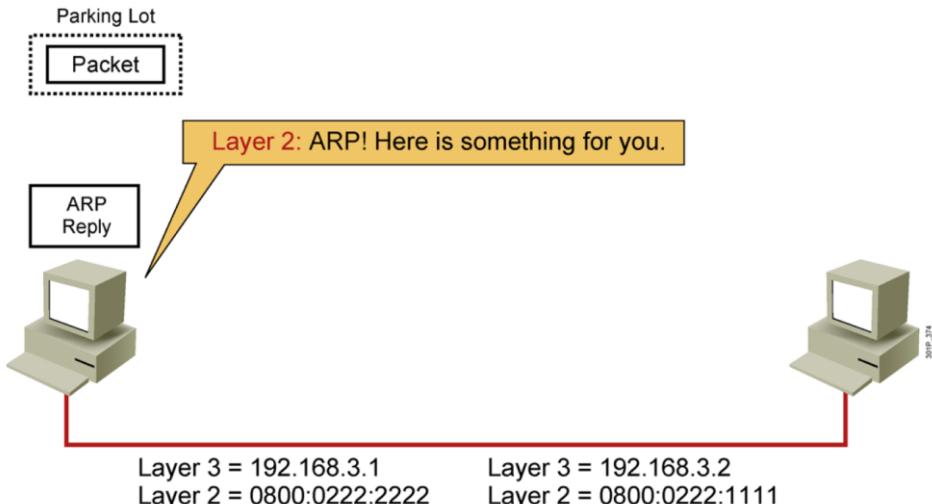
3.3 Host-to-Host Packet Delivery (11 of 22)



● Lesson Aim

- <Enter lesson aim here.>

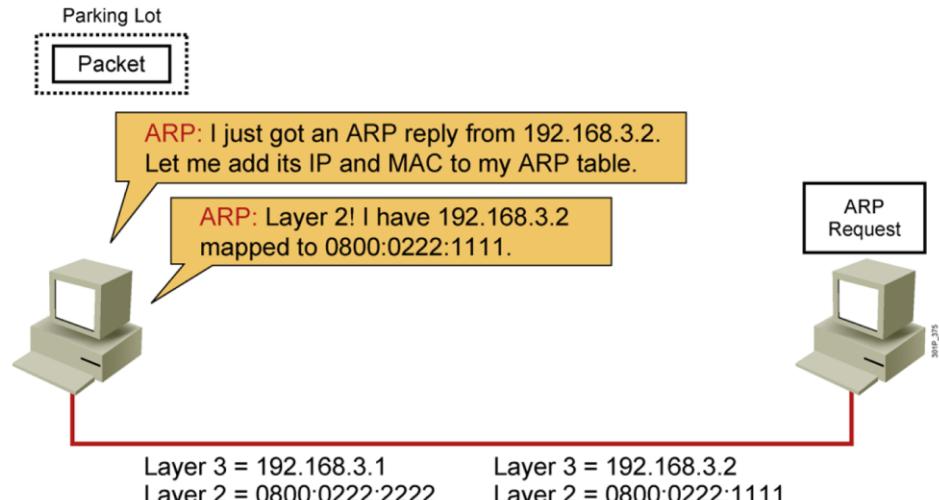
3.3 Host-to-Host Packet Delivery (12 of 22)



● Lesson Aim

- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (13 of 22)

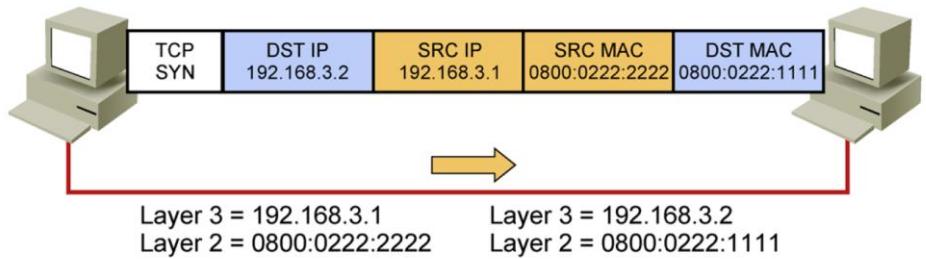


- Lesson Aim

- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (14 of 22)

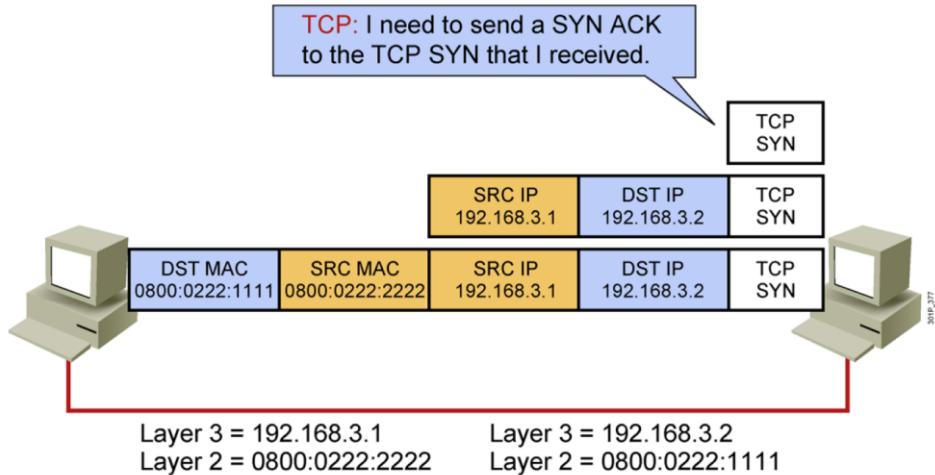
Layer 2: I can send out that pending packet.



● Lesson Aim

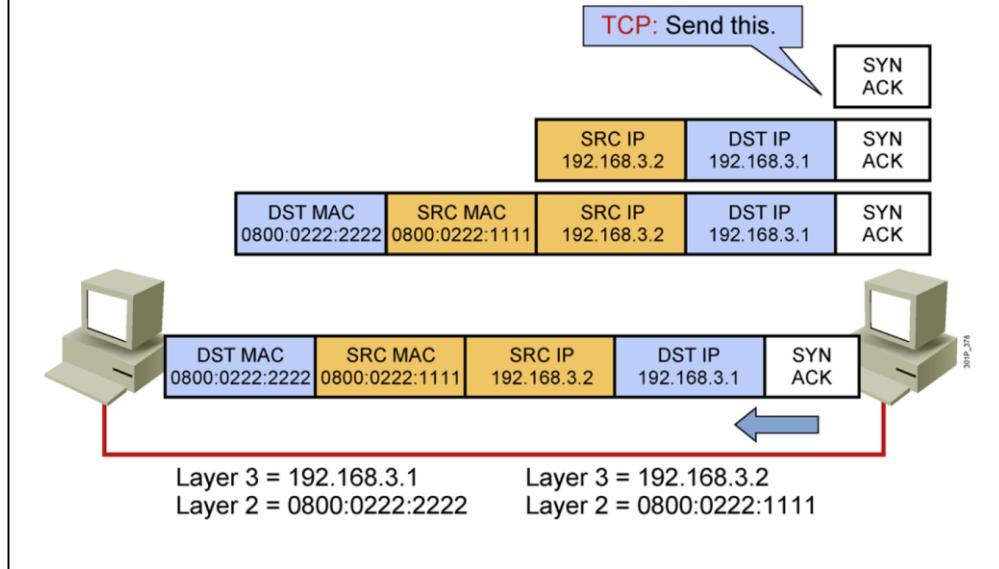
- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (15 of 22)



