主題

차세대 인터넷 라우팅 프로토콜 기술

숭실대학교 신 용 태

차 례

Ⅰ. 서 론

차세대 인터넷이란 현재의 인터넷 및 관련 기술이 지닌 문제점을 해결하고, 다양한 어플리케이션의 트래픽 특성을 수용하는 고속의 고도화된 인터넷이라고 정의할 수 있다. 즉, 효과적인 네트워킹 기술을 통해 사용자의 요구사항을 만족시키면서 신뢰성 및 보안성, 이동성 등을 지원하는 발전된 형태의 인터넷이다. 이러한 차세대 인터넷을 위한 기반기술은 크게 네트워크 기술과 응용 및 서비스 기술분야로 구분할 수 있다. 특히, 응용 및 서비스를 위한 인프라구조를 구성하는 네트워크 기술은 무엇보다 중요하며, 최근 선진 각국에서는 이에 대한 기술개발에 박차를 가하고 있다.

본 고에서는 이러한 네트워크 기술의 핵심을 이루는 차세대 인터넷 라우팅 프로토콜과 관련된 기술과 연구 및 표준화 동향을 소개한다. 특히, IETF (Internet Engineering Task Force)의 작업그룹을 중심으로 차세대 인터넷을 위한 라우팅 프로토콜 기술 및 표준화 현황을 살펴본다. 차세대 라우팅과 관련된 최근의 연구들은 고속 및 대규모의 유·무선 네트워크 환경에 기반하며, 이러한 환경에서의 QoS의 보장과 멀티캐스트, 이동성, 보안의 지원을 중심으로 연구되고 있다.

Ⅱ. 유니캐스트 라우팅 프로토콜

1. RIPng for IPv6

가. 개요 및 현황

RIP(Routing Information Protocol)는 제록스사의 XNS(Xerox Network System)에서 사용하기 위한 라우팅 프로토콜로 개발되었으며, 프로토콜의 단순성과 견고성으로 인해 빠르게 보급되어 표준 라우팅 프로토콜로서 받아들여졌다[1]. 그러나, RIP는 라우팅 테이블 전체를 30초마다 전송하므로 네트워크 대역폭의 효율적인 사용을 제한하는

단점을 가지고 있어, 홉(hop) 수가 15 이상인 대규모 네트워크에는 적합하지 못하다.

이러한 RIP의 단점들은 보완하기 위해 RIPv2가 개발되었으며, IPv6을 위한 RIPng는 이러한 RIPv2의 구조를 받아들이고 있다. RIPng는 IPv4의 RIP와 매우 유사하지만, authentication entry 대신에 IPv6의 보안 기능을 사용하였으며, 긴 IPv6 주소를 전달하기 위해서 패킷 형식이 일부 수정되었다.

나. IPv6의 보안 사용

IPv6의 보안은 RIPv2에서 제공하는 것보다 우수하며, IPv6의 인증 헤더는 RIP 인증 시스템에서 제공하지 못하는 데이터와 IP 주소를 모두 보호한다. 이에 RIP의 표준화 작업을 위한 워킹그룹은 RIPng에 인증구조를 포함하지 않기로 결정하였다. 따라서, 인증 엔트리(authenticate entry)와 경로 엔트리(route entry)를 구별할 필요가 없어졌으며, "address family identifier"를 제거하는 것이 가능하게 되어 프로토콜이 단순화되었다.

다. 포맷의 변화

RIPng는 32bit command 헤더 이후에 20-byte 경로 엔트리가 뒤따른다. command 코드, version number는 RIPv2와 동일하다.

command(1)	version(1)	must be zero(2)
Routing entry 1 (20bytes)		
...		
Routing entry N (20bytes)		

그림 1. 헤더 포맷

경로 엔트리의 포맷은 16 octet의 IPv6 주소를 고려하기 위해, 그림 2와 같이 변경되었다.

IPv6 address (16bytes)		
route tag (2)	prefix len (1)	metric (1)

그림 2. 경로 엔트리 포맷

IPv6의 주소와 prefix length의 조합은 광고된 라우터를 식별한다. route tag는 일반적으로 autonomous system을 통하여 라우팅될 패킷을 식별한다. metric은 단지 0과 16사이에서 다양하게 값을 가질 수 있으므로, 1 byte로 표현된다.

RIPng entry는 Address Family Identifier, subnet mask, Next Hop fields를 포함하고 있지 않다. RIPng 패킷은 단지 한 종류의 경로 엔트리만을 전달하므로 AFI는 사실상 필요성이 없고, subnet mask는 prefix length 필드에 의해서 표현된다. 그러나, next-hop정보는 여전히 필요하지만, 각 메시지마다 16-byte의 next-hop 주소를 포함하여 전달하는 것은 너무 낭비가 많기 때문에 RIPng 워킹그룹에서는 next-hop 정보를 경로 엔트리와 분리하였다.

Next hop IPv6 address (16bytes)	
must be zero (3)	metric = 0xFF

그림 3. Next-Hop 엔트리 포맷

next-hop 엔트리는 0xFF(또는 255)로 설정된 특정한 metric 값에 의해 유효한 범위의 metric 값을 갖는지 구분된다.

next-hop 정보는 적당한 경로 엔트리의 앞에 위치한다. 다음의 그림 4를 살펴보면, 처음 두 entry는 광고 라우터를 통해 라우팅 되므로 next-hop 정보가 앞에 놓이지 않고, entry 3과 4는 라우터 "a"를 통해서 라우팅 되고, entry 5는 라우터 "b"를 통해서 라우팅 된다.

Command
Routing entry (1)
Routing entry (2)
Next Hop (a)
Routing entry (3)
Routing entry (4)
Next Hop (b)
Routing entry (5)

그림 4. Next-hop 엔트리의 예

2. OSPF for IPv6

가. 개요 및 현황

1980년대 중반, RIP가 더 이상 대규모의 이질적인 망 사이의 라우팅을 수행하기에는 한계에 이르자, IETF에서는 SPF(Shortest Path First) 알고리즘에 기반한 IP 네트워크용 라우팅 알고리즘을 개발하게 되었다. 이의 결과로 OSPF(Open Shortest Path First)가 탄생하게 되었다[2].

OSPF는 링크상태(Link State) 라우팅 알고리즘으로서 라우터간에 변경된 최소한의 부분만을 교환하므로 네트워크 대역폭의 효율을 저하시키지 않으며, 라우터의 계위를 설정함으로써 확장성과 대규모 망에 적용할 수 있는 성질을 가지고 있다. RIP와 같이 특정 도메인 안에서 적용할 수 있는 인트라-도메인(Intra-domain) 라우팅 프로토콜로서 RIP가 가지고 있는 여러 단점을 해결하고 있으나, 그 프로토콜 자체가 복잡하다는 단점도 역시 가지고 있다[3].

현재, 인터넷을 비롯하여 대부분의 대규모 IP 망의 경우, OSPF의 적용은 일반화되고 있으며 기존의 RIP망을 OSPF로 바꾸는 작업도 활발하다. 이더넷 스위치의 보급으로 상대적으로 라우터의 중요성 및 역할이 많이 줄어들고 있는 상황이지만, 외부와 연결하기 위해서는 여전히 라우터가 필요하고, OSPF는 도메인 내부 라우팅 프로토콜로서 다른 어떤 라우팅 프로토콜보다도 주도적 역할을 수행할 것으로 예상된다.

나. IPv4와의 차이점[4]

OSPF를 구성하는 대부분의 알고리즘은 IPv4와 달라진 점이 없다. 그러나, IPv4와 IPv6의 프로토콜의 의미상의 차이와 길어진 어드레스 크기를 조정하기 위해 단순화된 몇 가지 측면 때문에 약간의 차이가 있다. 이러한 차이를 간략하게 기술하면 다음과 같다.

