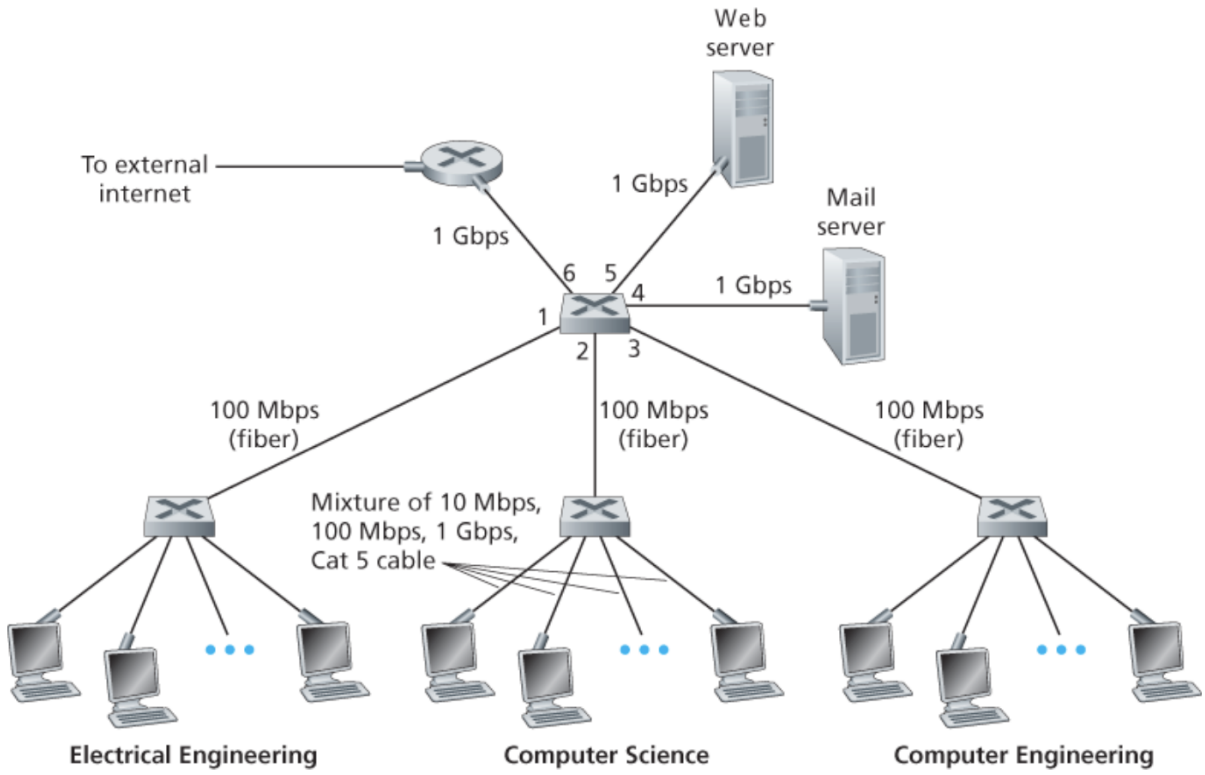
6.4 스위치 근거리 네트워크



스위치는 링크 계층에서 동작하기 때문에 링크 계층 프레임을 교환한다.

또한, 네트워크 계층 주소를 인식하지 않으며, 2계층 스위치들로 구성된 네트워크에서 경로를 결정하는 데 OSPF 같은 라우팅 알고리즘을 사용하지 않는다.

즉, IP 주소가 아닌 **링크 계층 주소를 사용**한다.

6.4.1 링크 계층 주소체계와 ARP

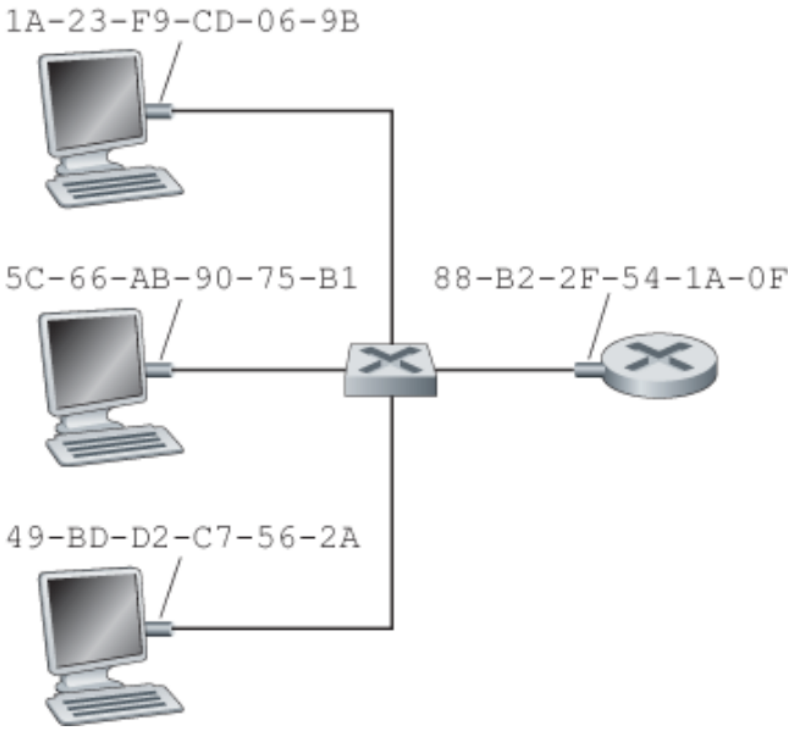
네트워크 계층 주소와 링크 계층 주소

네트워크 계층 주소 체계가 있는데도 링크 계층 주소를 갖는 이유

1. 랜은 IP와 인터넷만을 위해서가 아니라 임의의 네트워크 계층 프로토콜을 위해 설계되었기 때문이다.
2. 만일 어댑터가 MAC 주소 대신에 네트워크 계층 주소를 사용한다면, 네트워크 계층 주소를 어댑터 RAM에 저장하고 어댑터를 이동할 때마다 재구성해야 한다.

즉, 네트워크 구조에서 계층이 독립적인 구성요소가 되도록 하려면 각 계층은 자신만의 주소 기법을 가져야만 한다.

MAC 주소



실제로 링크 계층 주소를 가진 것은 호스트나 라우터가 아닌 호스트나 라우터의 어댑터(네트워크 인터페이스)다.

즉, 다수의 네트워크 인터페이스를 갖고있으므로 여러 개의 링크 계층 주소를 갖게된다.

