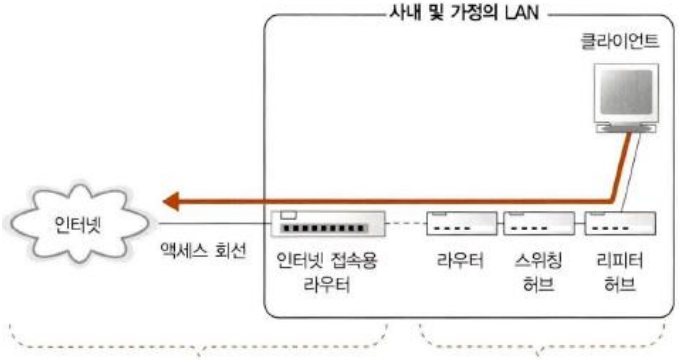
Chapter 04

스위치, 허브, 그리고 라우터

1. 케이블, 리피터, 허브

패킷의 동작

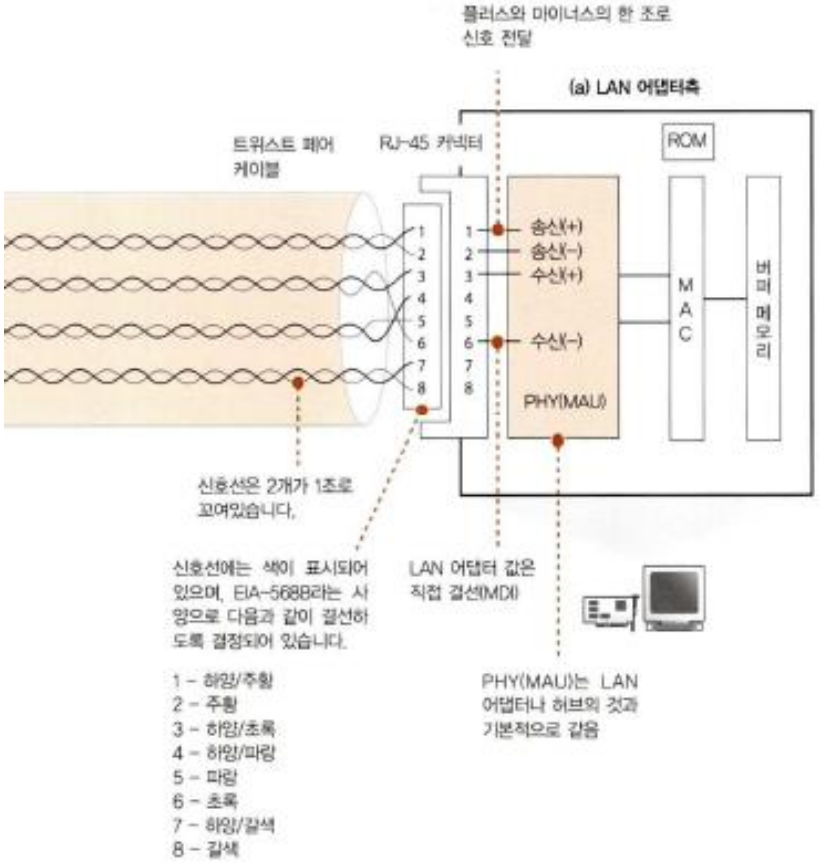
- 컴퓨터에서 송신된 패킷은 허브나 라우터라는 중계 장치에 의해 중계되어 목적지를 향해 진행한다.
- 중계 동작은 패킷의 헤더에 기록된 제어정보와 중계 장치의 내부에 있는 중계 대상을 등록한 표로 목적지를 판단하고 목적지에 가까워지도록 하여 패킷을 중계한다는 형태이다.
- 중계 동작을 할 때 우편배달부가 편지의 내용을 보지 않고 배달하는 것처럼 중계 장치는 데이터 부분을 보지 않고 패킷을 중계한다.
- 내용을 보지 않으므로 거기에 쓰여 있는 애플리케이션의 데이터나 TCP 프로토콜의 제어정보의 내용이 패킷을 운반하는 동작에 영향을 주지 않는다.
- 따라서 모든 패킷은 아무 관련도 없는 별개의 것으로 간주하고 목적지를 향해 중계된다.
- 이 장에서는 클라이언트 PC가 LAN에 접속되어 있는 것으로 가정한다.
- 즉 클라이언트 PC가 송신한 패킷이 리피터 허브, 스위칭 허브, 라우터를 경유하여 인터넷에 나가는 것으로 간주한다.



1. 케이블, 리피터, 허브

LAN 케이블

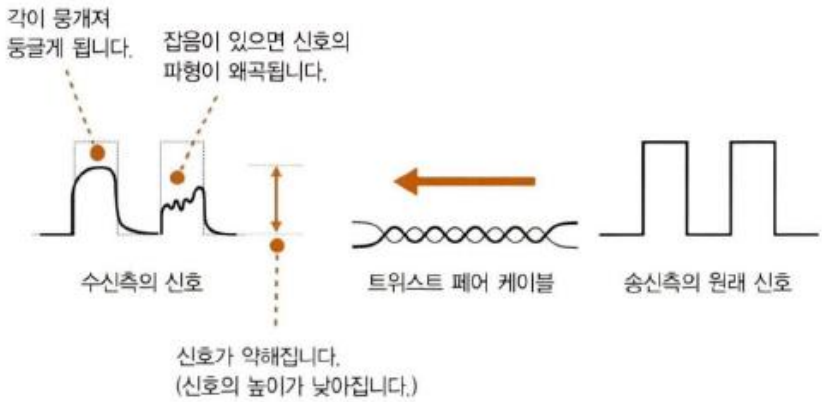
- 이 장은 LAN 어댑터에서 패킷이 송신되어 케이블로 나가는 부분부터 시작된다.
- LAN 어댑터의 PHY(MAU) 회로에서 전기 신호로 형태를 바꾼 패킷은 RJ-45 커넥터를 통해 트위스트 페어 케이블(꼰 선쌍)에 들어간다.
- 이더넷의 신호의 실체는 플러스와 마이너스의 전압이므로 LAN 어댑터의 PHY(MAU) 회로의 플러스와 마이너스 신호 단자에서 신호가 나온다고 생각하면 된다.
- LAN 어댑터의 PHY(MAU) 회로는 RJ-45 커넥터에 직접 결선되어 있으므로 커넥터의 1번 핀과 2번 핀에서 케이블로 신호가 흘러 나간다.
- 그 후 신호는 케이블 속을 흘러 리피터 허브의 커넥터 부분에 도착하고, 이 부분은 단순히 전기 신호가 케이블을 통해 전달되는 것 뿐이다.



1. 케이블, 리피터, 허브

LAN 케이블

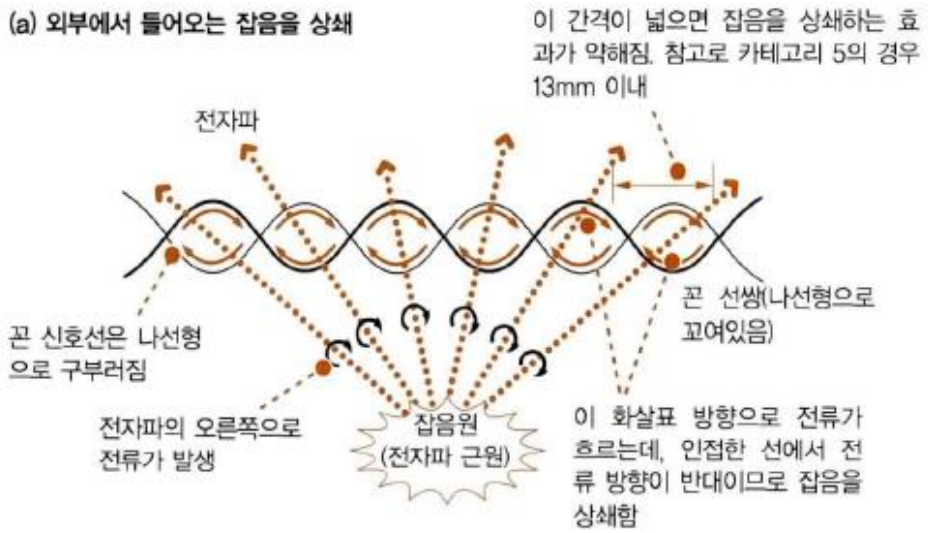
- 송출한 신호는 그대로의 모습으로 허브에 도착한 것이 아니라 허브에 도착할 때는 신호가 약해져 있다(그림).
- 케이블을 통과하는 사이에 신호의 에너지가 조금씩 떨어지므로 케이블의 길이가 길어질수록 신호가 약해진다.
- 신호는 단지 약해지기만 하는 것이 아니다.
- 이더넷은 사각형의 각진 신호를 사용하지만 이 각이 뭉개져서 둥글게 된다.
- 이 현상은 주파수가 높을수록 에너지가 떨어지는 비율이 높다는 전기 신호의 성질과 관계가 있다.
- 잡음이 없고 조건이 좋은 경우에도 신호가 도착할 때는 이와 같이 변형되는데, 이것에 잡음의 영향까지 더해지면 매우 심각하게 변형된다.
- 이 경우에는 약해진 신호가 더욱 변형되므로 0과 1을 잘못 판독할 수 있는데, 이것이 통신 오류의 원인이 된다.



1. 케이블, 리피터, 허브

트위스트 페어 케이블

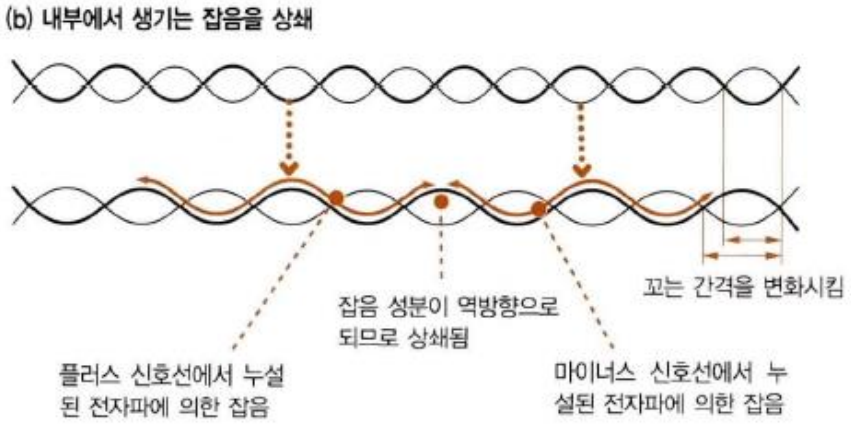
- LAN 케이블로 사용하는 트위스트 페어 케이블(꼰 선생)에는 이러한 잡음의 영향을 억제하는 대책이 마련되어 있는데 이것이 '꼼'이다.
- '트위스트 페어(꼰 쌍)'라는 말은 두 가닥의 신호선을 한 조로 하여 마주 꼬았다는 데서 붙인 이름으로, 신호선을 마주 꼬아서 잡음을 막을 수 있다.
- 잡음의 원인은 케이블의 주위에서 발생하는 전자파이다.
- 케이블에 영향을 받는 전자파는 두 종류로 나눌 수 있는데, 그 중 하나는 모터, 형광등, CRT 모니터와 같은 기기에서 누설되는 전자파이다.
- 이것은 케이블의 밖에서 오는 것으로 다음과 같이 '선을 꼼'으로써 막을 수 있다.



1. 케이블, 리피터, 허브

트위스트 페어 케이블

- 또 한 가지는 같은 케이블 안의 인접한 신호선에서 누설되는 전자파이다.
- 신호선 안에는 신호라는 전류가 흐르므로 전류에 의해 주위에 전자파가 생긴다.
- 이것이 다른 신호선에 대한 잡음이 되는데, 이러한 잡음에 의한 영향을 크로스토크(crosstalk)라고 한다.
- 이 잡음은 원래 강한 것이 아니지만 거리가 가까운 곳이 문제이다.
- 전자파는 발생 근원에서 떨어지면 확산되어 약해지는데 한 개의 케이블 안에 있는 신호선은 거리가 가까우므로 전자파가 약해지기 전에 인접 신호선에 도달해 버린다.
- 이 때문에 신호선에서 나오는 약간의 전자파가 주위의 신호선에 닿아 여기에서 전류를 발생시키는 것이다.
- 이것을 막는 대책도 신호선을 마주 꼬는 것이다.