- IPv4에서는 per-IP-subnet로 동작하던 것이 IPv6에서는 per-IP-link로 동작한다.
- IPv6상의 OSPF에서는 프로토콜 패킷과 메인 LSAs타입에서 주소에 대한 의미가 없어졌다.
- LSAs상의 플로딩스코프가 일반화되어졌고 LSA의 LS타입필드에 명백하게 코드화되어졌다.
- 하나의 링크에 여러 개의 프로토콜 인스턴스를 지원해준다.
- 하나의 싱글링크상에서 인접한 네트워크와 라우터를 발견하거나 자동설정 기능 등을 지원하기 위하여 IPv6 링크-로컬 주소가 사용되어진다.
- 인증에 관련된 부분이 자체 내에서는 모두 제거되었다. 오토타입과 인증필드가 OSPF의 패킷 헤더에서 없어졌고, 인증에 관계된 모든 필드와 인터페이스 구조도 모두 없어졌다.
- OSPF의 패킷 헤더 상에서의 주소에 대한 의미들이 모두 사라졌다. 이는 곧 네트워크 프로토콜에 대한 독립을 뜻하는데, 그 대신 모든 주소에 대한 정보는 다양화된 LSA 타입들에만 저장되어 있다.
- 라우터 LSAs로부터 네트워크 LSAs까지 LSA헤더로부터 주소에 대한 정보도 사라졌다. 이 두 개의 LSAs들은 현재 네트워크 프로토콜 독립을 위하여 라우팅도메인의 위상을 서술한

다. 그러나 새로운 LSAs는 IPv6의 주소 분산과 다음 홉을 경로 지정을 할 수 있는 데이터가 추가되어졌다.

- IPv4의 OSPF에서는 스텁영역이 링크상태에 대한 데이터베이스나 라우팅 테이블의 크기를 줄이기 위하여 디자인되어 사용되었다. 이러한 스텁영역은 IPv6에서도 개념적으로 그대로 유지되어 사용되어지고 있다.
- 주어진 링크 상에서의 OSPF라우터는 라우터 ID를 가지고 이웃된 라우터를 구분한다.

다. 현 황

현재 이와 같은 내용을 골자로 하는 RFC 문서가 1999년 2월에 draft로부터 승격되어졌다. 그 이 이러한 내용을 골자로 하여 국외의 G6(프랑스), DENet(덴마크), Virginia Tech 6Bone(미국), TICL(영국), JOIN(독일) 등이 IPv6 시험 구축을 통해 테스트 중에 있다.

3. BGP for IPv6

가. 개요 및 현황

BGP는 IETF의 인터도메인 라우팅(Inter-Domain Routing) 워킹그룹에서 표준화 작업을 수행하고 있는 차세대 인터넷 라우팅 프로토콜 중 하나이다. BGP는 기본적으로 AS간의 경로 배정 즉, 외부 게이트웨이 프로토콜(EGP, Exterior Gateway Protocol)로써 현재 가장 많이 사용되고 있으며, 유니캐스트를 포함한 멀티캐스트를 지원하고 있으며, 라우팅 정책을 다른 프로토콜에 비해 효율적으로 수립할 수 있도록 고안된 프로토콜이다.

AS 도메인간의 라우팅 프로토콜로서 인터넷에서 초기에는 EGP가 사용되었다. 그러나 인터넷이 확장될수록 라우팅 순환이 생기는 등의 심각한 문제들이 발생하여 이를 해결하기 위해 BGP가 등장하게 되었으며, 현재에는 EGP가 BGP, BGP-4 혹은 IDRP(Inter-Domain Routing Protocol)로 대체되고 있는 상황이다.

BGP는 AS간의 라우팅 정보를 신뢰성 있게 전송할 수 있는 외부 게이트웨이 프로토콜로 개발되었다. 최근의 BGP-4는 AS간에 라우팅 정보가 네트워크 내에서 무한히 돌아다니는 무한 루프 현상이 발생하는 것을 막고, CIDR(Classless Inter-Domain Routing)를 이용하여, 라우팅 정보를 최소화할 수 있는 기능을 지원하고 있다[5].

BGP와 관련된 표준화 현황을 보면, 현재 약 30개의 표준 문서가 발표되어 있으며, 대표적인 문서에는 다음과 같은 문서들이 있다.

- RFC Multiprotocol Extensions for BGP-4 (RFC 2858)
- BGP-4 Protocol Analysis (RFC 1774)
- Experience with the BGP-4 Protocol (RFC 1773)
- A Border Gateway Protocol 4 (BGP-4) (RFC 1771)
- Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (RFC 2545)

나. BGP-4의 동작 방식

서로 다른 AS (관리 도메인) 속한 BGP 라우터가 통신하기 위해서는 다른 망의 중계 없이 하나의 망으로 직접 연결되어 있어야 하며, 한 AS내에 복수 개의 BGP 라우터가 있는 경우, BGP 라우터들은 그 AS에 대한 일관된 정보와 AS 외부 통로로서의 역할을 수행하기 위해 서로를 인식하고 정보를 교환해야 한다[6]. 일반적으로 하나 이상의 BGP 라우터가 존재할 경우, 여러 개의 AS를 연결해 주는 BGP 라우터를 AS 보더 라우터(ASBR) 혹은 보더 라우터(Border Router)라고 한다.

BGP는 RIP와 같은 거리값(distance vector)에 기본한 라우팅 알고리즘이나, 목적지까지의 경로

값을 전송하는 것이 아니고, 목적지까지 도달하는데 경유하는 AS의 순서를 전송하므로, 거리값 알고리즘이 가지고 있는 무한 경로값(counting to infinity)의 단점을 가지고 있지 않다.

더불어, 경로 결정시 RIP는 하나의 매트릭스로 결정하는 반면에, BGP-4는 다수개의 다양한 매트릭스를 활용하여 결정하게 되며, 여러 개의 매트릭스에는 적당한 우선 순위가 부여되어 있다. 또한, 최종 목적지까지 통하는 여러 개의 경로가 존재할 경우, 이 모든 정보를 관리만 할 뿐 실제로는 우선 순위 값이 가장 높은 오직 한 개의 경로만을 다른 BGP 라우터에게 전달하게 된다.

BGP를 동작시키는 라우터는 TCP 포트 179를 이용하여 서로 통신하도록 되어 있다. 즉, TCP를 기반으로 동작하기 때문에 신뢰성 있는 라우팅 정보의 전달이 가능하며, 모든 라우팅 정보가 전달과 더불어 에러 경고 메시지까지 전달하고 연결 종료를 하게 된다.

BGP 프로토콜은 일반적으로 다음과 같이 4 가지 과정을 반복적으로 수행한다.

1) TCP를 이용하여 이웃 BGP 라우터들과 연결을 만든다.
2) 초기, 라우팅 정보 테이블을 전달하고, BGP 경로를 지속적으로 관리한다.
3) 만약, 변경된 라우팅 정보가 있다면, 전체 테이블을 보내지 않고, 변경된 부분만을 재전송한다.
4) 에러가 발생하게 되면, 경고 메시지를 보내고 해결한다.

다. 확장된 BGP-4

BGP-4는 기본적으로 IPv4에서만 적절하게 동작하도록 제안된 프로토콜이다. 다시 말해서, BGP가 동작하는 라우터의 IP 주소 버전이 4 라는 뜻으로 해석될 수 있다. 확장된 BGP-4는 IPv4 뿐만 아니라, 최근에 각광 받고 있는 여러 가지 차세대 인터넷 네트워크 프로토콜인 IPv6나 IPX와 같은 다양한 프로토콜에서도 동작할 수 있도록 기존의 BGP를 확장한 것이다[7][8].

RFC 2858과 RFC 2545는 이러한 기능을 지원하기 위한 IETF의 표준 문서이다. 본 문서에서는 BGP 라우터들간에 공유되는 정보에서 다음 홉에 대한 정보가 있는데, 이 정보를 IPv4 뿐만 아니라 다양한 여러 특정 네트워크 프로토콜에 맞게끔 보완되었으며, 몇 가지 새로운 옵션 속성이 추가되었다. 이러한 정보들은 원칙적으로 다른 여러 네트워크 프로토콜들이 독자적으로 사용될 수 있도록 하거나, 혹은 IPv4와 연동하여 사용될 수 있도록 지원하기 위해서 수정된 사항들이다.

