ICMP 리디렉션 메시지 이해

목차

소개

이 문서에서는 ICMP(Internet Control Message Protocol) 패킷 리디렉션 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Nexus 7000 플랫폼 아키텍처
- Cisco NX-OS Software 컨피그레이션
- RFC 792에 문서화된 인터넷 제어 메시지 프로토콜

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Nexus 7000
- Cisco NX-OS 소프트웨어

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.

배경 정보

이 문서에서는 ICMP(Internet Control Message Protocol)에서 제공하는 패킷 리디렉션 기능에 대해 설명합니다. 이 문서에서는 네트워크에 일반적으로 나타나는 ICMP 리디렉션 메시지의 존재 여부와 ICMP 리디렉션 메시지 생성을 유발하는 네트워크 조건과 관련된 부정적인 부작용을 최소화하기 위해 수행할 수 있는 작업에 대해 설명합니다.

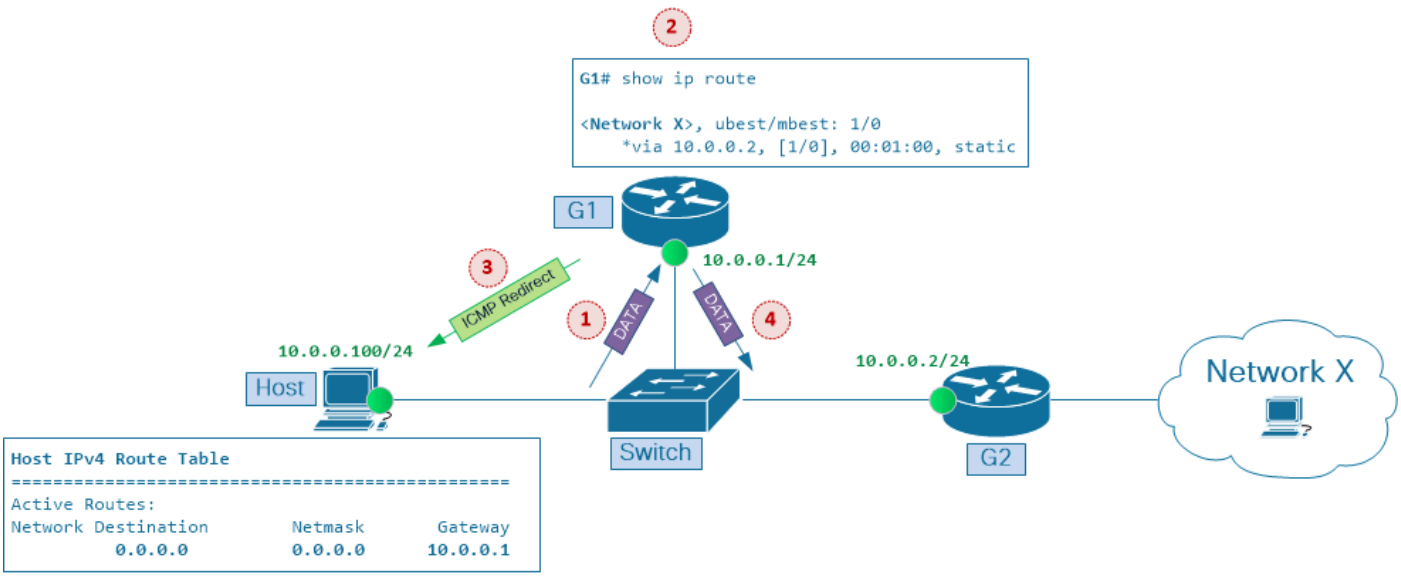
ICMP 리디렉션 메시지

ICMP 리디렉션 기능은 다음 예와 함께 RFC 792 Internet Control Message Protocol에 설명되어 있습니다.

> 이 경우 게이트웨이는 호스트에 리디렉션 메시지를 전송합니다.
>
> 게이트웨이 G1은 게이트웨이가 연결된 네트워크의 호스트에서 인터넷 데이터그램을 수신합니다. 게이트웨이 G1은 라우팅 테이블을 확인하고 데이터그램 인터넷 대상 네트워크 X에 대한 경로에서 다음 게이트웨이 G2의 주소를 가져옵니다
>
> G2와 데이터그램의 인터넷 소스 주소로 식별된 호스트가 동일한 네트워크에 있는 경우 리디렉션 메시지가 호스트로 전송됩니다. 리디렉션 메시지는 네트워크 X에 대한 트래픽을 게이트웨이 G2로 직접 전송하도록 호스트에 조언합니다. 이는 목적지로 가는 더 짧은 경로입니다.
>
> 게이트웨이는 원래 데이터그램 데이터를 인터넷 대상으로 전달합니다.

이 시나리오는 그림 1에 나와 있습니다. 호스트 및 두 라우터인 G1과 G2는 공유 이더넷 세그먼트에 연결되어 있으며 동일한 네트워크 10에 IP 주소가 있습니다.0.0.0/24

그림 1 다중 지점 이더넷 네트워크의 ICMP 리디렉션



다중 지점 이더넷 네트워크의 ICMP 리디렉션

호스트의 IP 주소는 10.0.0.100입니다. 호스트 라우팅 테이블에는 라우터 G1의 IP 주소 10.0.0.1을 기본 게이트웨이로 가리키는 기본 경로 항목이 있습니다. 라우터 G1은 목적지 네트워크 X에 트래픽을 전달할 때 라우터 G2의 IP 주소 10.0.0.2를 다음 홉으로 사용합니다.

이는 호스트가 목적지 네트워크 X에 패킷을 전송할 때 발생하는 일입니다.

1. IP 주소가 10.0.0.1인 게이트웨이 G1이 연결된 네트워크의 호스트 10.0.0.100에서 데이터 패킷을 수신합니다.

2. 게이트웨이 G1이 라우팅 테이블을 검사하고 데이터 패킷 대상 네트워크 X에 대한 경로에서 다음 게이트웨이 G2의 IP 주소 10.0.0.2를 가져옵니다.

