IGRP 소개

목차

소개

이 문서에서는 IGRP(Interior Gateway Routing Protocol)를 소개합니다. 두 가지 목적이 있습니다 .하나는 IGRP 기술을 사용, 평가 및 구현에 관심이 있는 사용자를 위해 IGRP 기술을 소개하는 것입니다.다른 하나는 IGRP에 구현된 몇몇 흥미로운 아이디어와 개념에 더 많이 노출시키는 것입니다 .IGRP를 구성하는 방법에 대한 자세한 내용은 IGRP 구성, Cisco IGRP 구현 및 IGRP 명령을 참조하십시오.

IGRP의 목표

IGRP 프로토콜을 사용하면 여러 게이트웨이가 라우팅을 조정할 수 있습니다.목표는 다음과 같습니다.

- 매우 크거나 복잡한 네트워크에서도 안정적인 라우팅트랜지먼트처럼 라우팅 루프가 발생하지 않아야 합니다.
- 네트워크 토폴로지 변경에 대한 신속한 대응
- 낮은 오버헤드.즉, IGRP 자체는 작업에 실제로 필요한 것보다 더 많은 대역폭을 사용하지 않아

야 합니다.
- 트래픽이 대략적으로 동일할 경우 여러 병렬 경로 간에 트래픽을 분할합니다.
- 여러 경로의 오류 비율 및 트래픽 수준을 고려합니다.

IGRP의 현재 구현은 TCP/IP에 대한 라우팅을 처리합니다.그러나 기본 설계는 다양한 프로토콜을 처리할 수 있도록 설계되었습니다.

어떤 툴로도 모든 라우팅 문제를 해결할 수 없습니다.통상적으로 라우팅 문제는 여러 부분으로 나뉘어 있습니다.IGRP와 같은 프로토콜을 "내부 게이트웨이 프로토콜"(IGP)이라고 합니다. 단일 관리 또는 긴밀하게 조정된 단일 네트워크 집합 내에서 사용하기 위한 것입니다.이러한 네트워크 집합은 "외부 게이트웨이 프로토콜"(EGP)에 의해 연결됩니다. IGP는 네트워크 토폴로지에 대한 많은 세부 사항을 추적하도록 설계되었습니다.IGP를 설계할 때는 최적의 경로를 생성하고 변경 사항에 신속하게 응답해야 합니다.EGP는 하나의 네트워크 시스템을 다른 시스템의 오류 또는 의도적 오인사로부터 보호하려는 것이며, BGP는 그러한 외부 게이트웨이 프로토콜 중 하나입니다.EGP를 설계할 때는 안정성 및 관리 제어에 우선합니다.EGP가 최적의 경로가 아닌 합리적인 경로를 생성하기에 충분한 경우가 많습니다.

IGRP는 Xerox의 Routing Information Protocol, Berkeley의 RIP, Dave Mills's Hello와 같은 이전 프로토콜과 유사점이 있습니다.이는 주로 더 크고 복잡한 네트워크를 위해 설계되는 프로토콜과 다릅니다.이전 세대 프로토콜에서 가장 널리 사용되는 RIP와의 자세한 비교는 Comparison with RIP 섹션을 참조하십시오.

이러한 이전 프로토콜과 마찬가지로 IGRP는 거리 벡터 프로토콜입니다.이러한 프로토콜에서 게이트웨이는 인접 게이트웨이와 라우팅 정보만 교환합니다.이 라우팅 정보에는 네트워크의 나머지 부분에 대한 정보가 요약되어 있습니다.모든 게이트웨이가 함께 사용되어 분산 알고리즘의 양을 기준으로 최적화 문제를 해결하는 것으로 수학적으로 나타날 수 있습니다.각 게이트웨이는 문제의 일부만 해결해야 하며, 전체 데이터의 일부만 수신해야 합니다.

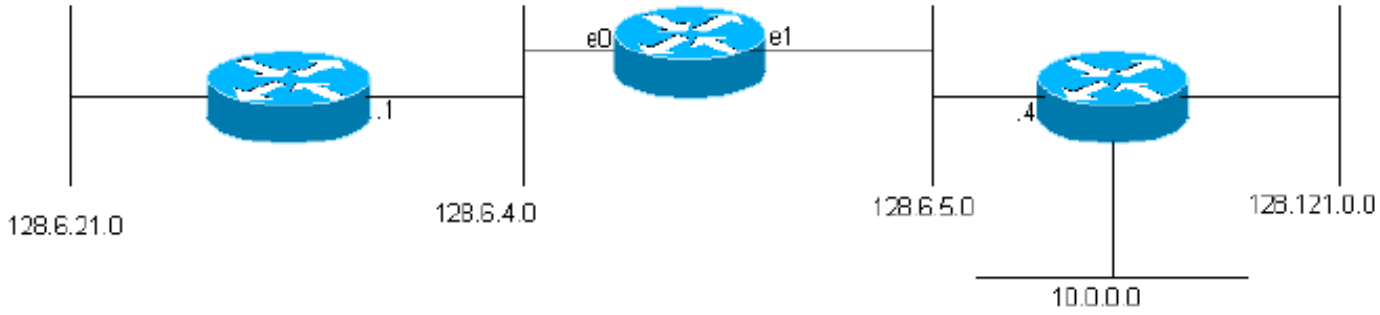
IGRP의 주요 대안은 EIGRP(Enhanced IGRP) 및 SPF(shortest-path first)라고 하는 알고리즘 클래스입니다.OSPF는 이 개념을 사용합니다.OSPF에 대한 자세한 내용은 OSPF 설계 가이드를 참조하십시오.OSPF 이러한 기능은 모든 게이트웨이가 다른 모든 게이트웨이의 모든 인터페이스 상태를 최신 상태로 유지하는 플러딩 기술을 기반으로 합니다.각 게이트웨이는 전체 네트워크에 대한 데이터를 사용하여 관점에서 최적화 문제를 독립적으로 해결합니다.각 접근 방식에는 이점이 있습니다.경우에 따라 SPF가 변경 사항에 더 신속하게 대응할 수 있습니다.라우팅 루프를 방지하기 위해 IGRP는 특정 종류의 변경 후 몇 분 동안 새 데이터를 무시해야 합니다.SPF는 각 게이트웨이에서 직접 정보를 제공하므로 이러한 라우팅 루프를 방지할 수 있습니다.따라서 즉시 새로운 정보를 적용할 수 있습니다.그러나 SPF는 내부 데이터 구조 및 게이트웨이 간 메시지 모두에서 IGRP보다 훨씬 많은 데이터를 처리해야 합니다.

라우팅 문제

IGRP는 여러 네트워크를 연결하는 게이트웨이에 사용하기 위한 것입니다.네트워크에서 패킷 기반 기술을 사용하는 것으로 가정합니다.실제로 게이트웨이는 패킷 스위치 역할을 합니다.한 네트워크에 연결된 시스템이 다른 네트워크의 시스템에 패킷을 전송하려는 경우 패킷을 게이트웨이로 처리합니다.대상이 게이트웨이에 연결된 네트워크 중 하나에 있는 경우 게이트웨이는 패킷을 대상으로 전달합니다.대상이 더 멀리 떨어져 있으면 게이트웨이는 대상에 더 가까운 다른 게이트웨이로 패킷을 전달합니다.게이트웨이는 라우팅 테이블을 사용하여 패킷으로 수행할 작업을 결정합니다.다음은 라우팅 테이블의 예입니다.(예제에 사용된 주소는 Rutgers University에서 가져온 IP 주소입니다.기본 라우팅 문제도 다른 프로토콜에서도 비슷하지만 이 설명에서는 IGRP가 라우팅 IP에 사용되고 있다고 가정합니다.)

그림 1

```
network      gateway     interface
  -------      -------     ---------
  128.6.4      none        ethernet 0
  128.6.5      none        ethernet 1
  128.6.21     128.6.4.1   ethernet 0
  128.121      128.6.5.4   ethernet 1
  10           128.6.5.4   ethernet 1
```



(실제 IGRP 라우팅 테이블에는 각 게이트웨이에 대한 추가 정보가 나와 있습니다.) 이 게이트웨이는 0과 1이라는 두 개의 이더넷에 연결됩니다. IP 네트워크 번호(실제 서브넷 번호) 128.6.4 및 128.6.5이 부여되었습니다. 따라서 이러한 특정 네트워크에 대해 주소가 지정된 패킷은 적절한 이더넷 인터페이스를 사용하여 목적지로 직접 전송할 수 있습니다.근처에 두 개의 게이트웨이 128.6.4.1 및 128.6.5.4이 있습니다. 128.6.4 및 128.6.5이 아닌 네트워크에 대한 패킷은 해당 게이트웨이 중 하나 또는 다른 게이트웨이로 전달됩니다.라우팅 테이블은 어떤 게이트웨이를 어떤 네트워크에 사용해야 하는지 나타냅니다.예를 들어, 네트워크 10의 호스트로 주소가 지정된 패킷은 게이트웨이 128.6.5.4으로 전달되어야 합니다. 이 게이트웨이가 네트워크 10에 가까울 수 있기를 바랍니다. 즉, 네트워크 10에 대한 최상의 경로가 이 게이트웨이를 통과하게 될 것입니다.IGRP의 주요 목적은 게이트웨이가 이와 같은 라우팅 테이블을 구축하고 유지할 수 있도록 하는 것입니다.

IGRP 요약

위에서 언급한 대로, IGRP는 게이트웨이가 다른 게이트웨이와 정보를 교환하여 라우팅 테이블을 구축할 수 있도록 하는 프로토콜입니다.게이트웨이는 직접 연결된 모든 네트워크에 대한 항목으로 시작합니다.인접 게이트웨이와 라우팅 업데이트를 교환하여 다른 네트워크에 대한 정보를 가져옵니다.가장 간단한 경우, 게이트웨이는 각 네트워크에 연결하는 가장 좋은 방법을 나타내는 하나의 경로를 찾습니다.경로는 패킷이 전송되어야 하는 다음 게이트웨이, 사용할 네트워크 인터페이스, 메트릭 정보로 특징화됩니다.메트릭 정보는 경로가 얼마나 좋은지를 나타내는 숫자 집합입니다.이렇게 하면 게이트웨이가 여러 게이트웨이에서 들은 경로를 비교하고 사용할 경로를 결정할 수 있습니다.둘 이상의 경로 간에 트래픽을 분할하는 것이 적합한 경우가 종종 있습니다.IGRP는 두 개 이상의 경로가 동일한 경우 이 작업을 수행합니다.또한 경로가 거의 동일하게 양호한 경우 트래픽을 분할하도록 구성할 수도 있습니다.이 경우 더 많은 트래픽이 더 나은 메트릭과 함께 경로를 따라 전송됩니다.트래픽은 9600bps 회선과 19200Bps 회선으로 분할할 수 있으며 19200bps 회선은 9600Bps 회선보다 약 2배 많은 트래픽을 얻을 수 있습니다.