그러나 링크 계층 스위치는 호스트와 라우터 간에 데이터그램을 전달하는 일을 하기 때문에 호스트나 라우터를 연결해주는 인터페이스에 링크 계층 주소를 할당받지 않는다.

MAC 주소 표기법

MAC 주소는 링크 계층 주소로, 대부분의 랜의 경우 MAC 주소는 길이가 6바이트이며, 따라서 2^48개만큼의 사용 가능한 랜 주소가 있다.

위 그림처럼, 주로 각 바이트는 2개의 16진수로 표기된다.

본래 MAC 주소는 영구적으로 설계되었으나, 이제는 소프트웨어를 사용해서 어댑터의 MAC 주소를 변경할 수 있다.

IEEE가 MAC 주소 공간을 관리하여 모든 어댑터가 다른 주소를 갖게끔 한다.

즉, 어떤 회사가 어댑터를 제조하려면 2^24개의 주소로 이루어진 주소 영역을 구매 후 첫 24비트를 고정하고, 나머지 24비트는 회사로 하여금 각 어댑터에게 유일하게 부여하는 방식으로 2^24개 주소를 할당한다.

MAC 주소는 계층 구조가 아닌 평면 구조를 가지고, 위치가 변하더라도 바뀌지 않는다.

IP 주소가 마치 우편번호 처럼 쓰였다면 MAC주소는 주민등록번호처럼 사용되는 것이다.

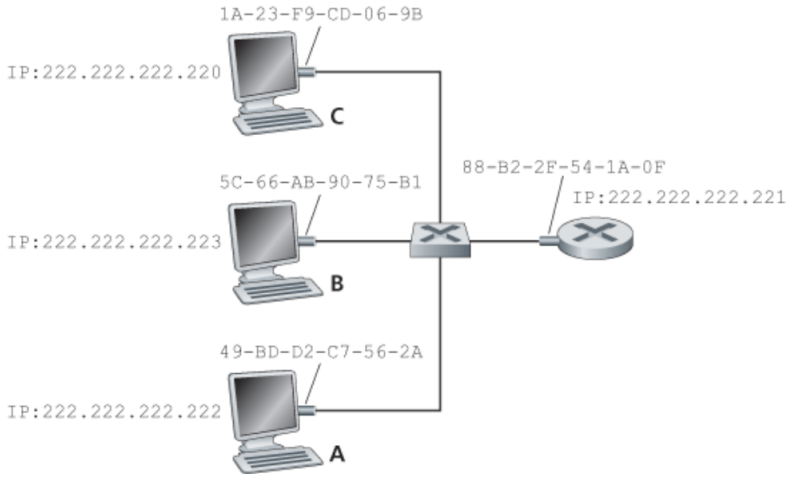
MAC 주소를 활용한 어댑터의 송수신

1. 송신 어댑터는 프레임에 목적지 어댑터의 MAC 주소를 넣고 랜상으로 전송한다.
    - 스위치는 종종 프레임을 자신의 모든 인터페이스로 브로드캐스트한다.
    - 즉, 자신을 목적지로 하지 않는 프레임을 수신할 수도 있다.
2. 프레임을 수신한 어댑터는 프레임 안의 목적지 MAC 주소와 자신의 MAC 주소가 일치하는지 검사한다.
3. 일치하면 데이터그램을 추출하여 프로토콜 스택의 위쪽으로 전달한다.
4. 일치하지 않으면 폐기한다.

랜상의 다른 모든 어댑터가 자신이 전송한 프레임을 수신하고 처리하기를 원할 때 `MAC 브로드캐스트 주소 (broadcast address)`를 넣는다.

이 주소는 모든 비트가 1로된 6바이트 주소이다.

ARP



네트워크 계층 주소와 링크 계층 주소가 있으므로 이들 주소 사이에 변환을 해주는 프로토콜을 `ARP(Address Resolution Protocol)` 이라고 한다.

`ARP 모듈`은 IP와 MAC 주소와 마찬가지로 인터페이스마다 존재한다.

위 그림에서 A에서 C로 데이터그램을 전송하려고 한다고 가정해보자.

데이터그램을 전송하기 위해 목적지 IP 뿐만 아니라 MAC 주소도 주어야만 랜이 적절하게 C로 전달할 수 있다.

송신 호스트 즉, A는 목적지 IP주소를 가진 호스트의 MAC 주소를 알아야하는데 이를 ARP가 해준다.

송신 호스트의 ARP 모듈은 입력값으로서 동일한 랜상의 임의의 IP 주소에 대해 대응되는 MAC 주소를 돌려준다.

이러한 면에서 DNS와 비슷한 면이 있다.

그러나 DNS는 인터넷의 임의의 장소에 있는 호스트의 호스트 네임을 해결하는 반면에, A**RP는 동일한 서브넷상에 있는 호스트나 라우터 인터페이스의 IP 주소만을 해결**한다.

ARP 동작 과정

각 호스트와 라우터는 자신의 메모리에 `ARP 테이블(ARP table)`을 갖고 있다.

이 테이블은 IP 주소와 MAC 주소 간의 매핑 정보를 포함하며, 테이블에서 각 매핑이 언제 삭제되는지를 나타내는 `TTL(time-to-live)` 값을 포함한다.

일반적으로 삭제 시간은 엔트리가 테이블에 들어간 후 20분이다.

테이블에 서브넷상의 모든 호스트와 라우터에 대한 엔트리를 갖고 있지 않아도 된다.

즉,데이터그램을 전송하려할 때, ARP 테이블에 목적지 노드에 대한 엔트리가 없을 수 있다.

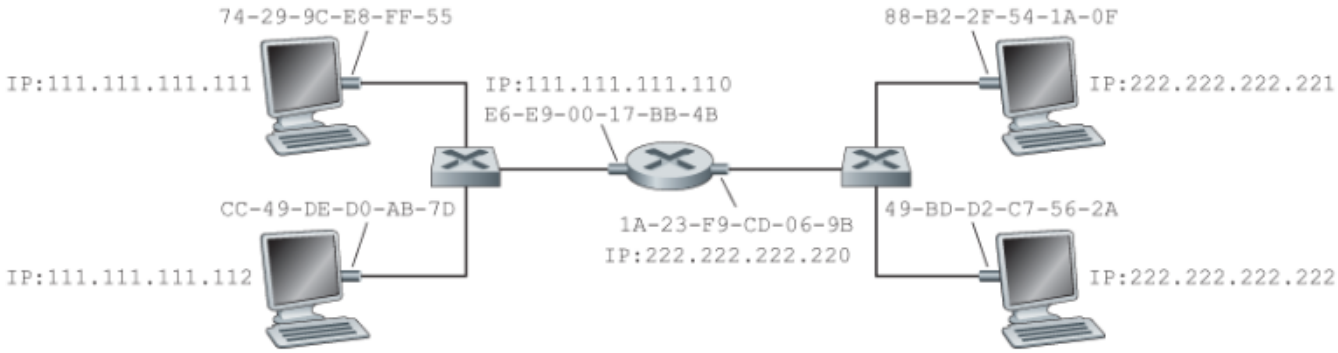
다음 동작 과정을 보자.

