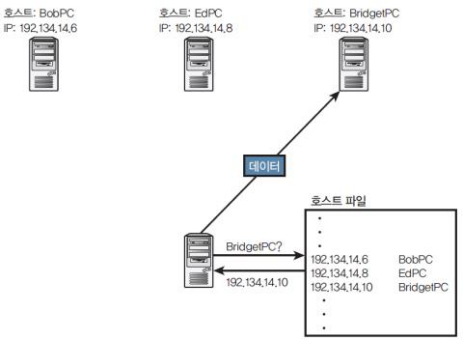
TCP/IP 교과서

10장 이름 확인

10.1 이름 확인은 무엇인가

TCP/IP 교과서

- 초기 TCP/IP 네트워크가 온라인으로 발전했을 때, 사용자는 네트워크의 모든 컴퓨터의 IP 주소를 기억하는 것이 비효율적이라는 것을 알아챘음
- 개발자들은 각 컴퓨터에 설명할 수 있는 인간 친화적 이름을 할당하고 네트워크의 컴퓨터가 주소를 이름과 연관시키도록 했음
- 호스트 파일을 이용한 이름 확인



10.1 이름 확인은 무엇인가

호스트 파일을 이용한 이름 확인

- 호스트 파일 시스템은 소규모 로컬 네트워크에서 잘 작동
- 대규모 네트워크에서는 비효율적임
- 호스트-주소 관계는 단일 파일에 속해 있어야 하고, 해당 파일의 검색 효율은 파일이 커질수록 줄어듦
- ARPAnet 시대에는 hosts.txt라고 하는 단일 마스터 파일이 이름-주소 관계 목록을 유지했고, 로컬 관리자는 hosts.txt를 지속해서 업데이트해야 했음
- 다음 내용을 수행할 수 있는 계층적 이름 확인 시스템이 필요했음
  - 이름 확인 서버들 간 이름 확인에 대한 책임을 분배
  - 로컬 관리자에게 로컬 이름 확인 권한을 부여함

10.3 DNS

DNS(Domain Name System)

- DNS는 이름 공간(name space)을 **도메인**이라고 하는 계층적 엔터티로 분할
  - 이름 공간은 주소를 이름에 대응시키는 컨테이너
- 계층적 이름 공간을 적용
  - Name이 여러 부분으로 구성되며
  - 일정한 규칙에 따라 이름이 부여됨

  예) 첫 번째 부분은 조직의 속성, 두 번째는 조직의 이름, 세 번째는 조직 내 부서, ….
- DNS 서버는 네트워크를 위한 이름 확인 서비스를 제공
- 만약 네트워크의 컴퓨터가 IP 주소를 기다리고 있는 호스트 이름이 있다면, 호스트 이름과 연관된 IP 주소를 요구하는 쿼리를 서버에 보냄
- 만약 DNS 서버에서 해당 주소를 가지고 있으면, 요청 컴퓨터에 해당 주소를 다시 전송

10.3 DNS 이름 확인

TCP/IP 교과서

- 단일 DNS 서버가 모든 이름 데이터베이스를 유지하는 것은 불가능
- 서버를 구성한 사람은 세계 모든 곳의 인터넷 호스트에 대한 모든 변경 사항을 알아야 함
- 더 나은 방법은 그림 10-2처럼 모든 사무실과 기관에서 로컬 이름 서버가 작동하도록 구성하고 모든 이름 서버가 서로 통신할 방법을 제공하는 것(그림 10-3 참고)

