

2025.10.02

DHCP

network

HTTP

CONTENTS

01

DHCP의 등장

02

DHCP란?

03

DHCP의 동작 원리

04

DHCP Spoofing

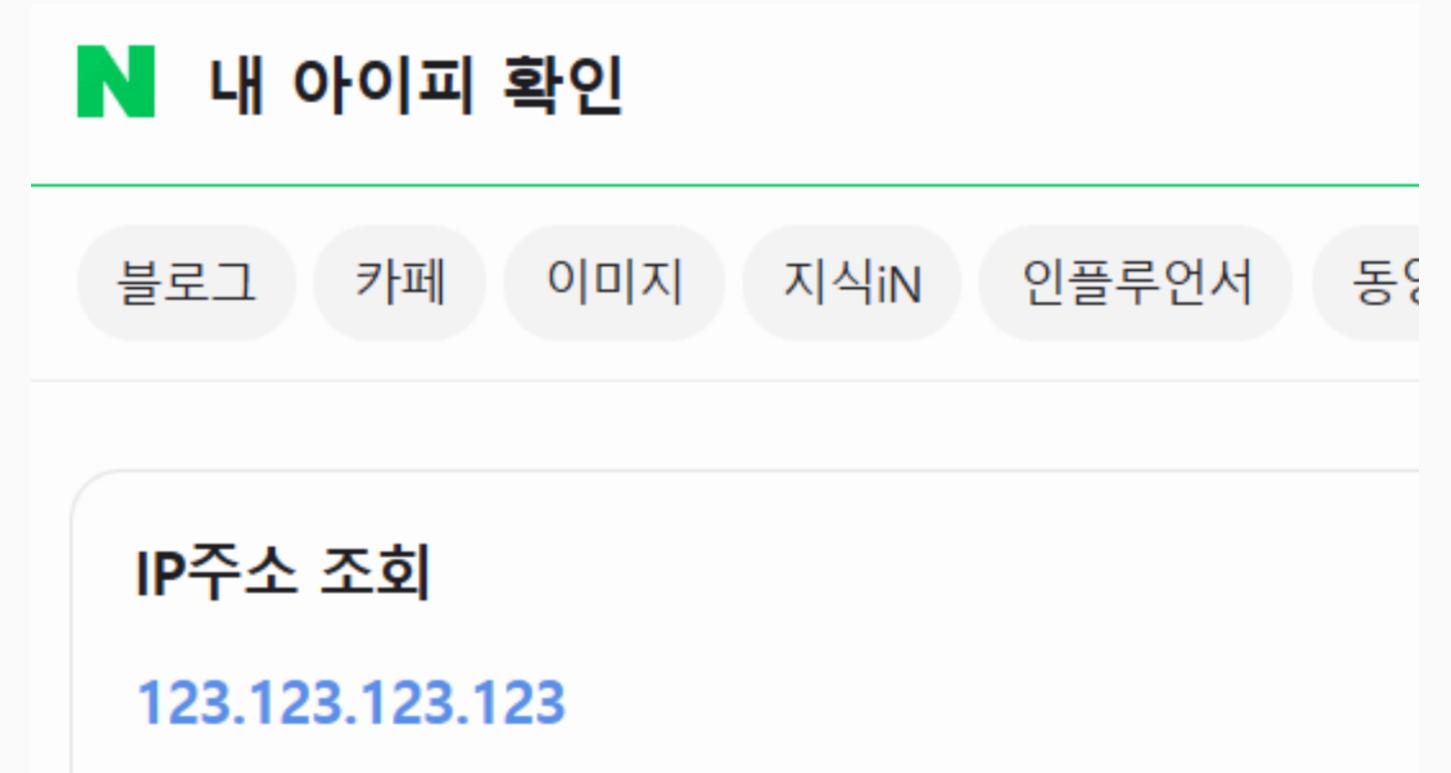
05

Relay Agent

01

DHCP의 등장

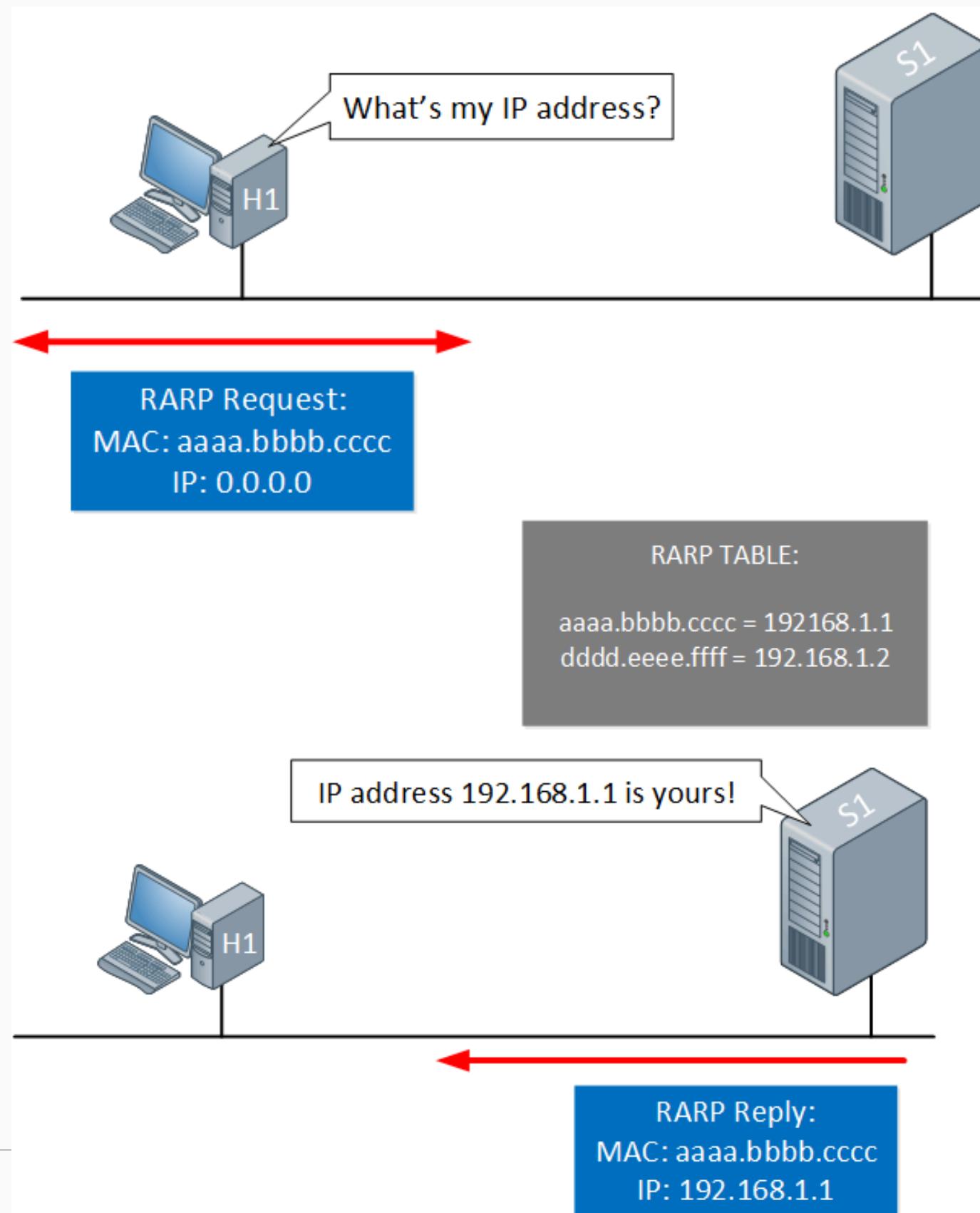
DHCP의 등장



내 IP 주소가 왜 필요할까?

- 서버로부터 응답을 받아야 하는데 어디로 받지?