● Lesson Aim

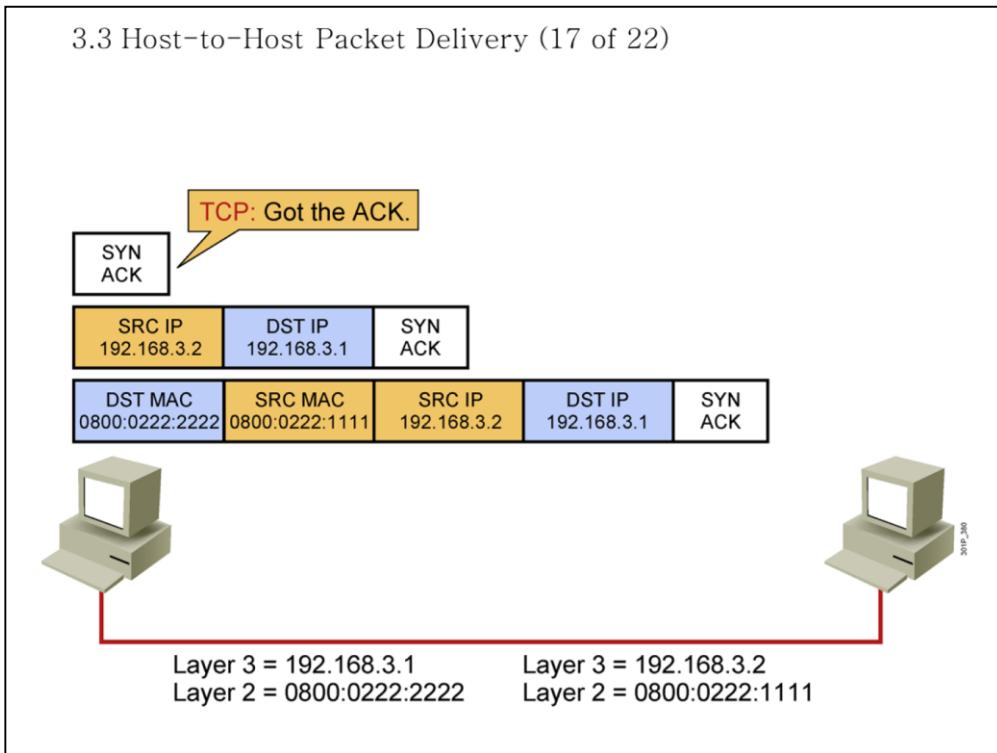
- <Enter lesson aim here.>



● Lesson Aim

- <Enter lesson aim here.>

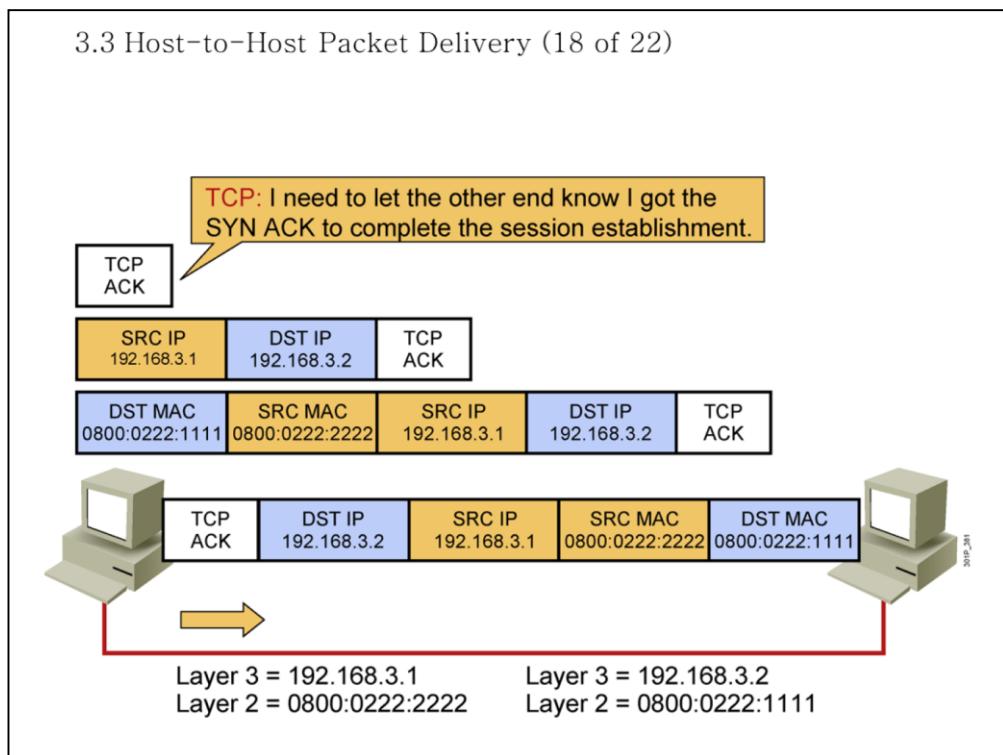
3.3 Host-to-Host Packet Delivery (17 of 22)



● Lesson Aim

- <Enter lesson aim here.>

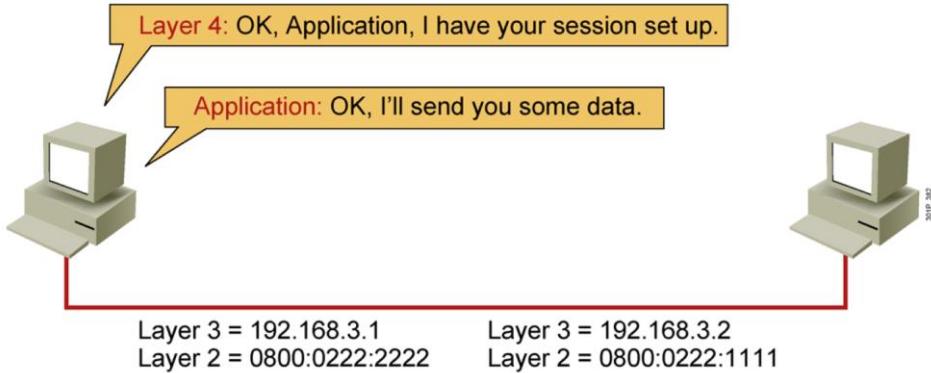
3.3 Host-to-Host Packet Delivery (18 of 22)



● Lesson Aim

- <Enter lesson aim here.>

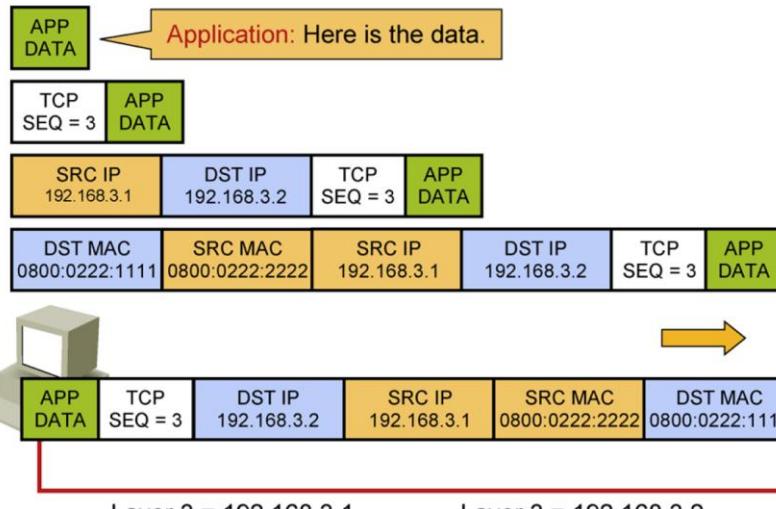
3.3 Host-to-Host Packet Delivery (19 of 22)

**● Lesson Aim**

- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (20 of 22)