IGRP에서 사용하는 메트릭은 다음과 같습니다.

- 토폴로지 지연 시간
- 경로의 가장 좁은 대역폭 세그먼트의 대역폭
- 경로의 채널 점유
- 경로의 신뢰성

토폴로지 지연 시간은 언로드된 네트워크를 가정하여 해당 경로를 따라 목적지에 도달하는 데 걸리는 시간입니다.물론 네트워크가 로드되면 추가로 지연이 발생합니다.그러나 실제 지연을 측정하지 않고 채널 점유 수치를 사용하여 로드를 고려합니다.경로 대역폭은 경로에서 가장 느린 링크의 초

당 비트 대역폭입니다.채널 점유율은 현재 사용 중인 대역폭의 양을 나타냅니다.측정되고 로드와 함께 변경됩니다.신뢰성은 현재 오류 속도를 나타냅니다.이는 손상되지 않은 상태로 대상에 도착하는 패킷의 비율입니다.측정됩니다.

이러한 정보는 메트릭의 일부로 사용되지 않지만 두 개의 추가 정보가 함께 전달됩니다.hop count 및 MTUhop count는 패킷이 목적지에 도달하기 위해 통과해야 하는 게이트웨이 수입니다.MTU는 조각화 없이 전체 경로를 따라 전송할 수 있는 최대 패킷 크기입니다.즉, 경로에 관련된 모든 네트워크의 최소 MTU입니다.

메트릭 정보를 기반으로 경로에 대해 단일 "복합 메트릭"이 계산됩니다.복합 메트릭은 다양한 메트릭 구성 요소의 효과를 해당 경로의 "선결"을 나타내는 단일 숫자로 결합합니다.최상의 경로를 결정하는 데 실제로 사용되는 복합 메트릭입니다.

각 게이트웨이는 정기적으로 전체 라우팅 테이블(분할 대상 기간 규칙 때문에 일부 설정)을 모든 인접 게이트웨이에 브로드캐스트합니다.게이트웨이가 다른 게이트웨이에서 이 브로드캐스트를 가져오면 테이블을 기존 테이블과 비교합니다.새 대상 및 경로가 게이트웨이의 라우팅 테이블에 추가됩니다.브로드캐스트의 경로는 기존 경로와 비교됩니다.새 경로가 더 나은 경우 기존 경로를 대체할 수 있습니다.또한 브로드캐스트의 정보는 채널 점유 및 기존 경로에 대한 기타 정보를 업데이트하는 데 사용됩니다.이 일반적인 절차는 모든 거리 벡터 프로토콜에서 사용되는 절차와 유사합니다.수학문학에서 벨만-포드 알고리즘이라고 불린다.이전 거리 벡터 프로토콜인 RIP를 설명하는 기본 절차의 자세한 개발 내용은 RFC 1058을 참조하십시오.

IGRP에서 일반 Bellman-Ford 알고리즘은 세 가지 중요한 측면에서 수정됩니다.먼저, 간단한 메트릭 대신 메트릭의 벡터를 사용하여 경로의 특성을 지정합니다.둘째, 메트릭이 가장 작은 단일 경로를 선택하는 대신, 트래픽은 메트릭이 지정된 범위에 속하는 여러 경로 간에 분할됩니다.셋째, 토폴로지가 변화하는 상황에서 안정성을 제공하기 위해 몇 가지 기능이 도입되었습니다.

복합 메트릭을 기반으로 최적 경로가 선택됩니다.

```
[(K1 / Be) + (K2 * Dc)] r
```

여기서 K1, K2 = 상수, Be = 언로드된 경로 대역폭 x (1 - 채널 점유), Dc = 토폴로지 지연 및 r = 안정성.

복합 메트릭이 가장 작은 경로가 가장 좋은 경로가 됩니다.동일한 대상에 대한 여러 경로가 있는 경우 게이트웨이는 둘 이상의 경로를 통해 패킷을 라우팅할 수 있습니다.이는 각 데이터 경로에 대한 복합 메트릭에 따라 수행됩니다.예를 들어, 한 경로의 복합 메트릭이 1이고 다른 경로의 복합 메트릭이 3인 경우 복합 메트릭이 1인 데이터 경로를 통해 전송되는 패킷의 수가 3배입니다.

메트릭 정보의 벡터를 사용하면 두 가지 이점이 있습니다.첫 번째는 동일한 데이터 집합에서 여러 유형의 서비스를 지원할 수 있는 기능을 제공한다는 것입니다.두 번째 장점은 정확성이 향상된다는 것입니다.단일 메트릭을 사용하면 일반적으로 지연인 것처럼 처리됩니다.경로의 각 링크가 총 메트릭에 추가됩니다.대역폭이 낮은 링크가 있으면 일반적으로 큰 지연으로 표시됩니다.그러나 대역폭 제한이 지연의 수행 방식을 누적하지는 않습니다.대역폭을 별도의 구성 요소로 간주하여 올바르게 처리할 수 있습니다.마찬가지로 로드는 별도의 채널 점유 번호로 처리할 수 있습니다.

IGRP는 루프를 포함한 일반 그래프 토폴로지를 안정적으로 처리할 수 있는 컴퓨터 네트워크를 상호 연결하기 위한 시스템을 제공합니다.시스템은 전체 경로 메트릭 정보를 유지 관리합니다. 즉, 게이트웨이가 연결된 다른 모든 네트워크에 대한 경로 매개변수를 알고 있습니다.트래픽은 병렬 경로를 통해 분산될 수 있으며, 전체 네트워크를 통해 여러 경로 매개변수를 동시에 계산할 수 있습니다.

RIP와 비교

이 섹션에서는 IGRP와 RIP를 비교합니다.이 비교는 RIP가 IGRP와 유사한 용도로 널리 사용되기 때문에 유용합니다.그러나, 이것을 하는 것이 전적으로 공평하지는 않다.RIP는 IGRP와 동일한 목표를 모두 충족하기 위한 것이 아닙니다.RIP는 상당히 통일된 기술을 갖춘 소규모 네트워크에서 사용하기 위한 목적이었습니다.그러한 응용에서는 대체로 적당하다.

IGRP와 RIP의 가장 기본적인 차이점은 메트릭의 구조입니다.그러나 이는 RIP에 간단히 적용할 수 있는 변화가 아닙니다.IGRP에 있는 새로운 알고리즘 및 데이터 구조가 필요합니다.

RIP는 네트워크를 설명하는 간단한 "hop count" 메트릭을 사용합니다.RIP에서는 모든 경로가 지연, 대역폭 등으로 설명되는 IGRP와 달리 RIP에서는 1에서 15 사이의 숫자로 설명됩니다. 일반적으로 이 숫자는 대상에 도달하기 전에 경로가 통과하는 게이트웨이 수를 나타내는 데 사용됩니다.즉, 느린 직렬 회선과 이더넷 간에 어떠한 차이도 발생하지 않습니다.일부 RIP 구현에서는 시스템 관리자가 지정된 홉을 두 번 이상 계산하도록 지정할 수 있습니다.느린 네트워크는 큰 홉으로 나타낼 수 있습니다.하지만 최대값이 15이므로 이 작업을 많이 수행할 수 없습니다.예를 들어, 이더넷이 1로 표시되고 56Kb 라인이 3으로 표시되는 경우, 경로에는 56Kb의 회선이 최대 5개 있을 수 있고 최대 15개를 초과할 수 있습니다.Cisco에서 실시한 연구에서는 사용 가능한 전체 네트워크 속도를 나타내고 대규모 네트워크를 허용하기 위해 24비트 메트릭이 필요하다는 것을 제시합니다.최대 메트릭이 너무 작으면 시스템 관리자에게 불쾌한 선택 사항이 표시됩니다.그가 빠른 경로와 느린 경로를 구별하지 못하거나 네트워크 전체를 한계에 맞출 수 없습니다.사실 이제 많은 전국 네트워크가 충분히 커서 모든 홉을 한 번만 계산해도 RIP가 이를 처리할 수 없습니다.RIP는 이러한 네트워크에 사용할 수 없습니다.

명확한 응답은 더 큰 메트릭을 허용하도록 RIP를 수정하는 것입니다.안타깝게도, 이것은 작동하지 않을 것입니다.모든 거리 벡터 프로토콜과 마찬가지로 RIP는 "무한대로 세기"의 문제를 안고 있습니다. 자세한 내용은 RFC 1058에 설명되어 있습니다 .토폴로지가 변경되면 잘못된 경로가 도입됩니다.이러한 허위 경로와 관련된 메트릭은 15까지 서서히 증가하여 경로가 제거될 때까지 늘어납니다.15는 트리거된 업데이트가 사용된다고 가정할 때 이 프로세스가 상당히 빠르게 통합될 수 있을 만큼 충분히 작은 최대값입니다.24비트 메트릭을 허용하도록 RIP를 수정한 경우 루프는 메트릭이 최대 2**24까지 계산될 만큼 충분히 오래 유지됩니다. 이 작업은 허용되지 않습니다.IGRP에는 잘못된 경로가 도입되지 않도록 설계된 기능이 있습니다.이러한 기능은 섹션 5.2에서 설명합니다. 이러한 기능을 도입하거나 SPF와 같은 프로토콜로 변경하지 않고 복잡한 네트워크를 처리하는 것은 적합하지 않습니다.

IGRP는 단순히 허용 가능한 메트릭 범위를 늘리는 것 이상의 작업을 수행합니다.또한 지연, 대역폭, 신뢰성 및 로드를 설명하기 위해 메트릭을 재구성합니다.RIP와 같은 단일 메트릭에서 이러한 고려사항을 나타낼 수 있습니다. 그러나 IGRP에서 적용하는 접근 방식은 잠재적으로 더 정확합니다.예를 들어, 단일 메트릭을 사용하면 연속적인 여러 고속 링크가 느린 단일 링크와 동일한 것으로 나타납니다.이는 인터랙티브 트래픽의 경우일 수 있으며, 여기서 지연은 주요 문제입니다.그러나 대량 데이터 전송의 경우 대역폭이 가장 큰 문제이며, 메트릭을 함께 추가하는 것은 적절한 방법이 아닙니다.IGRP는 지연과 대역폭을 별도로 처리하여 지연을 가중시키지만 대역폭은 최소한으로 줄입니다.안정성의 효과를 통합하고 단일 구성 요소 메트릭으로 로드하는 방법을 쉽게 확인할 수 없습니다.