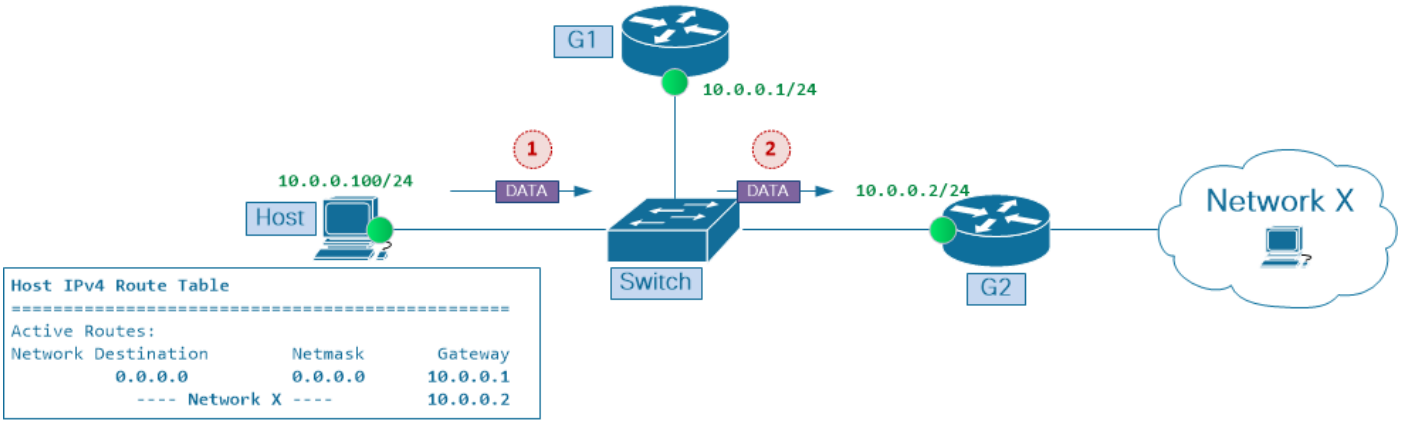
3. G2와 IP 패킷의 소스 주소로 식별된 호스트가 동일한 네트워크에 있는 경우 ICMP 리디렉션 메시지가 호스트로 전송됩니다. ICMP 리디렉션 메시지는 네트워크 X에 대한 트래픽을 게이트웨이 G2로 직접 전송하도록 호스트에 조언합니다. 이는 목적지로 가는 더 짧은 경로입니다.

4. 게이트웨이 G1은 원래 데이터 패킷을 목적지로 전달합니다.

호스트 컨피그레이션에 따라 G1이 전송하는 ICMP 리디렉션 메시지를 무시하도록 선택할 수 있습니다. 그러나 호스트가 라우팅 캐시를 조정하기 위해 ICMP 리디렉션 메시지를 사용하고 후속 데이터 패킷을 G2에 직접 전송하기 시작하면 이 시나리오에서 이러한 이점이 실현됩니다

- 네트워크를 통한 데이터 포워딩 경로 최적화 트래픽이 더 빨리 목적지에 도달함
- 대역폭 및 라우터 CPU 로드와 같은 네트워크 리소스 사용률 감소

그림 2 호스트 라우팅 캐시에 설치된 Next Hop G2



호스트 라우팅 캐시에 설치된 다음 홉 G2

그림 2에서 보여주는 것처럼, 호스트가 G2를 다음 홉으로 사용하는 네트워크 X에 대한 경로 캐시 항목을 생성한 후 네트워크에서 다음과 같은 이점이 나타납니다.

- 스위치와 라우터 G1 간의 링크에서 대역폭 사용률이 양방향으로 감소합니다.
- 호스트에서 네트워크 X로의 트래픽 흐름이 더 이상 이 노드를 통과하지 않으므로 라우터 G1의 CPU 사용률이 감소합니다.
- 호스트와 네트워크 X 간의 엔드 투 엔드 네트워크 지연이 개선됩니다.

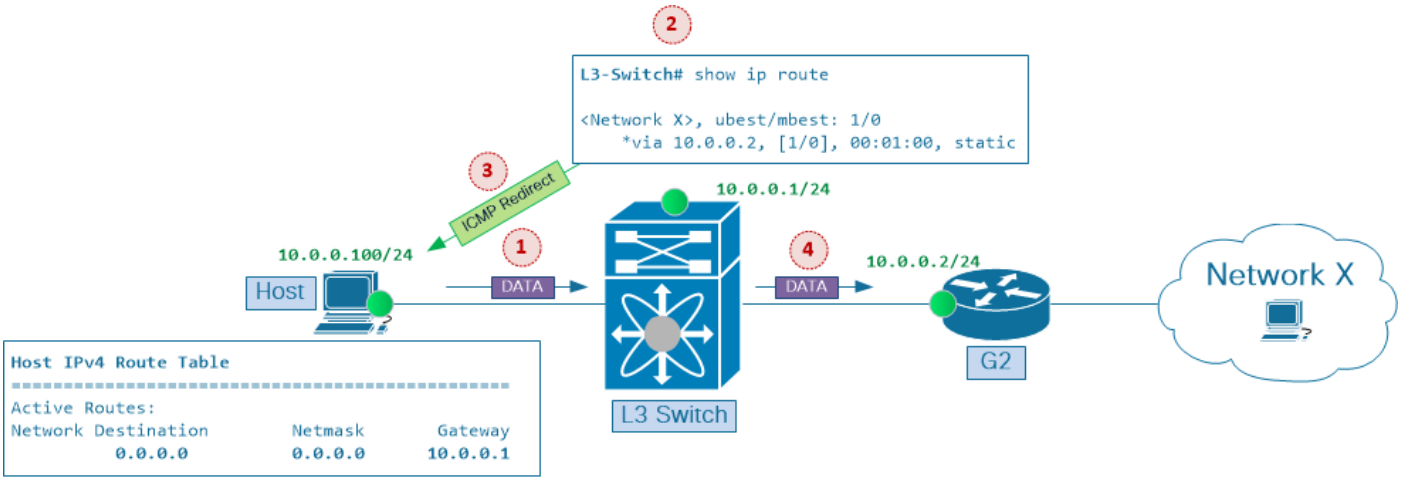
ICMP 리디렉션 메커니즘의 중요성을 이해하려면, 초기 인터넷 라우터 구현이 데이터 트래픽을 처리하는 데 주로 CPU 리소스에 의존했다는 점을 기억하십시오. 따라서 단일 라우터에서 처리해야 하는 트래픽 볼륨을 줄이고 특정 트래픽 흐름이 목적지로 가는 과정에서 거쳐야 하는 라우터 홉의 수를 최소화하는 것이 바람직했습니다. 이와 동시에 레이어 2 포워딩(스위칭이라고도 함)은 주로 맞춤형 ASIC(Application-Specific Integrated Circuits)에서 구현되었으며 포워딩 성능 관점에서는 레이어 3 포워딩(라우팅이라고도 함)에 비해 상대적으로 '저렴한' 방식이었습니다.