1. 케이블, 리피터, 허브

트위스트 페어 케이블

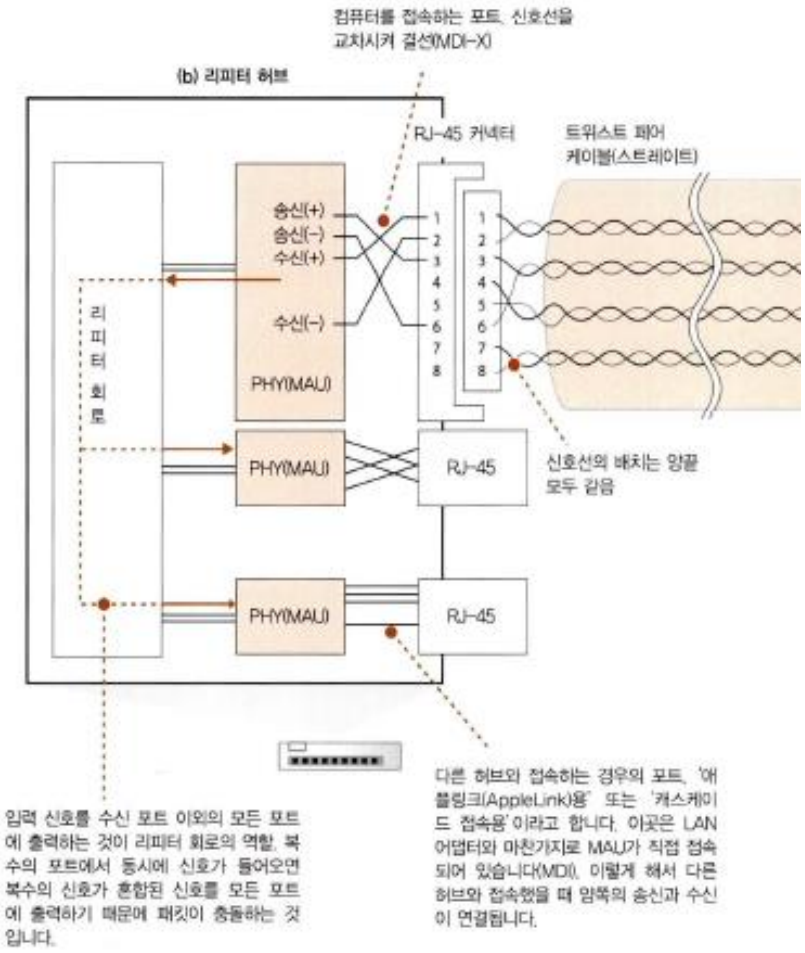
- 신호선을 마주 꼬면 잡음의 영향이 줄어들면서 케이블의 성능이 향상되지만 성능향상의 대책은 이것만이 아니다.
- 신호선 사이의 거리를 유지하기 위해 신호선 사이에 구분판을 넣거나 전자파를 차단하기 위해 금속성의 실드(shield, 차폐)라는 피복을 입히는 등 여러 가지 대책이 마련되어 있다
- 그 결과, 성능이 다른 몇 종류의 케이블이 판매되고 있으며, 카테고리(Category, 범주)라는 척도로 성능을 나타낸다.

카테고리	설명
카테고리 5(CAT-5)	10메가바이트의 이더넷(10BASE-T)과 100메가바이트의 이더넷(100BASE-TX)에 사용하는 것 125MHz까지의 주파수의 신호를 100m까지 전달할 수 있다.
인핸스드 카테고리(CAT-5e)	기가비트 이더넷(1000BASE-T)용으로 만들어진 것 카테고리 5를 개량하여 크로스토크의 특성을 개선했고, 10BASE-T와 100BASE-TX에서 이용할 수 있다.
카테고리 6(CAT-6)	최고 250MHz의 신호를 지원한다. 100BASE-TX라는 사양의 기가비트 이더넷이나 10BASE-T라는 10기가비트 이더넷에 사용하고, 10BASE- T, 100BASE-TX, 1000BASE-T에도 이용할 수 있다.
오그멘티드 카테고리 6	카테고리 6을 개량하고 에일리언 크로스토크라는 특성을 개선한 것. 10GBASE-T, 1000BASE-TX, 1000BASE-T, 100BASE-TX, 10BASE-T에 이용할 수 있다.
카테고리 7(CAT-7)	최고 600MHz의 고속 신호를 지원하는 케이블 10BASE-T, 1000BASE-TX, 1000BASE-TX, 100BASE-TX, 10BASE-T에 이용할 수 있다.

1. 케이블, 리피터, 허브

리피터 허브

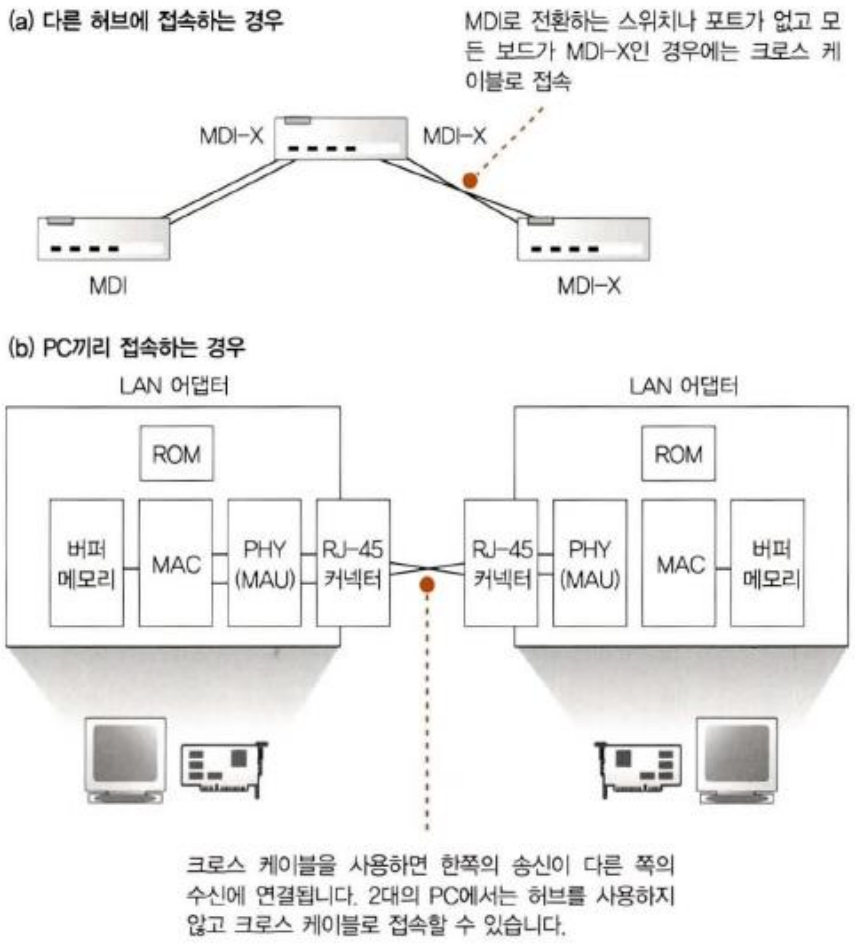
- 신호가 리피터 허브에 도달하면 LAN 전체에 신호가 흩어진다.
- 이더넷의 기본이라는 원리, 즉 전체에 패킷의 신호를 뿌리고 수신처 MAC 주소에 해당하는 기기만 패킷을 수신한다는 원리를 그대로 실현한 것이 리피터 허브이므로 이더넷의 기본에 따라 신호를 뿌리는 것이다.
- 리피터 허브의 내부는 그림과 같다.
- 먼저 각 커넥터의 안쪽에는 LAN 어댑터의 내부에 있는 PHY(MAU) 회로와 역할이 같은 회로가 있다.
- 이것을 LAN 어댑터측과 같이 RJ-45 커넥터에 직접 접속하면 신호를 제대로 수신할 수 없다.
- 제대로 수신하려면 '송신 단자'에서 보낸 신호를 '수신 단자'로 받도록 해야 한다.



1. 케이블, 리피터, 허브

리피터 허브

- 리피터 허브에서 끝의 커넥터에는 MDI/MDI-X와 같이 쓰여있는 전환 스위치가 붙어있는데, 이를 통해 의미를 알 수 있을 것이다.
- MDI는 RJ-45 커넥터와 신호 송 · 수신 회로를 직접 결선한 것으로, MDI-X는 교차하여 결선하는 것을 나타낸다.
- 허브의 커넥터 부분은 보통 MDI-X이므로 허브끼리 접속할 때는 한 쪽을 MDI로 설정해야 한다(그림).

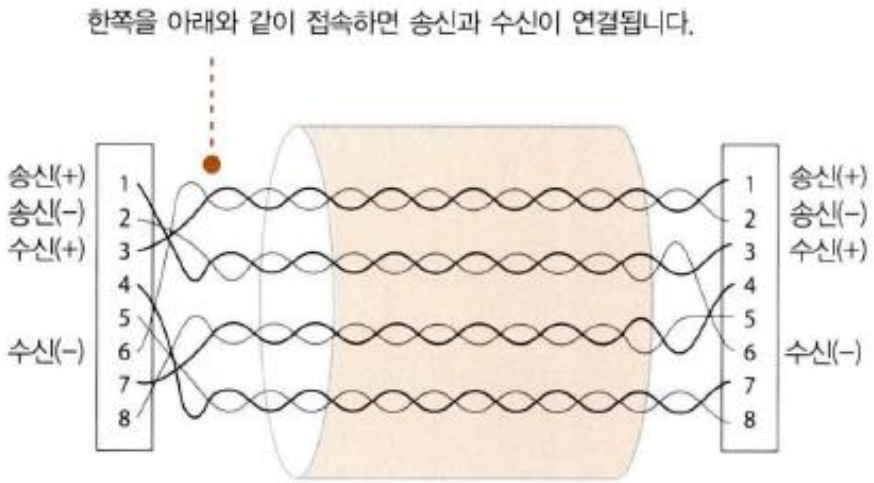


그림에서는 송신과 수신의 신호선을 각각 한 개의 선으로 사용했지만, 실제 신호선은 플러스와 마이너스라는 두 개의 선으로 구성되어 있습니다.

1. 케이블, 리피터, 허브

리피터 허브

- 만약 MDI로 전환하는 스위치가 없고 모든 커넥터가 MDI-X인 경우에는 크로스 케이블로 허브들을 접속한다.
- 크로스 케이블은 송신과 수신 단자가 바뀌어 들어오도록 신호선을 접속한 케이블이다(그림).
- 리피터 허브에서 PHY(MAU) 회로의 수신부에 도달한 신호는 여기부터 리피터 회로에 들어한다.
- 리피터 회로의 기본은 들어오는 신호를 리피터 허브의 커넥터 부분에 뿌리는 데 있다.
- 여기에서 신호의 파형을 다듬고 오류를 억제하도록 연구한 제품도 있지만, 기본은 들어온 신호를 그대로 커넥터 부분에 송출하는 것이다.



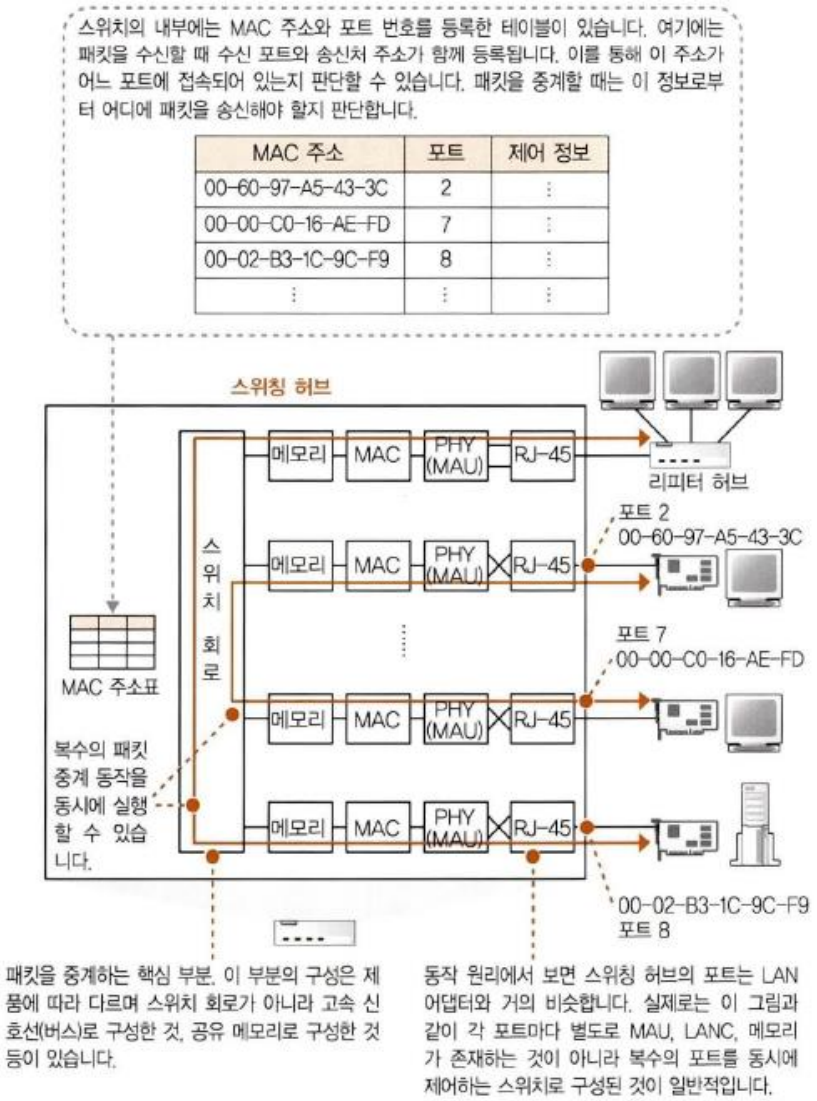
리피터 허브

- 이후 신호는 모든 커넥터에서 나가면서 리피터 허브에 접속한 전체 기기에 도달한다.
- 그리고 신호를 수신한 기기는 맨 앞에 있는 MAC 헤더에 쓰여 있는 수신처 MAC 주소를 조사하여 자신이 수신처에 해당하면 이것을 수신하고, 해당하지 않으면 수신한 신호를 무시한다.
- 이렇게 해서 패킷이 수신처 MAC 주소의 상대에게 도달한다.
- 리피터 회로의 기본은 신호를 그대로 뿌리는 것이므로 잡음의 영향을 받아 변형되고, 데이터가 변화한 것 같은 신호라도 그대로 흘려버린다.
- 이 경우 신호가 다음 기기, 즉 스위칭 허브, 라우터, 서버 등에 도달하여 디지털 데이터로 변환되고, FCS를 검사하는 곳에서 데이터 변화가 판명된 후 변화된 패킷은 폐기된다.
- 그러나 이를 통해 데이터가 없어지는 것은 아니다.
- 패킷을 폐기하면 수신 확인 응답을 되돌려주지 않으므로 프로토콜 스택의 TCP 담당부분이 패킷을 다시 보내기 때문이다.