1. 송신 노드는 MAC 주소를 해결하기 위해 ARP 프로토콜을 사용하여 `ARP 패킷`이라는 특수 패킷을 어댑터에 보낸다.
    - ARP 패킷은 송수신 IP주소와 MAC 주소를 포함하는 필드를 가지며 질의 패킷과 응답 패킷 모두 같은 형식을 갖는다.
    - 질의 패킷의 목적은 해결하려는 IP주소에 대응되는 MAC 주소를 결정하기 위해 서브넷의 다른 모든 호스트와 라우터들에게 질의하는 것이다.
    - 질의 패킷은 브로드캐스트 프레임으로 전송된다.
2. 어댑터는 ARP패킷을 링크 계층 프레임에 캡슐화하고, 목적지 주소를 MAC 브로드캐스트 주소(FF-FF-FF-FF-FF-FF)로 하여 패킷을 전송한다.
3. 이 질의는 서브넷 상의 다른 모든 어댑터에 의해 수신되며, 브로드캐스트 주소 때문에 각 어댑터는 프레임에 들어있는 ARP 패킷을 자신의 ARP 모듈로 전달한다.
4. ARP 모듈은 자신의 IP 주소가 ARP 패킷에 들어 있는 목적지 IP주소와 일치하는지 검사한다.
5. 일치하는 노드는 요구된 매핑 정보가 포함된 응답 패킷을 돌려보낸다.
    - 질의 패킷은 브로드캐스트 프레임으로 전송되는 반면 응답 패킷은 표준 프레임으로 전송된다.
6. 질의 호스트는 자신의 ARP 테이블을 갱신한다.

즉, 노드의 `ARP 테이블(ARP table)` 은 `플러그 앤 플레이(plug-and-play)`다. 즉, 관리자가 구성하지 않아도 자동으로 구축된다.

ARP는 링크 계층 주소도 포함하고, 네트워크 계층 주소도 포함하기 때문에 네트워크 계층과 링크 계층의 경계에 있는 프로토콜이다.

서브넷에 없는 노드로의 데이터그램 전송



위 그림에서 호스트 `111.111.111.111`이 호스트 `222.222.222.222`로 IP 데이터그램을 전송하려한다고 가정하자.

라우터는 2개의 IP 주소, 2개의 ARP 모듈, 2개의 어댑터(어댑터는 고유한 MAC 주소를 가지고 있으므로 MAC주소도 2개다.)를 가지고 있다.

송신 호스트는 적절한 목적지 MAC 주소와 IP 주소가 포함된 데이터그램을 자신의 어댑터로 전달해야한다.

만약, 송신 어댑터가 목적지 MAC 주소를 `49-BD-D2-C7-56-2A` 를 사용한다면 목적지 주소는 `111.111.111.111` 호스트가 포함된 서브넷에 있는 어떤 어댑터의 MAC 주소와도 일치하지 않으므로 서브넷에 있는 어떤 어댑터도 IP 데이터 그램을 자신의 네트워크 계층으로 전달하지 않는다.

즉, 데이터그램은 전달되지 않고 사라진다.

데이터그램이 전달되기 위해서는 라우터 인터페이스 `111.111.111.110`으로 전달해야만 한다. 따라서 이 프레임에 대한 적절한 MAC 주소는 라우터 인터페이스의 `E6-E9-00-17-BB-4B` 이다.

동작 과정

1. 송신 호스트가 `111.111.111.110` 의 MAC 주소를 ARP를 사용하여 알게된다.
2. MAC주소를 알게 되면 송신 호스트는 IP 목적지 주소가 `222.222.222.222` 를 포함하는 **데이터그램을 알아낸 MAC 주소와 함께 서브넷으로 전송**하고 서브넷의 라우터 어댑터는 MAC 주소가 일치하므로 네트워크 계층까지 전달한다.
3. 라우터의 포워딩 테이블을 통해 라우터에게 데이터그램을 라우터 인터페이스 `222.222.222.220` 을 거쳐서 전달하도록 지시한다.

4. 인터페이스는 데이터그램을 자신의 어댑터로 전달하고 어댑터는 데이터그램을 새 프레임에 캡슐화하여 그 프레임을 다른 서브넷으로 전달한다.
    - 여기서의 목적지 MAC 주소는 당연히 ARP를 통해 알게된다.

6.4.2 이더넷

오늘날 이더넷은 가장 우세한 랜 기술이다.

인터넷이 글로벌 네트워킹에 대한 것이라면, 이더넷은 근거리 네트워킹에 대한 것이다.

발전 과정

- 1980년대
    - 이더넷 랜은 노드를 연결하기 위해 동축 버스를 사용했다.
    - 버스 토폴로지의 이더넷은 브로드캐스트 랜으로, 전송되는 모든 프레임은 버스에 연결된 모든 어댑터를 거치며 이들에 의해 처리된다.
- 1990년대
    - 랜을 허브 기반의 스타 토폴로지를 사용하는 이더넷으로 대체
    - 꼬임쌍선을 사용해서 허브에 직접 연결된다.
    - `허브(hub)`는 프레임이 아닌 각각의 비트에 대한 처리를 하는 물리 계층 장치다.
    - `허브(hub)` 가 한 인터페이스로 비트를 수신하면 그 비트의 복사본을 다른 모든 인터페이스로 전송한다.
- 2000년대 초반
    - 중앙의 허브가 `스위치(switch)`로 대체되었다.
    - `스위치(switch)` 는 충돌 없는 장치일 뿐만 아니라 저장-후-전달 패킷 스위치이다.

이더넷 프레임 구조

- 데이터 필드(46~1500바이트)
    - 이 필드는 IP 데이터그램을 운반한다.
    - 1500바이트를 초과하면 호스트가 단편화해야한다는 것을 의미한다.
    - 46바이트보다 작으면 데이터 필드를 채워서 46바이트로 만들어야 한다. 채운 부분을 제거하기 위해 IP 데이터그램 헤더의 길이 필드를 사용한다.
- 목적지 주소(6바이트)
    - 목적지 MAC주소가 들어간다.
- 출발지 주소(6바이트)
    - 출발지 MAC주소가 들어간다.

