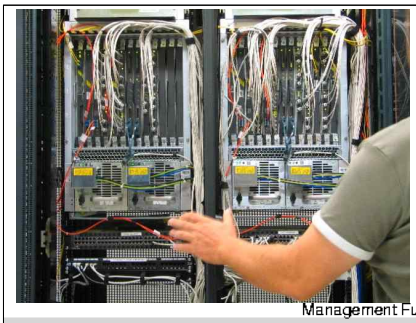
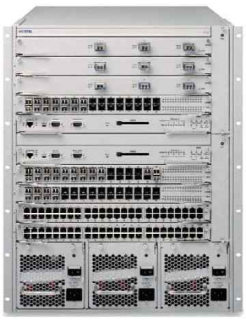
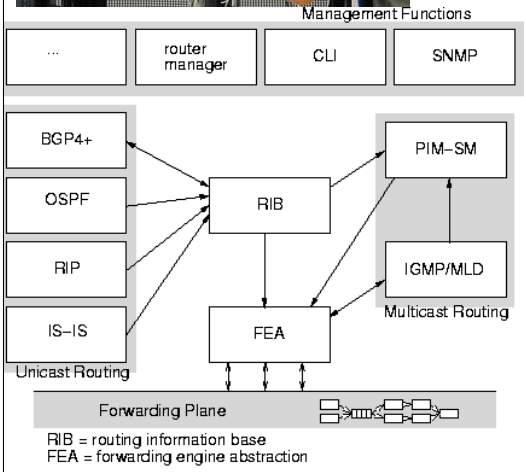
네트워크 (공유기)

홍지우

라우터란?







OSI 7계층에서 네트워크 계층에 포함되는 기기이다.
논리적으로 분리된 망, 혹은 물리적으로 분리된 망 사이를 지나가야하는 패킷들에게 경로를 뽑아 자기가 아는 **최상의 경로를 찾아낸 뒤** (안되는 라우터가 더 많음) **다른 망으로 패킷을 보내주는 역할**을 하는 기계이다. 비유하자면 택시기사 정도 (패킷은 손님, 분리된 망은 도시) 쉽게 풀이하면, 상위 통신망과 하위 통신망 사이를 중계해주는 기계이다. 게이트웨이 (관문. 흔히 톨-게이트 라고 불리는것도 게이트웨이로, 이 지점을 기준으로 다른 두 개의 장소로 나뉘며, 이 지점에서 출입통제가 가능하면 그게 게이트웨이. 네트워크의 게이트웨이도 똑같은 의미이다.) 역할도 하지만, 좀 더 많이 똑똑이해서 여러 가지 프로토콜을 통해 다른 라우터나 네임서버들과 통신하여 동적 라우팅을 지원한다던지, 라우터도 엄청난 인터페이스 카드를 제외하면 하드디스크부터 메모리에 X86 CPU나 DSP 및 파워PC CPU까지 잡다하게 들어간 컴퓨터라서 쉘 환경에 익숙하다면 컴퓨터 쓰듯이 프로그램을 올릴 수도 있다. 라우터는 반드시 전용 기계가 필요한 것이 아니고 일반적인 데스크탑에서도 얼마든지 라우터를 구축할 수 있다. 단지 라우터는 처음부터 네트워크 통신망 중계에 필요한 부품을 위주로 특별 제작되었기 때문에 일반 데스크탑으로 구축된 라우터에 비해 전기를 적게 먹고, 좀 더 안정적인 서비스가 가능하다.

공유기란?

Home Router. 가정용 및 소기업에서 사용하는 소용량 라우터. 기기에 따라서는 Wi-Fi 칩셋과 안테나를 더해 AP 기능까지 하기도 한다. 공유기의 가장 기본적인 기능은 ISP(인터넷 회사)에서 할당해 주는 하나의 IP를 사용하여 여러 대의 컴퓨터가 인터넷에 접속할 수 있도록 해 주는 것이다. 한편, 여러 대의 컴퓨터에서 인터넷을 사용하려면 ISP에서 공인 IP주소를 여러개 할당받는 게 원칙이나, ISP에서는 추가 IP마다 돈을 내라고 강요하기 때문에 IP를 하나만 할당받고 여러대의 컴퓨터가 인터넷을 할 수 없을까라는 고민 끝에, 라우터의 NAT기능과 게이트웨이,허브 및 네트워크 관리 도구를 통합하여 나온 물건이 인터넷 공유기 이다. 모든 공유기는 허브라는 네트워크를 분리하는 기능을 가지고 있으며, 이는 공유기에 연결된 컴퓨터들이 사설IP를 이용하여 통신할 수 있도록 해준다. NAT는 주소 변경 기술로, 우체국 사서함과 비슷한 기능을 한다. 패킷을 적당한 컴퓨터로 재전송해 주는 기능을 한다. 과거에는 어디까지나 보조 기능이였던 AP를 구성하는 기술이 지금에는 가장 중요한 기능이 되어서 수요가 폭등하였다.