제 생각에 IGRP의 큰 장점 중 하나는 손쉬운 구성입니다.물리적 의미가 있는 수량을 직접 나타낼 수 있습니다.즉, 인터페이스 유형, 회선 속도 등을 기준으로 자동으로 설정할 수 있습니다.단일 구성 요소 메트릭을 사용하면 여러 가지 다른 요소의 효과를 반영하기 위해 메트릭을 "조리"해야 할 가능성이 높습니다.

다른 혁신은 라우팅 프로토콜보다 알고리즘과 데이터 구조의 문제입니다.예를 들어 IGRP는 여러 경로 간에 트래픽을 분할하는 것을 지원하는 알고리즘과 데이터 구조를 지정합니다.이러한 작업을 수행하는 RIP의 구현을 설계할 수 있습니다.그러나 라우팅을 다시 구현하면 RIP를 계속 사용할 이유가 없습니다.

지금까지 저는 모든 네트워크 프로토콜에 대한 라우팅을 지원할 수 있는 기술인 "일반 IGRP"에 대해 설명했습니다.그러나 이 섹션에서는 특정 TCP/IP 구현에 대해 좀 더 자세히 살펴보겠습니다.이는 RIP와 비교할 구현입니다.

RIP 업데이트 메시지에는 단순히 라우팅 테이블의 스냅샷이 포함됩니다.즉, 목적지와 메트릭스 값이 많고 그 밖의 것은 거의 없습니다.IGRP의 IP 구현에는 추가 구조가 있습니다.먼저 업데이트 메시지는 "자동 시스템 번호"로 식별됩니다. 이 용어는 Arpanet의 전통에서 비롯되며, 거기서 구체적인 의미를 가집니다.그러나 대부분의 네트워크에서 이 기능이 의미하는 것은 동일한 네트워크에서 여러 가지 라우팅 시스템을 실행할 수 있다는 것입니다.이는 여러 조직의 네트워크가 통합되는 위치에 유용합니다.각 조직은 고유한 라우팅을 유지할 수 있습니다.각 업데이트의 레이블이 지정되므로 게이트웨이는 올바른 업데이트에만 집중하도록 구성할 수 있습니다.특정 게이트웨이는 여러 자동 시스템에서 업데이트를 수신하도록 구성됩니다.시스템 간에 통제된 방식으로 정보를 전달합니다.이는 라우팅 보안 문제에 대한 완전한 솔루션이 아닙니다.모든 게이트웨이는 자동 시스템에서 업데이트를 수신하도록 구성할 수 있습니다.그러나 네트워크 관리자 간에 상당한 신뢰 수준이 있는 라우팅 정책을 구현하는 데 여전히 매우 유용한 툴입니다.

IGRP 업데이트 메시지에 대한 두 번째 구조적 기능은 IGRP에서 기본 경로를 처리하는 방법에 영향을 줍니다.대부분의 라우팅 프로토콜은 기본 경로의 개념을 가지고 있습니다.전 세계 모든 네트워크를 나열하기 위해 업데이트를 라우팅하는 것은 종종 실용적이지 않습니다.일반적으로 게이트웨이 집합에는 조직 내 네트워크에 대한 자세한 라우팅 정보가 필요합니다.조직 외부의 대상에 대한 모든 트래픽을 몇 개의 경계 게이트웨이 중 하나로 전송할 수 있습니다.이러한 경계 게이트웨이에 대한 자세한 정보가 있을 수 있습니다.최상의 경계 게이트웨이에 대한 경로는 "기본 경로"입니다. 이는 내부 라우팅 업데이트에 특별히 나열되지 않은 목적지에 도달하는 데 사용된다는 점에서 기본값입니다.RIP 및 일부 다른 라우팅 프로토콜은 기본 경로에 대한 정보를 실제 네트워크인 것처럼 순환합니다.IGRP는 다른 접근 방식을 취합니다.IGRP는 기본 경로에 대한 단일 위조 항목 대신 실제 네트워크를 기본 경로로 사용할 후보로 플래그 지정할 수 있습니다.이 방법은 업데이트 메시지의 특수 외부 섹션에 해당 네트워크에 대한 정보를 배치하여 구현됩니다.그러나 이러한 네트워크와 관련된 것을 켜는 것으로 생각할 수도 있습니다.정기적으로 IGRP는 모든 후보 기본 경로를 스캔하고 가장 낮은 메트릭을 실제 기본 경로로 선택합니다.

이러한 기본 접근 방식은 대부분의 RIP 구현에서 적용하는 접근 방식보다 다소 유연합니다.일반적으로 RIP 게이트웨이는 지정된 특정 메트릭을 사용하여 기본 경로를 생성하도록 설정할 수 있습니다.이 작업은 경계 게이트웨이에서 수행되어야 합니다.

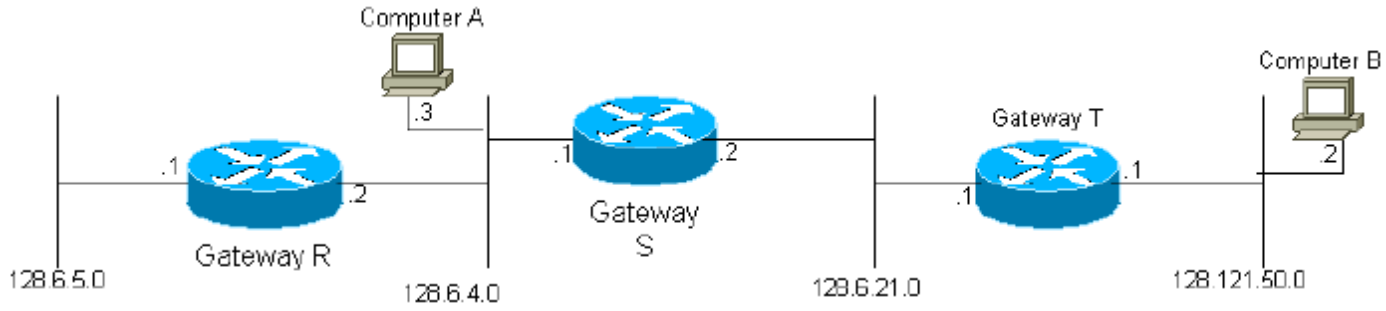
자세한 설명

이 섹션에서는 IGRP에 대한 자세한 설명을 제공합니다.

전체 설명

게이트웨이가 처음 켜지면 라우팅 테이블이 초기화됩니다.이 작업은 콘솔 터미널의 운영자가 수행하거나 구성 파일에서 정보를 읽어 수행할 수 있습니다.게이트웨이에 연결된 각 네트워크에 대한 설명(예: 링크를 이동하는 데 단일 비트가 걸리는 시간) 및 링크의 대역폭을 포함하여 제공됩니다.

그림 2



예를 들어 위의 다이어그램에서 게이트웨이 S는 해당 인터페이스를 통해 네트워크 2 및 3에 연결되었다고 합니다.따라서 처음에는 게이트웨이 2가 네트워크 2와 3의 모든 대상 컴퓨터에 연결할 수 있다는 것만 알고 있습니다. 모든 게이트웨이는 다른 게이트웨이에서 수집한 정보와 함께 초기화된 정보를 인접 게이트웨이로 주기적으로 전송하도록 프로그래밍됩니다.따라서 게이트웨이 S는 게이트웨이 R 및 T에서 업데이트를 수신하고 게이트웨이 R을 통해 네트워크 1의 컴퓨터와 게이트웨이 T를 통해 네트워크 4의 컴퓨터에 연결할 수 있다는 사실을 알게 됩니다. 게이트웨이 S는 전체 라우팅 테이블을 전송하므로 다음 주기 게이트웨이에서 게이트웨이 T를 통해 네트워크 1에 도달할 수 있음을 알게 됩니다. 시스템의 모든 네트워크에 대한 정보가 시스템의 모든 게이트웨이에 도달하여 네트워크가 완전히 연결되어 있다는 것만 제공된다는 것을 쉽게 알 수 있습니다.

그림 3

```
________ Network 1
       |
       gw A --nw2-- gw C
       |            / |
       |          /   |
       nw3    nw4     nw5
       |      /        |
       |    /          |
       gw B            gw D
      _|_______________|____ Network 6
```

각 게이트웨이는 대상 컴퓨터에 대한 데이터 경로의 적합성을 확인하기 위해 복합 메트릭을 계산합니다.예를 들어 위의 다이어그램에서 네트워크 6의 대상에 대해 게이트웨이 A(gw A)는 게이트웨이 B와 C를 통해 두 경로의 메트릭 기능을 계산합니다. 경로는 단순히 다음 홉에 의해 정의됩니다.실제로 A에서 네트워크 6으로 연결되는 경로는 3가지가 있습니다.

- B로 직접 이동
- C로, B로
- C, D 순으로

그러나 게이트웨이 A는 C와 관련된 두 경로 중에서 선택할 필요가 없습니다. A의 라우팅 테이블에는 C에 대한 경로를 나타내는 단일 항목이 있습니다. 해당 메트릭은 C에서 최종 대상으로 가져오는 최상의 방법을 나타냅니다.A가 C로 패킷을 전송하는 경우 B를 사용할지 아니면 D를 사용할지를 결정하는 것은 C에 달합니다.

수식 1

각 데이터 경로에 대해 계산된 복합 메트릭 함수는 아래와 같습니다.

```
[(K1 / Be) + (K2 * Dc)] r
```

여기서 r은 분수 안정성(다음 홉에서 성공적으로 수신되는 전송 비율), DC = 복합 지연, Be = 유효 대역폭:언로드된 대역폭 x(1 - 채널 점유), K1 및 K2 = 상수

수식 2

원칙적으로 복합 지연 DC는 아래와 같이 결정될 수 있습니다.

```
Dc = Ds + Dcir + Dt
```

여기서 Ds = 스위칭 지연, Dcir = 회로 지연(1비트 전파 지연), DT = 전송 지연(1500비트 메시지의 로드 없음 지연).

그러나 실제로 각 네트워크 기술 유형에 대해 표준 지연 수치가 사용됩니다.예를 들어 이더넷과 직렬 회선의 경우 특정 비트 전송률에 대한 표준 지연 수치가 있습니다.

위의 네트워크 6 다이어그램의 경우 게이트웨이 A의 라우팅 테이블이 어떻게 표시되는지 보여주는 예가 여기에 있습니다.(간소화를 위해 메트릭 벡터의 개별 구성 요소는 표시되지 않습니다.)

라우팅 테이블 예:

네트워크	인터페이스	다음 게이트웨이	메트릭
1	NW 1	없음	직접 연결
2	NW 2	없음	직접 연결
3	NW 3	없음	직접 연결
4	NW 2	C	1270
	NW 3	B	1180
5	NW 2	C	1270
	NW 3	B	2130
6	NW 2	C	2040
	NW 3	B	1180

인접 디바이스와 정보를 교환하여 라우팅 테이블을 구축하는 기본 프로세스는 Bellman-Ford 알고리즘에 의해 설명됩니다.이 알고리즘은 RIP(RFC 1058)와 같은 이전 프로토콜에서 사용되었습니다. 더 복잡한 네트워크를 처리하기 위해 IGRP는 기본 Bellman-Ford 알고리즘에 세 가지 기능을 추가합니다.

