6주차

라우터의 기본

라우터의 포트부분은 다음과 같다.

- **이더넷포트**:전통적인 유선 연결방식이다.(MAC주소 기반)
- **무선 LAN포트**:무선 주파수를 사용하여 데이터를 전송한다
- **ADSL포트** : 전화선을 사용한 디지털데이터 전송을 위한 포트이다
- **FTTH포트** : 광섬유를 통한 고속 인터넷 접속을 지원하는 포트이다

라우팅 테이블

라우팅테이블은 컴퓨터네트워크에서 목적지 주소를 목적지에 도달하기 위한 네트워크 노선으로 변환시키는 목적으로 사용한다. 각 라우터의 라우팅 테이블은 모든 목적지 정보에 대해 해당 목적지에 도달하기 위해서 거쳐야 할 다음 라우터의 정보를 가지고 있다.

출처:위키백과

즉 라우팅 테이블이란 네트워크상의 특정 목적지까지의 거리와 가는 방법등을 명시하는 테이블이다.

라우터는 어떤 목적지를 찾아갈 때 이 라우팅 테이블을 보고 찾아가게 된다.

라우팅 테이블의 주요개념

- **기본 라우팅 테이블** : VPC와 함께 자동으로 제공되는 라이팅 테이블이다. 다른 라우팅 테이블과 명시적으로 연결되지 않은 모든 서브넷의 라우팅을 제어한다.
- **사용자 지정 라우팅 테이블** : VPC에 대해 생성하는 라우팅 테이블이다.
- **대상(Destiantion)** : 트래픽을 이동항 대상IP주소의 범위이다.
- **대상(Target)** : 대상 트래픽을 전송할때 사용할 게이트웨이, 네트워크 인터페이스 또는 연결이다(인터넷 게이트웨이)
- **라우팅 테이블 연결** :라우팅 테이블과 서브넷, 인터넷 게이트웨이 또는 가상 프라이빗 게이트웨이간의 연결이다.
- **서브넷 라우팅 테이블(Subnet route table)** :서브넷과 연결된 라우팅 테이블이다.
- **로컬 라우팅(Local route)** : VPC 내 통신을 위한 기본 라우팅이다

- **전파** : 가상 프라이빗 게이트웨이를 VPC에 연결하고 라우팅 전파를 활성화한 경우 VPN 연결을 위한 경로를 서브넷 라우팅 테이블에 자동으로 추가한다. 따라서 VPN 경로를 수동으로 추가하거나 제거할 필요가 없다.
- **게이트웨이 라우팅 테이블(Gateway route table)** : 인터넷 게이트웨이 또는 가상 프라이빗 게이트웨이와 연결된 라우팅 테이블이다.
- **엣지 연결(Edge association)** :인바운드 VPC 트래픽을 어플라이언스로 라우팅하는 데 사용하는 라우팅 테이블이다. 라우팅 테이블을 인터넷 게이트웨이 또는 가상 프라이빗 게이트웨이와 연결하고 어플라이언스의 네트워크 인터페이스를 VPC 트래픽의 대상으로 지정한다.
- **Transit 게이트웨이 라우팅 테이블(Transit gateway route table)** :Transit 게이트웨이와 연결된 라우팅 테이블이다.
- **로컬 게이트웨이 라우팅 테이블(Local gateway route table)** : Outposts 로컬 게이트웨이와 연결된 라우팅 테이블이다.

라우터의 패킷 수신 동작

신호가 커넥터 부분에 도착하면 안쪽에 있는 PHY(MAU)회로와 MAC회로에서 신호를 디지털 데이터로 변환한다. 그리고 패킷 끝부분의 FCS를 대조하여 오류의 유무를 점검하고, 정상이면 MAC헤더의 수신처 MAC주소가 자신에게 해당하는지 조사하여 해당하면 패킷을 수신버퍼메모리에 저장한다.