2. 스위칭 허브의 패킷 중계 동작

스위칭 허브

- 다음은 패킷이 스위칭 허브를 경유하여 흘러 갈 때의 동작이다.
- 스위칭 허브는 이더넷의 패킷을 그대로 목적지를 향해 중계하도록 만들어져 있다.
- 먼저 신호가 커넥터 부분에 도달하여 PHY(MAU) 회로에서 수신되는 부분까지는 리피터 허브와 같다.
- PHY(MAU) 회로에서 케이블을 흐르는 신호의 형식부터 공통의 신호 형식으로 변환한 후 신호는 MAC 회로로 들어간다.
- 그리고 여기에서 디지털 데이터로 변환한 후 패킷의 맨 끝에 있는 FCS를 대조하여 오류의 유무를 검사하고, 문제가 없으면 버퍼 메모리에 저장한다.



2. 스위칭 허브의 패킷 중계 동작

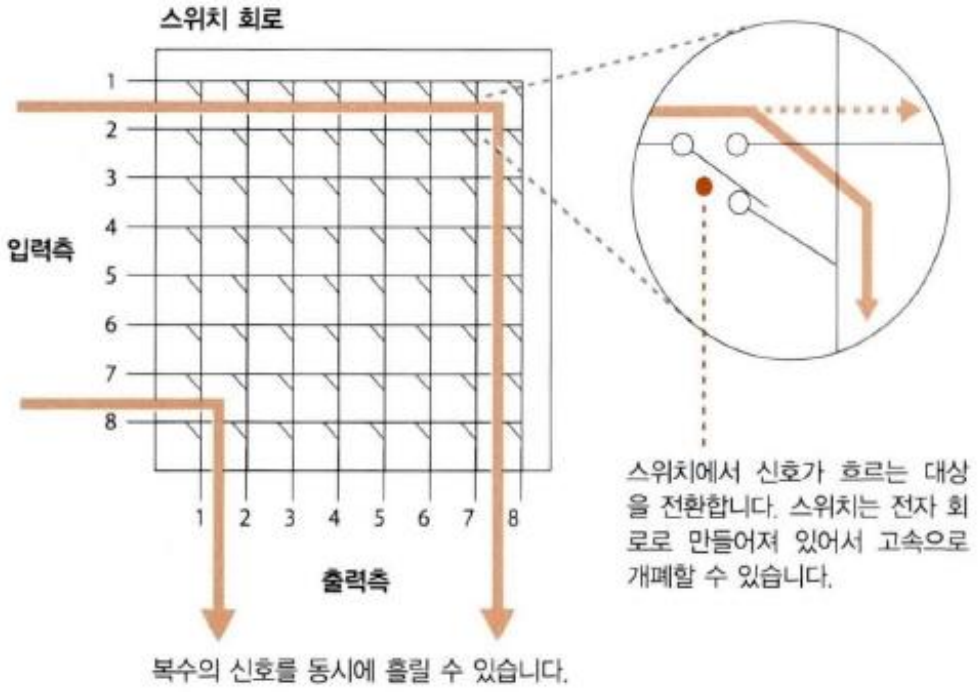
스위칭 허브

- 커넥터와 안쪽에 있는 회로 부분을 포트라고 부르므로 스위칭 허브의 각 포트는 PC의 LAN 어댑터와 거의 같다.
- 그러나 LAN 어댑터와 다른 부분이 있다.
- LAN 어댑터에는 MAC 주소가 할당되어 있어서 수신한 패킷의 수신처 MAC 주소가 자신에게 해당하지 않는 경우에는 패킷을 폐기한다.
- 반면 스위칭 허브의 포트는 수신처 MAC 주소를 검사하지 않고 모든 패킷을 수신하여 버퍼 메모리에 저장하기 때문에 스위칭 허브의 포트에는 LAN 어댑터와 달리 MAC 주소가 할당되어 있지 않다.
- 패킷을 버퍼 메모리에 저장하면 다음에 수신처 MAC 주소와 일치하는 것이 MAC 주소표에 등록되어 있는지 조사한다.
- 이것을 사용하여 수신한 패킷을 어느 포트에서 송신하면 좋을지를 판단한다.

2. 스위칭 허브의 패킷 중계 동작

스위칭 허브

- 스위치 회로는 그림과 같은 구조를 전자 회로로 만든 것으로 이를 통해 입력 포트와 출력 포트를 연결할 수 있다.
- 이 스위치는 전자적으로 개폐를 제어할 수 있고, 이 전자적 개폐를 통해 신호가 흐르는 대상을 제어한다.
- 그리고 입력측은 수신측 포트에, 출력측은 송신측 포트에 각각 접속되어 있다.



2. 스위칭 허브의 패킷 중계 동작

스위칭 허브

- 이 스위치 회로를 경유하여 송신측의 포트에 패킷을 운반하면 MAC 회로나 PHY(MAU) 회로가 송신 동작을 실행하고 케이블에 신호가 흘러간다.
- 이때 송신 동작도 LAN 어댑터의 송신 동작과 같다.
- 이더넷의 규칙에 따라 먼저 아무도 송신중이지 않다는 것을 확인한다.
- 누군가가 송신 중이면 그것이 끝날 때까지 기다린다.
- 그리고 송신 동작이 끝나거나 아무도 송신하지 않으면 소켓을 디지털 데이터에서 신호로 변환하여 송신한다.
- 송신 동작을 하고 있는 사이에 수신 신호를 감시하는 부분도 LAN 어댑터와 같다.
- 송신 동작중에 다른 기기가 보낸 신호가 수신측에 들어오면 패킷이 충돌하므로 재밍 신호를 보낸 후 송신 동작을 중지하고 잠시 기다렸다가 다시 보내는데, 이것도 LAN 어댑터와 같다.

2. 스위칭 허브의 패킷 중계 동작

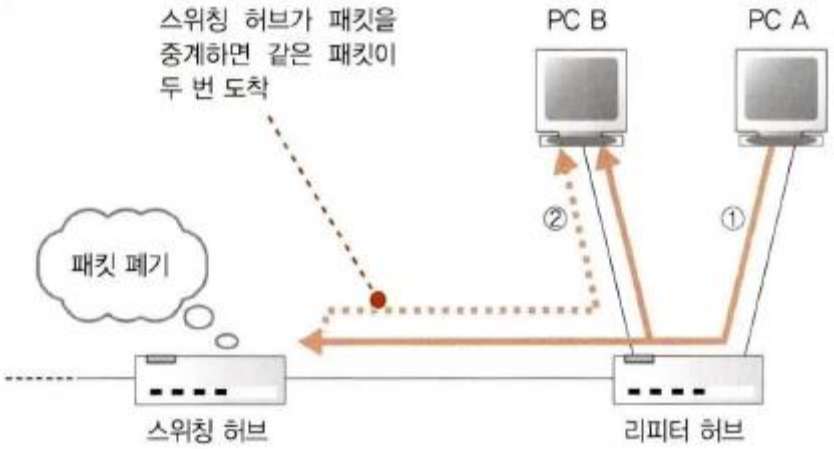
MAC 주소 테이블의 등록 및 갱신

- 스위칭 허브는 패킷을 중계할 때 MAC 주소표의 내용을 갱신하는 동작도 실행한다.
- 갱신 동작은 두 종류가 있는데 그 중 하나는 패킷을 수신했을 때 송신처 MAC 주소를 조사하고 이것을 수신한 입력 포트 번호와 하나의 세트로 MAC 주소표에 등록하는 것이다.
- 패킷이 들어온 포트의 앞에 패킷을 송신한 기기가 있을 것이므로 송신처 주소를 등록해 두면 MAC 주소로 갈 패킷을 수신했을 때 이것이 존재하는 포트에 중계할 수 있다.
- 스위칭 허브는 패킷을 수신할 때마다 이러한 등록 동작을 실행한 후 한 번이라도 패킷을 송신하면 해당 기기의 MAC 주소가 MAC 주소표에 등록된다.
- MAC 주소표에 등록되어 있는 내용을 지우는 또 하나의 동작이 있다.
- 이것은 기기를 이동한 경우의 불편함을 방지하기 위한 것이다.
- 사용하지 않고 일정 시간 경과한 경우 오래된 정보를 MAC 주소표에서 삭제하면 된다.
- MAC 주소표에서 지울 때까지의 시간은 보통 몇 분 정도이므로 오래된 정보가 지워지기 전에 이동한 기기로 갈 패킷이 도착하는 경우도 있다.
- 그러면 패킷은 이전 장소에 중계되어서 통신 동작이 올바르게 이루어지지 않는다.
- 이와 같은 경우 스위칭 허브를 리셋하면 MAC 주소표가 전부 지워지고 새로 정확한 정보가 등록되면서 네트워크는 정상으로 작동할 것이다.

2. 스위칭 허브의 패킷 중계 동작

예외적인 동작

- 주소표에서 일치하는 행을 찾아냈을 때 주소표에 등록되어 있는 송신 포트가 패킷을 수신한 포트와 같다고 가정해 보자.
- 이러한 상황은 그림과 같이 스위칭 허브에 리피터 허브가 접속되어 있는 경우에 발생한다.



- MAC 주소표에 수신처 MAC 주소와 일치하는 주소가 등록되어 있지 않은 경우도 있다.
- 주소의 기기에서 패킷이 한 번도 스위칭 허브에 도착하지 않은 경우나 어느 정도 시간이 경과하여 MAC 주소표에서 삭제된 경우이다.
- 이 경우에는 어느 포트에서 송신해야 할지 판단할 수 없으므로 패킷을 수신한 포트 이외의 전체 포트에서 패킷을 송신한다.

2. 스위칭 허브의 패킷 중계 동작

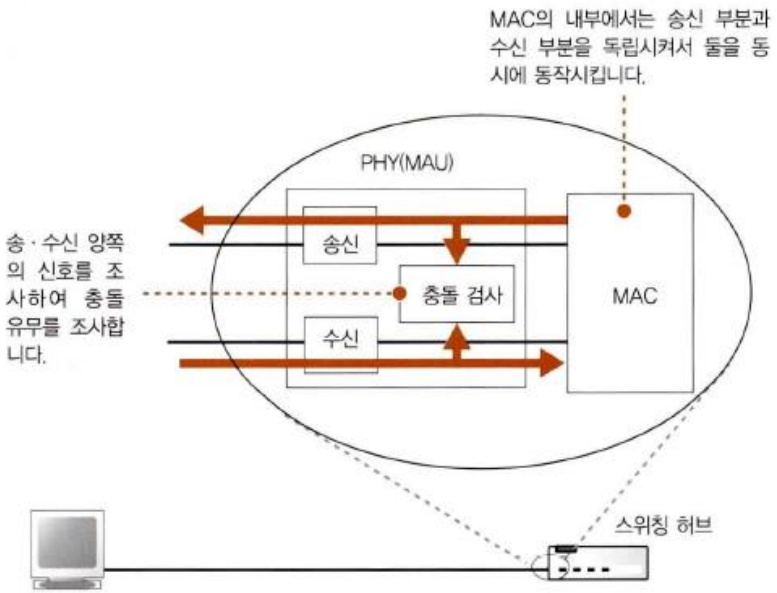
전이중 모드

- 전이중 모드, 즉 송신과 수신을 동시에 실행할 수 있는 성질도 리피터 허브에는 없는 스위칭 허브의 특징이다.
- 리피터 허브를 사용하는 경우 여러 대의 컴퓨터가 동시에 송신 동작을 개시하면 리피터 허브의 내부에서 신호가 뒤섞여서 신호가 파괴된다.
- 이것은 충돌이라는 현상으로 이더넷의 중요한 성질이지만, 스위칭 허브를 사용하면 이러한 사태가 일어나지 않는다.
- 트위스트 페어 케이블의 신호선은 송신용과 수신용으로 나뉘어져 있으므로 트위스트 페어 케이블의 송 · 수신 도중에 신호가 충돌하지 않는다.
- 케이블이 연결된 대상, 즉 스위칭 허브의 포트 부분이나 LAN 어댑터에 있는 PHY(MAU) 회로와 MAC 회로의 내부도 송신과 수신이 나뉘어져 있어서 신호가 따로 흐르기 때문에 충돌하지 않는다.
- 충돌이 일어나지 않으면 송신과 수신을 동시에 실행해도 상관없다.
- 그러나 이더넷에 신호가 흐르고 있을 때는 이것이 끝나기를 기다렸다가 송신 동작을 실행하므로 그대로는 송신과 수신을 동시에 실행할 수 없다.