1. 간단한 메트릭 대신 메트릭의 벡터를 사용하여 경로의 특성을 지정합니다.위의 수식 1에 따라 이 벡터에서 단일 복합 메트릭을 계산할 수 있습니다.벡터를 사용하면 게이트웨이가 방정식 1의 여러 가지 계수를 사용하여 다양한 서비스 유형을 수용할 수 있습니다. 또한 단일 메트릭보다 네트워크의 특성을 더 정확하게 표현할 수 있습니다.
2. 메트릭이 가장 작은 단일 경로를 선택하는 대신, 트래픽은 지정된 범위에 속하는 메트릭이 있는 여러 경로 간에 분할됩니다.이렇게 하면 여러 경로를 병렬로 사용할 수 있으므로 단일 경로보다 더 효과적인 대역폭을 제공합니다.분산 V는 네트워크 관리자가 지정합니다.최소 복합 메트릭 M을 가진 모든 경로가 유지됩니다.또한 메트릭이 V x M 미만인 모든 경로가 유지됩니다.트래픽은 복합 메트릭에 비례하여 여러 경로 간에 분산됩니다.
3. 이러한 변화 개념에는 몇 가지 문제가 있다.차이 값이 1보다 크고 패킷 루핑으로 이어지지 않는 전략을 수립하기가 어렵습니다.Cisco 릴리스 8.2에서는 분산 기능이 구현되지 않습니다.어떤 릴리스에서 기능이 제거되었는지 잘 모르겠습니다. 이 효과는 분산을 영구적으로 1로 설정합니다.
4. 토폴로지가 변경되는 상황에서 안정성을 제공하기 위해 몇 가지 기능이 도입되었습니다.이러한 기능은 라우팅 루프와 "무한대로 세기"를 방지하기 위한 것으로, 이 유형의 애플리케이션에

대해 포드 유형 알고리즘을 사용하려고 했던 이전의 시도가 특징이었습니다.주요 안정성 기능은 "보류", "트리거된 업데이트", "split horizon" 및 "fishing"입니다. 이러한 내용은 아래에서 자세히 설명합니다.

트래픽 분할(포인트 2)은 다소 미묘한 위험을 발생시킵니다.분산 V는 게이트웨이가 서로 다른 속도의 병렬 경로를 사용할 수 있도록 설계되었습니다.예를 들어 이중화를 위해 19200BPS 회선과 함께 9600BPS 회선이 동시에 실행될 수 있습니다.분산 V가 1이면 최상의 경로만 사용됩니다.따라서 19200BPS 회선의 신뢰성이 상당히 높은 경우 9600BPS 회선은 사용되지 않습니다.그러나 여러 경로가 동일한 경우 로드가 이들 경로 간에 공유됩니다. 분산을 높임으로써 최상의 경로와 거의 비슷한 다른 경로 간에 트래픽을 분할할 수 있습니다.큰 차이가 있으므로 트래픽이 두 행 간에 분할됩니다.위험성은 큰 차이가 있기 때문에 느린 길이 아니라 "잘못된 방향"인 경로가 허용됩니다. 따라서 트래픽이 "업스트림"으로 전송되지 않도록 하는 추가 규칙이 있어야 합니다.원격 복합 메트릭(다음 홉에서 계산된 복합 메트릭)이 게이트웨이에서 계산된 복합 메트릭보다 큰 경로를 따라 트래픽이 전송되지 않습니다.일반적으로 병렬 경로를 사용해야 하는 특정 상황을 제외하고 시스템 관리자는 분산을 1보다 높게 설정하지 않는 것이 좋습니다.이 경우 분산은 "오른쪽" 결과를 제공하도록 신중하게 설정됩니다.

IGRP는 여러 "서비스 유형" 및 여러 프로토콜을 처리하도록 설계되었습니다.서비스 유형은 경로 평가 방법을 수정하는 데이터 패킷의 사양입니다.예를 들어, TCP/IP 프로토콜을 사용하면 패킷이 높은 대역폭, 낮은 지연 또는 높은 신뢰성의 상대적 중요도를 지정할 수 있습니다.일반적으로 대화형 애플리케이션은 낮은 지연을 지정하지만 대량 전송 애플리케이션은 높은 대역폭을 지정합니다.이러한 요구 사항은 Eq에서 사용할 수 있는 K1 및 K2의 상대 값을 결정합니다.1. 지원대상이 되는 패킷의 세부 항목의 조합을 "서비스 유형"이라 한다. 서비스 유형별로 K1 및 K2 매개변수 집합을 선택해야 합니다.각 서비스 유형에 대해 라우팅 테이블이 유지됩니다.이 작업은 Eq에 의해 정의된 복합 메트릭에 따라 경로가 선택 및 정렬되기 때문에 수행됩니다.1. 서비스 유형별로 다릅니다.이러한 라우팅 테이블의 모든 정보가 결합되어 게이트웨이가 교환하는 라우팅 업데이트 메시지를 생성합니다(그림 7 참조).

안정성 기능

이 섹션에서는 보류, 트리거된 업데이트, 수평선 분할 및 중독에 대해 설명합니다.이러한 기능은 게이트웨이가 잘못된 경로를 선택하지 못하도록 설계되었습니다.RFC 1058 에 설명된 대로, 게이트웨이 또는 네트워크의 장애로 인해 경로를 사용할 수 없게 될 때 이러한 문제가 발생할 수 있습니다.원칙적으로 인접 게이트웨이는 장애를 탐지합니다.그런 다음 이전 경로를 사용할 수 없음으로 표시하는 라우팅 업데이트를 전송합니다.그러나 업데이트가 네트워크의 일부 부분에 전혀 연결되지 않거나 특정 게이트웨이에 도달하는 데 지연될 수 있습니다.기존 경로가 좋다고 여전히 믿는 게이트웨이는 해당 정보를 계속 분산하여 실패한 경로를 시스템에 다시 입력할 수 있습니다.결국 이 정보는 네트워크를 통해 전파되고 다시 삽입된 게이트웨이로 돌아갑니다.결과는 순환 경로입니다.

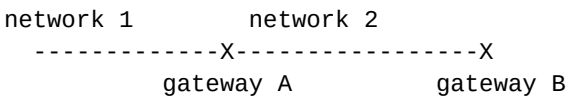
사실 그 대책에는 약간의 중복이 있다.원칙적으로 보류 및 트리거된 업데이트는 우선 잘못된 경로를 방지할 수 있는 충분한 것이어야 합니다.하지만 실제로, 다양한 종류의 통신 실패는 그것들의 불충분함을 야기시킬 수 있습니다.스플릿 라이즌 및 경로 중독은 어떤 경우에도 라우팅 루프를 방지하기 위한 것입니다.

일반적으로 새 라우팅 테이블은 정기적으로 인접 게이트웨이로 전송됩니다(시스템 관리자가 조정할 수 있지만 기본적으로 90초마다).트리거된 업데이트는 변경 사항에 따라 즉시 전송되는 새 라우팅 테이블입니다.가장 중요한 변경 사항은 경로 제거입니다.이 문제는 시간 제한이 만료되었거나(인접한 게이트웨이 또는 라인이 다운되었을 수 있음) 경로의 다음 게이트웨이에서 업데이트 메시지가 경로를 더 이상 사용할 수 없음을 표시하므로 발생할 수 있습니다.게이트웨이 G에서 더 이상 경로를 사용할 수 없음을 탐지하면 즉시 업데이트가 트리거됩니다.이 업데이트는 해당 경로를 사용할 수 없는 것으로 표시합니다.이 업데이트가 인접한 게이트웨이에 도달하면 어떻게 되는지 고려하십시오.인접 디바이스의 경로가 G로 다시 가리킬 경우 인접 디바이스가 경로를 제거해야 합니다.이로 인해 인접 디바이스가 업데이트 등을 트리거합니다.따라서 장애가 발생하면 업데이트 메시지가

급증합니다.이 물결은 경로가 실패한 게이트웨이 또는 네트워크를 통과하는 네트워크의 해당 부분 전체에 전파됩니다.

업데이트 흐름이 모든 적절한 게이트웨이에 즉시 도달하도록 보장할 수 있다면 트리거된 업데이트로도 충분할 것입니다.그러나 두 가지 문제가 있다.먼저, 업데이트 메시지가 포함된 패킷은 네트워크의 일부 링크에 의해 삭제되거나 손상될 수 있습니다.둘째, 트리거된 업데이트는 즉시 수행되지 않습니다.트리거된 업데이트를 아직 받지 않은 게이트웨이가 잘못된 시간에 정기적인 업데이트를 실행하여 트리거된 업데이트를 이미 가져온 네이버에 잘못된 경로를 다시 삽입하도록 할 수 있습니다.홀드다운은 이러한 문제를 해결하도록 설계되었습니다.holddown 규칙에서는 경로가 제거되면 일정 기간 동안 동일한 대상에 대해 새 경로가 수락되지 않는다고 말합니다.이렇게 하면 트리거된 업데이트 시간이 다른 모든 게이트웨이로 이동될 수 있으므로, 기존 게이트웨이를 다시 삽입하는 일부 게이트웨이가 아닌 새로운 경로를 확인할 수 있습니다.대기 기간은 트리거된 업데이트의 물결이 네트워크 전체에 전달될 수 있을 만큼 길어야 합니다.또한 삭제된 패킷을 처리하려면 몇 가지 정기적인 브로드캐스트 주기가 포함되어야 합니다.트리거된 업데이트 중 하나가 삭제되거나 손상된 경우 발생하는 상황을 고려하십시오.업데이트를 발급한 게이트웨이는 다음 정기 업데이트에서 다른 업데이트를 실행합니다.이렇게 하면 초기 물결을 놓친 인접 디바이스에서 트리거된 업데이트의 물결이 다시 시작됩니다.

트리거된 업데이트 및 보류 집합의 조합으로 만료된 경로를 제거하고 다시 삽입되지 않도록 충분히 해야 합니다.그러나, 어떤 추가적인 예방책들은 어쨌든 할 가치가 있다.매우 손실이 큰 네트워크와 분할된 네트워크를 허용합니다.IGRP에 의해 요구되는 추가적인 예방책들은 split horizon 및 route pointing입니다.수평선은 그 방향을 향해 다시 가는 것이 결코 이치에 맞지 않는다는 관찰에서 비롯된다.다음 상황을 고려하십시오.