- 타입 필드(2바이트)
  - 네트워크 계층 프로토콜을 이더넷으로 하여금 다중화하도록 허용한다.
  - 즉, IP 이외의 네트워크 계층 프로토콜을 사용할 수 있게끔 한다.
- 순환 중복 검사(CRC)(4바이트)
  - CRC 필드의 목적은 수신 어댑터가 프레임에 오류가 생겼는지 검출할 수 있게 한다.
- 프리앰블(8바이트)
  - 이더넷 프레임은 8바이트의 프리앰블(preamble) 필드로 시작한다.
  - 프리앰블의 첫 7바이트는 `10101010` 값을 갖고 마지막 바이트는 `10101011`이다.
  - 프리엠블의 첫 7바이트는 수신 어댑터를 깨우고, 수신자의 클록을 송신자의 클록과 동기화하는 역할을 한다.
  - 송신 어댑터는 이더넷 랜 종류에 따라 원하는 속도로 프레임을 전송하려 하지만 송신 어댑터는 목적지 속도에 정확히 맞게 전달할 수 없으므로 수신 어댑터는 단순히 프리앰블의 첫 7바이트에 있는 비트들에 맞춤으로써 송신 어댑터의 클록에 맞출 수 있다.
  - 8번째 바이트의 마지막 두비트는 수신 어댑터에게 중요한 것이 오고 있음을 알려준다.

이더넷의 비연결형 서비스(connectionless service), 비신뢰적인 서비스

송신 어댑터는 데이터그램을 전송할 때 핸드셰이킹 하지 않고 이더넷 프레임에 캡슐화해서 랜으로 전송한다.

수신 어댑터는 CRC 검사를 통해 프레임을 검사하지만 이에 대한 확인 응답 혹은 부정 확인 응답을 보내지 않는다.

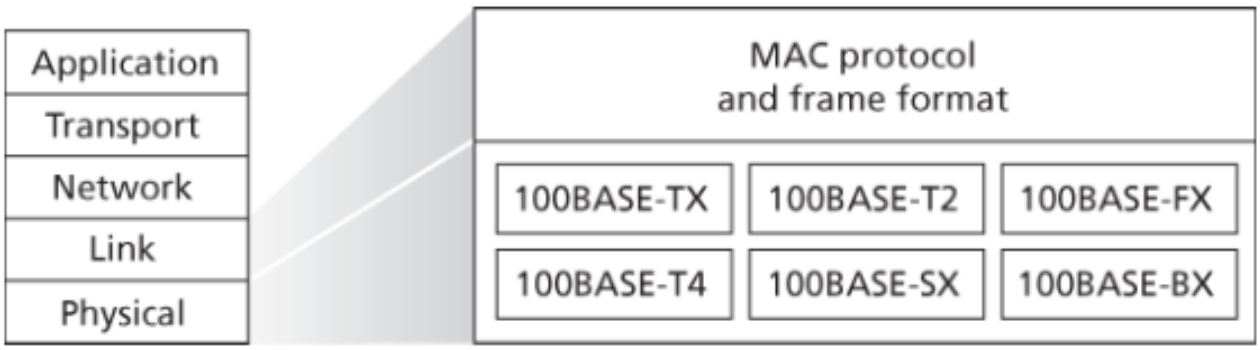
그저, 실패하면 폐기한다.

애플리케이션이 UDP 또는 TCP를 사용하는지에 따라 데이터그램의 손실을 알 수 있음이 결정된다.

UDP의 경우 알 수 없고, TCP는 확인 후 재전송하게 할 것이다.

즉, 이더넷은 전송하고 있는 데이터그램이 재전송인지 새로운 데이터그램인지 구분할 수 없다.

이더넷 기술



이더넷은 수년에 걸쳐 진화해왔으며, 오늘날의 이더넷은 동축케이블을 사용하는 초기 버스 토폴로지 설계와 상당히 다르다.

요즘은 노드가 꼬임쌍선이나 광섬유 케이블로 만들어진 점대점 세그먼트를 통해 스위치에 연결된다.

이더넷이 발전하여도, 프레임 형식은 그대로 유지되어 사용된다.

버스 토폴로지와 허브 기반의 스타 토폴로지의 이더넷 표준은 노드들이 동시에 전송하면 프레임 충돌이 발생하는 브로드캐스트 링크였다.

이 충돌을 처리하기 위해 CSMA/CD 프로토콜이 포함되었다.

현재 많이 사용하는 이더넷은 저장-후-전달 패킷 교환을 하는 스위치 기반의 스타 토폴로지인데, 여전히 MAC 프로토콜이 필요할까?

스위치 기반 이더넷 랜에는 충돌이 없어 MAC 프로토콜이 필요하지 않다.

6.4.3 링크 계층 스위치

스위치의 역할은 들어오는 링크 계층 프레임을 수신해서 출력 링크로 전달하는 것이다.

스위치는 그 자체가 서브넷의 호스트와 라우터들에게 투명하다.

즉, 호스트/라우터는 프레임을 스위치가 아닌 다른 호스트/라우터를 목적지로해서 랜상으로 보내며, 중간에 스위치가 프레임을 받아서 다른 노드에게 전달하는 것을 알지 못한다.

프레임이 스위치 출력 인터페이스들 중 하나에 도착하는 속도가 그 인터페이스의 링크 용량을 일시적으로 초과할 수 있다.

이 문제를 해결하기 위해, 스위치 출력 인터페이스는 버퍼를 갖고 있다.

포워딩과 필터링

- 필터링(filtering)
  - 프레임을 인터페이스로 전달할지 또는 폐기(drop)할지 결정하는 스위치의 기능
  - 스위치 테이블(switch table)을 이용
- 포워딩(forwarding)
  - 프레임이 전송될 인터페이스를 결정하고 프레임을 해당 인터페이스로 내보내는 기능
  - 스위치 테이블(switch table)을 이용
- 스위치 테이블(switch table)
  - 랜상의 모든 호스트와 라우터는 아니지만 일부 노드에 대한 엔트리가 포함되어 있다.
  - 스위치 테이블 엔트리 구성
    - MAC 주소
    - MAC 주소로 가게 하는 스위치 인터페이스
    - 해당 엔트리가 만들어진 시점

스위치 테이블 엔트리의 동작

목적지 주소를 가진 프레임이 스위치 인터페이스 x에 도달했다고 하자.

