

2026/10/14, 2026 보안 기초 세미나



TCP/IP 프로토콜

-18장 DHCP, 19장 DNS-

민 윤 홍(yunhong@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)

목 차

- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)

DHCP

- 등장 개요
  - 컴퓨터가 다른 망과 통신하기 위해 필수적으로 필요한 주소들을 제공하기 위한 프로토콜들이 등장함
  - 필수 주소
    - 내 컴퓨터의 IP 주소
    - 내 컴퓨터의 해당 서브 넷 마스크
    - 라우터의 IP 주소
    - 네임서버의 IP 주소
  - 종류
    - RARP (Reverse Address Resolution Protocol)
    - BOOTP (Bootstrap Protocol)
    - DHCP (Dynamic Host Configuration Protocol)

DHCP

- RARP (Reverse Address Resolution Protocol)
  - 정의
    - 자신의 MAC 주소를 IP 주소로 변환하는 프로토콜
  - 특징
    - 새 컴퓨터가 부팅되었을 때 IP 주소를 제공함
  - 동작 방식
    1. 클라이언트가 자신의 MAC 주소를 담고 있는 메시지를 브로드캐스트함
    2. 메시지를 수신한 RARP서버는 요청자의 MAC 주소에 대응하는 IP 주소를 담은 응답 메시지를 유니캐스트로 보냄
  - 한계점
    - RARP 서버가 각 망에 존재해야 IP 주소를 받을 수 있음
    - 통신에 필요한 4가지 주소 중 내 컴퓨터의 IP 주소만 받을 수 있음

DHCP

- BOOTP (Bootstrap Protocol) (1/2)
  - 정의
    - 처음으로 부팅된 컴퓨터나 디스크를 갖지 않은 컴퓨터에게 통신에 필요한 정보들을 정적으로 제공하는 프로토콜
  - 특징
    - IP 주소, 부트 파일이 존재하는 서버 이름, 부트 파일 이름을 제공함
      - 서브넷 마스크, 라우터의 IP, 네임서버의 IP는 옵션 필드를 사용하여 제공 가능함
    - 관리자가 정한 MAC – IP 주소 테이블을 확인하고 제공함

DHCP

- BOOTP (Bootstrap Protocol) (2/2)
  - 동작 방식
    1. 클라이언트가 자신의 MAC 주소를 담고 있는 메시지를 브로드캐스트함
    2. BOOTP 서버는 수신한 MAC 주소와 매핑되는 IP 주소를 테이블에서 찾아 메시지에 담아서 클라이언트에게 보냄
       - 매핑되는 IP 주소가 테이블에 없다면 응답하지 않음
  - 한계점
    - 정적으로 주소를 할당하므로 동적인 상황에 대응하지 못함
      - 클라이언트의 MAC 주소가 변하는 경우에 IP 주소를 사용할 수 없음
        - e.g., 추적 방지를 위한 무작위 MAC를 사용하는 경우
      - 클라이언트가 임시 IP를 사용할 수 없음
        - e.g., 공공 Wi-Fi를 사용하는 사용자들에게 임시 IP를 할당하는 경우

DHCP

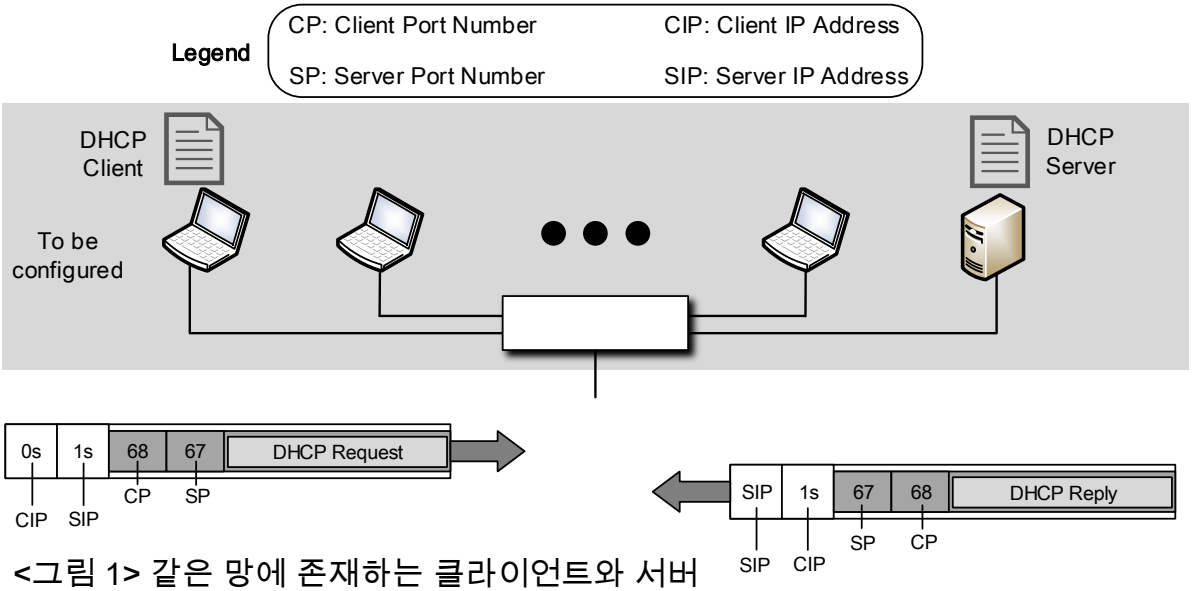
- DHCP (Dynamic Host Configuration Protocol)
  - 정의
    - 부팅된 컴퓨터나 디스크를 갖지 않은 컴퓨터에게 통신에 필요한 정보들을 동적으로 제공하는 프로토콜
  - 특징
    - 제한된 수량의 IP 주소를 재사용, 일시적 사용, 자동으로 재활용이 가능함
    - DHCP 클라이언트와 DHCP 서버가 다른 망에 존재할 수도 있음
      - DHCP 중계 에이전트가 작동하여 연결해줌
    - BOOTP 프로토콜과 패킷 구조가 거의 동일하여 BOOTP로 동작하는 클라이언트도 DHCP 서버에 의해 정적으로 주소 설정이 가능함

DHCP

- DHCP 동작 절차
  - 같은 망에 클라이언트와 서버가 존재하는 경우
    - 동작 과정 (1/2)
      1. DHCP 서버는 UDP 포트 번호 67에 passive open* 명령을 수행하고 클라이언트로부터 요청을 기다림
      2. 클라이언트는 포트 번호 68에 active open* 명령을 수행함
         - 클라이언트는 발신지 IP 주소를 모두 0으로 채우고 목적지 IP 주소를 모두1로 채워 브로드캐스트함

*passive open
서버가 포트를 열어두고 클라이언트의 요청이 올 때까지 기다리는 상태

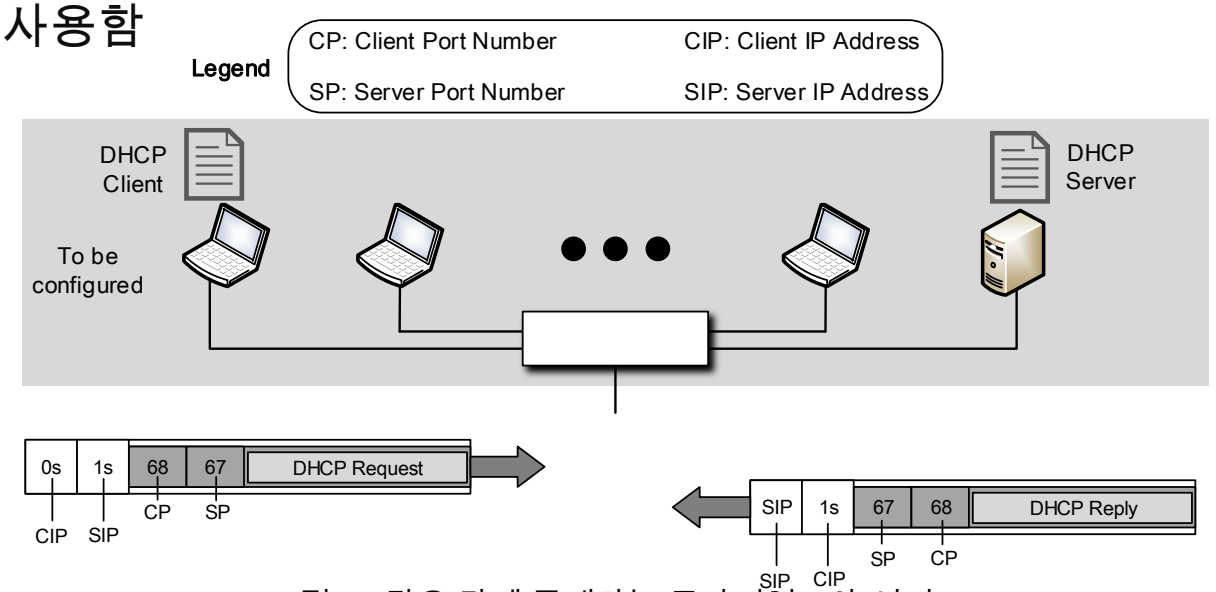
*active open
클라이언트가 서버에 연결을 요청하는 상태



<그림 1> 같은 망에 존재하는 클라이언트와 서버

DHCP

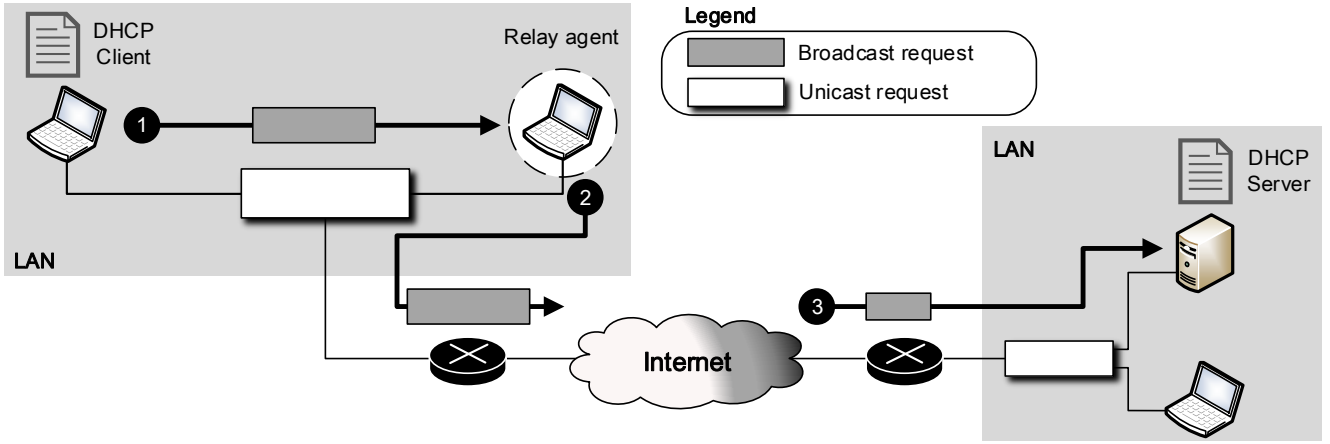
- DHCP 동작 절차
  - 같은 망에 클라이언트와 서버가 존재하는 경우
    - 동작 과정 (2/2)
      3. 서버는 UDP 목적지 포트 번호를 68, 발신지 포트 번호를 67로 지정한 후 유니캐스트나 브로드캐스트 메시지를 클라이언트에게 보냄
         - 클라이언트의 물리 주소를 알고 있으므로 유니캐스트가 가능함
         - 시스템이 물리 주소와 IP 주소를 매핑하는 과정을 요구하면 브로드캐스트를 사용함



<그림 1> 같은 망에 존재하는 클라이언트와 서버

DHCP

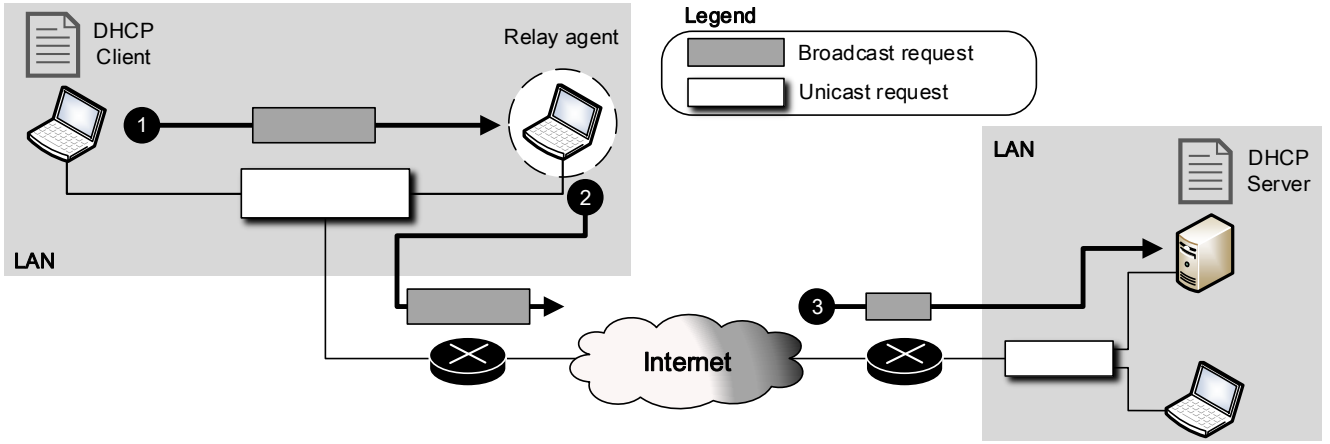
- DHCP 동작 절차
  - 다른 망에 클라이언트와 서버가 존재하는 경우
    - 특징
      - 중계 에이전트(Relay Agent)라고 하는 호스트가 필요함
        - 클라이언트가 브로드캐스트한 메시지는 라우터를 통과하지 못하기 때문임
        - 중계 에이전트는 DHCP 서버의 유니캐스트 주소를 알고 있음



<그림 2> 다른 망에 존재하는 클라이언트와 서버

DHCP

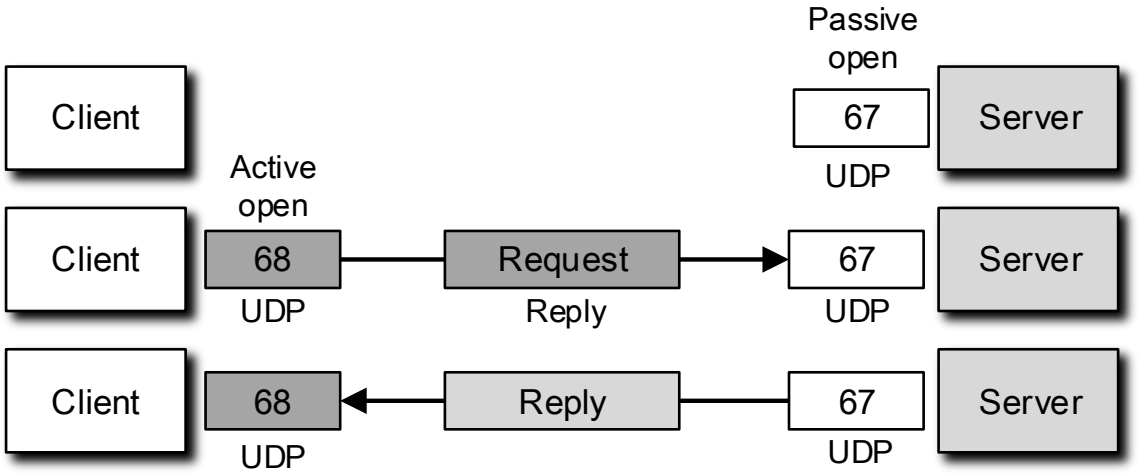
- DHCP 동작 절차
  - 다른 망에 클라이언트와 서버가 존재하는 경우
    - 동작 과정
      1. 중계 에이전트가 클라이언트의 브로드캐스트 메시지를 수신함
      2. 수신한 메시지를 유니캐스트 메시지에 캡슐화하여 DHCP 서버에 보냄
      3. DHCP 서버는 메시지의 필드를 확인하여 중계 에이전트로 온 메시지임을 식별하고 응답 메시지를 중계 에이전트에게 보냄
      4. 중계 에이전트가 클라이언트에게 메시지를 전달함