Ⅲ. 멀티캐스트 라우팅 프로토콜

다자간 전송을 위한 멀티캐스트는 크게 인트라 도메인과 인터 도메인 라우팅 프로토콜로 나누어질 수 있다. 지금까지 현저한 연구가 되어온 멀티캐스트 라우팅 프로토콜은 인터 도메인 라우팅 프로토콜로써, 그 대표적인 것이 DVMRP, MOSPF, PIM, CBT 등이 있다. 그러나 이러한 프로토콜들을 글로벌한 인터넷에 적용하기 위해서는 확장성의 문제에 봉착하게 된다. 이에 멀티캐스트 라우팅의 확장성을 위한 인터 도메인 라우팅 프로토콜로써, MSDP (Muticast Source Discovery Protocol)과 Multiprotocol BGP(Border Gateway Protocol)가 각 WG에서 활발히 연구되어 지고 있다. PIM(Protocol Independent Multicast) 또한 차세대 인터넷이라 불리는 IPv6환경에서 지원을 위한 개발이 진행되고 있다. 이에 각각에 대한 세부 사항은 다음과 같다.

1. PIM for IPv6

PIM은 IETF IDMR 워킹그룹에서 개발되어진 프로토콜이며 기초를 이루는 유니캐스트 라우팅 프로토콜 즉 DVMRP 등에 독립적인 멀티 캐스트 프로토콜로서 PIM-DM과 PIM-SM가 있다. PIM-DM은 그룹의 멤버가 조밀하게 분포되어있는 DVMRP나 MOSPF와 같은 사항에 적합하도록 설계되었으며, PIM-SM는 멀티캐스트 지역에 멤버가 희박한 환경에 적합하도록 설계되었다. 그러나 이들은 IPv4의 환경에 기반을 한 것이며, 차세대 인터넷이라는 IPv6에 적합한 PIM for IPv6이 워킹그룹에서 IPv6환경 하에서 효율적이며, 강건한 멀티캐스트 라우팅 프로토콜로 자리 맥임을 하기 위한 연구가 진행 중이다.

IPv6환경 하에서 PIM의 명확한 그룹 통신에 있어 효율적인 라우팅에 대하여 설명하고 있다[9]. 기존의 IPv4 환경 하에서 PIM과 다른 점은 PIM 헤더에 존재하는 체크섬 필드의 변화이다. 이로 인해 모든 메시지는 영향을 받게 된다. 이러한 체크섬은 16 비트의 값을 가지며, 1의 보수로 패킷의 모든 정보에 대해 체크한다. 다음은 PIM for IPv6에 사용되는 메시지에 관한 사항이다.

- Hello Message : Hello 메시지를 전송시, PIM 라우터는 IPv6 헤더상의 IPv6 주소의 다른 집합을 이용한다.
- Register & Register-Stop Messages : RP의 IPv6주소에 도달가능성에 대해 사용한다.
- Join/Prune, Graft, and Graft-Ack Messages : 이러한 메시지를 전송 시 라우터는 IPv6 주소 형태의 목적지 주소를 All-PIM-Routers 멀티캐스트 주소가 되게 한다.
- Bootstrap Message : 이 메시지를 전송 시, PIM 라우터는 IPv6 목적지 주소 필드를 All-PIM-Routers 멀티캐스트 주소가 되게 한다.
- Assert Message : 이 메시지는 All-PIM-Routers 멀티 캐스트 주소의 IPv6 목적지 주소와 메시지를 포워딩 하는 인터페이스의 링크의 로컬의 IPv6 소스 주소를 가진다.
- Candidate-RP-Advertisement Message : 이 메시지는 IPv6 목적지 주소로써 BSR의 IPv6 주소에 대한 도메인 범위의 도달성에 이용된다.

2. MSDP(Multicast Source Discovery Protocol)

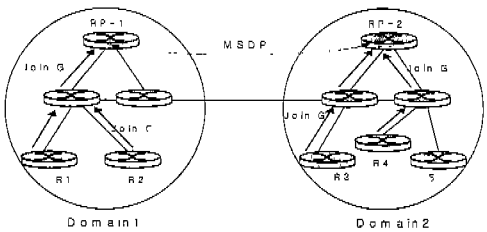
가. 개요 및 현황

PIM-SM에서 멀티캐스트 그룹을 RP에 접속시키기 위한 확장된 메커니즘을 디자인하는데 있어 문제점은 서로 각기 다른 ISP에 의해 서비스되는 도메인간은 서로 상호 의존성이 없다는 것이다[10]. 이에 MSDP는 한 개 이상의 PIM-SM 도메인을 연결해 주는 메커니즘으로서, 각 PIM-SM 도메인들은 자신의 고유한 RP(Rendezvous Point)를 사용하며, 다른 도메인의 RP와 독립적으로 동작한다[11]. MSDP는 인터넷에서 인터 도메인간의 멀티캐스트를 지원하기 위한 단기적인 해결 방법이라 할 수 있으며, MSDP는 도메인 내, 외부 라우팅을 구분하여 다자간 전송을 지원하는 프로토콜로서, 최근 IETF의 MSDP WG에서 활발히 연구가 진행되고 있다.

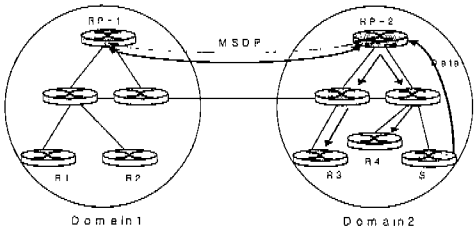
MSDP는 다음과 같은 특성을 가지고 있다.

1) 장 점

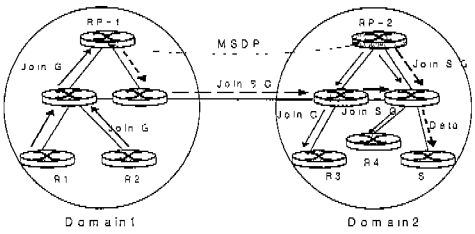
- PIM-SM 도메인은 자신의 RP만 고려하면 됨
- 송신자가 없는 즉 수신자만 존재하는 도메인에서는, 전체적인 그룹의 멤버십 정보를 교환하지 않아도 데이터를 수신할 수 있다.
- 전체적인 소스 상태 관리가 요구되지 않는다.



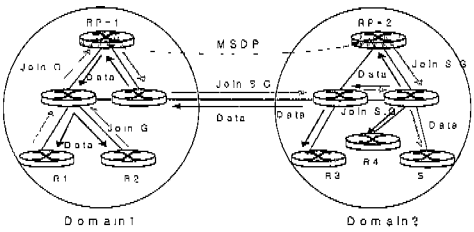
(A) 수신자들은 자신의 도메인 RP에 가입한다



(B) 소스 S가 전송하는 데이터는 RP-2를 통해 지역 라우터 들 에게 전달되며 . RP-2 는 다른 RP에게 Source Active 메시지를 전송한다.



(C) RP-2 는 S에게 source-specific join 메시지를 보낸다.



(D) S에서 그룹으로 전송하는 패킷은 R1, R2에게 도달한다.

그림 5. MSDP의 동작

2) 단 점

- 모든 도메인의 모든 RP가 그룹에 데이터를 전송하고자 하면 모든 소스에 대한 정보를 다른 도메인상의 RP에게 알려야 한다.
- MSDP는 만약 많은 멀티캐스트 그룹과 소스들이 존재하는 글로벌한 환경 하에서는 네트워크의 부하 및 RP들 자체의 부하 등을 야기시켜 확장성의 문제를 가진다.

나. 동작 원리

MSDP의 동작에 관한 간단한 사항은 그림 5와 같다. 도메인 1에서, R1과 R2는 그룹 G에 대한 가입 메시지를 RP-1에게 전송하며, 이와 비슷하게 R3, R4 가입 메시지를 RP-2로 전송한다. 그룹의 소스인 S가 전송을 시작하면, PIM-SM의 방법과 같이 소스의 로컬 라우터에서 RP-2로 패킷을 캡슐화해서 전송한다. RP-2는 이를 디캡슐화 하여, 도메인 2의 R3, R4에 도달할 수 있도록 group-shared tree상에서 전송한다. 게다가 Source Active 메시지를 MSDP상의 모든 RP에게 전송한다. RP-1과 같이 이 그룹에 대해 가입자를 가지고 있는 RP들은 소스에 대한 source-specific 가입을 할 수 있다.

3. BGMP(Border Gateway Multicast Protocol)

가. 개요 및 현황

도메인 내부와 외부의 구분된 라우팅 프로토콜을 지원하는 BGMP는 최근 IETF의 IDMR(Inter Domain Multicast Routing) 워킹그룹에서 독립하여 연구되어지고 있으며, 멀티캐스트 패킷 전송을 위한 외부 라우팅 프로토콜로서 도메인들간의 양방향 공유 트리를 사용하고 있다[12]. 즉 BGMP는 멀티캐스트 그룹에 대한 트리 상태 테이블을 생성, 유지하고 이를 기반으로 멀티캐스트 패킷을 포워딩

한다.

