

가상 인터페이스 기반 2계층 스위칭 및 3계층 라우팅 동시 제공 시스템 설계

윤현식, 송광석
한국전자통신연구원 광통신연구센터
e-mail : x7hyhs@etri.re.kr

Design of a System for Simultaneously Offering Layer 2 Switching and Layer 3 Routing Based on a Virtual Interface

Hyeon-Sik Yoon, Kwang-Seok Song
Optical Communications Research Center, ETRI

요 약

인터넷상의 망 장비는 크게 2계층 스위치와 3계층 라우터로 구분할 수 있으며, 2계층 스위치는 IEEE 802.1D, IEEE 802.1Q 규격에 따라 수신된 이더넷(Ethernet) 프레임의 목적지 MAC 주소에 기반한 2계층 스위칭 기능을 제공하며, 3계층 라우터는 IETF의 규격에 따라 수신된 이더넷 프레임의 목적지 IP 주소에 기반한 3계층 라우팅 기능을 제공한다. 하지만 최근에는 기술의 발달에 따라서 엄연히 구분된 두 가지 기능을 하나의 시스템에서 제공하는 것에 대한 요구가 증가하게 되었다. 이에 본 논문에서는 가상 랜(VLAN) 기반의 2계층 스위치에서 가상 인터페이스 기반의 라우팅 기능을 구현한 후, 라우팅 기능을 원하는 가상 랜 가입자에게 해당 가상 랜을 가상 인터페이스(Virtual Interface)에 맵핑하는 것에 의해서 3계층 라우팅 기능을 제공하는 시스템 구조 및 제안된 시스템에서의 패킷 처리 절차를 제시하고자 한다. 본 논문에 제시된 방법에 의해서 가입자들은 저렴한 비용으로 인터넷 서비스를 제공받을 수 있으며, 망 사업자는 다른 가상 랜간의 통신을 위한 가상 랜 라우팅(VLAN Routing) 기능을 부가적으로 쉽게 제공할 수 있고, 해당 시스템의 인터페이스를 2계층 스위치 포트 또는 3계층 라우터 포트에 융통성있게 설정할 수 있다.

1. 서론

최근에 알려진 인터넷을 구성하는 이더넷 기반의 망 장비는 크게 2계층 스위칭 기능을 수행하는 스위치(Switch)와 3계층 라우팅 기능을 수행하는 라우터(Router)로 나누어진다.

이더넷 기반의 2계층 스위칭 기능은 IEEE 802.1D, IEEE 802.1Q 등의 규격을 따르고 있으며, 동작 절차를 간략히 설명하면 다음과 같다[1][2]. 가상 랜 기능을 가진 스위치 시스템에서 2계층 스위칭 기능은 학습 프로세스(Learning Process)에 의해서 입력 프레임의 포

워딩을 결정하기 위한 포워딩 테이블을 구축한다. 2계층 스위치의 포워딩 테이블은 일반적으로 MAC(Media Access Control) 주소, VLAN(Virtual LAN) ID, 출력 포트 등의 요소들로 구성된다. 포워딩 테이블이 구축된 후 입력되는 프레임에 대한 처리 절차는 입력 프레임의 목적지 MAC 주소를 파악한 후, 멀티캐스트 또는 브로드캐스트 MAC 주소를 가진 프레임의 경우에 입력 포트를 제외한 해당 VLAN 그룹의 모든 멤버 포트에 출력된다. 유니캐스트 MAC 주소를 가진 프레임의 경우는 해당 MAC 주소에 대한 엔트리가 포워딩 테이블에 있으면 해당 출력 포트에 전송되며, 없는 경우에는 입력 포트를 제외한 모든 포트에 전송(Flooding)된다.

이더넷 기반의 3 계층 라우팅 기능은 IETF 의 규격 들을 따르고 있으며, 동작 절차를 간략히 설명하면 다음과 같다. 라우터 시스템에서 3 계층 라우팅 기능은 라우팅 프로토콜을 이용한, 이웃한 라우터들과의 통신을 통해서 입력 패킷의 포워딩을 결정하기 위한 포워딩 테이블을 구축한다[3][4]. 3 계층 라우터의 포워딩 테이블은 일반적으로 IP 주소, Nexthop 주소, 출력 포트 등의 요소들로 구성된다. 포워딩 테이블이 구축된 후, 멀티캐스트 또는 브로드캐스트 IP 주소를 가진 패킷의 경우에 입력 포트를 제외한 모든 멤버 출력 포트에 전송된다. 반면에 유니캐스트 IP 주소를 가진 패킷은 해당 IP 주소에 대한 엔트리가 포워딩 테이블에 있으면 해당 출력 포트에 전송되며, 없는 경우에는 패기되거나 컨트롤러에서 예외 처리를 수행하게 된다.