게이트웨이 A는 B에게 네트워크 1에 대한 경로가 있음을 알려줍니다. B가 업데이트를 A로 보낼 때 네트워크 1을 언급할 이유가 없습니다. A가 1에 가깝기 때문에 B를 통해 진행할 이유가 없습니다. split horizon 규칙은 각 네이버(실제로 각 인접 네트워크)에 대해 별도의 업데이트 메시지가 생성되어야 한다고 말합니다. 지정된 인접 디바이스의 업데이트는 해당 인접 디바이스를 가리키는 경로를 생략해야 합니다.이 규칙은 인접 게이트웨이 간의 루프를 방지합니다.예를 들어 A의 네트워크 1에 대한 인터페이스가 실패할 경우스플릿 호라이즌 규칙이 없으면 B는 A에게 1에 도달할 수 있다고 말합니다. 더 이상 실제 경로가 없으므로 A가 해당 경로를 선택할 수 있습니다.이 경우 A와 B는 모두 1로 연결되는 경로를 가집니다. 그러나 A는 B와 B를 가리키며 A를 가리키게 됩니다. 물론 트리거된 업데이트와 다운타임은 이러한 상황을 방지해야 합니다.하지만 정보가 있던 곳으로 다시 보낼 이유가 없기 때문에, split horizon은 어쨌든 할 가치가 있습니다.split horizon은 루프를 방지하는 역할 외에도 업데이트 메시지의 크기를 줄입니다.

split horizon은 인접 게이트웨이 간의 루프를 방지해야 합니다.경로 중독은 더 큰 루프를 분해하기 위한 것이다.규칙은 업데이트가 기존 경로의 메트릭이 충분히 증가했음을 나타내는 경우 루프가 있다는 것입니다.경로를 제거하고 홀드다운에 넣어야 합니다.현재 규칙은 복합 메트릭이 1.1배 이상 증가하면 경로가 제거된다는 것입니다. 채널 점유 또는 신뢰성의 변경으로 인해 작은 메트릭 변경이 발생할 수 있으므로 복합 메트릭의 증가만으로 경로 제거를 트리거하는 것은 안전하지 않습니다.따라서 1.1의 요인은 단지 추론적 것입니다.정확한 값은 중요하지 않습니다.작은 루프는 트리거된 업데이트 및 중단으로 인해 차단되므로 이 규칙만 매우 큰 루프를 중단하면 됩니다.

보류 사용 안 함

릴리스 8.2부터 Cisco 코드는 보류 해제를 비활성화하는 옵션을 제공합니다.보류 중 단점은 기존 경로가 실패할 경우 새로운 경로 채택을 지연한다는 것입니다.기본 매개변수를 사용하면 라우터가 변경 후 새 경로를 채택하기 전에 몇 분 정도 걸릴 수 있습니다.그러나 위에서 설명한 이유로, 홀드다

운을 제거하는 것은 안전하지 않습니다.결과는 RFC 1058에 설명된 대로 무한대로 계산됩니다.우리는 추측하지만, 증명할 수 없지만, 더 강력한 경로 중독의 버전을 가지고, 홀드다운은 더 이상 무한대로 셀 것을 멈출 필요가 없다는 것입니다.따라서 홀드다운을 비활성화하면 이러한 강력한 형태의 경로 중독이 활성화됩니다.split horizon 및 triggered 업데이트는 여전히 유효합니다.

더 강력한 형태의 경로 중독은 홉의 수를 기준으로 합니다.경로에 대한 hop 카운트가 증가하면 경로가 제거됩니다.이렇게 하면 여전히 유효한 경로가 제거됩니다.경로가 이제 하나 이상의 게이트웨이를 통과하도록 네트워크의 다른 곳에서 변경된 경우 hop 카운트가 증가합니다.이 경우 경로는 여전히 유효합니다.그러나 라우팅 루프(카운트 대 무한대)와 이 사례를 구별하는 완전히 안전한 방법은 없습니다. 따라서 가장 안전한 방법은 홉의 수가 증가할 때마다 경로를 제거하는 것입니다.경로가 여전히 합법적인 경우 다음 업데이트에 의해 다시 설치되며, 이로 인해 시스템의 다른 위치에 경로를 재설치하는 트리거된 업데이트가 발생합니다.

일반적으로 거리 벡터 알고리즘1은 새로운 경로를 쉽게 채택합니다.시스템에서 오래된 것을 완전히 삭제하는 것이 문제입니다.따라서 의심스러운 경로를 제거하는 데 지나치게 공격적인 규칙은 안전해야 합니다.

업데이트 프로세스 세부 정보

그림 4~8에 설명된 프로세스 집합은 TCP/IP, DECnet 또는 ISO/OSI 프로토콜과 같은 단일 네트워크 프로토콜을 처리하기 위한 것입니다.그러나 프로토콜 세부 정보는 TCP/IP에 대해서만 제공됩니다.단일 게이트웨이는 둘 이상의 프로토콜을 따르는 데이터를 처리할 수 있습니다.각 프로토콜에는 서로 다른 주소 지정 구조와 패킷 형식이 있으므로 그림 4에서 8을 구현하는 데 사용되는 컴퓨터 코드는 일반적으로 각 프로토콜마다 다릅니다.그림 4에 설명된 프로세스는 그림 4에 대한 상세 노트에 설명된 대로 가장 많이 달라집니다. 그림 5 ~ 8에 설명된 프로세스는 동일한 일반 구조를 가집니다.프로토콜과 프로토콜의 주요 차이점은 라우팅 업데이트 패킷의 형식이며 특정 프로토콜과 호환되도록 설계되어야 합니다.

대상의 정의는 프로토콜마다 다를 수 있습니다.여기에 설명된 방법은 개별 호스트, 네트워크로 라우팅 또는 좀 더 복잡한 계층 주소 체계에 사용할 수 있습니다.사용되는 라우팅 유형은 프로토콜의 주소 지정 구조에 따라 달라집니다.현재 TCP/IP 구현에서는 IP 네트워크에 대한 라우팅만 지원합니다.따라서 "대상"은 IP 네트워크 또는 서브넷 번호를 의미합니다.서브넷 정보는 연결된 네트워크에만 저장됩니다.

그림 4~7은 게이트웨이에 사용되는 다양한 라우팅 프로세스의 의사 코드를 보여줍니다.프로그램이 시작되면 각 인터페이스를 설명하는 허용 가능한 프로토콜과 매개변수가 입력됩니다.

게이트웨이는 나열된 특정 프로토콜만 처리합니다.목록에 없는 프로토콜을 사용하는 시스템의 모든 통신은 무시됩니다.데이터 입력은 다음과 같습니다.

- 게이트웨이가 연결된 네트워크입니다.
- 각 네트워크의 언로드된 대역폭입니다.
- 각 네트워크의 토폴로지 지연.
- 각 네트워크의 신뢰성.
- 각 네트워크의 채널 점유.
- 각 네트워크의 MTU입니다.

그런 다음 각 데이터 경로에 대한 측정 단위 함수는 수식 1에 따라 계산됩니다. 처음 세 항목은 상당히 영구적입니다.기본 네트워크 기술의 기능이며 로드에 의존하지 않습니다.구성 파일 또는 직접 운영자 입력으로 설정할 수 있습니다.IGRP는 측정된 지연을 사용하지 않습니다.이론과 경험 모두 안정적인 라우팅을 유지하기 위해 측정된 지연을 사용하는 프로토콜은 매우 어렵다는 것을 시사합니다.두 가지 측정된 매개변수가 있습니다.신뢰성과 채널 점유.신뢰성은 네트워크 인터페이스 하드웨어 또는 펌웨어에서 보고하는 오류율을 기반으로 합니다.

이러한 입력 외에도 라우팅 알고리즘에는 여러 라우팅 매개변수의 값이 필요합니다.여기에는 타이머 값, 차이 및 보류 사용 여부가 포함됩니다.일반적으로 컨피그레이션 파일 또는 운영자 입력에 의해 지정됩니다.(Cisco 릴리스 8.2부터 분산은 영구적으로 1로 설정됩니다.)

초기 정보를 입력하면 네트워크 인터페이스 중 하나에 데이터 패킷이 도착하거나 타이머가 만료되는 이벤트(이벤트)에 의해 게이트웨이의 작업이 트리거됩니다.그림 4 ~ 7에 설명된 프로세스는 다음과 같이 트리거됩니다.

- 패킷이 도착하면 그림 4에 따라 처리됩니다. 그러면 패킷이 다른 인터페이스로 전송되거나 무시되거나 추가 처리를 위해 수락됩니다.
- 추가 처리를 위해 게이트웨이가 패킷을 수락하면 이 사양에 설명되어 있지 않은 프로토콜별 방식으로 분석됩니다.패킷이 라우팅 업데이트인 경우 그림 5에 따라 처리됩니다.
- 그림 6은 타이머에 의해 트리거된 이벤트를 보여줍니다.타이머가 초당 1회 인터럽트를 생성하도록 설정됩니다.인터럽트가 발생하면 그림 6에 표시된 프로세스가 실행됩니다.
- 그림 7은 라우팅 업데이트 서브루틴을 보여줍니다.이 서브루틴에 대한 통화는 그림 5와 6에 나와 있습니다.
- 또한 그림 8은 그림 5 및 7에 나와 있는 메트릭 계산 세부 사항을 보여줍니다.

경로 전파 및 만료를 제어하는 4가지 중요한 시간 상수가 있습니다.이러한 시간 상수는 시스템 관리자가 설정할 수 있습니다.그러나 기본값이 있습니다.다음 시간 상수는 다음과 같습니다.

- Broadcast time(브로드캐스트 시간) - 연결된 모든 인터페이스의 모든 게이트웨이에서 이러한 경우가 많습니다.기본값은 90초마다 한 번 있습니다.
- Invalid time(유효하지 않은 시간) - 이 시간 내에 지정된 경로에 대한 업데이트를 받지 못한 경우 시간 초과된 것으로 간주됩니다.업데이트가 포함된 패킷이 네트워크에서 삭제될 수 있도록 하려면 브로드캐스트 시간의 여러 배가 되어야 합니다.기본값은 브로드캐스트 시간의 3배입니다.
- Hold time(보류 시간) - 대상에 도달할 수 없거나 메트릭이 증가하여 독성을 유발하게 되면 대상이 "holddown"으로 이동합니다. 이 상태에서 이 시간 동안 동일한 대상에 대해 새 경로가 허용되지 않습니다.보류 시간은 이 상태가 지속되어야 하는 기간을 나타냅니다.방송 시간이 몇 배여야 합니다기본값은 브로드캐스트 시간의 3배와 10초입니다.Disable Holdings 섹션에 설명된 대로 Holdings를 비활성화할 수 있습니다.
- Flush time(플러시 시간) - 지정된 대상에 대해 이 시간 내에 업데이트가 수신되지 않은 경우 해당 항목이 라우팅 테이블에서 제거됩니다.잘못된 시간과 플러시 시간의 차이를 확인합니다.유효하지 않은 시간 후에 경로가 시간 초과되어 제거됩니다.대상에 대한 나머지 경로가 없는 경우 이제 대상에 연결할 수 없습니다.그러나 대상에 대한 데이터베이스 항목은 그대로 유지됩니다.그것은 그 홀드다운을 집행하기 위해 남아 있어야 합니다.플러시 시간이 지나면 데이터베이스 항목이 테이블에서 제거됩니다.잘못된 시간과 대기 시간보다 약간 더 길어야 합니다.기본값은 브로드캐스트 시간의 7배입니다.