BGMP는 TCP 기반의 프로토콜로서 연결 설정에 있어 포트 번호 264를 사용하며, 각각의 BGMP 피어는 TCP 연결을 구성, 설정 및 연결 파라미터 확인을 위한 메시지들을 교환한다. 연결이 이루어진 직후 그룹 멤버십 수정을 위한 가입, 탈퇴, 업데이트 메시지를 상호간 교환하며, KeepAlive 메시지는 연결을 확인하기 위해 주기적으로 전송된다.

Notification 메시지는 오류 등의 응답을 위해 전송되며, 연결 상에 오류가 발생하면, Notification 메시지가 전송되고, 연결은 끊어진다.

BGMP와 기존의 공유 트리 기반의 프로토콜의 차이점은 다음과 같다.

- 양방향 트리를 제공한다.
- 특정 소스 중심의 트리를 제공할 수 있다.
- 그룹 공유 트리의 루트를 결정함에 있어, 성능 측면에서 특정한 정책을 제공한다.

나. BGMP 프로토콜 개요 및 동작과정

BGMP는 BGMP 피어와 인트라 도메인 라우팅 프로토콜인 DVMRP, MOSPF, PIM으로부터 notification의 결과를 모아, Group-prefix 상태를 유지한다. 수신자들이 특정 그룹 주소에 가입하고자 할 때, 경계 라우터는 루트 도메인을 향하여 그룹-기반 가입 메시지를 전송하고 이는 경계 라우터들을 통해 포워드 된다. 이러한 BGMP의 가입 및 탈퇴 메시지는 BGMP 피어간의 TCP 연결을 통해 이루어지며, KEEPALIVE 메시지에 의해 refresh된다. 그림 6의 예를 보면, Transit_1 도메인에서 Src_A로부터 온 데이터는 BR12에 도착한다. 그러나, BR11에 의해 주입되어야 한다. 대리자 라우터는 공유 트리 상태가 존재하지 않으면, 소스 기반의 BGMP 브랜치를 생성할 수도 있다. 그림에서 단일 경계 라우터를 가지는 Revr_Stub_7 같은 stub 도메인들은 모든 멀티캐스트 데이터 패킷을 그 라우터를 통해 받는다. 따라서 stub 도메인

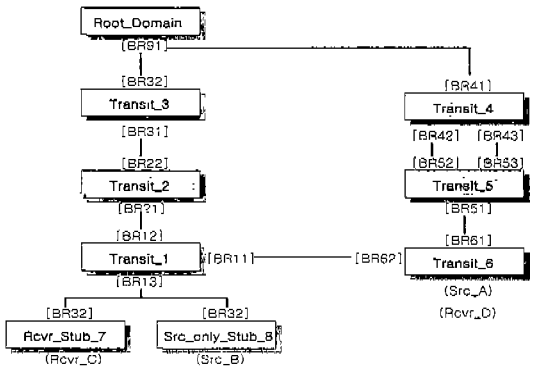


그림 6. 인터도메인 토폴로지의 예

들은 절대 소스 기반의 상태를 만들지 않는다.

그룹이나 특정 소스 기반의 그룹 가입 및 탈퇴 메시지의 송, 수신을 통해 그룹 공유 트리를 생성 및 유지한다. 하나의 도메인 안에서는 기존의 멀티캐스트 내부 라우팅 프로토콜이 운영되며, 서로 다른 도메인간에는 BGMP 라우터를 통해 패킷을 전송한다. 멀티캐스트 내부 라우팅 프로토콜들은 서로 다른 특성을 가지므로 BGMP와 완벽하게 연동한다는 것은 불가능하다.

BGMP 라우터는 TCP 연결을 이루는데 서로간에 BGMP 메시지를 처리할 때, 그룹-기반 양방향 전송 상태를 구성한다. 양방향 전송 상태는 어는 타켓(EGP 피어)으로부터 받은 패킷이라도 모든 RPF 체크없이 타켓 목록에 있는 다른 모든 타켓으로 전송이 가능하다는 것을 의미한다. 또한 BGMP 라우터는 필요에 따라, DVMRP, PIM과 호환 가능한 소스-기반 단방향 전송 상태를 구성할 수도 있다.

Ⅳ. 이동 인터넷 라우팅 프로토콜

1. Mobile IP for IPv4

가. 배 경

초기에는 모든 컴퓨터의 위치가 고정되어 있다는 가정 하에 네트웍을 만들었으나 이제 많은 컴퓨터들이 고정되지 않은 상태로 네트웍에 접속되어 있다. 즉, 컴퓨터, 호스트들이 움직이는 경우가 많아지고 있다. 특히 모든 컴퓨터가 항상 통신을 할 수 있는 상태를 유지하여야 하므로 컴퓨터 통신 기술에서 이를 지원하여야만 하게 되었다. 현재의 IP 프로토콜에서는 호스트가 인터넷을 사용하기 위해서는 접속되는 위치가 반드시 고정적으로 지정되어 있어야 했다. 이러한 현재의 IP에서 단말기의 이동성을 제공하기 위하여 Mobile IP 워킹그룹이 IETF에서 1992년 여름에 결성되었으며 최근 모빌 IP를 제안하였다[16].

나. Mobile IP의 필요성

IP 라우팅은 목적지 호스트의 IP 주소, 특히 network-prefix에 의존한다는 것을 배웠다. 따라서 어떤 호스트가 접속된 물리적인 위치가 달라져서 network-prefix가 바뀐다면 이 호스트와 관련된 모든 라우팅 정보는 근본적으로 바뀔 수밖에 없다. 왜냐하면 기존의 라우팅 정보들을 잘못 된 것이므로 이 호스트로 전달될 패킷들이 제대로 전달될 수 없기 때문이다. (호스트가 다른 곳으로 이동되어 연결이 안되므로 Host Unreachabable 오류가 발생한다) 위와 같은 문제를 혹시 host-specific 루트를 사용하면 해결되지 않을까? 앞에서 설명한 바와 같이 host-specific 루트가 존재하면 이것이 우선적으로 라우팅에 사용된다.

다. host-specific 라우팅 방식

그러면 인터넷에서 이동성을 제공하기 위하여 host-specific 라우팅을 사용하는 것이 타당한 해결책일까? 먼저 인터넷에서 이동노드의 수가 어느 규모가 될 지를 예측해 보아야 할 것이다. 현재의 노트북 보급 속도로 볼 때 수년 내에 수백만 대의 이동노드가 생길 것으로 예상되고 있다. 또한 각 이동노드에 대하여 home 링크로부터 foreign 링크 사이에 있는 모든 라우터들은 그 노드에 대하여 home-specific 루트를 제공하고 있어야 한다. 더욱이 이동노드가 네트웍에 접속되는 지점을 바꾸면 즉, foreign 링크를 바꾸면 이에 따라 중간에 있던 라우터들이 변경되므로 이 변경된 라우터에 대하여 home-specific 루트들이 새로 갱신되어야 한다. 결론적으로 위의 host-specific 라우팅 방법은 인터넷에서 일반적인 이동성 제공을 위한 해결책으로 사용되기에 곤란하다.

라. IP 주소 변경 방식

그러면 노드가 foreign 링크를 바꿀 때마다 매번 이동노드의 주소를 새로 옮긴 링크의 network-prefix에 맞추어 바꾸어 주는 방법은 어떠한가? 이 방법은 TCP 연결 시간동안 계속 필요로 하는 IP 주소가 바뀌게 되므로 통신을 계속 유지하는 것을 보장하지 못한다. 즉, 이동노드는 통신을 그대로 유지할 수 없게 된다. 즉, 이 방법은 노드의 nomadicity만 제공한다고 할 수 있다. 노드의 nomadicity란 현재 진행중인 통신을 종료하고 노드가 다른 곳으로 이동한 후에 통신을 다시 시작할 수 있는 환경을 말한다. 더욱이 nomadicity 만으로 불충분한 경우로 다음과 같은 예를 들 수 있다. 많은 응용 프로그램들이 지정된 IP 주소를 사용하고 있으므로 이것을 수시로 바꾸면 서비스가 안 되는 경우가 있다. 클라이언트뿐 아니라 서버 자신도 이동노드가 될 수 있으며 이때에는 이와 관련된 클라이언트들의 프로그램이 실행이 안 될 수가 있다. 이동노드가 접속되는 foreign 링크에서 새로 배정할 IP 주소가 없을 수도 있다. 따라서 이동노드가 이동

할 때마다 IP 주소를 매번 변경하여 nomadicity가 가능한 경우라도 Mobile IP의 기능을 사용하는 것이 안정적인 것을 알 수 있다.

