제7장
IP 주소 지정

이 장에서는 다음과 같은 CompTIA Network+ 시험 목표를 다룹니다.

- **1.4 주어진 시나리오에 따라 서브넷을 구성하고 적절한 IP 주소 지정 체계를 사용하십시오.**
  - 공공 vs. 민간
    - RFC1918
    - 네트워크 주소 변환(NAT)
  - IPv4와 IPv6의 차이점
    - 자동 사설 IP 주소 지정(APIPA)
    - 확장 고유 식별자(EUI-64)
    - 멀티캐스트
    - 유니캐스트
    - 애니캐스트
    - 방송
    - 로컬 링크
    - 루프백
    - 기본 게이트웨이
  - IPv4 서브넷팅
    - 클래스리스(가변 길이 서브넷 마스크 **)**
    - 클래스풀
      - 에이
      - 비
      - 기음
      - 디
      - 이자형
    - 클래스리스 도메인 간 라우팅(CIDR) 표기법
  - IPv6 개념

        - 터널링
        - 듀얼 스택
        - 속기 표기법
        - 라우터 광고
        - 상태 비저장 주소 자동 구성(SLAAC)
    - 가상 IP(VIP)
    - 서브인터페이스

TCP/IP에 대한 논의에서 가장 중요한 주제 중 하나는 IP 주소 지정입니다. IP 주소는 IP 네트워크상의 각 장치에 할당되는 숫자 식별자입니다. 이는 네트워크 상에서 장치의 특정 위치를 나타냅니다.

IP 주소는 하드웨어 주소가 아닌 논리적 주소입니다. 하드웨어 주소는 네트워크 인터페이스 카드(NIC)에 하드코딩되어 있으며 로컬 네트워크에서 호스트를 찾는 데 사용됩니다. IP 주소 체계는 호스트가 속한 LAN의 종류에 관계없이 한 네트워크의 호스트가 다른 네트워크의 호스트와 통신할 수 있도록 설계되었습니다.

IP 주소 지정의 더 복잡한 측면을 다루기 전에 몇 가지 기본 사항을 이해해야 합니다. 먼저 IP 주소 지정의 기본 원리와 용어를 설명하겠습니다. 그런 다음 계층적 IP 주소 지정 체계와 사설 IP 주소에 대해 알아보겠습니다.

유니캐스트, 멀티캐스트, 브로드캐스트 주소를 정의하고 IPv6에 대한 설명으로 이 장을 마무리하겠습니다. 최대한 쉽고 간결하게 설명해 드리겠습니다.

(물론 목표를 설명하는 것 외에도) IPv6에 대해 논의하는 이유는 미래 네트워크에서 사용할 IPv4 주소가 부족하기 때문입니다. 기업 및 개인 네트워크는 물론 인터넷까지 운영하는 데 필요한 주소가 부족해지고 있는 것이죠. 간단히 말해, 새로운 호스트에 할당할 주소가 고갈되고 있는 것입니다! IPv6는 이 문제를 해결해 줄 것입니다.

Todd Lammle의 CompTIA 동영상 및 연습 문제를 보려면 다음 링크를 참조하십시오 www.lammle.com .

IP 용어

이 장에서는 인터넷 프로토콜을 이해하는 데 필수적인 몇 가지 중요한 용어를 배우게 됩니다. 시작하기에 좋은 몇 가지 용어를 소개합니다.

- **비트** (Bit) 는 1 또는 0으로 이루어진 하나의 이진 숫자입니다.
- **바이트는** 패리티 사용 여부에 따라 7비트 또는 8비트입니다. 이 장의 나머지 부분에서는 항상 바이트를 8비트로 가정합니다 .
- **옥텟(Octet**)은 8비트로 구성된 일반적인 8비트 이진수입니다. 이 장에서는 *바이트(byte)* 와 *옥텟이라는* 용어를 완전히 같은 의미로 사용하며, 일반적으로 십진수로 255까지 표시합니다.
- **네트워크 주소** 는 원격 네트워크로 패킷을 전송하기 위해 라우팅에서 사용되는 지정자입니다. 예를 들어 10.0.0.0, 172.16.0.0, 192.168.10.0 등이 있습니다.
- **IP 주소는** 단일 호스트를 정의하는 데 사용되는 논리적 주소입니다. 하지만 IP 주소는 여러 호스트 또는 모든 호스트를 참조하는 데에도 사용될 수 있습니다. 만약 IP라고만 표기된 것을 본다면, 그것은 IPv4를 의미합니다. IPv6는 항상 IPv6로 표기됩니다.
- **브로드캐스트** *주소는* 애플리케이션 과 호스트가 네트워크상의 모든 호스트에게 정보를 전송하는 데 사용됩니다. 예를 들어, 255.255.255.255는 모든 네트워크와 모든 호스트를 지정하고, 172.16.255.255는 172.16.0.0 네트워크의 모든 서브넷과 호스트를 지정하며, 10.255.255.255는 10.0.0.0 네트워크의 모든 서브넷과 호스트에 브로드캐스트합니다.

계층적 IP 주소 지정 체계

IP 주소는 32비트의 정보로 구성됩니다. 이 비트는 옥텟 또는 바이트라고 하는 네 부분으로 나뉘며, 네 개의 옥텟을 합하면 32비트(8 × 4 = 32)가 됩니다. IP 주소는 다음 세 가지 방법 중 하나로 표시할 수 있습니다.

- 점으로 구분된 십진수 형식, 예: 172.16.30.56
- 이진수, 예를 들어 10101100.00010000.00011110.00111000
- AC.10.1E.38과 같이 16진수

이 예시들은 모두 동일한 IP 주소를 유효하게 나타냅니다. IPv6에서는 16진수를 사용하고, IP 주소 지정에는 점으로 구분된 십진수 또는 이진수가 사용되지만, 일부 프로그램에서는 여전히 IP 주소를 16진수로 저장하는 경우가 있습니다. Windows는 컴퓨터의 IP 주소를 16진수로 저장하는 대표적인 프로그램입니다. Windows 10(및 기타 모든 Windows 버전)은

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfa
경로의 하위 키에 IP 주소를 16진수로 저장합니다.

32비트 IP 주소는 평면 주소(비계층 주소)와 달리 구조화된 주소 또는 계층적 주소로 알려져 있습니다. 두 가지 주소 체계 모두 사용할 수 있지만, *계층적 주소 체계가* 선택된 데에는 매우 중요한 이유가 있습니다. 이 체계의 가장 큰 장점은 43억 개의 주소(32비트 주소 공간은 각 위치에 0 또는 1의 두 가지 값만 가질 수 있으므로 2^{32}, 즉 4,294,967,296개)를 처리할 수 있다는 것입니다. 평면 주소 체계의 단점, 그리고 IP 주소 체계에 사용되지 않는 이유는 라우팅과 관련이 있습니다. 모든 주소가 고유하다면 인터넷상의 모든 라우터는 인터넷에 있는 모든 컴퓨터의 주소를 저장해야 합니다. 이렇게 되면 전체 주소 중 일부만 사용하더라도 효율적인 라우팅이 불가능해집니다.

이 문제에 대한 해결책은 네트워크와 호스트 또는 네트워크, 서브넷 및 호스트를 기준으로 구성된 2단계 또는 3단계 계층적 주소 지정 체계를 사용하는 것입니다.

이 2~3단계 체계는 전화번호와 유사합니다. 첫 번째 부분인 지역번호는 매우 넓은 지역을 나타냅니다. 두 번째 부분인 접두사는 통화 범위를 지역 통화 구역으로 좁힙니다. 마지막 부분인 고객 번호는 특정 고객을 정확하게 연결합니다.연결. IP 주소는 동일한 유형의 계층 구조를 사용합니다. 평면 주소 지정 방식처럼 32비트 전체를 고유 식별자로 처리하는 대신, 주소의 일부는 네트워크 주소로 지정되고 나머지 부분은 서브넷 및 호스트 주소 또는 호스트 주소로 지정됩니다.

다음으로는 IP 네트워크 주소 지정과 네트워크에 사용되는 다양한 주소 클래스에 대해 설명하겠습니다.

네트워크 주소 지정

네트워크 *주소* (네트워크 번호라고도 함)는 각 네트워크를 고유하게 식별합니다. 동일한 네트워크에 있는 모든 컴퓨터는 IP 주소의 일부로 네트워크 주소를 공유합니다. 예를 들어 IP 주소 172.16.30.56에서 172.16은 네트워크 주소입니다(잠시 후 이것이 사실임을 보여드리겠습니다).

호스트 *주소는* 네트워크 상의 각 컴퓨터에 할당되며, 각 컴퓨터를 고유하게 식별합니다. 주소의 이 부분은 특정 컴퓨터, 즉 개별 컴퓨터를 식별하기 때문에 고유해야 합니다. 네트워크는 여러 컴퓨터를 묶어 놓은 집합체이기 때문입니다. 따라서 예시 IP 주소 172.16.30.56에서 30.56은 호스트 주소입니다.

인터넷 설계자들은 네트워크 규모에 따라 네트워크를 분류하기로 결정했습니다. 호스트 수가 매우 많은 소수의 네트워크를 위해 *A급 네트워크를* 만들었습니다 . 그 반

대편에는 호스트 수는 적지만 네트워크 수가 *많은 C급 네트워크가* 있습니다 . 매우 큰 네트워크와 매우 작은 네트워크 사이의 중간 규모 네트워크를 구분하기 위해 *B급 네트워크가* 사용됩니다 .

IP 주소를 네트워크 주소와 호스트 주소로 구분하는 기준은 네트워크의 클래스 분류입니다. 그림 7.1은 네트워크 클래스를 요약한 것으로, 이 장 전체에 걸쳐 더 자세히 설명하겠습니다.