공유기 = NAT + 스위치 + 허브 + 라우터

NAT(Network Address Translation,네트워크 주소 변환)

공유기는 공인 IP주소를 가상 IP주소로, 또는 그 반대로 변환시켜 주는 역할을 한다.

HUB

네트워크에서 사용되는 허브는 이더넷 허브, 토큰링 허브 등이 있지만 허브라고 하면 보통 이더넷 허브를 말한다. 여러 개의 포트가 있는데 그 중 한 포트로 들어온 패킷을 단순하게 들어온 포트를 제외한 모든 포트로 보내주는 역할은 한다. OSI 1계층에 속하는 기기로 허브에 연결된 케이블 중 한 케이블로 신호가 들어오면 같은 신호를 다른 모든 케이블로 전달하는데, 이것을 플로딩이라 한다. 예를 들어 허브에 랜 카드 여럿이 연결되 있는데 한 랜 카드에서 허브에 연결된 케이블로 신호를 보내면 다른 랜 카드들은 그 신호를 받고 싶은 지 여부와 관계 없이 무조건 신호를 받아야 하는 것이다. 신호를 받은 랜 카드는 자신에게 온 신호인지 확인하고 자신에게 온 신호가 아니면 무시한다. 언뜻 보면 비효율적인 동작으로 보일 수 있지만, 신호를 받고 싶은 랜 카드에게만 신호를 보내기 위해서는 어떤 포트에 어떤 랜 카드가 연결되어 있는지 기억해야 할 것이고, 따라서 내부에 저장장치가 필요할 것이고, 또 저장된 내용을 읽어 어떤 포트로 신호를 내보내야 할 지를 결정해야 하기 때문에 시간이 걸릴 것이며, 이런 동작을 하도록 장비를 만들어야 하기 때문에 장비 가격이 더 비싸질 것이다. 이런식으로 동작을 하는 기기를 스위치라고 한다.
예전에는 가격 문제 등의 이유로 모든 허브를 스위치를 바꾸는 것도 곤란했던 시절도 있었지만, 2000년대를 넘어서는 순수한 허브는 소규모, 대규모를 따지지 않고 대부분 사장되었고 모두 스위치로 교체되었다.

스위치

허브가 단순하게 한 포트로 신호가 들어오면 같은 신호를 다른 모든 포트로 전달하는 것에 비해, 스위치는 필요로 하는 포트로만 신호를 전달한다. 따라서 스위치에서는 불필요한 트래픽이 감소하게 되며, 이는 곧 네트워크에서의 데이터 전송 속도의 향상으로 이어진다.
OSI 2계층의 데이터링크 계층의 용도로 사용되는 스위치를 L2스위치라고 불린다.
IP주소를 기반으로 동작하는 상위 계층의 장비의 경우 IP 스위치,OSI 3계층 네트워크 계층의 용도로 L3 스위치라고 불린다. 스위치를 간단하게 정리하자면, 라우터에 붙어있는 네트워크 포트 수가 부족할 때 따로 연결해서 사용하는 기계이다.

AP(Access Point)

흔히 인터넷 공유기=AP 라고 생각하는데, 인터넷 공유기가 AP의 한 종류라고 보는 것이 맞다. 꼴랑 LAN포트 하나와 안테나 하나로 이루어진 담배갑 크기의 AP나, 아예 LAN포트 없이 다른 AP를 이용하여 릴레이 방식으로 서비스를 제공하는 AP도 있으며, 건물 외부 설치용으로 지향성 안테나를 설치하는 경우도 있다. 노트북도 설정만 잡아주면 AP로 사용할 수 있다. 최근에는 외장하드등을 끼워서 이동식 NAS 처럼 쓸수 있는 충전식 무선 AP도 나온다
집 주변에 보안설정이 안 된 AP가 있다면 공짜로 인터넷을 즐길 수 있다. 반대로 AP 보안설정에 소홀히 하면, 어느 순간 네트워크 안에 모르는 컴퓨터가 존재하는 황당한 경우를 볼 수 있으며, 재수가 없으면 접속자의 컴퓨터에서 공유기나 공유기에 연결된 다른 컴퓨터로 웜이 옮을 수도 있다. WPA/WPA2 PSK설정이나 MAC주소 인증 정도는 켜 두도록 하자.