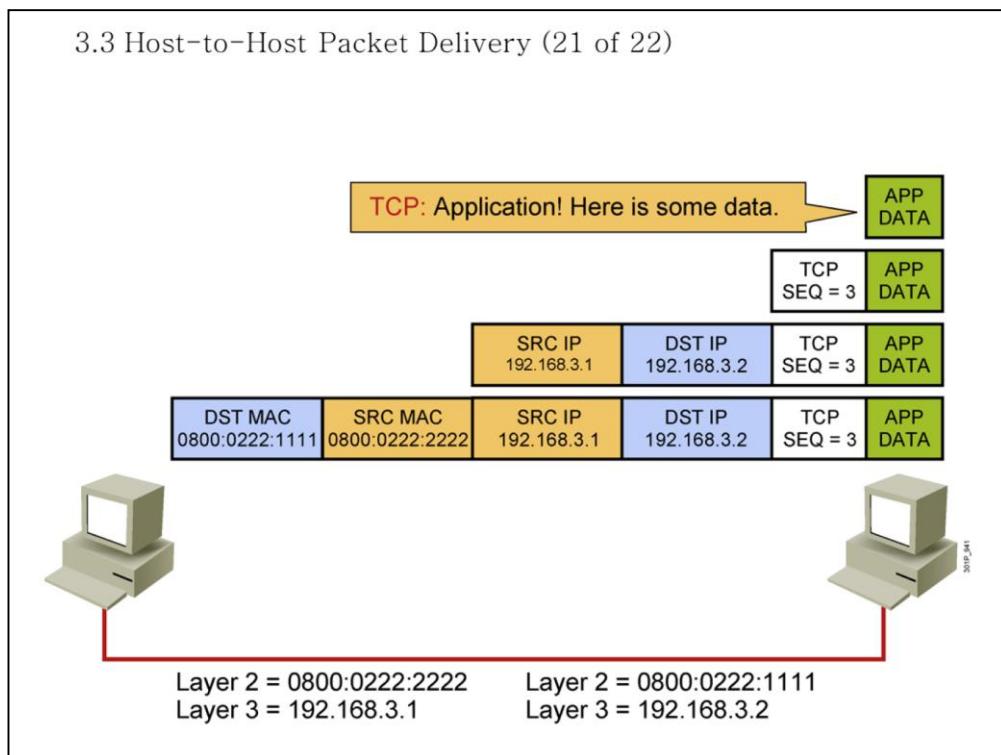
트롤 기본



● Lesson Aim

- <Enter lesson aim here.>

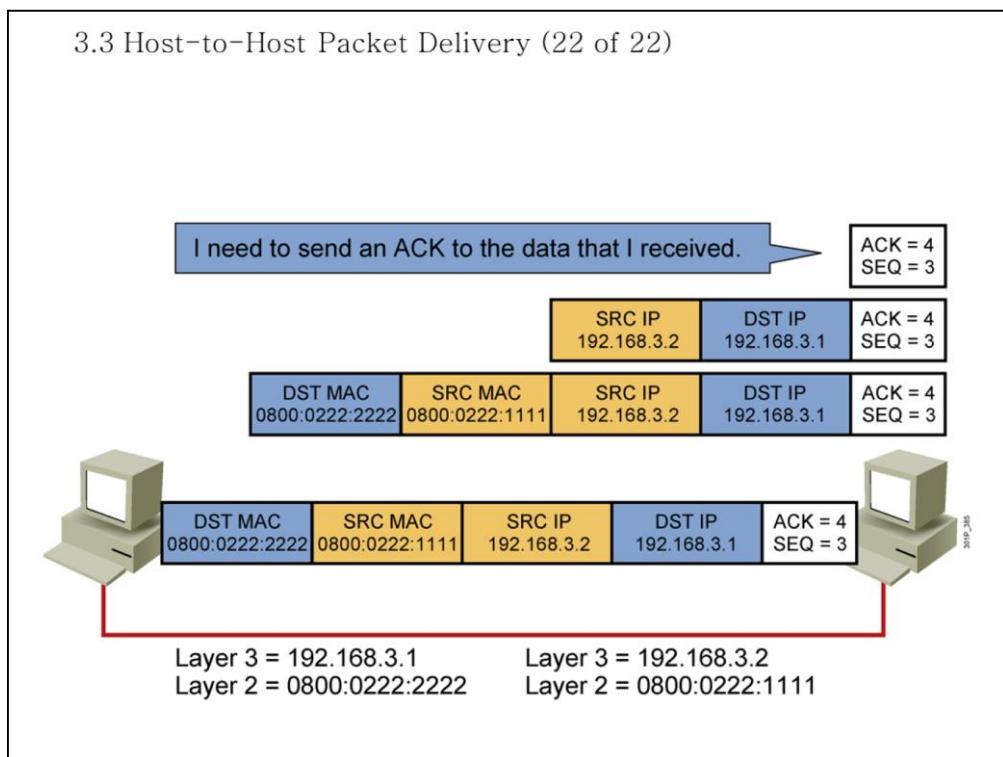
3.3 Host-to-Host Packet Delivery (21 of 22)



● Lesson Aim

- <Enter lesson aim here.>

3.3 Host-to-Host Packet Delivery (22 of 22)

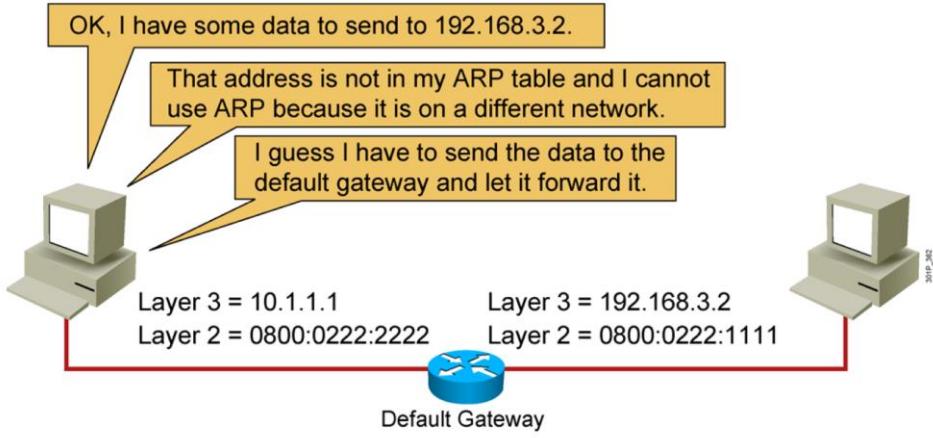


● Lesson Aim

- <Enter lesson aim here.>

3.3 Default Gateway

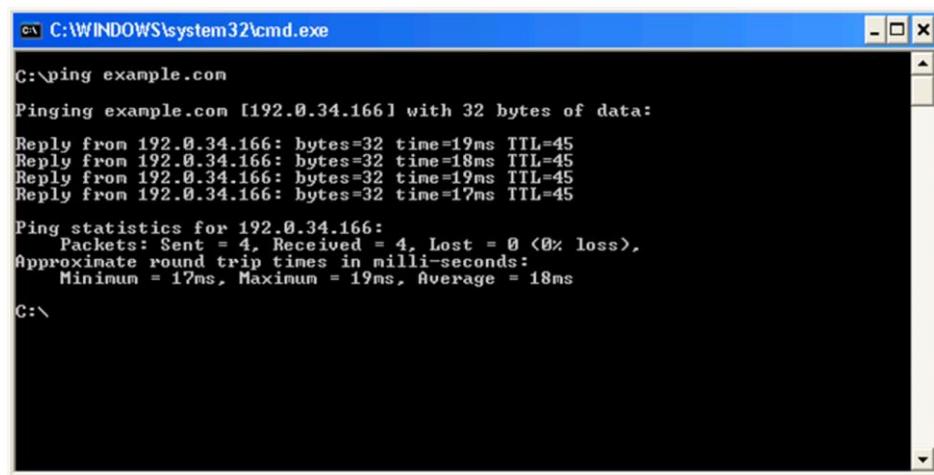
도 콜 기 본



● Lesson Aim

- <Enter lesson aim here.>

3.3 Host-Based Tools: ping



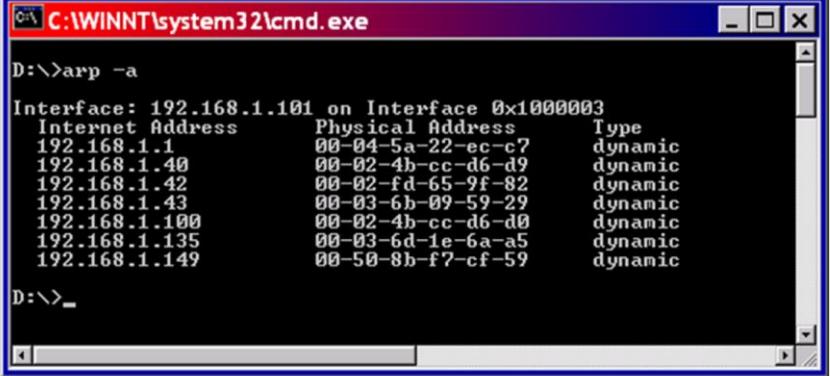
```
C:\> ping example.com

Pinging example.com [192.0.34.166] with 32 bytes of data:
Reply from 192.0.34.166: bytes=32 time=19ms TTL=45
Reply from 192.0.34.166: bytes=32 time=18ms TTL=45
Reply from 192.0.34.166: bytes=32 time=19ms TTL=45
Reply from 192.0.34.166: bytes=32 time=17ms TTL=45

Ping statistics for 192.0.34.166:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 19ms, Average = 18ms

C:\>
```