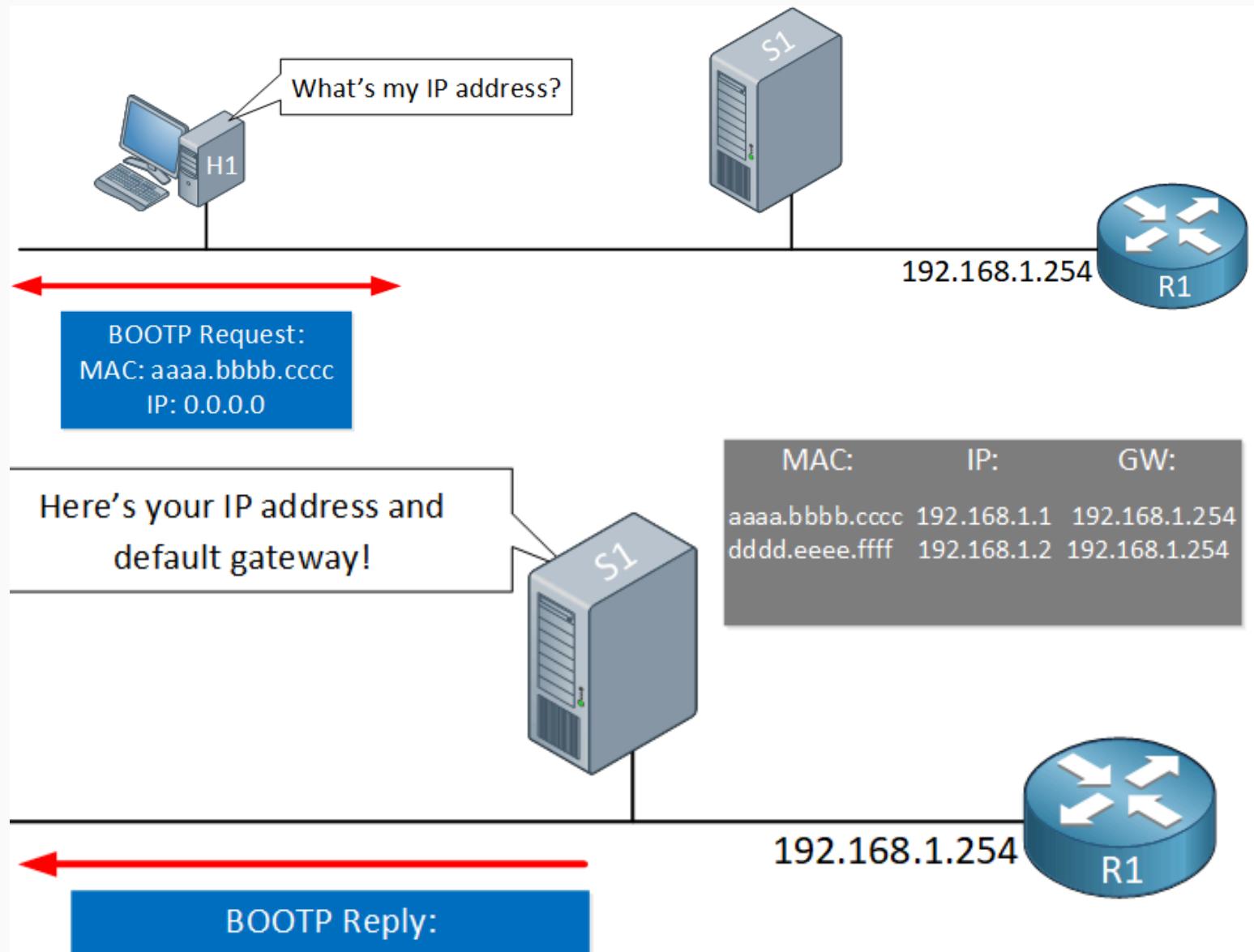
DHCP의 등장



RARP

- 내 컴퓨터의 IP의 주소가 궁금하다면?
- MAC 주소로 IP 주소를 알 수 있음

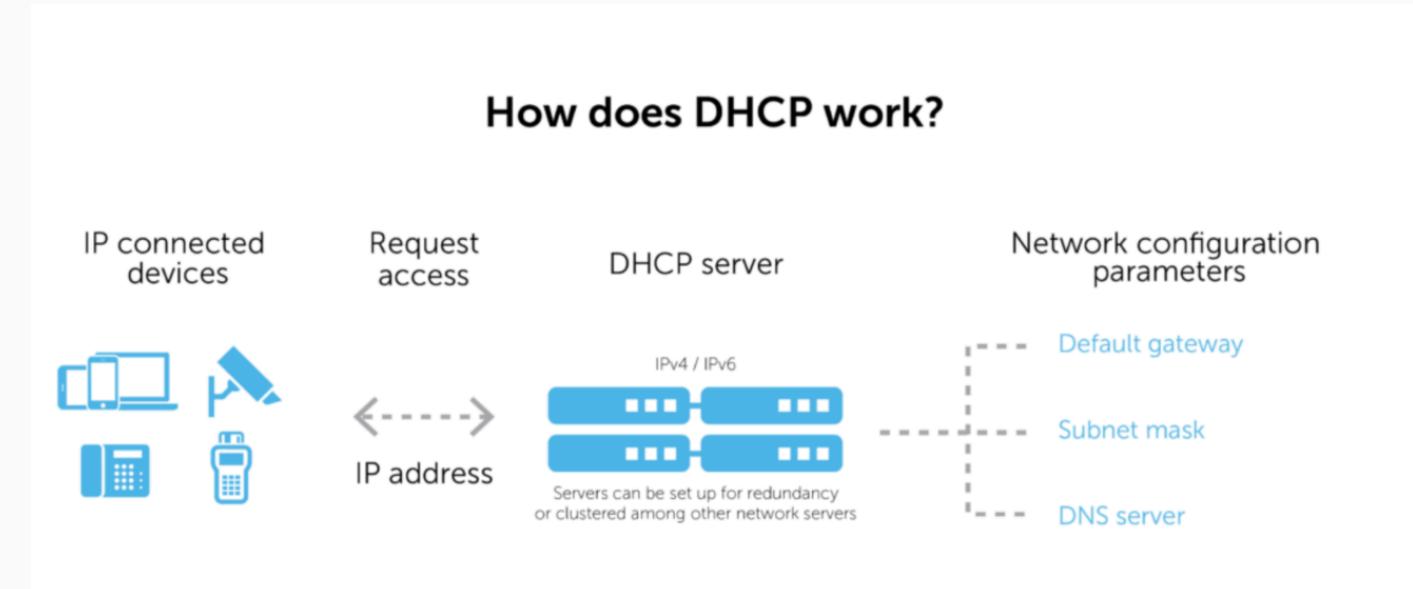
DHCP의 등장



BOOTP (BOOtstrap Protocol)