MAC(Medium/Media Access Control)

데이터 통신에서 쓰이는 프로토콜의 계층, OSI 7계층에서 데이터 링크 계층의 일부에 해당한다. MAC주소는 간단히 말해 인터넷을 할 수 있는 **이더넷 기반 기기에는 모두 다 하나씩 할당되어 있는 고유한 ID**이다. PC의 랜카드나 스마트폰의 와이파이 모듈에도 1개씩 할당되어 있다. 인터넷전화나 IPTV역시 마찬가지이다. 또한 인터넷과 직접적으로 연결되지는 않지만 블루투스를 이용하는 장치에도 고유의 주소가 할당 되어 있다. (블루투스 주소라고 한다.)자세히 안보면 맥주소랑 같아 보이고 많은 경우에 맥주소라고 뭉뚱그려 부르기도 하지만 엄연히 다르다. 총 48비트로 구성되어 있고 편의상 8비트씩 6자리로 구분하여 표기한다. AB-CD-EF-12-34-56 같은 형식. 앞의 3자리(24비트)는 제조사 코드, 뒤의 3자리(23비트)는 기기 고유코드이다. 48비트 이므로 가질 수 있는 가짓수는 2^48=약 281조개의 서로 다른 ID가 존재한다.
초창기에는 그냥 ROM에 박아버려서 변경이 불가능했지만, 요즘은 플래시 메모리 같은 곳에 저장하기에 간단히 변경이 가능하다. 또한, MAC 주소를 가상으로 부여해서 다른 MAC 주소를 가진 것처럼 동작하는 것도 가능하다. 실제로 이렇게 MAC 주소를 도용하여 이루어지는 해킹 기법인 MAC 스푸핑이 존재한다. 공유기의 경우에도 MAC을 변경하는 기능이 있는데, 이는 ISP에서 공유기의 MAC을 차단하는 경우에 이를 우회하기 위해서 주로 쓰이

며, IP 주소를 바꿀 때도 사용된다. 이렇게 WIFI나 LAN같은 각각의 인터페이스에 MAC 주소가 부여된다면, 이제 IP 주소와 MAC 주소를 연결짓는 ARP 프로토콜을 이용해 IP와 MAC를 대응시키면 드디어 기기의 정보를 인터넷으로 연결시킬 수 있게 되는것. 물론 아직도 OSI 모형에 따른 단계가 한참 남아있긴 하지만...

자신의 컴퓨터의 MAC 주소를 알고 싶다면 명령 프롬프트를 켜고 'getmac'을 쳐주자.

DMZ

인터넷 공유기를 통해 네트워크 외부에 노출된 컴퓨터. 어원은 원본 단어가 맞다. 말 그대로 공유기가 방어를 하지 않는 구역이라서 이런 명칭을 붙게 된 것.

공유기에는 방화벽 기능이 있어서 특정 포트를 제외하고는 기본적으로 모두 차단되어 있다. 일상적인 업무나 웹 서핑에서는 별 문제가 없지만, 공유기를 통해 IP를 공유하는 컴퓨터로 eMule같은 P2P를 사용하려 들면 네트워크 에러를 띄우면서 여러 가지 제한사항이 따르는 로우아이디를 받는 등의 문제가 생기기 마련이다. 이럴 때 공유기에서 해당 PC를 DMZ로 지정을 하면 해당 PC에 한해 모든 포트를 열어주기 때문에 문제를 해결할 수 있다. 하지만 공유기의 보호를 해제하고 모든 포트를 여는 것이기 때문에 큰 위험이 따른다는 점은 주의해야 할 부분. 그래서 DMZ를 설정하지 않고 특정 포트만 여는 방법을 쓰는 경우도 있다.

VPN

가상 사설망/Virtual Private Network / VPN

덩치 큰 집단의 여러 곳에 퍼져있는 컴퓨터를 잇는 사설 네트워크를 만들 때, 일일이 전선으로 연결하기는 돈이 많이 들고 물리적으로 보안에 취약하다. 그래서 그 대신 인터넷 네트워크와 암호화 기술을 이용하여 통신 시스템을 구축하는 것을 말한다.