- 테이블에 **목적지 주소에 대한 엔트리가 없는 경우**
  - 스위치는 프레임의 복사본을 프레임이 수신된 인터페이스를 제외한 모든 인터페이스의 출력 버퍼로 전달한다.
  - 즉, 브로드캐스트한다.
- 테이블에 목적지 주소가 x **인터페이스에 연관된 엔트리**가 있는 경우
  - 프레임은 송신자 어댑터를 포함하는 랜 세그먼트로부터 왔다.
  - 프레임을 다른 인터페이스로 전달할 필요가 없으며, 프레임을 제거함으로써 필터링 기능을 수행한다.
- 테이블에 목적지 주소가 y≠x 인터페이스와 연관된 엔트리가 있는 경우
  - 프레임은 y 인터페이스에 접속된 랜 세그먼트로 전달되어야 한다.
  - 즉, 해당 인터페이스 출력 버퍼에 프레임을 넣음으로써 포워딩 기능을 수행한다.

자가학습

스위치는 테이블을 자동으로, 동적으로, 자치적으로 `자가학습(self-learning)`하는 특징이 있다.

동작 과정

1. 스위치 테이블은 초기에 비어있다.
2. 인터페이스로 수신한 각 프레임에 대해 스위치는 다음과 같은 정보를 저장한다.
   - 프레임의 출발지 주소 필드에 있는 MAC 주소
     - 즉, 다음번 수신 때 다른 랜에서 목적지 주소 필드를 해당 MAC 주소를 갖게되면 프레임을 알맞게 전달할 수 있게 된다.
   - 프레임이 도착한 인터페이스
   - 현재 시간
3. 랜에 있는 모든 호스트가 프레임을 송신하면, 결국 모든 호스트에 대한 정보가 테이블에 기록된다.
4. `수명 시간(aging time)`이 지난 후에도 스위치가 해당 주소를 출발지 주소로 하는 프레임을 수신하지 못하면 테이블에서 이 주소를 삭제한다.
   - 즉, PC가 다른 PC로 대체되면 원래 PC의 MAC 주소는 스위치 테이블에서 삭제된다.

스위치는 네트워크 관리자나 사용자의 개입을 요구하지 않으므로 `플러그 앤 플레이 장치(plug-and-play device)`다.

링크 계층 스위치의 특성

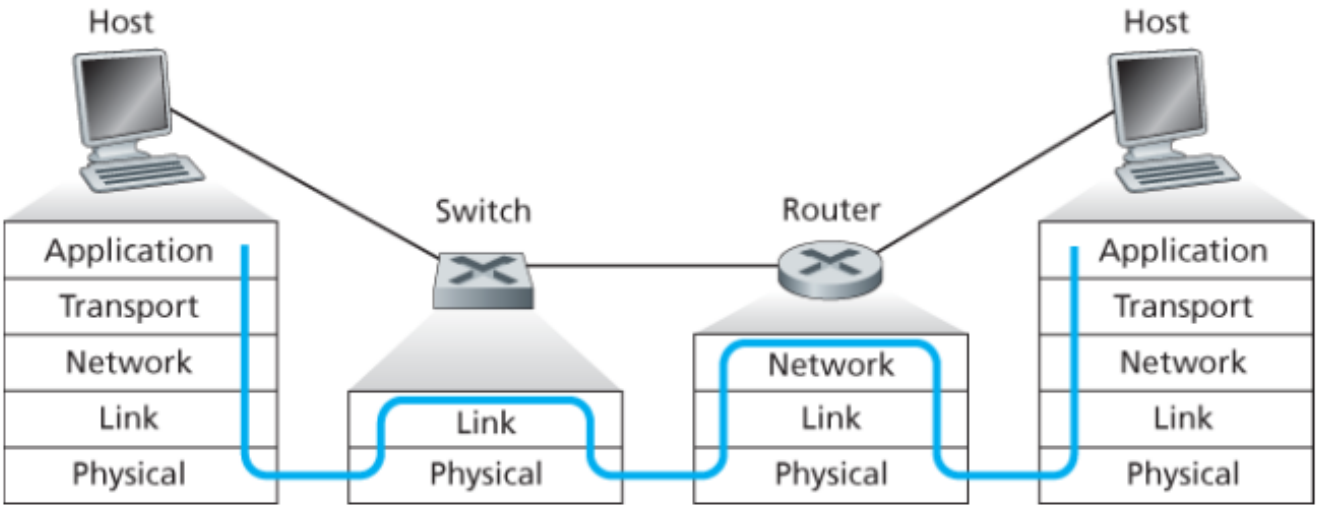
- 충돌 제거
  - 스위치로 구축된 랜에는 충돌로 인해 낭비되는 대역폭이 없다.
  - 프레임을 버퍼링하며 어느 시점이든 세그먼트에 하나 이상의 프레임을 전송하지 않는다.
  - 브로드캐스트 링크를 사용하는 랜보다 성능이 월등히 향상된다.
- 이질적인 링크들
  - 링크들을 별개로 분리하기 때문에 랜의 각 링크는 상이한 속도로 동작할 수 있으며 상이한 매체를 사용할 수 있다.
- 관리
  - 스위치는 향상된 보안을 제공할 뿐만 아니라 네트워크 관리를 쉽게 할 수 있게 한다.

    - e.g. 케이블이 끊긴다면 그쪽 호스트의 연결만 끊어진다, 오동작으로 프레임을 계속 보내는 경우 이 문제를 감지하고 오동작하는 어댑터의 연결을 의도적으로 끊는다.
    - 대역폭 사용, 충돌률, 트래픽 종류에 대한 통계치를 수집하여 볼 수 있다.

보안 초점

- 스위치 테이블에 엔트리가 있을 때
    - 호스트가 스위치에 연결되면 보통 자신을 목적지로 해서 전송된 프레임만 수신하기 때문에 다른 호스트는 프레임을 훔쳐볼 수 없다.
- 스위치 테이블에 엔트리가 없을 때
    - 스위치가 프레임을 브로드캐스트하기 때문에 스니퍼는 자신을 목적지로 하지 않는 일부 프레임을 훔쳐볼 수 있다.
    - 이를 이용해 `스위치 독(switch poisoning)`이라는 공격 수법을 사용하여 프레임을 훔쳐본다.
        - `스위치 독(switch poisoning)` 은 여러 가짜 출발지 MAC 주소를 갖는 패킷을 상당수 보내 스위치 테이블을 가짜 엔트리로 가득채워 합법적인 호스트들의 MAC 주소를 넣을 공간을 없애는 것을 말한다.