3.3 Host-Based Tools: Table



C:\WINNT\system32\cmd.exe

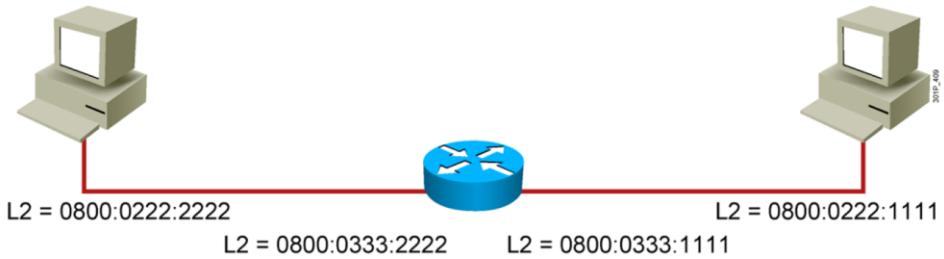
```
D:\>arp -a
Interface: 192.168.1.101 on Interface 0x1000003
Internet Address      Physical Address      Type
192.168.1.1           00-04-5a-22-ec-c7    dynamic
192.168.1.40          00-02-4b-cc-d6-d9    dynamic
192.168.1.42          00-02-fd-65-9f-82    dynamic
192.168.1.43          00-03-6b-09-59-29    dynamic
192.168.1.100         00-02-4b-cc-d6-d0    dynamic
192.168.1.135         00-03-6d-1e-6a-a5    dynamic
192.168.1.149         00-50-8b-f7-cf-59    dynamic

D:\>_
```

4장 Network to network 통신

3.4 Default-gateway의 역할

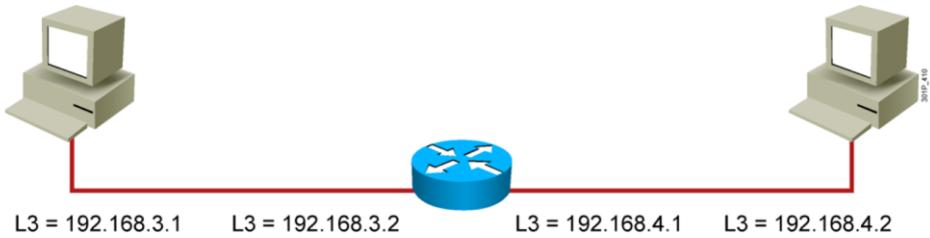
Layer 2 Addressing



- 각각의 host와 라우터는 위의 예와 같은 MAC 주소 정보를 가지고 있고, 하나의 네트워크 내에서 통신을 할 때 L2 주소인 MAC 주소를 이용한다.

3.4 Default-gateway의 역할

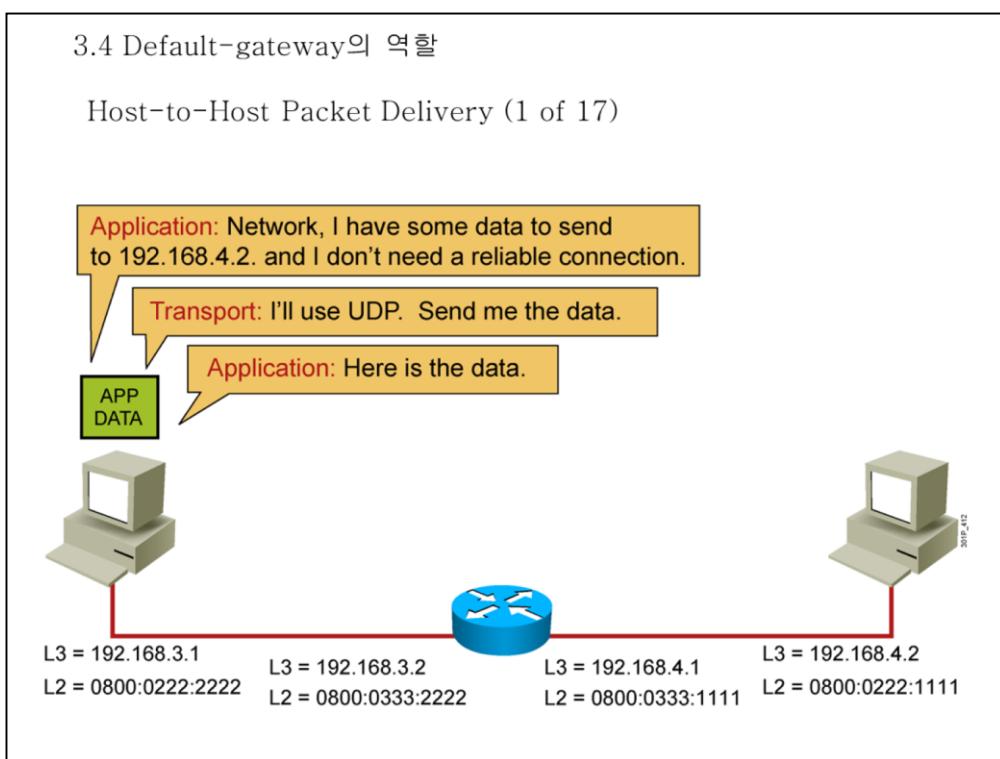
Layer 3 Addressing



- 각각의 host와 라우터는 위의 예와 같은 IP 주소 정보를 가지고 있고, 네트워크 간에 통신을 할 때 L3 주소인 IP 주소를 이용한다.
- 기본적으로 라우터 기능을 가지고 있지 않은 일반 시스템은 직접적으로 다른 네트워크에 있는 시스템과 통신할 수 없다.
- 그렇기 때문에 반드시 default-gateway에 대한 정보를 가지고 있어야 한다.
- 이 default-gateway 역할을 하며 다른 네트워크 간에 통신을 지원하는 장비가 router이다.

3.4 Default-gateway의 역할

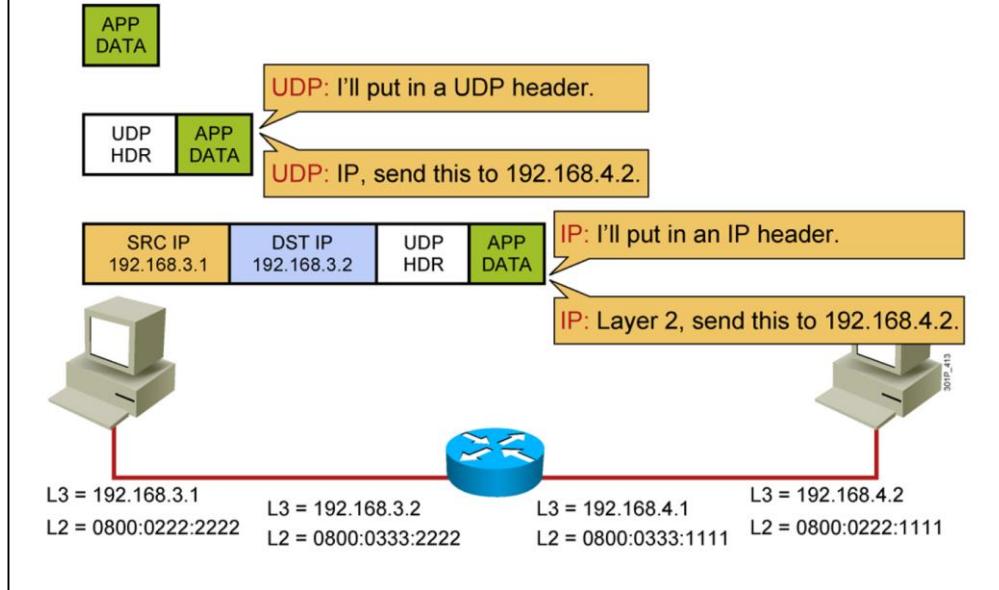
Host-to-Host Packet Delivery (1 of 17)



- 응용계층에서는 user가 만든 데이터를 받아 적절한 통신 프로그램으로 연계시키고 transport 계층에 적절한 방법을 통해 전송해 줄 것을 요청한다.