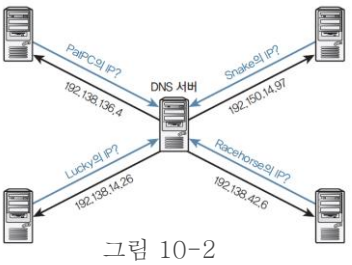


그림 10-2

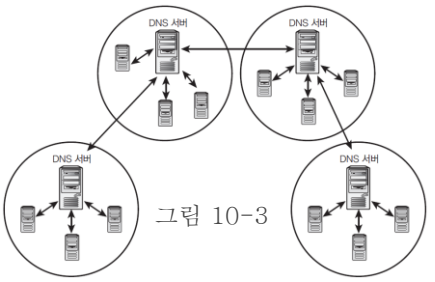


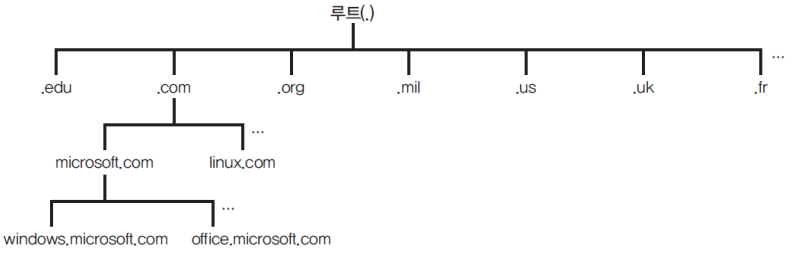
그림 10-3

첫 번째 이름 서버가 쿼리 과정을 시작할 때 어떤 이름 서버에 연락해서 주소를 알아낼까?

10.3 DNS 이름 확인

TCP/IP 교과서

- DNS 이름 공간
  - DNS 이름 공간은 도메인의 다중 계층 배열(그림 10-4 참조)
  - 도메인은 이름 공간의 subtree로 공통 공간을 공유하는 단일 권한에 속한 컴퓨터의 집합으로
  - DNS 트리의 상단에는 루트(root)라고 하는 단일 노드가 있음
  - 루트 밑에는 최상위 도메인(TLD, Top-Level Domain)이라고 하는 도메인 그룹이 있음

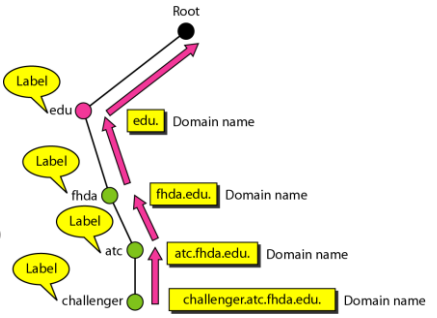


10.3 DNS 이름 확인

TCP/IP 교과서

» DNS 이름 공간

- 레이블(Label)
  - 트리의 각 노드가 가지는 최대 63개 길이의 문자열
  - root label은 null (빈 문자열)
  - 한 노드의 자식 노드들은 서로 다른 레이블을 가져야 함
- 도메인 이름
  - 트리의 각 노드는 하나의 도메인 이름을 가짐
  - dot (.)에 의해 구분되는 레이블들의 연속
  - 노드로부터 root 방향으로 읽혀짐
  - 마지막 레이블은 root의 레이블 (null) 즉, 마지막 문자는 dot