스위치 대 라우터



- 라우터
    - 네트워크 계층 주소를 사용해서 패킷을 전달하는 저장 후 전달 패킷 스위치다.
    - 3계층 패킷 스위치이다.
- 스위치
    - 저장후 전달 패킷 스위치이지만 MAC 주소를 사용해서 패킷을 전달한다.
    - 2계층 패킷 스위치이다.

이 둘은 근본적으로 다르지만(MAC 주소, IP 주소를 사용한다는 점에서), 네트워크 관리자는 상호연결 장치를 설치할 때 종종 이들 중에서 선택해야만 한다.

실제로, 라우터는 충돌 없이 학과 간의 통신이 가능하게 할 수 있다.

스위치의 장점

- `플러그 앤 플레이 장치(plug-and-play device)` 로 관리자가 크게 신경쓸 필요가 없다.
- 높은 패킷 필터링 및 전달률을 갖는다.

스위치의 단점

- 브로드캐스트 프레임의 순환을 방지하기 위해 스위치 네트워크의 실제 사용되는 토폴로지는 스패닝 트리로 제한된다.
- 대규모 스위치 네트워크에서는 호스트와 라우터가 커다란 ARP 테이블을 갖게 되며 상당한 양의 ARP 트래픽이 생성되고 처리된다.
- 브로드캐스트 트래픽의 폭주에 대비한 방안을 제공하지 않는다.

라우터의 장점

- 계층구조이므로, 네트워크에 중복된 경로가 있을 때 조차도 패킷은 라우터를 따라 순환하지 않는다. 즉, 스패닝 트리로 제한받지 않고 최상의 경로를 사용할 수 있다.
- 제한이 없으므로 인터넷 토폴로지가 자유롭게 구축될 수 있게 한다.
- 브로드캐스트 폭풍에 대비한 방화벽 보호기능이 있다.

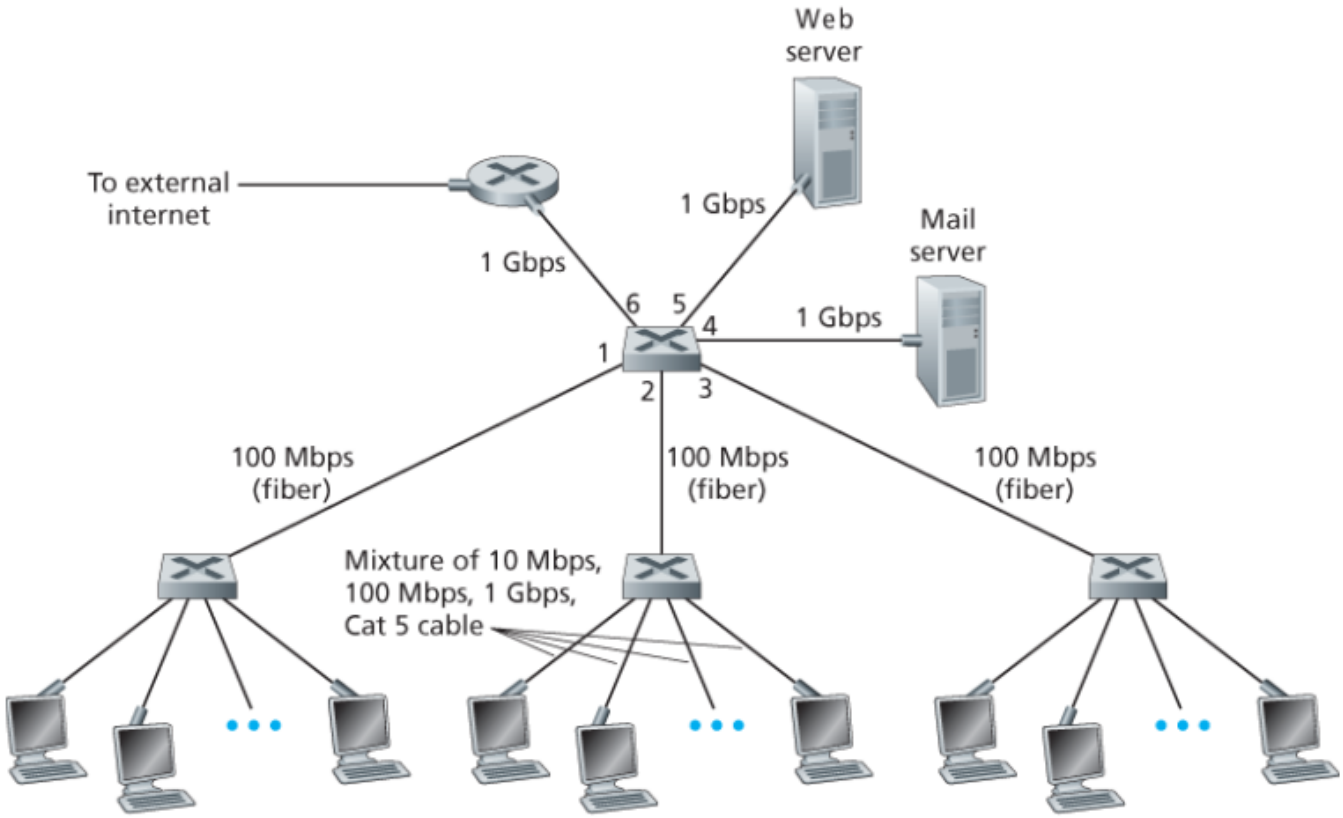
라우터의 단점

- `플러그 앤 플레이 장치(plug-and-play device)` 가 아니다.
- 스위치보다 패킷당 처리 시간이 더 크다.

일반적으로, 작은 네트워크는 트래픽이 지역적으로 제한되어 있고 IP 주소의 구성을 요구하지 않으면서도 총 처리율을 증가시키므로 스위치로도 충분하다.

그러나 보통 수천 개의 호스트로 구성된 큰 네트워크에서는 라우터도 포함한다.

6.4.4 가상 근거리 네트워크(VLAN)



위 구조에서 스위치는 계층적으로 구성되어있는데, 이러한 구성의 단점은 다음과 같다.