<그림 2> 다른 망에 존재하는 클라이언트와 서버

DHCP

- DHCP 동작 절차
  - UDP 포트
    - 서버는 메시지를 송, 수신할 때 잘 알려진 포트 (well-known port)를 사용함
      - 목적지 포트 번호가 동일한 메시지를 두 개 이상 보내지 않기 위함임
      - 클라이언트는 잘 알려진 포트 (Well-known port) 68을 사용하여 서버에게 요청 메시지를 보냄



<그림 3> UDP 포트의 사용

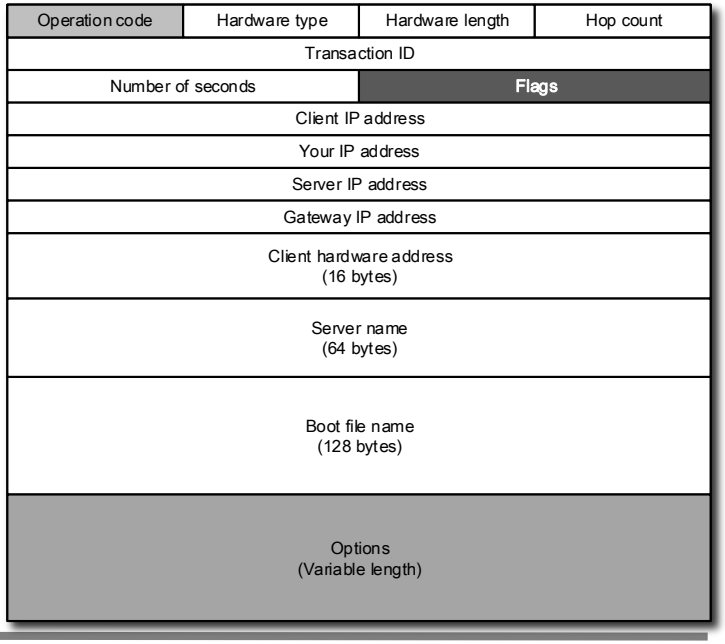
DHCP

- DHCP 동작 절차
  - 에러 제어
    - 개요
      - DHCP에서 사용하는 UDP는 에러 제어를 제공하지 않으므로 DHCP에서 에러 제어 기능을 제공함
    - 제어 방식
      - 체크섬
        - UDP 헤더와 데이터를 16비트씩 나눠 더한 값을 보수 처리하여 체크섬 필드에 넣어서 전송하도록 요구함
        - 수신한 데이터로 같은 계산을 다시 하여 결과가 동일하면 수신, 다르면 폐기함
      - 재전송
        - 클라이언트가 서버로부터 응답메시지를 받지 못하면 서버에게 Request 메시지를 재전송함
      - 타이머
        - 클라이언트들이 서버에 Request 메시지를 동시에 보내는 걸 방지하기 위해 클라이언트가 설정한 랜덤값임

DHCP

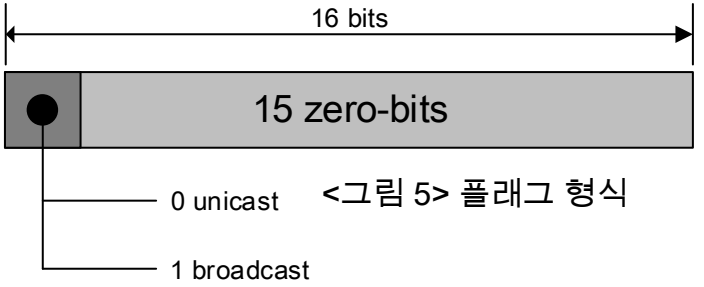
- DHCP 동작 절차
  - DHCP 패킷 형식 (1/5)
    - 동작 코드(Operation code)
      - DHCP 패킷의 종류를 나타내는 8비트 필드
        - 요청(Reply)은 1 응답(Request)는 2임
    - 하드웨어 유형(Hardware type)
      - 물리 네트워크 유형을 나타내는 8비트 필드
        - 망의 유형에 따라 정수 값을 할당받음
          - e.g., 이더넷의 경우 1임
    - 하드웨어 길이(Hardware length)
      - 물리 주소의 길이를 바이트 단위로 나타내는 8비트 필드
        - e.g., 이더넷의 경우 6임
    - 홉 개수(Hop count)
      - 패킷이 전달될 수 있는 최대 홉 개수를 나타내는 8비트 필드

<그림 4> DHCP 패킷 형식



DHCP

- DHCP 동작 절차
  - DHCP 패킷 형식 (2/5)
    - 트랜잭션 식별자(Transaction ID)
      - 클라이언트에 의해 설정되는 4바이트 필드
        - 요청에 대한 응답을 확인하기 위해 사용됨
        - 서버는 요청메시지 내에 있는 트랜잭션 식별자와 동일한 값을 응답메시지에 기록함
    - 초 단위 경과시간(Number of seconds)
      - 클라이언트가 부팅된 후 경과된 시간을 초 단위로 나타내는 16비트 필드
    - 플래그(Flags)
      - 해당 메시지가 브로드캐스트되야함을 나타내는 16비트 필드
        - 앞의 1비트가 0이면 유니캐스트, 1이면 브로드캐스트를 나타냄
        - 나머지 15비트 필드는 추가 기능을 위해 남겨놓음



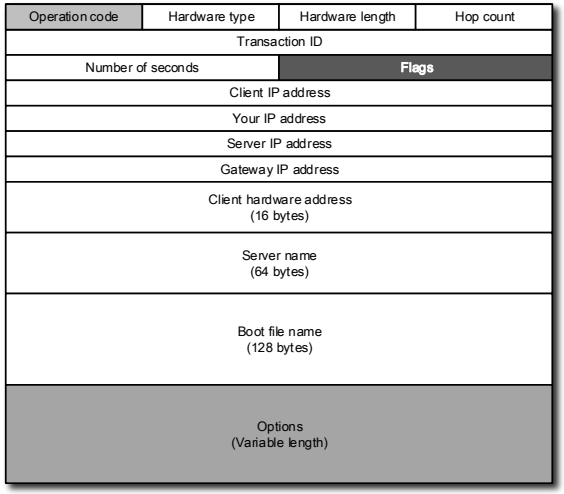
<그림 5> 플래그 형식

<그림 4> DHCP 패킷 형식

Operation code	Hardware type	Hardware length	Hop count
Transaction ID			
Number of seconds		Flags	
Client IP address			
Your IP address			
Server IP address			
Gateway IP address			
Client hardware address (16 bytes)			
Server name (64 bytes)			
Boot file name (128 bytes)			
Options (Variable length)			

DHCP

- DHCP 동작 절차
  - DHCP 패킷 형식 (3/5)
    - 클라이언트 IP 주소(Client IP address)
      - 클라이언트 IP 주소를 포함한 4바이트 필드
        - 클라이언트가 자신의 IP 주소에 대한 정보를 가지고 있지 않다면 모두 0으로 지정됨
    - 상대방 IP 주소(Your IP address)
      - 클라이언트 IP 주소를 포함하는 4바이트 필드
        - 요청을 받은 서버에 의해 응답 메시지에 기록됨
    - 서버 IP 주소(Server IP address)
      - 서버의 IP 주소를 포함하는 4바이트 필드
        - 서버는 자신의 IP 주소를 응답 메시지에 기록함
    - 게이트웨이 IP 주소(Gateway IP 주소)
      - 라우터의 IP 주소를 나타내는 4바이트 필드
        - 서버에 의해 응답 메시지에 기록됨

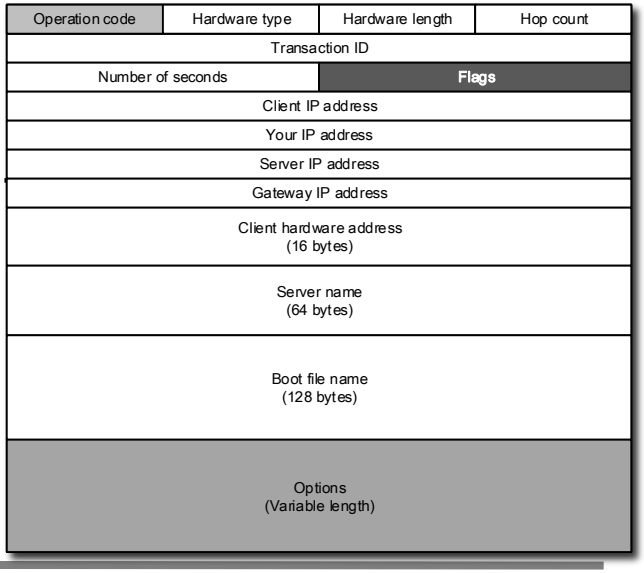


<그림 4> DHCP 패킷 형식

DHCP

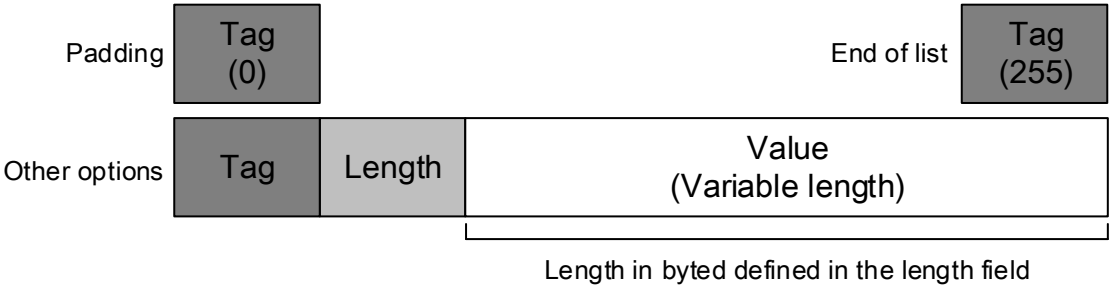
- DHCP 동작 절차
  - DHCP 패킷 형식 (4/5)
    - 클라이언트 하드웨어 주소(Client hardware address)
      - 클라이언트에 물리 주소를 나타내는 필드
        - 서버는 클라이언트가 보낸 주소에서 클라이언트 물리 주소를 알아낼 수 있음
    - 서버 이름(Server name)
      - 서버의 도메인 이름을 포함하는 64바이트 필드
        - 서버가 응답 메시지에 선택적으로 기록함
        - 널 문자열(Null string)으로 끝남
    - 부트 파일 이름(Boot filename)
      - 부트 파일의 전체 경로명을 포함한 128바이
        - 서버가 응답 메시지에 선택적으로 기록함
        - 클라이언트는 다른 부팅 정보들을 추출하기 위해 해당 경로를 사용할 수 있음
        - 서버가 데이터를 채우기 원하지 않으면 0으로 채워야만 함

<그림 4> DHCP 패킷 형식



DHCP

- DHCP 동작 절차
  - DHCP 패킷 형식 (5/5)
    - 옵션(Option)
      - 네트워크 마스크나 기본 라우터 주소와 같은 추가적인 정보를 전달하는 64바이트 필드
        - 서버가 IP 주소 형태로 응답 메시지에 기록함



<그림 6> 옵션 형식

[표 1] DHCP의 옵션들

Tag	Length	Value	Description
0	-	-	Padding
1	4	Subnet mask	Subnet mask
2	4	Time of the day	Time offset
3	Variable	IP addresses	Default router
4	Variable	IP addresses	Time server
5	Variable	IP addresses	IEN 16 server
6	Variable	IP addresses	DNS server
7	Variable	IP addresses	Log server
8	Variable	IP addresses	Quote server
9	Variable	IP addresses	Print server
10	Variable	IP addresses	Impress
11	Variable	IP addresses	RLP server
12	Variable	DNS name	Host name
13	2	Integer	Boot file size
53	1	Discussed later	Used for dynamic configuration
128~254	Variable	Specific information	Vendor specific
255			End of list

DHCP

- DHCP 주소 설정
  - 고정 주소 할당
    - 개요
      - DHCP 서버가 클라이언트에게 고정된 IP 주소를 할당하는 방식
    - 동작 방식
      - 클라이언트가 IP 주소를 요구했을 때 물리 주소와 매핑된 IP 주소가 데이터베이스에 존재하면 서버가 IP 주소를 할당함
    - 특징
      - IP 주소가 변하지 않아 다른 장비가 항상 같은 주소로 확인 가능함
        - 서버, 프린터, 라우터 같은 장비에 적합함
    - 한계점
      - 사용하지 않는 호스트에도 IP 주소를 계속 할당해야함
      - IP 주소가 고정이라 한 번 노출되면 지속적으로 위협에 노출될 수 있음

DHCP

- DHCP 주소 설정
  - 동적 주소 할당
    - 개요
      - DHCP 서버가 클라이언트에게 임시로 IP 주소를 할당하는 방식
    - 동작 방식
      - 클라이언트가 IP 주소를 요구했을 때 물리 주소와 매핑된 IP 주소가 데이터베이스에 존재하지 않으면 서버가 IP 주소를 할당하고 동적 데이터베이스에 항목을 추가함
    - 특징
      - 주소 임대기간(lease)이 끝나게 되면 클라이언트는 주소를 반납하거나 임대를 새로 요청해야함
      - 호스트가 한 망에서 다른 망으로 이동하는 경우에 필요함
    - 한계점
      - IP가 계속 변하므로 추적과 감시가 어려움

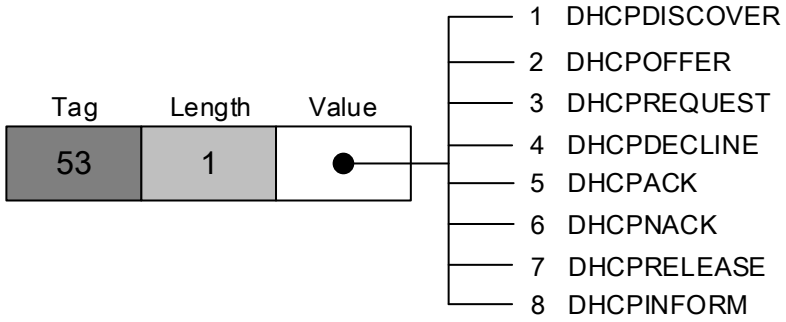


<그림 7> 동적 IP주소 할당의 임대 시스템

DHCP

- DHCP 주소 설정
  - 상태 천이(State transition)*
    - 개요
      - DHCP 클라이언트가 IP 주소를 할당 받고 반납하기까지의 과정을 상태(state)와 상태 간 이동(transition)으로 나타낸 방식
    - 특징
      - DHCP 클라이언트는 수신하거나 전송되는 메시지에 근거하여 동작함
      - 메시지 형식은 DHCP 패킷에 포함된 53번 옵션에 의해 정의됨