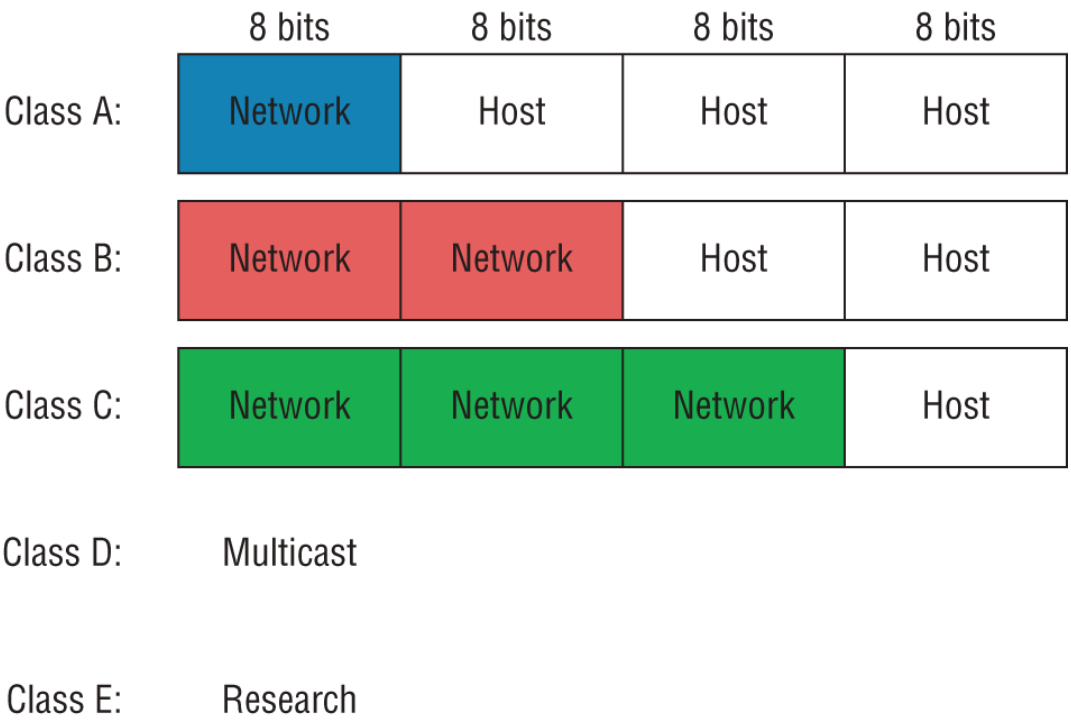

그림 7.1 세 가지 네트워크 유형 요약

효율적인 라우팅을 보장하기 위해 인터넷 설계자들은 각기 다른 네트워크 클래스에 대해 주소의 앞부분 비트에 대한 규칙을 정했습니다. 예를 들어, 라우터는 클래스 A 네트워크 주소가 항상 0으로 시작한다는 것을 알고 있으므로, 주소의 첫 번째 비트만 읽고도 패킷의 속도를 높일 수 있습니다. 바로 이 부분에서 주소 체계는 클래스 A, 클래스 B, 클래스 C 주소를 구분합니다. 앞으로 이 세 클래스의 차이점을 살펴본 후 클래스 D와 클래스 E 주소에 대해 설명하겠습니다. 지금은 클래스 A, B, C가 네트워크에서 호스트를 지정하는 데 사용되는 유일한 주소 범위라는 것만 알아두시면 됩니다.

A급 주소

클래스 A 네트워크 주소에서 첫 번째 바이트는 네트워크 주소로 할당되고, 나머지 세 바이트는 호스트 주소로 사용됩니다. 클래스 A 형식은 다음과 같습니다.

```
network.host.host.host
```

예를 들어, IP 주소 49.22.102.70에서 49는 네트워크 주소이고 22.102.70은 호스트 주소입니다. 이 특정 네트워크에 있는 모든 장치는 고유한 네트워크 주소인 49로 시작합니다.

클래스 A 네트워크 주소는 1바이트 길이이며, 해당 바이트의 첫 번째 비트는 예약되어 있고 나머지 7비트는 조작 또는 주소 지정에 사용할 수 있습니다. 따라서 이론적으로 생성할 수 있는 클래스 A 네트워크의 최대 개수는 128개입니다. 그 이유는 무엇일까요? 7비트 각각은 0 또는 1일 수 있으며, 2^7은 ^{128} 이 되기 때문입니다.

IP 주소 체계 설계자들은 클래스 A 네트워크 주소의 첫 번째 바이트의 첫 번째 비트가 항상 꺼져 있어야 한다고 규정했습니다. 즉, 클래스 A 주소의 첫 번째 바이트는 0에서 127 사이의 값이어야 합니다.

다음 네트워크 주소를 고려해 보세요.

```
0xxxxxxx
```

나머지 7비트를 모두 끈 다음 모두 켜면 클래스 A 네트워크 주소 범위를 찾을 수 있습니다.

```
00000000 = 0
01111111 = 127
```

따라서 클래스 A 네트워크는 0에서 127 사이의 첫 번째 옥텟으로 정의되며, 이 값은 그보다 작거나 클 수 없습니다.

문제를 더욱 복잡하게 만드는 것은, 모든 비트가 0인 네트워크 주소(0000 0000)는 기본 경로를 지정하기 위해 예약되어 있다는 점입니다(표 7.1 참조). 또한 진단용으로 예약된 주소 127도 사용할 수 없습니다. 즉, 실제로 클래스 A 네트워크 주소를 지정하는 데 사용할 수 있는 숫자는 1부터 126까지뿐입니다. 따라서 실제로 사용 가능한 클래스 A 네트워크 주소의 수는 128에서 2를 뺀 126개입니다.

표 7.1 예약된 IP 주소

주소	기능
네트워크 주소가 모두 0으로 되어 있습니다.	이는 "이 네트워크 또는 부문"을 의미하는 것으로 해석됩니다.
모든 문자가 1인 네트워크 주소	"모든 네트워크"를 의미하는 것으로 해석됩니다.
네트워크 127.0.0.1	루프백 테스트용으로 예약되어 있습니다. 로컬 호스트를 지정하고 해당 호스트가 네트워크 트래픽을 발생시키지 않고 자체적으로 테스트 패킷을 보낼 수 있도록 합니다.
호스트 주소가 모두 0으로 되어 있습니다.	"네트워크 주소" 또는 지정된 네트워크 상의 모든 호스트를 의미하는 것으로 해석됩니다.
모든 문자가 1인 호스트 주소	지정된 네트워크의 "모든 호스트"를 의미하는 것으로 해석됩니다. 예를 들어, 126.255.255.255는 네트워크 126(클래스 A 주소)의 "모든 호스트"를 의미합니다.
전체 IP 주소가 모두 0으로 설정되었습니다.	시스코 라우터에서 기본 경로를 지정하는 데 사용됩니다. "모든 네트워크"를 의미할 수도 있습니다.
전체 IP 주소를 모두 1로 설정합니다 (255.255.255.255와 동일).	현재 네트워크의 모든 호스트에 브로드캐스트합니다. 때때로 "모든 호스트에 1을 브로드캐스트" 또는 제한적 브로드캐스트라고도 합니다.

각 클래스 A 주소는 컴퓨터의 호스트 주소를 나타내는 3바이트(24비트 위치)로 구성됩니다. 즉, 2^{24}, 즉 16,777,216가지의 고유한 조합이 가능하며, 따라서 각 클래스 A 네트워크에는 정확히 그만큼의 고유한 호스트 주소가 존재할 수 있습니다. 모

든 비트가 0이거나 모두 1인 두 가지 패턴의 호스트 주소는 예약되어 있으므로, 클래스 A 네트워크에서 실제로 사용 가능한 최대 호스트 수는 2^{24}에서 ^{2} 를 뺀 16,777,214개입니다. 어떤 경우든, 네트워크 세그먼트에 이처럼 엄청난 수의 호스트가 존재한다는 것을 알 수 있습니다!

다음은 클래스 A 네트워크 주소에서 유효한 호스트 ID를 확인하는 방법의 예입니다.

- 호스트 비트를 모두 끄면 네트워크 주소는 10.0.0.0이 됩니다.
- 호스트 비트의 모든 부분은 브로드캐스트 주소인 10.255.255.255입니다.

유효한 호스트 주소는 네트워크 주소와 브로드캐스트 주소 사이에 있는 숫자들입니다. 즉, 10.0.0.1부터 10.255.255.254까지입니다. 0과 255도 유효한 호스트 ID가 될 수 있다는 점에 유의하세요. 유효한 호스트 주소를 찾을 때 기억해야 할 것은 호스트 비트가 동시에 모두 꺼지거나 모두 켜질 수 없다는 것입니다.

클래스 B 주소

클래스 B 네트워크 주소에서 처음 2바이트는 네트워크 주소로 할당되고 나머지 2바이트는 호스트 주소로 사용됩니다. 형식은 다음과 같습니다.

```
network.network.host.host
```

예를 들어, IP 주소 172.16.30.56에서 네트워크 주소는 172.16이고 호스트 주소는 30.56입니다.

네트워크 주소는 2바이트(각 8비트)이므로 2^{16}개의 ^{고유} 한 조합이 가능합니다. 하지만 인터넷 설계자들은 모든 클래스 B 네트워크 주소가 1로 시작하고 그 다음이 0이어야 한다고 결정했습니다. 따라서 14개의 비트 위치를 사용할 수 있으므로 실제로는 16,384개(즉, 2^{14}개 $^)$ 의 고유한 클래스 B 네트워크 주소를 만들 수 있습니다.

클래스 B 네트워크에서 RFC(Request For Comments)에 따르면 첫 번째 바이트의 첫 번째 비트는 항상 켜져 있어야 하고 두 번째 비트는 항상 꺼져 있어야 합니다. 나머지 6비트를 모두 끈 다음 모두 켜면 클래스 B 네트워크의 범위를 알 수 있습니다.

```
10000000 = 128
10111111 = 191
```

보시는 바와 같이, 첫 번째 바이트가 128에서 191 사이로 구성될 때 클래스 B 네트워크가 정의됩니다.

클래스 B 주소는 호스트 주소에 2바이트를 사용합니다. 이는 2^{16} 에서 예약된 두 패턴(모두 0과 모두 1)을 뺀 값으로, 클래스 B 네트워크당 총 65,534개의 호스트 주소를 사용할 수 있습니다.

다음은 클래스 B 네트워크에서 유효한 호스트를 찾는 방법의 예입니다.

- 호스트 관련 모든 비트를 끄면 네트워크 주소는 172.16.0.0이 됩니다.
- 호스트 비트가 모두 켜져 있는 경우 브로드캐스트 주소는 172.16.255.255입니다.

유효한 호스트는 네트워크 주소와 브로드캐스트 주소 사이에 있는 숫자, 즉 172.16.0.1부터 172.16.255.254까지입니다.

클래스 C 주소

클래스 C 네트워크 주소의 처음 3바이트는 네트워크 주소 부분에 할당되고, 호스트 주소에는 단 1바이트만 남습니다. 형식은 다음과 같습니다.

```
network.network.network.host
```

예시 IP 주소 192.168.100.102를 사용하면 네트워크 주소는 192.168.100이고 호스트 주소는 102입니다.

클래스 C 네트워크 주소에서 처음 3비트 위치는 항상 이진수 110입니다. 계산은 다음과 같습니다. 3바이트(24비트)에서 예약된 3비트 위치를 빼면 21비트가 남습니다. 따라서 2^{21} , 즉 2,097,152개의 클래스 C 네트워크가 가능합니다.

클래스 C 네트워크의 경우, RFC에서는 첫 번째 옥텟의 처음 2비트는 항상 켜져 있지만 세 번째 비트는 절대 켜져 있을 수 없다고 정의합니다. 이전 클래스와 동일한 과정을 따라 이진수를 십진수로 변환하여 범위를 찾습니다. 다음은 클래스 C 네트워크의 범위입니다.

```
11000000 = 192
11011111 = 223
```

따라서 IP 주소 범위가 192부터 223까지인 경우, 해당 주소는 클래스 C IP 주소임을 알 수 있습니다.

각 클래스 C 네트워크는 호스트 주소에 1바이트를 사용합니다. 따라서 총 2^8, 즉 256개의 호스트 주소를 사용할 수 있으며, 여기서 예약된 0과 1로 구성된 두 패턴을 제외하면 각 클래스 C 네트워크에는 총 254개의 호스트 주소를 사용할 수 있습니다.

다음은 클래스 C 네트워크에서 유효한 호스트 ID를 찾는 방법의 예입니다.

- 호스트 관련 모든 비트가 꺼진 상태의 네트워크 ID는 192.168.100.0입니다.
- 호스트 비트가 모두 켜져 있는 경우 브로드캐스트 주소는 192.168.100.255입니다.