- IP 정보만 얻을 수 있는 RARP의 단점 극복
- 서버에서 클라이언트로 네트워크 정보 할당 가능
- 테이블 리스트로 관리

DHCP의 등장



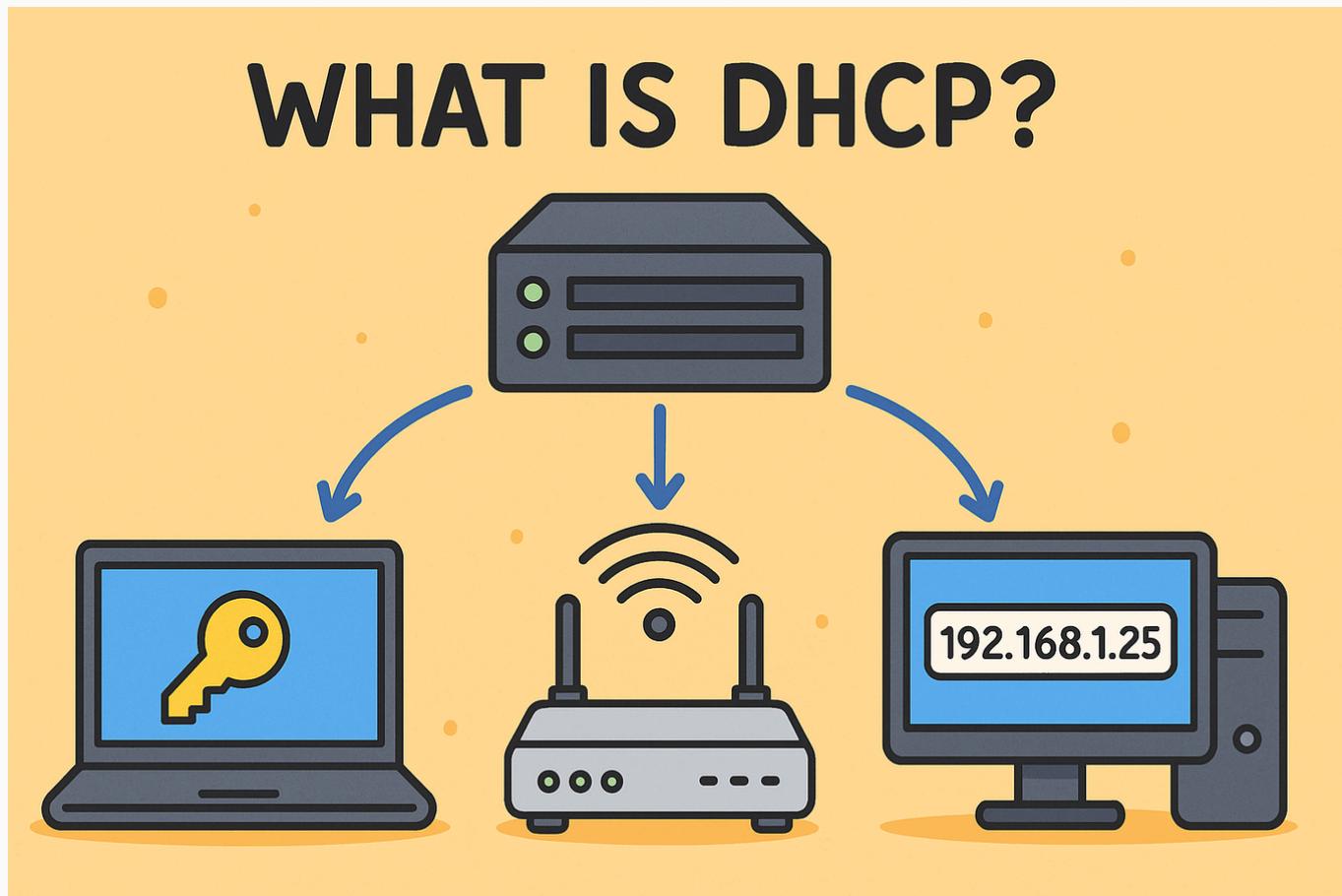
DHCP (Dynamic Host Configuration Protocol)