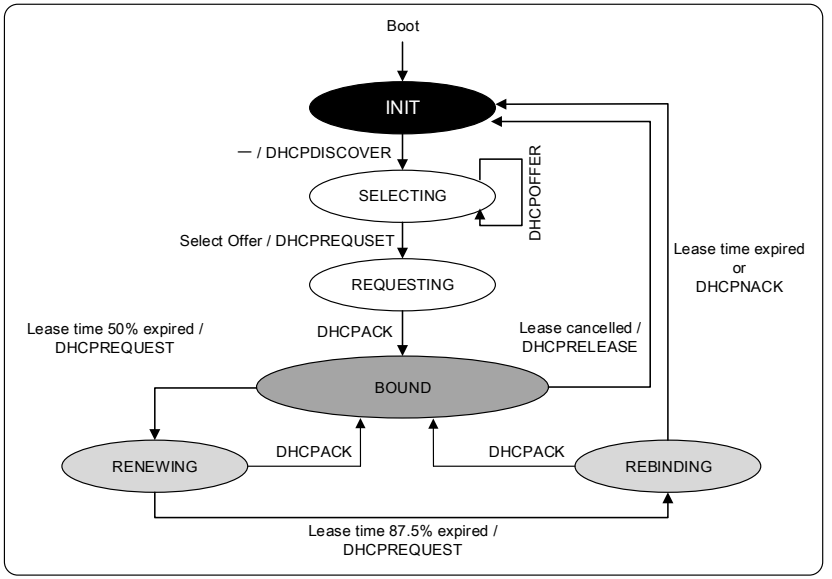
*천이
프로그램이나 프로세스 등이 특정 입력이나 신호를 받아 현재 상태에서 다음 상태로 이동하는 것



<그림 8> 태그 53을 가지는 옵션

DHCP

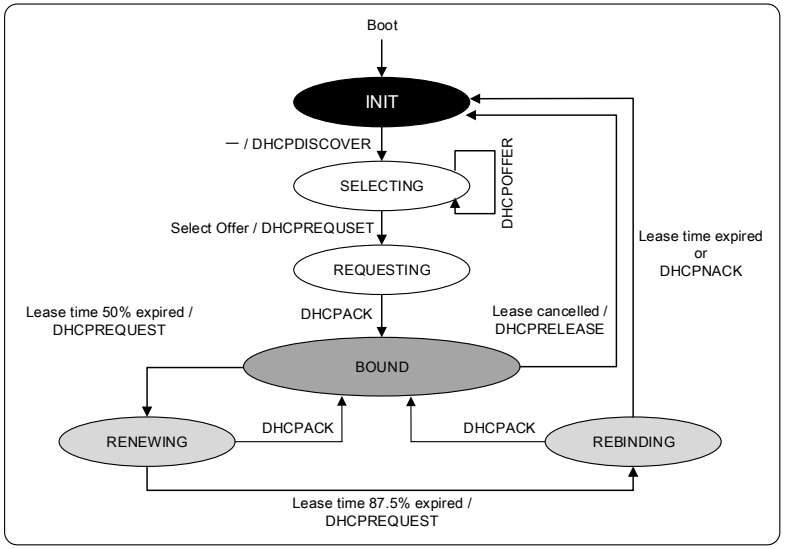
- DHCP 주소 설정
  - 상태 천이
    - 종류 (1/3)
      - 초기 상태(INIT)
        - DHCP 클라이언트가 처음 시작된 상태임
        - 클라이언트는 DHCPDISCOVER 메시지를 67번 포트를 사용하여 브로드캐스트함
      - 선택 상태(SELECTING)
        - 서버로부터 사용 가능한 IP 주소 목록을 받기를 기다리는 상태임



<그림 9> DHCP 클라이언트 상태 천이도

DHCP

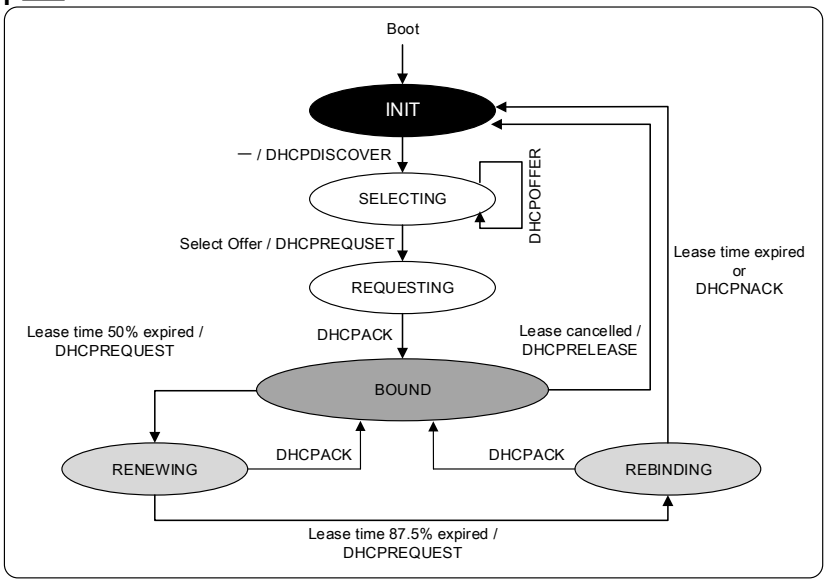
- DHCP 주소 설정
  - 상태 천이
    - 종류 (2/3)
      - 요청 상태(REQUESTING)
        - 클라이언트의 물리 주소와 선택 상태에서 골랐던 IP 주소 간의 매핑 정보 생성을 기다리는 상태임
      - 바운드 상태(BOUND)
        - 클라이언트가 IP 주소를 사용하는 상태임
        - 임대 기간의 50%가 지나면 클라이언트는 다른 DHCPREQUEST 메시지를 보내 임대 기간을 새롭게 설정함
        - 임대를 취소하고 초기 상태로 갈 수 있음



<그림 9> DHCP 클라이언트 상태 천이도

DHCP

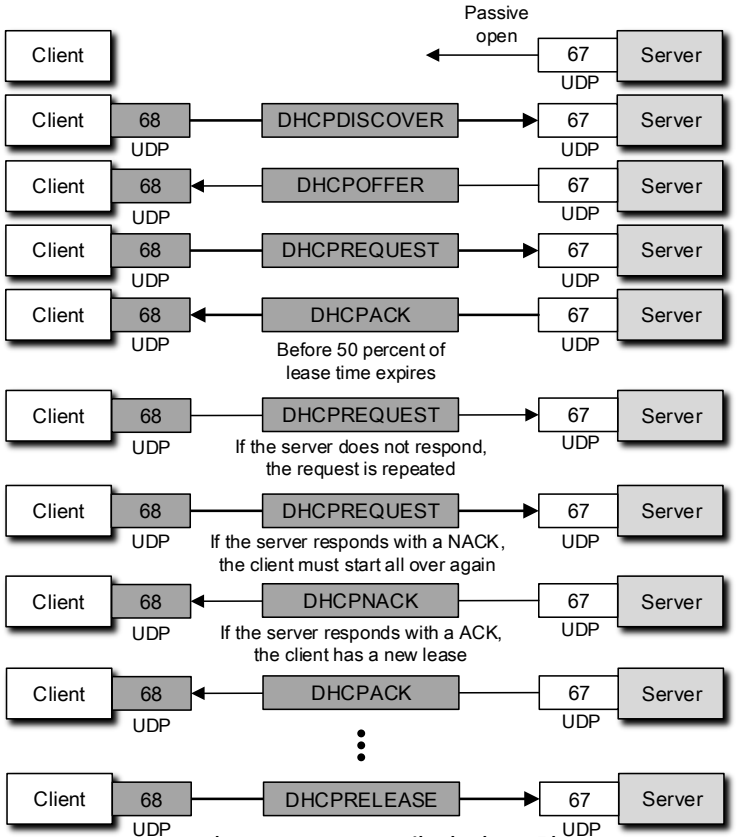
- DHCP 주소 설정
  - 상태 천이
    - 종류 (3/3)
      - 재설정 상태(RENEWING)
        - 클라이언트가 새로운 IP 임대 계약을 위해 다른 DHCPREQUEST 메시지를 보낸 상태임
      - 재연결 상태(REBINDING)
        - 서버로부터 DHCPACK를 수신하지 못하고 임대 기간이 87.5% 가 지난 상태임
        - DHCPACK 를 수신하거나 임대 기간이 만료되면 초기 상태로 돌아가고 다른 IP 주소 임대를 시도함



<그림 9> DHCP 클라이언트 상태 천이도

DHCP

- DHCP 주소 설정
  - DHCP 메시지 교환
    - 동작 과정 (1/2)
      1. 클라이언트는 DHCPDISCOVER 메시지를 67번 포트를 사용하여 브로드캐스트함
      2. 서버가 DHCPOFFER 메시지에 IP 주소를 담아 응답함
         - 제공한 IP 주소는 다른 클라이언트가 사용하지 못하게 함
         - 클라이언트가 DHCPOFFER 메시지를 받지 못하면 2초 간격으로 4번 재시도함
         - 재시도에도 응답이 없으면 5분 동안 기다린 후 재시도함
      3. 클라이언트는 IP 주소를 선택하고 DHCPREQUEST 메시지를 전송함
         - 클라이언트는 IP 주소를 선택하고 DHCPREQUEST 메시지를 전송한 후 요청 상태로 천이함

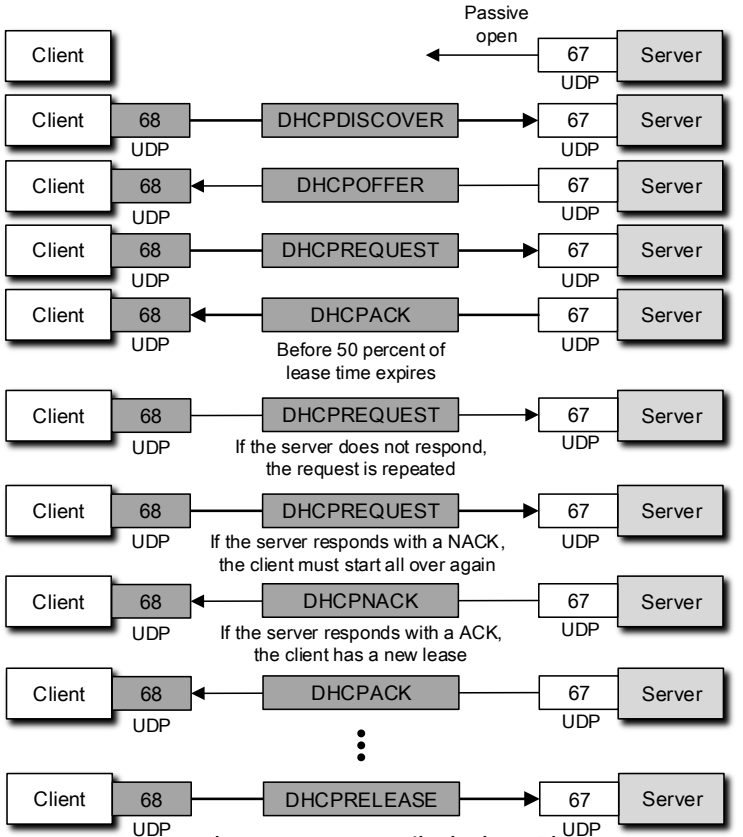


<그림 10> DHCP 메시지 교환

DHCP

- DHCP 주소 설정
  - DHCP 메시지 교환
    - 동작 과정 (2/2)

4. 클라이언트가 DHCPACK 메시지를 받으면 임대가 만료될 때까지 IP 주소를 사용함
   - 임대 기간의 50%가 지나면 클라이언트는 다른 DHCPREQUEST 메시지를 보내 임대 기간을 새롭게 설정함
   - 서버로부터 DHCPACK를 수신하지 못하고 임대 기간이 87.5% 가 지나는 경우 재연결 상태로 천이함



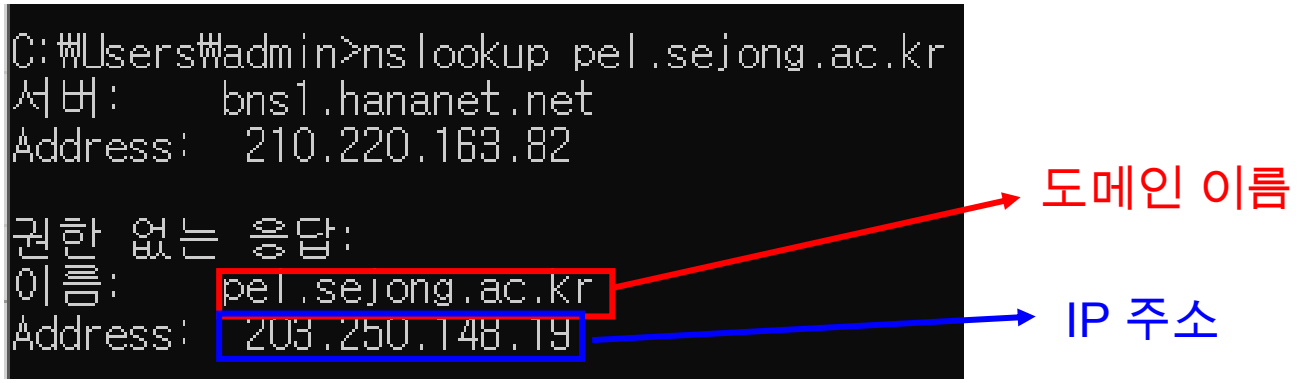
<그림 10> DHCP 메시지 교환

목 차

- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)