2. 스위칭 허브의 패킷 중계 동작

전이중 모드

- 그래서 이더넷의 규칙을 개정하여 신호가 흐르고 있어도 상관하지 않고 송신해도 좋다는 동작 모드를 새로 추가했다.
- 동시에 이 동작 모드로 동작할 때는 신호의 충돌을 검출하는 회로를 무효화하기로 했는데 (그림), 이것이 '전이중'이라는 동작 모드이다.
- 전이중 모드는 송신할 때 신호가 흐르고 있어도 이것이 끝나기를 기다릴 필요가 없으므로 그만큼 반이중 모드보다 빠르게 동작한다.
- 또한 전이중 모드는 양방향으로 동시에 송신할 수 있으므로 송신할 수 있는 데이터 양의 상한선도 높아서 성능이 좋다.



2. 스위칭 허브의 패킷 중계 동작

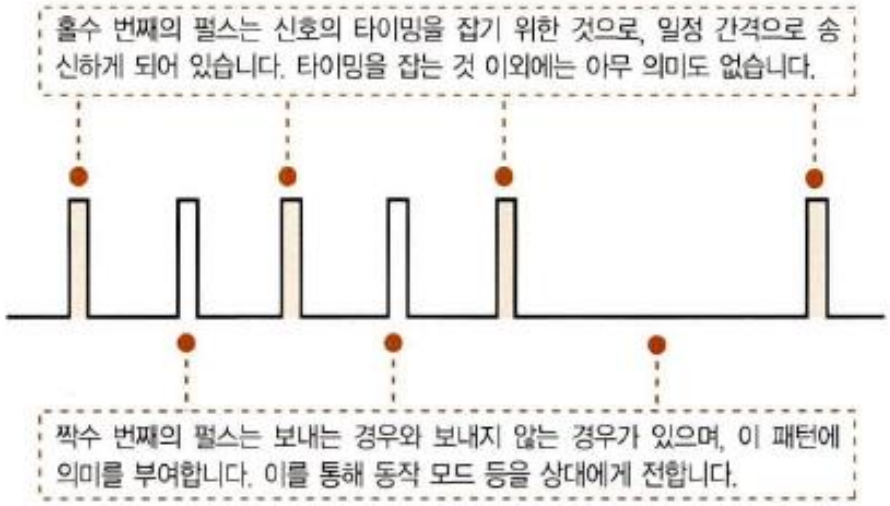
자동 속도 조정

- 전이중 모드가 등장함에 따라 전이중 모드와 반이중 모드를 전환할 필요가 생겼다.
- 전이중 모드가 등장한 후 한동안 수동으로 동작 모드를 전환했지만 불편하므로 나중에 동작 모드를 자동으로 전환하는 기능이 나왔다.
- 동작모드 뿐만아니라 상대의 전송속도를 검출하여 전송 속도도 자동으로 전환하는데, 이 기능을 자동 조정(auto negotiation)이라고 한다.
- 이더넷은 데이터가 흐르고 있지 않을 때는 링크 펄스라는 펄스형의 신호를 흘린다.
- 데이터가 흐르고 있지 않을 때 이 신호를 흘려서 항상 무언가의 신호가 흐르게 되고, 이것을 통해 상대가 올바르게 작동하는지, 케이블이 단선되지 않았는지 등의 사항을 확인할 수 있다.
- 이더넷의 기기에는 커넥터 주변에 초록 LED의 표시등이 붙어있으며 이것을 통해 펄스형 신호가 흐르는 지를 나타낸다.
- 이 표시등이 켜져있으면 PHY(MAU) 회로와 케이블에는 이상이 없는 것이다.

2. 스위칭 허브의 패킷 중계 동작

자동 속도 조정

- 트위스트 페어 케이블을 사용하는 이더넷이 최초로 만들어졌을 때는 펄스 신호를 일정 간격으로 보낸다는 규정밖에 없었다.
- 따라서 동작 확인용으로만 사용했는데, 나중에 그림과 같이 특정 패턴으로 펄스 신호를 송신하여 자신의 상황을 상대에게 전하는 방법이 고안되었다.
- 자동 조정 기능은 이 방법을 이용한다.
- 즉 이 패턴에 의해 지원 가능한 모드와 전송 속도를 서로 통지하고 그 중에서 최적의 조합을 선택하여 각각 자기 자신을 설정한다.



2. 스위칭 허브의 패킷 중계 동작

자동 속도 조정

- 표와 같이 LAN 어댑터는 모든 속도와 동작 모드를 지원하고 스위칭 허브는 100메가비트/초의 전이중 모드만 지원한다고 가정해보자.

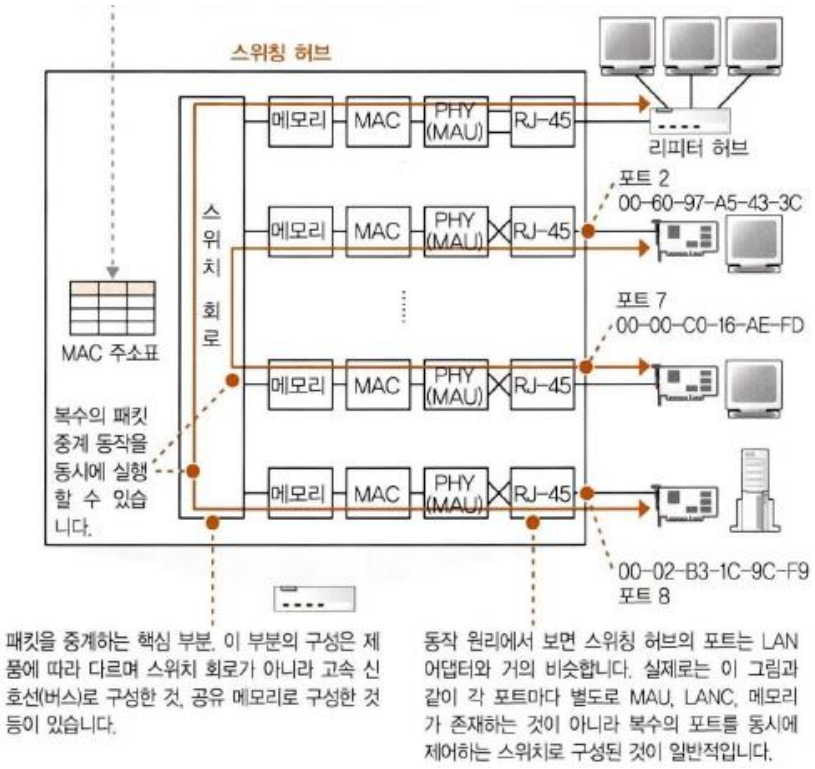
전송 속도, 동작 모드	LAN 어댑터	스위칭 허브
1기가비트/초의 전이중	○	×
1기가비트/초의 반이중	○	×
100메가비트/초의 전이중	○	○
100메가비트/초의 반이중	○	○
10메가비트/초의 전이중	○	○
10메가비트/초의 반이중	○	○

- 두 기기의 전원을 켜고 하드웨어의 초기화 동작이 끝나면 자체에서 지원하는 속도와 동작 모드를 펄스 신호로 보내기 시작하다.
- 그러면 신호가 상대에게 도착하며 도착한 펄스의 패턴을 읽고 상대가 어느 모드를 지원하는지 조사한다.
- 모드에는 우선 순위가 결정되어 있고 우선 순위가 높은 것부터 차례대로 조사하면서 자신과 상대 모두가 지원하는 것을 찾는다.

2. 스위칭 허브의 패킷 중계 동작

스위칭 허브의 복수 중계

- 스위칭 허브는 수신처 MAC 주소의 기기가 존재하는 포트 이외에는 송신 동작을 실행하지 않으므로 다른 포트는 빈 상태가 된다.
- 그림과 같이 맨 위와 맨 아래 포트에 패킷이 흐르고 있을 때 다른 포트는 빈 상태가 된다.
- 비어있으므로 여기에서 별도의 패킷을 흘릴 수 있으며, 이렇게 해서 동시에 여러 개의 패킷을 중계할 수 있다.
- 리피터 허브쪽은 들어온 신호를 모든 포트에서 뿌리므로 동시에 두 개 이상의 신호가 들어오면 패킷이 충돌하기 때문에 복수의 신호를 동시에 흘릴 수 없다.
- 따라서 기기 전체에서 중계할 수 있는 패킷의 수는 스위칭 허브쪽이 리피터 허브쪽보다 많다.



3. 라우터의 패킷 중계

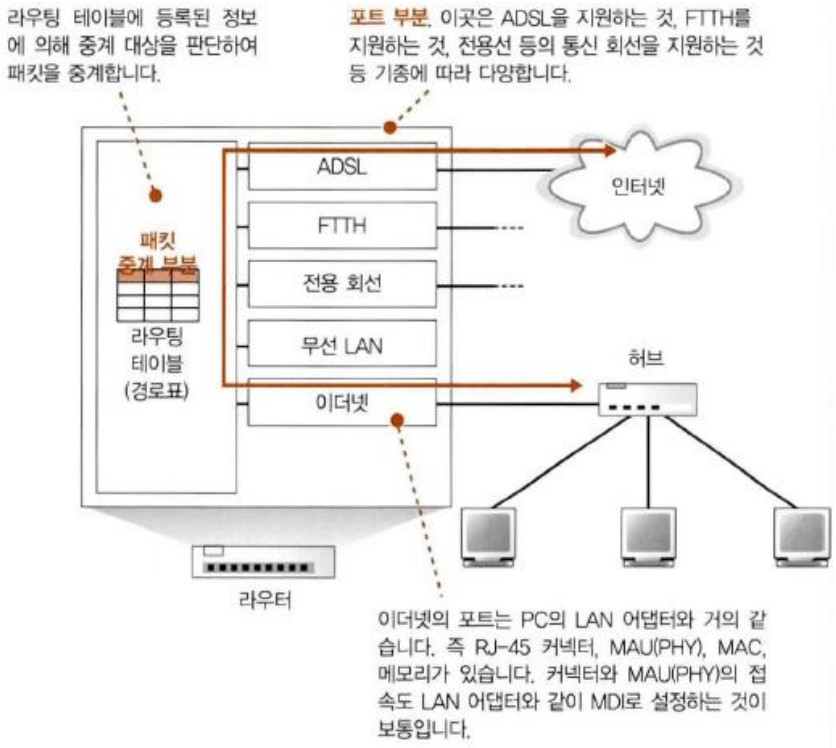
라우터의 기본

- 리피터 허브나 스위칭 허브를 경유한 패킷은 결국 라우터에 도착하고, 라우터에서 다음 라우터로 중계될 것이다.
- 이러한 중계의 원리는 스위칭 허브와 비슷하다.
- 중계 대상을 등록한 표를 보고 패킷을 어디로 중계해야 할지 판단하는 부분이 공통이기 때문이다.
- 그러나 구체적인 동작은 스위칭 허브와 다른데, 이것은 라우터의 바탕이 되는 IP라는 개념이 스위칭 허브의 바탕이 되는 이더넷과 다르기 때문이다.

3. 라우터의 패킷 중계

라우터의 기본

- 라우터의 내부 구조는 그림에 나타나 있다.



- 상당히 간략화했지만 중계 부분과 포트 부분이라는 두 부분으로 구성된다.
- 그리고 중계 부분이 패킷의 중계 대상을 판단하는 동작을 담당하고, 포트 부분이 패킷을 송 · 수신하는 동작을 담당한다.

3. 라우터의 패킷 중계

라우터의 기본

- 라우터의 내부 구조를 알면 어떻게 동작하는지 대략 알 수 있다.
- 먼저 포트 부분에서 패킷을 수신하는데 이 동작은 포트 부분의 통신 기술의 규칙을 따른다.
- 포트 부분이 이더넷이라면 이더넷의 규칙에 따라 동작하고, 무선 LAN이라면 무선 LAN의 규칙대로 동작하며 통신 회선이면 통신 회선의 규칙에 따라 동작한다.
- 포트 부분의 하드웨어에 의뢰하여 패킷을 수신한다고 생각하면 되는데, 중계 부분에서 받은 패킷의 IP 패킷에 기록되어 있는 수신처 IP 주소와 중계 대상을 등록한 표를 대조하여 중계 대상을 판단한다.
- 그리고 중계 대상측의 포트로 패킷을 옮기고 포트 부분의 하드웨어 규칙에 따라 패킷 송신 동작을 실행한다.

3. 라우터의 패킷 중계

라우터의 기본

- 앞에서 포트 부분의 통신 기술의 규칙에 따라 패킷을 송 · 수신한다고 설명했는데, 이것은 포트 부분이 패킷의 송신처 또는 수신처가 되어 패킷을 송 · 수신한다는 것이다.
- 예를 들어 포트가 이더넷인 경우 라우터의 포트에는 MAC 주소가 할당되어 이더넷의 송신처나 수신처가 된다.
- 포트에는 IP 주소도 할당되므로 이런 의미에서도 컴퓨터의 LAN 어댑터와 같다.
- 그러고 패킷을 중계할 때는 먼저 라우터의 포트 부분이 수신처가 되어 이더넷의 패킷 수신 동작을 실행한다.
- 중계 대상을 조사한 후 이번에는 포트 부분이 송신처가 되어 이더넷의 패킷 송신 동작을 실행하는데 이곳이 스위칭 허브와 다른 부분이다.
- 즉 스위칭 허브는 들어온 패킷을 전송하기만 하고 자신이 송신처나 수신처가 되지 않는다.