- 정적으로만 할당 가능한 BOOTP의 단점 극복
- 네트워크에 접속하는 장치에게 네트워크 정보를 자동 할당 및 관리

02

DHCP란?

DHCP란?



DHCP (Dynamic Host Configuration Protocol)

- 네트워크에 접속하는 장치에게 네트워크 정보를 자동 할당 및 관리
- 클라이언트에게 IP 주소를 동적으로 임대
- 이미 할당한 IP 주소
- 할당할 수 있는 IP 주소

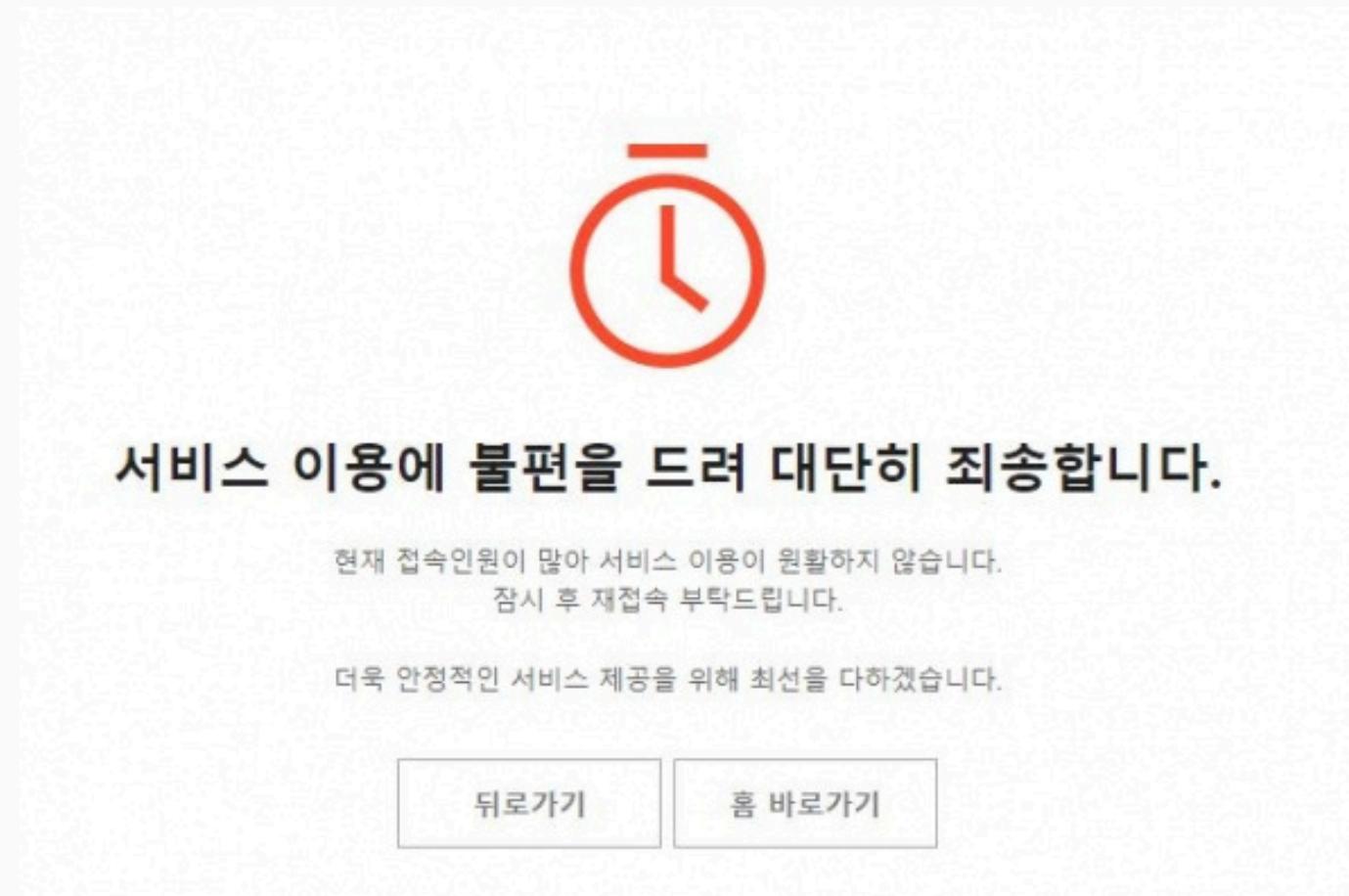
DHCP란?