FQDN

10.3 DNS 이름 확인

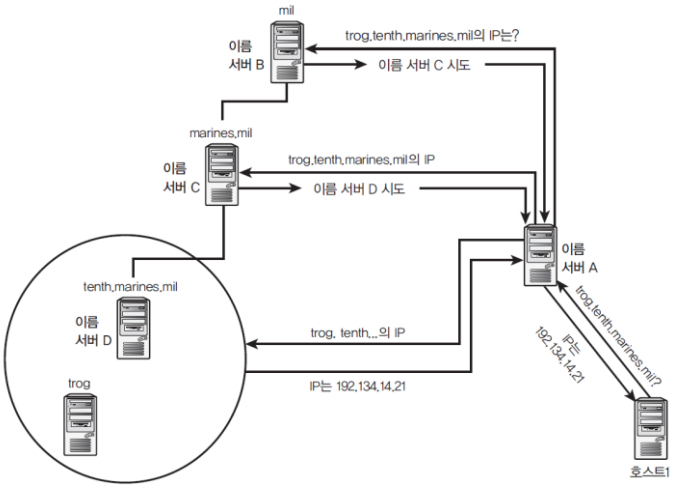
TCP/IP 교과서

» DNS

- 도메인 이름은 트리의 상단에서부터 연결된 도메인 고리를 보여줌
- 도메인 fhda.edu의 이름 서버는 fhda.edu 도메인 내 호스트를 위한 이름 확인 정보를 가지고 있음
- 도메인의 신뢰할 수 있는 이름 서버는 하위 도메인의 이름 확인을 다른 서버에 위임할 수 있음
- 예를 들어, fhda.edu의 신뢰할 수 있는 이름 서버는 하위 도메인 afc.fhda.edu 의 권한을 다른 이름 서버에 위임할 수 있음
- 하위 도메인 afc.fhda.edu의 이름 확인 기록은 해당 하위 도메인의 권한을 위임받은 이름 서버에 위치
- 이름 확인 권한은 트리를 통해 위임되고, 지정된 도메인 관리자는 해당 도메인 호스트에 대한 이름-주소 매핑 제어권을 가질 수 있음

10.3 DNS 이름 확인

그림 10-6 이름 확인 과정 (반복적 방법)



10.4 도메인 등록하기

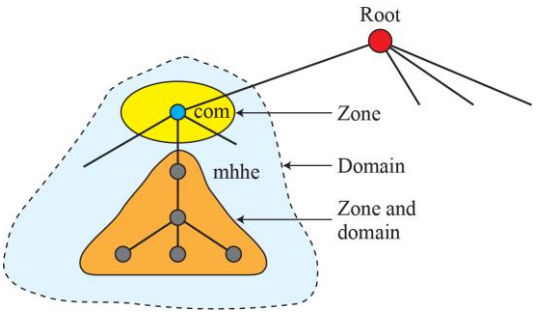
- 자신만의 도메인 이름을 가지고 싶은 기관(예: BuddysCars.com)은 반드시 해당 이름을 올바른 등록 기관에 등록해야 함
- 국제 인터넷 주소 관리 기구(ICANN)는 도메인 이름 등록에 대한 전반적인 권한을 가지고 있지만, 특정 TLD 등록은 다른 그룹에 권한을 위임
  - 베리싸인은 .com과 .net 도메인에 대한 권위 있는 등록 기관이며, PIR(Public Internet Registry)은 .org을 유지
  - **.gov**: .gov 도메인은 미국 연방 정부와 미국 TLD의 지방 정부를 위해 예약되어 있음
- 많은 국가는 자신만의 도메인 이름을 가지고 있으며, 별도의 도메인 이름 등록 기관을 운영함
  - 한국은 한국인터넷진흥원에서 등록 관리

10.5 이름 서버 유형

- 네트워크에 DNS를 구현할 때, 도메인을 유지하기 위한 적어도 2개 이상의 서버를 선택해야 함
- 이는 주 이름 서버를 의미하고, 맡아야 할 구역의 모든 정보는 로컬 파일에서 가져옴
- 도메인의 모든 변경은 해당 서버에서 이루어짐
- 많은 네트워크는 최소 하나 이상의 서버를 백업으로 두거나 보조 이름 서버를 둠
- 주 이름 서버에 문제가 생겨도 계속해서 서비스 요청을 수행할 수 있음
- 보조 서버는 주 서버의 **존 파일**(zone file)에서 정보를 가져옴
- 이러한 정보 교환을 존 전송(zone transfer)이라고 함

10.5 이름 서버 유형

- 존(zone)
  - 이름서버가 책임을 지거나 권한을 가지는 영역
    - 이름서버가 도메인에 대한 책임을 맡고 이를 더 작은 도메인으로 나누지 않았다면 도메인=영역
    - 이름서버는 영역 내의 모든 노드 정보 (zone file)을 가짐