최신 ASIC 세대는 레이어 2 및 레이어 3 패킷 포워딩을 모두 수행할 수 있습니다. 하드웨어에서 수

행되는 레이어 3 테이블 조회는 라우터의 패킷 처리와 관련된 성능 비용을 줄이는 데 도움이 됩니다. 또한 레이어 3 포워딩 기능을 레이어 2 스위치로 통합하여(레이어 3 스위치로 불림) 패킷 포워딩 작업을 더욱 효율적으로 할 때 **단일 무장 라우터**(스틱의 **라우터** 라고도 함) 설계 옵션**이** 필요하지 않으며 이러한 네트워크 컨피그레이션과 관련된 제한을 피할 수 있습니다.

그림 3은 그림 1의 시나리오를 기반으로 합니다. 이제 원래 스위치 및 라우터 G1이라는 두 개의 개별 노드에서 제공되던 레이어 2 및 레이어 3 기능이 Nexus 7000 Series 플랫폼과 같은 단일 레이어 3 스위치에 통합됩니다.

그림 3 "단일 무장 라우터" 구성을 대체하는 레이어 3 스위치



"단일 무장 라우터" 구성을 대체하는 레이어 3 스위치

이는 호스트가 목적지 네트워크 X로 패킷을 전송할 때 발생하는 일입니다.

1. IP 주소가 10.0.0.1인 게이트웨이 L3 스위치는 연결된 네트워크의 호스트 10.0.0.100에서 데이터 패킷을 수신합니다.

2. 게이트웨이 L3 스위치는 라우팅 테이블을 확인하고 데이터 패킷 대상 네트워크 X에 대한 경로에서 다음 게이트웨이 G2의 주소 10.0.0.2를 가져옵니다.

3. G2와 IP 패킷의 소스 주소로 식별된 호스트가 동일한 네트워크에 있는 경우 ICMP 리디렉션 메시지가 호스트로 전송됩니다. ICMP 리디렉션 메시지는 네트워크 X에 대한 트래픽을 게이트웨이 G2로 직접 전송하도록 호스트에 조언합니다. 이는 목적지로 가는 더 짧은 경로입니다.

4. 게이트웨이는 원래 데이터 패킷을 대상으로 전달합니다.

레이어 3 스위치가 이제 ASIC 레벨에서 레이어 2 및 레이어 3 패킷 포워딩을 모두 수행할 수 있게 되면서 ICMP 리디렉션 기능의 두 가지 이점, 즉 (a) 네트워크를 통한 지연 개선, (b) 네트워크 리소스 사용률 감소 등이 모두 달성되며, 더 이상 다중 지점 이더넷 세그먼트의 경로 최적화 기술에 신경 쓸 필요가 없습니다.

그러나 레이어 3 인터페이스에서 ICMP 리디렉션 기능이 활성화된 경우, 이 문서의 뒷부분에 나오는 Nexus 플랫폼 고려 사항 섹션에서 설명한 것과 같이 다른 이유로 인해 다중 지점 이더넷 세그먼트를 통한 하위 최적 포워딩에서는 잠재적인 성능 병목 현상이 계속 발생합니다.

> **참고:** ICMP 리디렉션은 Cisco IOS 및 Cisco NX-OS 소프트웨어의 레이어 3 인터페이스에서 기본적으로 활성화됩니다.

참고: ICMP 리디렉션 메시지가 생성될 때의 조건 요약: Layer3 스위치는 데이터 패킷이 이 패킷이 수신된 Layer 3 인터페이스 외부로 전달되어야 하는 경우 데이터 패킷의 소스로 ICMP 리디렉션 메시지를 다시 생성합니다.

이더넷 네트워크를 통한 최적의 미달 경로

OSFP(Open Shortest Path First) 및 Cisco EIGRP(Enhanced Interior Gateway Routing Protocol)와 같은 IGP(Interior Gateway Protocol)는 라우터 간 라우팅 정보를 동기화하고, 해당 정보를 준수하는 모든 네트워크 노드에서 일관되고 예측 가능한 패킷 포워딩 동작을 제공하도록 설계되었습니다. 예를 들어, 다중 지점 이더넷 네트워크의 경우 세그먼트의 모든 레이어 3 노드가 동일한 라우팅 정보를 사용하고 목적지까지의 동일한 종료 지점에 동의하는 경우, 이러한 네트워크 전반에서 최적화되지 않은 포워딩은 거의 불가능합니다.

하위 최적 포워딩 경로의 원인을 파악하려면 레이어 3 노드가 서로 독립적인 패킷 포워딩 결정을 내린다는 점에 유의하십시오. 즉, 라우터 B가 결정한 패킷 전달 결정은 라우터 A가 결정한 패킷 전달 결정에 의존하지 않습니다. 이는 IP 네트워크를 통한 패킷 포워딩 문제를 해결할 때 기억해야 할 핵심 원칙 중 하나이며, 다중 지점 이더넷 네트워크에서 최적 상태가 아닌 포워딩 경로를 조사할 때 유의해야 할 중요한 원칙입니다.

