

01.17

포트 포워딩

포트 포워딩(port forwarding)은 컴퓨터 네트워크 상에서 패킷이 방화벽이나 라우터 같은 네트워크 게이트를 지날 때 IP 주소와 포트 번호 결합의 통신 요청을 다른 곳으로 넘겨주는 네트워크 주소를 변환해주는 것입니다. 즉, 외부에서 특정 포트로 통신 요청을 했을 경우, 이를 받을 장비를 미리 지정하고 장비에서 받을 내부 포트를 정해주는 것입니다.

OSI 7계층 - 세션 계층, 표현 계층, 응용 계층

• 세션 계층

- 애플리케이션 간의 대화를 유지하기 위한 세션을 구축하고 관리하며 종료시키는 역할을 하는 계층입니다.
- 상위 계층인 표현 계층 사이의 연결을 설정하고 관리 및 종료시키며 데이터 교환을 관리합니다. TCP/IP 세션도 이 계층에서 관리한다고 볼 수 있으며, SSH, TLS 등의 프로토콜이 이 계층에 속합니다.

• 표현 계층

- 응용 계층의 다양한 정보의 표현 형식을 공통의 전송 형식으로 변환하고 암호화 및 데이터 압축 기능 등을 수행합니다. 즉, 한 시스템의 애플리케이션에서 보낸 정보를 다른 시스템에서 애플리케이션이 읽을 수 있도록 하는 계층입니다.
- 사용자가 이해하는 문장(추상 구문)을 전송 형태의 구문(전송 구문)으로 변환하는 기능을 수행합니다(암호화, 압축). ASCII, JPEG 등의 프로토콜이 이에 속합니다.

• 응용 계층

- 사용자가 네트워크 자원에 접근할 수 있는 방법(인터페이스)을 제공하는 계층입니다.
- 세션 계층 및 표현 계층과 함께 설명될 때가 많은데, 이는 세션 계층 및 표현 계층에서의 과정이 응용 어플리케이션 내에서 이루어지기 때문입니다.
- 해당하는 프로토콜로 HTTP, SMTP, FTP, DNS 등이 있습니다.

브라우저에 www.naver.com을 입력했을 때

*해당 단계에서 도메인에 매핑된 IP를 찾으면 → O, 못 찾으면 → X

1) 현재 컴퓨터(로컬)의 hosts 파일을 찾습니다. 찾는 도메인이 있으면, 매핑된 IP가 클라이언트의 브라우저에 반환됩니다.

- O → 8), X → 2)

2) DNS 캐시 테이블에서 도메인을 찾습니다. 찾는 도메인이 있으면, 매핑된 IP가 클라이언트의 브라우저에 반환됩니다.

- O → 8), X → 3)

3) 로컬 DNS 서버로 DNS query를 보냅니다. 로컬 DNS 서버는 내 PC에 설정되어 있는 네임 서버입니다.(ex. KT DNS, google DNS..) 로컬 DNS 서버는 질의된 도메인 명을 자신의 DNS 캐시 정보에서 확인합니다. 찾는 도메인이 있으면, 매핑된 IP가 클라이언트의 브라우저에 반환됩니다.

- O → 8), X → 4)

4) 로컬 DNS 서버가 Root DNS 서버로 도메인에 대한 DNS query를 보냅니다. Root DNS는 자신의 zone 파일에 도메인과 매핑되는 IP가 있으면 이를 로컬 DNS로 반환합니다.

- O → 7), X → 5)

5) Root DNS 서버가 도메인의 최상단 도메인인 com DNS 서버의 IP 주소를 응답합니다. 로컬 DNS 서버는 이를 받고, com DNS 서버에 DNS query를 보냅니다. (최상단 도메인은 Top-Level-Domain Nameserver, 즉 TLD 네임 서버라고 부르기도 합니다) com DNS 서버는 자신의 zone 파일에 도메인과 매핑되는 IP가 있으면 이를 로컬 DNS로 반환합니다.

- O → 7), X → 6)

6) 최상단 DNS(com)가 naver.com DNS 서버 주소를 반환합니다. 로컬 DNS는 받은 naver.com DNS 서버 주소로 www.naver.com에 대한 IP 주소를 요청하는 DNS query를 보냅니다. naver.com DNS는 존 파일 정보를 확인하고, 매핑된 IP 주소를 로컬 DNS로 반환합니다.

7) 로컬 DNS 서버는 응답 받은 IP 주소를 클라이언트의 브라우저에게 전달합니다. 그리고 TTL 시간(쿼리에 대한 결과를 받아갔을 경우 결과 값을 캐시에 저장하는 시간을 의미) 동안 해당 내용을 캐싱합니다.

8) 브라우저는 받은 IP주소로 3-way handshake요청을 합니다. 그리고 TTL 시간 동안 해당 주소를 캐싱합니다.

- 9) 브라우저의 접속 요청이 연결된 라우터로 전달되고, 이 라우터는 받은 IP주소를 가진 라우터로의 최적 경로를 라우팅 테이블에서 찾아 요청을 전송합니다.
- 10) 목적지 IP 주소의 라우터가 요청을 받아, 적합한 장비로 요청을 전달합니다.
- 11) 3-way handshake 후에, http 요청 메시지를 전달됩니다.
- 12) 요청을 받은 www.naver.com 서버는 브라우저에게 http 응답 메시지를 전달합니다.