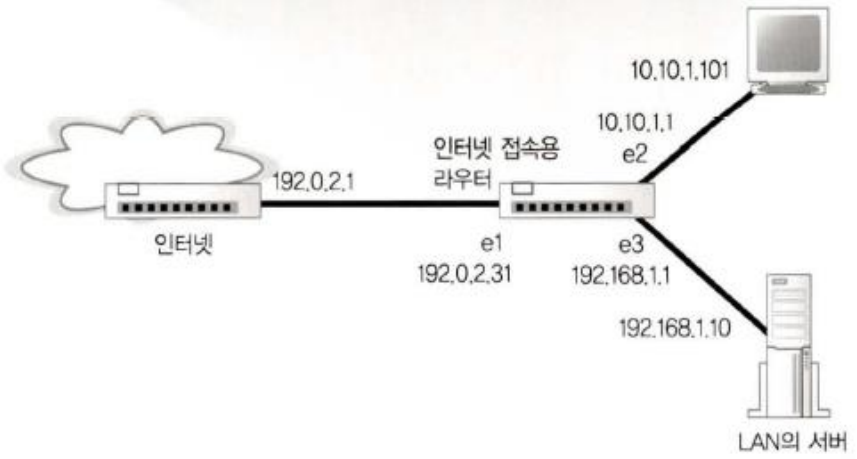
3. 라우터의 패킷 중계

경로표에 등록된 정보

- 중계 부분의 개념, 즉 테이블을 사용하여 중계 대상을 조사한다는 개념은 비슷하지만, 구체적인 동작은 스위칭 허브와 다르다.
- 스위칭 허브가 MAC 헤더에 기록되어 있는 수신처 MAC 주소로 중계 대상을 판단하지만, 라우터는 IP 헤더에 기재되어 있는 수신처 IP 주소로 중계 대상을 판단하기 때문이다.
- 취급하는 주소가 다르므로 중계 대상의 주소를 등록하는 테이블의 내용도 다르다.
- 라우터의 테이블은 라우팅 테이블 또는 경로표라고 부르며, 여기에 그림과 같은 정보를 등록한다.
- 주소 비교 동작을 실행할 때 네트워크 번호의 비트 수를 판단해야 하므로 경로표에는 넷마스크 항목도 마련되어 있으며, 이 값에 따라 네트워크 번호의 비트 수를 판단한다.

라우터의 경로표

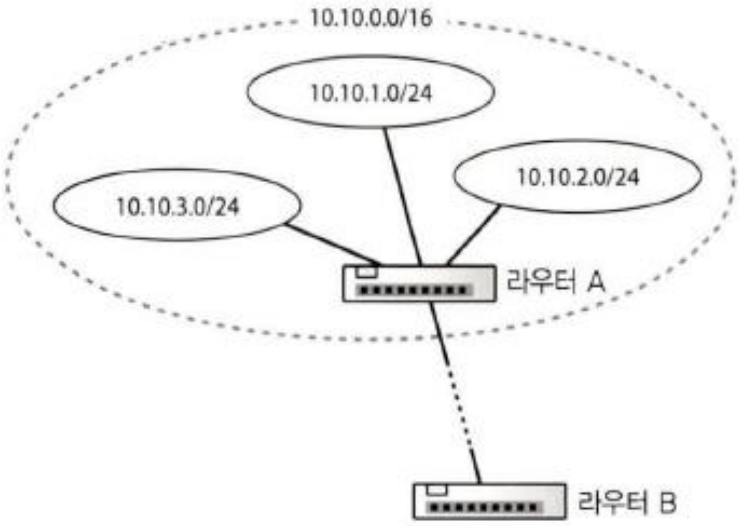
수신처 (Destination)	넷마스크 (Netmask)	게이트웨이 (Gateway)	인터페이스 (Interface)	메트릭(Metric)
10.10.1.0	255.255.255.0	——	e2	1
10.10.1.101	255.255.255.255	——	e2	1
192.168.1.0	255.255.255.0	——	e3	1
192.168.1.10	255.255.255.255	——	e3	1
0.0.0.0	0.0.0.0	192.0.2.1	e1	1



3. 라우터의 패킷 중계

경로표에 등록된 정보

- '수신처' 항목에는 서브넷을 나타내 는 IP 주소가 등록되었다고 설명했는데 그렇지 않은 경우도 있다.
- 실제로 서브넷에 할당된 넷마스크의 값과 경로표에 등록된 넷마스크의 값이 다를 수도 있다.
- 주소 집약이라는 개념을 이용하면 몇 개의 서브넷을 모아서 한 개의 서브넷으로 간주한 후 묶은 서브넷을 경로표에 등록할 수 있다.
- 예를 들어 그림과 같이 10.10.1.0/24, 10.10.2.0/24, 10.10.3.0/24라는 3개의 서브넷이 있다고 가정하고, 이 서브넷에 라우터 B에서 패킷을 건네주는 것을 생각해 보자.



3. 라우터의 패킷 중계

경로표에 등록된 정보

- 이때 라우터 B의 경로표에 3개의 서브넷을 별도로 등록하는 것이 원칙이다.
- 그러나 이 예에서는 어느 서브넷에 패킷을 건네줄 때도 라우터 A에 패킷을 중계 하는 것으로 바뀌지 않으므로 3개의 서브넷을 일괄적으로 통합한 10.10. 0.0/16 이라는 서브넷이 있는 것으로 간주한다.
- 그리고 이것을 경로표에 등록해도 패킷 중계 동작을 정확하게 실행할 수 있다.
- 이렇게 하여 경로표를 등록하는 건수를 줄일 수 있는데, 이것이 주소 집약의 개념이다.
- 이 주소 집약을 실행할 때 복수의 서브넷을 하나인 것으로 간주하기 위해 넷마스크 값을 변경하여 경로표에 등록하고, '수신처' 항목에 집약한 주소를 등록한다.
- 이것과는 반대로 한 개의 서브넷을 세분화하여 경로표에 등록하고, 복수의 서브넷이 있는 것처럼 보이는 경우도 있다.
- 결국 경로표의 '넷마스크' 항목은 경로표에서 수신처를 대조할 때 비교 동작을 실행하는 비트 수를 나타내는 데 불과하다.
- 또한 '수신처' 항목에 등록된 주소가 실제 서브넷에 할당한 네트워크 번호와 다른 경우도 있다.
- 그러나 라우터는 제대로 동작하므로 걱정할 필요는 없다.

3. 라우터의 패킷 중계

경로표에 등록된 정보

- 이 방법을 사용한다면 호스트 번호 부분에 값이 들어있는 개별 컴퓨터를 나타내는 주소를 '수신처' 항목에 등록할 수 있다.
- 넷마스크 값을 255.255.255.255, 즉 32비트를 전부 1로 만들면 된다.
- 이렇게 하면 호스트 번호 부분의 비트 값을 전부 0으로 한 서브넷을 나타내는 주소와 호스트 번호 부분에 값이 들어있는 개별 컴퓨터를 나타내는 주소를 같은 방법으로 취급할 수 있다.
- 넷마스크의 오른쪽에 있는 '게이트웨이' 항목과 '인터페이스' 항목은 패킷의 중계 대상을 나타낸다.
- '수신처' 항목과 '넷마스크' 항목에서 해당 행을 찾아내면 '인터페이스' 항목에 등록되어 있는 인터페이스(포트)에서 '게이트웨이' 항목에 등록되어 있는 IP 주소를 가진 라우터에 대해 패킷을 중계한다.

3. 라우터의 패킷 중계

경로표에 등록된 정보

- 마지막의 메트릭은 수신처 IP 주소에 기록되어 있는 목적지가 가까운지, 먼지를 나타낸다
- 여기에 등록되어 있는 수가 작으면 목적지가 가까이에 있고, 이 수가 크면 먼 것을 나타낸다.
- 또한, 이 경로표에 경로 정보를 등록하는 원리도 라우터와 스위칭 허브에서 서로 다르다.
- 스위칭 허브는 패킷 중계 동작의 일환으로 MAC 주소 테이블에 정보를 등록하는 동작을 실행하지만, 라우터가 경로표에 경로 정보를 등록하거나 갱신하는 동작은 패킷을 중계하는 동작과 분리되어 있다.
- 즉 패킷을 중계할 때 경로표의 내용에 손대지 않는다.
- 라우터의 경로표에 경로 정보를 등록하는 방법은 다음과 같이 크게 두 가지로 분류할 수 있다.
  a. 사람이 수동으로 경로 정보를 등록/갱신
  b. 라우팅 프로토콜이라는 구조를 사용하여 라우터들끼리 경로 정보를 교환하고 라우터가 자체에서 경로표에 등록

- (b)는 한 가지의 프로토콜이 아니라 RIP, OSPF, BGP라는 라우팅 프로토콜처럼 복수의 프로토콜이 존재한다.

3. 라우터의 패킷 중계

라우터의 패킷 수신 동작

- 라우터의 포트에는 여러 가지 변형이 있는데, 여기에서는 이더넷의 포트에서의 패킷 수신 동작에 초점을 맞추어 보자.
- 이더넷의 포트 부분의 구조는 PC의 LAN 어댑터와 거의 같으므로 패킷을 수신하여 버퍼 메모리에 저장하는 부분까지의 동작도 LAN 어댑터와 거의 같다.
- 먼저 신호가 커넥터 부분에 도착하면 안쪽에 있는 PHY(MAU) 회로와 MAC 회로에서 신호를 디지털 데이터로 변환한다.
- 그리고 패킷 끝부분의 FCS를 대조하여 오류의 유무를 점검하고 정상이면 MAC 헤더의 수신처 MAC 주소가 자신에게 해당하는지 조사하여 해당하면 패킷을 수신 버퍼 메모리에 저장한다.
- 여기에서 수신처 MAC 주소에 자신이 해당하지 않을 경우에는 패킷을 폐기한다.
- 자신이 수신처에 해당하지 않는 경우 도착한 패킷은 다른 기기가 수신할 것이므로 이것을 수신하면 이더넷의 규칙에 위반되기 때문이다.

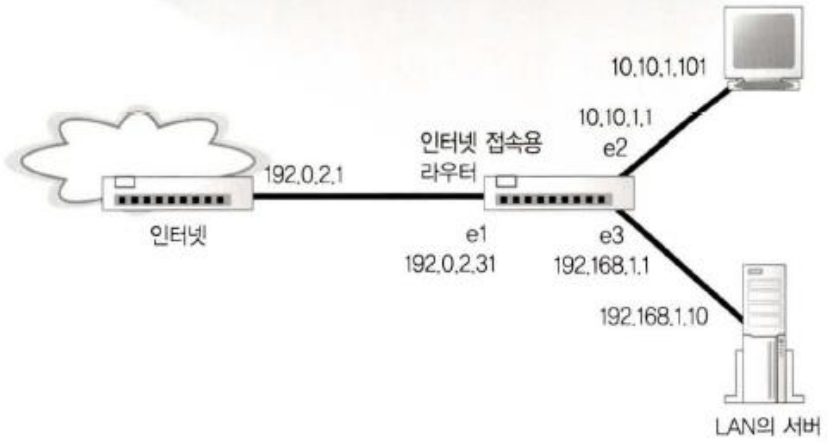
3. 라우터의 패킷 중계

경로표를 이용한 출력포트 조회

- 라우터는 패킷 수신 동작이 끝나면 맨 앞의 MAC 헤더를 폐기한다.
- MAC 헤더의 역할은 이 라우터에 패킷을 건네주는 것이다.
- 이것은 MAC 헤더의 수신처 MAC 주소 항목에 이 라우터의 포트에 할당한 MAC 주소가 기록된 것을 보고 알 수 있다.
- 그러므로 패킷을 수신하면 역할이 끝나기 때문에 MAC 헤더를 폐기하는 것이다.
- MAC 헤더의 뒤에 있는 IP 헤더의 내용을 보고 패킷 중계 동작에 들어간다.
- 중계 동작에는 몇 단계가 있는데 우선 경로표에서 중계 대상을 조사한다.
- 이 동작은 구체적인 예를 보는 것이 이해하기 쉬우므로 그림과 같은 상황에서 10.10.1.101인 PC의 경우 192.168.1.10이라는 서버에 보낸 패킷이 라우터에 들어온 것으로 가정하자.

라우터의 경로표

수신처 (Destination)	넷마스크 (Netmask)	게이트웨이 (Gateway)	인터페이스 (Interface)	메트릭(Metric)
10.10.1.0	255.255.255.0	——	e2	1
10.10.1.101	255.255.255.255	——	e2	1
192.168.1.0	255.255.255.0	——	e3	1
192.168.1.10	255.255.255.255	——	e3	1
0.0.0.0	0.0.0.0	192.0.2.1	e1	1



3. 라우터의 패킷 중계

경로표를 이용한 출력포트 조회

- 중계 대상을 조사할 때 가장 먼저 수신한 패킷의 수신처 IP 주소와 경로표의 '수신처' 항목을 조사하여 해당하는 행을 찾는다.
- 이때 앞에서 설명한 것처럼 32비트 전부를 비교하는 것은 아니다.
- '넷마스크' 항목에 등록된 값에서 네트워크 번호의 비트 수를 판단하여 네트워크 번호 부분만 비교한다.
- 예를 들어 그림의 3행을 조사한다면 '넷마스크' 항목은 255.255.255.0이므로 '수신처' 항목의 왼쪽에서 24비트 부분만 조사한다.
- 왼쪽부터 24비트 부분을 조사하면 패킷의 수신처 IP 주소는 192.168.1이고, 경로표의 '수신처' 항목도 192.168.1로서 둘이 일치하므로 이 행이 중계 대상의 후보라고 생각하면 된다.