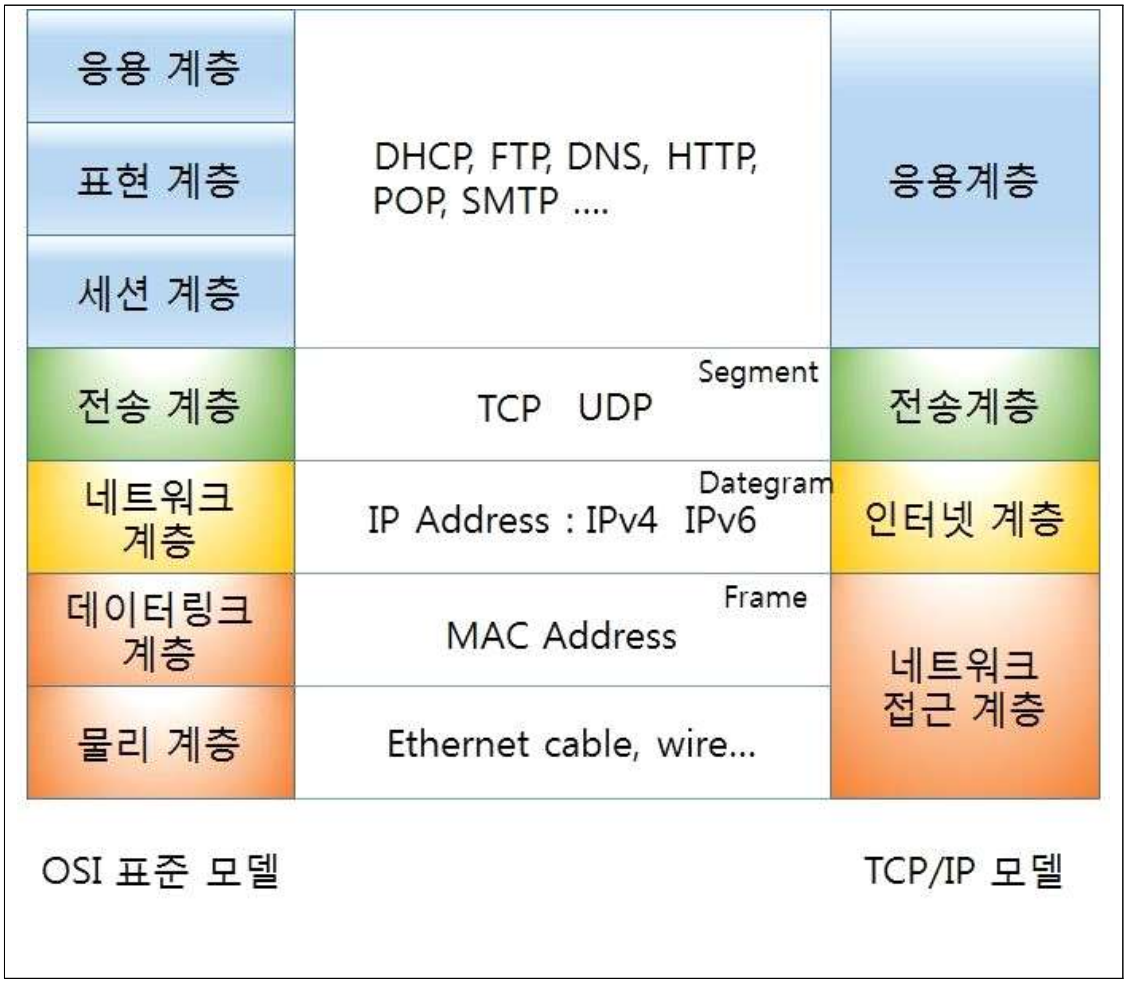
공공기관이나 사기업 등 단체에서 내부인들만 쓸 수 있는 특수목적의 인트라넷을 구축할 때는 보통 해당되는 컴퓨터만 전용선으로 연결해서 제3자가 함부로 접근하지 못하는 서버를 쓴다. 그러나 회선이 없는 지역에서는 망 자체에 접근이 불가능해진다. 또한 전국, 해외 단위로 회사가 커지면 커질수록 전용선 구축 비용이 천문학적으로 늘어난다. 따라서 확장성이 뛰어난 인터넷을 인트라넷처럼 사용할 수 있도록 하는 기술이 개발되었다. 그게 바로 가상 사설망, 즉 VPN이다.

가상 사설망은 업무에만 쓰이는 기술이 아니다. 인트라넷의 확장 또는 검열, 지역제한이 있는 인터넷의 자유로운 인터넷을 중계해주기도 한다.

대부분의 사람에게는 인터넷 검열을 피하는 도구로만 알려져 있다.

<원리>
인터넷에만 연결된 단말기, 인터넷과 인트라넷에 동시에 연결된 VPN 라우터와 인트라넷에만 연결된 단말기가 있다.
인터넷에만 연결된 단말기에서는 인트라넷에 접근할 수는 없다. 왜냐하면 망이 완전히 분리되어 있기 때문인데, 이를 이어주는 브릿지 같은 역할을 하는것이 VPN 라우터다.
인터넷 단말기에서 라우터에 VPN 프로토콜 중 하나를 이용하여 연결을 시도한다. 연결시에는 비밀번호 같은 자격 증명이 필요한 경우가 보통이며 성공시에는 단말기와 VPN 라우터 사이에 암호화된 연결이 형성되게 된다. 이를 터널링이라고 한다.
VPN 라우터는 해당 단말기가 마치 인트라넷에 연결된 것처럼 단말기와 인트라넷 사이를 중계하는 역할을 수행하게 된다. 따라서 단말기는 인터넷과 인트라넷을 동시에 사용할 수 있는 상태가 되는것인데, 단말기를 통해 인트라넷에 접속한 경로를 보면 인터넷/인트라넷 상에는 전부 라우터까지의 접속만 수행한 것으로 보인다.
이를 이용해 정부나 ISP의 검열이나 접속 차단을 피할수도 있는데, 라우터까지의 모든 통신 기록이 암호화되므로 패킷을 열어보기 힘들다. 또 패킷 도착지가 라우터 주소에서 끊기기 때문에 어느 사이트에 접속하는지도 알 수 없게된다.