DNS

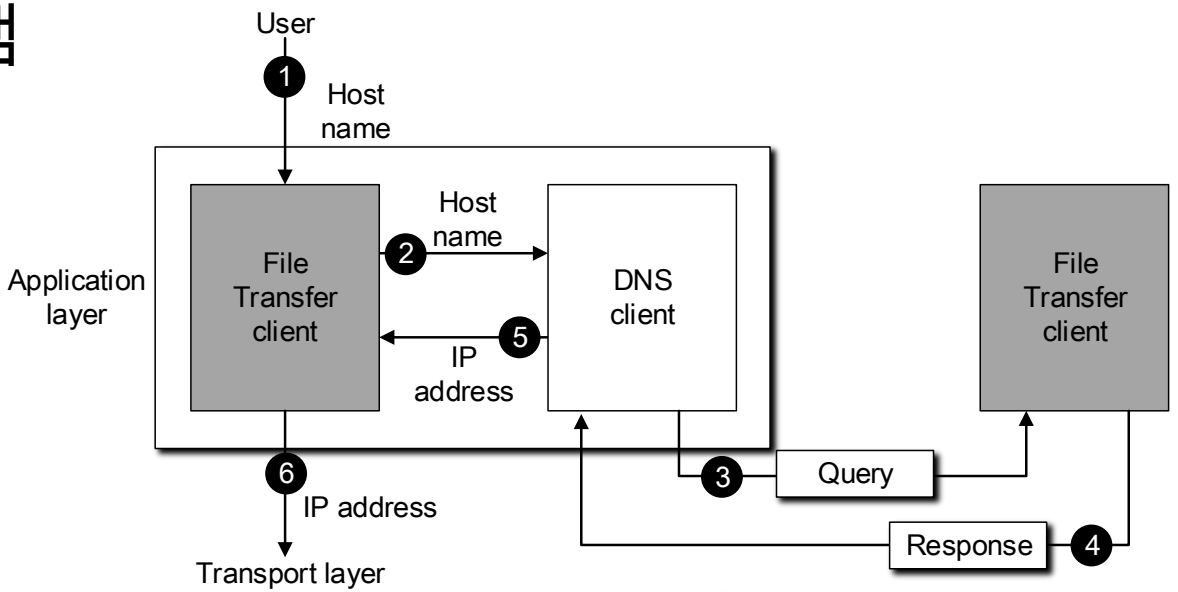
- DNS (Domain Name Systems)
  - 정의
    - TCP/IP 프로토콜에서 도메인 이름을 컴퓨터가 식별하도록 IP 주소로 변환하는 프로토콜
      - 도메인(Domain)
        - 인터넷에 연결된 컴퓨터를 사람이 쉽게 기억하고 입력할 수 있도록 문자로 만든 인터넷 주소
  - 특징
    - 도메인 이름을 트리 구조로 하여 구성함
    - 분산 데이터베이스를 사용함



<그림 11> 도메인 이름과 매핑된 IP 주소

DNS

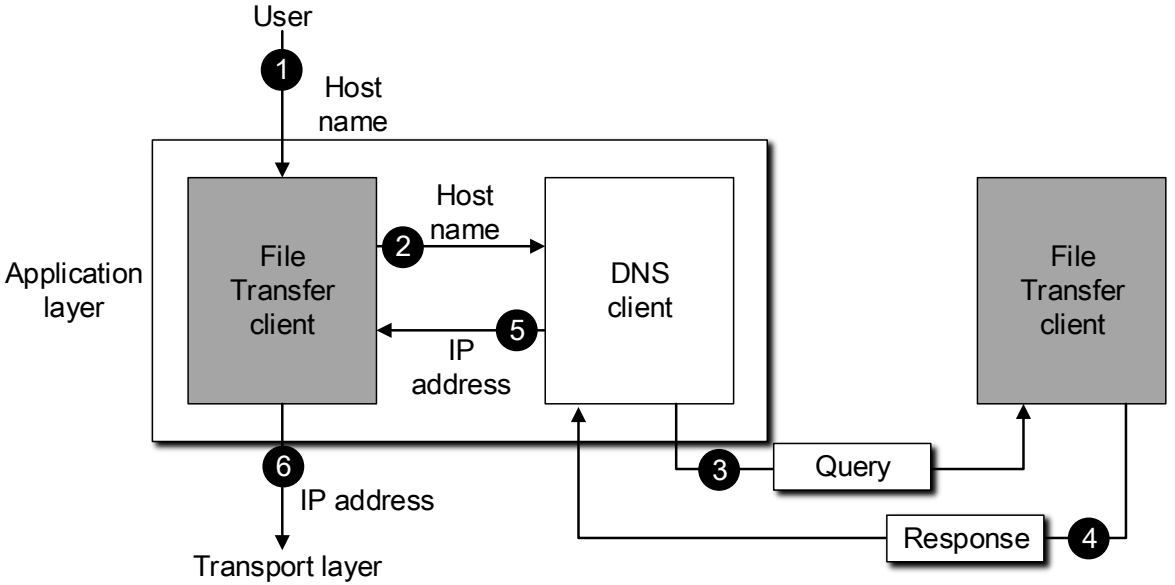
- DNS (Domain Name Systems)
  - 동작 과정 (1/2)
    1. 사용자는 호스트 이름을 파일 전송 클라이언트에 전달함
    2. 파일 전송 클라이언트는 호스트 이름을 DNS 클라이언트에 전달함
    3. DNS 클라이언트는 DNS 서버의 알려진 주소를 사용하여 호스트 이름에 매핑되는 IP 주소를 질의하는 메시지를 DNS 서버에 보냄



<그림 12> DNS 동작 과정

DNS

- DNS (Domain Name Systems)
  - 동작 과정 (2/2)
    4. DNS 서버는 원하는 IP 주소를 응답함
    5. DNS 클라이언트는 IP 주소를 파일 전송 클라이언트에 전달함
    6. 파일 전송 클라이언트는 수신한 IP 주소를 사용하여 파일 전송 서버에 접속함



<그림 12> DNS 동작 과정

DNS

- 네임 공간(Name space)
  - 개요
    - 장치의 이름과 IP 주소 간의 매핑을 담당하는 공간
  - 특징
    - IP 주소에 매핑되는 호스트의 이름은 유일해야함
  - 종류
    - 단층적 네임 공간(Flat name space)
    - 계층적 네임 공간(Hierarchical name space)
    - 도메인 네임 공간(Domain name space)

DNS

- 네임 공간
  - 단층적 네임 공간(Flat name space)
    - 정의
      - 호스트의 이름을 하나의 문자열로 정하고 IP 주소에 매핑하는 방식
    - 특징
      - 이름들이 중복되지 않고 사용되기 위해선 중앙에서 전체적으로 관리해야함
      - 매핑되는 이름을 바로 테이블에서 찾아 연결해줌
    - 한계점
      - 호스트 수가 많아질수록 중앙 서버의 부담이 커짐
        - 수억 개의 호스트를 가진 인터넷에서는 사용할 수 없음



<그림 13> 단층적 이름 공간

DNS

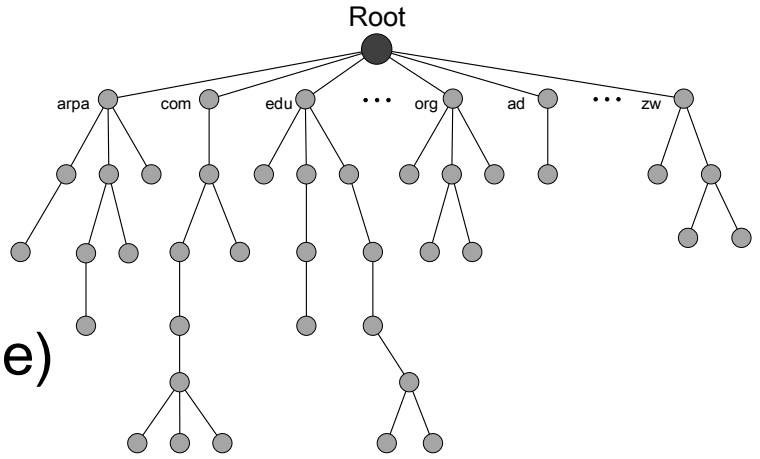
- 네임 공간
  - 계층적 네임 공간(Hierarchical name space)
    - 정의
      - 호스트의 이름을 여러 부분으로 나누어 저장하는 방식
    - 특징
      - 호스트의 이름을 루트에서 시작하는 형태의 계층 구조로 구성하여 주소에 할당함
      - 이름 정보를 여러 네임 서버에 나눠 저장하고 루트부터 한 단계씩 내려가며 주소를 찾음
      - 나누어진 각 부분은 호스트의 소속과 위치를 나타냄



<그림 14> 계층적 이름 공간

DNS

- 네임 공간
  - 도메인 네임 공간 (Domain name space)
    - 정의
      - 계층적 네임 공간을 구현하기 위해 설계된 역 트리 형태의 이름 구조
    - 특징
      - 트리는 0에서 127까지의 128 레벨을 가짐
      - 모든 트리는 루트에서 연결되며 트리의 각 레벨이 계층 레벨을 나타냄
    - 구성 요소
      - 레이블(Lable)
      - 도메인 네임(Domain name)
      - FQDN (Fully Qualified Domain Name)
      - PQDN (Partially qualified domain name)

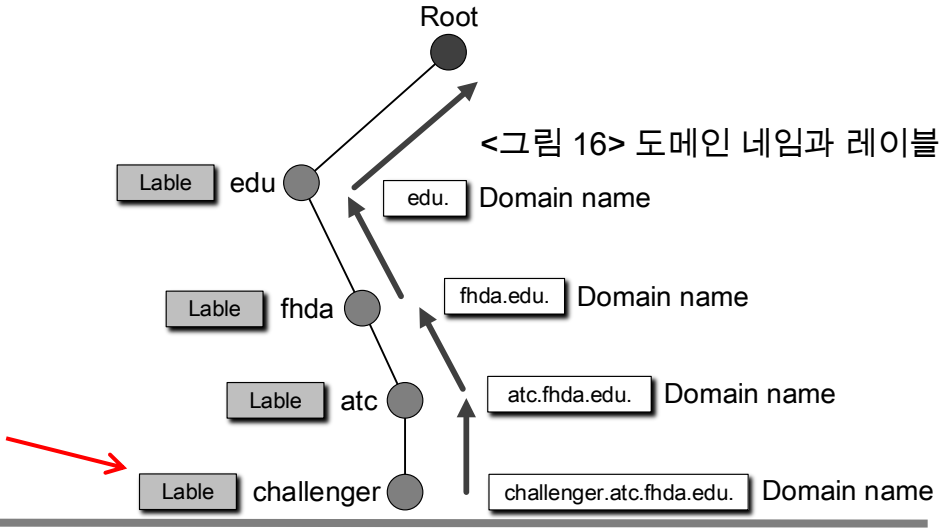


<그림 15> 도메인 네임 공간

DNS

- 도메인 네임 공간
  - 레이블(Lable)
    - 정의
      - 트리의 각 노드가 가지는 문자열
    - 특징
      - 동일 노드에서 연결되어 지는 노드들을 자식 노드라고 함
        - 자식 노드들은 다른 레이블을 가질 수 있도록 하여 도메인 네임의 유일성을 보장함
      - 최소 1글자에서 최대 63글자로 구성되어 있음
      - 루트의 레이블은 빈 문자열임

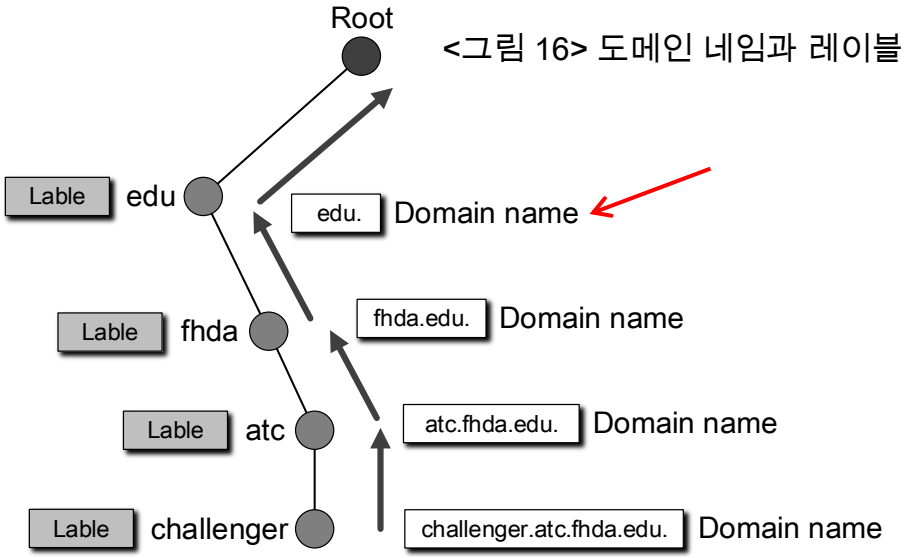
*pel.sejong.ac.kr 에서 pel, sejong, ac, kr 이 레이블임



<그림 16> 도메인 네임과 레이블

DNS

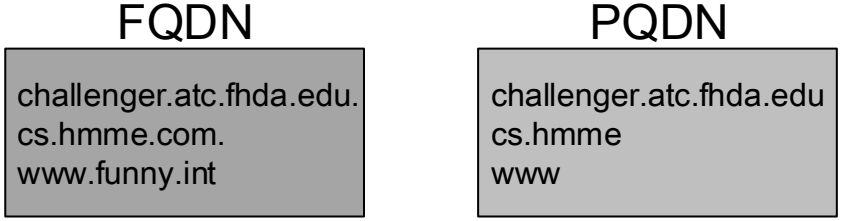
- 도메인 네임 공간
  - 도메인 네임(Domain name)
    - 정의
      - 숫자로 된 IP 주소를 사람이 기억하기 쉽도록 문자로 만든 웹 주소
    - 특징
      - 점(.)으로 구분되는 레이블의 연속으로 이루어짐
      - 노드에서 루트 방향으로 읽음
      - 루트의 레이블이 널이기 때문에 도메인 네임은 항상 널로 끝남



<그림 16> 도메인 네임과 레이블

DNS

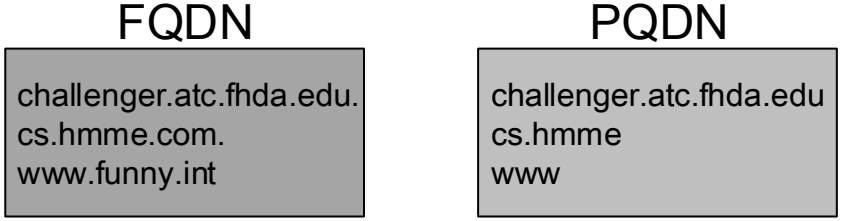
- 도메인 네임 공간
  - FQDN (Fully Qualified Domain Name)
    - 정의
      - 호스트를 정확하게 식별할 수 있는 완전한 도메인 네임
    - 특징
      - DNS 서버는 하나의 주소에 대해 하나의 FQDN만을 가질 수 있음
        - e.g., pel.sejong.ac.kr.은 FQDN임
      - 도메인 네임은 항상 널 레이블로 끝나야 하지만 널 레이블은 아무 의미가 없으므로 점(.)으로 표기함



<그림 17> FQDN과 PQDN

DNS

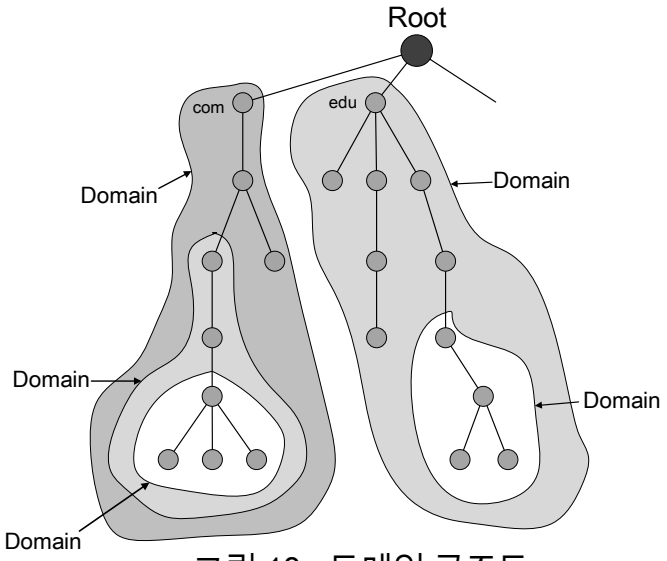
- 도메인 네임 공간
  - PQDN (Partially qualified domain name)
    - 정의
      - 노드에서 시작하지만 루트까지 가지 않는 도메인 네임
    - 특징
      - 텍스트로 쓸 때 마지막에 점(.)이 붙지 않음
      - 사용자가 PQDN을 입력하면 해석기(Resolver)가 미리 설정된 서픽스(suffix)를 붙여 FQDN을 만듦
        - pel를 입력하면 해석기가 sejong.ac.kr.을 붙임