3. 라우터의 패킷 중계

경로표를 이용한 출력포트 조회

- 이렇게 해서 해당하는 것을 찾으면 복수의 후보가 발견될지도 모른다.
- 이 예라면 3, 4, 5행의 3개가 해당된다.
- 그러면 네트워크 번호의 비트 수가 가장 긴 것을 찾는데, 네트워크 번호의 비트 수가 길면 호스트 번호의 비트 수가 짧아진다.
- 호스트 번호의 비트 수가 짧다는 것은 호스트 번호로 할당 가능한 번호의 수가 적다는 것이다.
- 이것은 여기에 있는 서브넷에 접속 가능한 대수가 적다는 뜻이므로 서브넷이 작다는 것과 같은 의미이며, 그만큼 범위가 축소된다.
- 그러므로 이 방식을 선택하는 쪽이 중계 대상을 정확하게 판단할 수 있다.
- 그림의 3행은 192.168.1.0/255.255.255.0이라는 '서브넷'을 나타내며, 4행은 서브넷 안에 있는 192.168.1.10/255.255.255.255 라는 '서버'를 나타낸다.
- 서버가 속한 서브넷을 나타내는 주소보다 서버 자체를 나타내는 주소쪽이 범위가 축소되므로 4행을 선택한 것이다.
- 이렇게 해서 후보가 1개만 남으면 이것을 중계 대상으로 선택한다.

3. 라우터의 패킷 중계

경로표를 이용한 출력포트 조회

- 네트워크 번호의 길이가 같은 것이 여러 행 존재하는 경우도 있다.
- 라우터의 고장이나 케이블의 단선 등을 고려하여 우회로를 두는 경우가 해당되는데 이러한 경우에는 메트릭 값으로 판단한다.
- 메트릭 값이 작은 쪽이 가까이 있는 것을 의미하므로 값이 작은 쪽을 중계 대상으로 선택한다.
- 이 예와 달리 해당하는 행이 한 개도 발견되지 않는 경우도 있다.
- 이 경우 라우터는 패킷을 폐기하고 ICMP 메시지로 송신처에 이 사실을 통지한다.
- 이것이 스위칭 허브와 다른 부분인데 그 이유는 가정하는 네트워크의 규모 때문이다.
- 스위칭 허브는 많아야 수천 대 정도의 그다지 크지 않은 네트워크를 가정하여 만든 것이다.
- 수천 대 정도의 규모인 경우 중계 대상이 발견되지 않으면 모든 포트에 패킷을 뿌린다는 거친 방법으로도 문제를 일으키지 않는다.
- 한편 라우터가 가정하는 네트워크, 즉 인터넷의 규모는 헤아릴 수 없이 큰다.
- 그래서 모두가 중계 대상을 모르는 패킷을 뿌린다면 대량의 패킷이 뿌려지기 때문에 네트워크가 혼잡해진다.
- 그러므로 라우터는 중계 대상이 분명하지 않은 패킷을 폐기하는 것이다.

3. 라우터의 패킷 중계

기본 경로

- 이번에는 라우터에 중계 대상을 전부 등록해야 하는 상황이 된다.
- 회사나 가정의 LAN만 있다면 별로 문제가 되지 않겠지만, 인터넷의 중계 대상은 20만을 초과하므로 이것을 전부 등록하는 것은 보통 일이 아니다.
- 그러나 걱정하지 않아도 된다.
- 앞에 나온 그림의 경로표에서 마지막 I행이 중계 대상을 전부 등록한 것과 같은 역할이기 때문이다.
- 이 행은 넷마스크가 0.0.0.0으로 되어 있는데 이것이 중요한 부분이다.
- '넷마스크' 항목이 0.0.0.0이라는 것은 패킷의 수신처 IP 주소와 경로표의 '수신처' 항목을 비교할 때의 비트 수가 0이라는 것이므로 비교 동작을 실행하지 않아도 된다.
- '넷마스크' 항목을 0.0.0.0으로 하면 모든 주소에 일치하기 때문이다.
- 이렇게 해서 중계 대상이 분명하지 않다는 사태가 발생하지 않는다.

3. 라우터의 패킷 중계

기본 경로

- 이 행의 '게이트웨이' 항목에 인터넷으로 나가는 라우터를 등록해 두면 다른 행에 해당하는 것이 없는 경우에는 패킷을 그곳으로 중계한다.
- 이 행을 기본 경로라고 하며 여기에 등록한 라우터를 기본 게이트웨이라고 한다.
- PC의 TCP/IP 설정 화면에 있는 '기본 게이트웨이' 라는 항목과 같은 의미이다.
- PC에도 라우터와 같이 경로표가 있고 기본 게이트웨이에 입력한 값이 경로표의 기본 게이트웨이로 등록된 것이다.
- 이렇게 해서 '수신처' 항목에 서브넷을 나타내는 IP 주소와 개별 컴퓨터를 나타내는 IP 주소가 뒤섞였어도 같은 방법으로 중계 대상을 검색할 수 있다.
- 또한 중계 대상이 분명하지 않은 사태도 방지할 수 있다.

3. 라우터의 패킷 중계

패킷의 유효 기한

- 경로표에서 중계 대상을 찾아내면 패킷을 출력측의 포트로 옮기고 여기에서 송신하는데, 라우터에는 그 전에 몇 가지 해야 할 일이 있다.
- 우선 TTL(Time To Live, 생존 기간) 이라는 IP 헤더의 필드를 갱신하는 것이다.
- TTL이란 필드는 패킷의 생존 기간을 나타낸다.
- 라우터를 경유할 때마다 이 값을 1씩 줄이다가 이 숫자가 0이 되면 패킷의 생존 기간이 만료되는 것으로 간주하여 패킷을 폐기한다.
- 이 원리는 패킷이 같은 장소를 뱅글뱅글 순환하는 사태를 막기 위한 것이다.
- 경로표에 중계 대상이 정확하게 등록되어 있으면 이러한 사태가 일어나지 않는다.
- 하지만 경로표에 등록된 정보에 오류가 있거나 기기의 고장 등으로 우회로로 전환될 때 일시적으로 경로가 혼란에 빠지면 이러한 사태에 빠진다.
- 송신처가 처음 패킷을 송신할 때 64 또는 128이라는 값을 설정하고 나서 그 수만큼만 라우터를 경유하면 패킷의 수명이 다한 것으로 간주한다.
- 현재의 인터넷은 지구의 반대편까지 액세스해도 경유하는 라우터 수가 많아야 수십 개 정도이다.
- 따라서 패킷이 계속 순환하지 않으면 수명이 다하기 전에 목적지에 도착할 것이다.

3. 라우터의 패킷 중계

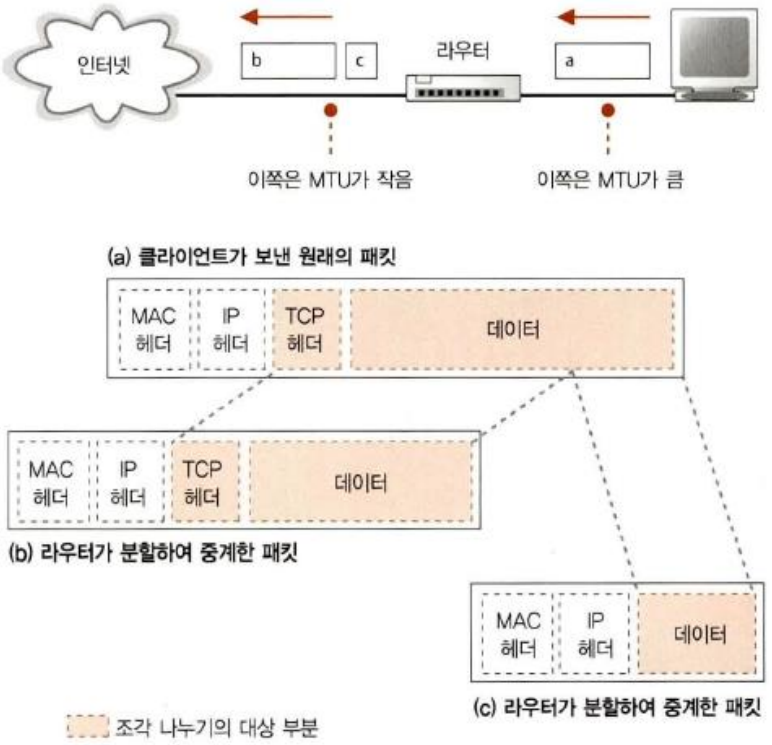
조각 나누기

- 라우터의 포트 부분은 이더넷뿐만 아니라 이더넷 이외의 LAN이나 통신 회선의 경우도 있다.
- 이 회선이나 LAN의 종류에 따라 패킷의 최대 길이가 달라지므로 출력 포트측의 패킷의 최대 길이가 입력측보다 작은 경우도 있다.
- 패킷의 최대 길이는 같아도 여분으로 헤더를 부가해서 패킷의 실질적인 길이가 짧아지는 경우도 있다.
- ADSL이나 FTTH 등 이른바 광대역 액세스 회선에서 PPPoE 프로토콜을 이용하는 경우가 그 예이다.
- 어느 경우든지 중계하는 패킷의 크기가 출력측의 패킷 최대 길이를 초과하면 그대로는 패킷을 송신할 수 없다.
- 이 경우에는 IP 프로토콜에 규정된 조각 나누기(fragmentation)라는 방법을 사용하여 패킷을 분할하고, 패킷의 길이를 짧게 만든 후 중계한다.
- 조각나누기는 TCP가 데이터를 조각으로 분할하는 것과 다르다.
- TCP의 데이터 분할은 패킷에 데이터를 저장하기 전에 이루어진다.
- 반면 조각 나누기쪽은 패킷이 만들어진 후에 패킷을 분할하는 것을 가리킨다.

3. 라우터의 패킷 중계

조각 나누기

- 조각 나누기의 동작은 다음과 같이 이루어진다(그림).
- 먼저 출력측의 MTU를 조사하여 중계하는 패킷을 그대로 출력측에서 송신할 수 있는지 조사한다.
- 패킷의 최대 길이는 포트의 종류에 따라 결정되므로 여기에서 헤더의 길이를 빼서 MTU를 산출하고 중계하는 패킷의 길이와 비교한다.
- 그리고 출력측의 MTU가 충분히 커서 분할하지 않아도 송신할 수 있으면 분할하지 않는다.
- 출력측의 MTU가 작은 경우에는 여기에 저장할 수 있는 크기로 패킷을 분할하는데 그 전에 IP 헤더의 플래그 필드를 조사하여 분할해도 좋을지 확인한다.



3. 라우터의 패킷 중계

조각 나누기

- 플래그 필드가 분할 불가로 되어 있으면 분할할 수 없으므로 패킷을 폐기하고 ICMP 메시지로 송신처에 통지한다.
- 그렇지 않으면 출력측의 MTU에 맞춰 데이터 부분을 맨 앞부분부터 차례대로 잘라낸다.
- 이때 TCP 헤더 이후의 부분을 분할 대상 데이터로 간주한다.
- TCP 헤더는 사용자 데이터가 아니지만 IP 입장에서 보면 TCP에서 송신을 의뢰받은 부분이므로 데이터가 된다.
- 이렇게 해서 데이터를 분할하면 여기에 IP 헤더를 덧붙인다.
- 그 내용은 원래 패킷의 IP 헤더를 그대로 복사한 것이라고 생각하면 되는데, 이때 일부 필드는 고쳐쓴다.
- 왜냐하면 조각 나누기로 분할한 핵심 정보를 IP 헤더에 기록하기 위해서이다.

3. 라우터의 패킷 중계

라우터의 송신 동작

- 이렇게 해서 송신 전의 일이 끝나므로 패킷의 송신 동작으로 넘어간다.
- 이때의 동작은 출력측의 포트에 따라 다르다.
- 이더넷이라면 이더넷의 규칙에 따라 패킷을 신호로 변환하여 송신하고 ADSL이라면 ADSL의 규칙에 따라 신호를 변환하여 송신한다는 식이다.
- 가정용 LAN이라면 라우터 쪽은 AD니 등의 통신 회선을 경유하여 인터넷에 연결되어 있으므로 통신회선의 규칙에 따라 패킷 송신 동작을 실행할 것이다.
- 이더넷의 패킷 송신 동작은 이더넷의 규칙에 규정되어 있으므로 기종이 달라도 마찬가지이다.
- 즉 패킷 송신 동작의 기본은 프로토콜 스택의 IP 담당부분이 패킷을 보낼 때와 같다.
- 다시 말하면 패킷의 맨 앞부분에 MAC 헤더를 부가하고, 여기에 값을 설정하여 패킷을 완성시킨 후 전기 신호로 변환해서 보낸다.