이러한 수치는 다음과 같은 주요 데이터 구조를 미리 가정합니다.이러한 데이터 구조의 개별 집합은 게이트웨이가 지원하는 각 프로토콜에 대해 유지됩니다.각 프로토콜 내에서 지원되는 각 서비스 유형에 대해 별도의 데이터 구조 집합이 유지됩니다.

시스템에 알려진 각 대상에 대해 대상에 대한 경로 목록(Null일 수 있음), 보류 만료 시간 및 마지막 업데이트 시간이 있습니다.마지막 업데이트 시간은 이 대상에 대한 경로가 다른 게이트웨이의 업데이트에 마지막으로 포함된 시간을 나타냅니다.각 경로에 대해 업데이트 시간도 유지됩니다.대상에 대한 마지막 경로가 제거되면, 보류가 비활성화되지 않는 한 대상이 보류됩니다(자세한 내용은 Disable Holdings 섹션 참조). 보류 만료 시간은 보류 만료 시간을 나타냅니다.0이 아닌 사실은 대상이 홀드다운임을 나타냅니다.계산 시간을 절약하려면 각 대상에 대해 "최상의 메트릭"을 유지하는 것도 좋습니다.이는 대상에 대한 모든 경로에 대한 복합 메트릭의 최소값입니다.

대상에 대한 각 경로에 대해 경로에 다음 홉의 주소, 사용할 인터페이스, 토폴로지 지연, 대역폭, 신

뢰성, 채널 점유 등 경로를 특성화하는 메트릭 벡터가 있습니다.다른 정보는 또한 홉수, MTU, 정보 소스, 원격 복합 측정 단위 및 방정식 1에 따라 이 수치에서 계산된 복합 측정 단위를 포함하여 각 경로와 연결됩니다. 마지막 갱신 시간도 있습니다.정보 소스는 해당 경로에 대한 최신 업데이트가 어디에서 왔는지를 나타냅니다.실제로 이는 다음 홉의 주소와 동일합니다.마지막 업데이트 시간은 이 경로에 대한 최신 업데이트가 도착한 시간입니다.시간 초과 경로를 만료하는 데 사용됩니다.

IGRP 업데이트 메시지에는 3개의 부분이 있습니다.내부, 시스템("이 자동 시스템"을 의미하지만 내부적으로는 아님) 및 외부내부 섹션은 서브넷에 대한 경로를 위한 것입니다.일부 서브넷 정보는 포함되지 않습니다.하나의 네트워크의 서브넷만 포함됩니다.업데이트가 전송되는 주소와 연결된 네트워크입니다.일반적으로 업데이트는 각 인터페이스에서 브로드캐스트되므로 브로드캐스트가 전송되는 네트워크일 뿐입니다.(IGRP 요청에 대한 응답을 위해 발생하며 IGRP를 가리킵니다.) 주요 네트워크(예: 비 서브넷)는 외부 플래그가 지정되지 않는 한 업데이트 메시지의 시스템 부분에 배치됩니다.

네트워크가 다른 게이트웨이에서 학습되고 업데이트 메시지의 외부 부분에 정보가 도착한 경우 외부 네트워크로 플래그가 지정됩니다.Cisco의 구현을 통해 시스템 관리자는 특정 네트워크를 외관으로 선언할 수 있습니다.외부 경로는 "후보 기본값"이라고도 합니다. 이러한 경로는 기본적으로 적합하고 대상에 대한 명시적 경로가 없는 경우 사용할 게이트웨이로 이동하거나 게이트웨이를 통과하는 경로입니다.예를 들어 Rutgers에서는 NSFnet 백본으로 연결되는 경로를 외관으로 플래그 지정하기 위해 Rutgers를 지역 네트워크에 연결하는 게이트웨이를 구성합니다.Cisco의 구현에서는 가장 작은 메트릭으로 외부 경로를 선택하여 기본 경로를 선택합니다.

다음 섹션에서는 그림 4 ~ 8의 특정 부분을 명확하게 설명합니다.

패킷 라우팅

그림 4는 입력 패킷의 전반적인 처리에 대해 설명합니다.이것은 단순히 용어를 명확히 하는 데 사용된다.IP 게이트웨이가 수행하는 작업에 대한 완전한 설명은 아닙니다.

이 프로세스에서는 지원되는 프로토콜 목록 및 게이트웨이가 초기화될 때 입력된 인터페이스에 대한 정보를 사용합니다.패킷 처리에 대한 세부 정보는 패킷에서 사용하는 프로토콜에 따라 달라집니다.이는 A단계에서 결정됩니다. A단계는 모든 프로토콜에서 공유하는 그림 4의 유일한 부분입니다.프로토콜 유형이 알려지면 프로토콜 유형에 적합한 그림 4의 구현이 사용됩니다.패킷 내용의 세부 정보는 프로토콜의 사양에 의해 설명됩니다.프로토콜의 사양에는 패킷의 목적지를 결정하는 절차, 게이트웨이 자체가 목적지인지 확인하기 위해 목적지를 게이트웨이의 고유 주소와 비교하는 절차, 패킷이 브로드캐스트인지 여부를 확인하는 절차, 대상이 지정된 네트워크의 일부인지 여부를 확인하는 절차가 포함됩니다.이러한 절차는 그림 4의 B단계와 C단계에서 사용됩니다. D단계의 테스트를 수행하려면 라우팅 테이블에 나열된 대상을 검색해야 합니다.대상에 대한 라우팅 테이블에 항목이 있고 해당 대상이 하나 이상의 사용 가능한 경로와 연결되어 있으면 테스트가 충족됩니다.이 및 다음 단계에서 사용되는 대상 및 경로 데이터는 지원되는 각 서비스 유형에 대해 별도로 유지 관리됩니다.따라서 이 단계는 패킷에 의해 지정된 서비스 유형을 확인하고 이 단계와 다음 단계에 사용할 해당 데이터 구조 집합을 선택하는 것으로 시작합니다.

원격 복합 메트릭이 복합 메트릭보다 작은 경우 경로는 D단계와 E단계에서 사용할 수 있습니다.원격 복합 메트릭이 복합 메트릭보다 큰 경로는 메트릭으로 측정된 대로 다음 홉이 대상에서 "더 멀리" 있는 경로입니다.이를 "업스트림 경로"라고 합니다. 일반적으로 메트릭을 사용하면 업스트림 경로를 선택할 수 없습니다.업스트림 경로가 최상의 경로가 될 수 없다는 것을 쉽게 알 수 있습니다.그러나 큰 분산이 허용되면 가장 적합한 경로가 아닌 경로를 사용할 수 있습니다.그 중 일부는 업스트림일 수 있습니다.

단계 E는 사용할 경로를 계산합니다.원격 복합 메트릭이 복합 메트릭보다 높지 않은 경로는 고려하지 않습니다.둘 이상의 경로를 사용할 수 있는 경우 이러한 경로가 라운드 로빈 대체 가중치 형태로

사용됩니다.경로가 사용되는 빈도는 해당 합성 메트릭에 반비례합니다.

라우팅 업데이트 수신

그림 5는 인접 게이트웨이에서 수신한 라우팅 업데이트 처리에 대해 설명합니다.이러한 업데이트는 항목 목록으로 구성되며 각 항목은 단일 대상에 대한 정보를 제공합니다.여러 유형의 서비스를 수용하기 위해 단일 라우팅 업데이트에서 동일한 대상에 대해 둘 이상의 항목이 발생할 수 있습니다.이러한 각 항목은 그림 5에 설명된 대로 개별적으로 처리됩니다. 항목의 외부 부분이 업데이트의 외부 섹션에 있는 경우 이 프로세스의 결과로 추가된 경우 외부 플래그가 대상에 대해 설정됩니다.

그림 5에 설명된 전체 프로세스는 게이트웨이가 지원하는 각 서비스 유형에 대해 해당 서비스 유형과 연결된 대상/경로 정보 집합을 사용하여 한 번 반복되어야 합니다.그림 5의 가장 바깥쪽 루프에 나와 있습니다. 서비스 유형별로 전체 라우팅 업데이트가 한 번 처리되어야 합니다.(현재 IGRP의 구현은 여러 유형의 서비스를 지원하지 않으므로 가장 바깥쪽 루프가 실제로 구현되지 않습니다.)

A 단계에서는 경로에 대해 기본 허용 가능성 테스트가 수행됩니다.여기에는 대상에 대한 타당성 테스트가 포함되어야 합니다.Impossible("Martian") 네트워크 번호는 거부해야 합니다.(자세한 내용은 RFC 1009 및 RFC 1122 를 참조하십시오.) 참조하는 대상이 보류 중인 경우, 즉 보류 만료 시간이 0이 아닌 현재 시간보다 이후인 경우에도 업데이트가 거부됩니다.

B단계에서 라우팅 테이블이 검색되어 이 항목이 이미 알려진 경로를 설명하는지 여부를 확인합니다.라우팅 테이블의 경로는 연결된 대상, 경로의 일부로 나열된 다음 홉과 경로에 사용할 출력 인터페이스, 정보 소스(일반적으로 다음 홉과 동일한 방식으로 업데이트가 시작된 주소)에 의해 정의됩니다. 업데이트 패킷의 항목은 항목에 대상이 나열되는 경로, 출력 인터페이스는 업데이트가 들어온 인터페이스이고 다음 홉과 정보 소스가 업데이트를 보낸 게이트웨이의 주소("소스" S)에 대한 경로를 설명합니다.

H단계 및 T단계에서는 그림 7에 설명된 업데이트 프로세스가 예약되어 있습니다.이 프로세스는 그림 5에 설명된 전체 프로세스가 완료된 후에 실제로 실행됩니다.즉, 그림 7에 설명된 업데이트 프로세스는 그림 5에 설명된 처리 중에 여러 번 트리거되더라도 한 번만 수행됩니다. 또한 네트워크가 빠르게 변화하는 경우 업데이트가 너무 자주 실행되지 않도록 주의를 기울여야 합니다.