10.5 이름 서버 유형

TCP/IP 교과서

존 파일

- DNS 서버는 쿼리에 응답하고 요청을 처리하기 시작할 때 존 파일의 정보를 참조
- 표준화된 구조를 가진 텍스트 파일이며, 여러 **자원 레코드**로 구성되어 있음
- 자원 레코드는 DNS 구성에 대한 유용한 정보를 제공하는 한 줄짜리 구문
- 자원 레코드 유형

RR format: (name, type, class, ttl, rdlength, rdata)

- **Name: 도메인 이름**
- **Type: RR이 참조하는 자원의 유형**
  - **Type=A**
    - **name → 호스트 이름**
    - **rdata → IP 주소**
  - **Type=NS**
    - **name → 도메인 이름 (e.g. gwnu.ac.kr)**
    - **rdata → DNS 서버의 이름**
  - **Type=SOA(Start of Authority)**
    - **name → 도메인 이름 (e.g. gwnu.ac.kr)**
    - **rdata → zone에 대한 권한을 갖는 DNS 서버의 이름**
  - **Type=CNAME**
    - **name → 진짜 (canonical) 이름의 별칭**
    - **rdata → canonical name**
  - **Type=MX**
    - **name → 호스트 또는 도메인 이름**
    - **rdata → 메일 서버의 이름**

10.5 이름 서버 유형

TCP/IP 교과서

존 파일

- 다음은 존 파일의 예

```
@ IN    SOA    boris.cocacola.com.   hostmaster.cocacola.com. (
        201.9      ; serial number incremented with each
                   ; file update
                   ;
        3600       ; refresh time (in seconds)
        1800       ; retry time (in seconds)
        4000000    ; expiration time (in weeks)
        3600)      ; minimum TTL
IN    NS     horace.cocacola.com.
IN    NS     boris.cocacola.com.
;
; Host to IP address mappings
;
localhost     IN    A     127.0.0.1
chuck         IN    A     181.21.23.4
amy           IN    A     181.21.23.5
darrah        IN    A     181.21.23.6
joe           IN    A     181.21.23.7
bill          IN    A     181.21.23.8
;
; Aliases
;
ap             IN CNAME    amy
db             IN CNAME    darrah
bu             IN CNAME    bill
```

- refresh time: 보조 DNS 서버가 존 정보의 업데이트를 위해 주 서버에 요청해야 하는 시간 간격
- retry time: 존 업데이트가 실패했을 때 다시 시도하기 전까지 기다려야 하는 시간
- expiration time: 보조 이름 서버가 새로 고침 없이 레코드를 가지고 있어야 하는 최대 시간 한도
- minimum TTL: 내보낸 존 레코드에 대한 기본 TTL

10.5 이름 서버 유형

DNS 보안 확장

- 클라이언트는 DNS 쿼리 응답이 존을 관리하는 실제 DNS 서버에서 왔다는 것을 보장하는 수단이 필요함
- 공격자들은 DNS 쿼리에 가짜 응답을 보내는 여러 기술을 개발
- DNS 쿼리를 낚아채려는 공격자는 공격을 시작하는 수단으로 사용될 비밀 DNS 서버로 클라이언트를 보내는 가짜 응답을 보낼 수 있음
- 실제 응답이 오기 전에 가짜 응답이 도착하는 한 DNS 클라이언트는 이를 대처할 수 없음
- **DNS 보안 확장**(DNSSEC, DNS Security Extension)은 DNS 데이터를 검증하기 위한 시스템을 제공
- 오늘날 많은 운영 시스템은 비록 대규모로 구현되진 않았지만 DNSSEC 옵션을 제공