3.4 Default-gateway의 역할

Host-to-Host Packet Delivery (2 of 17)



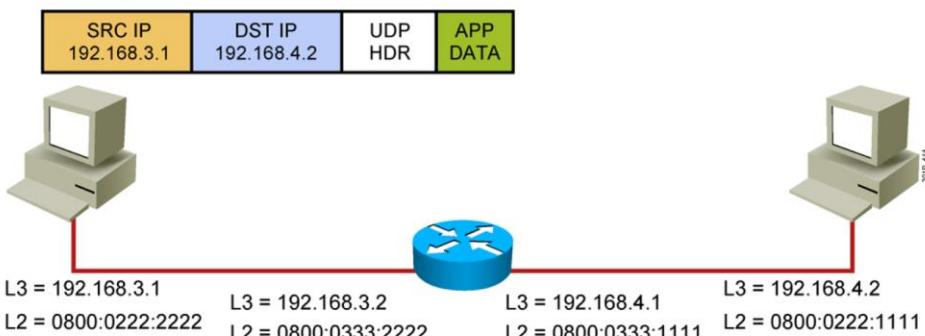
- 응용계층으로부터 데이터를 받은 transport 계층은 요청에 맞게 UDP를 통해 전송할 것을 결정하고 네트워크 계층 쪽으로 전송할 데이터 정보를 전달한다.
- Transport층을 통해 받은 Data를 전송하기 위해 network 계층에서는 상대방의 주소 정보를 확인하고 데이터 링크 계층 쪽으로 전송할 데이터 정보를 전달한다.

3.4 Default-gateway의 역할

Host-to-Host Packet Delivery (3 of 17)

Layer 2: ARP, do you have a mapping for 192.168.4.2?

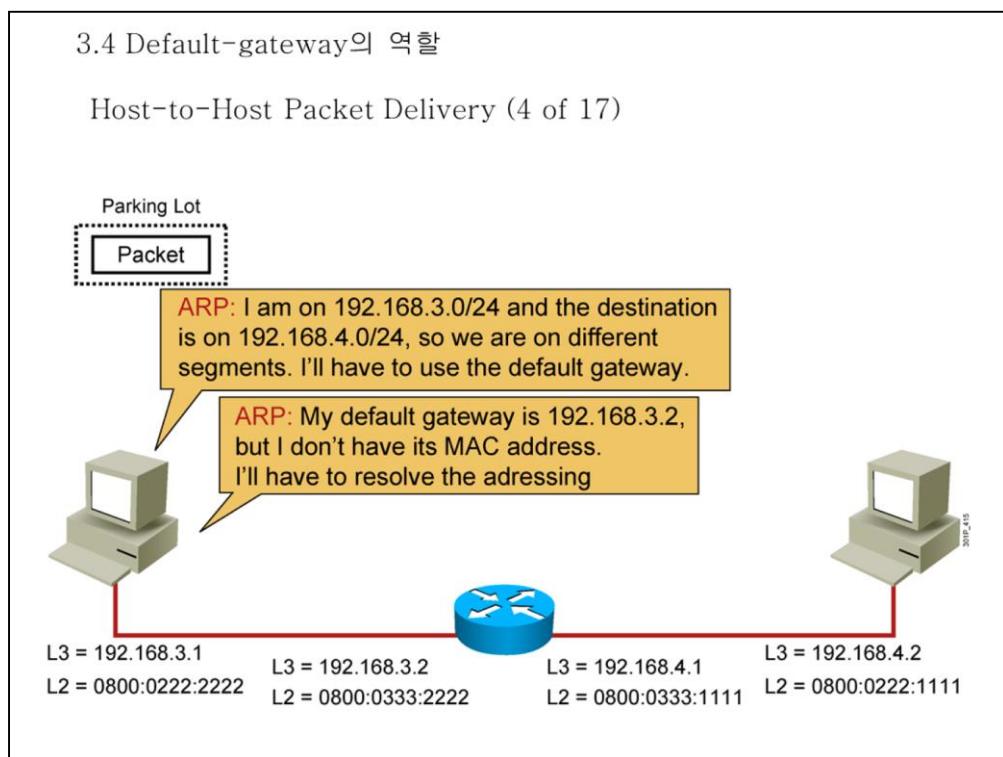
ARP: No, Layer 2 will have to hold the packet while I resolve the addressing.



- 데이터 링크 계층에서는 목적지 시스템에게 데이터를 전송하기 위한 L2 정보를 가지고 있는지를 확인한다.
- 목적지 IP에 해당하는 L2 정보를 가지고 있지 않으면 ARP를 통해 이 문제를 해결하려고 한다.

3.4 Default-gateway의 역할

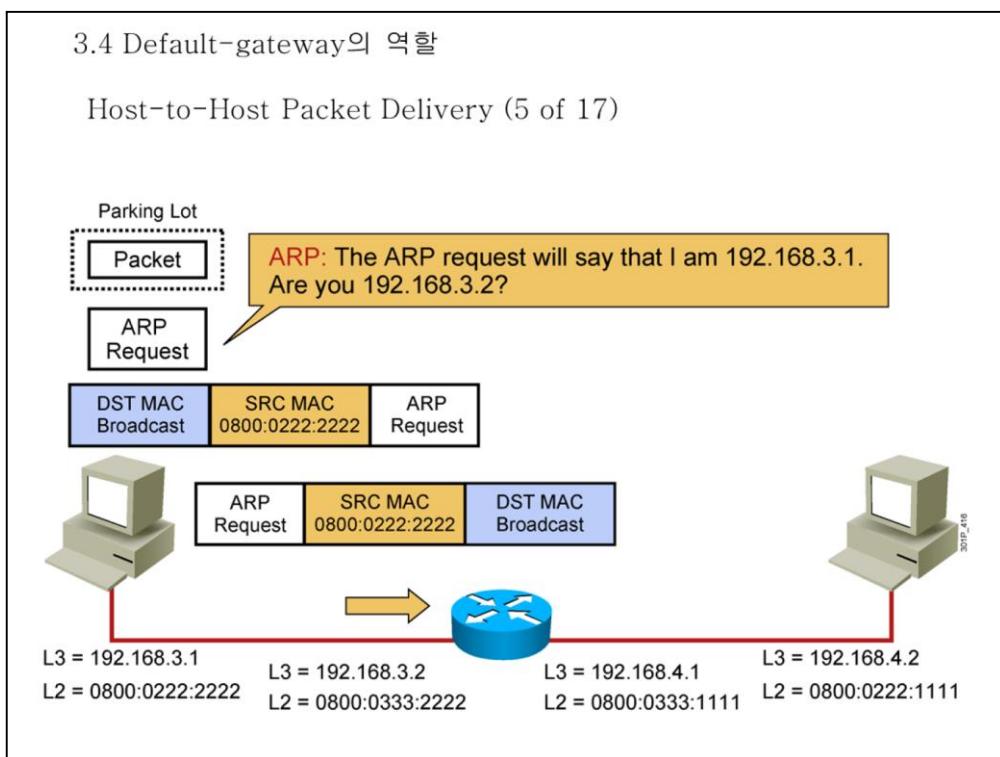
Host-to-Host Packet Delivery (4 of 17)



- 목적지 시스템의 MAC 정보를 찾기 위한 과정을 진행하기 위해 데이터 전송을 일시 중지하고 ARP 과정을 우선 진행한다.
 - 송신자와 목적지 시스템의 네트워크가 다름을 확인한다.
 - Default gateway에 대한 정보가 있는지 확인한다.
 - Default gateway에 대한 L2 정보가 있는지 확인한다.