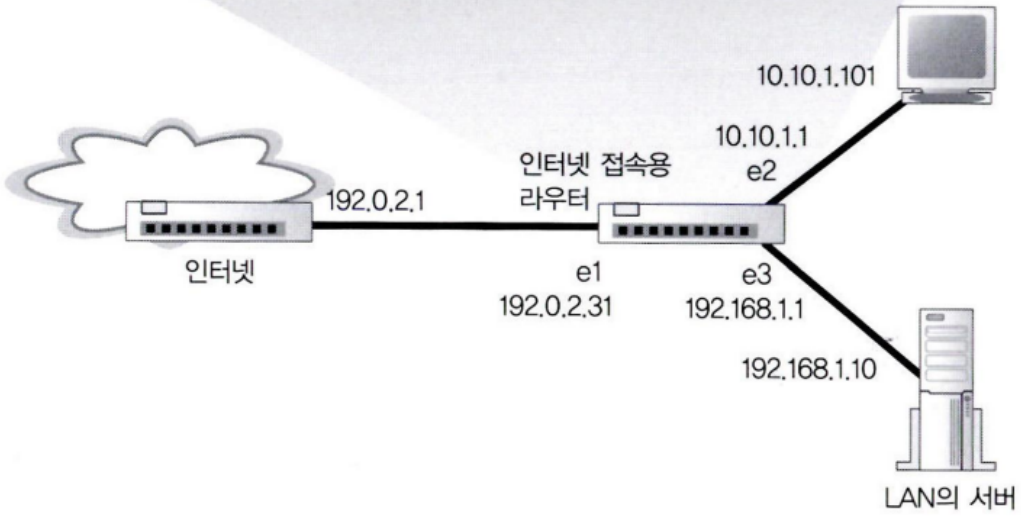
여기에서 수신처 MAC주소에 자신이 해당하지 않을 경우에는 패킷을 폐기한다. 자신이 수신처에 해당하지 않는 경우 도착한 패킷은 다른 기기가 수신할 것이므로 이것을 수신하면 이더넷의 규칙에 위반되기 때문이다.

해당하는 경로가 없는 경우에 선택하는 기본경로

인터넷의 중계 대상은 많이 존재한다.

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



하지만 그림에서 아랫부분이 중계대상을 전부 등록시킨 것과 같다.

넷마스크가 0.0.0.0으로 되어 있는데, 이것은 패킷의 수신처IP주소와 경로표의 수신처 항목을 비교할 때의 비트수가 0이라는 것이므로 비교 동작을 실행하지 않아도 된다.

게이트웨이 항목에 인터넷으로 나가는 라우터를 등록해 두면 다른 행에 해당하는 것이 없는 경우에는 패킷을 그곳으로 중계하는데, 이것을 **기본경로**라고 하고 여기에 등록한 라우터를 **기본 게이트웨이**라고 한다.(위의 라우팅 테이블 개념 참고)

패킷의 유효기간

TTL(패킷의 생존기간)이라는 IP헤더의 필드를 갱신한다

TTL이란 인터넷에서 IP패킷이 라우팅 되며 남아있는(거쳐야할) 라우터의 갯수를 표한한는 수이다.

각 라우터는 IP패킷을 라우팅 할때마다 TTL의 값을 감소시킨다.

TTL이 0이 되면 생존기간이 만료되는 것으로 간주하여 패킷을 폐기한다.

라우터의 부가기능

주소변환

2011년2월경 인터넷 주소 관리기구인 IANA는 더이상의 IPv4할당이 없을 것이라고 선언하였다. IPv4는 약43억개의 한정된 주소를 사용할 수 있는데 반해 인터넷의 수요가 빠르게 증가하여 각 대륙에 할당한 IPv4가 고갈되어 할당 할수 없게 된 것이다. 하지만 현재까지도 IPv4를 잘 쓰고 있는 이유가 있는데 **Private Network** 때문이다.

Private Network의 탄생

사설망 도는 프라이빗 네트워크(private network)는 인터넷 어드레싱 아키텍쳐에서 사설IP 주소공간을 이용하는 네트워크이며 RFC 1918과 RFC4193표준을 준수한다. 이러한 주소는 가정,사무실, 기업 랜에 쓰인다.