유효한 호스트는 네트워크 주소와 브로드캐스트 주소 사이에 있는 숫자, 즉 192.168.100.1부터 192.168.100.254까지입니다.

클래스 D 및 E 주소

첫 번째 옥텟이 224에서 255 사이인 주소는 클래스 D 및 E 네트워크에 예약되어 있습니다. 클래스 D(224~239)는 멀티캐스트 주소로 사용되고, 클래스 E(240~255)는 과학 연구 목적으로 사용됩니다. 멀티캐스트 주소 범위는 224.0.0.0부터 239.255.255.255까지라는 점을 기억해야 합니다. 멀티캐스트에 대한 자세한 내용은 이 장의 뒷부분에서 다룹니다.

네트워크 주소의 특수 용도

일부 IP 주소는 특별한 용도로 예약되어 있으므로 네트워크 관리자는 해당 주소를 호스트에 할당할 수 없습니다. 표 7.1에는 이러한 특별한 IP 주소 그룹에 속한 호스트와 그 이유가 나와 있습니다.

사설 IP 주소(RFC 1918)

IP 주소 체계를 만든 사람들은 *사설 IP 주소* 라고 부르는 것도 만들었습니다 . 이 주소는 사설 네트워크에서 사용할 수 있지만 인터넷을 통해 라우팅할 수는 없습니다. 이는 필요한 보안 수준을 확보하기 위한 것이며, 동시에 귀중한 IP 주소 공간을 절약하는 데에도 도움이 됩니다.

만약 모든 네트워크의 모든 호스트가 실제로 라우팅 가능한 IP 주소를 가져야 한다면, 우리는 이미 오래전에 할당할 수 있는 IP 주소가 모두 소진되었을 것입니다. 하

지만 사설 IP 주소를 사용하면 ISP, 기업, 그리고 가정 사용자들은 네트워크를 인터넷에 연결하는 데 필요한 실제 IP 주소의 수가 상대적으로 적습니다. 이는 내부 네트워크에 사설 IP 주소를 사용하면서도 충분한 성능을 발휘할 수 있기 때문에 경제적인 이점입니다.

이러한 작업을 수행하기 위해 ISP와 기업, 즉 최종 사용자(누구든 상관없이)는 NAT(네트워크 주소 변환)라는 것을 사용해야 합니다. NAT는 기본적으로 사설 IP 주소를 인터넷에서 사용할 수 있는 공용 IP 주소로 변환하는 역할을 합니다. NAT는 외부 사용자가 이러한 IP 주소를 볼 수 없도록 보안을 제공합니다. 외부 사용자는 사설 IP 주소가 매핑된 공용 IP 주소만 볼 수 있습니다. 또한 동일한 사설 네트워크 내의 여러 장치가 동일한 실제 IP 주소를 사용하여 인터넷으로 데이터를 전송할 수 있습니다. 이러한 방식을 통해 엄청난 양의 주소 공간을 절약할 수 있으며, 이는 우리 모두에게 매우 유익한 일입니다!

표 7.2 에는 RFC 1918에서 예약된 개인 주소가 나열되어 있습니다.

표 7.2 RFC 1918에 따라 예약된 IP 주소 공간

주소 클래스	예약된 주소 공간
A급	10.0.0.0부터 10.255.255.255까지 (접두사 /8)
클래스 B	172.16.0.0부터 172.31.255.255까지 (접두사 /12)
클래스 C	192.168.0.0부터 192.168.255.255까지 (접두사 /16)

실제 시나리오

그렇다면 어떤 사설 IP 주소를 사용해야 할까요?

정말 좋은 질문입니다. 네트워크를 설정할 때 A급, B급, 아니면 C급 사설 주소를 사용해야 할까요? 샌프란시스코에 있는 Acme Corporation을 예로 들어보겠습니다. 이 회사는 새 건물로 이전하면서 완전히 새로운 네트워크가 필요합니다(정말 좋은 일이죠!). 14개의 부서가 있고 각 부서에는 약 70명의 사용자가 있습니다. 아마 C급 주소를 3~4개 정도 사용할 수 있을 것 같고, 아니면 재미 삼아 B급이나 A급 주소를 하나 더 사용할 수도 있겠죠.

컨설팅 업계에서 통용되는 일반적인 원칙은 기업 네트워크를 구축할 때 규모와 관계없이 클래스 A 네트워크 주소를 사용하는 것입니다. 클래스 A 주소는 가장 큰 유연성과 확장성을 제공하기 때문입니다. 예를 들어, 10.0.0.0 네트워크 주소에 /24 마스크를 사용하면 각각 254개의 호스트를 가진 65,536개의 네트워크를 생성할 수 있습니다. 이러한 네트워크 설계는 확장에 매우 유리합니다! 그런 다음 CIDR(Classless Inter-Domain Routing, 가변 길이 서브넷 마스크 또는 VLSM이라고도 함)을 사용하여 이 네트워크 주소 공간을 서브넷으로 분할합니다. CIDR은 IP 주소를 낭비하지 않고 각 부서 또는 건물에 필요한 호스트 수만 할당합니다. (/24는 서브넷 마스크의 32비트 중 24비트가 서브넷팅에 사용됨을 나타냅니다. CIDR과 서브넷팅에 대한 자세한 내용은 8장 에서 다룹니다 .)

하지만 가정용 네트워크를 구축하는 경우, 사람들이 이해하고 설정하기 가장 쉬운 클래스 C 주소를 선택하는 것이 좋습니다. 기본 클래스 C 마스크를 사용하면 254개의 호스트를 연결할 수 있는 네트워크 하나가 생성되는데, 이는 가정용 네트워크에 충분한 용량입니다.

Acme Corporation의 경우, /24 마스크(*x 는 각 부서의 서브넷 마스크)를 사용하는 깔끔한 10.1 x* .0 규격 덕분에 설계, 설치 및 문제 해결이 용이합니다.

가상 IP(VIP)

장치의 네트워크 인터페이스에 할당된 실제 사설 IP 주소를 공용 IP 주소로 대체하면, 해당 공용 IP 주소는 *가상 IP 주소* 의 한 예가 됩니다 . 즉, 실제 물리적 네트워크 인터페이스에 대응하지 않습니다. 대표적인 예로 라우터의 물리적 인터페이스에 구성된 서브인터페이스를 들 수 있는데, 이를 통해 하나의 인터페이스에 여러 개의 IP 주소 또는 서브넷을 생성할 수 있습니다.

가상 IP 주소의 예는 이 외에도 여러 가지가 있습니다. 예를 들어, 웹 프록시 서버가 패킷을 인터넷으로 전송하기 전에 발신자의 IP 주소 대신 자신의 IP 주소를 사용하는 경우가 있는데, 이는 가상 IP 주소를 생성하는 또 다른 예입니다.

APIPA

6장 "인터넷 프로토콜 소개" 에서 이미 다뤘 지만, 여기서 다시 한번 강조할 가치가 있습니다. 스위치나 허브로 여러 호스트가 연결되어 있고 DHCP 서버가 없는 경우 어떻게 해야 할까요? 호스트에 고정 IP 주소를 추가하거나 APIPA(자동 개인 IP 주소 지정)를 사용할 수 있습니다. APIPA는 권장하지 않지만, 하나의 "기능"이므로 기억해 두었다가 두 장에 걸쳐 언급했습니다!

APIPA를 사용하면 클라이언트가 IP 주소와 서브넷 마스크를 자동으로 구성할 수 있습니다. 이는 DHCP 서버를 사용할 수 없을 때 호스트 간 통신에 필요한 최소 정보입니다. 이러한 점에서 APIPA는 DHCP 장애 조치 방식과 유사하다고 볼 수 있습니다. 모든 호스트가 APIPA 주소를 설정하면 호스트 간 통신은 가능하지만, 기본 게이트웨이와 같이 정적으로 구성된 주소와는 통신할 수 없습니다.

APIPA의 IP 주소 범위는 169.254.0.1부터 169.254.255.254까지입니다. 클라이언트는 또한 기본 클래스 B 서브넷 마스크인 255.255.0.0으로 자체 구성됩니다.

하지만 회사 네트워크에서 DHCP 서버를 실행 중인데 호스트가 APIPA IP 주소 범위를 사용하고 있다고 표시되는 경우, 이는 호스트의 DHCP 클라이언트가 작동하지 않거나 DHCP 서버가 다운되었거나 네트워크 문제로 연결할 수 없다는 의미입니다. 예를 들어, DHCP 클라이언트를 비활성화된 포트에 연결하면 호스트는 APIPA 주소를 할당받게 됩니다. 호스트가 APIPA 주소 범위를 사용하는 것을 반기는 사람은 거의 없을 것입니다! 사용자가 인터넷에 연결할 수 없고 IP 주소가 APIPA 범위에 속하는 경우, DHCP 서버에 문제가 있을 가능성이 가장 높습니다.

IPv4 주소 유형

대부분의 사람들은 *브로드캐스트* 라는 용어를 일반적인 의미로 사용하며, 대부분의 경우 그 의미를 이해합니다. 하지만 항상 그런 것은 아닙니다. 예를 들어, "호스트가 라우터를 통해 DHCP 서버로 브로드캐스트했다"라고 말할 수 있지만, 실제로 이런 일이 일어날 가능성은 매우 낮습니다.정확한 기술 용어를 사용하자면, 아마도 "DHCP 클라이언트가 IP 주소를 요청하는 브로드캐스트를 보냈고, 라우터가 이를 유니캐스트 패킷으로 DHCP 서버로 전달했다"라는 의미일 겁니다. 아, 그리고 IPv4에서는 브로드캐스트가 매우 중요하지만, IPv6에서는 브로드캐스트가 전혀 전송되지 않는다는 점을 기억하세요. 이 부분은 잠시 후에 자세히 설명하겠습니다!

네, 앞 장에서 브로드캐스트 주소에 대해 여러 번 언급했고, 다양한 IP 주소의 예시도 보여드렸습니다. 하지만 아직 브로드캐스트 주소와 관련된 용어와 사용법에 대해서는 자세히 다루지 않았는데요, 이제 그럴 때가 된 것 같습니다. 그래서 IPv4 주소 유형 네 가지를 정의해 보겠습니다.

- **레이어 2 브로드캐스트** 는 LAN의 모든 노드로 전송됩니다.
- **브로드캐스트(레이어 3)** 는 네트워크의 모든 노드로 전송됩니다.
- **유니캐스트** 는 단일 인터페이스에 대한 주소이며, 패킷을 단일 목적지 호스트로 전송하는 데 사용됩니다.
- **멀티캐스트 는 단일 소스에서 전송되어 서로 다른 네트워크에 있는 여러 장치로 전송되는 패킷입니다. 이를** *일대다 통신* 이라고 합니다 .

레이어 2 브로드캐스트

먼저, 레이어 2 브로드캐스트는 하드웨어 브로드캐스트라고도 하며, LAN 내에서만 전송되고 LAN 경계(라우터)를 넘어서지 않는다는 점을 이해해야 합니다.

일반적인 하드웨어 주소는 6바이트(48비트)이며 0c.43.a4.f3.12.c2와 같은 형식입니다. 브로드캐스트는 이진수로는 모두 1이고, 16진수로는 모두 *F* 로 표현되며, FF.FF.FF.FF.FF.FF와 같습니다.