장점

- 자동 할당 및 관리
- IP 주소 중복 방지
- 회수 후 재할당
- 임대 시간 설정 가능

DHCP란?



단점

- 서버가 죽는다면?
- 인증 방식이 없어 보안에 취약함
 - DHCP Spoofing

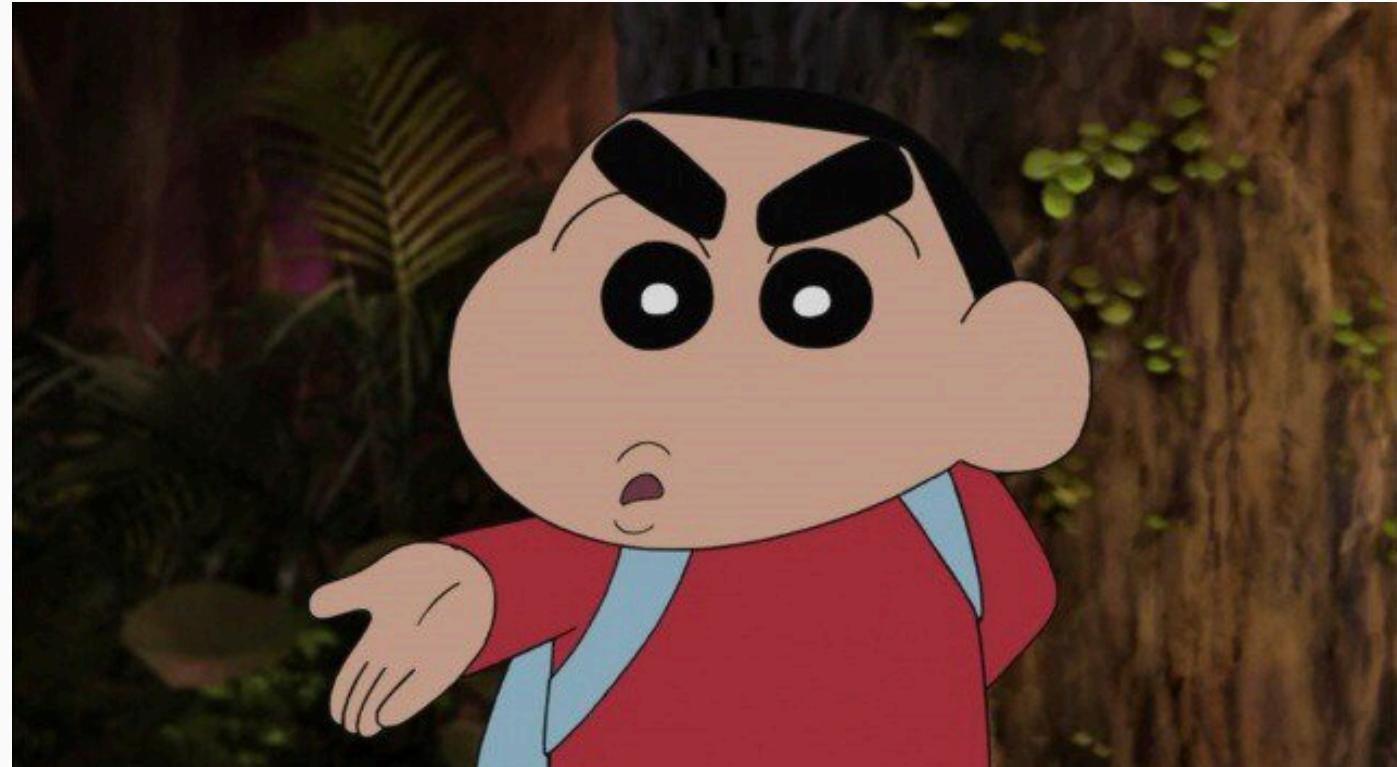
DHCP란?

DHCP의 동작 원리

- 영구적인 것이 아니라 임대 기간을 명시하여 해당 기간만 사용함
- 임대 기간 이후에도 해당 IP 주소 사용을 원한다면?
- 임대 받은 IP 주소가 더 이상 필요하지 않다면?

임대 시작 날짜 : 2025년 9월 30일 화요일 오후 8:06:30
임대 만료 날짜 : 2025년 10월 1일 수요일 오전 12:38:36

구성요소



DHCP 클라이언트

- 시스템 시작 시 DHCP 서버에 IP 주소 요청
- IP 주소를 받으면 다른 호스트와의 통신이 가능함

구성요소



DHCP 서버

- IP 주소를 클라이언트에게 자동으로 할당
- 할당된 IP 주소를 변경 없이 유지
- 앞으로 할당 가능한 IP 주소를 관리

03

임대

임대



Lease

- DHCP 서버가 클라이언트에게 IP 주소와 관련된 네트워크 설정을 일정 시간 동안 빌려주는 것
- 클라이언트는 기간이 지나면 갱신 또는 반환 필요