<그림 17> FQDN과 PQDN

DNS

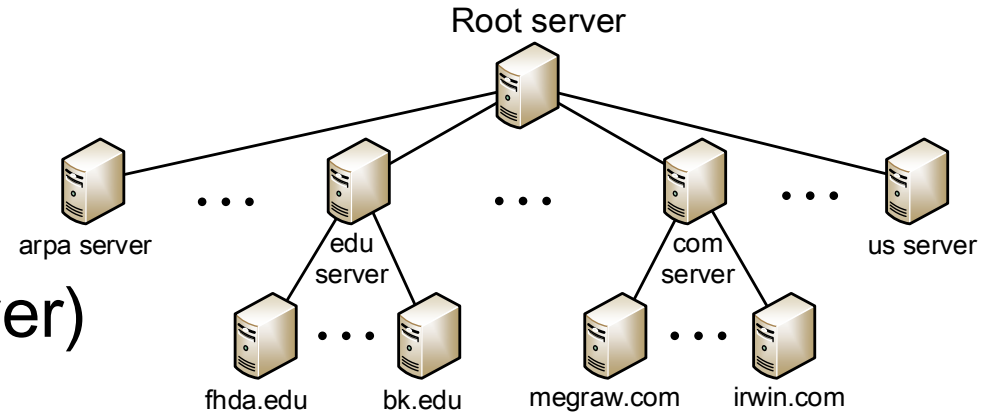
- 도메인(Domain)
  - 정의
    - 인터넷에 연결된 컴퓨터를 사람이 쉽게 기억하고 입력할 수 있도록 문자로 만든 인터넷 주소
  - 특징
    - 도메인 네임 공간의 서브 트리임
    - 도메인 자체가 다른 도메인 혹은 서브 도메인으로 나뉠 수 있음



<그림 18> 도메인 구조도

DNS

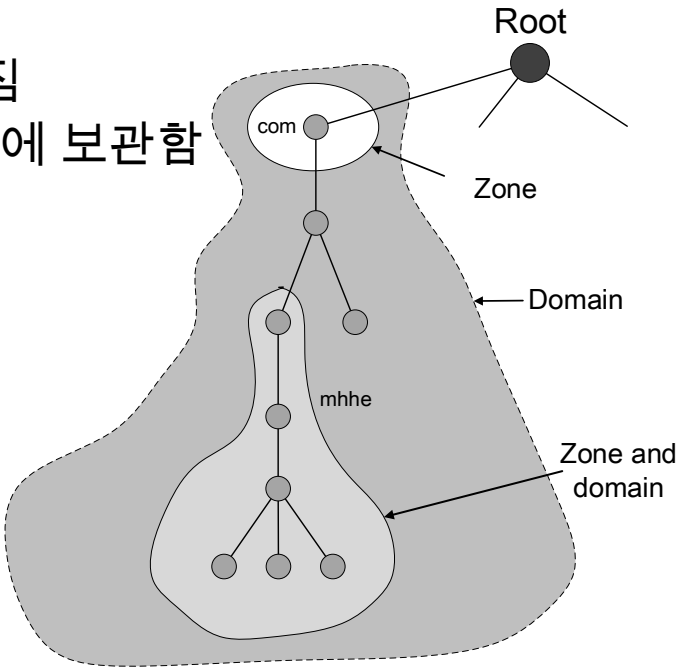
- 네임 서버의 계층
  - 개요
    - 도메인 네임 공간에 포함된 정보를 저장하기 위해 DNS 서버에 정보를 분산시킴
  - 특징
    - 루트를 독립적으로 두고 첫 번째 레벨의 노드만큼 도메인을 둠
    - 도메인을 더 작은 도메인인 서브 도메인으로 나눌 수 있음
  - 구성 요소
    - 영역(Zone)
    - 루트 서버(Root server)
    - 일차 서버(Primary server)
    - 이차 서버(Secondary server)



<그림 19> 네임 서버의 계층

DNS

- 네임 서버의 계층
  - 구성 요소 (1/3)
    - 영역(Zone)
      - 정의
        - 서버가 도메인을 관리하는 범위
      - 특징
        - 서버는 영역 파일이라는 데이터베이스를 가짐
          - 도메인 내의 모든 노드 정보를 영역 파일에 보관함
        - 서버가 도메인을 서브 도메인으로 나누고 다른 서버에 권한을 이양할 수 있음
          - 서브 도메인의 노드에 대한 정보는 더 낮은 레벨의 서버에 저장되고 기존 서버는 더 낮은 레벨의 서버에 대한 참조 정보만 가지게 됨



<그림 20> 영역과 도메인

DNS

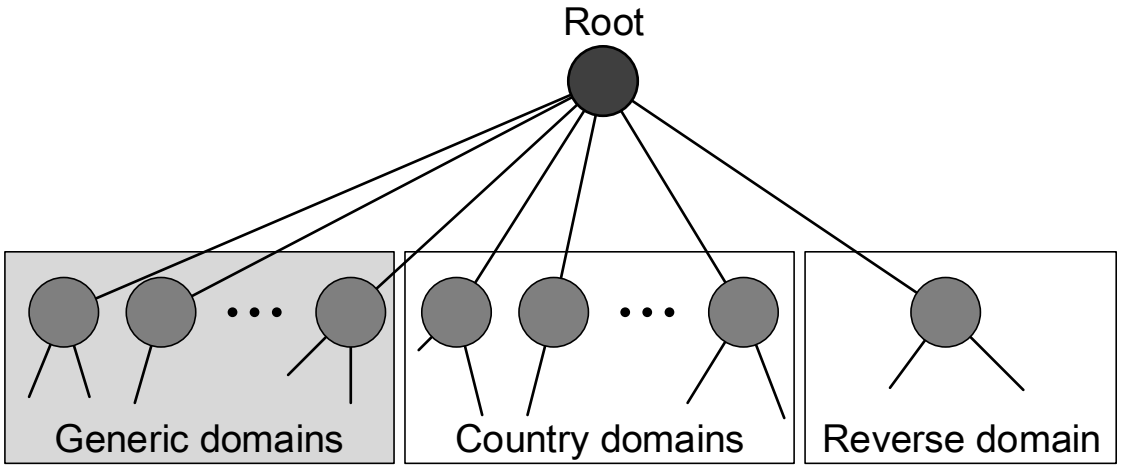
- 네임 서버의 계층
  - 구성 요소 (2/3)
    - 루트 서버(Root server)
      - 정의
        - 전체 트리를 영역으로 가지는 서버
      - 특징
        - 도메인에 대해 직접 알려주지는 않지만 해당 도메인으로 가기 위해선 어느 서버에 물어봐야 하는지를 알려줌
    - 일차 서버(Primary server)
      - 정의
        - 자신이 권한을 가지는 영역에 대한 파일을 가지는 서버
      - 특징
        - 영역 파일에 대한 생성, 관리, 갱신에 대한 책임을 가지며 로컬 디스크에 영역 파일을 저장함

DNS

- 네임 서버의 계층
  - 구성 요소 (3/3)
    - 이차 서버(Secondary server)
      - 정의
        - 다른 서버로부터 영역에 관한 완전한 정보를 수신하여 로컬 디스크에 파일을 저장하는 서버
      - 특징
        - 영역 파일을 생성하거나 갱신하지 않음
          - 갱신이 필요하면 일차 서버에서 이루어진 후 이차 서버로 보냄

DNS

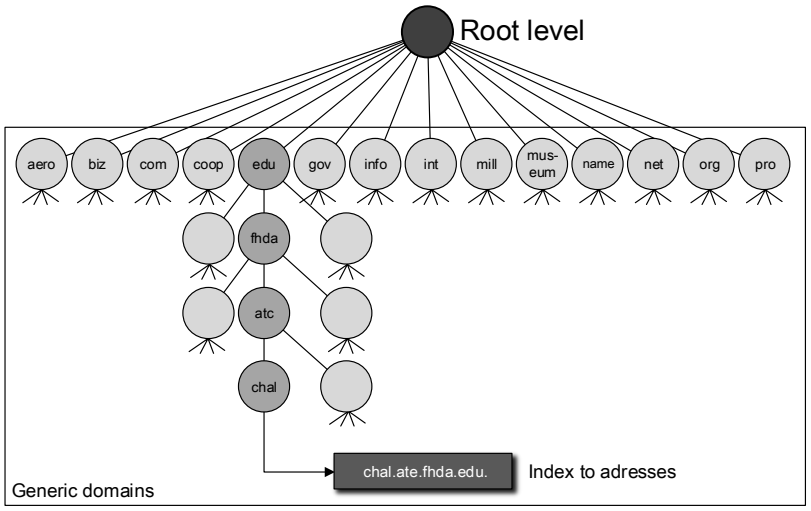
- 인터넷에서 사용되는 도메인 네임 공간
  - 종류
    - 일반 도메인(Generic domains)
    - 국가 도메인(Country domains)
    - 리버스 도메인(Reverse domain)
    - 레지스트라(Registrar)



<그림 21> 인터넷에서 사용되는 도메인 네임 공간

DNS

- 인터넷에서 사용되는 도메인 네임 공간
  - 일반 도메인(Generic domains)
    - 정의
      - 특정 구가나 지역에 상관없이 목적에 따라 누구나 사용할 수 있도록 만들어진 최상위 도메인
    - 특징
      - 도메인 네임을 보고 기관의 성격을 알 수 있음



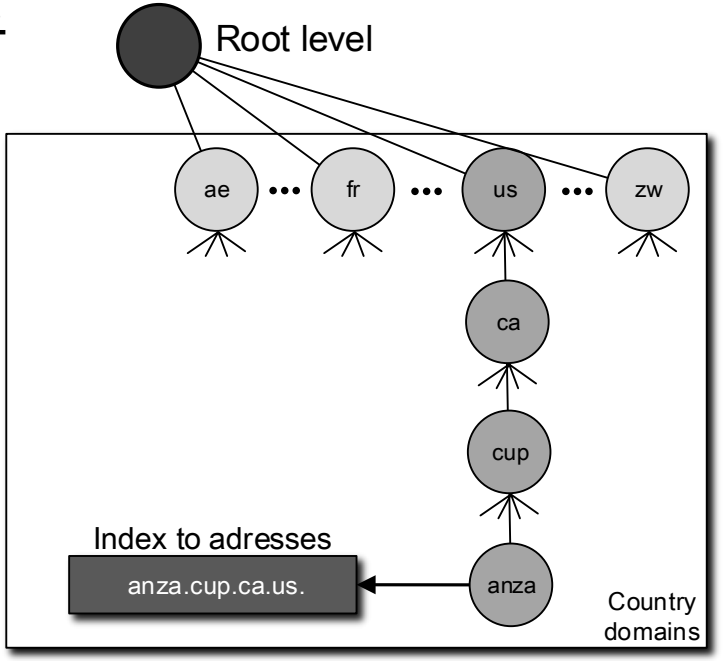
<그림 22> 일반 도메인

Parameter	Description
aero	항공사와 항공우주 기업 전용 도메인
biz	사업 전용 도메인
com	영리 단체 전용 도메인
coop	협동 단체 전용 도메인
edu	교육 기관 전용 도메인
gov	미국 정부 기관 전용 도메인
info	정보 서비스 제공자 전용 도메인
int	국제법 절차에 따라 결성된 국제 기관 전용 도메인
mil	미군 전용 도메인
museum	박물관, 미술관 전용 도메인
name	개인 사용자 전용 도메인
net	네트워크 관련 사이트 전용 도메인 (현재는 제한 해제)
org	비영리단체 전용 도메인
pro	전문직종 전용 도메인

[표 2] 일반 도메인 종류

DNS

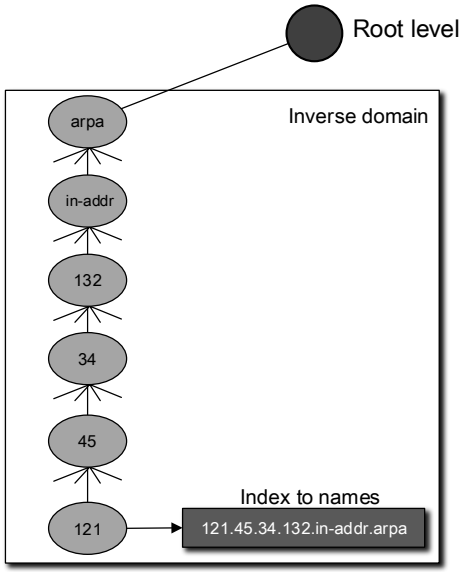
- 인터넷에서 사용되는 도메인 네임 공간
  - 국가 도메인(Country domains)
    - 정의
      - 특정 국가나 지역을 나타내기 위해 부여한 최상위 도메인
    - 특징
      - ISO 3166(나라 이름 코드 표준)에 따라 두 글자로 구성됨
      - 한국(.kr), 미국(.us), 일본(.jp) 등이 있음



<그림 23> 국가 도메인

DNS

- 인터넷에서 사용되는 도메인 네임 공간
  - 리버스 도메인(Reverse domains)
    - 정의
      - IP 주소를 도메인 이름으로 변환하는데 사용되는 도메인
    - 활용 사례
      - 메일을 보낸 서버의 IP를 역방향으로 조회해서 스팸인지 아닌지 확인함
      - 접속한 클라이언트의 IP로 이름을 확인하여 허가된 호스트인지 판단함
    - 특징
      - IP 주소를 할당 받은 기관이 관리함
        - 보통 통신사가 관리하는 경우가 많음
      - IP 주소를 거꾸로 적어 표현함



<그림 24> 인버스 도메인

DNS

- 인터넷에서 사용되는 도메인 네임 공간
  - 레지스트라(Registrar)
    - 정의
      - 새로운 도메인을 DNS에 추가해주는 기관
    - 특징
      - ICANN (International Corporation for Assigned Names and Numbers, 국제인터넷주소관리기구)의 승인을 받은 공인 대행 기관임
      - 요청된 도메인 네임이 유일한지를 확인한 후 DNS 데이터베이스에 삽입함
        - DNS 데이터베이스에 삽입할 때 요금을 부과함