레이어 3 브로드캐스트

다음으로 레이어 3에는 일반적인 브로드캐스트 주소가 있습니다. 브로드캐스트 메시지는 브로드캐스트 도메인의 모든 호스트에 도달하도록 설계되었습니다. 이러한 브로드캐스트는 호스트 비트가 모두 활성화된 네트워크 브로드캐스트입니다.

이미 익숙한 예시를 하나 들어보겠습니다. 네트워크 주소 172.16.0.0의 브로드캐스트 주소는 172.16.255.255입니다. 모든 호스트 비트가 켜져 있는 것이죠. 브로드캐스트는 255.255.255.255처럼 "모든 네트워크 및 모든 호스트"를 대상으로 할 수도 있습니다.

브로드캐스트 메시지의 좋은 예는 ARP(주소 확인 프로토콜) 요청입니다. 호스트가 패킷을 받으면 목적지의 논리적 주소(IP)를 알고 있습니다. 패킷을 목적지까지 전달하려면 목적지가 다른 IP 네트워크에 있는 경우 호스트는 패킷을 기본 게이트웨이로 전달해야 합니다. 목적지가 로컬 네트워크에 있는 경우 출발지는 패킷을 목적지로 직접 전달합니다. 출발지는 프레임을 전달해야 할 MAC 주소를 모르기 때문에 브로드캐스트를 전송합니다. 이 브로드캐스트는 로컬 브로드캐스트 도메인에 있는 모든 장치가 수신합니다. 이 브로드캐스트는 본질적으로 "IP 주소 192.168.2.3의

소유자라면 MAC 주소를 저에게 전달해 주십시오"라는 의미이며, 출발지는 필요한 정보를 제공합니다.

유니캐스트 주소

유니캐스트 주소는 단일 인터페이스에 할당되며, 이 용어는 IPv4와 IPv6 모두에서 호스트 인터페이스의 IP 주소를 설명하는 데 사용됩니다.

멀티캐스트 주소(클래스 D)

멀티캐스트는 완전히 다른 개념입니다. 언뜻 보기에는 유니캐스트와 브로드캐스트 통신의 혼합처럼 보이지만, 정확히는 그렇지 않습니다. 멀티캐스트는 브로드캐스트와 유사하게 지점 간 통신을 가능하게 하지만, 그 방식은 다릅니다. *멀티캐스트* 의 핵심 은 브로드캐스트 도메인의 모든 호스트에 메시지를 전송하지 않고도 여러 수신자가 메시지를 받을 수 있도록 한다는 점입니다. 하지만 이는 기본 동작이 아니라, 올바르게 설정했을 때 가능한 동작 방식입니다!

멀티캐스트는 메시지나 데이터를 IP 멀티캐스트 그룹 주소로 전송하는 방식으로 작동합니다. 라우터는 브로드캐스트와 달리 패킷의 복사본을 특정 그룹 주소를 구독하는 모든 인터페이스로 전달합니다. 이것이 멀티캐스트가 브로드캐스트 메시지와 다른 점입니다. 멀티캐스트 통신에서는 이론적으로 패킷 복사본이 구독한 호스트에만 전송됩니다. 여기서 '이론상'이란, 예를 들어 224.0.0.10으로 향하는 멀티캐스트 패킷(EIGRP 패킷이며 EIGRP 프로토콜을 실행하는 라우터만 읽을 수 있음)을 수신한다고 가정해 보겠습니다. 브로드캐스트 LAN(이더넷은 브로드캐스트 다중 액세스 LAN 기술임)의 모든 호스트는 멀티캐스트 그룹에 속해 있지 않으면 프레임을 수신하고 목적지 주소를 읽은 후 즉시 프레임을 폐기합니다. 이는 PC 처리 능력을 절약하는 것이지 LAN 대역폭을 소모하는 것은 아닙니다. 멀티캐스팅은 신중하게 구현하지 않으면 심각한 LAN 혼잡을 유발할 수 있습니다.

사용자 또는 애플리케이션이 구독할 수 있는 다양한 그룹이 있습니다. 멀티캐스트 주소 범위는 224.0.0.0부터 239.255.255.255까지입니다. 보시다시피, 이 주소 범위는 클래스 기반 IP 할당 방식에 따라 IP 클래스 D 주소 공간에 속합니다.

인터넷 프로토콜 버전 6(IPv6)

IPv6는 "차세대 인터넷 프로토콜"로 불리며, 원래 IPv4의 불가피한 주소 고갈 위기에 대한 해결책으로 개발되었습니다. IPv6에 대해 이미 어느 정도 들어보셨겠지만, 유연성, 효율성, 역량, 그리고 최적화된 기능을 제공하여 끊임없이 증가하는 우리의 요구를 진정으로 충족시키기 위해 지속적으로 개선되어 왔습니다. 이전 프로토콜인

IPv4의 용량은 이에 비하면 훨씬 부족하며, 바로 이 때문에 IPv4는 결국 역사 속으로 완전히 사라지게 될 것입니다.

IPv6 헤더와 주소 구조는 완전히 개편되었으며, IPv4에서는 부가적인 기능에 불과했던 많은 기능들이 IPv6에서는 완전한 표준으로 포함되었습니다. IPv6는 앞으로 다가올 인터넷의 엄청난 요구 사항을 처리할 수 있도록 완벽하게 준비되어 있습니다.

IPv6가 필요한 이유는 무엇일까요?

간단히 말해서, 우리는 소통해야 하는데 현재 시스템으로는 더 이상 충분하지 않기 때문입니다. 마치 포니 익스프레스가 항공 우편과 경쟁할 수 없었던 것과 같죠. 대역폭과 IP 주소를 절약하기 위한 기발한 새로운 방법을 고안하는 데 얼마나 많은 시간과 노력을 투자했는지 생각해 보세요.

현실은 이렇습니다. 네트워크에 연결되는 사람과 기기의 수는 매일 증가하고 있습니다. 이는 결코 나쁜 일이 아닙니다. 우리는 끊임없이 더 많은 사람들과 소통할 수 있는 새롭고 흥미로운 방법들을 발견하고 있으며, 이는 오늘날 우리 문화의 필수적인 부분이 되었습니다. 사실, 이제는 거의 기본적인 인간의 욕구라고 할 수 있습니다. 하지만 전망이 그리 밝지만은 않습니다. 이 장의 서두에서 언급했듯이, 현재 우리의 통신 능력에 필수적인 IPv4 주소가 곧 고갈될 것이기 때문입니다. IPv4는 이론상으로 약 43억 개의 주소만 사용할 수 있지만, 실제로 그마저도 모두 사용하지 못하는 경우가 많습니다. 기기에 할당될 수 있는 주소는 약 2억 5천만 개에 불과합니다. 물론, CIDR(Classless Inter-Domain Routing, 가변 길이 서브넷 마스크 또는 VLSM이라고도 함)과 NAT/PAT의 사용은 불가피한 주소 부족 현상을 늦추는 데 도움이 되었지만, 현실은 주소가 고갈될 것이고, 몇 년 안에 그렇게 될 것이라는 점입니다. 중국은 엄청난 인구에 비해 인터넷 접속률이 매우 낮고, 그곳의 기업들은 분명히 인터넷에 진출하고 싶어 합니다. 다양한 수치를 제시하는 보고서들이 많지만, 제가 과장하는 것이 아니라는 것을 확신하려면 현재 세계 인구가 약 78억 명인데, 그중 59% 정도만 인터넷에 연결되어 있다는 사실만 생각해 보면 됩니다. 정말 놀라운 수치죠! IPv6가 바로 그 문제를 해결해 줄 것입니다!

저 통계는 IPv4의 용량 한계 때문에 모든 사람이 IP 주소를 가진 컴퓨터를 한 대씩 갖는 것조차 불가능하다는 불편한 진실을 여실히 보여주고 있습니다. 하물며 우리가 매일 사용하는 다른 기기들에 IP 주소를 할당하는 것은 말할 것도 없죠. 저도 컴퓨터를 여러 대 가지고 있고, 여러분도 마찬가지일 겁니다. 게다가 전화기, 노트북, 게임 콘솔, 팩스, 라우터, 스위치 등 매일 사용하는 수많은 기기들은 말할 것도 없고요! 그러니 IP 주소가 고갈되어 우리가 알고 있는 방식으로 서로 연결할 수 없게 되기 전에 뭔가 조치를 취해야 한다는 것이 분명해졌습니다. 그리고 그 "뭔가"가 바로 IPv6를 도입하는 것입니다.

IPv6의 장점 및 활용법

IPv6의 놀라운 점은 무엇일까요? IPv6가 우리가 직면한 문제에 대한 진정한 해답일까요? IPv4에서 IPv6로 업그레이드할 가치가 정말 있을까요? 모두 좋은 질문입니다. 아마 더 많은 질문이 떠오를지도 모릅니다. 물론, 예전부터 잘 알려진 "변화에 대한 저항"을 가진 사람들도 있겠지만, 그들의 말에 귀 기울이지 마세요. 만약 우리가 과거에 그랬다면, 지금도 우편물이 말을 타고 배달되는 데 몇 주, 몇 달씩 기다려야 했을 겁니다. 이제 분명한 답은 "네!"입니다. IPv6는 충분한 주소(3.4×10^{38} = 확실히 충분함)를 제공할 뿐만 아니라, 마이그레이션에 필요한 비용, 시간, 노력을 충분히 보상해 줄 다양한 기능들을 갖추고 있습니다.

오늘날의 네트워크와 인터넷에는 IPv4가 만들어졌을 당시에는 고려하지 못했던 수많은 예상치 못한 요구 사항들이 있습니다. 우리는 이러한 요구 사항들을 표준으로 의무화하는 대신, 구현을 오히려 더 어렵게 만드는 여러 가지 추가 기능들을 통해 보완해 왔습니다. IPv6는 기본적으로 이러한 기능들을 개선하고 표준으로 의무화했습니다. 이러한 새로운 표준 중 하나가 바로 종단 간 보안을 제공하는 IPSec입니다. 또 다른 유용한 기능은 *모빌리티(Mobility)* 로 , 이름에서 알 수 있듯이 장치가 연결을 끊지 않고 한 네트워크에서 다른 네트워크로 로밍할 수 있도록 해줍니다.

하지만 진정한 혁신은 효율성 향상에 있습니다! 우선, IPv6 패킷 헤더의 필드 수가 절반으로 줄었고, 64비트로 정렬되어 있어 처리 속도가 획기적으로 향상되었습니다. IPv4와 비교하면 조회 속도가 빛의 속도에 가깝습니다. 기존 IPv4 헤더에 포함되던 대부분의 정보는 제거되었지만, 이제는 기본 헤더 필드 뒤에 선택적 확장 헤더 형태로 해당 정보 또는 일부를 다시 포함할 수 있습니다.