TCP/IP



TCP (Transmission Control Protocol)
IP (Internet Protocol)
현재 수많은 프로그램들이 인터넷으로 통신하는 데 있어 가장 기반이 되는 프로토콜로 실제 대다수 프로그램은 TCP와 IP로 통신(정확히는 '네트워킹')하고 있다. ARPANET이 개발된 이후 현재의 인터넷으로 발전해나가는 과정에서 대부분의 데이터 통신이 TCP와 IP 기반으로 이루어졌기에 인터넷 프로토콜 그 자체를 표현하는 용어이기도 했고, 다양한 프로토콜이 개발된 현 시점에도 사실상 인터넷 프로토콜을 대표하는 용어로 사용 중이다. 이를 이용해서 컴퓨터를 연결하는 체계를 이더넷(Ethernet)이라고 부른다. 크게 4개의 계층으로 되어 있다. OSI 모형 7계층과 맵핑이 가능하다.
그 때문에 프로그램 설명서에 "**TCP/IP 지원**"이라 써 있으면 인터넷에 연결하여 쓰는 기능이 포함되어 있다는 소리이다.
보통 하나로 싸잡아 표현하긴 하나 TCP와 IP는 별개이다. 네트워크의 경우 계층이 정의되어 있고 각 계층마다 하는 역할과 책임지는 영역이 나뉘어져 있기 때문에 묶어서 표현한다는 것뿐이지 역할에는 많은 차이가 있다.

Transmission Control Protocol: TCP
컴퓨터가 다른 컴퓨터와 데이터 통신을 하기 위한 규약(프로토콜)의 일종이다. 한국어로 번역하면 전송 제어 프로토콜. TCP는 세계 통신표준으로 개발된 OSI 모형에서 4번째 계층인 전송 계층(Transport Layer)에서 사용하는 규약으로, 보통 하위 계층에서 사용하는 IP와 엮어서 TCP/IP로 표현하는 경우가 많다. 동일 계층에서 사용하는 또 다른 프로토콜로 UDP가 존재한다.

Internet Protocol :IP
이 프로토콜에서 각 장치를 나타내는 IP 주소를 가리키는 말로 쓰인다.각 장치들의 주민등록번호라고 생각하면 쉽다.
컴퓨터의 경우 사용하는 운영체제도 서로 다르고, 프로그램의 경우 아예 구현된 언어가 다르기 때문에 네트워크에서 이들이 통신할 수 있도록 하려면 공통된 통신 규약(프로토콜)이 필요하다. 컴퓨터 통신의 태동기였던 1960년대에는 장비 제조사마다 각기 다른 프로토콜을 사용하고 있었고, 다른 회사의 장비 사이에는 통신이 힘들거나 아예 불가능했다. 이 때문에 관련 프로토콜을 국제적으로 표준화하기 위한 ISO 위원회가 발족되었고, 1977년에 OSI 7계층 모델을 발표한다. 한편, 인터넷을 위한 통신 프로토콜을 만들고 있던 IETF는 독자적으로 Internet Protocol Suite를 발표, ISO의 X.200이 이해관계자들(IBM/DEC/Intel/Apple.. etc) 사이의 다툼으로 지연되는 사이 TCP/IP가 사실상의 표준(de facto standard)이 된다.

IP는 OSI의 Layer 3(Network Layer)와 Internet Protocol Suite의 Layer 3(Internet Layer)에 위치하는 프로토콜이다.

호스트에서 호스트까지의 통신, 즉 보내는 컴퓨터에서 받는 컴퓨터까지의 통신을 책임진다. 하는 작업을 아주 이해하기 쉽게 대략적으로 설명하면 편지 봉투에 보내는 주소, 받는