DNS

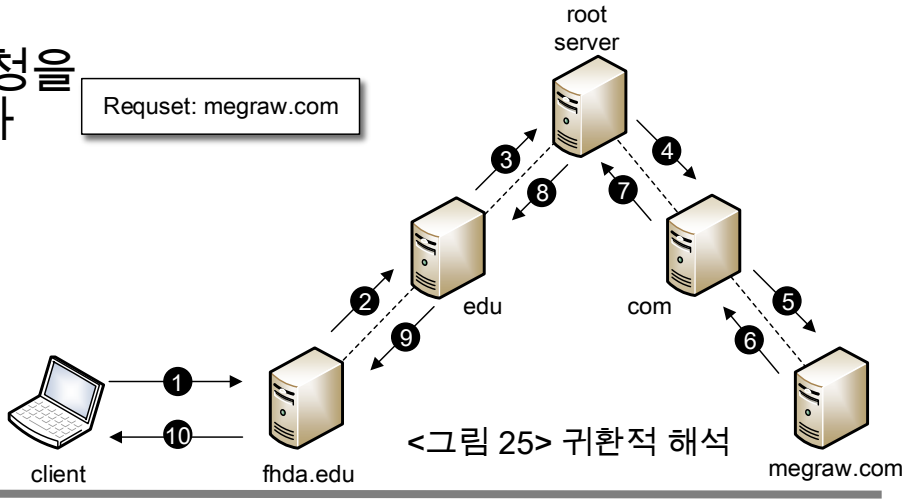
- DNS 해석
  - 개요
    - DNS는 이름–주소 해석을 이용해 도메인 이름을 IP 주소로 변환하거나 IP 주소를 도메인 이름으로 변환함
      - 이름을 주소로 매핑하거나 주소를 이름으로 매핑하는 것을 이름-주소 해석(name-address resolution)이라고 함
  - 동작 과정
    1. 해석기 호출
    2. 이름으로 주소를 매핑 / 주소로 이름을 매핑
    3. 귀환적 해석 / 반복적 해석
    4. 캐싱

DNS

- DNS 해석
  - 동작 과정 (1/4)
    1. 해석기 호출
       - 호스트는 해석기라고 불리는 DNS 클라이언트를 호출함
         - 해석기(Resolver)
           - 도메인 이름을 IP 주소로 바꿔달라고 요청하고 답을 받아오는 구성 요소
    2. 이름으로 주소를 매핑 / 주소로 이름을 매핑
       - 이름으로 주소를 매핑
         - 해석기는 도메인 네임을 서버에 주고 해당 주소를 질의(Query)로 요청함
         - 서버는 매핑을 찾기 위해 일반 도메인 혹은 국가 도메인을 검색함
       - 주소로 이름을 매핑
         - 해석기는 도메인 네임을 찾기 위해 IP 주소를 서버에 질의하기도 함
           - IP 주소를 질의하는 경우 인버스 도메인을 사용함

DNS

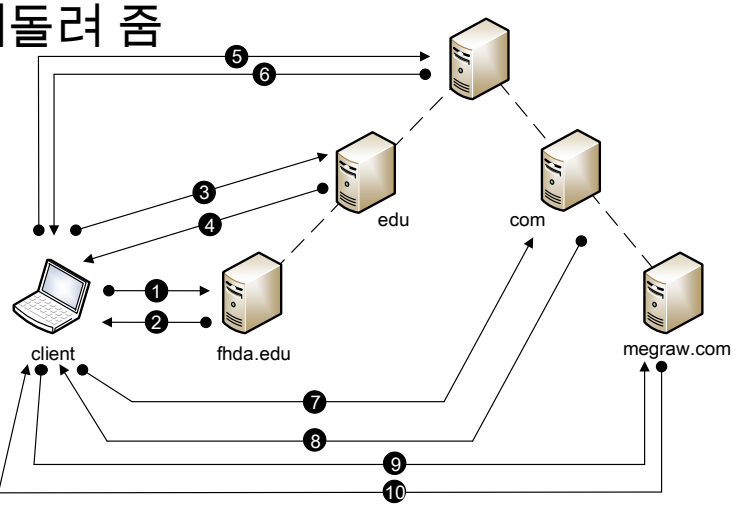
- DNS 해석
  - 동작 과정 (2/4)
    3. 귀환적 해석 / 반복적 해석
       - 귀환적 해석(Recursive resolve)
         - 해석기는 네임 서버에 귀환적인 응답을 요청할 수 있음
           - 서버로부터 최종적인 해석 결과를 얻을 수 있다고 기대함
         - 서버가 도메인 네임에 대한 권한을 가진다면 데이터베이스를 찾아본 뒤 응답함
         - 서버가 도메인 네임에 대한 권한이 없다면 다른 서버에게 요청을 보내고 응답을 기다림
           - 다른 서버가 권한을 가진다면 응답을 하고 그렇지 않다면 또 다른 서버에게 질의를 보냄
         - 질의가 최종적으로 해석이 되면 요청을 보낸 클라이언트에게 거슬러 올라가 응답을 전달함



<그림 25> 귀환적 해석

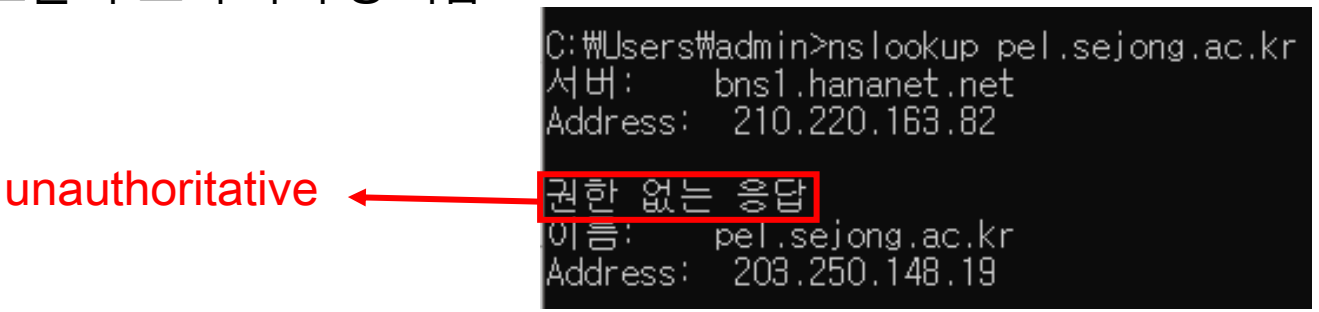
- DNS 해석
  - 동작 과정 (3/4)
    3. 귀환적 해석 / 반복적 해석
       - 반복적 해석(Iterative resolve)
         - 클라이언트가 귀환적 해석을 요청하지 않으면 매핑은 반복적으로 진행됨
         - 서버가 이름에 대한 권한을 가진다면 응답을 보냄
         - 권한이 없다면 질의를 해석할 수 있을 거 같은 서버의 IP 주소를 클라이언트에게 되돌려 줌
         - 클라이언트는 두 번째 서버에 질의를 반복할 의무를 가짐
         - 두 번째 서버가 이름에 대한 권한을 가진다면 응답을 보내고 그렇지 않다면 세 번째 서버의 IP 주소를 클라이언트에게 되돌려 줌

<그림 26> 반복적 해석



DNS

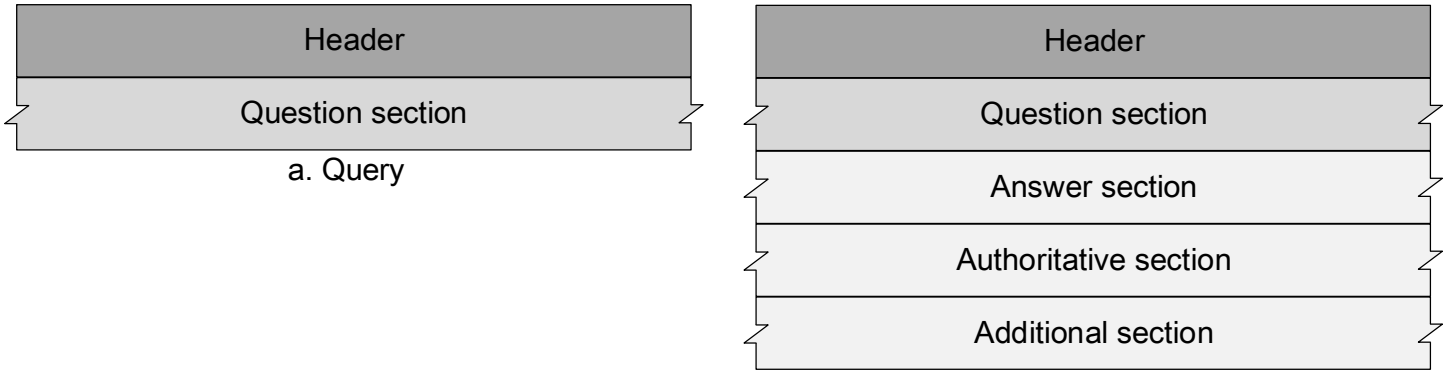
- DNS 해석
  - 동작 과정 (4/4)
    4. 캐싱(Caching)
       - 서버가 다른 서버에 매핑 정보를 요청하고 수신한 응답을 클라이언트에 전달하기 전에 저장함
       - 클라이언트가 동일한 매핑을 문의해오면 서버는 자신의 캐시 메모를 검색한 후 저장된 답을 응답함
         - 캐시를 사용해 보낸 답에는 'unauthoritative' 표시를 함
       - 주소 해석 속도를 높이지만 서버가 잘못된 매핑 정보를 보낼 수도 있음
         - 서버가 매핑 정보에다 TTL (Time To Live) 정보를 넣어 시간이 경과되면 매핑 정보를 무효화시켜 방지함



<그림 27> 캐싱을 사용한 IP 주소 탐색

DNS

- DNS 메시지
  - 개요
    - 도메인 네임을 IP주소로 변환하거나 IP 주소를 도메인 네임으로 변환하기 위해 클라이언트와 서버가 주고 받는 메시지
  - 종류
    - 질의 메시지(Query message)
    - 응답 메시지(Response message)



<그림 28> DNS 메시지 구조도

DNS

- DNS 메시지
  - 질의 메시지
    - 도메인 이름에 대응하는 IP 주소 등을 얻기 위해 클라이언트나 서버가 다른 DNS 서버에 보내는 요청 메시지
    - 헤더
      - 식별자
      - 플래그
      - 질의 레코드의 수
      - 응답 레코드의 수
      - 권한 레코드의 수
      - 추가 레코드의 수

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

<그림 29> DNS 메시지 헤더 형식

DNS

- DNS 메시지
  - 질의 메시지
    - 헤더 (1/4)

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

<그림 29> DNS 메시지 헤더 형식

      - 식별자
        - 클라이언트에서 질의에 대한 응답과의 비교를 위해 사용하는 16비트 필드
        - 클라이언트는 질의를 보낼 때마다 서로 다른 식별자 번호를 사용함
        - 서버는 해당 응답에 클라이언트가 사용한 식별자 번호를 복사하여 삽입함
      - 플래그
        - 서브 필드들로 구성되는 16비트 필드
        - QR (Query / Response)
          - 메시지의 종류를 나타내는 1비트 필드
          - 0이면 질의, 1이면 응답임
        - OpCode
          - 질의나 응답의 종류를 나타내는 4비트 필드
          - 0은 표준, 1은 인버스, 2는 서버 상태 요청임



<그림 30> 플래그 필드 형식

DNS

- DNS 메시지
  - 질의 메시지
    - 헤더 (2/4)
      - 플래그
        - AA (Authoritative Answer)
          - 응답 메시지에만 사용되는 1비트 필드
          - 네임 서버가 권한이 인정된 서버임을 나타냄
        - TC (Truncated)
          - 응답이 허용 바이트인 512 바이트를 초과했음을 알리는 1비트 필드
          - DNS가 UDP 서비스를 사용할 때 이용함
        - RD (Recursion Desired)
          - 클라이언트가 귀환적 응답을 바란다는 걸 나타내는 1비트 필드
          - 질의 메시지에서 지정되며 응답 메시지에서 반복됨
        - RA (Recursion Available)
          - 반복적인 응답이 가능함을 나타내는 1비트 필드
          - 응답 메시지에서만 지정됨

<그림 30> 플래그 필드 형식



- DNS 메시지
  - 질의 메시지
    - 헤더 (3/4)
      - 플래그
        - Reserved
          - 000으로 지정된 3비트 필드
        - rCode
          - 오류의 상태를 보여주는 4비트 필드
          - 권한이 인정된 서버만이 오류를 판단할 수 있음



<그림 30> 플래그 필드 형식

[표 3] rCode 값 종류

Value	Meaning	Value	Meaning
0	No error	4	Query type not supported
1	Format error	5	Administratively prohibited
2	Problem at name server	6-15	Reserved
3	Domain reference problem	-	-

DNS

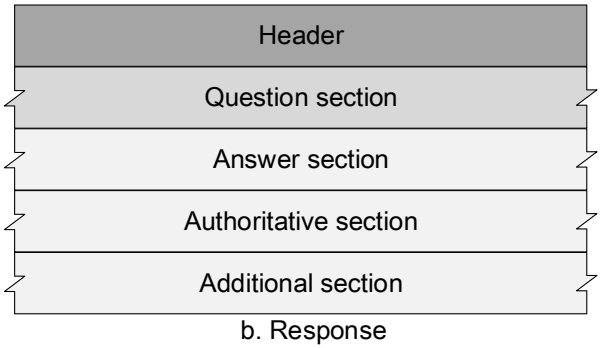
- DNS 메시지
  - 질의 메시지
    - 헤더 (4/4)
      - 질의 레코드의 수
        - 질의 섹션내의 질의 수를 포함하는 16비트 필드
      - 응답 레코드의 수
        - 응답 섹션에 있는 응답 수를 포함하는 16비트 필드
      - 권한 레코드의 수
        - 응답 메시지의 권한 섹션에 있는 권한 레코드의 수를 포함한 16비트 필드
      - 추가 레코드의 수
        - 응답 메시지의 추가 섹션에 있는 추가 레코드의 수를 포함한 16비트 필드

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

<그림 29> DNS 메시지 헤더 형식

DNS

- DNS 메시지
  - 응답 메시지
    - 문의 섹션(Question section)
      - 하나 이상의 문의레코드들로 구성되는 섹션
      - 질의와 응답 메시지에 모두 존재함
    - 응답 섹션(Answer section)
      - 하나 이상의 자원 레코드들로 구성되는 섹션
      - 응답 메시지에서만 존재함
    - 권한 섹션(Authoritative section)
      - 질의에 대한 하나 이상의 권한이 있는 서버에 대한 정보를 제공하는 섹션
      - 하나 이상의 자원 레코드들로 구성됨
    - 추가 정보 섹션(Additional section)
      - 해석기에게 도움이 될 만한 추가적인 정보를 제공하는 섹션
        - e.g., 서버가 다른 서버의 도메인 네임을 줄 때 자신이 권한이 있는 IP 주소 제공



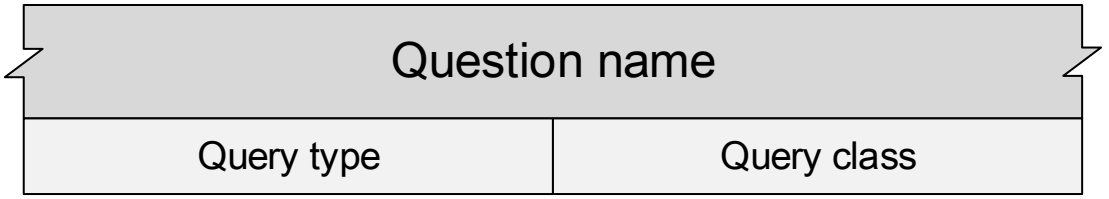
<그림 31> DNS 응답 메시지 구조도

DNS

- DNS 레코드
  - 정의
    - DNS 서버에 저장되는 텍스트 기반 지시 파일
  - 특징
    - 도메인에 매핑된 IP 주소 및 해당 도메인에 대한 요청의 처리 방법을 제공함
  - 종류
    - 질의 레코드(Query Record)
    - 자원 레코드(Resource Record)