- 트래픽 격리의 부족
  - 계층 구조는 그룹 트래픽을 단일 스위치 내로 격리해주지만, 브로드캐스트 트래픽은 여전히 전체 네트워크로 전달되어야만 한다.
  - 즉, 브로드캐스트의 범위를 제한하면 랜 성능을 향상할 수 있다.
- 스위치의 비효율적인 사용
  - 기관에 그룹이 3개가 아닌 10개가 있는 경우 첫 단계 스위치가 10개가 필요하다.
  - 그룹 내 인원수가 10명보다 작으면 96 포트 스위치 하나로 모든 사람을 수용할 수 있지만 스위치 하나로는 트래픽 격리를 할 수 없다.
- 사용자 관리
  - 사원이 한 그룹에서 다른 그룹으로 이동하는 경우 이 사원을 다른 스위치에 연결하기 위해 물리적 케이블 연결을 변경해야만 한다.

위와 같은 단점을 가상 근거리 네트워크(virtual local area network, VLAN)를 지원하는 스위치를 사용해서 해결할 수 있다.

VLAN을 지원하는 스위치는 하나의 물리적 근거리 네트워크 인프라스트럭처상에서 여러 개의 가상 근거리 네트워크들을 정의할 수 있게한다.

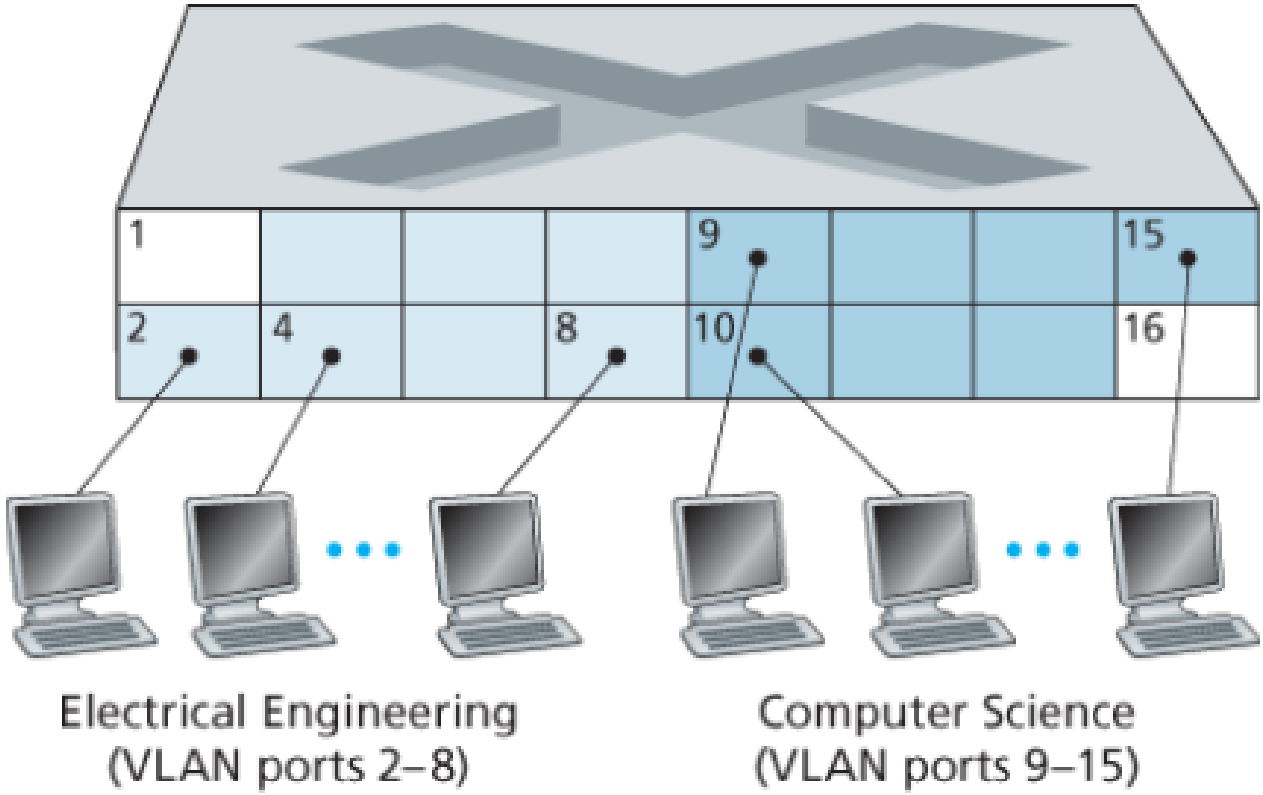
VLAN에 속한 호스트들은 마치 스위치에 자신들만(다른 호스트들은 없이) 연결된 것처럼 서로 통신한다.

포트 기반 VLAN에서는 네트워크 관리자가 스위치 포트(인터페이스)를 그룹으로 나눈다.

나뉜 각 그룹은 하나의 VLAN을 구성하며, 한 VLAN 포트들은 하나의 브로드캐스트 도메인을 형성한다.

즉, 같은 그룹의 다른 포트에만 브로드캐스트 트래픽을 전달할 수 있다.

기본 VLAN



위 그림은 16개의 포트를 갖고 있는 단일 스위치를 보여준다.

포트 2~8은 EE VLAN이고, 9~15는 CS VLAN에 속한다.

- VLAN은 각각의 프레임을 서로 격리해준다.
- 그룹을 변경하려면 관리자가 포트가 속한 그룹이 바뀌도록 재구성한다.
- 2개의 그룹을 위해 있던 2개의 스위치가 하나의 스위치로 대체되었다.

즉, 위의 단점을 모두 해결한다.

VLAN 스위치는 포트-VLAN 매핑 테이블을 관리하고 네트워크 관리자가 스위치 관리 소프트웨어를 사용해서 이를 바꿀 수 있다.

또한, 스위치 하드웨어는 같은 VLAN에 속한 포트들 간에만 프레임을 전달한다.

EE VLAN to CS VLAN 트래픽 전송 과정

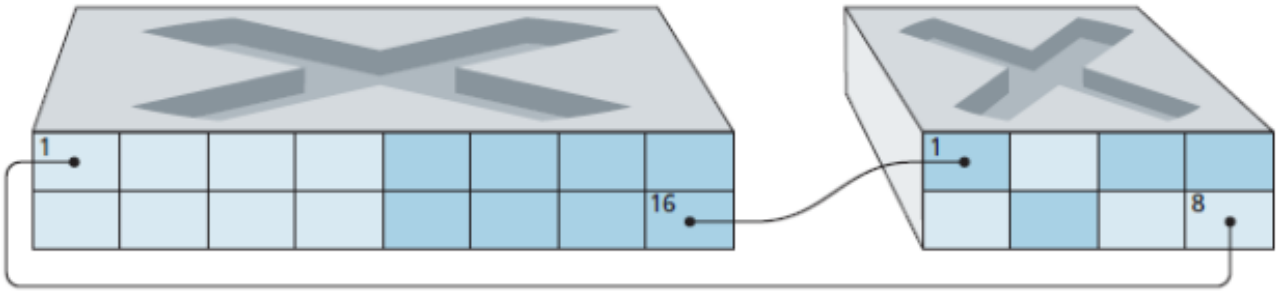
EE VLAN과 CS VLAN은 물리적으로는 붙어있지만 논리적으로는 다른 LAN이기 때문에 트래픽 전송이 다른 스위치나 라우터를 거쳐야만 한다.