주소를 작성하고 우표를 붙여서 우체통에 넣는 일과 우편함에 들어온 편지를 꺼내서 나한테 온 편지가 맞는지 확인하는 정도의 작업이라고 생각하면 된다. 제대로 설명하려고 하면, IP의 역할(flow control 외), Network layer에서의 보안, IP packet(datagram) 구조 등은 관련학부 및 대학원 한학기 이상 분량이다. 이 글에서는 일상생활에 필요한 지식 정도를 다루기로 한다.
원래 설계하던 시기에는 주 작업 이외에도 몇 가지 부가적인 작업을 할 수 있도록 만들었는데, 실제 상위 계층에서 다 처리할 수 있는 작업이라서 현재는 그냥 공기 취급. IP를 통하지 않고 현 인터넷을 통해 통신한다는 건 불가능하기 때문에 매우 중요한 계층이다. 다만 LAN 환경 등에서는 MAC 주소 기반 통신이 필요한 경우도 있는 등, IP가 만능은 아니다.
스크립트 키디들은 IP만 알면 컴퓨터를 해킹할 수 있다고 하기도 하는데, IP만으로 가능한 공격 방식은 DDoS 하나뿐인데다 개인 PC에서 그렇게 많은 트래픽이 발생하면 ISP에서 막는다.

Domain Name System : DNS

IP 네트워크에서 사용하는 시스템이다. 우리가 인터넷을 편리하게 쓰게 해주는 것으로, 영문/한글 주소를 IP 네트워크에서 찾아갈 수 있는 IP로 변환해 준다. 모든 웹 사이트 주소를 도메인 대신 아이피로 외운다고 생각하면 머리 아파진다.
DNS는 도메인 이름과 IP주소를 변환하는 역할을 한다.
리소스 레코드를 가지며, 이 리소스 레코드는 A,AAAA,CNAME,NS,MX,SPF,PTR등으로 이루어져 있다.
Forward Zone과 Reverse Zone을 가진다. 주로 Forward Zone에는 도메인을 구성하는 호스트에 대한 정보를, Reverse Zone에는 DNS 서버 자기 자신에 대한 정보를 기록한다.
DNS 서버에 질의하면 돌아오는 응답은 Authoritative answer와 Non-authoritative answer로 나뉜다.

Authoritative answer
DNS 서버가 질의 받은 도메인 또는 IP 주소의 레코드를 Forward Zone, Reverse Zone 모두 가지고 있을 경우에 하는 응답이다. 여러 호스트로 구성되어 있는 도메인의 네임서버에 도메인을 구성하고 있는 호스트의 주소를 직접 질의할 때 얻을 수 있다.
Non-authoritative answer
DNS 서버가 질의 받은 도메인 또는 IP 주소의 레코드를 Forward Zone, Reverse Zone 중 하나 이상 가지고 있지 않을 경우에 하는 응답이다. 도메인의 네임 서버에 해당 도메인을 구성하지 않은 호스트, 즉 외부 서버의 주소를 질의했을 때 받을 수 있는 응답이다.
가정집에서 DNS 서버에 질의할 때 받게 되는 응답이 바로 이것이다.

DDNS : Dynamic DNS

실시간으로 DNS를 갱신하는 방식이다. 주로 **도메인의 IP가 유동적인 경우** 사용된다. ip가 바뀌어도 **DDNS로 설정한 도메인 값은 변하지 않기 때문에 용이하게 접속**가능하다.

일반적으로 우리가 이용하는 포털사이트나 각 기업, 정부기관의 홈페이지 들은 해당 기업이나 기관 등이 소유한 고정 IP를 통해서 DNS 주소를 할당 받기 마련인데, 가정 단위에 있어서 고정 IP를 할당받는 것은 상당한 비용이 들 뿐더러 IP 추적에 의한 사생활 침해 요소가 있기 때문에 유동 IP를 사용하게 된다. 그런데 유동 IP 에 그냥 DNS 주소를 할당해 버리면 사용자의 IP가 바뀌기 전 까지는 멀쩡히 작동하지만, IP 유동이 일어나는 순간 해당 주소로 들어온 트래픽은 본래 그 주소를 할당받은 사용자에게 가지 않고 새로이 그 IP를 차지하게된 엉뚱한 사용자에게 가게된다. 이를 극복하기 위해 나온것이 바로 DDNS이며 일반적으로는 유동 IP로 인터넷을 공급받는 대다수의 인터넷 사용자들이 개인 서버나 NAS 구축을 하려 할 때 이용하게 된다.

한국에서 가장 널리 알려진 것으로는 EFM 네트웍스에서 ipTIME 공유기 내장 기능으로 DDNS 기능을 제공하는 것이 널리 알려져 있으며 **주소는 *.iptime.org** 형식으로만 사용이 가능하다.
그 외 자가 소유의 고유한 도메인을 DDNS 서비스가 제공되는 네임서버 서비스 업체(DNSEver, DNSZi 등)에 등록 후, 해당 네임서버 서비스 업체에서 제공하는 방법(주기적으로 서버가 위치한 IP에서 네임서버 서비스 업체에 쿼리를 날려주는 방식 등)으로 네임서버 서비스 업체의 A 레코드 IP를 갱신시켜 주는 방식 등으로 DDNS 서비스를 제공받을 수 있다.