업데이트 패킷의 현재 항목에 의해 설명된 대상이 라우팅 테이블에 이미 있는 경우 K단계가 수행됩니다.K는 업데이트 패킷의 데이터에서 계산된 새 복합 메트릭을 대상에 대한 최상의 복합 메트릭과 비교합니다.최상의 복합 메트릭은 현재 다시 계산되지 않으므로 고려 중인 경로가 이미 라우팅 테이블에 있는 경우 이 테스트는 동일한 경로에 대한 새 메트릭과 이전 메트릭을 비교할 수 있습니다.

L 단계는 기존의 최상의 복합 메트릭보다 낮은 경로에 대해 수행됩니다.여기에는 기존 경로보다 더 나쁜 새 경로와 복합 메트릭이 증가한 기존 경로가 모두 포함됩니다.L단계에서는 새 경로가 허용되는지 여부를 테스트합니다.이 테스트에서는 새 경로가 유지하기에 충분한지 여부와 라우팅 중독에 대한 테스트를 모두 구현합니다.허용하려면 지연 값이 연결할 수 없는 대상(현재 IP 구현의 경우 24비트 필드의 모든 대상)을 나타내는 특수 값이 아니어야 하며 복합 메트릭(그림 8에 지정된 대로 계산)을 허용해야 합니다.복합 메트릭을 허용할지 여부를 결정하려면 대상에 대한 다른 모든 경로의 복합 메트릭과 비교합니다.이 중에서 M을 최소로 합니다.새 경로는 < V X M, 여기서 V는 게이트웨이를 초기화할 때 설정된 분산 경로입니다.V = 1(CISCO 릴리스 8.2의 경우 항상 TRUE임)인 경우 기존 메트릭보다 더 나쁜 메트릭은 허용되지 않습니다.여기에는 한 가지 예외가 있습니다.경로가 이미 존재하고 대상에 대한 유일한 경로인 경우 메트릭이 10% 이상 증가하지 않은 경우 또는 홉 수가 증가하지 않은 경우 경로가 유지됩니다.).

V단계는 경로에 대한 새 정보가 복합 메트릭이 감소됨을 나타내는 경우 수행됩니다.대상 D에 대한 모든 경로의 복합 메트릭이 비교됩니다.이 비교에서는 라우팅 테이블에 나타나는 것이 아니라 P에 대한 새 복합 메트릭이 사용됩니다.최소 복합 메트릭 M이 계산됩니다.그런 다음 D에 대한 모든 경

로를 다시 검사합니다.임의의 경로에 대한 복합 메트릭이 M x V 이상인 경우 해당 경로가 제거됩니다.V는 게이트웨이가 초기화될 때 입력된 차이입니다.(Cisco 릴리스 8.2부터 분산은 영구적으로 1로 설정됩니다.)

주기적 처리

그림 6에 설명된 프로세스는 1초에 한 번 트리거됩니다.라우팅 테이블의 다양한 타이머를 검사하여 만료된 타이머가 있는지 확인합니다.이러한 타이머에 대해서는 위에서 설명합니다.

U단계에서 그림 7에 설명된 프로세스가 활성화됩니다.

라우팅 테이블에 저장된 복합 메트릭은 측정 결과에 따라 시간별로 변경되는 채널 점유율에 따라 달라지므로 R단계 및 S단계가 필요합니다.인터페이스를 통해 측정된 트래픽의 이동 평균을 사용하여 정기적으로 채널 점유 값이 다시 계산됩니다.새로 계산된 값이 기존 값과 다른 경우 해당 인터페이스와 관련된 모든 복합 메트릭을 조정해야 합니다.라우팅 테이블에 표시된 모든 경로가 검사됩니다.next hop이 인터페이스 "I"를 사용하는 모든 경로의 복합 메트릭이 다시 계산됩니다.이 작업은 Equation 1에 따라 수행되며, 경로 메트릭의 일부로 라우팅 테이블에 저장된 값의 최대값과 새로 계산된 인터페이스의 채널 점유 값을 채널 점유 채널로 사용합니다.

업데이트 메시지 생성

그림 7에서는 게이트웨이가 다른 게이트웨이로 전송할 업데이트 메시지를 생성하는 방법을 설명합니다.게이트웨이에 연결된 각 네트워크 인터페이스에 대해 별도의 메시지가 생성됩니다.그런 다음 이 메시지는 인터페이스를 통해 연결할 수 있는 다른 모든 게이트웨이로 전송됩니다(J 단계). 일반적으로 이 작업은 메시지를 브로드캐스트로 전송하는 방식으로 수행됩니다.그러나 네트워크 기술 또는 프로토콜에서 브로드캐스트를 허용하지 않는 경우 메시지를 각 게이트웨이로 개별적으로 보내야 할 수 있습니다.

일반적으로 메시지는 G단계의 라우팅 테이블에서 각 대상에 대한 항목을 추가하여 작성됩니다. 각 서비스 유형과 연관된 대상/경로 데이터를 사용해야 합니다.최악의 경우 각 서비스 유형의 각 대상에 대한 업데이트에 새 항목이 추가됩니다.그러나 G단계에서 업데이트 메시지에 항목을 추가하기 전에 이미 추가된 항목이 스캔됩니다.새 항목이 업데이트 메시지에 이미 있으면 다시 추가되지 않습니다.새 항목은 대상 및 next hop 게이트웨이가 동일한 경우 기존 항목을 복제합니다.

단순성을 위해 pseudocode는 한 가지를 생략합니다. IGRP 업데이트 메시지에는 세 가지 부분이 있습니다.내부, 시스템, 외부 등 3개의 루프가 목적지에 있습니다.첫 번째 에는 업데이트를 전송할 네트워크의 서브넷만 포함됩니다.두 번째는 외부 플래그가 지정되지 않은 모든 주요 네트워크(예: 비 서브넷)를 포함합니다.세 번째는 외관으로 플래그가 지정된 모든 주요 네트워크를 포함합니다.

단계 E는 split horizon 테스트를 구현합니다.일반적인 경우, 이 테스트는 업데이트가 전송될 인터페이스와 동일한 경로가 나가는 경로에 대해 실패합니다.그러나 다른 게이트웨이에서 IGRP 요청에 대한 응답이나 "IGRP 지점"의 일부로서 특정 대상으로 업데이트를 전송하는 경우, 해당 대상에서 원래 가져온 최상의 경로(해당 "정보 소스"가 대상과 동일함)와 해당 출력 인터페이스가 요청에서 보낸 것과 동일한 경우에만 split horizon이 실패합니다.

메트릭 정보 계산

그림 8은 게이트웨이가 수신한 업데이트 메시지에서 메트릭 정보가 처리되는 방법 및 게이트웨이가 전송하는 업데이트 메시지에 대해 메트릭 정보가 생성되는 방법을 설명합니다.항목은 대상에 대한 특정 경로를 기반으로 합니다.대상에 대한 경로가 둘 이상인 경우 복합 메트릭이 최소인 경로가 선택됩니다.둘 이상의 경로에 최소 복합 메트릭이 있는 경우 임의 연결 끊기 규칙이 사용됩니다.(대

부분의 프로토콜에서 이는 다음 hop 게이트웨이의 주소를 기반으로 합니다.)

그림 4 - 수신 패킷 처리

```
Data packet arrives using interface I

A   Determine protocol used by packet

    If protocol is not supported
      then discard packet

B   If destination address matches any of gateway's addresses
    or the broadcast address
      then process packet in protocol-specific way

C   If destination is on a directly-connected network
      then send packet direct to the destination, using
      the encapsulation appropriate to the protocol and link type

D   If there are no paths to the destination in the routing
    table, or all paths are upstream
      then send protocol-specific error message and discard the packet

E   Choose the next path to use. If there are more than
    one, alternate round-robin with frequency proportional
    to inverse of composite metric.

    Get next hop from path chosen in previous step.

    Send packet to next hop, using encapsulation appropriate
    to protocol and data link type.
```

그림 5 - 수신 라우팅 업데이트 처리

```
Routing update arrives from source S

    For each type of service supported by gateway
      Use routing data associated with this type of service

      For each destination D shown in update

A       If D is unacceptable or in holddown
          then ignore this entry and continue loop with next destination D

B       Compute metrics for path P to D via S (see Fig 8)

        If destination D is not already in the routing table
        then Begin

          Add path P to the routing table, setting last
          update times for P and D to current time.

H         Trigger an update

          Set composite metric for D and P to new composite
          metric computed in step B.

          End

        Else begin (dest. D is already in routing table)
```

```
K         Compare the new composite metric for P with best
          existing metric for D.

           New > old:

L            If D is shown as unreachable in the update,
             or holddowns are enabled and
              the new composite metric >
                (the existing metric for D) * V
                [use 1.1 instead of V if V = 1,
                as it is as of Cisco release 8.2]
O            or holddowns are disabled and
             P has a new hop count > old hop count
             then Begin

              Remove P from routing table if present

              If P was the last route to D
                then Unless holddowns are disabled
                    Set holddown time for D to
                     current time + holddown time
T                  and Trigger an update

              End

             else Begin

              Compute new best composite metric for D

              Put the new metric information into the
              entry for P in the routing table

              Add path P to the routing table if it
              was not present.

              Set last update times for P and D to
              current time.

              End

           New <= OLD:

V            Set composite metric for D and P to new
             composite metric computed in step B.

             If any other paths to D are now outside the
             variance, remove them.

             Put the new metric information into the
             entry for P in the routing table

             Set last update times for P and D to
             current time.

          End

        End of for

      End of for
```

그림 6 — 주기적 처리

```
Process is activated by regular clock, e.g. once per second
```

```
    For each path P in the routing table (except directly
    connected interfaces)

      If current time < P'S LAST UPDATE TIME + INVALID TIME
        THEN CONTINUE WITH THE NEXT PATH P

      Remove P from routing table

      If P was the last route to D
        then Set metric for D to inaccessible
          Unless holddowns are disabled,
            Start holddown timer for D and
          Trigger an update

        else Recompute the best metric for D

      End of for

    For each destination D in the routing table

      If D's metric is inaccessible
        then Begin

        Clear all paths to D

        If current time >= D's last update time + flush time
          then Remove entry for D

        End

      End of for

    For each network interface I attached to the gateway

R     Recompute channel occupancy and error rate

S     If channel occupancy or error rate has changed,
        then recompute metrics

      End of for

    At intervals of broadcast time

U     Trigger update
```

그림 7 — 업데이트 생성

```
Process is caused by "trigger update"

    For each network interface I attached to the gateway

      Create empty update message

      For each type of service S supported

        Use path/destination data for S

        For each destination D

E         If any paths to D have a next hop reached through I
            then continue with the next destination
```

```
          If any paths to D with minimal composite metric are
          already in the update message
            then continue with the next destination

G         Create an entry for D in the update message, using
          metric information from a path with minimal
          composite metric (see Fig. 8)

          End of for

        End of for

J     If there are any entries in the update message
       then send it out interface I

      End of for
```

그림 8 — 메트릭 계산 세부 정보

이 섹션에서는 도착 라우팅 업데이트에서 메트릭 및 홉을 계산하는 절차에 대해 설명합니다.이 함수에 대한 입력은 라우팅 업데이트 패킷의 특정 대상에 대한 항목입니다.출력은 복합 메트릭을 계산하는 데 사용할 수 있는 메트릭의 벡터이며 hop count입니다.이 경로가 라우팅 테이블에 추가된 경우 측정 단위의 전체 벡터가 테이블에 입력됩니다.다음 정의에 사용되는 인터페이스 매개변수는 인터페이스를 통해 측정된 트래픽의 이동 평균을 기준으로 하는 점을 제외하고 라우팅 업데이트가 도착한 인터페이스에 대해 게이트웨이를 초기화할 때 설정된 매개변수입니다.