물론 앞서 이야기했던 것처럼 주소의 방대한 규모(3.4×10^{38})가 있습니다. 그런데 이 주소들은 어디서 나온 걸까요? 크리스 앤젤이라는 천재 과학자가 갑자기 나타나서 뿅 하고 나타나게 한 걸까요 ? *당연히* 아니겠지만, 이렇게 엄청나게 늘어난 주소는 분명 어딘가에서 비롯된 것이겠죠? 바로 IPv6가 훨씬 더 큰 주소 공간을 제공하기 때문입니다. 즉, 주소 자체가 훨씬 더 커졌다는 뜻입니다. 실제로 네 배나 더 커졌습니다! IPv6 주소는 128비트 길이이며, 걱정 마세요. 다음 섹션인 "IPv6 주소 지정 및 표현"에서 주소를 각 요소별로 자세히 설명해 드리겠습니다. 지금은 이 추가 공간 덕분에 주소 공간 내에서 더 많은 계층 구조를 만들고 더욱 유연한 주소 아키텍처를 구현할 수 있다는 점만 알아두시면 됩니다. 또한 주소를 훨씬 효율적으로 집계할 수 있기 때문에 라우팅이 훨씬 더 효율적이고 확장 가능해집니다. 그리고 IPv6는 호스트와 네트워크에 여러 개의 주소를 할당할 수 있도록 지원합니다. 또한, 새로운 IP 버전에는 멀티캐스트 통신(하나의 장치가 여러 호스트 또는 특정 그룹으로 메시지를 전송하는 것)의 확장된 사용이 포함되어 있어 통신이 더욱 구체화되므로 네트워크 효율성 향상에 기여할 것입니다.

IPv4는 브로드캐스트를 매우 많이 사용하는데, 이로 인해 여러 문제가 발생합니다. 그중 가장 심각한 것은 바로 브로드캐스트 스톰입니다. 이는 제어되지 않는 브로드캐스트 트래픽의 폭증으로, 네트워크 전체를 마비시키고 대역폭을 모두 소모해 버릴 수 있습니다. 브로드캐스트 트래픽의 또 다른 문제점은 네트워크상의 모든 장치에 영향을 미친다는 것입니다. 브로드캐스트가 전송되면 모든 장치는 작업을 중단하고 해당 트래픽을 분석해야 하는데, 이는 브로드캐스트가 자신을 대상으로 한 것인지 여부와는 관계없습니다.

하지만 모두 웃으세요! IPv6에서는 브로드캐스트라는 개념이 없습니다. 대신 멀티캐스트 트래픽을 사용하기 때문입니다. 그리고 두 가지 다른 통신 방식이 있습니다. IPv4와 동일한 유니캐스트와 *애니캐스트* 라는 새로운 방식이 있습니다 . 애니캐스트 통신을 사용하면 동일한 주소를 여러 장치에 할당할 수 있습니다. 따라서 이러한 방식으로 주소가 지정된 장치로 트래픽이 전송되면 동일한 주소를 공유하는 가장 가까운 호스트로 라우팅됩니다. 이것은 시작에 불과합니다. 이 장의 뒷부분 "주소 유형" 섹션에서 다양한 통신 방식에 대해 더 자세히 알아보겠습니다.

IPv6 주소 지정 및 표현

IPv4 주소 체계에서 IP 주소의 구조와 사용 방식을 이해하는 것이 중요했던 것처럼, IPv6에서도 마찬가지로 중요합니다. IPv6 주소는 128비트로 IPv4 주소보다 훨씬 크다는 사실을 이미 알고 계실 겁니다. 이러한 점과 주소 사용 방식의 변화 때문에 IPv6 관리가 더 복잡할 것이라고 짐작하셨을 것입니다. 하지만 걱정하지 마세요! 제가 기본적인 내용부터 차근차근 설명해 드리겠습니다. 주소의 형태, 작성 방법, 그리고 일반적인 사용 사례들을 알려드리겠습니다. 처음에는 조금 생소하게 느껴질 수 있지만, 곧 익숙해지실 겁니다.

그럼 그림 7.2 를 살펴보겠습니다 . 이 그림은 IPv6 주소를 각 부분별로 나누어 보여줍니다.

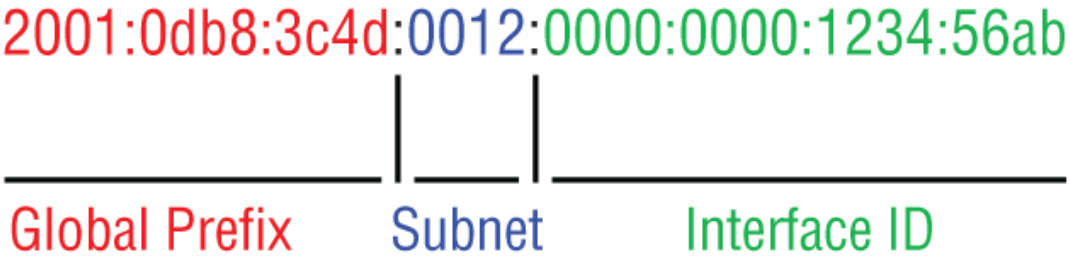

그림 7.2 IPv6 주소 예시

보시다시피, 주소가 훨씬 더 길어졌습니다. 그런데 또 무엇이 다를까요? 우선, 숫자 그룹이 네 개가 아니라 여덟 개라는 점, 그리고 그 그룹들이 마침표 대신 콜론으로 구분되어 있다는 점을 주목하세요. 그리고 잠깐만요... 주소에 문자가 있네요! 네, 맞

습니다. 이 주소는 MAC 주소처럼 16진수로 표현되어 있습니다. 즉, 16비트 16진수 블록이 여덟 개 있고, 각 블록은 콜론으로 구분되어 있다고 할 수 있습니다. 벌써부터 입에 착 달라붙는 주소인데, 아마 아직 소리 내어 읽어보지도 않으셨겠죠?

IPv6를 테스트하기 위해 테스트 네트워크를 설정할 때 한 가지 더 말씀드리고 싶은 점이 있습니다. 아마 IPv6를 사용해 보고 싶으실 테니까요. 웹 브라우저를 사용하여 IPv6 장치에 HTTPS 연결을 시도할 때는 주소를 입력할 때 반드시 대괄호로 묶어야 합니다. 왜냐하면 콜론(:)은 이미 브라우저에서 포트 번호를 지정하는 데 사용되고 있기 때문입니다. 따라서 주소를 대괄호로 묶지 않으면 브라우저가 해당 정보를 인식할 수 없게 됩니다.

이것이 어떻게 보이는지 예시를 보여드리겠습니다.

```
https://[2001:0db8:3c4d:0012:0000:0000:1234:56ab]/default.html
```

물론, 가능하다면 목적지를 지정할 때 이름(예: www.lammle.com)을 사용하는 것이 가장 좋겠지만, 불편하더라도 어쩔 수 없이 주소 번호를 직접 입력해야 하는 경우가 있습니다. IPv6를 구현할 때 DNS가 얼마나 중요한지 이제 분명해졌을 것입니다.

축약된 표현

다행히도 이렇게 긴 주소를 작성할 때 도움이 될 만한 몇 가지 요령이 있습니다. 우선, 주소의 일부를 생략하여 간략하게 만들 수 있는데, 그러려면 몇 가지 규칙을 따라야 합니다. 첫째, 어떤 부분이든 생략할 수 있습니다.각 블록의 앞에 0을 붙입니다. 이렇게 하면 앞서 보여드린 주소 예시는 다음과 같이 표시됩니다.

```
2001:db8:3c4d:12:0:0:1234:56ab
```

확실히 개선된 점입니다. 적어도 불필요한 0을 모두 입력할 필요는 없으니까요! 하지만 0으로만 채워진 블록은 어떻게 처리해야 할까요? 그런 부분도 어느 정도는 없앨 수 있습니다. 앞서 예시로 든 주소를 다시 살펴보면, 두 개의 0 블록을 이중 콜론(:)으로 바꾸면 제거할 수 있습니다. 예를 들어 다음과 같이 말이죠.

```
2001:db8:3c4d:12::1234:56ab
```

멋지네요! 연속된 0 블록을 콜론 두 개로 바꾸셨군요. 이렇게 하려면 주소에서 연속된 0 블록은 하나만 바꿀 수 있다는 규칙을 따라야 합니다. 따라서 주소에 0 블록이 네 개 있고 각각 분리되어 있다면, 모든 블록을 바꿀 수는 없습니다. 다음 예시를 확인해 보세요.

```
2001:0000:0000:0012:0000:0000:1234:56ab
```

그리고 콜론 두 개를 이렇게 두 번 사용할 *수 없다*는 점을 알아두세요 .

```
2001::12::1234:56ab
```

대신, 이것이 당신이 할 수 있는 최선입니다.

```
2001::12:0:0:1234:56ab
```

이 예시가 가장 적합한 이유는 두 쌍의 0을 제거하면 해당 주소를 보는 장치가 0이 어디에 다시 들어가야 하는지 알 수 없기 때문입니다. 기본적으로 라우터는 잘못된 주소를 보고 "첫 번째 콜론 두 개에 2블록을 넣고 두 번째 콜론 두 개에도 2블록을 넣어야 할까, 아니면 첫 번째 콜론 두 개에 3블록을 넣고 두 번째 콜론 두 개에 1블록을 넣어야 할까?"라고 판단하게 됩니다. 라우터에 필요한 정보가 없기 때문에 이러한 과정이 계속 반복되는 것입니다.

주소 유형

IPv4에서는 유니캐스트, 브로드캐스트, 멀티캐스트 주소가 있는데, 이는 기본적으로 우리가 통신하는 대상 또는 최소한 몇 대의 장치를 정의하는 역할을 합니다. 하지만 앞서 언급했듯이 IPv6에서는 애니캐스트 주소 유형이 도입되었습니다. 기존의 브로드캐스트 주소는 비효율적이고 번거로워 IPv6에서 더 이상 사용되지 않습니다.

하나의 인터페이스에 다양한 용도로 여러 유형의 IPv6 주소를 할당할 수 있으므로, 각 IPv6 주소 유형과 각 유형의 통신 방식을 알아보겠습니다.

- **유니캐스트 주소로 전송된 유니캐스트** 패킷은 IPv4와 마찬가지로 단일 인터페이스로 전달됩니다. 로드 밸런싱을 위해 여러 인터페이스가 동일한 주소를 사용할 수 있습니다.

- **글로벌 유니캐스트 주소** 는 일반적인 공용 라우팅 가능 주소이며, IPv4에서 전역 고유 주소와 동일한 방식으로 사용됩니다.
- **링크 로컬 주소** 는 IPv4의 APIPA 주소와 유사하게 라우팅용이 아니며 각 링크(LAN)마다 고유합니다. 편리한 도구로 생각하면 됩니다.이를 통해 회의를 위한 임시 LAN을 구성하거나 라우팅되지 않지만 로컬에서 파일과 서비스를 공유하고 액세스해야 하는 소규모 LAN을 만들 수 있습니다. 하지만 링크 로컬은 라우터 인터페이스에 연결되는 모든 LAN에서도 사용됩니다.
- **고유 로컬 주소(Unique Local Addresses,** ULA)는 라우팅 목적이 아닌 용도로 사용되지만, 거의 전 세계적으로 고유하기 때문에 다른 주소와 중복될 가능성은 매우 낮습니다. ULA는 사이트 로컬 주소를 대체하기 위해 설계되었으며, 기본적으로 IPv4 사설 주소와 거의 동일한 기능을 수행합니다. 즉, 사이트 내 통신을 허용하는 동시에 여러 로컬 네트워크로 라우팅될 수 있습니다. 링크 로컬 주소와 ULA의 차이점은 ULA는 조직 또는 회사 내에서 라우팅이 가능하다는 점입니다.
- **IPv4에서와 마찬가지로 멀티 캐스트** 주소로 지정된 패킷은 해당 멀티캐스트 주소로 식별되는 모든 인터페이스로 전달됩니다. 때때로 이러한 주소를 *일대다 주소라고 부르기도 합니다. IPv6에서 멀티캐스트 주소는 항상 FF* 로 시작하기 때문에 쉽게 구분할 수 있습니다 .
- **애니** 캐스트 주소는 멀티캐스트 주소와 마찬가지로 여러 인터페이스를 식별하지만, 중요한 차이점이 있습니다. 애니캐스트 패킷은 단 하나의 주소, 즉 라우팅 거리를 기준으로 정의된 첫 번째 IPv6 주소로만 전달됩니다. 그리고 이 주소가 특별한 이유는 하나의 주소를 여러 인터페이스에 적용할 수 있기 때문입니다. 이를 일대다 주소(one-to-one-of-many addresses)라고도 하지만, 그냥 애니캐스트라고 부르는 것이 훨씬 간단합니다. 이는 일대최근접 주소 지정(one-to-nearest addressing)이라고도 합니다.