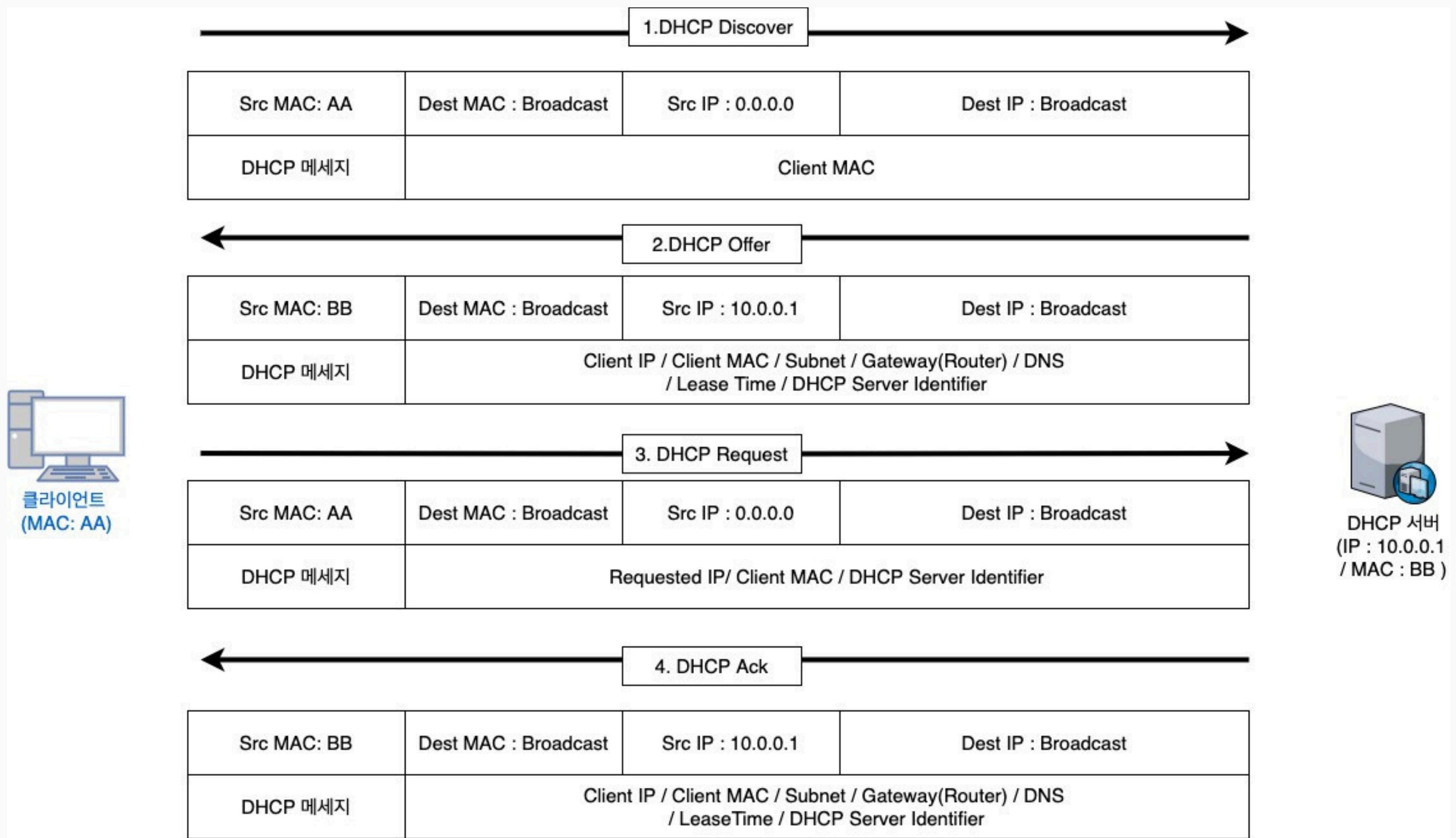
임대



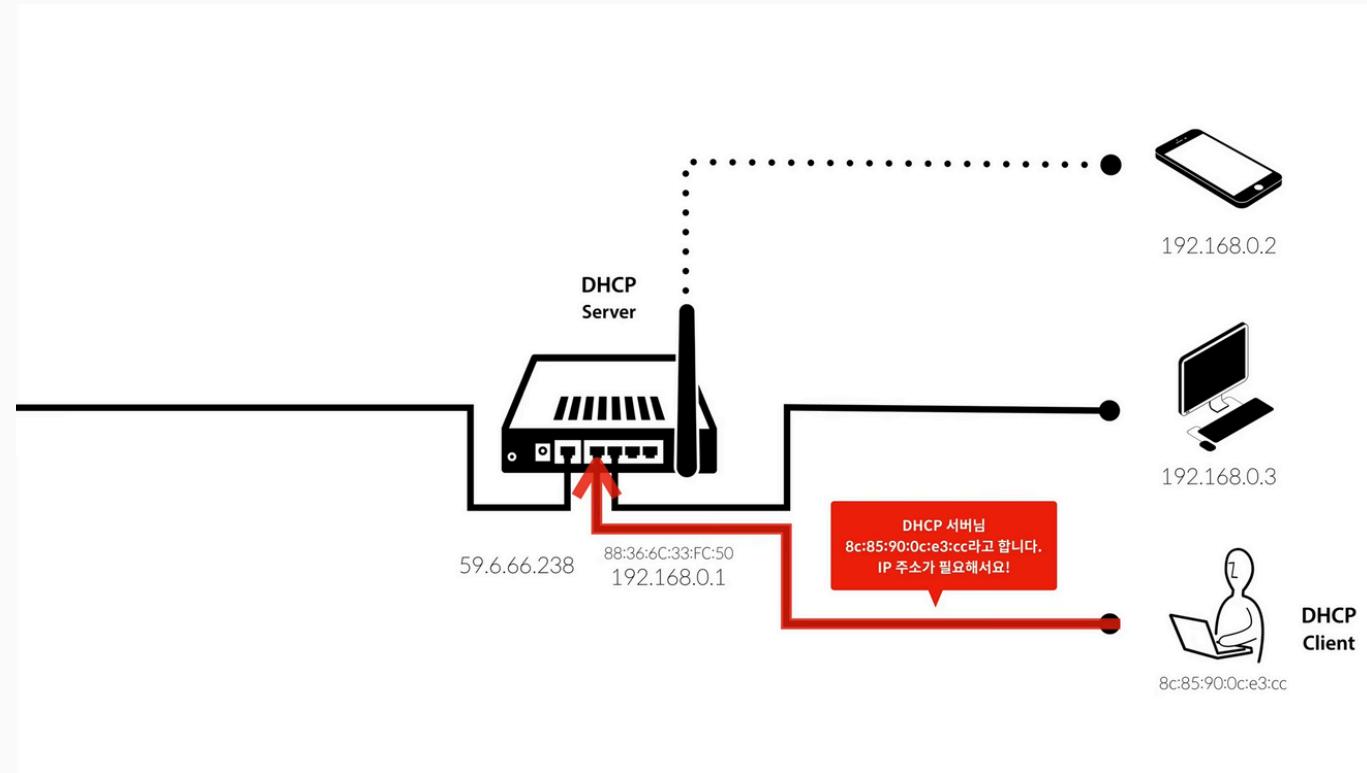
DORA?

- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Acknowledge

임대



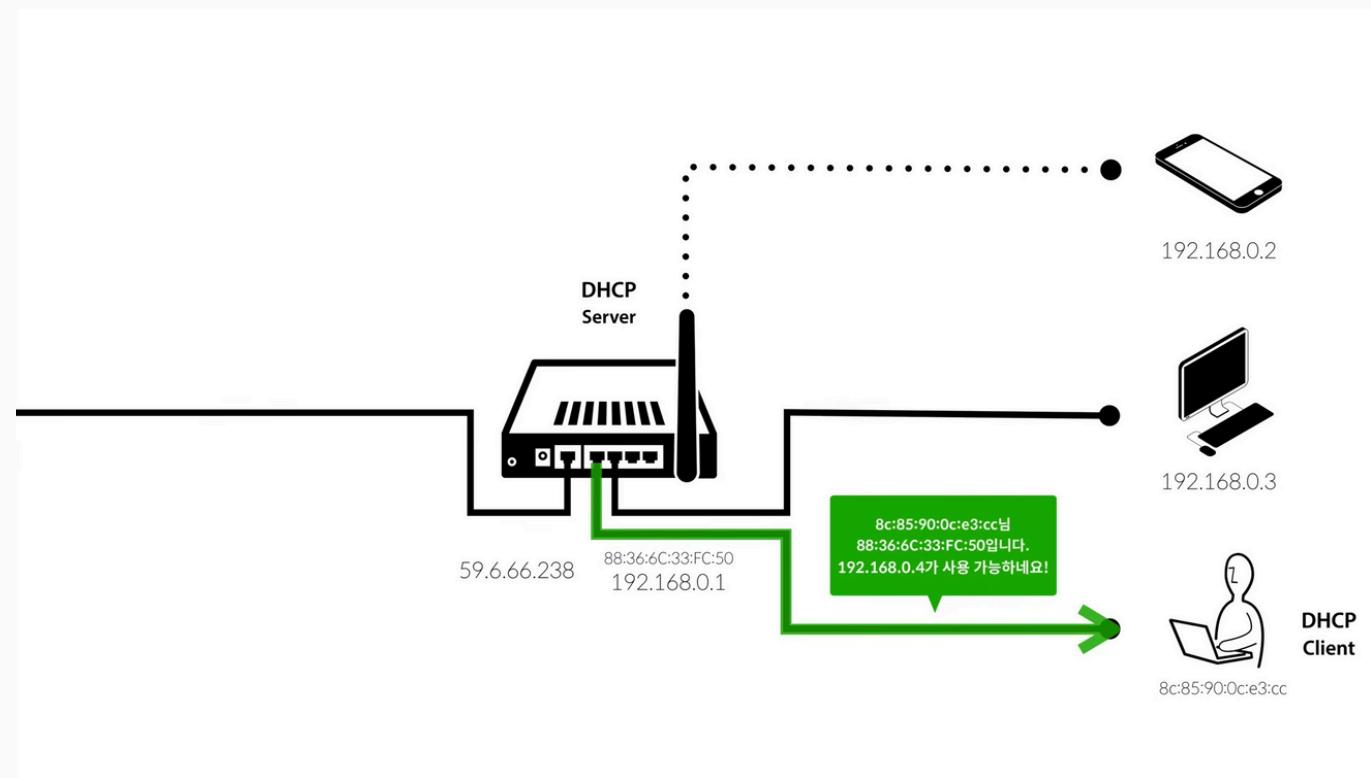
임대



DHCP Discover

- 클라이언트가 서버를 찾는 과정
- 브로드캐스트 메시지(255.255.255.255) 전송
- 클라이언트의 IP는 0.0.0.0
- 주요 파라미터
 - Client MAC Address