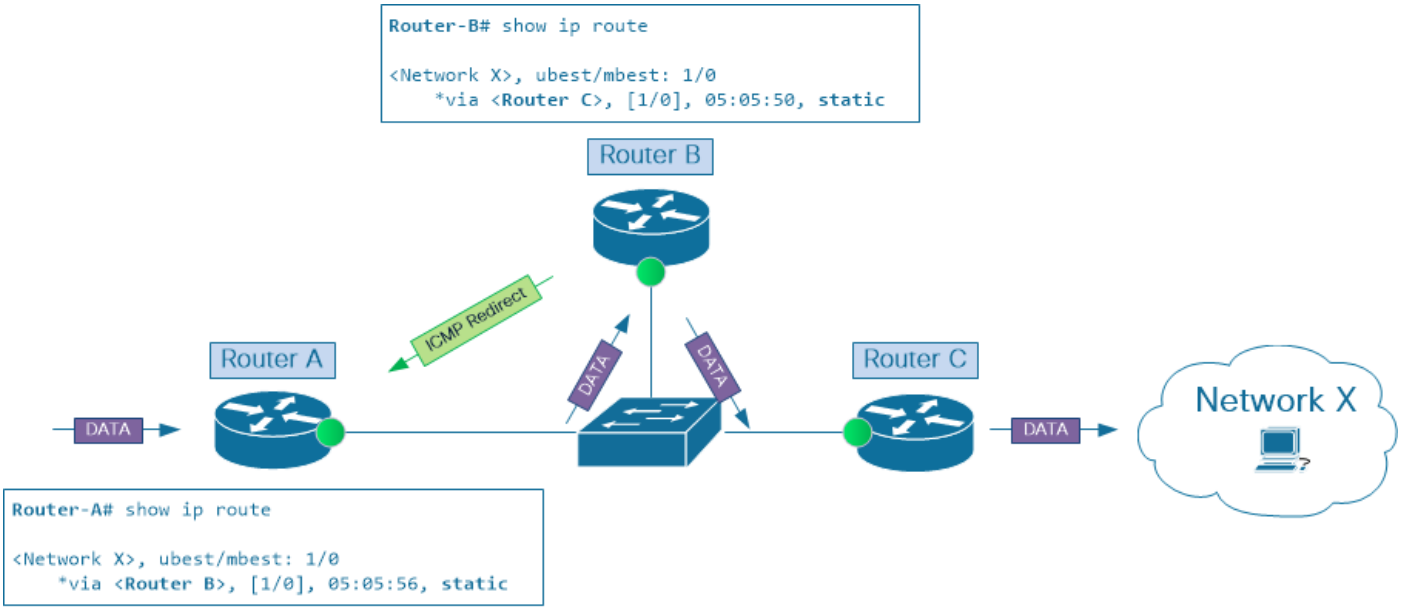
앞에서 언급한 것처럼, 모든 라우터가 단일 동적 라우팅 프로토콜을 사용하여 엔드포인트 간에 트래픽을 전달하는 네트워크에서는 멀티포인트 이더넷 세그먼트를 통해 최적화되지 않은 포워딩이 발생하지 않아야 합니다. 그러나 실제 네트워크에서는 다양한 패킷 라우팅 및 전달 메커니즘의 조합을 찾는 것이 매우 일반적입니다. 이러한 메커니즘의 예로는 다양한 IGP, 정적 라우팅 및 정책 기반 라우팅이 있습니다. 이러한 기능은 일반적으로 네트워크를 통해 원하는 트래픽 포워딩을 수행하는 데 함께 사용됩니다.

이러한 메커니즘을 복합적으로 사용하면 트래픽 흐름을 세부적으로 조정하고 특정 네트워크 설계의 요구 사항을 충족하는 데 도움이 될 수 있지만, 다중 지점 이더넷 네트워크에서 이러한 도구를 함께 사용하면 전반적인 네트워크 성능이 저하될 수 있는 부작용을 간과합니다.

정적 라우팅

이를 설명하기 위해 그림 4의 시나리오를 고려해 보십시오. 라우터 A는 네트워크 X에 대한 고정 경로를 가지며 라우터 B를 다음 홉으로 사용합니다. 동시에 라우터 B는 네트워크 X에 대한 고정 경로에서 라우터 C를 다음 홉으로 사용합니다.

그림 4 정적 라우팅을 사용하는 최적 상태 이하의 경로



고정 라우팅이 있는 최적 상태 이하의 경로

트래픽이 라우터 A에서 이 네트워크로 들어가 라우터 C를 통해 나가고 결국 대상 네트워크 X로 전달되는 동안 패킷은 목적지로 가는 과정에서 이 IP 네트워크를 두 번 통과해야 합니다. 이는 네트워크 리소스의 효율적인 사용이 아닙니다. 대신 라우터 A에서 라우터 C로 패킷을 직접 전송하면 동일한 결과를 얻는 동시에 네트워크 리소스를 덜 소비하게 됩니다.

> **참고:** 이 시나리오에서는 라우터 A와 라우터 C가 이 IP 네트워크 세그먼트의 인그레스 및 이그레스 레이어 3 노드로 사용되지만, 두 노드가 동일한 패킷 포워딩 동작을 수행하는 라우팅 컨피그레이션을 가지고 있으면 두 노드 모두 네트워크 어플라이언스(예: 로드 밸런서 또는 방화벽)로 교체할 수 있습니다.

정책 기반 라우팅

PBR(Policy Based Routing)은 이더넷 네트워크를 통해 최적의 경로를 제공하지 못하게 하는 또 다른 메커니즘입니다. 그러나 정적 또는 동적 라우팅과 달리 PBR은 라우팅 테이블 레벨에서 작동하지 않습니다. 대신 PBR은 스위치 하드웨어에서 직접 트래픽 리디렉션 ACL(Access Control List)을 프로그래밍합니다. 따라서 선택한 트래픽 흐름의 경우 인그레스 라인 카드에서 패킷 전달 조회가 정적 또는 동적 라우팅을 통해 얻은 라우팅 정보를 우회합니다.