IPv4에는 있는 특별한 예약 주소가 IPv6에도 있는지 궁금하실 겁니다. 네, 있습니다. 그것도 아주 많이요! 지금부터 하나씩 살펴보겠습니다.

특별 주소

표 7.3 에 나와 있는 주소와 주소 범위 중 나중에 반드시 사용하게 될 몇 가지를 나열해 보겠습니다 . 이 주소들은 모두 특정 용도로 특별하거나 예약되어 있지만, IPv4와 달리 IPv6는 매우 많은 주소를 제공하므로 몇 개를 예약해 두는 것은 전혀 문제가 되지 않습니다.

표 7.3 특수 IPv6 주소

주소	의미
0:0:0:0:0:0:0:0	::와 같습니다. 이는 IPv4의 0.0.0.0에 해당하며, 일반적으로 DHCP 기반 상태 저장 구성을 사용할 때 호스트가 IP 주소를 수신하기 전의 호스트 소스 주소입니다.
0:0:0:0:0:0:0:1	::1과 같습니다. IPv4에서 127.0.0.1에 해당합니다.
0::FFFF:192.168.100.1	IPv6/IPv4 혼합 네트워크 환경에서 IPv4 주소를 표기하는 방법은 다음과 같습니다.
2000::/3	인터넷 접속을 위해 할당된 글로벌 유니캐스트 주소 범위입니다.
FC00::/7	독특한 로컬 유니캐스트 범위.
FE80::/10	링크 로컬 유니캐스트 범위.
FF00::/8	멀티캐스트 범위.
3FFF:FFFF::/32	예시 및 자료용으로 예약되어 있습니다.
2001:0DB8::/32	예시 및 문서용으로도 사용됩니다.
2002::/16	IPv4에서 IPv6로의 전환 시스템인 6to4 터널링과 함께 사용됩니다. 이 구조를 통해 명시적인 터널 구성 없이 IPv6 패킷을 IPv4 네트워크를 통해 전송할 수 있습니다.

상태 비저장 주소 자동 구성(SLAAC)

자동 구성은 네트워크상의 장치가 링크 로컬 유니캐스트 주소와 글로벌 유니캐스트 주소를 모두 사용하여 자체적으로 주소를 지정할 수 있도록 해주기 때문에 특히 유용한 솔루션입니다. 이 과정은 먼저 라우터로부터 접두사 정보를 학습한 다음 장치 고유의 인터페이스 주소를 인터페이스 ID로 추가하는 방식으로 이루어집니다. 그렇다면 이 인터페이스 ID는 어디에서 오는 걸까요? 이더넷 네트워크의 모든 장치는 물리적 MAC 주소를 가지고 있으며, 이 MAC 주소가 바로 인터페이스 ID로 사용됩니다. 하지만 IPv6 주소에서 인터페이스 ID는 64비트이고 MAC 주소는 48비트이므로, 나머지 16비트는 어디에서 오는 걸까요? MAC 주소의 중간에 FF:FE로 16비트가 채워져 있습니다.

예를 들어, MAC 주소가 0060:d673:1987인 장치가 있다고 가정해 보겠습니다. 패딩을 추가하면 0260:d6FF:FE73:1987과 같이 표시됩니다. 그림 7.3은 EUI-64 주소의 형식을 보여줍니다.

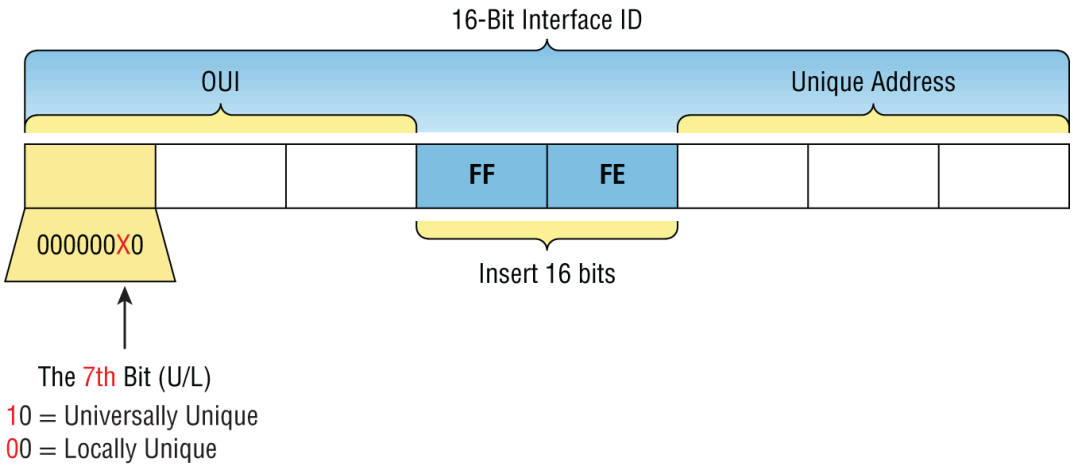

그림 7.3 EUI-64 인터페이스 ID 할당

그렇다면 주소 앞부분의 숫자 2는 어디서 온 걸까요? 좋은 질문입니다. 패딩 과정의 일부인 수정된 EUI-64 형식에서는 주소가 로컬에서 고유한지 아니면 전역적으로 고유한지를 지정하기 위해 Universal/Local(U/L) 비트를 변경합니다. 변경되는 비트는 주소의 7번째 비트입니다.

U/L 비트를 수정하는 이유는 인터페이스에 수동으로 주소를 할당할 때, 훨씬 긴 2001:db8:1:9:0200::1/64 대신 2001:db8:1:9::1/64와 같이 간단하게 주소를 지정할 수 있기 때문입니다. 또한, 링크 로컬 주소를 수동으로 할당할 경우, 긴 fe80::0200:0:0:1 또는 fe80:0:0:0:0200::1 대신 짧은 fe80::1을 지정할 수 있습니다. 따라서 언뜻 보기에 IETF가 7번째 비트를 변경함으로써 IPv6 주소 지정 방식을 이해하기 어렵게 만든 것처럼 보일 수 있지만, 실제로는 주소 지정을 훨씬 간단하게 만들었습니다. 또한, 대부분의 사용자는 기본적으로 설정된 주소를 변경하지 않으므로 U/L 비트는 기본적으로 0입니다. 따라서 대부분의 경우 이 값이 반전되어 1로

표시됩니다. 하지만 시험 목표를 공부하는 것이기 때문에, 이를 역으로 생각해 봐야 합니다.

다음은 몇 가지 예입니다.

- MAC 주소 0 **0** 90:2716:fd0f
- IPv6 EUI-64 주소: 2001:0db8:0:1:0 **2** 90:27ff:fe16:fd0f

너무 쉬웠어! 시험 목표에 비해 너무 쉬웠으니, 다른 문제를 풀어보자.

- MAC 주소 a **a** 12:bcbc:1234
- IPv6 EUI-64 주소: 2001:0db8:0:1:a **8** 12:bcff:febc:1234

101010 **1** 0은 MAC 주소(aa)의 처음 8비트를 나타냅니다. 여기서 7번째 비트를 반전시키면 101010 **0** 0이 됩니다. 따라서 답은 a8입니다. 이 내용을 이해하는 것이 얼마나 중요한지 아무리 강조해도 지나치지 않으니, 조금만 더 차근차근 따라와 주세요!

- MAC 주소 0 **c** 0c:dede:1234
- IPv6 EUI-64 주소: 2001:0db8:0:1:0 **e** 0c:deff:fede:1234

0c는 MAC 주소의 처음 8비트가 00001100이고, 7번째 비트를 뒤집으면 00001110이 됩니다. 따라서 답은 0e입니다. 하나 더 연습해 보겠습니다.

- MAC 주소 0 **b** 34:ba12:1234
- IPv6 EUI-64 주소: 2001:0db8:0:1:0 **9** 34:baff:fe12:1234

0b를 이진수로 나타내면 000010 **1** 1이 되는데, 이는 MAC 주소의 처음 8비트이며, 이를 다시 000010 **0** 1로 변환합니다. 따라서 정답은 09입니다.

EUI-64 주소 지정 방식에 특히 주의하고, EUI-64 규칙에 따라 7번째 비트를 변환할 수 있어야 합니다!

DHCPv6 (상태 유지형)

DHCPv6는 IPv4의 DHCP와 거의 동일한 방식으로 작동하며, IPv6의 새로운 주소 지정 체계를 지원한다는 점이 가장 큰 차이점입니다. 놀랍게도 DHCP는 자동 구성

에서는 제공하지 않는 몇 가지 옵션을 여전히 제공합니다. 농담이 아닙니다. 자동 구성에서는 DNS 서버, 도메인 이름, 그리고 IPv4에서 DHCP가 항상 제공해 왔던 여러 옵션들을 전혀 언급하지 않습니다. 이것이 바로 향후 IPv6에서도 DHCP가 적어도 부분적으로, 어쩌면 대부분의 경우 계속 사용될 가능성이 높은 중요한 이유 중 하나입니다.

즉, 필요한 추가 정보를 제공하고 배포하려면 (필요한 경우 주소 할당 관리까지 포함하여) 별도의 서버가 반드시 필요하다는 뜻입니다!

IPv6로 마이그레이션

IPv6의 작동 방식과 네트워크에서 IPv6를 사용하도록 설정하는 방법에 대해서는 많은 이야기를 나누었지만, 실제로 이를 구현하는 데 드는 비용은 얼마나 될까요? 그리고 얼마나 많은 작업이 필요할까요? 물론 좋은 질문이지만, 그 답은 모든 사람에게 똑같지는 않습니다. 최종적으로 지출해야 할 비용은 기존 인프라에 따라 크게 달라지기 때문입니다. 만약 아주 오래된 라우터와 스위치를 "최대한 오래" 사용하고 있어서 IPv6를 준수하도록 모든 장비를 업그레이드해야 한다면, 상당한 비용이 발생할 수 있습니다! 게다가 이 비용에는 서버 및 컴퓨터 운영 체제(OS)와 모든 애플리케이션을 IPv6에 맞추기 위해 쏟는 노력과 시간까지 포함되지 않습니다. 그러니, 생각보다 훨씬 많은 비용이 들 수 있다는 점을 명심하세요! 다행인 점은, 여러분이 정말로 방치하지 않았다면, 많은 운영체제와 네트워크 장치들이 이미 몇 년 전부터 IPv6를 지원하고 있다는 것입니다. 다만 지금까지 우리가 그 모든 기능을 활용하지 못했을 뿐입니다.