마. 터널링

터널(tunnel)이란 IP 패킷이 다른 IP 패킷에 실려 전달될 수 있는 환경(전송채널)을 말한다. HA가 FA로 패킷을 전달할 때 터널을 사용할 수 있다. 이동노드는 현재 다른 링크에 접속되어 있더라도, 원칙적으로 home address를 사용하여 통신을 한다. 즉, 자신이 보내는 패킷의 송신지 주소와 자신이 받을 IP 패킷의 목적지 주소는 바로 home address가 된다. Tunneling의 방법으로는 두 가지가 가능하다. 첫 번째 방법은 HA가 FA로 패킷을 보내고 FA가 MN에게 패킷을 전달하는 방법이고 두 번째는 HA가 MN에게 직접 패킷을 전달하는 방법이다. 첫 번째 방법에서는 FA Care-of address를 사용하고 두 번째 방법에서는 co-located care-of address를 사용한다.

바. Mobile IP의 동작

1) HA와 FA는 주기적으로 자신이 어느 링크에 접속되어 있는지를 광고로 알린다. 이 때 Agent Advertisement 라는 Mobile IP 메시지를 사용한다.

2) 이동노드는 이 Agent Advertisement 메시지를 받아보고 자신이 home 링크에 있는지 어떤 foreign 링크에 있는지를 판단한다. 자신이 home 링크에 있으면 일반 IP 프로토콜로 동작하며 foreign 링크에 있는 경우만 아래의 순서로 Mobile IP를 실행한다.

3) foreign 링크에 있는 이동노드는 먼저 COA를 얻어야 한다. FA COA를 얻는 경우는 단순히 FA가 보낸 Agent Advertisement 메시지 내에서 FA COA를 읽어 사용하면 되나 collocated COA를 얻는 경우는 Dynamic Host Configuration 프로토콜 또는 PPP IP Control 프로토콜을 통하여 COA를 배정받거나 수동으로 배정해야 한다.

4) 이동노드는 위에서 얻은 COA를 자신의 HA에 등록(Register)한다.

5) HA는 (또는 home 링크에 있는 다른 라우터는) 이동노드의 network-prefix에 대한 접근성(reachability)을 광고한다. 다음에 이 이동노드로 오는 패킷들을 HA가 받아서 COA로 터널링해 준다.

6) COA에서 (즉, FA 또는 이동노드 자체에서) 터널링되어 도착한 원래 패킷이 추출되어 이동노드에게 전달된다.

7) 반대방향으로의 패킷 전송시에는 터널링을 이용하지 않고 목적지로 바로 전송된다. 이 때 FA가 이동노드의 라우터의 역할을 한다.

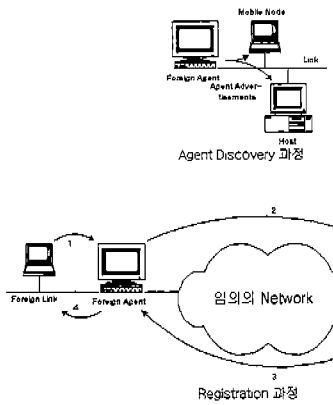


그림 7. Agent Discovery/Registration

Mobile IP의 동작은 다음과 같이 세 가지로 나누어진다.

1) Agent Discovery - MN이 다른 서브네트웍으로 이동하였을 때 자신이 어떤 서브네트웍에 속하여 있는지를 알아내는 동작을 말한다.

2) Registration - 이동노드는 네트웍에 접속되는 위치가 달라지면 등록절차를 거쳐야 한다. 즉,

이동노드가 FA에게 서비스를 요청하고 HA에게는 자신의 COA를 알려주는 것 또한 등록은 일정한 시간동안만 유효하므로 이동노드가 다른 곳으로 이동하지 않았어도 일정시간(lifetime)이 지나면 등록을 하여야 한다.

3) FA를 통하여 패킷이 전달되는 과정

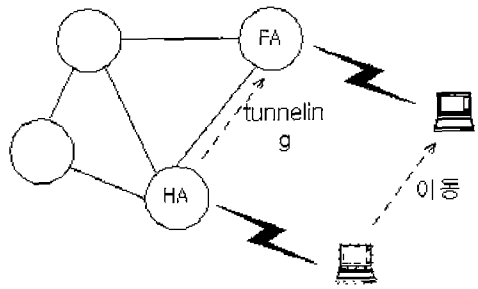


그림 8. Mobile IP의 터널링

2. Mobile IP for IPv6

가. 개 요

인터넷에 접속되고 있는 컴퓨터의 수가 급속히 증가하고 있으며 이미 현재 사용중인 IPv4의 32비트 주소체계는 IP 주소 할당이 원활히 이루어지지 못하고 있다. 따라서 IP 주소 크기를 확대할 필요성이 절실하며 이것이 IPng 또는 IPv6을 만들어진 첫 번째 동기라 할 수 있다. IPv6에서는 128비트(16바이트) 주소 체계를 사용한다. IPv6이 필요하게 된 두 번째 배경은 네트워크의 수가 증가함에 따라서 네트워크의 Exterior gateway에 요구되는 라우팅 테이블의 크기가 급속히 증가하기 때문이다. IPv6에서는 게이트웨이에 필요한 라우팅 테이블의 크기를 줄일 수 있도록 하였다. 세 번째 배경은 멀티캐스팅의 제공, 호스트의 이동성 제공 및 향상된 네트워크의 보안성을 향상시키기 위해서이다. IPv6 데이터그램은 IPv4보다 많은 기능을 제공하기 때문에 더 큰 헤더를 가지고 있다. 따라서 헤더의 처리를 빠르게 하기 위해서 IPv6의 헤더를 Basic Header와 Extension Header의 두 부분으로 나누고 기본적으로는 Basic Header만 처리하며 추가기능을 처리할 때만 Extension Header를 사용한다.

나. 확장헤더(Extension Header)

- Hop-by-hop header : 송수신지 사이에 있는 모든 게이트웨이들이 확인해야할 정보를 실어 보내는데 사용한다.
- End-to-end header : 목적지 게이트웨이에만 확인할 정보를 포함한다.
- Routing header : 소스에 라우팅을 사용할 때 이용하며 목적지까지 가는데 거쳐야 모든 게이트웨이의 주소를 포함한다. 이 정보에 따라 Basic header 내의 목적지 주소는 데이터그램이 게이트웨이를 지날 때마다 바뀌게 된다.
- Fragment header : 서브 네트웍이 지원하는 최대 메시지의 길이보다 큰 메시지를 전송할 때 사용한다.
- Authentication header : 데이터그램의 송신지 확인용으로 사용한다.
- Privacy header : 인터넷상에서 데이터 보안을 유지할 때 사용하는데 암호화된 데이터는 이 헤더의 데이터 부분에 실려서 전송된다.

3. Cellular IP

가. 개 요

최근 인터넷에 이동성과 3세대 Cellular 시스템에 패킷 데이터를 서비스하는 것은 이동 사용자들에게 IP데이터의 전송을 위한 가능한 참여자들에게 이동성 서비스 제공자들이 생겨남으로써 고려되어 왔다. 그러나 이 두 가지 모두 많은 단점을 가지고 있다. 이동IP는 간단하고 확장성 있는 글로벌 이동성 솔루션에 적합하나, 빠르고 끊김 없는 핸드오프제어에는 맞지 않다. 반대로, 부드러운 이동성을 제공하

는 3세대 Cellular 시스템은 유연성에 약하고 복잡한 네트워크 하부를 만든다.

