서브넷 0 및 모든 서브넷 구성

목차

소개

이 문서에서는 서브넷 0 및 모든 서브넷 서브넷의 사용에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 기술 팁 및 기타 내용에 형식 규칙 사용을 참조하십시오.

배경 정보

서브넷은 지정된 네트워크 주소를 더 작은 서브넷으로 나눕니다. NAT(Network Address Translation) 및 PAT(Port Address Translation)와 같은 다른 기술과 결합하여 사용 가능한 IP 주소 공간을 더 효율적으로 사용하고 주소 고갈 문제를 크게 줄여줍니다. 서브넷에는 각각 서브넷 0과 올

원 서브넷이라고 하는 첫 번째와 마지막 서브넷의 사용을 다루는 지침이 있습니다.

서브넷 0

네트워크 주소를 서브넷에 추가하면 네트워크 주소를 서브넷에 넣은 후 얻은 첫 번째 서브넷을 서브넷 0이라고 합니다.

클래스 B 주소 172.16.0.0을 고려하십시오. 기본적으로 클래스 B 주소 172.16.0.0에는 호스트 부분을 나타내기 위해 예약된 16비트가 있으므로 65534(2^{16}-2)개의 유효한 호스트 주소를 허용합니다. 네트워크 172.16.0.0/16이 호스트 부분에서 3비트를 차용하므로 서브넷을 추가하면 8개(23)의 서브넷을 얻을 수 있습니다. 이 표는 주소 172.16.0.0을 서브넷에 넣어서 얻은 서브넷, 결과 서브넷 마스크, 연결된 브로드캐스트 주소, 유효한 호스트 주소 범위를 보여 주는 예입니다.

서브넷 주소	서브넷 마스크	브로드캐스트 주소	유효한 호스트 범위
172.16.0.0	255.255.224.0	172.16.31.255	172.16.0.1~172.16.31.254
172.16.32.0	255.255.224.0	172.16.63.255	172.16.32.1~172.16.63.254
172.16.64.0	255.255.224.0	172.16.95.255	172.16.64.1~172.16.95.254
172.16.96.0	255.255.224.0	172.16.127.255	172.16.96.1~172.16.127.254
172.16.128.0	255.255.224.0	172.16.159.255	172.16.128.1~172.16.159.254
172.16.160.0	255.255.224.0	172.16.191.255	172.16.160.1~172.16.191.254
172.16.192.0	255.255.224.0	172.16.223.255	172.16.192.1~172.16.223.254
172.16.224.0	255.255.224.0	172.16.255.255	172.16.224.1~172.16.255.254

앞의 예에서 첫 번째 서브넷(서브넷 172.16.0.0/19)을 서브넷 0이라고 합니다.

서브넷에 있는 네트워크의 클래스와 서브넷을 넣은 후 얻은 서브넷 수는 서브넷 0을 결정하지 않습니다. 네트워크 주소를 서브넷에 추가할 때 처음 얻는 서브넷입니다. 또한 서브넷 0 주소의 이진 등가물을 쓸 때 모든 서브넷 비트(이 경우 비트 17, 18, 19)는 0입니다. 서브넷 0은 모두 0 서브넷이라고도 합니다.

모두 서브넷

네트워크 주소를 서브넷에 추가하면 마지막으로 가져온 서브넷을 모두 서브넷이라고 합니다.

앞의 예를 참조하면, 네트워크 172.16.0.0(서브넷 172.16.224.0/19)을 서브넷에 추가할 때 얻은 마지막 서브넷을 모든 서브넷(all-ones subnet)이라고 합니다.

서브넷에 있는 네트워크의 클래스와 서브넷을 넣은 후 얻은 서브넷 수가 모든 서브넷을 결정하지는 않습니다. 또한, 서브넷 0 주소의 이진수 값을 쓸 때 모든 서브넷 비트(이 경우 비트 17, 18, 19)는 1이므로 이름이 지정됩니다.