이상에서와 같이 각 장비가 수행하는 기능에 따라서 인터넷을 구성하는 이더넷 기반의 망 장비는 각 각 스위치와 라우터로 나누어 지게 되었다. 하지만 최근 에 기술의 발달에 따라서 엄연히 구분된 두 가지 기능을 하나의 시스템에서 제공하는 것에 대한 요구가 증가하게 되었다. 특히 라우터에 비해 저렴한 비용으로 구축되며 상대적으로 쉬운 기능을 수행하는 스위치 장비에서 라우팅 기능을 수행하도록 함으로써, 사용자에게 인터넷 서비스를 제공하기 위해서 망 사업자가 스위치와 라우터 두 장비를 모두 구매하는 대신에 하나의 라우팅 기능을 수행하는 스위치 장비만을 구매하도록 함으로써 가격적인 측면에서 매우 큰 장점을 제공할 수 있다.

본 논문에서는 이와 같은 사용자 요구 사항을 만족 시키기 위해 가상 인터페이스 기반의 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템 설계 방안을 제시 한다. 이를 위해 먼저 2 장에서는 가상 인터페이스 기반 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템 구조를 제시하였다. 3 장에서는 제안된 시스템상에 이더넷 프레임이 도착한 경우에 패킷 처리 절차를 설명 하였다. 또한 4 장에서는 제안된 시스템상에서 Ping 프로그램의 실행을 통해서 동작을 분석하였다. 마지막으로 5 장에서 결론을 맺는다.

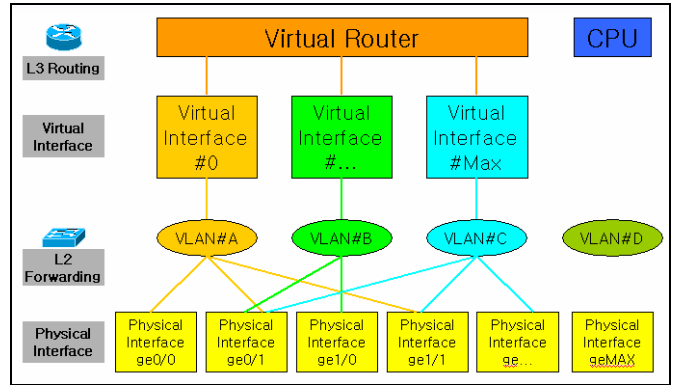
2. 시스템 구조

상기와 같은 사용자 요구 사항을 만족시키기 위해 서 본 논문에서는 그림 1 과 같은 가상 인터페이스 기 반의 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템 구조를 제시한다.

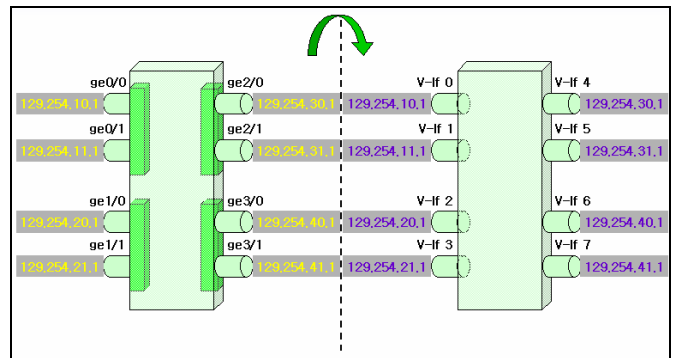
제시된 구조는 실제 시스템의 물리적인 인터페이스 와 해당 물리적인 인터페이스를 맴버로 하는 가상 랜 으로 구성되며, 가상 랜 기반의 2 계층 스위칭 기능을 제공한다. 그리고 3 계층 라우팅 기능을 제공하고자 하는 가상 랜에 대하여 가상 인터페이스 ID 와 가상 랜 ID 를 맴핑하는 것에 의해서 가상 인터페이스 기 반의 3 계층 라우팅 기능을 제공하게 된다.