DNS

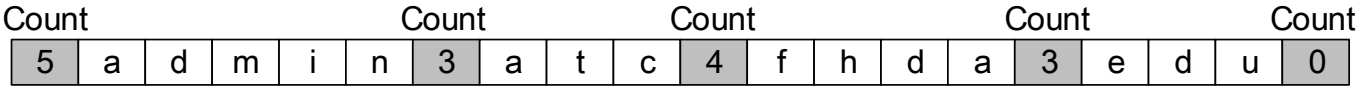
- DNS 레코드
  - 질의 레코드(Query record)
    - 정의
      - 클라이언트가 서버로부터 정보를 얻기 위해 사용하는 지시 파일
    - 구성 필드
      - 질의 이름(Query name)
      - 질의 종류(Query type)
      - 질의 클래스(Query class)



<그림 32> 질의 레코드 형식

DNS

- DNS 레코드



<그림 33> 질의 이름 형식

  - 질의 레코드(Query record)
    - 질의 이름(Query name)
      - 도메인 네임을 포함한 가변 길이 필드
    - 질의 종류(Query type)
      - 질의 종류를 나타내는 16비트 필드

[표 4] 질의 종류

Type	Mnemonic	Description
1	A(Address)	32비트 IPv4주소, 한 번에 주소를 찾을 수 있음
2	NS (Name Server)	해당 영역의 권한을 가진 서버를 알려줌
5	CNAME (Canonical name)	도메인 주소를 또 다른 도메인 주소로 이중 매핑시킴
6	SOA (Start Of Authority)	네임서버가 해당 도메인에 관해 인증된 데이터를 가지고 있음을 증명함
11	WKS (Well-Known Services)	호스트가 제공하는 네트워크 서비스를 정의함
12	PTR (Pointer)	IP 주소에 대한 도메인 주소를 확인할 때 사용함
13	HINFO (Host Information)	호스트의 하드웨어와 운영체제에 대한 정보를 얻는데 사용함
15	MX (Mail exchange)	메일 서버를 확인하는데 사용함
16	TXT	사람이 읽을 수 있는 설명을 도메인에 추가할 때 사용됨
28	AAAA (Address)	128비트 IPv6주소, 한 번에 주소를 찾을 수 있음
252	AXFR	영역 전체를 전송해달라는 요청임
255	ANY	모든 레코드를 달라는 요청임

DNS

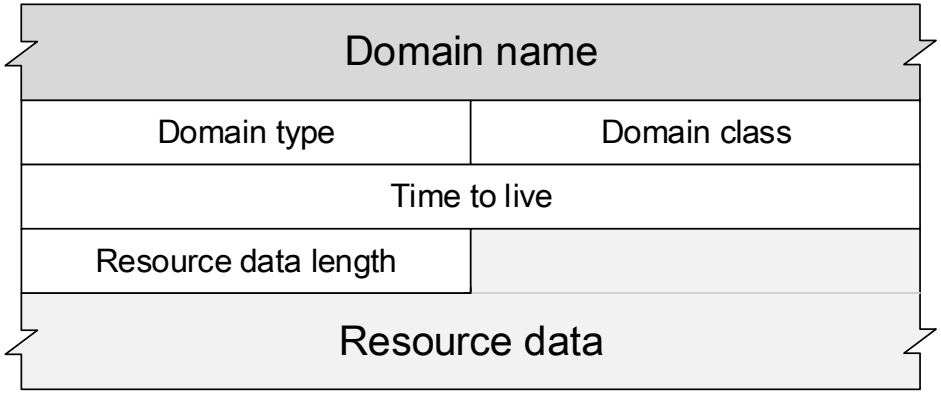
- DNS 레코드
  - 질의 레코드(Query record)
    - 질의 클래스(Query class)
      - DNS를 사용하는 특정 프로토콜을 정의하는 16비트 필드

[표 4] 질의 클래스 종류

Type	Mnemonic	Description
1	IN (Internet)	32비트 IPv4주소, 도메인 이름을 주소로 변환함
2	CSNET (CSNET network)	해당 영역의 권한을 가진 서버를 알려줌
3	CS (The COAS network)	호스트의 공식 이름에 대한 별칭을 정의함
4	HS (The Hesiod server developed by MIT)	하나의 영역이 시작되는 지점을 표시함

DNS

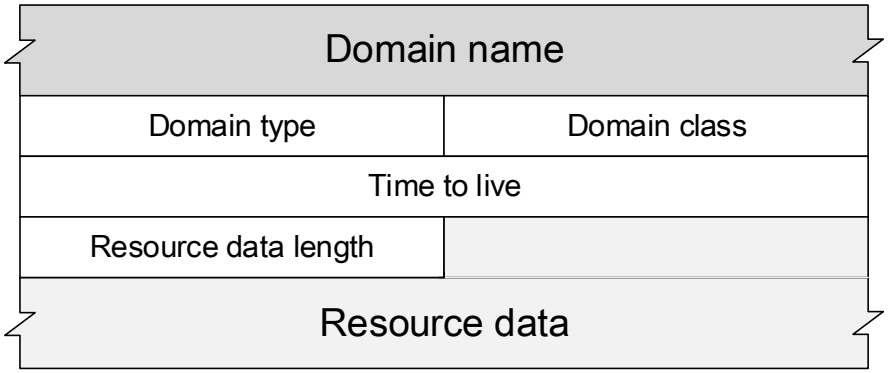
- DNS 레코드
  - 자원 레코드(Resource record)
    - 정의
      - 서버가 클라이언트의 문의 레코드에 대해 요청된 정보를 돌려주는 데이터 단위
    - 구성 필드
      - 도메인 네임(Domain name)
      - 도메인 유형(Domain type)
      - 도메인 클래스(Domain class)
      - 수명(Time to live)
      - 자원 데이터 길이(Resource data length)
      - 자원 데이터(Resource data)



<그림 34> 지원 레코드 형식

DNS

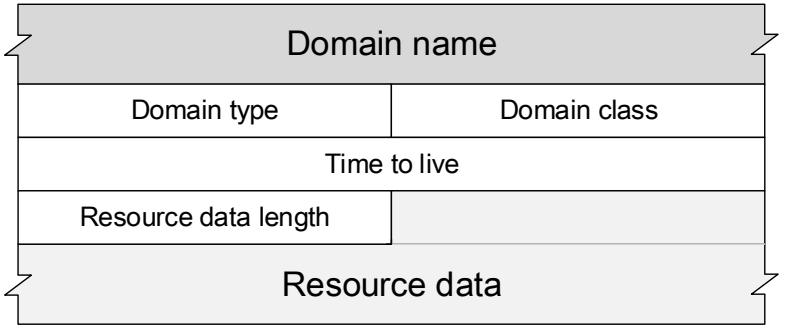
- DNS 레코드
  - 자원 레코드(Resource record)
    - 구성 필드 (1/3)
      - 도메인 네임(Domain name)
        - 도메인 네임을 포함한 가변 길이 필드
        - 문의 레코드에 있는 도메인 네임을 복사한 필드임
        - 문의 레코드에 있는 도메인 네임 필드에 대한 포인터 오프셋을 나타냄
      - 도메인 유형(Domain type)
        - 도메인 유형을 나타내는 16비트 필드
        - AXFR, ANY를 제외한 질의 유형과 동일함
      - 도메인 클래스(Domain class)
        - 문의 레코드의 질의 클래스와 동일함
      - 수명(Time to live)
        - 시간을 초 단위로 나타내는 32비트 필드
        - 수신자는 설정된 기간 동안 응답을 캐싱할 수 있음
        - 필드가 0으로 되어있으면 자원 레코드가 처리에 한 번만 사용되고 캐시에 저장되지 않음을 나타냄



<그림 34> 지원 레코드 형식

DNS

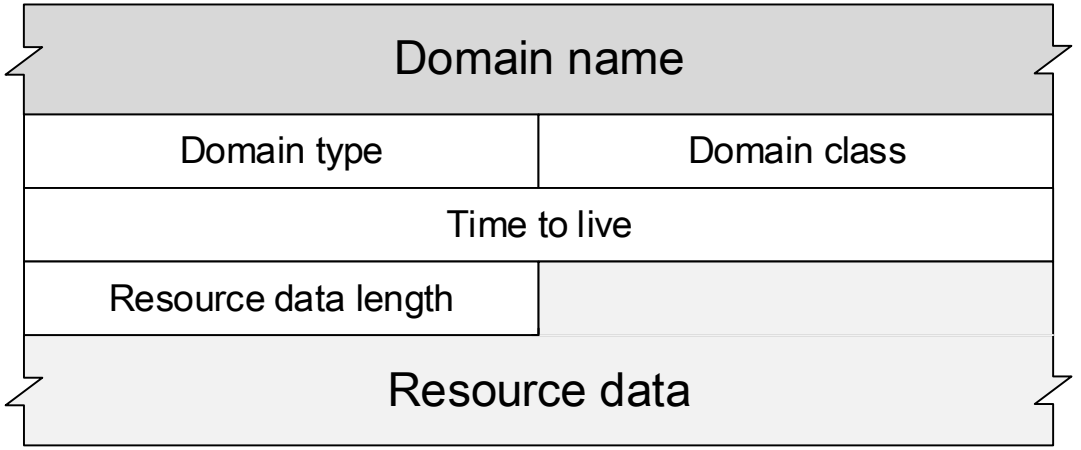
- DNS 레코드
  - 자원 레코드(Resource record)
    - 구성 필드 (2/3)
      - 자원 데이터 길이(Resource data length)
        - 자원 데이터의 길이를 나타내는 16비트 필드
      - 자원 데이터(Resource data)
        - 질의에 대한 응답을 포함하거나 권한이 있는 서버의 도메인 네임을 포함한 가변 길이 필드
        - 4가지 형태 중 하나만 사용함
        - 번호
          - IP 주소 같은 숫자값을 그대로 담음
          - IPv4 주소인 경우 4바이트를 가짐
          - IPv6 주소인 경우 8바이트를 가짐
        - 도메인 네임
          - 응답이 다른 도메인 이름일 경우 다른 도메인을 담는 가변 크기를 가짐
          - 도메인 네임은 레이블의 순서로 표시됨
          - 모든 도메인 네임의 마지막 바이트는 0을 가짐



<그림 34> 지원 레코드 형식

DNS

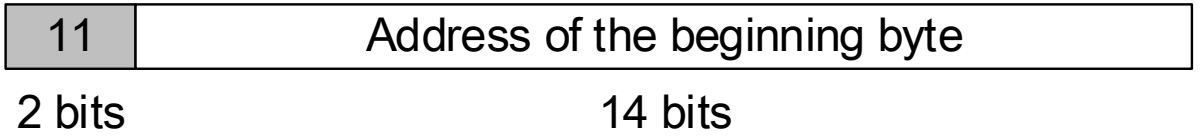
- DNS 레코드
  - 자원 레코드(Resource record)
    - 구성 필드 (3/3)
      - 자원 데이터(Resource data)
        - 오프셋 포인터
          - 앞선 메시지에 이미 나온 이름을 가리켜 반복을 줄이는 2바이트 필드
        - 문자 스트링
          - 일반 텍스트 정보를 담는 가변 길이 필드
          - 길이 필드를 포함하여 255문자 길이만큼 가질 수 있음



<그림 34> 지원 레코드 형식

DNS

- 메시지 압축 (Message Compression)
  - 개요
    - 메시지 안에 반복해서 나오는 도메인 이름을 다시 쓰지 않고 앞에 나온 위치를 가리키는 포인터로 바꾸는 메커니즘
  - 특징
    - UDP 메시지의 512바이트 제한을 넘지 않기 위해 제안됨
    - 2바이트 오프셋 포인터를 정의함
    - 나머지 14비트는 메시지 내 해당 도메인 이름이 적혀 있는 위치를 가리킴
      - 14비트가 00000001100인 경우 바이트 12를 가르킴



<그림 35> 오프셋 포인터의 형식

DNS

- 메시지 압축

QR	OpCode	AA	TC	RD	RA	Three 0s	rCode

<그림 30> 플래그 필드 형식

  - 예제 19.1

해석기가 호스트 “chal.fhda.edu.”에 대한 IP 주소를 찾기 위해 로컬 서버에게 질의 메시지를 그림과 같이 전송한다. 이를 통해 질의 메시지의 각 필드가 어떤 걸 표현하는지, DNS 메시지가 어떻게 압축되고 서버는 응답 메시지를 어떻게 보내는지 설명하시오.

- 처음 두 바이트는 식별자인 $(1333)_{16}$을 보여줌
- 다음 바이트는 플래그 값인 0x0100을 보여줌
  - 이를 2진수로 표현하면 0000000100000000임
- 2진수를 다음과 같은 필드로 나눔

0x1333		0x0100	
1		0	
0		0	
4	'c'	'h'	'a'
'l'	'4'	'f'	'h'
'd'	'a'	'3'	'e'
'd'	'u'	0	Continued on next line
1	1		

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
0	0000	0	0	1	0	000	0000

DNS

- 메시지 압축



<그림 30> 플래그 필드 형식

  - 예제 19.1

해석기가 호스트 “chal.fhda.edu.”에 대한 IP 주소를 찾기 위해 로컬 서버에게 질의 메시지를 그림과 같이 전송한다. 이를 통해 질의 메시지의 각 필드가 어떤 걸 표현하는지, DNS 메시지가 어떻게 압축되고 서버는 응답 메시지를 어떻게 보내는지 설명하시오.

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
0	0000	0	0	1	0	000	0000

- QR 값이 0이므로 질의 메시지임을 나타냄
- OpCode값이 0000이므로 표준 질의임을 나타냄
- RD 값이 1이므로 메시지는 한 개의 질의 메시지를 가짐
- 도메인 네임은 4chal4fhda3edu0임
  - 다음 레이블의 글자 개수를 나타냄

DNS

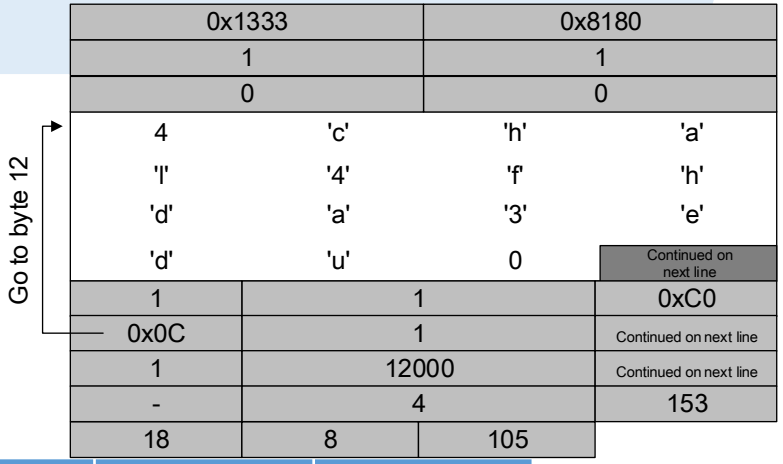
- 메시지 압축

QR	OpCode	AA	TC	RD	RA	Three 0s	rCode

<그림 30> 플래그 필드 형식

  - 예제 19.1

해석기가 호스트 “chal.fhda.edu.”에 대한 IP 주소를 찾기 위해 로컬 서버에게 질의 메시지를 그림과 같이 전송한다. 이를 통해 질의 메시지의 각 필드가 어떤 걸 표현하는지, DNS 메시지가 어떻게 압축되고 서버는 응답 메시지를 어떻게 보내는지 설명하시오.