그림 4에서 라우터 A와 B는 대상 네트워크 X에 대한 라우팅 정보를 동적 라우팅 프로토콜 중 하나와 교환합니다. 둘 다 라우터 B가 이 네트워크에 가장 적합한 다음 홉이라는 데 동의합니다.

그러나 라우팅 프로토콜에서 수신한 라우팅 정보를 재정의하고 라우터 C를 네트워크 X에 대한 next-hop으로 설정하는 라우터 B의 PBR 컨피그레이션에서는 ICMP 리디렉션 기능을 트리거할 조건이 충족되며 패킷이 라우터 B의 CPU로 전송되어 더 자세히 처리됩니다.

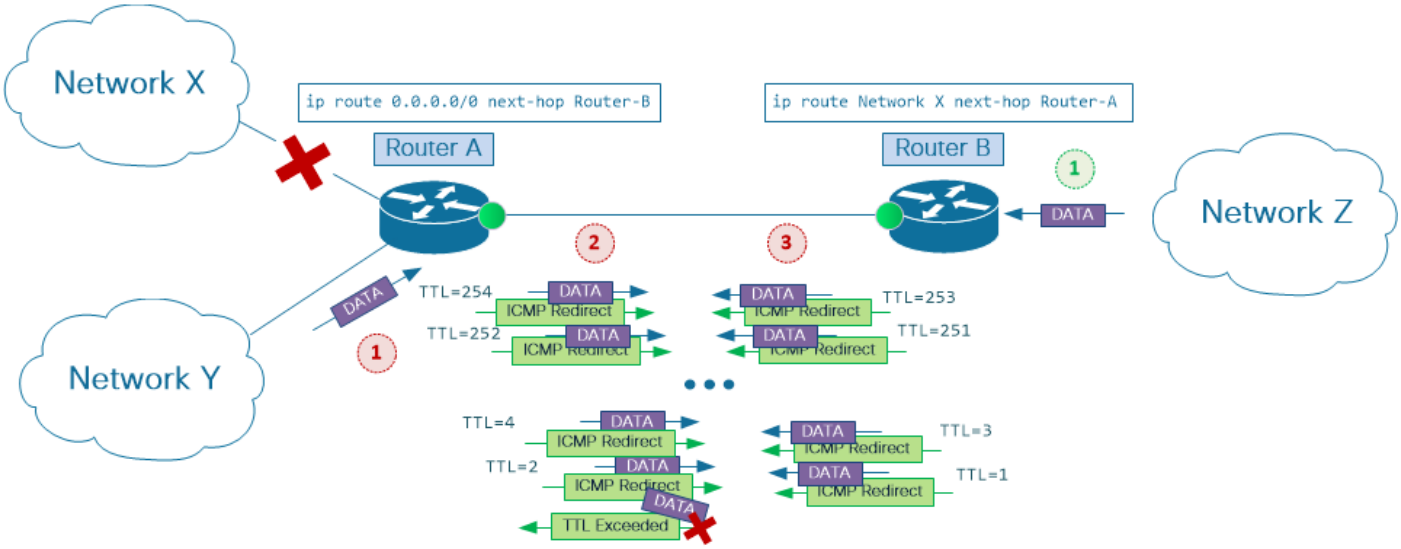
Point-to-Point 링크의 ICMP 리디렉션

지금까지 이 문서에서는 3개 이상의 레이어 3 노드가 연결된 이더넷 네트워크를 언급했으며, 따라서 멀티 포인트 이더넷 네트워크라고 명명했습니다. 그러나 ICMP 리디렉션 메시지는 포인트-투-포인트 이더넷 링크에서도 생성될 수 있습니다.

그림 5의 시나리오를 가정해 보십시오. 라우터 A는 정적 기본 경로를 사용하여 라우터 B로 트래픽

을 전송하는 반면, 라우터 B는 네트워크 X로 향하는 정적 경로가 있으며 이 경로는 라우터 A를 가리킵니다.

그림 5 Point-to-Point 링크의 ICMP 리디렉션



고정 라우팅이 있는 최적 상태 이하의 경로

싱글 홈(single-homed) 연결이라고도 하는 이 설계 옵션은 소규모 사용자 환경을 통신 사업자 네트워크에 연결할 때 널리 사용되는 옵션입니다. 여기서 라우터 B는 PE(Provider Edge) 디바이스이고 라우터 A는 CE(User Edge) 디바이스입니다.

일반적인 CE 컨피그레이션에는 Null0 인터페이스를 가리키는 사용자 IP 주소 블록에 대한 집계 고정 경로가 포함됩니다. 이 컨피그레이션은 고정 라우팅을 사용하는 싱글 홈 CE-PE 연결 옵션에 권장되는 모범 사례입니다. 그러나 이 예의 목적상 그러한 컨피그레이션이 존재하지 않는다고 가정합니다.

그림과 같이 라우터 A가 네트워크 X와의 연결이 끊긴다고 가정합니다. 사용자 Network Y 또는 원격 Network Z의 패킷이 Network X에 도달하려고 할 때 라우터 A와 B는 서로 간에 트래픽을 반송할 수 있으며, 값이 1에 도달할 때까지 모든 패킷의 IP Time-To-Live 필드를 줄일 수 있습니다. 이 경우 패킷의 추가 라우팅은 불가능합니다.

네트워크 X에 대한 트래픽이 PE와 CE 라우터 사이에서 앞뒤로 반송되는 동안 CE-PE 링크 대역폭 사용률이 급격하게(그리고 불필요하게) 증가하지만, 포인트-투-포인트 PE-CE 연결의 한 쪽 또는 양쪽에서 ICMP 리디렉션이 활성화되면 문제가 더 심각해집니다. 이 경우, 네트워크 X로 향하는 흐름의 모든 패킷은 각 라우터의 CPU에서 여러 번 처리되어 ICMP 리디렉션 메시지를 생성할 수 있습니다.