가상 인터페이스 기반의 가상 라우터의 구조는 그림 2 와 같이 나타낼 수 있다. 일반적인 라우터는 물

리적인 인터페이스에 IP 서브넷(Subnet)을 할당한 후 이웃한 라우터 시스템과의 라우팅 프로토콜의 통신을 통해 3 계층 포워딩 테이블을 구축하는 반면, 가상 인터페이스 기반의 3 계층 라우팅 기능은 가상 인터페이스에 IP 서브넷을 할당한 후, 이웃한 라우터 시스템과의 라우팅 프로토콜의 통신을 통해 가상 인터페이스 기반의 3 계층 포워딩 테이블을 구축하는 것이다.



(그림 1) 가상 인터페이스 기반의 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템 구조



(그림 2) 가상 인터페이스 기반의 가상 라우터 구조

여기서 가상 인터페이스의 생성은 특정 가상 인터 페이스 ID 에 IP 서브넷과 해당 가상 인터페이스의 MAC 주소를 할당하는 것에 의해서 수행된다. 가상 인터페이스와 가상 랜과의 관계는 일대일 맴핑을 원칙으로 하며, 가상 랜이 여러 개의 물리적인 인터페이스를 맴버로 할 수 있으므로 하나의 가상 인터페이스는 여러 개의 물리적인 인터페이스에 맴핑될 수 있다.

3. 제안된 시스템에서의 패킷 처리 절차

상기 제시된 가상 인터페이스 기반 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템에 이더넷 프레임이 도착했을 때, 패킷 처리 절차는 그림 3 과 같은 순서도로 나타낼 수 있다.

그림 3 에 도시된 바와 같이, 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템에 이더넷 프레임이 수신

되었을 때, 수신된 이더넷 프레임의 가상 랜 그룹을 결정한 후 해당 가상 랜의 VLAN ID 가 운용자의 설정에 의해서 가상 인터페이스 ID 와 맵핑되었는지를 판단한다.

만일 판단 결과 해당 가상 랜의 VLAN ID 가 가상 인터페이스와 맵핑되어 있지 않다면, 가상 랜 기반 2 계층 스위치와 동일한 처리 절차를 수행하면 된다. 즉, 이더넷 프레임의 목적지 MAC 주소가 멀티캐스트(Multicast) 또는 브로드캐스트(Broadcast) MAC 주소라면 입력 포트를 제외한 해당 가상 랜(VLAN)의 모든 멤버 포트로 전송하고, 유니캐스트(Unicast) MAC 주소라면 2 계층 포워딩 테이블을 검색한 후 해당 엔트리가 존재하면 출력 포트로 전송하고, 존재하지 않으면 입력 포트를 제외한 해당 가상 랜의 모든 멤버 포트로 전송(Flooding)한다.

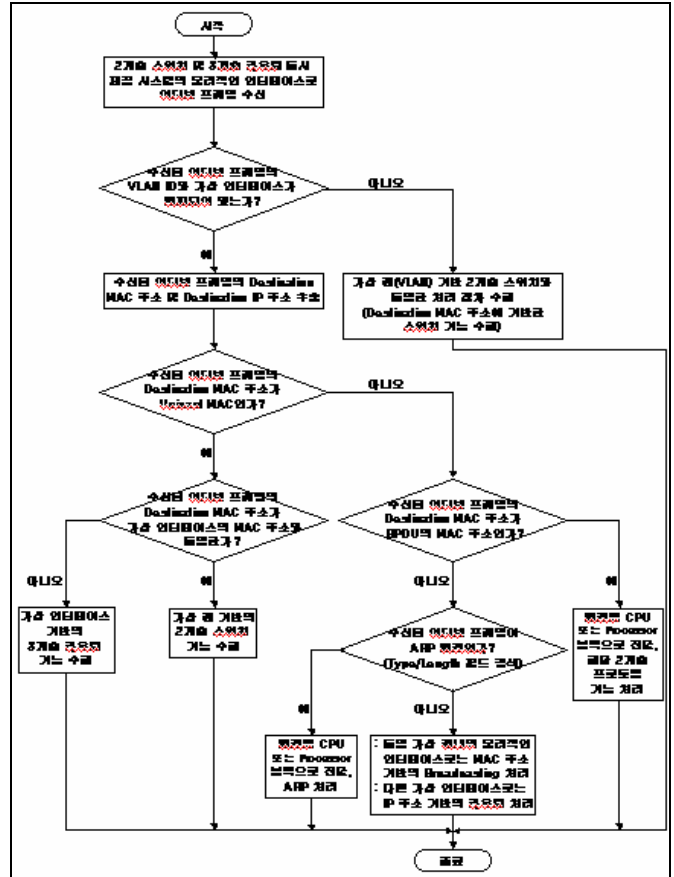
만일 판단 결과 해당 가상 랜의 VLAN ID 가 가상 인터페이스와 맵핑되어 있다면, 수신된 이더넷 프레임의 목적지 MAC 주소 및 목적지 IP 주소를 검색한다.