Cellular IP는 부드럽고 빠른 핸드오프와 active user의 효과적인 위치관리와 유연성을 갖는 idle user의 위치관리를 제공한다. 또한, IP네트워크에서 발견된 강력함과 확장성을 소유한다. 인터넷을 위한 고속의 패킷 무선 액세스의 발달은 이동 텔레커뮤니케이션 산업에 많은 영향을 줄 것이다. 저렴함, 많은, 그리고 신뢰성 있는 무선 인터넷 액세스는 무선 인터넷 서비스 제공자로부터 나타나는 이동 텔레커뮤니케이션에서 발견된 전통적인 서비스 기반으로 이동할 것이다. 이것은 현존하고 차세대 Cellular와 IP 네트워크로 옮겨지는 동안 요구되는 중요한 결과물일 것이다.

Cellular IP는 빠른 이동성 무선의 호스트를 지원함에 있어서 이동성 IP가 가능한 인터넷에 대해서 액세스를 제공하기 위한 최적화 된 새로운 이동성 호스트를 재 표현한다. Cellular IP는 많은 중요한 Cellular원리로 구성되어 있다.

나. 프로토콜 개요

다음으로 우리는 Cellular IP 특징과 알고리즘을 설명한다. 즉 Cellular IP 라우팅, 핸드오프, 페이징 알고리즘을 설명한다.

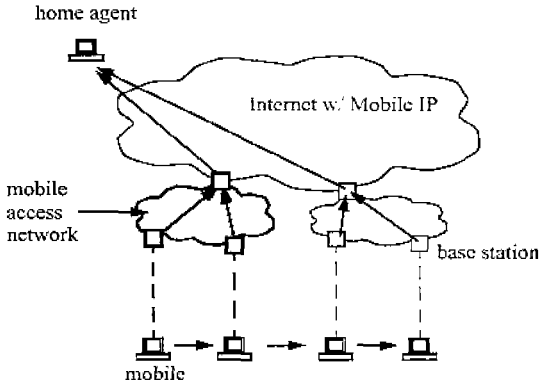


그림 8. Cellular IP

그림 8은 Cellular IP의 개략적인 그림을 보여주고 있다. 크게는 Internet(Mobile IP)를 사용하지만 지역적인 이동(Mobile Access Network)에서 계층적인 셀을 사용한 Cellular IP를 구현한다. Cellular IP는 이동성 관리, 수동적인 연결, 핸드오프 제어를 위해서 Cellular 시스템 원리를 사용한다. 그러나 IP 파라다임에 기초를 두어 설계되었다. Cellular IP네트워크의 전체적인 콤포넌트는 무선의 액세스 포인트로써 서비스를 하는 Base station이 있다. 그러나 IP 패킷 라우팅 할 때와 Cellular 제어 기능을 통합 할 때는 MSC(Mobile Switching Center)와 BSC (Base Station Controller)에 의하여 동작이 된다. Base station은 규칙적인 IP전달 엔진으로 만들어진다. 그러나 IP 라우팅은 Cellular IP라우팅과 위치관리에 의해서 대체된다. Cellular IP네트워크는 게이트웨이 라우터를 거쳐 인터넷에 연결된다. 게이트웨이 사이의 이동(Cellular IP 액세스 네트워크)은 이동IP에 의해서 관리된다. 반면에 액세스 네트워크 안에서 이동성은 Cellular IP에 의해서 다뤄진다. 네트워크에게 붙는 이동호스트들은 이동 IP COA로서 게이트웨이의 IP주소를 사용한다. Mobile IP와 Cellular IP와의 연결을 위해서 Cellular IP Gateway가 사용된다. Base Station은 주기적으로 beacon 신호를 보낸다. 이동 호스트는 그 beacon 신호를 사용해서 가장 근접한 base station에게 자신의 위치를 말하게 된다. 이동 호스트는 이런 방법을 연속적으로 사용해서 Cellular IP Gateway가 정보를 전달하게 된다.

4. MANET(Mobile Ad-hoc NETwork)

가. 개요 및 현황

최근 컴퓨터와 무선 통신 기술의 성능 향상에 따라 진보된 이동 무선 컴퓨팅은 급격히 그 응용 범위

와 사용빈도가 증가할 것으로 기대되고, 기존의 인터넷 프로토콜들의 사용을 대부분 포함할 것이다. MANET의 목표는 이동 노드에 라우팅 기능을 통합함으로써 이동 무선 네트워크 상에서의 견고하고 효율적인 동작을 지원하는 것이다.

MANET을 구성하는 각 노드들은 자유롭고 빠른 이동에 따른 위상의 변화와 무선 링크에서 대역폭 사용이 상대적으로 제한되므로 다중 홉 토폴로지들을 가지도록 요구되어진다. 이동 호스트들의 라우팅 지원은 Mobile IP 기술에서 일반화 되어가고 있다. 이 기술은 이동호스트에 로밍을 지원하며, 로밍 호스트는 잘 알려진 고정된 주소를 갖는 도메인 영역과는 다른 인터넷에 다양한 방법을 통해 연결될 것이다. 호스트는 무선링크나 dial-up line등을 통해 연결되거나 직접 외부 서브넷 상의 고정된 네트워크에 물리적으로 연결될 것이다.

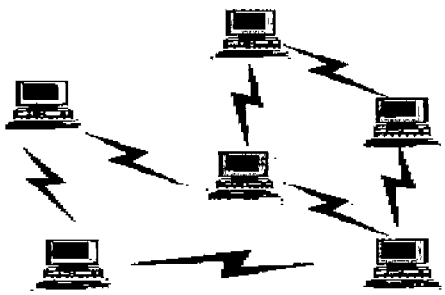


그림 9. MANET 토폴로지의 예

이러한 형태의 호스트의 이동성을 지원하는 것은 주소관리와 프로토콜의 상호운영성의 증대가 필요하지만, 홉-대-홉 라우팅과 같이 라우팅의 핵심이 되는 네트워크 기능들은 이미 사용되고 있는 고정된 네트워크 안에서 동작하는 라우팅 프로토콜에 의존한다.

이와는 다르게 MANET의 목표는 이동 노드에 라우팅 기능을 통합함으로써 이동 무선 네트워크의 이동성을 자치적으로 이동할 수 있는 무선 영역으로 확대하는 것이다. 그리고 각각의 노드들은 스스로가 독특한 형태의 네트워크 라우팅 구조를 갖는다.

다. MANET의 특징

MANET은 이동 플랫폼들로 되어 있고 MANET을 구성하는 각 노드들은 자유 자재로 이동하는데 따른 제약 사항이 없는 것으로 간단하게 언급했다. 노드들은 비행기, 배, 트럭, 차들의 안에 위치해있거나 어쩌면 사람 위에나 매우 작은 장치들, 그리고 라우터당 많은 호스트들이 있을 것이다. MANET은 이동 노드들의 자치적인 시스템이다. 이 시스템은 분리된 상태 안에서 동작하거나 고정된 네트워크에 접속할 수 있는 게이트웨이를 갖는다. 후자에서 작동되는 모드에서는 고정된 인터네트워크에 연결되는 stub 네트워크에서의 작동을 위하여 대체로 계획된다. Stub 네트워크들은 안에 있는 노드들에게는 신호를 전달하지만 stub 네트워크를 통해 지나가는 외부 신호는 전달하지 않는다. MANET 노드들은 전방향성이고, 지향성이며, 조정 가능하거나 약간 그것에 대하여 복합된 안테나를 사용한 무선 발신기들과 수신기들을 갖추고 있다. 이 시점에서의 중점적인 것은 발신기와 수신기의 패턴 범위, 전송 전력 레벨, co-channel 방해 레벨, 임의적인 형태의 무선 접속, 다중 홉 그래프나 노드들 사이에 존재하는 ad hoc 네트워크는 노드들의 위치에 의존한다. Ad hoc 토폴로지는 노드가 움직이거나 전송과 수신범위를 조정하는 시간에 따라 바뀔 것이다.