WoL (Wake on Lan)

네트워크 메시지를 보냄으로써 컴퓨터의 전원을 켜거나 절전 모드에서 깨어나게 하는 이더넷 컴퓨터 네트워킹 표준이다. 공유기와 바이오스에서 WOL 설정이 사전 적용되어 있어야 한다. 일반적으로 대다수의 네트워크 카드가 WOL 기능을 지원하므로 설정항목에 없는 경우 네트워크 드라이버 업데이트를 권장한다.
WOL은 일반적으로 유선 상으로만 동작하는 기능이다. 유선 LAN 카드는 일반적으로 전원이 인가되어 있고, 컴퓨터가 완전히 종료된 상태에서도 대기전력을 사용하여 특정 신호를 감지한다. 하지만 무선 LAN의 경우 데스크탑보다는 노트북에 장착되어 있는 경우가 많다. 노트북은 특성상 전력 소모를 최소화 하여야 하기 때문에 전원이 꺼져 있는 상태에서는 무선 LAN이 아예 동작하지 않는다. 설령 동작을 하더라도 주변에 개방형 AP가 없다면 말짱 꽝. 무선랜에서도 WOL을 사용 할 수 있는 WOWLAN이 있긴 하지만 설정하기 힘들고 지원을 안하는 랜카드도 많으며 기껏 설정해도 작동을 안하는 경우가 잦아 써먹을수 없다.
WoL이 활성화된 컴퓨터들은 컴퓨터의 전원이 꺼진 동안에 Magic Packet이 도착하기를 기다린다. 매직 패킷은 16진수 FF FF FF FF FF FF 뒤에 해당 컴퓨터의 MAC ADDRESS를 16번 나열한 102Bytes짜리 패킷이며, 보통은 UDP 7 또는 9 포트로 전송된다. 이 매직패킷은 보통 모든 플랫폼에서 작동할 수 있는 소프트웨어로 보내지나, 라우터와 인터넷 기반 웹사이트에서도 보낼 수 있다.

최근의 메인보드/OS가 컴퓨터의 전원을 완전히 종료하지 않고, 무조건 최대절전모드를 유도하면서(S0~S5), 실제 컴퓨터가 완전히 종료되지 않아. 과거의 문서를 참고할 경우 WOL이 정상적으로 수행되지 않는 이슈가 다수 보고된다.
무선랜 사용중이나 기타 이유로 WOL을 사용 할수 없다면 전력 차단/인가 기능이 있는 스마트플러그를 구매 후 메인보드 설정에서 전력 인가시 컴퓨터가 켜지는 옵션을 설정해두면 이를 이용해 WOL처럼 써 먹을수 있다.
공유기의 경우 거의 모든 공유기가 이 기능을 지원하며 메인보드의 경우는 MSI는 WOL기능을 켜놓고 윈도우를 포멧하여도 사용할수 있는 것으로 파악된다. 기가바이트는 켜놓고 포멧한다면 다시는 사용할 수 없게 된다.

OSI 7 계층

1: [물리 계층]
물리 계층(Physical Layer, 1계층)은 OSI 모델의 맨 밑에 있는 계층으로서, 네트워크 데이터가 전송되는 물리적인 매체이다. 데이터는 0과 1의 비트열로 ON, OFF의 전기적 신호 상태로 이루어져 있다. 이 계층은 전압, 허브, 네트워크 어댑터, 중계기 및 케이블 사양을 비롯해 사용된 모든 하드웨어의 물리적 및 전기적 특성을 정의한다. 물리 계층은 연결을 설정 및 종료하고 통신 자원을 공유하는 수단을 제공하며 디지털에서 아날로그로 또는 그 반대로 신호를 변환하는 역할을 한다. OSI 모델에서 가장 복잡한 계층으로 간주된다.

2: [데이터링크 계층]
데이터링크 계층(DataLink Layer, 2계층)은 물리적인 네트워크를 통해 데이터를 전송하는 수단을 제공한다. 1홉 통신을 담당한다고도 말한다. 홉(hop)은 컴퓨터 네트워크에서 노드에서 다음 노드로 가는 경로를 말한다. 1홉 통신이면 한 라우터에서 그다음 라우터까지의 경로를 말한다. 주목적은 물리적인 장치를 식별하는 데 사용할 수 있는 주소 지정 체계를 제공하는 것이다. 데이터 링크 계층은 포인트 투 포인트 간의 신뢰성 있는 전송을 보장하기 위한 계층으로 CRC 기반의 오류 제어와 흐름 제어가 필요하다. 네트워크 위의 개체들 간 데이터를 전달하고 물리 계층에서 발생할 수 있는 오류를 찾아내고 수정하는 데 필요한 기능적, 절차적 수단을 제공한다. 이 계층의 예시를 들자면 브리지 및 스위치 그리고 이더넷 등이 있다.