수신된 이더넷 프레임의 목적지 MAC 주소가 유니캐스트 MAC 주소인지를 판단한 후 유니캐스트 MAC 주소인 경우에는 해당 주소가 가상 인터페이스의 MAC 주소와 동일한지를 판단한다. 판단 결과 유니캐스트 MAC 주소가 가상 인터페이스의 MAC 주소와 동일하지 않은 경우에는 상기에 기술된 가상 랜 기반의 2 계층 스위칭 기능을 수행한다. 반면, 유니캐스트 MAC 주소가 가상 인터페이스의 MAC 주소와 동일한 경우에는 가상 인터페이스 기반의 3 계층 라우팅 기능을 수행한다. 즉, 목적지 IP 주소를 Key 값으로 3 계층 포워딩 테이블을 검색해서 일치하는 엔트리가 존재하는 경우에는 해당 출력 가상 인터페이스로 패킷을 포워딩하고, 존재하지 않는 경우는 폐기하거나 예외 처리를 해야 한다.

수신된 이더넷 프레임의 목적지 MAC 주소가 유니캐스트 MAC 주소가 아닌 경우에는 BPDU(Bridge Protocol Data Unit)의 MAC 주소인지를 판단한다. BPDU 패킷은 목적지 MAC 주소의 상위 3 바이트가 "01:80:C2"로 시작되는 패킷이다. 판단 결과, BPDU의 MAC 주소인 경우에는 해당 패킷을 CPU 또는 프로세서(Processor) 블록으로 전달해서 해당 2 계층 프로토콜 기능을 처리하도록 한다.

상기 판단 결과 BPDU MAC 주소가 아닌 경우는 해당 패킷이 ARP(Address Resolution Protocol) 패킷인지를 판단한다. 해당 이더넷 프레임이 ARP 패킷인지는 이더넷 헤더의 "Type/Length" 필드값을 검색하는 것에 의해 판단이 가능하다. 판단 결과 수신된 패킷이 ARP 패킷인 경우에는 해당 패킷을 CPU 또는 프로세서 블록으로 전달해서 ARP 처리를 수행한다.

상기 판단 결과 수신된 패킷이 ARP 패킷이 아닌 경우는 해당 패킷이 속한 동일 가상 랜의 멤버인 물리적인 인터페이스로는 MAC 주소 기반의 브로드캐스팅을 한다. 그리고, 동일한 패킷을 복사한 후 다른 가상 인터페이스로는 해당 패킷의 목적지 IP 주소에 근거해서 가상 인터페이스 기반의 라우팅 처리를 수행한다.