  - 응답 메시지는 다음과 같음
  - 플래그값은 0x8180임
    - 이를 2진수로 표현하면 1000000110000000임
  - 2진수를 필드로 나타내면 다음과 같음

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
1	0000	0	0	1	1	000	0000

  - QR 비트는 응답 메시지임을 나타냄

DNS

- 메시지 압축

QR	OpCode	AA	TC	RD	RA	Three 0s	rCode

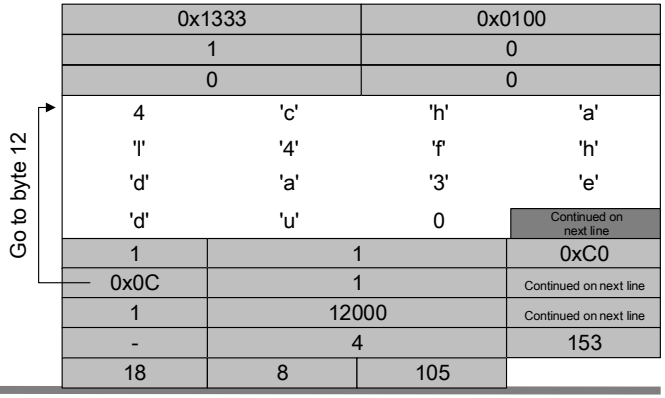
<그림 30> 플래그 필드 형식

  - 예제 19.1

해석기가 호스트 “chal.fhda.edu.”에 대한 IP 주소를 찾기 위해 로컬 서버에게 질의 메시지를 그림과 같이 전송한다. 이를 통해 질의 메시지의 각 필드가 어떤 걸 표현하는지, DNS 메시지가 어떻게 압축되고 서버는 응답 메시지를 어떻게 보내는지 설명하시오.

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
1	0000	0	0	1	1	000	0000

- RA비트와 RD비트는 1로 저장됨
- 응답 레코드는 포인터 0xC00C 값을 가짐
  - 도메인 네임을 반복하는 대신 질의 레코드를 지정하는 것임



DNS

- 메시지 압축



<그림 30> 플래그 필드 형식

  - 예제 19.2

FTP 서버가 153.2.7.9라는 주소를 가지는 FTP 클라이언트로부터 패킷을 수신함. FTP 서버가 FTP 클라이언트가 인증된 클라이언트임을 확인하는 과정을 인버스 질의를 통한 과정을 가질 때 주고받는 질의와 응답 메시지를 분석하시오.

- 처음 두 바이트 0x1200은 식별자임
- 플래그 값은 0x0900임
  - 이를 2진수로 나타내면 0000100100000000임

0x1200		0x0900	
1		0	
0		0	
1	'9'	'1'	'7'
1	'2'	3	'1'
'5'	'3'	7	'i'
'n'	'-'	a	'd'
'd'	'a'	4	'a'
'r'	'p'	'a'	0
12		1	

- 이를 필드로 나누어 보면 다음과 같음

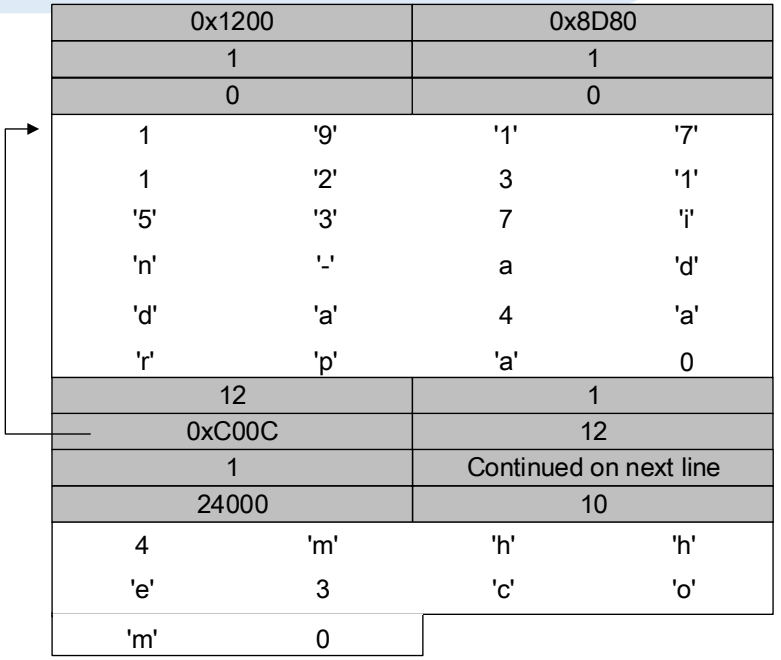
QR	OpCode	AA	TC	RD	RA	Reserved	rCode
0	0001	0	0	1	0	000	0000

DNS

- 메시지 압축
  - 예제 19.2

FTP 서버가 153.2.7.9라는 주소를 가지는 FTP 클라이언트로부터 패킷을 수신함. FTP 서버가 FTP 클라이언트가 인증된 클라이언트임을 확인하는 과정을 인버스 질의를 통한 과정을 가질 때 주고받는 질의와 응답 메시지를 분석하시오. 질의와 응답 메시지는 다음과 같다.

- 응답 레코드는 0xC00C 포인터 값을 가짐
  - 도메인 네임을 반복하는 대신에 문의 레코드를 지정함
- 도메인 종류는 12를 가르킴
- 마지막 필드는 도메인 네임이 4mhhe3com0 임을 나타냄



DNS

- 캡슐화(Capsulation)
  - 개요
    - DNS는 전송 계층의 UDP나 TCP에 캡슐화 되어 전송됨
  - 특징
    - 응답 메시지의 크기가 512바이트 미만이면 UDP를 사용함
    - 응답 메시지의 크기가 512바이트 이상이면 TCP를 사용함
    - 해석기가 응답 메시지의 크기에 대해 알지 못하면 먼저 UDP를 사용함
    - UDP를 사용했는데 응답 메시지의 크기가 512바이트 이상이면 서버는 메시지를 512바이트 크기로 자른 후 TC 비트를 1로 설정하여 TCP 연결을 개설함

DNS

- DDNS (Dynamic Domain Name System)
  - 개요
    - 유동 IP 주소가 변경될 때 실시간으로 도메인 이름에 업데이트하여 고정 IP처럼 접속할 수 있게 하는 DNS의 확장 메커니즘
  - 동작 과정
    1. 이름과 주소의 매핑이 필요하게 되면 DHCP로부터 1차 DNS 서버로 정보가 전송되고 1차 서버는 영역을 갱신함
    2. 2차 서버는 1번 과정의 결과를 스스로 알거나 1차 서버로부터 통보 받음
    3. 2차 서버는 결과를 알게된 후 전체 영역에 대한 정보를 요청함

DNS

- DNS의 보안
  - 개요
    - 웹 접속이나 이메일과 같은 응용 프로그램은 DNS 동작에 의존하므로 보안이 필수적임
  - 위협 공격
    - DNS 스니핑(DNS Sniffing)
      - 공격자는 DNS 서버의 응답을 읽어 사용자가 접속하는 사이트의 이름이나 성질을 알 수 있음
      - DNS 메시지의 비밀성을 보장하여 방지할 수 있음
    - DNS 스푸핑(DNS Spoofing)
      - 공격자는 DNS 서버의 응답을 중간에서 변경하거나 위조 응답을 만들어 사용자의 접속을 유도할 수 있음
      - 송신자 인증 및 메시지 무결성을 사용해 방지할 수 있음

DNS

- DNS의 보안
  - DNSSEC (DNS Security)
    - 개요
      - 메시지 송신자 인증과 디지털 서명을 사용하는 기법
    - 작동 방식
      - 권한 서버가 자기 영역의 자원 레코드에 개인 키로 서명함
      - 해석기는 공개 키로 서명을 검증함
      - 자원 레코드 타입에 서명값, 공개키, 서명을 추가해 전송함
  - DoH (DNS over HTTPS)
    - 개요
      - DNS 메시지를 HTTPS 요청 안에 담아 전송하는 기법
    - 작동 방식
      - DNS 질의 메시지를 평문이 아닌 HTTPS를 사용하여 암호화한 후 전송함

Thanks!

민 윤 홍(yunhong@pel.sejong.ac.kr)

부 록

• 18년도 6월 국어 모의평가에 나온 DNS 스푸핑 지문

DNS(도메인 네임 시스템) 스푸핑은 인터넷 사용자가 어떤 사이트에 접속하려 할 때 사용자를 위조 사이트로 접속시키는 행위를 말한다. 이는 도메인 네임을 IP 주소로 변환해 주는 과정에서 이루어진다.

인터넷에 연결된 컴퓨터들이 서로를 식별하고 통신하기 위해서 각 컴퓨터들은 IP(인터넷 프로토콜)에 따라 ㉠ 만들어지는 고유 IP 주소를 가져야 한다. 프로토콜은 컴퓨터들이 연결되어 서로 데이터를 주고받기 위해 사용하는 통신 규약으로 소프트웨어나 하드웨어로 구현된다. 현재 주로 사용하는 IP 주소는 '***.126.63.1'처럼 점으로 구분된 4개의 필드에 숫자를 사용하여 ㉡ 나타낸다. 이 주소를 중복 지정하거나 임의로 지정해서는 안 되고 공인 IP 주소를 부여받아야 한다.

공인 IP 주소에는 동일한 번호를 지속적으로 사용하는 고정 IP 주소와 번호가 변경되기도 하는 유동 IP 주소가 있다. 유동 IP 주소는 DHCP라는 프로토콜에 의해 부여된다. DHCP는 IP 주소가 필요한 컴퓨터의 요청을 받아 주소를 할당해 주고, 컴퓨터가 IP 주소를 사용하지 않으면 주소를 반환받아 다른 컴퓨터가 그 주소를 사용할 수 있도록 해 준다. 한편, 인터넷에 직접 접속은 안 되고 내부 네트워크에서만 서로를 식별할 수 있는 사설 IP 주소도 있다.

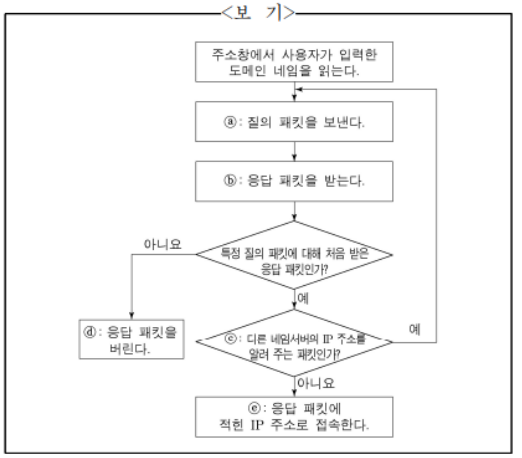
인터넷은 공인 IP 주소를 기반으로 동작하지만 우리가 인터넷을 사용할 때는 IP 주소 대신 사용하기 쉽게 'www.***.***' 등과 같이 문자로 ㉢ 이루어진 도메인 네임을 이용한다. 따라서 도메인 네임을 IP 주소로 변환해 주는 DNS가 필요하며 DNS를 운영하는 장치를 네임서버라고 한다. 컴퓨터에는 네임서버의 IP 주소가 기록되어 있어야 하는데, 유동 IP 주소를 할당받는 컴퓨터에는 IP 주소를 받을 때 네임서버의 IP 주소가 자동으로 기록되지만, 고정 IP 주소를 사용하는 컴퓨터에는 사용자가 네임서버의 IP 주소를 직접 기록해 놓아야 한다. 인터넷 통신사는 가입자들이 공동으로 사용할 수 있는 네임서버를 운영하고 있다.

㉮ 사용자가 어떤 사이트에 정상적으로 접속하는 과정을 살펴보자. 웹 사이트에 접속하려고 하는 컴퓨터를 클라이언트라 한다. 사용자가 방문하고자 하는 사이트의 도메인 네임을 주소창에 직접 입력하거나 포털 사이트에서 그 사이트를 검색해 클릭하면 클라이언트는 기록되어 있는 네임서버에 도메인 네임에 해당하는 IP 주소를 물어보는 질의 패킷을 보낸다. 네임서버는 해당 IP 주소가 자신의 목록에 있으면 클라이언트에 이 IP 주소를 알려 주는 응답 패킷을 보낸다. 응답 패킷에는 어느 질의 패킷에 대한 응답인지가 적혀 있다. 만일 해당 IP 주소가 목록에 없으면 네임서버는 다른 네임서버의 IP 주소를 알려 주는 응답 패킷을 보내고, 클라이언트는 다시 그 네임서버에 질의 패킷을 보내는 단계로 돌아가 같은 과정을 반복한다. 클라이언트는 이렇게 ㉣ 알아낸 IP 주소로 사이트를 찾아간다. 네임서버와 클라이언트는 UDP라는 프로토콜에 ㉤ 맞추어 패킷을 주고받는다. UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대에게 패킷을 보내기만 할 뿐 도착 여부는 확인하지 않으며, 특정 질의 패킷에 대해 처음 도착한 응답 패킷을 신뢰하고 다음에 도착한 패킷은 확인하지 않고 버린다. DNS 스푸핑은 UDP의 이런 허점들을 이용한다.

㉯ DNS 스푸핑이 이루어지는 과정을 알아보자. 악성 코드에 감염되어 DNS 스푸핑을 행하는 컴퓨터를 공격자라 한다. 클라이언트가 네임서버에 특정 IP 주소를 묻는 질의 패킷을 보낼 때, 공격자에도 패킷이 전달되고 공격자는 위조 사이트의 IP 주소가 적힌 응답 패킷을 클라이언트에 보낸다. 공격자가 보낸 응답 패킷이 네임서버가 보낸 응답 패킷보다 클라이언트에 먼저 도착하고 클라이언트는 공격자가 보낸 응답 패킷을 옳은 패킷으로 인식하여 위조 사이트로 연결된다.

31. <보기>는 ㉮ 또는 ㉯에서 이루어지는 클라이언트의 동작을 나타낸 것이다. 이에 대한 이해로 적절한 것은? [3점]

<보 기>



① ㉮: ⓐ가 두 번 동작했다면, 두 질의 내용이 동일하고 패킷을 받는 수신 측도 동일하다.
② ㉮: ⓑ가 두 번 동작했다면, 두 응답 내용이 서로 다르고 패킷을 보낸 송신 측은 동일하다.
③ ㉮: ⓒ는 ⓐ에서 질의한 도메인 네임에 해당하는 IP 주소를 네임서버가 찾았는지 여부를 확인하는 절차이다.
④ ㉯: ⓓ의 응답 패킷에는 공격자가 보내 온 IP 주소가 포함되어 있다.
⑤ ㉯: ⓔ의 IP 주소는 ⓐ에서 질의한 도메인 네임에 해당하는 IP 주소이다.