3: [네트워크 계층]
네트워크 계층(Network Layer, 3계층)에서는 2홉 이상의 통신(멀티 홉 통신)을 담당한다. OSI 7 계층에서 가장 복잡한 계층 중 하나로서 실제 네트워크 간에 데이터 라우팅을 담당한다. 이때 라우팅이란 어떤 네트워크 안에서 통신 데이터를 짜여진 알고리즘에 의해 최대한 빠르게 보낼 최적의 경로를 선택하는 과정을 라우팅이라고 한다. 네트워크 계층은 네트워크 호스트의 논리 주소 지정(ex : ip 주소 사용)을 확인한다. 또한 데이터 스트림을 더 작은 단위로 분할하고 경우에 따라 오류를 감지해 처리한다. 그리고 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층으로서 다양한 길이의 데이터를 네트워크들을 통해 전달하고 그 과정에서 전송 계층이 요구하는 서비스 품질을 제공하기 위한 기능적, 절차적 수단을 제공한다. 네트워크 계층은 라우팅, 흐름 제어, 세그멘테이션, 오류제어, 인터네트워킹 등을 수행한다. 라우터가 3계층에서 동작하고, 3계층에서 동작하는 스위치도 있다.

4: [전송 계층]

전송 계층(Transport Layer, 4계층)의 주목적은 하위 계층에 신뢰할 수 있는 데이터 전송 서비스를 제공하는 것이다. 컴퓨터와 컴퓨터 간에 신뢰성 있는 데이터를 서로 주고받을 수 있도록 해주어 상위 계층들이 데이터 전달의 유효성이나 효율성을 생각하지 않도록 부담을 덜어주는데, 이때 시퀀스 넘버 기반의 오류 제어 방식을 사용한다. 흐름 제어, 분할/분리 및 오류 제어를 통해 전송 계층은 데이터가 오류 없이 점-대-점으로 전달되게 하는데 신뢰할 수 있는 데이터 전송을 보장하는 것은 매우 번거롭기에 OSI 모델은 전체 계층을 사용한다. 전송 계층은 연결형 프로토콜과 비 연결형 프로토콜을 모두 사용한다. 전송 계층의 예로는 특정 방화벽이나 프록시 서버가 있다.

5: [세션 계층]

세션 계층(Session Layer, 5계층)에서는 두 컴퓨터 간의 대화나 세션을 관리하며, 포트(Port) 연결이라고도 한다. 모든 통신 장치 간에 연결을 설정하고 관리 및 종료하고 또한 연결이 전이중(Full duplex / 양방향)인지 반이중(half duplex / 단방향)인지 여부를 확인하고 체크 포인팅과 유휴, 재시작 과정 등을 수행하며 호스트가 갑자기 중지되지 않고 정상적으로 호스트를 연결하는 데 책임이 있다. 즉 이 계층에서는 TCP/IP 세션을 만들고 없애고 통신하는 사용자들을 동기화하고 오류 복구 명령들을 일괄적으로 다루며 통신을 하기 위한 세션을 확립, 유지, 중단하는 작업을 수행한다.

6: [표현 계층]

표현 계층(Presentation Layer, 6계층)에서는 응용 계층으로부터 전달받은 데이터를 읽을 수 있는 형식으로 변환하는데 표현 계층은 응용 계층의 부담을 덜어주는 역할이 되기도 한다. 응용 계층으로부터 전송받거나 응용 계층으로 전달해야 할 데이터의 인코딩과 디코딩이 이 계층에서 이루어진다. 그리고 표현 계층은 데이터를 안전하게 사용하기 위해서 암호화와 복호화를 하는데 이 작업도 표현 계층에서 이루어진다. 예를 들면 유니코드(UTF-8)로 인코딩 되어있는 문서를 ASCII로 인코딩 된 문서로 변환하려 할 때 이 계층에서 변환이 이루어진다.

7: [응용 계층]

응용 계층(Application Layer, 7계층)에서는 OSI 7계층 모델에서 최상위 계층으로 사용자가 네트워크 자원에 접근하는 방법을 제공한다. 그리고 계층 7은 최종적으로 사용자가 볼 수 있는 유일한 계층으로 모든 네트워크 활동의 기반이 되는 인터페이스를 제공하는데, 즉 사용자가 실행하는 응용 프로그램들이 계층 7에 속한다고 보면 된다. 예를 들면 가상 터미널인 텔넷(telnet), 구글의 크롬(chrome), 이메일(전자우편), 데이터베이스 관리 등의 서비스를 제공한다. 사용자와 가장 가까운 계층이다.