다음으로 작업량과 시간에 대한 질문이 있습니다. 솔직히 말해서, 이 작업은 여전히 상당히 까다로울 수 있습니다. 어떤 경우든 모든 시스템을 이전하고 모든 것이 제대로 작동하는지 확인하는 데는 시간이 걸립니다. 특히 수많은 장치가 있는 대규모 네트워크라면 훨씬 더 오랜 시간이 걸릴 수 있습니다! 하지만 걱정하지 마세요. 점진적인 통합을 위해 마이그레이션 전략이 마련되어 있습니다. 사용 가능한 주요 전환 전략 세 가지를 보여드리겠습니다. 첫 번째는 듀얼 스태킹이라고 하는데, 장치가 IPv4와 IPv6 프로토콜 스택을 모두 실행할 수 있도록 하여 기존 통신을 유지하면서 동시에 새로운 IPv6 통신이 구현될 때 사용할 수 있도록 합니다. 다음은 6to4 터널링 방식입니다. 모든 장치가 IPv6로 구성된 네트워크에서 다른 IPv6 네트워크에 도달하기 위해 IPv4 네트워크를 거쳐야 하는 경우에 적합한 방식입니다. 세 번째 전략은 재미 삼아 알려드리겠습니다!

이중 스태킹

이는 가장 일반적인 마이그레이션 전략 유형입니다. 왜냐하면 가장 간편하기 때문입니다. 이 방식을 사용하면 장치들이 IPv4 또는 IPv6를 사용하여 통신할 수 있습

니다. 듀얼 스태킹을 통해 네트워크상의 장치와 애플리케이션을 한 번에 하나씩 업그레이드할 수 있습니다. 네트워크상의 호스트와 장치가 업그레이드될수록 IPv6를 통한 통신이 점점 더 많이 이루어집니다. 마이그레이션이 완료되면 모든 것이 IPv6에서 실행되고 더 이상 필요하지 않은 기존 IPv4 프로토콜 스택을 모두 제거할 수 있습니다.

6to4 터널링

IPv6에서 IPv4로의 터널링은 IPv4 네트워크를 통해 IPv6 패킷을 전송하는 데 매우 유용합니다. IPv6 서브넷이나 네트워크의 다른 부분이 모두 IPv6로 구성되어 있고, 이러한 네트워크들이 서로 통신해야 하는 경우가 종종 있습니다. 그리 복잡해 보이지는 않지만, WAN이나 제어할 수 없는 다른 네트워크에서 이러한 상황이 발생할 수 있다는 점을 고려하면 문제가 될 수 있습니다. 그렇다면 전체 네트워크를 제어할 수 없는 경우 어떻게 해야 할까요? IPv4 네트워크를 통해 IPv6 트래픽을 전송하는 터널을 생성하는 것입니다.

터널링이라는 개념 자체는 그리 어렵지 않고, 터널을 만드는 것 또한 생각보다 어렵지 않습니다. 핵심은 네트워크를 통해 전송되는 IPv6 패킷을 가로채서 그 앞에 IPv4 헤더를 붙이는 것뿐입니다. 마치 잡았다가 놓아주는 낚시와 비슷하지만, 물고기에게 뭔가를 묻히지 않고 다시 물속으로 돌려보내는 방식이라는 점이 다릅니다.

이를 이해하려면 그림 7.4 를 참조하십시오 .

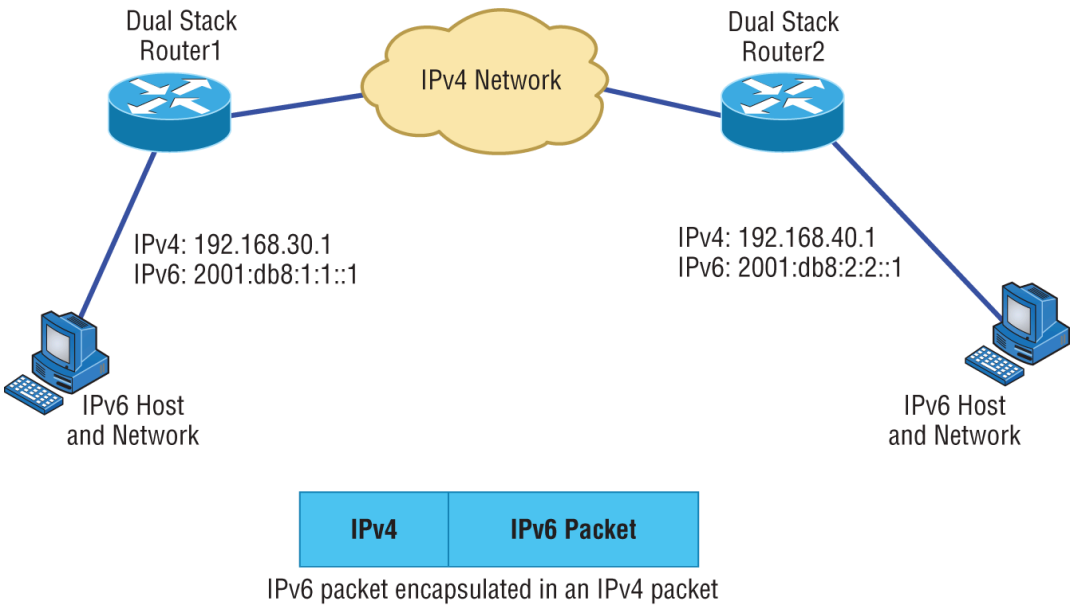

그림 7.4 6대4 터널

좋습니다. 하지만 이를 구현하려면 제가 방금 보여드린 것처럼 듀얼 스택 라우터 두 대가 필요합니다. 이제 라우터 간에 터널을 설정하기 위해 약간의 구성이 필요합니다. 터널은 매우 간단합니다. 각 라우터에 터널의 시작점과 끝점을 알려주기만 하면

됩니다. 이와 반대되는 경우는 *4to6 터널* 인데 , 이는 흔하지 않습니다. 왜냐하면 전체 비즈니스 네트워크가 IPv4 기반인데(여기까지는 일반적인 이야기처럼 들리죠?), IPv6 전용 인터넷을 통해 다른 IPv4 네트워크에 접속해야 하기 때문입니다. 현재로서는 이러한 구성은 흔하지 않습니다.

여기서 중요한 점은, 6to4 상황에서 통과하는 IPv4 네트워크에 NAT 변환 지점이 있다면, 방금 생성한 터널 캡슐화가 완전히 깨진다는 것입니다! NAT/PAT는 수년에 걸쳐 특정 프로토콜과 동적 연결을 처리할 수 있도록 많은 업그레이드가 이루어졌지만, 이러한 업그레이드가 적용되지 않은 경우 대부분의 연결이 끊어지게 됩니다. 대부분의 NAT 구현에는 이러한 전환 전략이 없기 때문에 문제가 발생합니다.

하지만 이 작은 문제를 해결할 방법이 있습니다(앞서 말씀드린 세 번째 전략). 바로 *Teredo*를 사용하는 것인데 , 이를 통해 모든 터널 트래픽을 UDP 패킷으로 전송할 수 있습니다. NAT는 UDP 패킷을 차단하지 않기 때문에 다른 프로토콜 패킷처럼 손상되지 않습니다. 따라서 Teredo를 사용하고 패킷을 UDP로 위장하면 NAT를 쉽게 통과하여 안전하게 전송될 수 있습니다!

Miredo 는 네이티브 IPv6 Linux 및 BSD Unix 시스템에서 듀얼 스택 라우터나 6to4 터널 없이 IPv4 인터넷을 통해 직접 통신하기 위해 사용되는 터널링 기술입니다. 하지만 실제로 사용되는 경우는 드뭅니다.

요약

이 장에서는 IPv4와 IPv6의 가장 기본적인 개념과 이들이 인터넷 네트워크에서 어떻게 작동하는지 살펴보았습니다(*IP* 라는 약어가 단독으로 사용될 때는 IPv4만을 의미한다는 점을 기억하세요). 이 장을 읽으면서 알 수 있듯이, 기본적인 내용을 다루고 설정하는 것조차 이해해야 할 것이 많으며, 우리는 이제 겨우 빙산의 일각만을 살펴본 것입니다. 또한 RFC 1918, APIPA 주소, 주소 클래스 AD, NAT, EUI-64, 터널링, 듀얼 스택 및 가상 IP 주소 지정에 대해서도 다루었습니다. 하지만 장담컨대, 이제 여러분은 Network+ 시험 목표를 달성하는 데 필요한 것보다 훨씬 더 많은 것을 알게 되었습니다.

각 주소 클래스 간의 차이점과 네트워크 주소, 브로드캐스트 주소 및 유효 호스트 범위를 찾는 방법에 대해 자세히 설명했습니다.

IPv6가 필요한 이유와 그 장점에 대해 설명드렸습니다. 이어서 IPv6 주소 지정 방법과 단축 표현식 사용법을 다뤘습니다. IPv6 주소 지정에 대한 설명에서는 다양한 주소 유형과 IPv6에서 예약된 특수 주소에 대해서도 보여드렸습니다.

다음 장은 매우 중요하지만, 다소 어렵게 느껴지는 부분도 있으니 잠시 쉬었다가 IP 서브넷팅에 대한 재미있지만 긴 장을 준비하세요. 너무 힘들게 하지는 않을게요!

시험 필수 사항

클래스 A 네트워크의 IP 주소 범위는 1부터 126까지입니다. 기본적으로 이 범위는 8비트의 네트워크 주소와 24비트의 호스트 주소를 제공합니다.

클래스 B IP 주소 범위를 기억하세요. 클래스 B 네트워크의 IP 주소 범위는 128부터 191까지입니다. 클래스 B 주소 지정 방식은 기본적으로 16비트의 네트워크 주소와 16비트의 호스트 주소를 제공합니다.

클래스 C 범위에 대해 기억하세요. 클래스 C 네트워크의 IP 범위는 192부터 223까지입니다. 클래스 C 주소 지정은 기본적으로 24비트의 네트워크 주소와 8비트의 호스트 주소를 제공합니다.

사설 IP 주소 범위를 기억하세요. 클래스 A 사설 주소 범위는 10.0.0.0부터 10.255.255.255까지입니다.

> *클래스 B 사설 주소 범위는 172.16.0.0부터 172.31.255.255까지입니다.*
>
> *클래스 C 사설 주소 범위는 192.168.0.0부터 192.168.255.255까지입니다.*

APIPA의 IP 주소 범위를 기억하세요 . APIPA의 IP 주소 범위는 169.254.0.1부터 169.254.255.254까지입니다. 클라이언트는 또한 기본 클래스 B 서브넷 마스크인 255.255.0.0으로 자체 구성됩니다.

IPv6가 왜 필요한지 이해하십시오 . IPv6가 없다면 전 세계는 곧 IP 주소 부족 사태에 직면하게 될 것입니다.

링크 로컬 주소를 이해하세요 . 링크 로컬 주소는 IPv4 APIPA IP 주소와 유사하지만, 조직 내에서조차 라우팅이 불가능합니다.