10.5 이름 서버 유형

DNS 유틸리티

- 이름 확인을 제공하는 모든 네트워크 유틸리티를 사용해 네트워크가 올바르게 이름을 확인하는지 테스트할 수 있음
- 웹 브라우저, FTP 클라이언트, 텔넷 클라이언트 혹은 핑 유틸리티는 여러분의 컴퓨터가 이름 확인에 성공했는지 여부를 말해줌
- 만약 IP 주소를 사용해서 리소스에 연결할 수 있는 호스트 이름이나 FQDN을 사용해서는 연결할 수 없다고 하면, 이름 확인에 문제가 있을 가능성이 큼

10.5 이름 서버 유형

TCP/IP 교과서

» 핑으로 이름 확인 체크하기

- 다음과 같이 DNS 이름으로 원격 컴퓨터에 핑을 보내 보자

```
ping williepc.remotenet.com
```

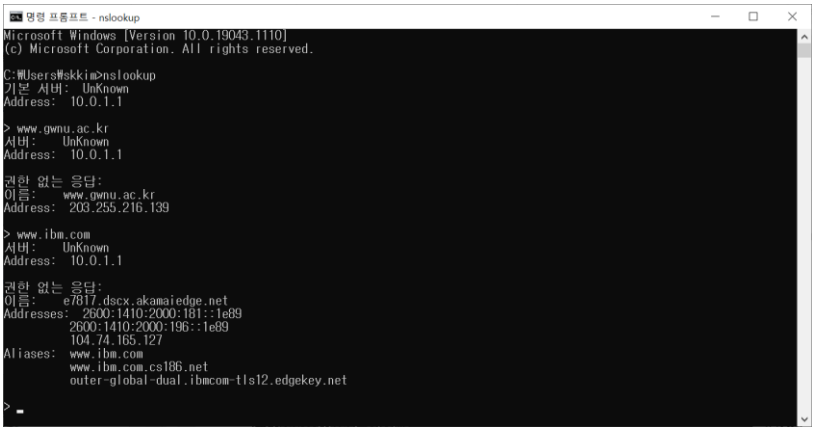
- IP 주소로는 원격 컴퓨터에 핑을 보낼 수 있는데 DNS 이름으로는 안 된다면 이름 확인에 문제가 있을 수 있음
- DNS 이름으로 핑을 보낼 수 있다면 이름 확인은 정상적으로 작동하고 있다는 의미

10.5 이름 서버 유형

TCP/IP 교과서

» NSLookup을 통해 이름 확인 체크하기

- NSLookup 유틸리티로 DNS 서버에 쿼리를 보내고 리소스 레코드와 같은 정보를 볼 수 있으며, DNS 문제를 해결할 때 유용함



10.5 이름 서버 유형

» 도메인 정보 그로퍼(dig,Domain Information Groper)

- 리눅스 유틸리티
- 가장 기본적인 형태로, dig는 다음의 호스트 이름을 입력하면 해당 IP 주소를 반환

```
dig host.domain.com
```

- 호스트 앞에 @server을 추가해서 쿼리할 DNS 서버를 명시하자

```
dig @14.13.18.20 host.domain.com
```