- VLAN 스위치 포트(미사용 포트, e.g. 위 그림에서 1번 포트)를 외부 라우터에 연결한다.
- VLAN 스위치 포트를 두개의 LAN 모두에 속하게 한다.
- 데이터그램이 먼저 CS VLAN(스위치 포트)를 통과해서 라우터에 도달한다.

- 라우터에 의해 CS VLAN을 통해 CS 호스트로 전달된다.

스위치 생산자들은 VLAN 스위치와 라우터를 모두 포함시켜 네트워크 관리자가 위 과정을 쉽게할 수 있도록 한다.

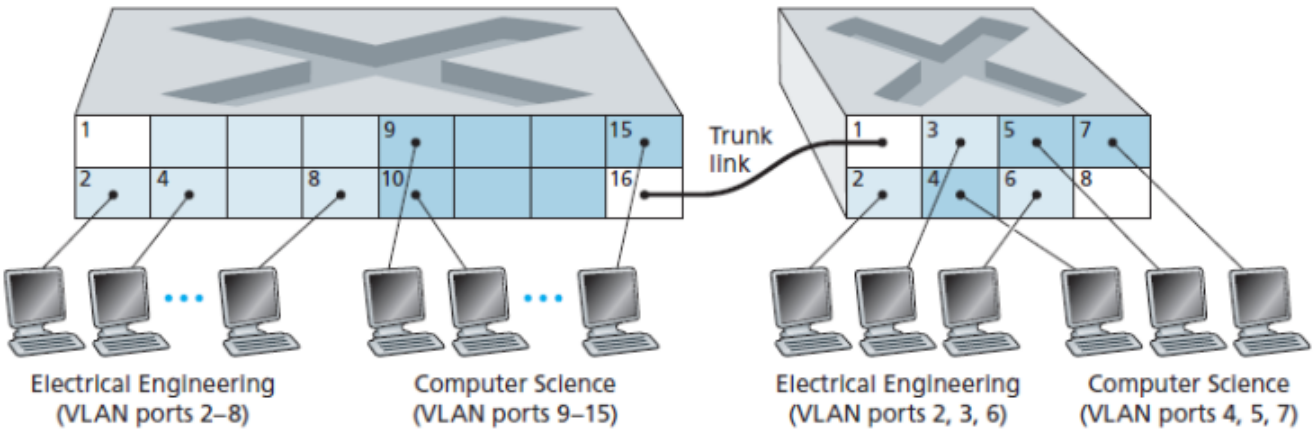
외부 스위치가 VLAN에 속하길 원하는 경우



a.

스위치에 N개의 VLAN이 있다고 하면 N개의 포트를 N개의 VLAN에 속하게 하고, 외부 스위치에 하나씩 연결해주면 외부 스위치도 VLAN 스위치와 같이 일할 수 있다.

그러나 N개의 VLAN에는 N개의 포트가 필요하므로 확장에 문제가 있다.



b.

위 방법은 VLAN 트렁킹(VLAN Trunking) 방식이다.

스위치 마다 하나의 특수 포트가 2개의 VLAN을 연결하는 트렁크 포트(trunk port)로 구성되어있다.

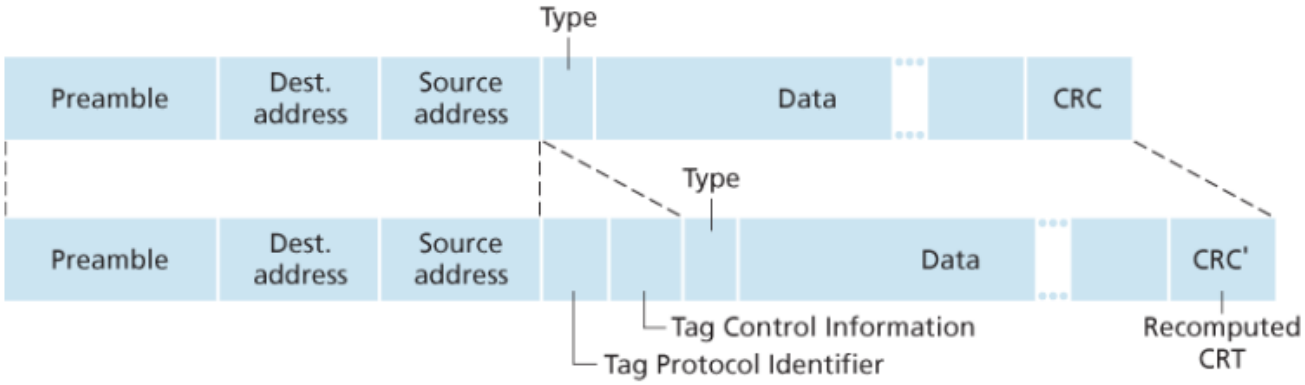
트렁크 포트(trunk port) 는 모든 VLAN에 속하며 한 VLAN에서 전송한 프레임들을 트렁크 링크를 통해 다른 스위치로 전달해준다.

이때 어떤 트렁크 포트로 온 프레임이 어떤 VLAN에 속하는지 알 수 없다.

이를 위해 IEEE는 VLAN 트렁크를 통과하는 프레임을 위한 확장된 형태의 이더넷 프레임 형식을 정의했다.

확장된 이더넷 프레임 형식은 VLAN을 식별해주는 4바이트 VLAN 태그(VLAN Tag)를 헤더에 갖고 있다.

VLAN 태그(VLAN Tag) 는 당연하지만, 송신 측의 스위치에 의해 추가되고, 수신 측에 있는 스위치에 의해 파싱되고 제거된다.



VLAN 태그(VLAN Tag) 구성

- 2바이트 태그 프로토콜 식별자(Tag Protocol Identifier, TPID) 필드
- 2바이트 태그 제어 정보(Tag Control Information) 필드
    - 12비트의 VLAN 식별자(identifier) 필드 <- 추가 필요
    - 3비트 우선순위(priority) 필드