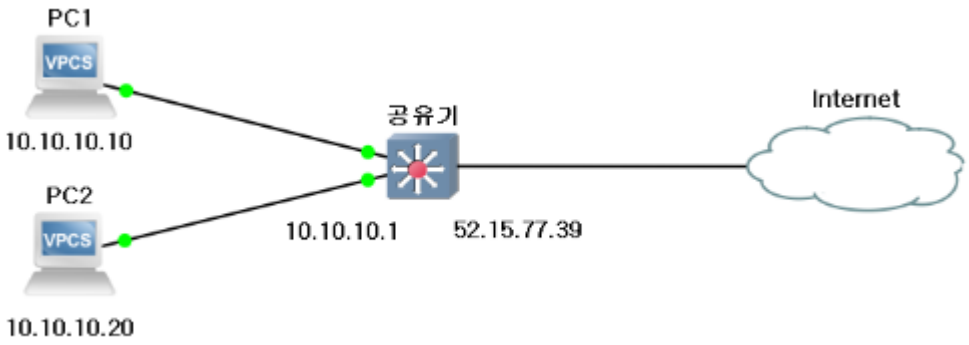
출처:위키백과

Pirvate Network는 IPv4 중 특정 대역을 공인 인터넷이 아닌 가정,기업 등의 한정된 공간에 사용한 네트워크를 의미한다. 사설망에 소속된 IP인 사설 IP대역은 다음과 같으며 오로지 사설망에서만 사용가능하기 때문에 공인망에선 사용할 수 없다.

RFC1918 이름	IP 주소 범위	주소 개수	클래스 내용	최대 사이더 블록 (서브넷 마스크)	호스트 ID 크기
24비트 블록	10.0.0.0 – 10.255.255.255	16,777,216	클래스 A 하나	10.0.0.0/8 (255.0.0.0)	24 비트
20비트 블록	172.16.0.0 – 172.31.255.255	1,048,576	16개의 인접 클래스 B	172.16.0.0/12 (255.240.0.0)	20 비트
16비트 블록	192.168.0.0 – 192.168.255.255	65,536	256개의 인접 클래스 C	192.168.0.0/16 (255.255.0.0)	16 비트

이 사설IP는 사설망에서만 해당한다면 어디에서나 사용할 수 있다. 일반적으로 집에서 사용하는 컴퓨터,IPTV,휴대폰,플레이스테이션 등은 공유기가 할당해주는 사설 IP를 사용한다.

이와 같이 기업또한 스위치,라우터,방화벽과 같은 네트워크 장비 혹은 비슷한 장비에 사설IP와 서브넷 마스크를 지정하고 게이트웨이(사설 IP할당)로 사용하여 이에 연결괸 컴퓨터 사설IP를 할당한다.



이렇게 사설망과 공인망이 사용하는 IP에 따라 분리되면서 공인망과 사설망의 경계에서는 별도의 조치를 취해야할 필요성이 생겼다.(사설망에서 공인 인터넷으로 나가고자 할때 자신의 출발지IP를 사설 IP그대로 사용할 수 없기 때문이다)

IP를 변환하는 것은 사설망과 공인망의 통신에서만 필요한 것은 아니다. 자사의 사설망(내부망)과 전용회선을 통해 대외사의 사설망을 연결할 경우, 이 경우의 통신에서도 IP를 변환해야할 필요가 많다.

자신의 실제 IP를 노출시키지 않아야 하거나 반대편 기업의 실제 IP로 목적지IP를 변환하여야 할 필요가 있을때 사용한다. 소위 '대외망'라 불리는 결제 대행사와 유통회사의 통신이 대표적이다. 이에 IP를 변환하기 위한 방법을 고안한 것이 바로 NAT(Network Address Translation)이다.

NAT(Network Address Translation)

네트워크 주소 변환(network address translation)은 컴퓨터 네트워킹에서 쓰이는 용어로써, Ip패킷의 TCP/UDP포트 숫자와 소스 및 목적지의 IP주소등을 재기록하면서 라우터를 통해 네트워크 트래픽을 주고받는 기술을 말한다.

출처: 위키백과

위키백과의 설명처럼 NAT는 IP주소 혹은 IP패킷의 TCP/UDP Port숫자를 변환 및 재기록하여 네트워크 트래픽을 주고받는 기술을 의미한다. 지금까지 설명한 내용을 적용해보자면 사설망에서 공인망으로, 공인망에서 사설망으로 통신하고자 할때 공인망/사설망에서 사용하는 IP로 변환하는 것을 의미한다고 볼 수 있다.