3.4 Default-gateway의 역할

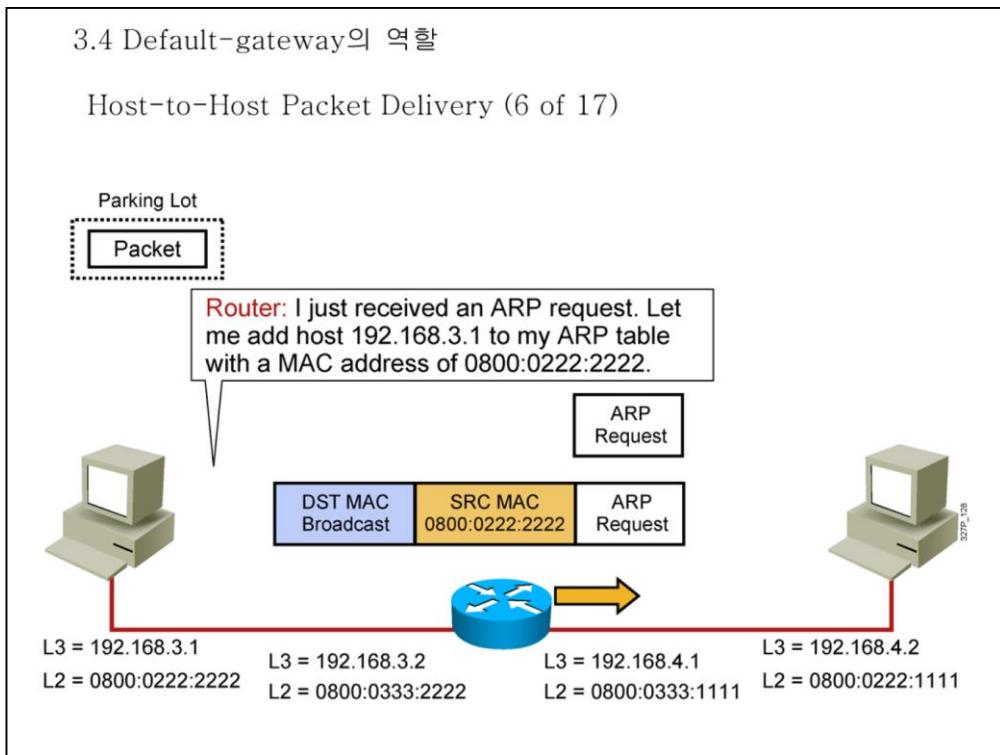
Host-to-Host Packet Delivery (5 of 17)



- Default gateway의 MAC 정보를 찾기 위한 ARP request 과정이 진행된다.

3.4 Default-gateway의 역할

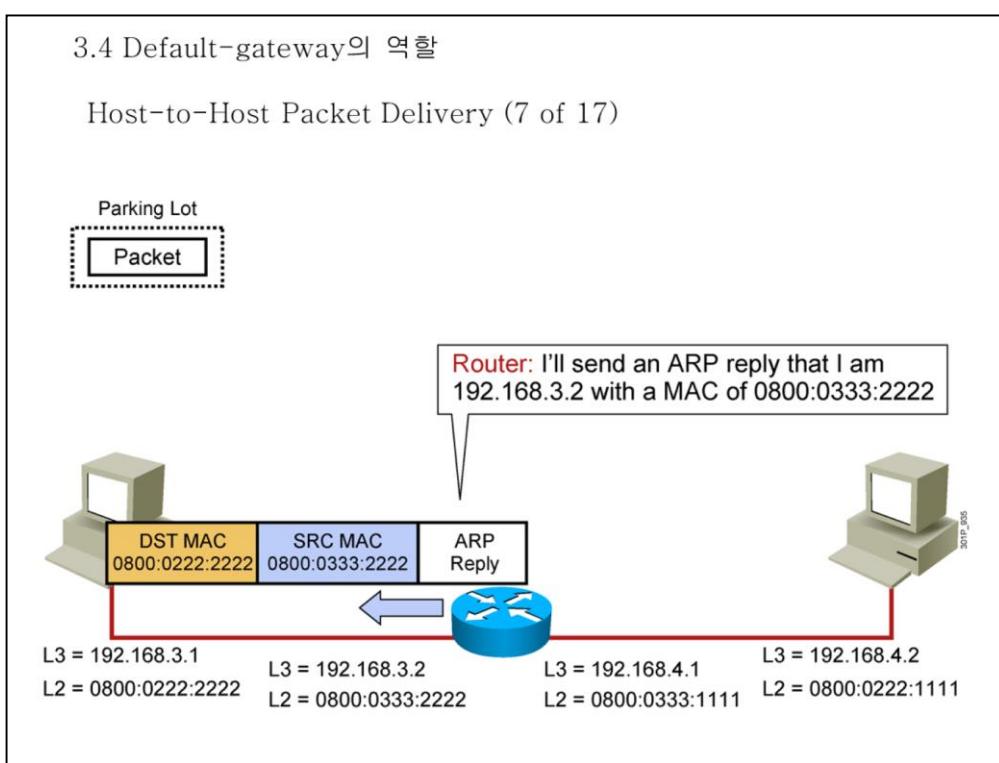
Host-to-Host Packet Delivery (6 of 17)



- ARP request Broadcast 프레임을 받은 라우터는 자신의 MAC 정보를 요청하는 것임을 확인한다.

3.4 Default-gateway의 역할

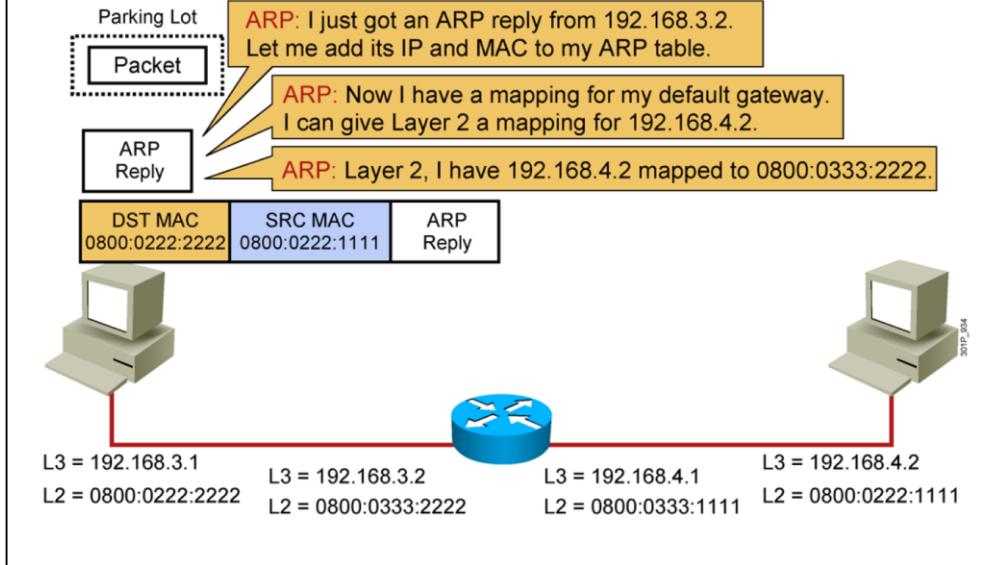
Host-to-Host Packet Delivery (7 of 17)



- 라우터가 자신의 MAC 정보를 ARP reply를 통해 알려준다.

3.4 Default-gateway의 역할

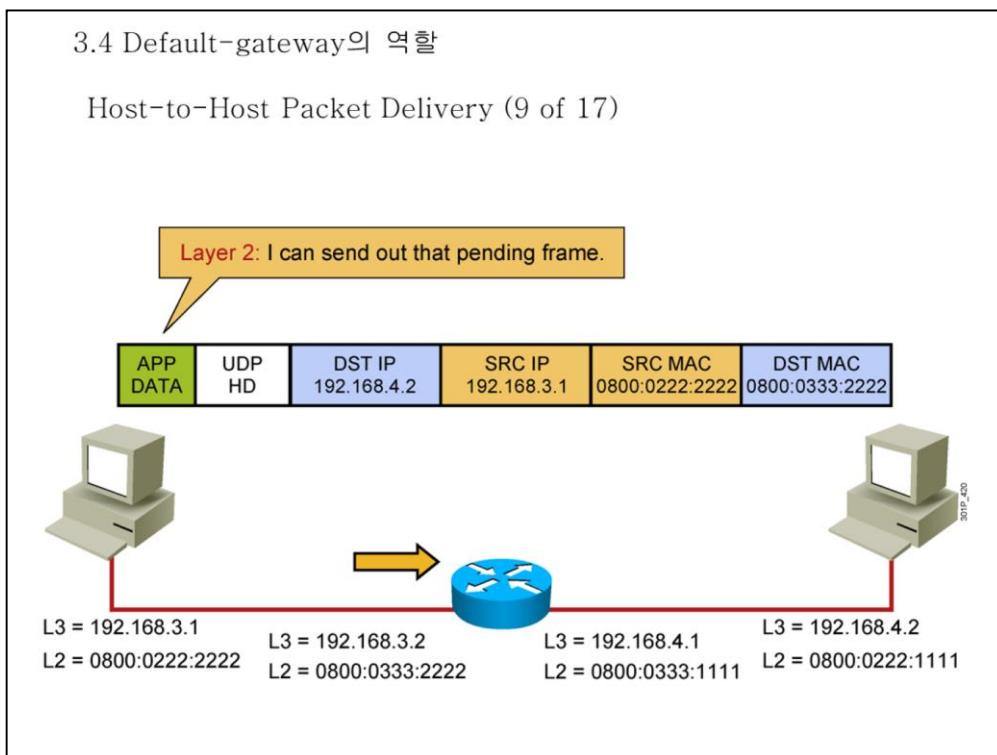
Host-to-Host Packet Delivery (8 of 17)