서브넷 0 및 모든 서브넷 문제

기존에는 IP 주소에 대해 서브넷 0 및 올-원 서브넷을 사용하지 않는 것이 좋습니다. RFC 950에 따르면, "서브넷된 네트워크에서 이러한 특수(네트워크 및 브로드캐스트) 주소의 해석을 보존하고 확

장하는 것이 유용합니다. 즉, 모든 0의 값과 서브넷 필드의 모든 값을 실제(물리적) 서브넷에 할당해서는 안 됩니다." 네트워크 엔지니어가 3비트를 빌릴 때 얻는 서브넷 수를 계산해야 하는 이유는 23-2(6)가 아니라 23-2(8)를 계산하는 것입니다. -2는 일반적으로 서브넷 0과 모든 서브넷 서브넷이 사용되지 않음을 알고 있습니다.

서브넷 제로 문제

IP 주소 지정에 서브넷 0을 사용하는 것은 네트워크의 혼동과 구별할 수 없는 주소의 서브넷 때문에 권장되지 않았습니다.

이전 예를 참조하여 IP 주소 172.16.1.10을 고려하십시오. 이 IP 주소와 연결된 서브넷 주소를 계산하면 서브넷 172.16.0.0(서브넷 0)이 검색됩니다. 이 서브넷 주소는 애초에 서브넷이 있던 네트워크 주소 172.16.0.0과 동일하므로 서브넷을 수행할 때마다 네트워크 및 식별 불가능한 주소를 가진 서브넷(서브넷 0)을 가져옵니다. 이것은 이전에 큰 혼란의 원인이었다.

Cisco IOS® Software Release 12.0 이전에는 기본적으로 Cisco 라우터가 서브넷 0에 속하는 IP 주소를 인터페이스에서 구성하는 것을 허용하지 않았습니다. 그러나 12.0 이전의 Cisco IOS 소프트웨어 릴리스와 함께 작동하는 네트워크 엔지니어가 서브넷 0을 사용하는 것이 안전하다고 판단될 경우 글로벌 컨피그레이션 모드에서 **ip subnet-zero 명령**을 사용하여 이 제한을 극복할 수 있습니다. Cisco IOS Software Release 12.0부터 Cisco 라우터의 **ip 서브넷 제로**가 기본적으로 활성화되어 있지만 네트워크 엔지니어가 서브넷 제로를 사용하는 것이 안전하지 않다고 생각할 경우 **no ip subnet-zero 명령**을 사용하여 서브넷 제로 주소 사용을 제한할 수 있습니다.

Cisco IOS Software Release 8.3 이전 버전에서는 **service subnet-zerocommand**가 사용되었습니다.

모두 서브넷 문제

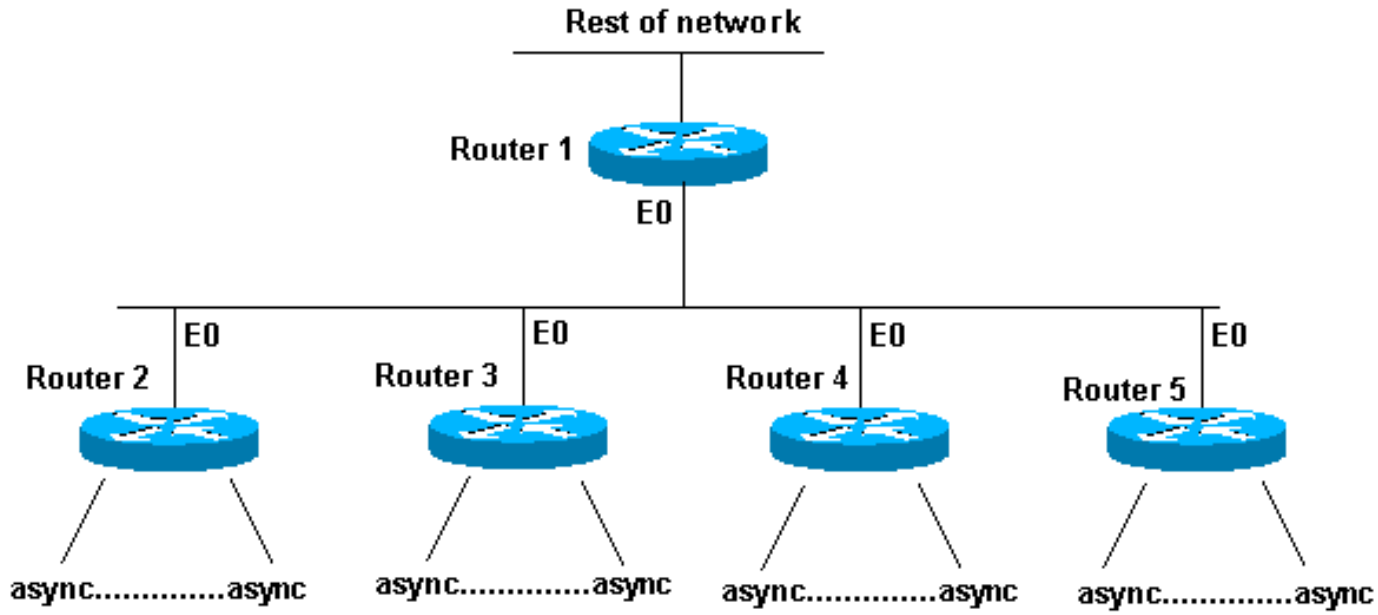
IP 주소 지정에 올원 서브넷을 사용하는 것은 과거에는 네트워크 및 동일한 브로드캐스트 주소를 갖는 서브넷에 내재된 혼란 때문에 권장되지 않았습니다.