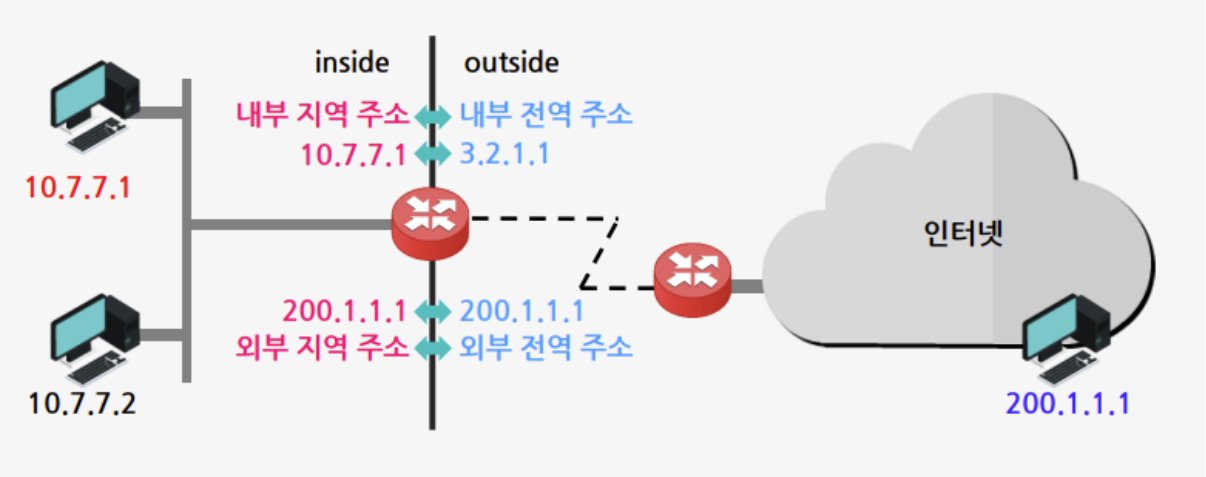
여기서 IP주소 뿐만 아니라 IP패킷의 TCP/UDP Port 숫자를 변환한다고 말한 이우는 실제로 NAT의미가 IP주소 뿐만 아니라 Port까지 변환시켜 사용하는 것을 포함하기 때문이다. 이를 Port Address Translation(PAT or NAPT)라고 부른다.

NAT의 종류

구분	NAT	PAT
정적	정적 NAT	정적 PAT (PAR : Port Address Redirection)
동적	동적 NAT	동적 PAT (NAT Overload)

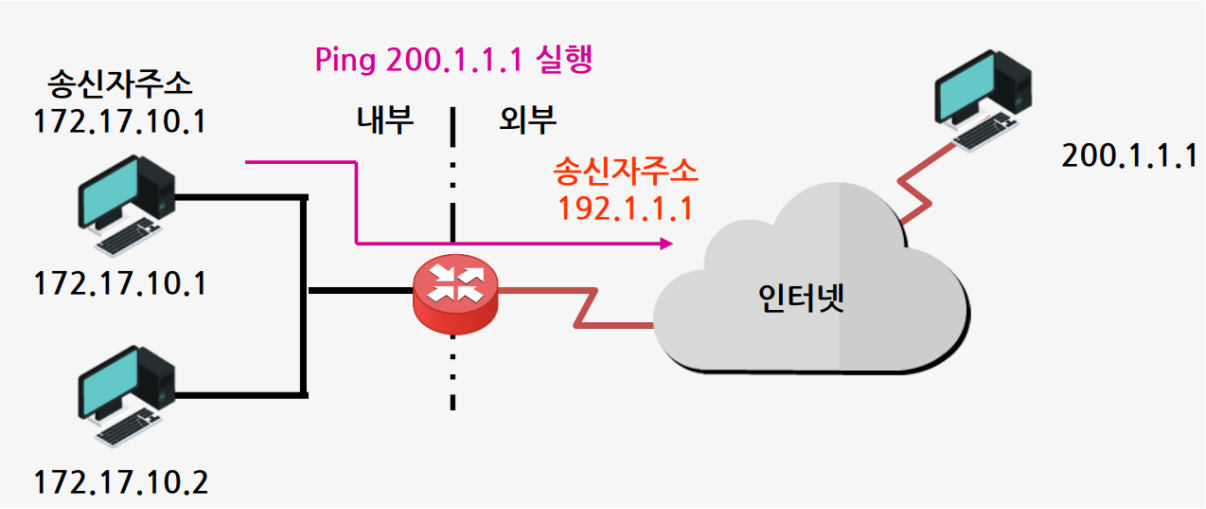
사설주소와 공인주소간에 1:1변환인 경우는 NAT라고 하며, 사설주소와 공인주소간 N:1변환인 경우 PAT라고 한다.

또한 사설주소와 공인주소간의 주소변환이 고정된 경우 정적 변환이라고 하며, 유동적으로 변하는 경우는 동적변환이라고 한다.