- 앞의 명령어는 14.13.18.20 주소로 DNS 서버를 쿼리함

10.5 이름 서버 유형

» 도메인 정보 그로퍼

- 특정한 리소스 레코드 유형을 쿼리하려면 리소스 유형의 이름을 추가

```
dig host.domain.com NS
```

- 앞의 명령어는 해당 도메인과 연관된 NS 레코드를 표시
- 이름 서버를 찾으려면 다음과 같이 하자

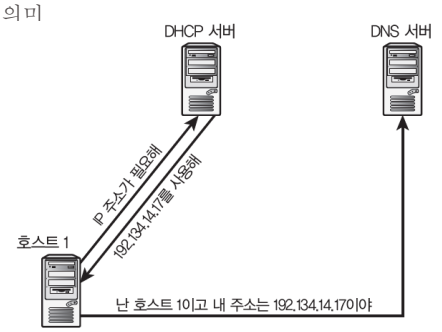
```
dig host.domain.com MX
```

- -x 옵션은 IP 주소를 명시했을 때 역방향 조회를 수행
- -4 옵션은 쿼리를 IPv4로 제한
- IPv6에는 -6을 사용

10.6 동적 DNS

TCP/IP 교과서

- DNS는 호스트 이름과 IP 주소의 영구적으로(또는 적어도 반영구적) 연관이 있는 상황을 위해 설계
- 오늘날의 네트워크에서는 IP 주소가 종종 동적으로 할당
- 다시 말해 컴퓨터가 시작할 때마다 새로운 IP 주소가 DHCP을 통해 컴퓨터에 할당
- 이는 만약 컴퓨터가 DNS에 등록되어 있고 자신의 호스트 이름을 통해 접근이 가능하다면 DNS 서버는 반드시 컴퓨터가 사용 중인 IP 주소를 알아낼 방법이 있어야 한다는 의미



10.7 NetBIOS 이름 확인

TCP/IP 교과서

- NetBIOS는 API이며, 마이크로소프트 윈도 네트워크의 발전에 매우 중요했던 IBM이 개발한 이름 확인 시스템
- 레거시 윈도 시스템에서 NetBIOS 이름은 윈도 컴퓨터에 할당하는 컴퓨터 이름
- NetBIOS는 TCP/IP를 사용하지 않는 네트워크를 위해 개발
- 마이크로소프트는 윈도 2000/XP에서 NetBIOS를 강조하지 않았고, 윈도 비스타, 윈도 7 및 윈도 10은 계속해서 그 추세를 이어감
- 마이크로소프트의 공식 발언을 보면 NetBIOS 이름 확인 대신 DNS를 사용하는 것이 모범 사례
- NetBIOS는 브로트캐스트를 통해 작동하기 때문에 소규모 네트워크의 사용자는 NetBIOS 이름 확인을 구성하기 위해 (네트워크 설정 및 컴퓨터 이름 할당 이외에) 아무것도 할 것이 없음

10.8 요약

- 이름 확인은 컴퓨터에 할당된 IP 주소 대신 컴퓨터에 의미 있고 기억하기 쉬운 이름을 사용할 수 있게 함
- 이 장에서는 호스트 이름과 DNS를 통한 이름 확인을 살펴봤음
- DNS 구성 파일과 이름 확인 과정, 그리고 동적 DNS와 DNSSEC 같은 최신 기술도 알아봤음
- 마지막으로 NetBIOS 이름 확인 시스템이 여전히 윈도와 다른 SMB 기반 네트워크에 사용됨

10.11 핵심 용어

- **DNSSEC(DNS 보안 확장):** DNS 쿼리 응답의 신뢰성을 확인하기 위한 시스템
- **도메인:** DNS 이름 공간의 계층적 분할
- **도메인 이름:** DNS 이름 공간의 계층적 파티션에 지정된 이름
- **DNS(도메인 이름 시스템):** TCP/IP 네트워크의 리소스 이름 지정 시스템
- **동적 DNS:** 정적 DNS 이름을 동적 IP 주소로 연결하기 위한 기술
- **FQDN(전체 주소 도메인 이름):** 호스트 이름과 도메인 이름을 연결해서 생성된 이름
- **호스트 이름:** 컴퓨터(호스트)를 식별하기 위해 사용하는 단일 이름
- **호스트 파일:** IP 주소를 호스트 이름으로 연결하는 파일
- **NetBIOS:** IBM에서 개발한 이름 확인 시스템
- **리소스 레코드:** 큰 파일에 추가된 엔트리. 여러 리소스 레코드 유형이 있으며, 각 유형은 특정 목적을 가지고 있음
- **WINS(윈도 인터넷 이름 서비스):** NetBIOS 이름 서버의 마이크로소프트 구현 버전
- **존 파일:** DNS 서버가 사용하는 구성 파일