앞의 예를 참조하면, 마지막 서브넷(서브넷 172.16.224.0/19)의 브로드캐스트 주소는 172.16.255.255이며, 이는 애초에 서브넷된 네트워크 172.16.0.0의 브로드캐스트 주소와 동일하므로, 서브넷을 수행할 때마다 동일한 브로드캐스트 주소를 가진 네트워크 및 서브넷(모든 서브넷)을 얻게 됩니다. 즉, 네트워크 엔지니어는 라우터에서 주소 172.16.230.1/19을 구성할 수 있지만, 그렇게 하면 로컬 서브넷 브로드캐스트(172.16.255.255(/19))와 전체 클래스 B 브로드캐스트(172.16.255.255(/16))를 더 이상 구별할 수 없습니다.

이제 올원 서브넷을 사용할 수 있지만 컨피그레이션이 잘못되면 문제가 발생할 수 있습니다.

> **참고**: 자세한 내용은 호스트 및 서브넷 수량을 참조하십시오.

어떤 일이 일어날 수 있는지 알려드리려면 다음을 고려하십시오.



잘못 구성된 All-in-One 서브넷

라우터 2~5는 각각 여러 개의 수신 비동기(또는 ISDN) 연결이 있는 액세스 라우터입니다. 네트워크(192.168.1.0/24)는 이러한 수신 사용자를 위해 4개로 분할됩니다. 각 부분은 액세스 라우터 중 하나에 제공됩니다. 또한 비동기 라인은 unnum **e0으로 구성됩니다**. 라우터 1에는 올바른 액세스 라우터를 가리키는 고정 경로가 있으며 각 액세스 라우터에는 라우터 1에 기본 경로 지점이 있습니다.

라우터 1 라우팅 테이블은 다음과 같습니다.

```
C  192.168.2.0/24   E0
      S  192.168.1.0/26   192.168.2.2
      S  192.168.1.64/26  192.168.2.3
      S  192.168.1.128/26 192.168.2.4
      S  192.168.1.192/26 192.168.2.5
```

액세스 라우터에는 이더넷에 대해 동일한 연결 경로, 비동기식 회선에 대해 동일한 기본 경로 및 여러 호스트 경로가 있습니다(PPP(Point-to-Point Protocol) 적용).

```
Router 2 routing table:

      C  192.168.2.0/24   E0
      S  10.0.0.0/0      192.168.2.1
      C  192.168.1.2/32   async1
      C  192.168.1.5/32   async2
      C  192.168.1.8/32   async3
      C  192.168.1.13/32   async4
      C  192.168.1.24/32   async6
      C  192.168.1.31/32   async8
      C  192.168.1.32/32   async12
      C  192.168.1.48/32   async15
      C  192.168.1.62/32   async18
```

```
Router 3 routing table:

      C  192.168.2.0/24   E0
      S  10.0.0.0/0      192.168.2.1
      C  192.168.1.65/32   async1
      C  192.168.1.68/32   async2
      C  192.168.1.74/32   async3
      C  192.168.1.87/32   async4
      C  192.168.1.88/32   async6
      C  192.168.1.95/32   async8
      C  192.168.1.104/32   async12
      C  192.168.1.112/32   async15
      C  192.168.1.126/32   async18
```

```
  Router 4 routing table:

      C  192.168.2.0/24   E0
      S  10.0.0.0/0      192.168.2.1
      C  192.168.1.129/32   async1
      C  192.168.1.132/32   async2
      C  192.168.1.136/32   async3
      C  192.168.1.141/32   async4
      C  192.168.1.152/32   async6
```

```
Router 5 routing table:

      C  192.168.2.0/24   E0
      S  10.0.0.0/0      192.168.2.1
      C  192.168.1.193/32   async1
      C  192.168.1.197/32   async2
      C  192.168.1.200/32   async3
      C  192.168.1.205/32   async4
      C  192.168.1.216/32   async6
```

```
C  192.168.1.159/32   async8              C  192.168.1.223/32   async8
C  192.168.1.160/32   async12             C  192.168.1.224/32   async12
C  192.168.1.176/32   async15             C  192.168.1.240/32   async15
C  192.168.1.190/32   async18             C  192.168.1.252/32   async18
```