- 내부지역주소: 망 내부에서만 사용하는 주소
- 내부 전역주소: 외부에서 공인된 내부 식별 주소, 내부지역주소가 외부로 나갈경우 변환되어 내부 전역주소가 된다.
- 외부 지역 주소: 외부 전역 주소가 변환되어 내부에서 통용되는 주소(중복 네트워크 변환이 일어나지 않을 경우 외부전역주소와 동일하다)
- 외부 전역 주소: 외부에 존재하는 사용자에게 할당된 주소

정적NAT



특징

- 내부 지역 주소와 내부 전역주소 간에 1:1변환이 고정적으로 일어나며, 관리지가 직접 변환 주소 지정한다
- 내부 전역 주소가 항상 동일한 내부 지역 주소로 변환되므로 웹서버,메일서버 등 주로 사설 주소를 사용하는 내부 서버들을 위해 사용한다

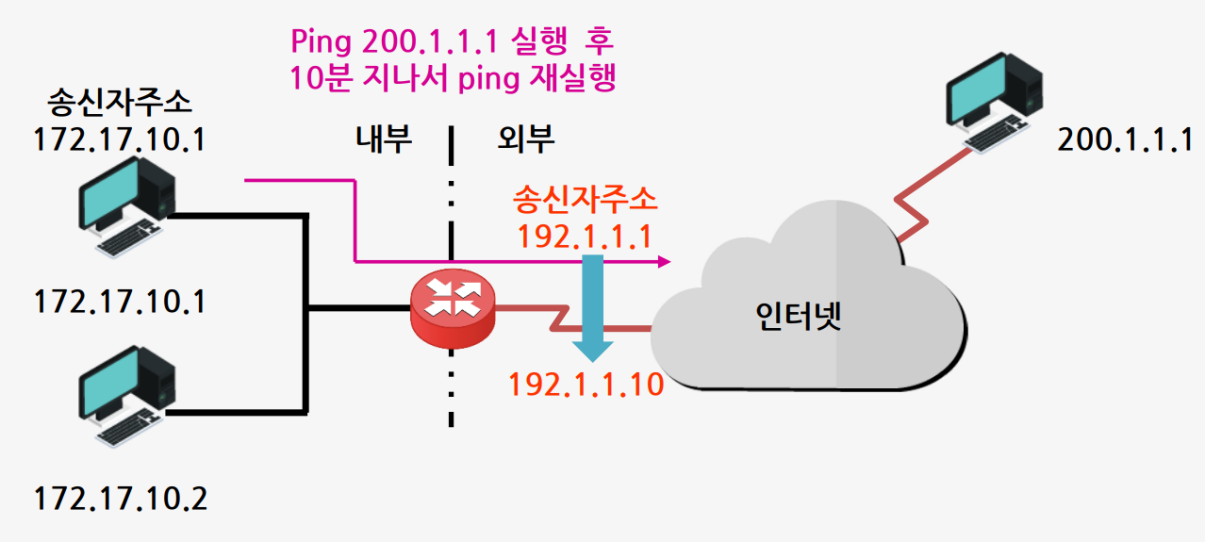
장점

- 기존 주소를 유지하면서 웹과 다른 공개 서비스들을 지속적으로 사용할 수 있도록 해준다

단점

- 정적 NAT주소 부족 문제를 해결하지 못하였다.(고정적인 1:1변환이므로 내부지역 주소와 내부전역주소의 수가 동일해야하기 때문이다)
- 내부전역주소가 C클래스이고 내부지역주소를 사용하는 사용자가 1000여명이라면 모든 내부사용자가 인터넷에 접속할 수 없다

동적NAT



특징

- 내부 지역 주소와 내부전역 주소간 1:1 변환이 자동으로 이루어진다.
- 동적 NAT는 인터넷을 접속할때마다 다른 내부전역 주소가 할당될 수 있다.