- 라우터의 응답을 들은 송신지 시스템은 그 정보를 자신의 ARP cache에 저장한다.

3.4 Default-gateway의 역할

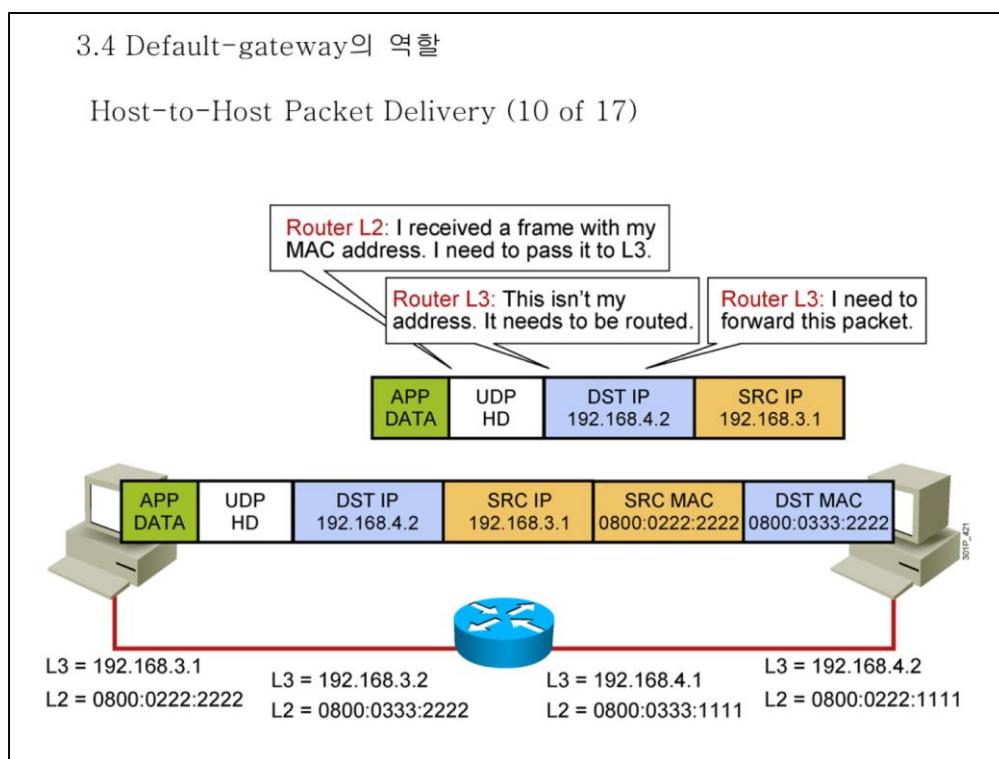
Host-to-Host Packet Delivery (9 of 17)



- 라우터(default gateway)의 MAC 정보를 이용해서 목적지 시스템으로 데이터를 전송한다.

3.4 Default-gateway의 역할

Host-to-Host Packet Delivery (10 of 17)

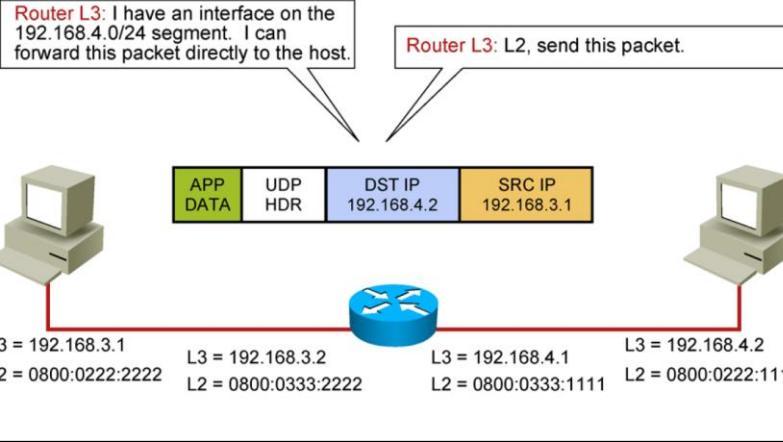


- 라우터는 들어온 frame으로부터 자신의 주소를 확인하고 packet의 내용을 확인한다.

3.4 Default-gateway의 역할

Host-to-Host Packet Delivery (11 of 17)

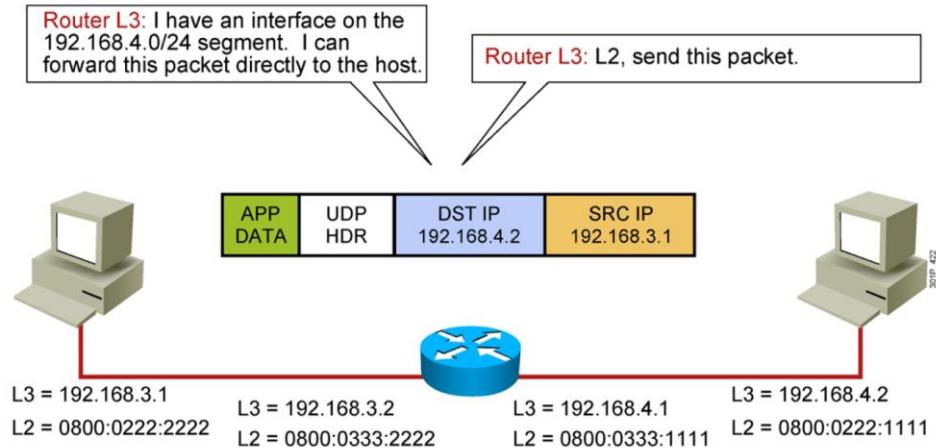
Destination	Next Hop	Interface
192.168.3.0/24	Connected	fa 0/0
192.168.4.0/24	Connected	fa 0/1



- 라우터는 자신의 라우팅 테이블에 있는 정보를 확인하여 자신이 받은 데이터를 해당 네트워크로 전송할 수 있음을 확인한다.

3.4 Default-gateway의 역할

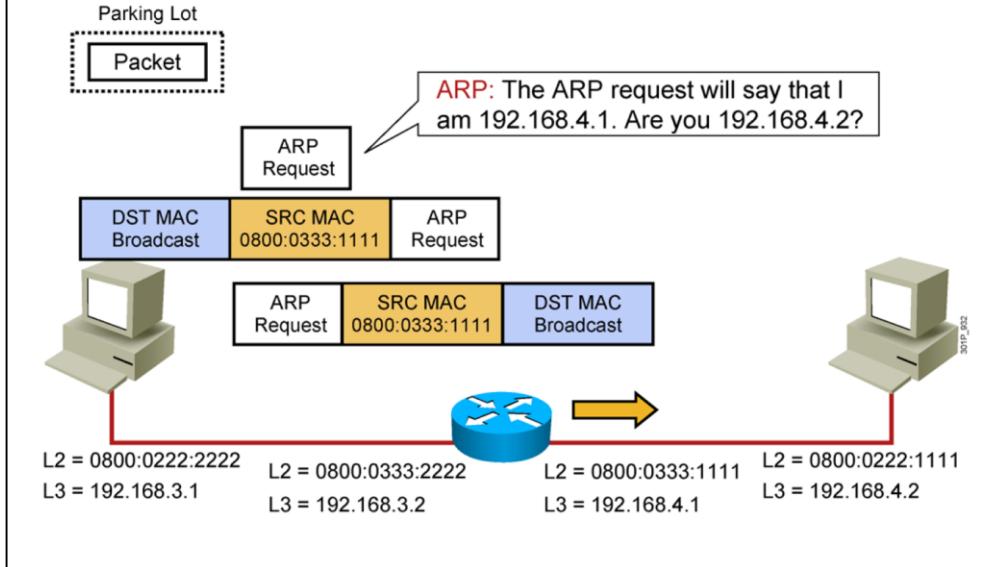
Host-to-Host Packet Delivery (12 of 17)



- 라우터는 데이터를 전송하기 위해서 데이터 링크 계층으로 데이터를 전송할 것을 요청한다.