Nexus 플랫폼 고려 사항

레이어 3 인터페이스에서 ICMP 리디렉션이 활성화되고 수신 데이터 패킷이 이 인터페이스를 사용하여 레이어 3 스위치를 인그레스 및 이그레스(egress)하는 경우 ICMP 리디렉션 메시지가 생성됩니다. 레이어 3 패킷 포워딩은 Cisco Nexus 7000 플랫폼의 하드웨어에서 수행되지만 ICMP 리디렉션 메시지를 구성하는 것은 스위치 CPU의 책임입니다. 이렇게 하려면 Nexus 7000 Supervisor 모듈의 CPU에서 네트워크 세그먼트를 통과하는 경로를 최적화할 수 있는 흐름의 IP 주소 정보를 얻어야 합니다. 이는 인그레스 라인 카드가 수퍼바이저 모듈로 전송한 데이터 패킷의 원인입니다.

ICMP 리디렉션 메시지의 수신자가 이를 무시하고 ICMP 리디렉션이 활성화된 Nexus 스위치의 레

이어 3 인터페이스에 데이터 트래픽을 계속 전달하는 경우 각 데이터 패킷에 대해 ICMP 리디렉션 생성 프로세스가 트리거됩니다.

라인 카드 레벨에서 하드웨어 포워딩 예외 형식으로 프로세스가 시작됩니다. 라인 카드 모듈에서 패킷 전달 작업을 성공적으로 완료할 수 없는 경우 ASIC에서 예외가 발생합니다. 이 경우 올바른 패킷 처리를 위해 데이터 패킷을 수퍼바이저 모듈로 전송해야 합니다.

> **참고:** 수퍼바이저 모듈의 CPU는 ICMP 리디렉션 메시지를 생성할 뿐 아니라 TTL(Time To Live) 값이 1로 설정된 IP 패킷 또는 다음 홉으로 전송되기 전에 프래그먼트화되어야 하는 IP 패킷과 같은 기타 많은 패킷 전달 예외를 처리합니다.

수퍼바이저 모듈의 CPU가 ICMP 리디렉션 메시지를 소스로 보낸 후 이그레스 라인 카드 모듈을 통해 다음 홉으로 데이터 패킷을 전달하여 예외 처리를 완료합니다.

Nexus 7000 수퍼바이저 모듈은 대량의 트래픽을 처리할 수 있는 강력한 CPU 프로세서를 사용하지만, 패킷 포워딩 프로세스에서 수퍼바이저 CPU 프로세서를 관여시킬 필요 없이 라인 카드 레벨에서 대부분의 데이터 트래픽을 처리하도록 설계되었습니다. 따라서 CPU는 핵심 작업에 집중할 수 있으며 패킷 포워딩 작업은 라인 카드의 전용 하드웨어 엔진에 맡깁니다.

안정적인 네트워크에서는 패킷 전달 예외가 발생할 경우 비교적 낮은 속도로 발생할 수 있습니다. 이 경우 성능에 큰 영향을 주지 않고 수퍼바이저 CPU에서 처리할 수 있습니다. 반면, 매우 빠른 속도로 발생하는 패킷 포워딩 예외를 처리하는 CPU의 경우 전반적인 시스템 안정성 및 응답성에 부정적인 영향을 미칠 수 있습니다.

Nexus 7000 플랫폼 설계는 대량의 트래픽으로부터 스위치 CPU를 보호하기 위한 다양한 메커니즘을 제공합니다. 이러한 메커니즘은 시스템의 다른 지점에서 구현됩니다. 라인 카드 레벨에는 하드웨어 레이트 리미터 및 컨트롤 플레인이 있습니다 Policing (CoPP) 기능. 두 가지 모두 트래픽 속도 임계값을 설정하여 각 라인 카드 모듈에서 수퍼바이저로 전달될 트래픽의 양을 효과적으로 제어합니다.

이러한 보호 메커니즘은 OSPF, BGP 또는 SSH와 같이 네트워크 안정성 및 스위치 관리 용이성에 중요한 다양한 제어 프로토콜의 트래픽을 우선시하는 동시에, 스위치의 컨트롤 플레인 기능에 중요하지 않은 트래픽 유형을 공격적으로 필터링합니다. 패킷 전달 예외로 인해 CPU로 전달되는 데이터 트래픽의 대부분은 이러한 메커니즘에 의해 크게 보호됩니다.

하드웨어 레이트 리미터 및 CoPP policing 메커니즘은 스위치의 컨트롤 플레인의 안정성을 제공하며 항상 사용하도록 설정하는 것이 좋습니다. 이러한 메커니즘은 데이터 패킷 삭제, 전송 지연, 네트워크 전반의 전반적인 애플리케이션 성능 저하의 주요 원인 중 하나일 수 있습니다. 따라서 트래픽 흐름이 네트워크를 통과하는 경로와 ICMP 리디렉션 기능을 사용할 수 있거나 사용할 것으로 예상되는 네트워크 장비를 모니터링하기 위한 도구 사용을 이해하는 것이 중요합니다.

트래픽 모니터링 및 진단 툴

show ip traffic

Cisco IOS와 Cisco NX-OS 소프트웨어는 모두 CPU가 처리하는 트래픽의 통계를 확인할 수 있는 방법을 제공합니다. 이 작업은 **show ip traffic** 명령을 실행합니다. 이 명령은 레이어 3 스위치 또는 라우터를 통해 ICMP 리디렉션 메시지의 수신 및/또는 생성을 확인하는 데 사용할 수 있습니다.

```
Nexus7000#show ip traffic | begin ICMP

ICMP Software Processed Traffic Statistics
----------------------------------------
Transmission:
Redirect: 1000, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

ICMP originate Req: 0, Redirects Originate Req: 1000
Originate deny - Resource fail: 0, short ip: 0, icmp: 0, others: 0
Reception:
Redirect: 0, unreachable: 0, echo request: 0, echo reply: 0,

<output omitted for brevity>

Nexus7000#
```

실행 show ip traffic 명령을 몇 번 실행하여 ICMP 리디렉션 카운터가 증가하는지 확인합니다.