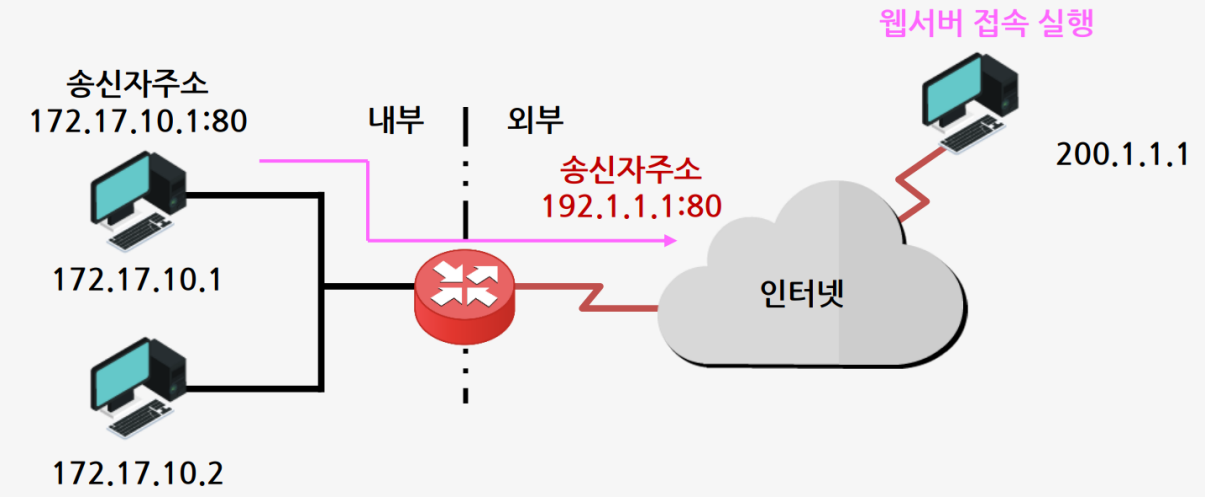
장점

- 주소변환이 불규칙적으로 이루어지므로 보안측면에서 장점을 가지고 있다.
- 내부전역주소로 원하는 내부의 컴퓨터로 접속하기 어렵다.

단점

- 정적 NAT와 마찬가지로 주소부족 문제를 해결하지 못한다.

정적PAT



특징

- PAR(Port Address Redirection)이라 불린다.(하나의 공인 주소를 사용하면서 TCP나 UDP포트번호별로 변환될 내부지역 주소를 직접 지정한다)
- 정적 NAT와 마찬가지로 사설 IP주소를 사용하는 DNS,WEB,FTP등의 서버주소 변환에 사용한다.

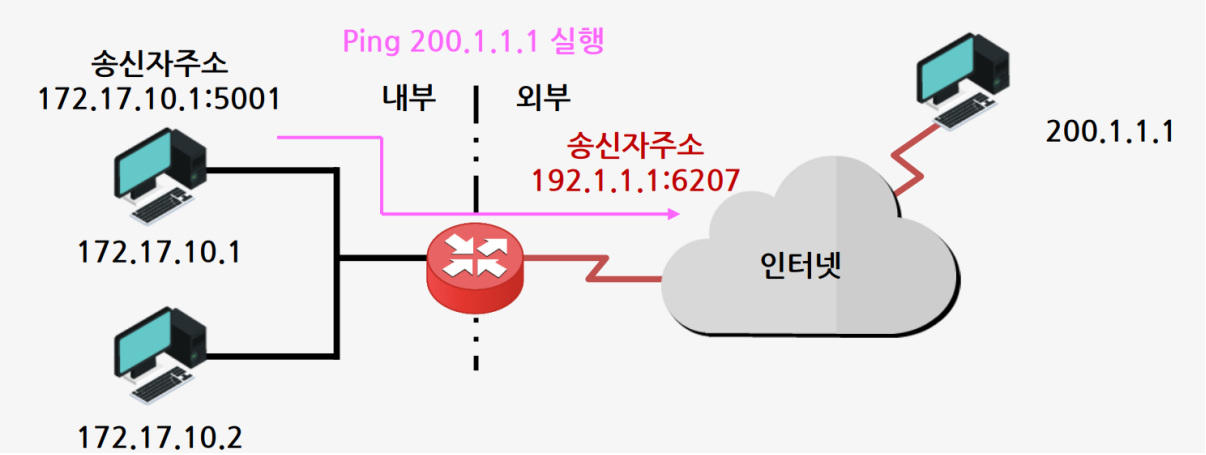
장점

- 서로 다른 사설 주소를 사용하는 서버를 하나의 공인주소로 나타낼 수 있다
- 변환시킬 공인 IP주소가 부족하거나 절약하고자 할 때 유용하다

단점

- 고정적인 변환을 수행하므로 보안 효과가 없다

동적 PAT



특징

- 포트번호를 이용하여 내부지역주소와 내부전역주소간에 N:1변환이 자동으로 이루어지며 NAT오버로드(Overload)라고 한다.
- 포트번호를 IP주소와 함께 표기하여 내부 사용자를 식별한다