비동기식 라인에서 호스트가 255.255.255.192 마스크가 아닌 255.255.255.0 마스크를 갖도록 잘못 구성되면 어떻게 합니까? 모든 게 잘 풀리나요?

이러한 호스트(192.168.1.24) 중 하나가 로컬 브로드캐스트(NetBIOS, WINS)를 수행할 때 발생하는 상황을 살펴보십시오. 패킷은 다음과 같습니다.

```
s: 192.168.1.24 d: 192.168.1.255
```

패킷이 라우터 2에서 수신됩니다. 라우터 2는 TTL(Time To Live)이 만료될 때까지 라우터 1로 보내고 라우터 5로 보내고 라우터 1로 보냅니다.

다음은 또 다른 예입니다(호스트 192.168.1.240).

```
s: 192.168.1.240  d: 192.168.1.255
```

이 패킷은 라우터 5에서 수신됩니다. 라우터 5는 TTL이 만료될 때까지 라우터 1로 보내고 라우터 5로 보내고 라우터 1로 보내고 라우터 5로 보내는 등의 작업을 수행합니다. 이 상황이 발생하면 패킷 공격을 받았다고 생각할 수 있습니다. 라우터 5의 부하를 감안할 때, 이는 불합리한 가정은 아닐 것이다.

이 예에서는 라우팅 루프가 생성되었습니다. 라우터 5가 올원 서브넷을 처리하므로 해당 서브넷이 블라스팅됩니다. 라우터 2~4는 "브로드캐스트" 패킷을 한 번만 확인합니다. 라우터 1도 공격을 받았지만 Cisco 7513인 경우 이 상황을 처리할 수 있습니까? 이 경우 올바른 서브넷 마스크로 호스트를 구성해야 합니다.

올바르게 구성되지 않은 호스트를 보호하려면 루프백 주소에 대한 고정 경로 192.168.1.255를 사용하여 각 액세스 라우터에 루프백 인터페이스를 생성합니다. Null0 인터페이스를 사용할 수 있지만 이렇게 하면 라우터가 ICMP(Internet Control Message Protocol) "연결 불가" 메시지를 생성합니다.

서브넷 0 및 모든 서브넷 사용

권장하지 않는 경우에도 서브넷 0 및 모든 서브넷 서브넷을 포함하는 전체 주소 공간을 항상 사용할 수 있다는 점에 유의해야 합니다. Cisco IOS Software 릴리스 12.0 이후로 모든 서브넷의 사용이 명시적으로 허용되었고 서브넷 0의 사용이 명시적으로 허용되었습니다. Cisco IOS Software Release 12.0 이전에도 **ip subnet-zero** 글로벌 컨피그레이션 명령을 입력한 경우 **서브넷 0을** 사용할 수 있습니다

서브넷 0 및 올원 서브넷 사용의 문제에 대해서는 RFC 1878을 참조하십시오. 현재, 서브넷 0 및 올원 서브넷의 사용은 일반적으로 수락 되고, 대부분의 공급 업체는 사용을 지원 합니다. 그러나 특정 네트워크, 특히 레거시 소프트웨어를 사용하는 네트워크에서는 서브넷 0 및 올원 서브넷을 사용하면 문제가 발생할 수 있습니다.

> **참고**: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

관련 정보

- IP Routed Protocols 기술 지원 페이지
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.