3. 라우터의 패킷 중계

라우터의 송신 동작

- 먼저 MAC 헤더의 맨 앞에 있는 수신처 MAC 주소 필드에 값을 설정하기 위해 경로표의 '게이트웨이' 항목에서 패킷을 건네줄 상대를 판단한다.
- '게이트웨이' 항목에 IP 주소가 쓰여있으면 이 IP 주소가 건네줄 상대이고, 이곳이 비어있으면 IP 헤더의 수신처 IP 주소가 건네줄 상대가 된다.
- 이를 통해 상대의 IP 주소가 결정되면 ARP로 IP 주소에서 MAC 주소를 조사하고, 결과를 수신처 MAC 주소로 설정한다.
- 라우터에도 ARP 캐시가 있으므로 먼저 ARP 캐시를 찾아보고, 해당하는 것이 없으면 ARP로 조회를 보내 MAC 주소를 조회한다.
- 그 다음은 송신처 MAC 주소 필드인데 이것은 출력 측의 포트에 할당된 MAC 주소를 설정한다.
- 그리고 타입 필드에 0800(16진수)을 설정한다.

3. 라우터의 패킷 중계

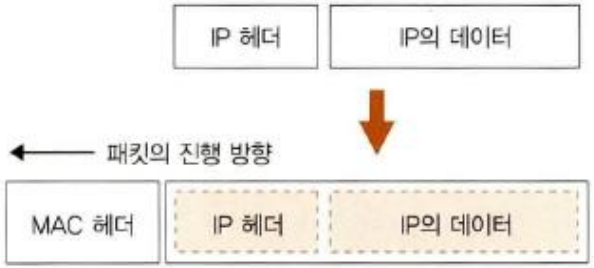
라우터의 송신 동작

- 이렇게 해서 송신 패킷이 만들어졌으므로 이것을 전기 신호로 변환하여 포트에서 송신하는데, 이 동작도 컴퓨터와 같다.
- 출력측의 포트가 이더넷이면 송신한 패킷은 스위칭 허브를 경유하여 다음 라우터에 도달할 것이다.
- 수신처 MAC 주소에 다음 라우터의 주소가 쓰여 있으므로 스위칭 허브가 이것을 보고 다음 라우터까지 패킷을 운반해 오기 때문이다.
- 그러면 그 라우터가 다시 그 다음의 라우터에 패킷을 중계한다. 이렇게 해서 패킷은 착착 진행되어 최종적으로 목적지에 도착한다.

3. 라우터의 패킷 중계

라우터와 스위칭 허브의 관계

- 둘의 관계를 알고 있는 상태에서 컴퓨터가 패킷을 송신할 때 또는 라우터가 패킷을 중계할 때 맨 앞에 MAC 헤더를 부가하는 부분이 중요하다.
- 지금까지는 맨 앞에 MAC 헤더를 부가한다고 표현했지만 그림과 같이 이더넷의 패킷의 데이터 부분에 IP의 패킷을 넣는다고 표현하는 것이 원래의 개념에 가깝다.



- 라우터는 패킷을 운반하는 일을 스위칭 허브에 의뢰한다.
- 패킷을 어디까지 운반할 것인가 하는 점에 착안하면 라우터가 스위칭 허브에 의뢰할 때의 개념을 잘 이해할 수 있다.
- IP가 이더넷에 의뢰하는 것은 최종 목적지까지 패킷을 운반하는 것이 아니라 다음 라우터에 패킷을 운반하는 것이다.
- 그리고 다음 라우터에 패킷이 도착하면 또 여기에서부터 다음 라우터에 패킷을 운반하도록 고쳐서 이더넷에 의뢰한다.
- 이 동작을 반복하여 패킷이 IP의 목적지, 즉 송신 상대에게까지 운반하는 것이다.

3. 라우터의 패킷 중계

라우터와 스위칭 허브의 관계

- 네트워크에는 이더넷 뿐만 아니라 무선 LAN도 있고 인터넷에 나가면 통신 회선도 있다.
- 이러한 것과 IP와의 관계는 어떻게 될까?
- 이것은 무선 LAN이나 통신 회선을 이더넷과 치환하여 생각하면 된다.
- 즉 다음 라우터와의 사이가 무선 LAN으로 연결되었으면 무선 LAN에 의뢰하여 패킷을 운반하며, 통신 회선으로 연결되었으면 통신 회선에 의뢰하여 패킷을 운반한다.
- 여기에서 예로 든 것 이외에도 다양한 통신 기술이 많지만 이것들도 전부 마찬가지이다.
- 요컨대 이 통신 기술에 의뢰하여 패킷을 운반하는 것이다.
- 이렇게 해서 다음 라우터까지 스스로 패킷을 운반하지 않고 다양한 통신 기술에 의뢰하여 패킷을 운반하는 것은 중요하다.
- 이것은 다양한 통신 기술을 적재적소에 구분하여 사용할 수 있다는 것으로 IP의 큰 특징이다.
- 이 특징 덕분에 인터넷과 같은 거대한 네트워크를 만들 수 있었던 것이다.

4. 라우터의 부가 기능

주소 변환

- 현재의 라우터는 기본 동작과 더불어 몇 가지 부가 기능을 가지고 있다.
- 그 중에서 중요한 두 가지 기능이 주소 변환과 패킷 필터링이다.
- 주소는 각 기기를 식별하는 것이므로 다른 것과 중복되지 않는 고유한 주소를 할당하는 것이 기본이다.
- 그러므로 인터넷에 접속하는 기기는 원래 고유의 주소를 가져야만 하는 것이며, 이전에는 그렇게 되어 있었다.
- 1990년 대에 들어 인터넷이 일반에게 공개되자 급속하게 접속 대수가 늘어나기 시작하면서 사정이 바뀌었다.
- 그때까지의 방법을 계속 사용하면 가까운 장래에 할당할 주소가 없어져버린다는 예측이 나왔다.
- 다른 것과 중복되지 않는 고유한 주소를 할당한다는 것은 패킷을 운반하는 원리의 근간이므로 그 예측대로 된다면 큰 문제이다.
- 만약 이것을 방치하면 가까운 장래에 고유한 주소가 고갈될 것이며, 그렇게 되면 새로 기기를 접속할 수 없게 되므로 인터넷은 파국에 이를 것이다.

4. 라우터의 부가 기능

주소 변환

- 이 문제를 해결하는 방법의 요체는 무엇을 가지고 고유하다고 간주할 것인가 하는 것이다.
- 예를 들어 A사와 B사가 있는데 완전히 별개로 독립된 사내 네트워크를 구축했다고 가정하자.
- 이 경우 서로 패킷이 왕래할 리가 없으므로 A사의 서버에 할당한 주소와 같은 주소를 B사의 클라이언트에 할당해도 이 때문에 패킷을 건네 줄 대상을 모르게 되는 일은 없다.
- 두 회사 모두 자사의 네트워크 안에서 패킷을 건네 줄 대상이 명확해야 하므로 다른 회사에 같은 주소가 존재해도 상관없다.
- 두 회사가 같은 주소를 사용했어도 네트워크가 독립되어 있으면 문제가 일어나지 않는다
- 주소 부족에 대처하기 위해 이 성질을 이용했다.
- 즉 사내의 기기에 할당하는 주소는 다른 회사와 중복되어도 좋다고 한 것이다.
- 이렇게 하면 사내의 기기에는 고유의 주소를 할당할 필요가 없어져서 주소를 대폭 절약할 수 있다.
- 단 아무리 사내라고 해도 모두 자기 편한대로 주소를 할당하면 문제가 일어날 수 있으므로 특정 주소를 사내용으로 사용한다는 규칙을 세웠다.

4. 라우터의 부가 기능

주소 변환

- 이러한 규칙에 기초한 사내용 주소는 프라이빗 주소(private address)로, 이 전의 고유한 주소는 글로벌 주소(global address)로 부른다.
- 프라이빗 주소의 규칙은 어렵지 않다.
- 프라이빗 주소로 사내에서 사용하는 것은 아래의 범위로 한정한다는 것뿐이다.

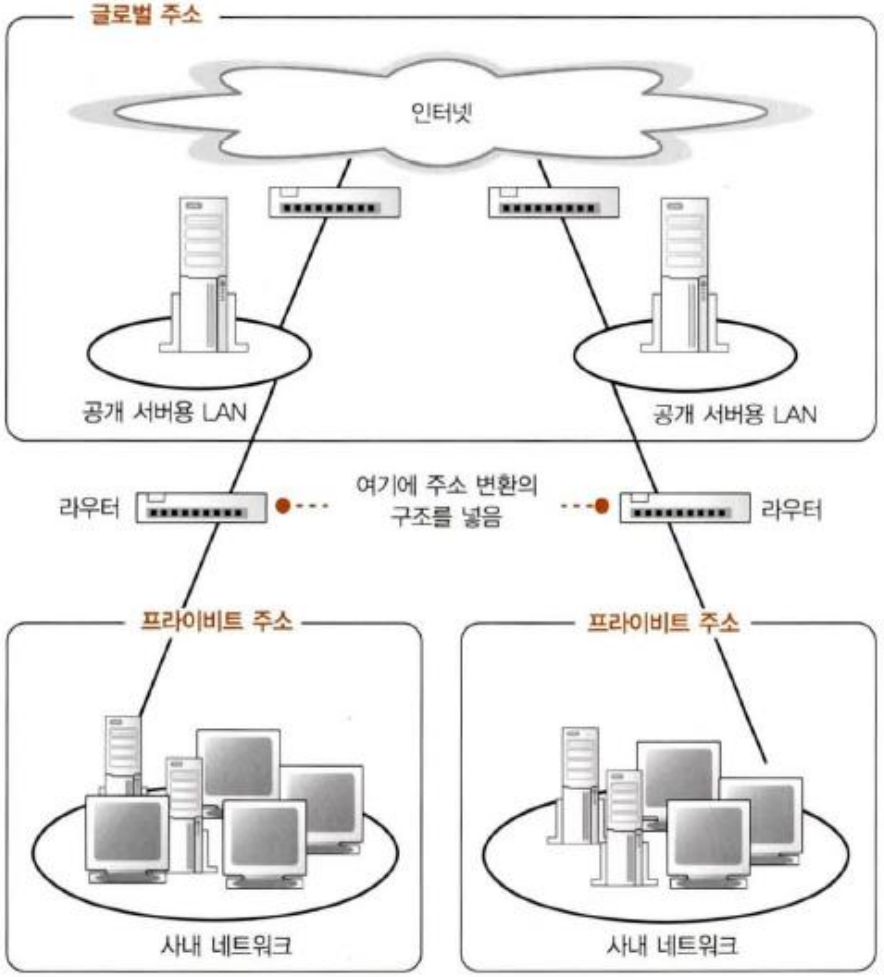
```
10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.1 68.0.0 ~ 192.168.255.255
```

- 이 범위는 프라이빗 주소의 규칙을 만드는 시점에서 어디에도 할당하지 않았던, 이를 테면 미사용의 글로벌 주소 중에서 선택한 것이다.
- 프라이빗 주소는 특별한 구조를 가지고 있는 것이 아니라 원래 글로벌 주소에 포함되어 있던 주소 중에서 범위를 정하고 사내에서 사용한다고 약속한 것에 불과하다.
- 이 범위는 다른 회사와 중복해도 좋으므로 일원화하여 관리하지 않는다.
- 그러므로 신청할 필요가 없고 누구나 자유롭게 사용할 수 있다.
- 단, 사내에서 중복되면 패킷을 운반할 수 없게 되므로 사내에서의 중복은 피해야 한다.