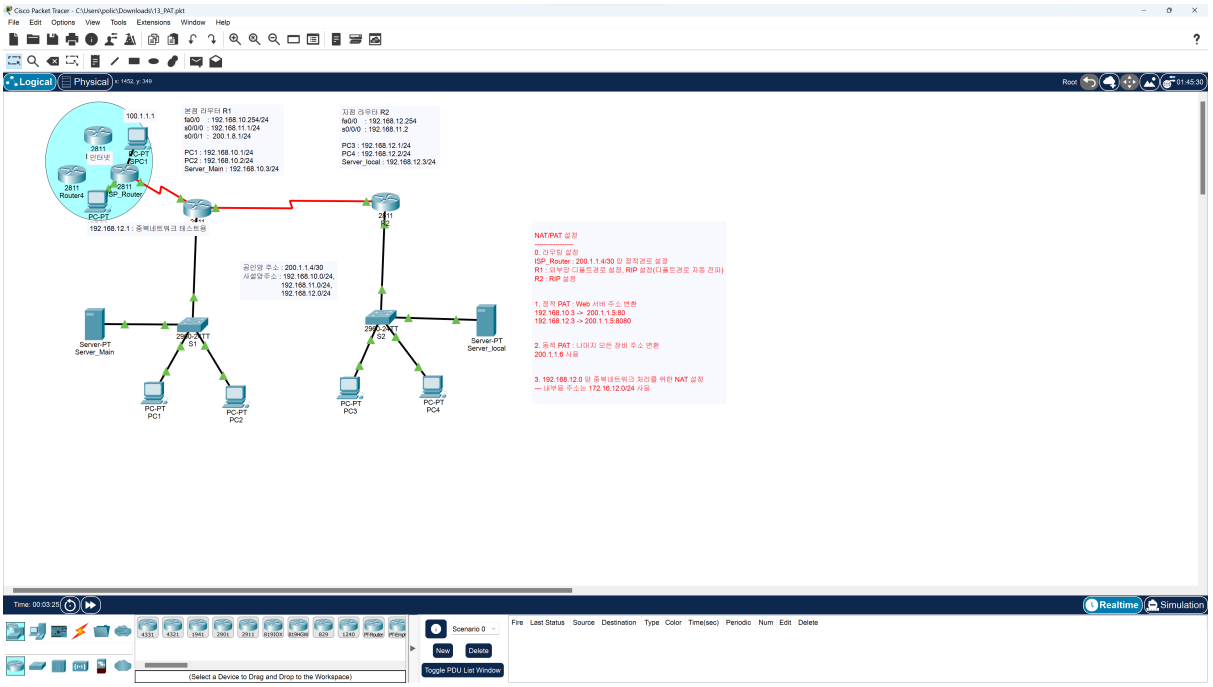
장점

- 주소 부족 문제 해결할 수 있다.
- 이론상 65000여개의 사설IP주소가 1개의 공인IP주소 사용가능하다

단점

- 해킹을 시도하는 해커가 동적 PAT상ㅇ시 해커 추적이 어렵다

Cisco PacketTracer 를 이용해 구현한 PAT/NAT



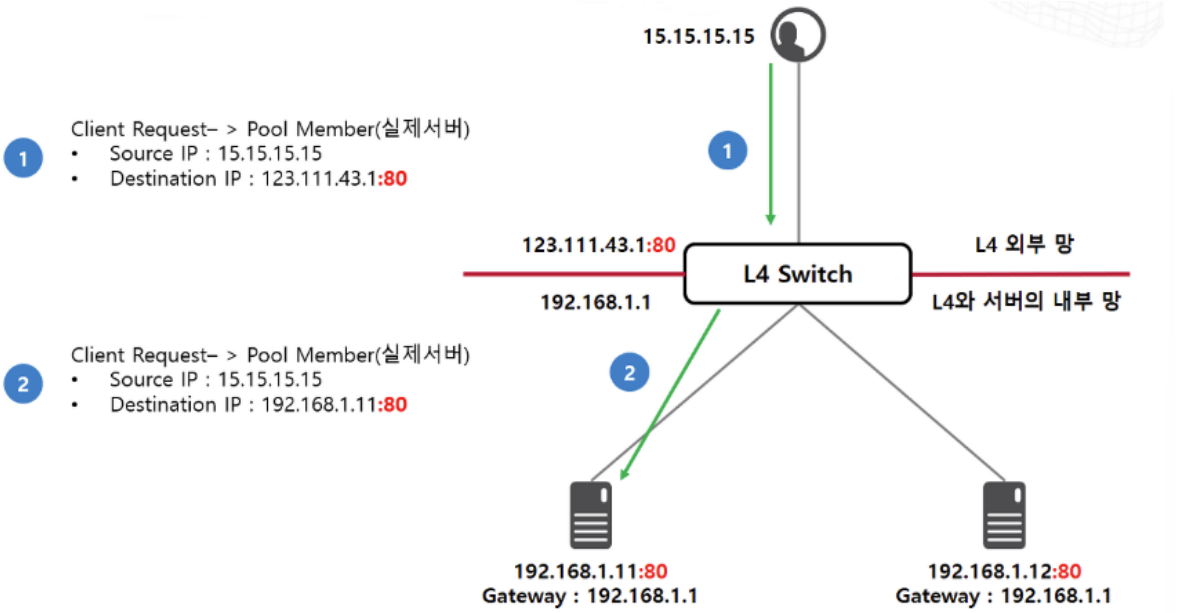
Session Table & Stateful

NAT를 수행하는 네트워크 장비의 종류는 매우 다양하다. 주로 관문(GateWay)을 하는 네트워크 장비가 주로 NAT를 수행한다. 가정에서는 공유기가 내부망과 공인망의 경계에서 NAT를 실시하며, 기업에서는 과거 라우터가 이 역할을 자주 맡았으나, 요즘에는 방화벽, VPN,L4스위치 등이 이 역할을 좀더 많이 수행한다.

공인망에 노출되는 관문에 해당하는 장비인 만큼 보안기능을 포함된 장비가 맡는다. NAT를 수행하는 장비들은 자신에게 설정된 규칙(Rule)에 따라 허용/거부를 판단하고, NAT를 실시하고 이를 기록해둔다. 이를 수행하는 장비들을 보통 Session장비(이하 세션장비)라고 부르며 NAT를 실시한 내역을 기록한 테이블을 Session Table이라고 부른다.

내부 지역 주소	내부 전역 주소	외부 지역 주소	외부 전역 주소
10.7.7.1	3.2.1.1	200.1.1.1	200.1.1.1

위의 그림과 같이 주소 변환 결과는 NAT테이블에 저장하여 관리된다.



Origin IP	Origin Port	NAT IP	NAT Port
123.111.43.1	80	192.168.1.11	80