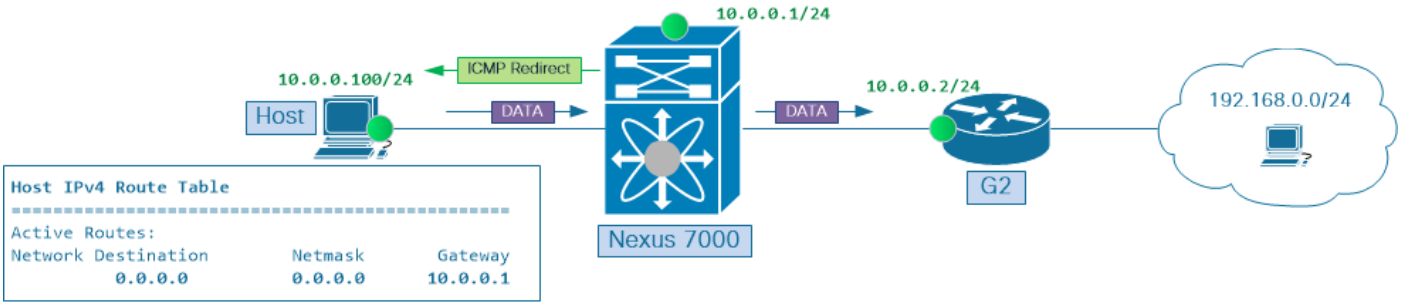
에트분석기

Cisco NX-OS 소프트웨어에는 트래픽을 캡처하는 툴이 내장되어 있습니다 flowing Ethanalyzer로 알려진 스위치 CPU와 주고받습니다.

> **참고:** Ethanalyzer에 대한 자세한 내용은 Nexus 7000의 Ethanalyzer 트러블슈팅 가이드를 참조하십시오.

그림 6은 그림 3의 시나리오와 유사한 시나리오를 보여줍니다. 여기서 네트워크 X는 192.168.0.0/24 네트워크로 교체됩니다.

그림 6 Ethanalyzer 캡처 실행



Ethanalyzer 캡처 실행

호스트 10.0.0.100은 ICMP 에코 요청의 연속 스트림을 대상 IP 주소 192.168.0.1로 전송합니다. 호스트는 Nexus 7000 스위치의 SVI(Switch Virtual Interface) 10을 원격 네트워크 192.168.0.0/24에 대한 다음 홉으로 사용합니다. 데모용으로 호스트는 ICMP 리디렉션 메시지를 무시하도록 구성됩니다.

다음 명령을 사용하여 Nexus 7000 CPU에서 수신 및 전송한 ICMP 트래픽을 캡처합니다.

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000

Capturing on inband
2018-09-15 23:45:40.124077   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.124477     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.124533   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126344   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.126607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.126655   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128348   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
    2018-09-15 23:45:40.128611     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
    2018-09-15 23:45:40.128659   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130362   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.130621     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.130669   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132392   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.132652     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.132700   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.134612     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.134660   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136347   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.136598     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.136645   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138351   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request
2018-09-15 23:45:40.138607     10.0.0.1 -> 10.0.0.100   ICMP Redirect (Redirect for host)
2018-09-15 23:45:40.138656   10.0.0.100 -> 192.168.0.1      ICMP Echo (ping) request

...
```

이전 출력의 타임스탬프는 이 예에서 강조 표시된 3개의 패킷이 동시에 캡처되었음을 나타냅니다 (2018-09-15 23:45:40.128). 다음은 이 패킷 그룹의 패킷별 분석입니다

- 첫 번째 패킷은 인그레스 데이터 패킷이며, 이 예에서는 ICMP 에코 요청입니다.
  2018-09-15 23:45:40.128348 10.0.0.100 -> 192.168.0.1 ICMP 에코(ping) 요청
- 두 번째 패킷은 게이트웨이에 의해 생성되는 ICMP 리디렉션 패킷입니다. 이 패킷은 호스트로 다시 전송됩니다.
  2018-09-15 23:45:40.128611 10.0.0.1 -> 10.0.0.100 ICMP 리디렉션(호스트에 대해 리디렉션)
- 세 번째 패킷은 CPU에서 라우팅된 후 이그레스 방향으로 캡처된 데이터 패킷입니다. 이전에 표시된 것은 아니지만 이 패킷의 IP TTL이 감소하고 체크섬이 다시 계산됩니다.
  2018-09-15 23:45:40.128659 10.0.0.100 -> 192.168.0.1 ICMP 에코(ping) 요청

다양한 유형 및 흐름의 패킷이 많은 대규모 Ethanalyzer 캡처를 탐색하는 동안 ICMP 리디렉션 메시지를 이에 해당하는 데이터 트래픽과 상호 연결하기 어려울 수 있습니다.

이러한 상황에서는 ICMP Redirect 메시지에 중점을 두고 서브최적으로 전달된 트래픽 흐름에 대한 정보를 검색합니다. ICMP 리디렉션 메시지에는 인터넷 헤더와 원래 데이터그램 데이터의 처음 64비트가 포함됩니다. 이 데이터는 데이터그램의 소스에서 메시지를 적절한 프로세스와 일치시키는 데 사용됩니다.

Ethanalyzer 패킷 캡처 툴을 **detail 키워드**와 함께 사용하여 ICMP 리디렉션 메시지의 내용을 표시하고 최적의 상태가 아닌 데이터 플로우의 IP 주소 정보를 찾습니다

```
Nexus7000#ethanalyzer local interface inband capture-filter icmp limit-captured-frames 1000
detail