4. 라우터의 부가 기능

주소 변환

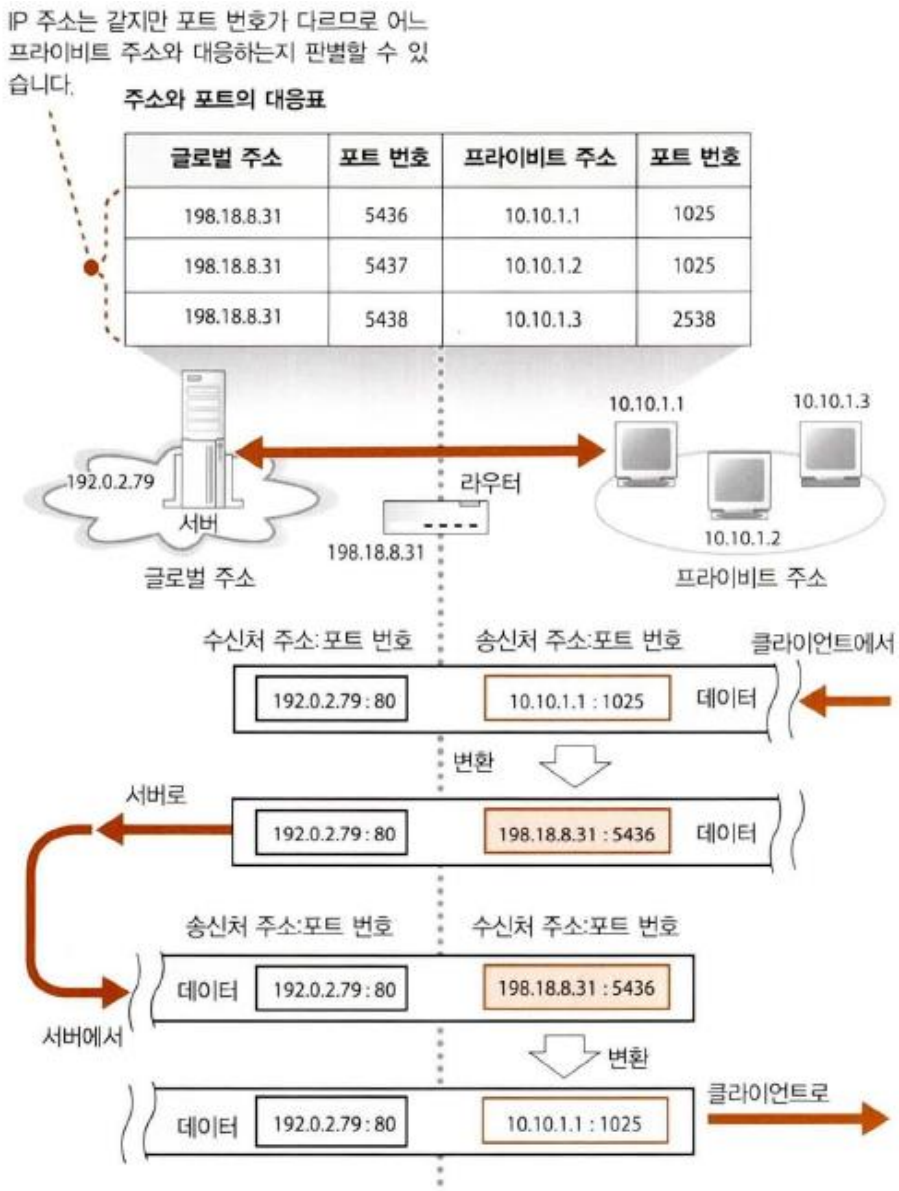
- 이렇게 해서 주소를 절약할 수 있게 되었지만 이것만으로는 문제가 해결되지 않는다.
- 사내 네트워크는 완전히 독립되어 있는 것이 아니라 인터넷을 통해 많은 회사에 연결되므로 패킷이 사내와 인터넷을 왕래하면 여기저기에 같은 주소가 있게 되어 패킷을 정확하게 운반할 수 없게 된다.
- 사내 네트워크를 인터넷에 접속할 때는 그림과 같이 구성해야 한다.
- 그림은 사내의 네트워크를 인터넷에 공개하는 서버를 접속하는 부분과 사내용 네트워크의 두 가지로 나눈 것이다.
- 그리고 공개용 서버쪽에는 글로벌 주소를 할당하고 인터넷과 직접 통신해야 하는데, 이 부분은 이전의 방법과 같다.
- 한편 사내 네트워크에는 프라이빗 주소를 할당하고 인터넷과는 직접 패킷을 주고받지 않도록 특별한 구조를 사용하여 접속하는데, 이 구조가 주소 변환이다.



4. 라우터의 부가 기능

주소 변환의 기본 동작

- 주소 변환의 구조는 패킷을 중계할 때 IP 헤더에 기재된 IP 주소와 포트 번호를 바꿔 쓰는 것이다.
- 구체적인 방법은 동작을 추적해 보면 알 수 있다.
- 웹 서버에 액세스할 때 흐르는 패킷을 차례대로 살펴보자.
- 먼저 TCP의 접속 동작에서 최초로 흐르는 패킷을 인터넷에 중계할 때 그림과 같이 송신처의 IP 주소를 프라이빗 주소에서 글로벌 주소로 변경한다.
- 여기에서 사용하는 글로벌 주소는 주소 변환 장치의 인터넷측에 있는 포트에 할당된 주소로 이것과 동시에 포트 번호도 변경한다.
- 그리고 바꿔쓰기 전의 프라이빗 주소와 포트 번호, 바꿔쓴 후의 글로벌 주소와 포트 번호를 한 세트로 하여 주소 변환 장치 내부에 있는 대응표에 기록해 둔다.



4. 라우터의 부가 기능

주소 변환의 기본 동작

- 송신처의 IP 주소와 포트 번호를 바꿔쓴 후 패킷을 인터넷에 송출한다.
- 그러면 패킷은 서버에 도착하며 여기에서 회신 패킷이 돌아온다.
- 서버는 송신처에 회신을 돌려보내므로 회신 패킷의 수신처는 바꿔쓴 글로벌 주소와 포트 번호가 되어 있을 것이다.
- 이 글로벌 주소는 주소 변환 장치에 할당되어 있으므로 회신 패킷은 주소 변환 장치에 되돌아온다.
- 주소 변환 장치는 주소의 대응표에서 글로벌 주소와 포트 번호를 찾이서 수신처를 대응하는 프라이빗 주소와 포트 번호로 바꿔 쓰고, 사내 네트워크에 패킷을 보낸다.
- 이렇게 해서 송신처에 응답 패킷이 도착한다.
- 그 후 패킷을 주고받을 때는 대응표에서 프라이빗 주소와 글로벌 주소의 대응 관계를 조사하여 주소와 포트 번호를 바꿔 쓰고 나서 패킷을 중계한다.
- 그리고 데이터 송 · 수신을 끝내고 연결 끊기 동작의 패킷이 흐르다가 인터넷에 대한 접속 동작이 끝나면 대응표에 등록한 것을 삭제한다.
- 이렇게 해서 프라이빗 주소를 할당한 기기도 인터넷에 접속할 수 있다.
- 인터넷측에서 보면 주소 변환 장치 (여기에서는 라우터)가 통신 상대로 되어 있는 것으로 보인다.

4. 라우터의 부가 기능

포트 번호를 바꿔쓰는 이유

- 현재 사용하고 있는 주소 변환의 원리는 주소와 포트 번호 두 가지를 바꿔쓰지만, 초기의 주소 변환은 포트 번호 바꿔 쓰기를 실행하지 않고 주소만 바꿔썼다.
- 이 방법으로도 사내와 인터넷에서 주고받기가 가능하면서 구조가 간단하다.
- 이 방법을 선택한다면 프라이빗 주소와 글로벌 주소가 1 대 1로 대응해서 인터넷에 접속하는 대 수만큼 글로벌 주소가 필요하다.
- 접속 동작이 끝나고 대응표에서 삭제하면 같은 글로벌 주소를 다른 기기에서 사용하므로 동시에 접속하는 대수만 있으면 되지만 사내의 사원 수가 많으면 동시에 액세스하는 인원 수도 늘어난다.
- 수천 명 규모의 회사라면 수백 명이 동시에 접속하는 경우가 있지만 이 경우 수백 개의 글로벌 주소가 필요하다.
- 포트 번호도 바꿔 쓰는 방법은 이 점을 개선하기 위해 고안되었다.
- 포트 번호는 16 비트 수치이므로 수만 개의 값을 취할 수 있다.
- 이것을 글로벌 주소와 한 세트로 하여 프라이빗 주소에 대응시키면 한 개의 글로벌 주소를 수만 개의 프라이빗 주소에 대응시킬 수 있는데 이렇게 하는 쪽이 글로벌 주소의 이용 효율이 높아진다.

4. 라우터의 부가 기능

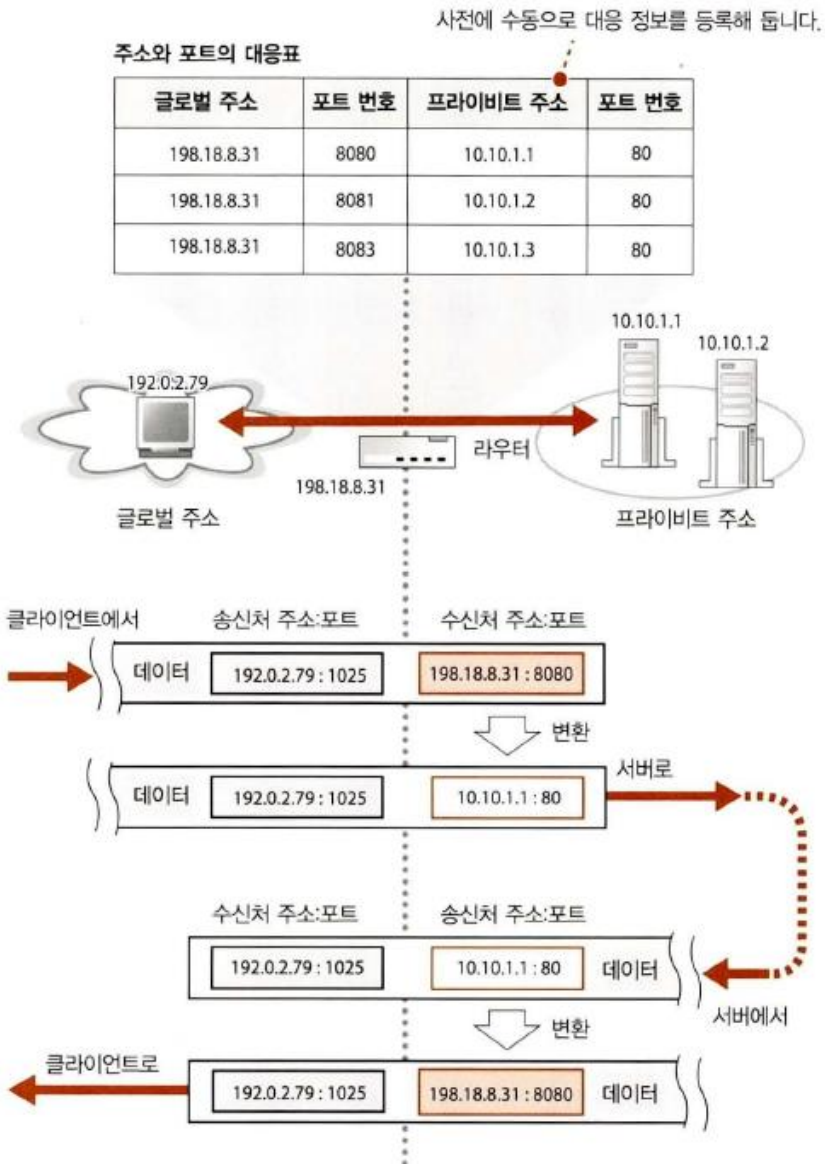
인터넷에서 회사로 액세스

- 사내에서 인터넷으로 액세스하는 패킷을 중계할 때는 대응표에 송신처의 프라이빗 주소와 포트 번호가 등록되어 있지 않아도 패킷을 중계할 수 있다.
- 바꿔 쓰는 글로벌 주소는 주소 변환 장치(라우터)에 할당되어 있고, 포트 번호는 적당히 비어있는 것을 사용하면 되므로 주소 변환 장치 자체에서 적당히 판단할 수 있기 때문이다.
- 그러나 인터넷에서 사내로 패킷을 중계할 때는 대응표에 등록되어 있지 않으면 중계할 수 없다.
- 대응표에 기록이 없으면 주소 변환 장치가 글로벌과 프라이빗의 대응 관계를 판단할 수 없기 때문이다.
- 이것은 인터넷에서 액세 스하지 않는 기기에는 인터넷측에서 패킷을 송신할 수 없다는 이야기이다.
- 액세스중인 기기라고 해도 인터넷과의 통신에 사용하고 있는 포트 번호 이외의 포트에 패킷을 보낼 수 없다.
- 즉 사내에서 의도적으로 인터넷에 액세스하지 않는 한 인터넷측에서 사내에 패킷을 보낼 수 없다.
- 이것은 부정 침입을 방지하는 효과를 가지고 있다.

4. 라우터의 부가 기능

인터넷에서 회사로 액세스

- 사내에 액세스하고 싶은 경우 조금 연구하면 그것도 가능하다.
- 인터넷에서 사내에 액세스할 수 없는 이유는 대응표에 등록되어 있지 않기 때문이므로 사전에 수동으로 대응표에 등록해 두면 된다(그림).
- 보통 공개용 서버는 주소 변환 장치의 밖으로 나가 글로벌 주소를 할당하지만, 서버의 프라이빗 주소를 주소 변환장치에 수동으로 등록해 두면 사내에 있는 프라이빗 주소를 할당한 서버를 공개할 수도 있다.



4. 라우터의 부가 기능

라우터의 패킷 필터링 기능

- 패킷 필터링 기능도 라우터의 중요한 부가 기능 중 하나이다.
- 주소 변환은 조금 복잡했지만, 패킷 필터링의 원리는 그다지 복잡하지 않다.
- 패킷을 중계할 때 MAC 헤더, IP 헤더, TCP 헤더에 기록되어 있는 내용을 조사하여 그것이 사전에 설정한 조건에 합치되면 패킷을 중계하거나 폐기하는 동작을 실행할 뿐이다.
- 대부분의 방화벽이라는 기기나 소프트웨어는 이 원리를 이용하여 부정 침입을 방지한다.
- 이와 같이 패킷 필터링의 개념은 간단하지만 부정 침입과 정상 액세스를 분간하여 부정 침입만 차단하도록 조건을 설정하는 것은 간단하지 않다.
- 예를 들어 인터넷에서의 침입을 방지하기 위해 인터넷에서 들어오는 패킷을 전부 차단하면 어떻게 될까?
- TCP 동작에서 알 수 있듯이 패킷은 양방향으로 흐르므로 단순히 인터넷에서 들어오는 패킷을 전부 차단하면 사내에서 인터넷으로 액세스하는 동작도 정상 작동하지 않게 된다.

Thank You