- 지연 = 패킷 + 인터페이스 토폴로지 지연으로부터의 지연
- 대역폭 = 최대(패킷의 대역폭, 인터페이스 대역폭)
- 안정성 = 최소(패킷의 신뢰성, 인터페이스 안정성)
- 채널 점유 = 최대(패킷에서 채널 점유, 인터페이스 채널 점유)대역폭 메트릭은 역형 형식으로 저장되므로 대역폭에 최대값이 사용됩니다.개념적으로, 최소 대역폭을 원합니다.) 인터페이스 채널 점유 변경 시 유효 채널 점유 수를 재계산해야 하므로 패킷의 원래 채널 점유 공간을 저장해야 합니다.

다음은 메트릭 벡터의 일부가 아니라 경로 특성으로 라우팅 테이블에 유지됩니다.

- Hop count = 패킷의 hop count.
- MTU = min(패킷의 MTU, 인터페이스 MTU).
- 원격 복합 메트릭 = 패킷의 메트릭 값을 사용하여 수식 1에서 계산됩니다.즉, 메트릭 구성 요소는 패킷의 구성 요소이며 위에 표시된 대로 업데이트되지 않습니다.분명히 이 값은 위에 표시된 조정을 수행하기 전에 계산되어야 합니다.
- 복합 측정 단위 = 이 섹션에 설명된 대로 계산된 측정 단위 값을 사용하여 수식 1에서 계산됩니다.

이 섹션의 나머지 부분에서는 라우팅 업데이트를 전송하기 위한 메트릭 및 hop 수를 계산하는 절차에 대해 설명합니다.

이 함수는 발신 업데이트 패킷에 넣을 메트릭 정보 및 hop 수를 결정합니다.사용 가능한 경로가 있는 경우 대상에 대한 특정 경로를 기반으로 합니다.경로가 없거나 경로가 모두 업스트림이면 대상을 "액세스할 수 없음"이라고 합니다.

```
If destination is inaccessible, this is indicated by using a specific
        value in the delay field. This value is chosen to be larger
        than the largest valid delay. For the IP implementation this is
        all ones in a 24-bit field.

   If destination is directly reachable through one of the interfaces, use
```

```
        the delay, bandwidth, reliability, and channel occupancy of the
        interface. Set hop count to 0.

   Otherwise, use the vector of metrics associated with the path in the
        routing table. Add one to the hop count from the path in the
        routing table.
```

IP 구현 세부 정보

이 섹션에서는 Cisco IGRP에서 사용하는 패킷 형식에 대해 설명합니다.IGRP는 IP IGP(Protocol 9)가 있는 IP 데이터그램을 사용하여 전송됩니다. 패킷은 헤더로 시작합니다.IP 헤더 바로 다음에 시작됩니다.

```
unsigned version: 4;  /* protocol version number */
    unsigned opcode: 4;   /* opcode */
    uchar edition;        /* edition number */
    ushort asystem;       /* autonomous system number */
    ushort ninterior;     /* number of subnets in local net */
    ushort nsystem;       /* number of networks in AS */
    ushort nexterior;     /* number of networks outside AS */
    ushort checksum;      /* checksum of IGRP header and data */
```

업데이트 메시지의 경우 헤더 바로 뒤에 라우팅 정보가 옵니다.

버전 번호는 현재 1입니다. 다른 버전 번호가 있는 패킷은 무시됩니다.

opcode는 1 = update 또는 2 = request일 수 있습니다.

메시지 유형을 나타냅니다.두 메시지 유형의 형식은 아래에 제공됩니다.

*버전*은 라우팅 테이블이 변경될 때마다 증가하는 일련 번호입니다.(이는 위의 의사 코드가 라우팅 업데이트를 트리거한다고 말하는 조건에서 수행됩니다.) 버전 번호를 사용하면 게이트웨이가 이미 확인한 정보가 포함된 업데이트를 처리하지 않아도 됩니다.(현재 구현되지 않았습니다.즉, 에디션 번호가 올바르게 생성되지만 입력에서는 무시됩니다.패킷이 삭제될 수 있으므로 버전 번호만으로 중복 처리를 방지할 수 있는지 명확하지 않습니다.에디션과 연결된 모든 패킷이 처리되었는지 확인해야 합니다.)

*시스템*은 자동 시스템 번호입니다.Cisco 구현에서 게이트웨이는 둘 이상의 자동 시스템에 참여할 수 있습니다.각 시스템은 자체 IGRP 프로토콜을 실행합니다.개념적으로 각 자율 시스템에 대해 완전히 별도의 라우팅 테이블이 있습니다.하나의 자율 시스템에서 IGRP를 통해 도착하는 경로는 해당 AS에 대한 업데이트에서만 전송됩니다.이 필드를 사용하면 게이트웨이가 이 메시지를 처리하는 데 사용할 라우팅 테이블 집합을 선택할 수 있습니다.게이트웨이가 구성되지 않은 AS에 대해 IGRP 메시지를 수신하면 무시됩니다.실제로, Cisco 구현에서는 한 AS에서 다른 AS로 정보를 "유출"할 수 있습니다.그러나 나는 그것을 프로토콜의 일부가 아니라 관리 도구라고 생각한다.

내부, *시스템* 및 외부는 업데이트 메시지의 3개 섹션 각각에 있는 항목 수를 나타냅니다.이러한 섹션은 위에서 설명한 것입니다.섹션 간에는 다른 경계가 없습니다.첫 번째 내부 항목은 내부, 다음 시스템 항목은 시스템으로, 최종 외관은 외관으로 사용됩니다.

체크섬은 UDP 체크섬과 동일한 체크섬 알고리즘을 사용하여 계산된 IP 체크섬입니다.체크섬은 IGRP 헤더와 그 뒤에 오는 모든 라우팅 정보를 기준으로 계산됩니다.체크섬을 계산할 때 체크섬 필드는 0으로 설정됩니다.체크섬에는 IP 헤더가 포함되지 않으며 UDP 및 TCP에서와 같이 가상 헤더가 없습니다.

요청

IGRP 요청이 수신자에게 라우팅 테이블을 전송하도록 요청합니다.요청 메시지에 헤더만 있습니다.버전, opcode 및 시스템 필드만 사용됩니다.다른 모든 필드는 0입니다.수신자는 일반 IGRP 업데이트 메시지를 요청자에게 보내야 합니다.

업데이트

IGRP 업데이트 메시지에는 헤더가 포함되어 있으며, 그 뒤에 라우팅 엔트리가 바로 옵니다.1500바이트 데이터그램(IP 헤더 포함)에 들어갈 만큼 많은 라우팅 엔트리가 포함됩니다. 현재 구조 선언을 사용하면 최대 104개의 엔트리를 사용할 수 있습니다.더 많은 항목이 필요한 경우 여러 업데이트 메시지가 전송됩니다.업데이트 메시지는 입력만으로 처리되므로 여러 개별 메시지 대신 단편화된 단일 메시지를 사용할 수 없습니다.

다음은 공정순서 항목의 구조입니다.

```
uchar number[3];       /* 3 significant octets of IP address */
    uchar delay[3];        /* delay, in tens of microseconds */
    uchar bandwidth[3];    /* bandwidth, in units of 1 Kbit/sec */
    uchar mtu[2];          /* MTU, in octets */
    uchar reliability;     /* percent packets successfully tx/rx */
    uchar load;            /* percent of channel occupied */
    uchar hopcount;        /* hop count */
```

uchar[2] 및 uchar[3]에 정의된 필드는 일반 IP 네트워크 순서에서 16비트 및 24비트 이진 정수입니다.

숫자는 설명되는 대상을 정의합니다.IP 주소입니다.공간을 절약하려면 내부 섹션을 제외하고 IP 주소의 처음 3바이트만 제공됩니다.내부 섹션에서 마지막 3바이트가 제공됩니다.시스템 및 외부 경로의 경우 서브넷이 없으므로 하위 바이트 값은 항상 0입니다.내부 경로는 항상 알려진 네트워크의 서브넷이므로 해당 네트워크 번호의 첫 번째 바이트가 제공됩니다.

지연은 10 마이크로초 단위로 이루어집니다.10마이크로초 ~ 168초 범위, 충분해 보입니다.모든 네트워크의 지연은 네트워크에 연결할 수 없음을 나타냅니다.

대역폭은 1.0e10의 배율로 확장되는 초당 비트 단위의 역대역폭입니다. 범위는 1200BPS 회선에서 10Gbps까지입니다.(즉, 대역폭이 N Kbps인 경우 사용된 번호는 10000000/N입니다.)

MTU는 바이트 단위입니다.

신뢰성은 255의 극히 일부일 뿐입니다. 즉, 255는 100%입니다.

로드는 255의 비율로 지정됩니다.

hop count는 간단한 카운트입니다.

대역폭과 지연에 다소 이상한 유닛이 사용되기 때문에 일부 예제가 순서대로 나타납니다.여러 공통 미디어에 사용되는 기본값입니다.

	Delay	Bandwidth
Satellite	200,000 (2 sec)	20 (500 Mbit)
Ethernet	100 (1 ms)	1,000
1.544 Mbit	2000 (20 ms)	6,476
64 Kbit	2000	156,250
56 Kbit	2000	178,571

```
      10 Kbit            2000             1,000,000
      1 Kbit             2000            10,000,000
```

메트릭 계산

다음은 Cisco 버전 8.0(3)에서 실제로 복합 메트릭을 계산하는 방법에 대한 설명입니다.

```
metric = [K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] *
                         [K5/(reliability + K4)]

    If K5 == 0, the reliability term is not included.

    The default version of IGRP has K1 == K3 == 1, K2 == K4 == K5 == 0
```

관련 정보

- IP 라우팅 지원 페이지
- IGRP 지원 페이지
- Technical Support - Cisco Systems