...
Frame 2 (70 bytes on wire, 70 bytes captured)
Arrival Time: Sep 15, 2018 23:54:04.388577000
[Time delta from previous captured frame: 0.000426000 seconds]
[Time delta from previous displayed frame: 0.000426000 seconds]
[Time since reference or first frame: 0.000426000 seconds]
Frame Number: 2
Frame Length: 70 bytes
Capture Length: 70 bytes
[Frame is marked: False]
[Protocols in frame: eth:ip:icmp:ip:icmp:data]
Ethernet II, Src: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf), Dst: 00:0a:00:0a:00:0a
(00:0a:00:0a:00:0a)
Destination: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
Address: 00:0a:00:0a:00:0a (00:0a:00:0a:00:0a)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Source: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
Address: 00:be:75:f2:9e:bf (00:be:75:f2:9e:bf)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
Type: IP (0x0800)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.100 (10.0.0.100)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 56
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
Fragment offset: 0
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0xadd9 [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.1 (10.0.0.1)
Destination: 10.0.0.100 (10.0.0.100)
Internet Control Message Protocol
 Type: 5 (Redirect)
 Code: 1 (Redirect for host)
Checksum: 0xb8e5 [correct]
Gateway address: 10.0.0.2 (10.0.0.2)
Internet Protocol, Src: 10.0.0.100 (10.0.0.100), Dst: 192.168.0.1 (192.168.0.1)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 84
Identification: 0xf986 (63878)
Flags: 0x00
0.. = Reserved bit: Not Set
.0. = Don't fragment: Not Set
..0 = More fragments: Not Set
```

```
Fragment offset: 0
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0xa8ae [correct]
[Good: True]
[Bad : False]
Source: 10.0.0.100 (10.0.0.100)
Destination: 192.168.0.1 (192.168.0.1)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0 ()
Checksum: 0x02f9 [incorrect, should be 0xcae1]
Identifier: 0xa01d
Sequence number: 36096 (0x8d00)

...
```

ICMP 리디렉션 비활성화

네트워크 설계에서 트래픽 흐름을 스위치 또는 라우터로 들어온 동일한 레이어 3 인터페이스 밖으로 라우팅해야 하는 경우, 이에 해당하는 레이어 3 인터페이스에서 ICMP 리디렉션 기능을 비활성화하면 흐름이 CPU를 통해 라우팅되지 않도록 할 수 있습니다.

실제로 대부분의 네트워크에서는 모든 레이어 3 인터페이스에서 ICMP 리디렉션을 사전 예방적으로 비활성화하는 것이 좋습니다. 물리적 인터페이스는 이더넷 인터페이스와 가상 인터페이스는 모두 Port-Channel 및 SVI 인터페이스와 같습니다. 이 no ip redirects 레이어 3 인터페이스에서 ICMP 리디렉션을 비활성화하는 Cisco NX-OS interface-level 명령입니다. ICMP 리디렉션 기능이 비활성화되었는지 확인하려면

- 확인**no ip redirects** 명령이 인터페이스 컨피그레이션에 추가됩니다.

```
Nexus7000#show run interface vlan 10

interface Vlan10
no shutdown no ip redirects
  ip address 10.0.0.1/24
```

- 인터페이스에서 ICMP 리디렉션의 상태가 "disabled"로 표시되는지 확인합니다.

```
Nexus7000#show ip interface vlan 10 | include redirects
  IP icmp redirects: disabled
```

- 스위치 수퍼바이저에서 하나 이상의 라인 카드로 인터페이스 컨피그레이션을 푸시하는 Cisco NX-OS 소프트웨어 구성 요소에 의해 ICMP Redirect enable/disable 플래그가 **0**으로 설정되었는지 확인합니다.

```
Nexus7000#show system internal eltm info interface vlan 10 | i icmp_redirect
  per_pkt_ls_en = 0, icmp_redirect = 0, v4_same_if_check = 0
```

- 하나 이상의 라인 카드에서 특정 레이어 3 인터페이스에 대한 ICMP 리디렉션 활성화/**비활성화** 플래그가 **0**으로 설정되어 있는지 확인합니다.

```
Nexus7000#attach module 7
Attaching to module 7 ...
To exit type 'exit', to abort type '$.'
```

```
Last login: Wed Sep 15 23:56:25 UTC 2018 from 127.1.1.1 on pts/0
module-7#

!--- Optionally, jump to non-admin Virtual Device Context (VDC) if verification needs to be done
in one of the custom VDCs
module-7#vdc 6

module-7#show system internal iftmc info interface vlan 10 | include icmp_redirect
icmp_redirect : 0x0 ipv6_redirect : 0x1
```

요약

RFC 792에 설명된 대로 ICMP 리디렉션 메커니즘은 다중 지점 네트워크 세그먼트를 통한 포워딩 경로를 최적화하도록 설계되었습니다. 인터넷을 시작할 때 이러한 최적화를 통해 링크 대역폭 및 라우터의 CPU 사이클과 같은 값비싼 네트워크 리소스를 보호할 수 있었습니다. 네트워크 대역폭이 더욱 저렴해지고 상대적으로 느린 CPU 기반 패킷 라우팅이 전용 하드웨어 ASIC에서 더 빠른 레이어 3 패킷 포워딩으로 진화하면서 다중 지점 네트워크 세그먼트를 통한 최적의 데이터 전송 중요성이 감소했습니다. 기본적으로 ICMP 리디렉션 기능은 모든 레이어 3 인터페이스에서 활성화됩니다. 그러나 다중 지점 이더넷 세그먼트의 네트워크 노드에 최적의 전달 경로를 알리려는 시도가 네트워크 담당자에 의해 항상 이해되고 수행되는 것은 아닙니다. 고정 라우팅, 동적 라우팅 및 정책 기반 라우팅과 같은 다양한 전달 메커니즘을 함께 사용하는 네트워크에서 ICMP 리디렉션 기능을 사용하도록 설정하고 제대로 모니터링하지 않으면 프로덕션 트래픽을 처리하기 위해 트랜짓 노드 CPU를 원치 않게 사용할 수 있습니다. 이는 결과적으로 프로덕션 트래픽 흐름과 네트워크 인프라의 컨트롤 플레인 안정성 모두에 상당한 영향을 미칠 수 있습니다.

대부분의 네트워크에서는 네트워크 인프라의 모든 레이어 3 인터페이스에서 ICMP 리디렉션 기능을 사전에 비활성화하는 것이 좋습니다. 따라서 다중 지점 네트워크 세그먼트를 통해 더 나은 포워딩 경로가 있을 때 레이어 3 스위치 및 라우터의 CPU에서 처리되는 프로덕션 데이터 트래픽의 시나리오를 방지할 수 있습니다.

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.