3.4 Default-gateway의 역할

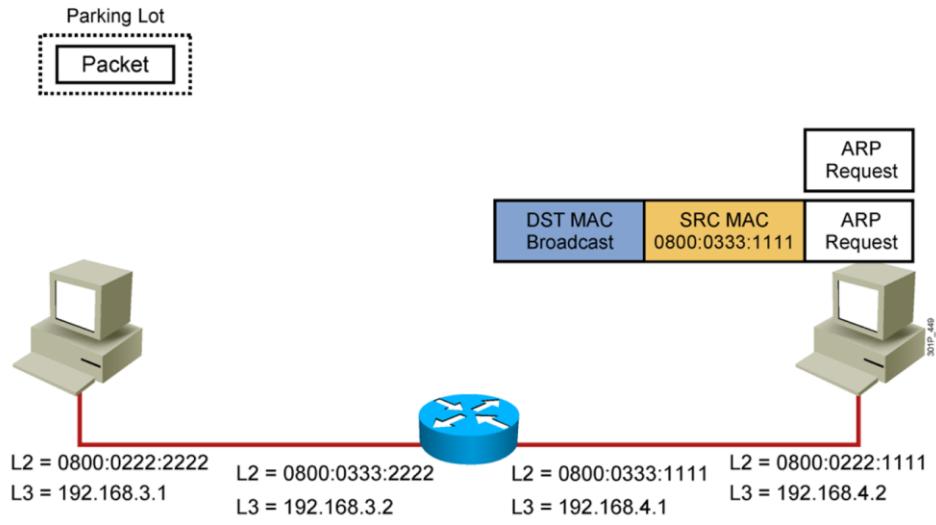
Host-to-Host Packet Delivery (13 of 17)



- 라우터는 데이터를 전송하기 전에 목적지 시스템의 MAC 정보를 알기 위한 ARP request Broadcast를 전달한다.

3.4 Default-gateway의 역할

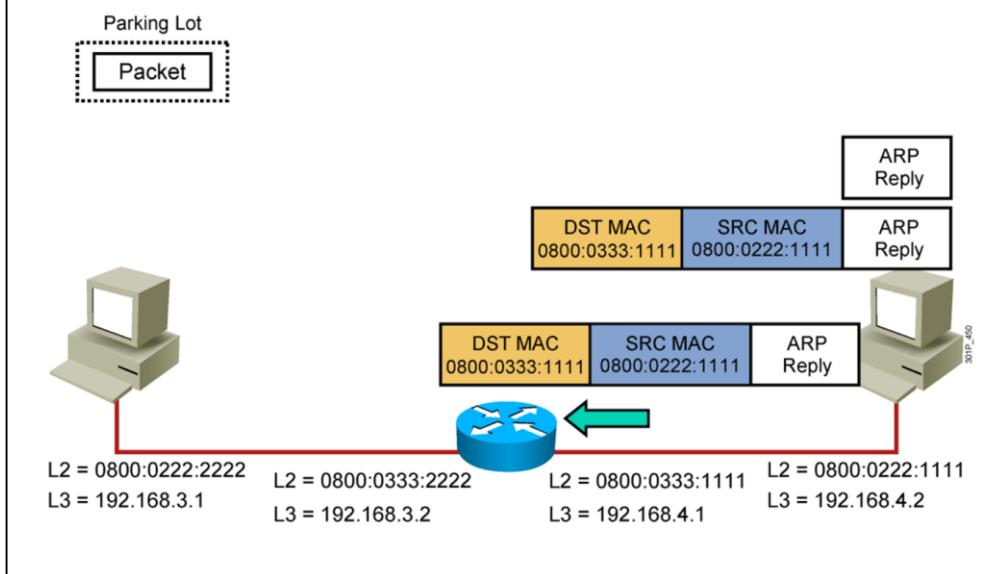
Host-to-Host Packet Delivery (14 of 17)



- 라우터로부터 ARP request를 받은 목적지 시스템은 라우터가 원하는 MAC이 자신의 MAC 정보임을 확인한다.

3.4 Default-gateway의 역할

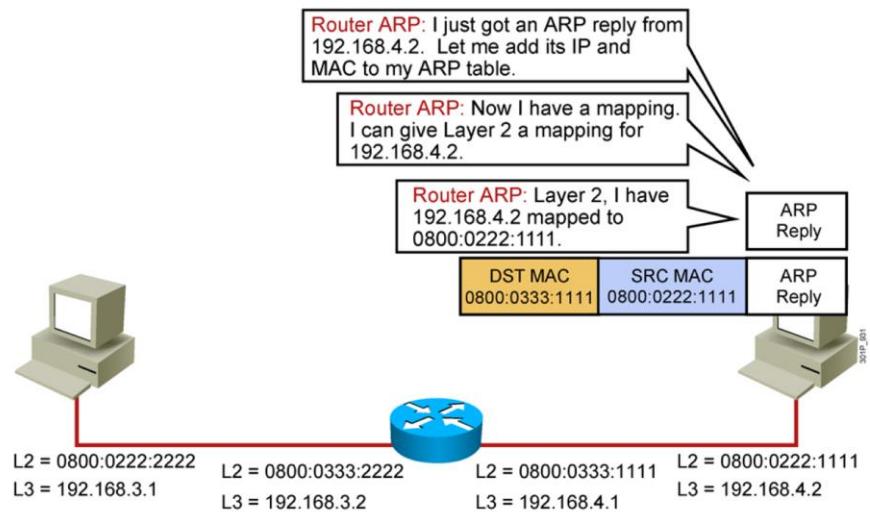
Host-to-Host Packet Delivery (15 of 17)



- 목적지 시스템으로부터 ARP reply가 전송된다.

3.4 Default-gateway의 역할

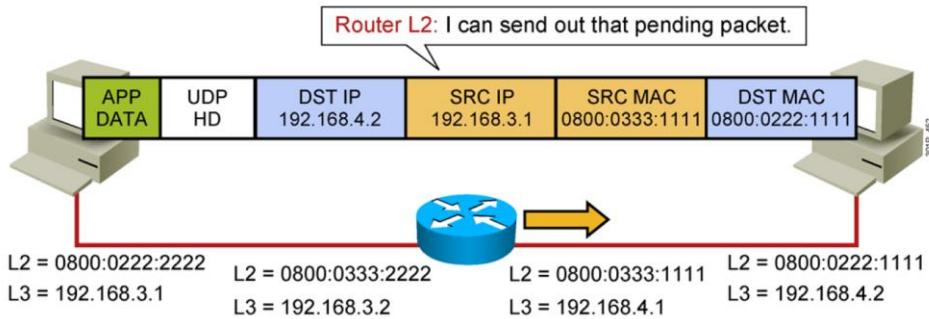
Host-to-Host Packet Delivery (16 of 17)



- 라우터는 ARP reply 정보를 받아 자신의 ARP cache에 IP 정보와 함께 mapping한다.

3.4 Default-gateway의 역할

Host-to-Host Packet Delivery (17 of 17)



- 라우터는 목적지 시스템의 MAC 정보를 이용해서 데이터를 목적지 시스템으로 전송한다.
- 최종적으로 목적지에 데이터가 전송되고 목적지 시스템은 L2 정보를 확인하여 자신에게 온 정보인지를 확인한다.