라. 표준 IP 라우팅의 상호작용

가까운 기간에 일반적으로 계획된 MANET은 stub와 같은 기능일 것이고, 모든 신호가 MANET 노드들에 의해 운반된다는 의미는 MANET안에서 sinked 되거나 sourced 될 것이다. 대역폭과 아마 전력의 한계 때문에 MANET에 들어가고 나가는 움직이는 신호는 네트워크에서 운반과 같은 기능은 곧 계획되지 않는다. (비록 이 제한은 다음의 기

술의 진보에 의해 제거될 것이다.) 라우트 광고의 양을 실질상 줄어든 것은 존재한 고정된 인터넷과 상호 동작을 요구했다. Stub 동작을 위해 가까운 기간에 라우팅 상호운용은 MANET에 근거한 anycast와 이동 IP같은 메커니즘들의 몇몇 조합에 의해 이루어 질 것이다. 미래의 상호운용은 mobile IP와 다른 메커니즘 사용이 이루어질 것이다. 표준 IP 라우팅의 상호작용은 모든 MANET 라우팅 프로토콜들에 접근하는 공통의 MANET addressing 사용에 의해 매우 쉽게 될 것이다. 이러한 접근의 개발은 다중 기술 조직을 통한 라우팅의 허가나 라우터당 다중 호스트들의 허가, 그리고 긴 기간의 상호운용을 IP 주소 구조의 지지를 통하여 확실하게 한다. 이 특징들의 지원은 요구하는 오직 IP 주소를 갖는 호스트와 라우터 인터페이스들을 확인하고, 분리된 라우터 ID와 라우터의 확인, 많은 유무선 접속장치를 갖는 라우터의 허락의 요구를 위하여 나타낸다.

V. 스위칭 프로토콜

1. MPLS

가. MPLS 개요

MPLS(Multi-Protocol Label Switching)란 Label Swapping 기능에 의하여 패킷을 전송하는 방식으로, 기존의 라우터가 담당하는 L3 기능을 분리하였다고 할 수 있다. 즉, Routing(L3) + Forwarding(L2, Switching 기능)으로 설명할 수 있는데, 이는 상·하위 계층 프로토콜에 무관하게 동작한다.

MPLS의 장점은 근본적으로 간단하다는 것과 빠른 포워딩을 지원한다는 것이다. 이에 따라, 부수적으로 높은 성능을 낼 수 있고, 효율적인 을 할 수 있고, 보다 싼 비용이 예상된다는 것 등이다.

MPLS 기술은 차세대 인터넷 서비스를 위한 핵심기술로서 국내에서는 슈퍼 NSP 서비스, 슈퍼 ISP 서비스라는 명칭으로 인터넷 백본서비스 및 인터넷 프리미엄서비스를 위해 2004년까지 단계별로 확대 예정인 국책사업 중 하나다.

나. MPLS의 등장배경

현재의 라우터들은 프로세서 기반으로 패킷별로 포워딩하기 때문에 빠르지 못하여 효율적이지 못하다. 따라서, 인터넷에서 IP 트래픽의 증가와 QoS 보장을 필요로 하는 멀티미디어 서비스의 등장으로 인해 라우터의 패킷처리 능력향상과 QoS 보장을 위한 다양한 기법들이 개발되고 있고, ATM과 같은 고속 스위칭기술이 백본 노드에 도입되고 있다.

이에 IP 라우팅의 성능 및 확장성을 개선하기 위해 multi-layer 스위칭을 지원하기 위한 해결책이 MPLS이다.

다. MPLS 동작

네트워크의 입출력시에 라우팅을 처리해주는 Label에 의해 고속으로 포워딩을 해준다. MPLS에서는 Label을 사용하여 패킷전송을 제어하는데, Label은 짧은 고정길이의 패킷 식별자로서 MPLS 망내에서 인접한 두 노드사이에서만 유효하며 FEC(Forwarding Equivalence Class)에서 부여하며, 그 형식은 그림 10과 같다.

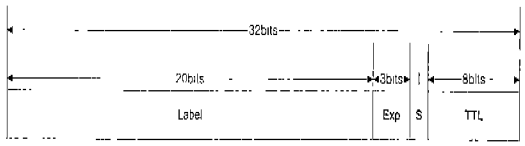


그림 10. 레이블 포맷

라. Label 할당과 분배

기존의 라우팅 프로토콜(OSPF, BGP 등)을 이용하여 라우팅 정보를 구성하여 FEC를 구성한다.

즉, 동일 경로를 따르는 패킷들의 집합들을 "stream"으로써 하나의 흐름을 만들어 놓음을 말하는데, 아래 그림에 따라, 여러 응용들에서의 flow들이 하나의 경로를 향한다면 하나의 Label을 할당하게 된다.

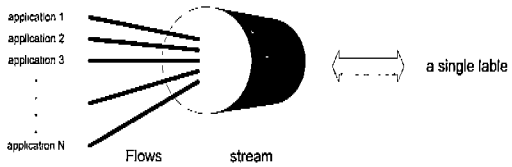


그림 11. 레이블의 할당

Label 할당은 3가지 방식이 있는데, 첫째로, Downstream방식은 downstream peer에서 레이블을 바인딩하여 분배하는 방식이고, 두 번째, Downstream On Demand방식은 Upstream peer의 요청에 의해서 downstream peer로부터 레이블을 분배하는 방식으로 Request Driven Label Assignment라고 하며, RSVP와 비슷한 방식이다. 마지막으로, Upstream방식은 Upstream peer에서 레이블을 바인딩하여 downstream peer로 piggyback하는 방식이다.

마. MPLS 구현기술

기존의 IP 라우터는 IP 패킷 포워딩 시 패킷의 재조립이 필요하고 패킷 단위로 다음 홉을 결정하므로 패킷의 재조립과 라우팅 테이블 참조로 인한 지연 때문에 패킷 처리 속도를 높이는데 제약 사항이 많았다. 이러한 단점을 없애기 위해 여러 회사에서 MPLS 기술을 규격화하고 제품화하였는데, 입실론의 IP 스위칭과 시스코의 Tag 스위칭 등이 그것이다.

바. IP 스위칭

입실론은 최초로 IP 계층 스위칭의 개념을 적용한 상용제품인 IP 스위치를 발표하였는데 ATM 하드웨어 위에 IP 라우팅 프로토콜을 구현하고, 흐름의 분류 기능과 흐름에 대한 입·출력 VPI/VCI의 매핑 정보를 ATM 하드웨어 내에 캐쉬할 수 있는 라우터다. 여기에서 흐름은 동일한 출발지/목적지 IP 주소를 갖는 IP 패킷 스트림 또는 IP 주소 외에 같은 TCP/UDP 포트 번호를 갖는 패킷 스트림으로 정의된다.

IP 패킷 라우팅 경로에 있는 인접 노드간 ATM 링크는 IP 계층에서 VC의 설정과 해제를 제어하는 비연결형 방식으로 이루어진다.

사. Tag 스위칭

시스코사가 발표한 이 기술은 IP 헤더 처리 과정 없이 ATM 계층에서 택(VPI/VCI)의 변환에 의해 고속의 스위칭을 실현하지만, IP 스위칭과는 지원되는 프로토콜과 스위칭되는 IP 패킷의 분류방법이 다르다.

즉, IP 스위칭에서는 특정 흐름에 대해 VPI/VCI를 바인딩하지만 Tag 스위칭에서는 IP 포워딩 테이블(FIB: Forwarding Information Base)의 엔트리에 Tag을 바인딩하여 모든 IP 트래픽을 Tag 변환에 의해 스위칭한다. 즉, 그림 12와 같이 동작을 한다.

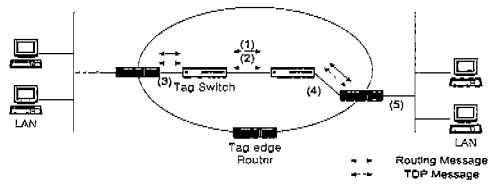


그림 12. Tag 스위칭

1) 라우팅 소프트웨어는 라우팅 정보 교환에 의해 FIB에 네트워크 루트와 출력포트로 구성되는 엔트리들을 만든다.

2) 제어요소는 상위 노드의 요청에 의해 네트워크 루트에 Tag을 할당하고, 하위 노드로부터 동일

한 네트워크 루트에 대한 Tag 바인딩 정보를 받으면 자신의 TIB내에 엔트리를 생성한다. 이러한 절차는 FIB의 모든 엔트리에 대해 반복한다.

3) 단말로부터 IP 패킷을 수신한 TER(Tag Edge Router)은 목적지 IP 주소를 참조하여 TIB로부터 Tag을 선택하고, 이를 VPI/VCI 필드에 매핑한 다음 인접 홉으로 포워딩한다.

4) TER로부터 셀을 수신한 Tag스위치는 VPI/VCI 필드를 참조하여 ATM 계층에서 직접 스위칭한다.

5) 인접 Tag스위치로부터 셀을 수신한 TER은 IP 패킷을 재조립한 후 목적지 단말로 전달한다.