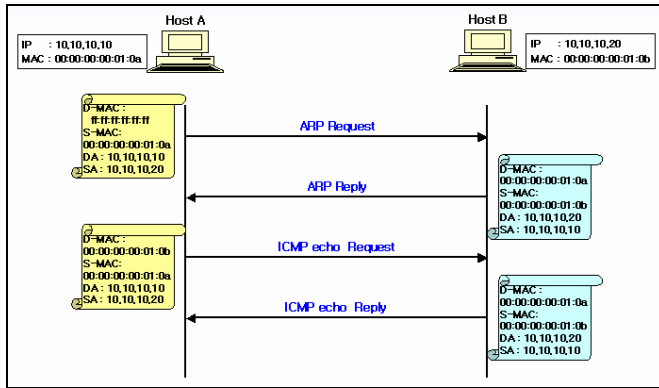
(그림 3) 제안된 시스템에서의 패킷 처리 절차

4. 제안된 시스템에서의 Ping 프로그램 동작 분석

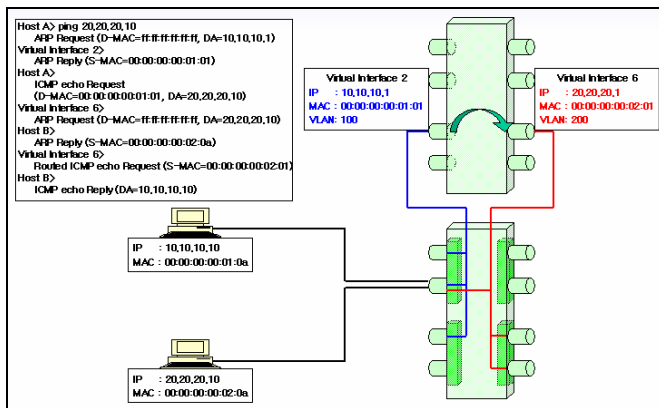
Ping 프로그램은 인터넷 망에서 특정 호스트(Host)가 도달 가능한지를 시험하는 프로그램이며, 기능은 ICMP(Internet Control Message Protocol), UDP(User Datagram Protocol) 또는 SNMP(Simple Network Management Protocol) 프로토콜을 이용해서 구현할 수 있다. 특별히 관련 규격이 존재하지는 않으나, 인터넷 장비의 동작을 시험하는 데 가장 널리 이용되는 범용 프로그램이다. 본 절에서는 Ping 프로그램을 가상으로 구동시켜서 제안된 시스템에서의 동작을 분석함으로써, 제안된 시스템이 2 계층 스위칭 기능과 3 계층 라우팅 기능을 동시에 제공함을 확인하고자 한다.

우선 ICMP 프로토콜 기반으로 구현된 Ping 프로그램의 동작 절차를 그림 4 에서처럼 나타낼 수 있다. 호스트 A 에서 호스트 B 의 IP 주소에 대한 Ping 프로그램을 실행한 경우에, 최초에는 ARP 프로토콜을 구동해서 해당 호스트 B 의 MAC 주소를 얻어 오며 얻어진 MAC 주소를 목적지 MAC 주소로 해서 ICMP echo Request 패킷을 발송하게 된다. 해당 호스트 B 가 ICMP echo Request 패킷을 수신한 후 ICMP echo Reply 패킷으로 응답하면 호스트 A 는 호스트 B 가 네트워크 상에서 도달 가능함을 알게 된다. 뿐만 아니라 Ping

프로그램을 이용해서 호스트 B 까지의 패킷 도달 시간에 대한 정보도 얻을 수 있다.



(그림 4) Ping 프로그램 동작 절차



(그림 5) 제안된 시스템에서의 Ping 프로그램 동작 결과

상기의 Ping 프로그램을 본 논문에서 제안된 시스템에 실행시켰을 경우의 동작 결과를 그림 5 에서처럼 나타낼 수 있다. 그림 5에서는 호스트 A와 호스트 B가 제안된 시스템에 연결되는 다양한 시나리오 중에서, 동일한 물리적인 인터페이스에 다른 가상 랜의 멤버로 연결된 경우에 대해서 제시하였다. 호스트 A에서 호스트 B에 대해 Ping 프로그램을 실행했을 때 가상 인터페이스 기반의 라우팅을 통해서 호스트 B의 네트워크 도달성을 확인할 수 있음을 알 수 있다.

5. 결론

본 논문에서는 사용자에게 인터넷 서비스를 제공하기 위해서, 망 사업자가 스위치와 라우터를 별도로 구매할 필요없이 하나의 시스템으로 서비스할 수 있도록 가상 인터페이스 기반의 2 계층 스위칭 및 3 계층 라우팅 동시 제공 시스템 구조 및 제안된 시스템에서의 패킷 처리 절차를 제시하였다.

제안된 시스템은 가상 랜 기반의 2 계층 스위치에서 가상 인터페이스 기반의 3 계층 라우팅 기능을 제공함

으로써 사용자 요구 사항을 만족하게 되며, 기존의 방법에 비해 하나의 시스템으로 서비스를 제공함으로써 저렴한 비용으로 구현이 가능하며 부가적으로 다른 가상 랜간의 통신을 위한 가상 랜 라우팅(VLAN Routing) 기능도 쉽게 제공할 수 있다. 또한 운용자에게 해당 시스템의 인터페이스를 2 계층 스위치 포트 또는 3 계층 라우터 포트에 자유롭게 설정토록 하는 융통성(Flexibility)을 제공한다.

다만, 최근에 주목받는 TPS(Triple Play Service)를 위해 핵심적인 QoS(Quality of Service) 기능, IPv6 기능 및 효율적인 멀티캐스트 기능의 제공 방안에 대해서는 추후에 고려되어야 한다.

참고문헌

- [1] IEEE Std 802.1D (ISO/IEC 15802-3), "Media Access Control(MAC) Bridges"
- [2] IEEE Std 802.1Q, "Virtual Bridged Local Area Networks"
- [3] G. Malkin, "RIP Version 2," RFC2453, IETF, 1998
- [4] J. Moy, "OSPF Version 2," RFC2328, IETF, 1998