그림에서는 L4스위치를 거쳐, 실제 서버로 Request가 유입되면서 목적지인 실제서버의 사설 IP로 NAT된 것이 세션테이블에 반영이 되어있다.

보통 세션 장비에 정해진 Rule(이하 규칙)에 의해 허용된 IP만이 NAT를 실시할 수 있고 세션 테이블에 이름(Session, 이하 세션)을 올릴 수 있게 된다. 주로 방확벽과 같은 장비가 이러한 작업을 수행한다. 그리고 테이블에 기록된 IP는 규칙에 의해 나가거나/들어온 뒤 다시 들어오거나/나갈 수 있다. 즉 규칙에 의해 한번 허용이 된 패킷은 반대방향에 대한 정책을 별도로 수립할 필요없이 테이블에 기록된 세션을 보고 네트워크장비가 통과시킨다는 것을 의미한다. 이러한 특성을 Stateful이라고 한다.

실무에서의 NAT

L4스위치에서의 SNAT,DAT

Juniper방화벽에서의 MIP,DIP,VIP

Fortinet방확벽에서의 SNAT,DNAT

등이 존재하며 어느 입장에 서느냐에 따라 사용하는 단어는 다르지만 결국 의미하는 것은 동일하다.(Source IP NAT Destination IP NAT)

출처:

성공과 실패를 결정하는 1%의 네트워크

컴퓨터 네트워킹 하향식 접근

https://yoo11052.tistory.com/40

https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/VPC_Route_Tables.html

http://www.ktword.co.kr/test/view/view.php?nav=2&no=1676&sh=nat

http://www.ktword.co.kr/test/view/view.php?nav=2&no=1327&sh=라우팅+테이블

https://aws-hyoh.tistory.com/145