이 외에도 도시바의 CSR(Cell Switch Router)와 IBM의 ARIS(Aggregate Route Based IP Switching)등이 MPLS를 구현한 기술들이다.

아. ATM기반 MPLS

MPLS기술은 기존의 라우터가 ATM네트웍에서 인터넷 트래픽을 라우팅하기 위해 탑재하여야하는 복잡한 ATM 프로토콜의 오버헤드로 인한 성능상의 한계, 확장성, QoS문제 등을 해결하는 기술로서, 기존 라우팅 프로토콜과 호환성을 유지하며 ATM스위치의 고속스위칭기술을 이용하는 효율적인 스위칭 기술이다.

또한, 이 기술은 ATM이 갖고있는 QoS 기능을 활용하여 서비스 품질을 차등화할 수 있으며 보다 쉽게 VPN(Virtual Private Network)을 지원할 수 있고 망 자원을 효율적으로 사용할 수 있는 트래픽 엔지니어링 기능을 지원한다.

즉, MPLS 기본개념이 ATM 셀 스위칭 방식과 유사함으로 이미 개발된 ATM 스위치 기술을 활용하여 MPLS 시스템을 개발한다. 이는 가입자 수용과 기존 서비스 연동이 유리하여 ATM 가입자를 포함하여 각종 Access Mux/Gateway 장비를 이용한 xDSL, FR, ISDN, PSTN 등 가입자 수용 및 기존 서비스 연동이 용이하고, ATM의 QoS 보장 기능을 통한 고품질의 서비스를 제공할 수 있다.

그러나, ATM MPLS 시스템을 개발하기 위해서는 몇 가지 고려사항이 있는데, Core LSR은 ATM Cell Switching에 의해서 전송해야 하며, Label Merging 지원이 어렵다. Label Merging 지원은 VP merging을 이용하거나 새로운 H/W를 개발하여 해결할 수밖에 없다.

자. 결 론

MPLS는 hop-by-hop 라우팅과 포워딩의 scalability를 향상시키는 유망한 기술로 더 나은 네트워크 전송 서비스를 제공하기 위한 traffic engineering을 제공한다. 또한, 라우팅에서 포워딩을 분리하여 기본 포워딩 파라다임에 대한 변화 없이 다중 프로토콜을 지원해 준다.

5.2. 광인터넷 기술

광인터넷이란 강력한 인터넷 서비스 제공을 위하여 IP와 광네트워킹 기술이 결합된 네트워크의 형태를 의미하는 것으로, IP 중심의 광채널 및 자원을 이용하여 IP와 광 계층에서의 라우팅과 시그널링 기능을 통합한 것을 말한다. 광네트워킹 기술은 대용량 트래픽 처리성, 경제성 및 단순성을 갖춘 미래의 인터넷 구성을 목표로 하고 있다.

가. 광인터넷의 특징

광인터넷의 특징은 4가지로 나눌 수 있는데, 첫째는, 고성능 라우터와 OXC/OADM 장치를 광채널을 통해 직접 연결한다는 것이고, 둘째는, 광 계층에서 cut-through 또는 bypass 연결기능을 제공한다는 것, 셋째는, SDH, Gigabit Ethernet SDL, Digital Wrapper 프레임을 사용한다는 것이고, 마지막으로 MPLS, ODSI 제어 프로토콜을 사용한다는 것이다.

나. 광인터넷의 장점

- 광 네트워킹 장비 적용으로 전체 망 구축비용을 절감하였다.
- 광인터넷 노드 구성에 의한 효율적인 상면 활용을 가능하게 하였다.

Ⅵ. 결 론

본고에서는 IETF의 관련 워킹그룹을 중심으로 차세대 인터넷 라우팅 프로토콜 기술 및 표준화 동향을 살펴보았다. 특히, 유니캐스트와 관련해서는 IPv6에 기반한 RIPng와 OSPF, BGP를 중심으로 살펴보았으며, 멀티캐스트와 관련해서는 IPv6에 기반한 PIM과 MSDP 및 BGMP를 살펴보았다. 또한, 이동성과 관련해서는 Mobile IP 및 Cellular IP와 MANET에 대해 기술하였다. 그 외에도 QoS의 보장과 스위칭 기술에 대해서도 간략히 살펴보았다.

즉, 최근의 라우팅 프로토콜은 QoS의 보장과 멀티캐스트, 이동성, 보안의 지원을 중심으로 진행되고 있다. 이러한 연구가 정착되면, 사용자는 시간과 공간에 제약받지 않고, 멀티미디어 등으로 대표되는 다양한 서비스를 편리하게 제공받을 수 있을 것으로 기대된다.

※참고문헌

[1] G. Malkin, R. Minnear, "RIPng for IPv6," RFC 2080, January 1997.

[2] C. Huitenma, "Routing in the Internet," Prentice Hall, 1999.

[3] J. Moy, "OSPF Version 2," RFC 2328, April 1998.

[4] R. Coltun, D. Ferguson, J. Moy, "OSPF for IPv6," RFC 2740, December 1999.

[5] Y. Rekhter, T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, March 1995.

[6] P. Traina, "BGP-4 Protocol Analysis," March 1995.

[7] P. Marques, F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing," RFC 2545, March 1999.

[8] T. Bates, Y. Rekhter, R. Chandra, D. Katz, "Multiprotocol Extensions for BGP-4," RFC 2858, June 2000.

[9] Haberman B. et al., "Protocol Independent Multicast Routing in the Internet Protocol Version 6 (IPv6)," IETF Internet Draft draft-ietf-msdp-pim-ipv6-03.txt, March 2000.

[10] Mark Handley, "Internet Multicast Today," The Internet Protocol Journal, Volume2, Number4, December 1999.

[11] Farinacci D. et al., "Multicast Source Discovery Protocol (MSDP)," IETF Internet Draft draft-ietf-msdp-spec-03.txt, January 2000.

[12] Thaler D. et al., "Border Gateway Multicast Protocol (BGMP)," IETF Internet Draft draft-ietf-bgmp-spec-01.txt, September 2000.

[13] Markus Hofmann, "Adding Scalability to Transport Level Multicast," Proceeding of Third IEEE Workshop on HPCS," Auguest 1995.

[14] Rajendra Yavatkar, James Griffioen, and Madhu Sudan, "A Reliable Dissemination Protocol for Interactive Collaborative Applications," ACM Multimedia 95, 1995.

[15] Markus Hofmann, "Enabling Group Communication in Global Networks," Proceeding of Global Networking '97, Calgary, Alberta, Canada, June 1997.

[16] C. Perkins et al., "IP Mobility Support," IETF RFC 2002, October 1996.

[17] D. Mills, "Network Time Protocol (Version 3): Specification, Implementation and Analysis," IETF RFC 1305, March 1992.

[18] R. Atkinson, "IP Authentication Header," IETF RFC 1826, August 1995.

[19] P. Metzger and W. Simpson, "IP Authentication using Keyed MD5," IETF RFC 1828, August 1995.

[20] A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, and A. Valko, C-Y Wan, "Cellular IP Performance," <draft-gomez-cellularip-performance-00>, October 1999.

[21] Andersson et al, "Label Distribution Protocol Specification" work in progress(draft-ietf-mpls-ldp-08), June 2000.

[22] Callon et al, "Framework for Multiprotocol Label Switching", work in progress (draft-ietf-mpls-framework-05), September 1999.

[23] Rosen et al, "Multiprotocol Label Switching Architecture", work in progress (draft-ietf-mpls-arch-06), August 1999.

[24] Awduche et al, "Requirements for Traffic Engineering Over MPLS", RFC 2702, September 1999.

[25] B. Gleeson, et. al., "A Framework for IP Based Virtual Private Networks", RFC 2764, ebruaryF 2000.

[26] B. Jamoussi, et. al., "Applicability Statement for CR-LDP," work in progress, (draft-ietf-mpls-crldp-applic-01), June 2000.

신 용 태

1985년 한양대학교 산업공학 학사
1990년 Univ. of Iowa, 전산학 석사
1994년 Univ. of Iowa 전산학 박사
1994년 미시간주립대학교 강의교수
1995년~현재 숭실대학교 컴퓨터학부 조교수
관심분야: 인터넷 라우팅, 멀티캐스팅, 이동라우팅, 그룹통신, 실시간통신