고유 로컬(Unique Local)에 대해 알아보세요 . 링크 로컬(Link Local)과 유사하게, 고유 로컬은 IPv4의 사설 IP 주소와 같으며 인터넷으로 라우팅될 수 없습니다. 하지만 링크 로컬과 고유 로컬의 차이점은 고유 로컬은 조직 또는 회사 내부에서 라우팅될 수 있다는 점입니다.

IPv6 주소 체계를 기억하세요 . IPv6 주소 체계는 IPv4 주소 체계와는 다릅니다. IPv6 주소 체계는 훨씬 더 넓은 주소 공간을 가지고 있으며, 주소는 128비트 길이로

16진수로 표현됩니다. 반면 IPv4 주소는 32비트 길이로 10진수로 표현됩니다.

7번째 비트가 반전된 EUI-64 주소를 이해하고 읽을 수 있어야 합니다 . 호스트는 자동 구성을 통해 IPv6 주소를 얻을 수 있으며, 그 방법 중 하나가 EUI-64라는 방식입니다. 이 방식은 호스트의 고유 MAC 주소 중간에 FF:FE를 삽입하여 48비트 MAC 주소를 64비트 인터페이스 ID로 변환합니다. 인터페이스 ID에 16비트가 삽입되는 것 외에도 첫 번째 바이트의 7번째 비트가 반전되는데, 일반적으로 0에서 1로 변경됩니다.

필기 실험

필기 실험 문제의 답은 부록 A 에서 확인할 수 있습니다 .

필기 실험 7.1

다음 질문에 답하십시오.

1. 클래스 C 사설 IP 주소에 사용되는 유효 범위는 무엇입니까?
2. IPv4에 비해 IPv6의 장점을 몇 가지 나열해 보세요.
3. 169.254로 시작하는 주소에 대한 자동 구성 기술을 무엇이라고 합니까?
4. 유니캐스트 주소란 무엇을 의미하나요?
5. 멀티캐스트 주소란 무엇을 의미하나요?
6. NIC와 같은 네트워크 인터페이스에 물리적으로 할당된 48비트(6바이트) 숫자 주소를 무엇이라고 합니까?
7. IPv6는 IPv4 주소에 비해 비트 수가 몇 개 더 많습니까?
8. 클래스 B 네트워크의 사설 IP 주소 범위는 무엇입니까?
9. 클래스 C에서 첫 번째 옥텟의 십진수 및 이진수 값 범위는 무엇입니까?
10. 127.0.0.1 주소는 무엇에 사용되나요?

필기 실험 7.2

이 실습에서 다음 IPv6 관련 질문에 대한 답을 작성하세요.

1. 어떤 유형의 패킷이 특정 인터페이스로만 전달됩니까?
2. IPv4에서 일반 공용 라우팅 가능 주소처럼 사용되는 주소 유형은 무엇입니까?
3. 라우팅 대상이 아닌 주소 유형은 무엇입니까?
4. 인터넷으로 라우팅되지 않지만 전 세계적으로 고유한 주소 유형은 무엇입니까?
5. 여러 인터페이스로 전달되도록 설계된 주소 유형은 무엇입니까?
6. 여러 인터페이스를 식별하지만 패킷은 처음 발견된 주소로만 전달되는 주소 유형은 무엇입니까?

7. 일대일(최근접) 주소 지정 방식이라고도 하는 것은 무엇입니까?
8. IPv4의 루프백 주소는 127.0.0.1이었습니다. IPv6의 루프백 주소는 무엇입니까?
9. 링크 로컬 주소는 항상 무엇으로 시작하나요?
10. 고유한 로컬 유니캐스트 범위는 무엇으로 시작합니까?

복습 문제

복습 문제에 대한 답은 부록 B 에서 찾을 수 있습니다 .

1. 다음 주소 중 인터넷에서 허용되지 않는 주소는 무엇입니까?
   A. 191.192.168.1
   B. 191.168.169.254
   C. 172.32.255.0
   D. 172.31.12.251
2. 호스트가 다음 범위 중 어느 범위에서 자동으로 주소가 구성되었는지 표시된다면 DHCP 서버에 연결할 수 없음을 나타냅니다.
   A. 169.254.0. *x* 마스크 255.255.255.0
   B. 169.254. *xx* 마스크 255.255.0.0 포함
   C. 169.254. *xx* 마스크 255.255.255.0
   D. 169.255.xx *마스크* 255.255.0.0 포함
3. 사설 IP 주소에 관한 다음 설명 중 가장 정확한 것은 무엇입니까?
   A. 라우팅이 필요한 인트라넷에서는 사설 IP 주소를 사용할 수 없습니다.
   B. 사설 IP 주소는 등록기관 또는 ISP에서 할당해야 합니다.
   C. 인터넷상의 원격 호스트가 사설 IP 주소를 사용하는 경우, 해당 호스트에 ping을 보낼 수 없습니다.
   D. 사설 IP 주소는 하나의 관리 도메인에서만 사용할 수 있습니다.
4. 다음 중 유효한 A급 주소는 무엇입니까?
   A. 191.10.0.1
   B. 127.10.0.1
   C. 128.10.0.1
   D. 126.10.0.1
5. 다음 중 유효한 클래스 B 주소는 무엇입니까?
   A. 10.1.1.1
   B. 126.1.1.1
   C. 129.1.1.1
   D. 192.168.1.1
6. 다음 중 브로드캐스트 주소를 설명하는 것은 무엇입니까?
   A. 모든 네트워크 비트가 켜져 있습니다(1).

B. 호스트 비트가 모두 켜져 있습니다(1).

C. 모든 네트워크 비트가 꺼져 있습니다(0).

D. 호스트 비트가 모두 꺼져 있습니다(0).

7. 다음 중 레이어 2 브로드캐스트는 무엇입니까?

A. FF.FF.FF.EE.EE.EE

B. FF.FF.FF.FF.FF.FF

C. 255.255.255.255

D. 255.0.0.0

8. 클래스 C IP 주소에서 네트워크 주소의 길이는 얼마나 됩니까?

A. 8비트

B. 16비트

C. 24비트

D. 32비트

9. 유니캐스트 주소를 설명할 때 다음 중 맞는 것은 무엇입니까?

A. 유니캐스트 주소로 전송된 패킷은 단일 인터페이스로 전달됩니다.

B. 이것들은 일반적인 IPv4 공용 라우팅 가능 주소와 마찬가지로, 여러분이 흔히 사용하는 공용 라우팅 가능 주소입니다.

C. 이것들은 IPv4의 사설 주소와 유사하게 라우팅용으로 사용되지 않습니다.

D. 이 주소들은 라우팅 목적이 아닌 용도로 사용되지만, 거의 전 세계적으로 고유하기 때문에 주소가 중복될 가능성은 매우 낮습니다.

10. 호스트가 재부팅되었고 할당된 IP 주소를 확인했습니다. 주소는 169.123.13.34입니다. 다음 중 어떤 상황이 발생한 것입니까?

A. 호스트는 APIPA 주소를 받았습니다.

B. 호스트가 멀티캐스트 주소를 수신했습니다.

C. 진행자는 공개 연설을 받았습니다.

D. 호스트는 비공개 주소를 받았습니다.

11. IPv4 주소는 32비트를 사용합니다. 그렇다면 IPv6 주소는 몇 비트를 사용합니까?

A. 64

B. 128

C. 192

D. 255

12. 멀티캐스트 주소를 설명할 때 다음 중 맞는 것은 무엇입니까?

A. 멀티캐스트 주소에서 유니캐스트 주소로 전송되는 패킷은 단일 인터페이스로 전달됩니다.

B. 패킷은 해당 주소로 식별된 모든 인터페이스로 전달됩니다. 이를 일대다 주소라고도 합니다.

C. 이 메시지는 여러 인터페이스를 식별하며 단 하나의 주소로만 전달됩니다. 이 주소는 일대다 방식이라고도 할 수 있습니다.

D. 이 주소들은 라우팅 목적이 아닌 용도로 사용되지만, 거의 전 세계적으로 고유하기 때문에 주소가 겹칠 가능성은 매우 낮습니다.

13. 애니캐스트 주소를 설명할 때 다음 중 맞는 것은 무엇입니까?
    A. 애니캐스트 주소에서 유니캐스트 주소로 전송된 패킷은 단일 인터페이스로 전달됩니다.
    B. 패킷은 해당 주소로 식별된 모든 인터페이스로 전달됩니다. 이를 일대다 주소라고도 합니다.
    C. 이 주소는 여러 인터페이스를 식별하며, 애니캐스트 패킷은 가장 가까운 주소 하나로만 전달됩니다. 이러한 방식을 일대일(one-to-nearest) 방식이라고도 합니다.
    D. 이 주소들은 라우팅 목적이 아닌 용도로 사용되지만, 거의 전 세계적으로 고유하기 때문에 주소가 겹칠 가능성은 매우 낮습니다.
14. 로컬 호스트의 루프백 주소로 핑을 보내려고 합니다. 입력할 수 있는 주소 두 개는 무엇입니까? (두 개를 선택하세요.)
    A. `ping 127.0.0.1`
    B. `ping 0.0.0.0`
    C. `ping ::1`
    D. `trace 0.0.::1`
15. IPv6 주소에 대한 다음 설명 중 맞는 두 가지는 무엇입니까? (두 가지를 선택하십시오.)
    A. 앞에 0을 붙여야 합니다.
    B. 두 개의 콜론(::)은 연속된 0으로 이루어진 16진수 필드를 나타내는 데 사용됩니다.
    C. 두 개의 콜론(::)은 필드를 구분하는 데 사용됩니다.
    D. 하나의 인터페이스에 여러 유형의 IPv6 주소가 할당될 수 있습니다.
16. IPv4 및 IPv6 주소에 대한 다음 설명 중 맞는 두 가지는 무엇입니까? (두 가지를 선택하십시오.)
    A. IPv6 주소는 32비트 길이이며 16진수로 표현됩니다.
    B. IPv6 주소는 128비트 길이이며 십진수로 표현됩니다.
    C. IPv4 주소는 32비트 길이이며 십진수로 표현됩니다.
    D. IPv6 주소는 128비트 길이이며 16진수로 표현됩니다.
17. 다음 중 클래스 C 네트워크 주소는 무엇입니까?
    A. 10.10.10.0
    B. 127.0.0.1
    C. 128.0.0.0
    D. 192.255.254.0
18. 다음 중 사설 IP 주소는 무엇입니까? (두 개를 선택하십시오.)
    A. 12.0.0.1
    B. 168.172.19.39

C. 172.20.14.36

D. 172.33.194.30

E. 192.168.24.43

19. 회사 라우터에서 IPv6 유니캐스트 라우팅이 실행 중입니다. 다음 주소 중 EUI-64 주소로 사용되는 주소는 무엇입니까?

```
Corp#sh int f0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000d.bd3b.0d80 (bia 000d.bd3b.0d80)
[output cut]
```

A. FF02::3c3d:0d:bdff:fe3b:0d80

B. FE80::3c3d:2d:bdff:fe3b:0d80

C. FE80::3c3d:0d:bdff:fe3b:0d80

D. FE80::3c3d:2d:ffbd:3bfe:0d80

20. 다음 중 호스트에 대해 유효하지 않은 IP 주소는 무엇입니까?

A. 10.0.0.1

B. 128.0.0.1

C. 224.0.0.1

D. 172.0.0.1