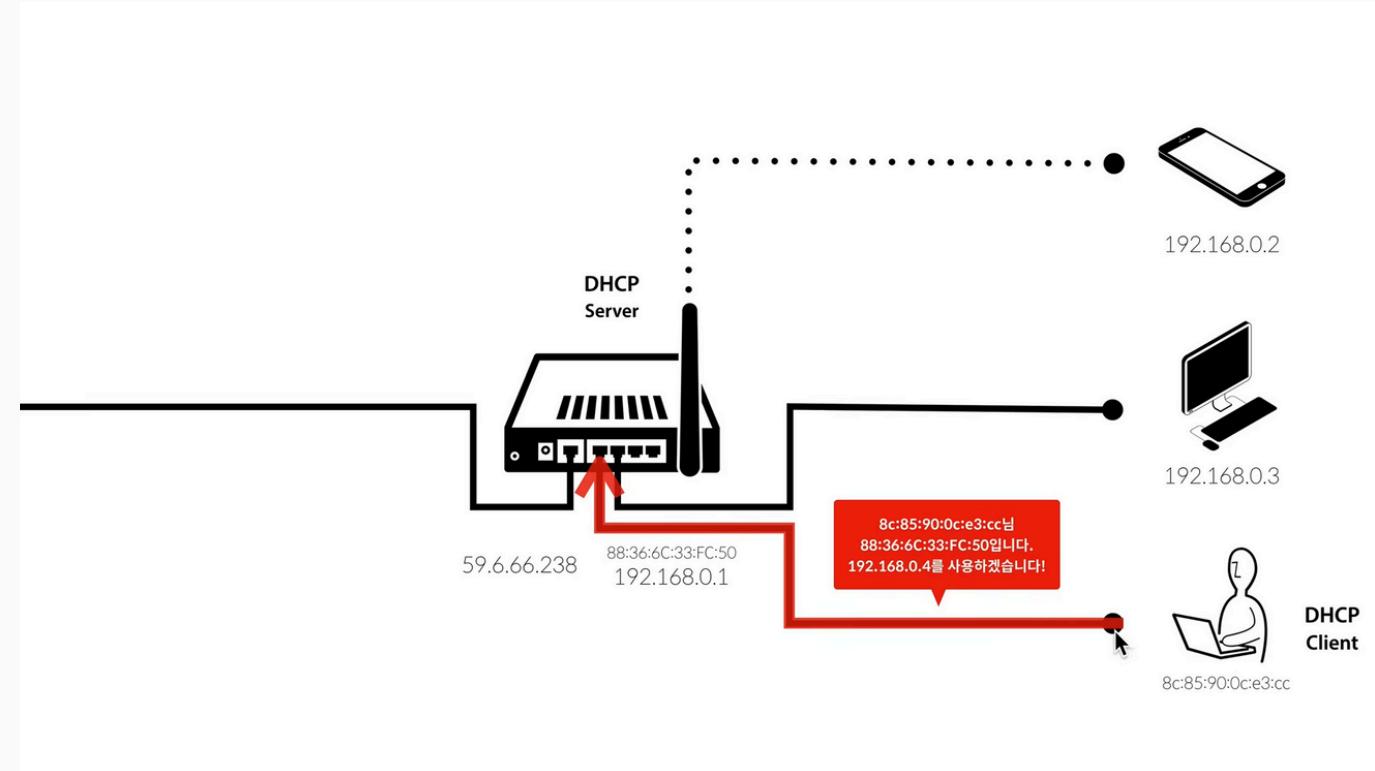
임대



DHCP Offer

- 서버는 클라이언트에게 네트워크 정보를 보냄
- 주요 파라미터
 - Your IP Address
 - Subnet Mask
 - Router
 - DNS
 - IP Lease Time
 - DHCP Server Identifier

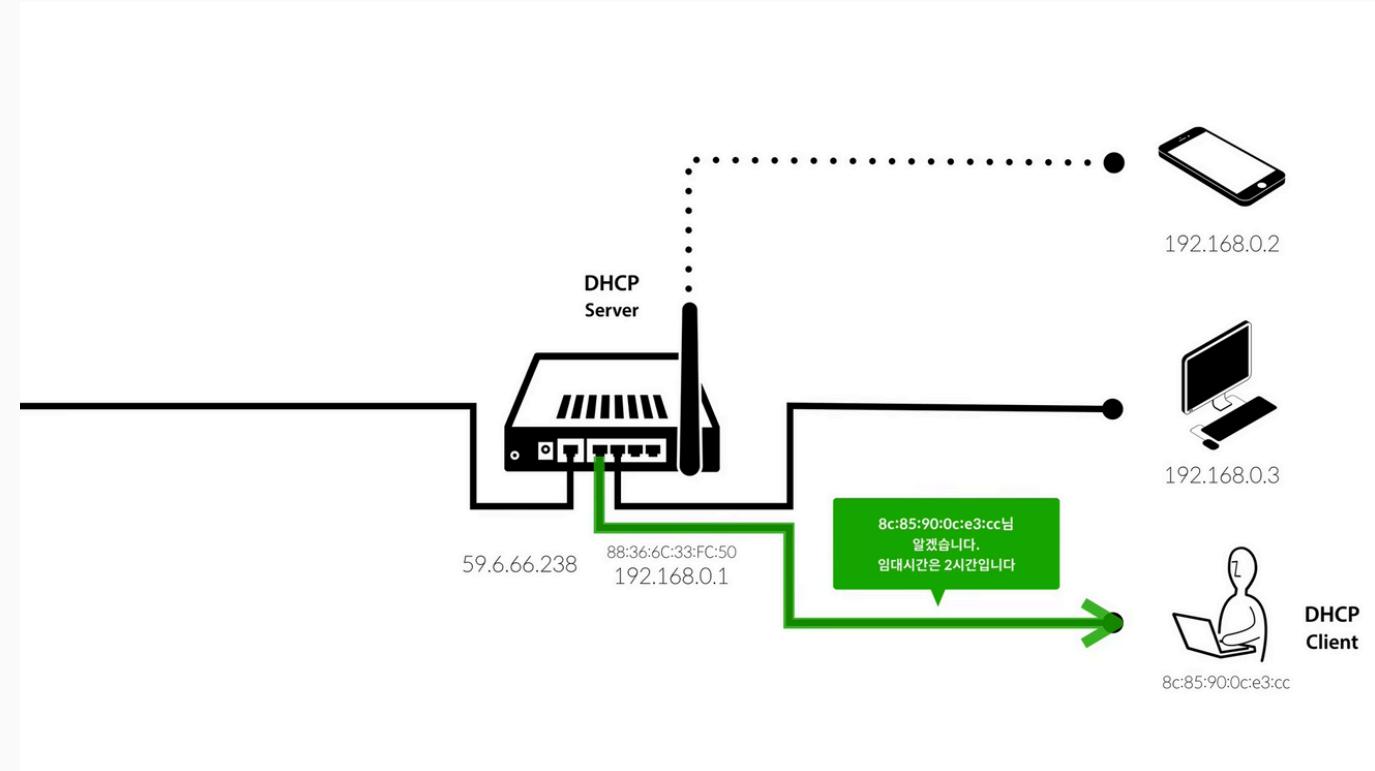
임대



DHCP Request

- 클라이언트는 IP 주소를 하나 선택하고 요청 메시지를 서버에게 보냄
- 주요 파라미터
 - Request IP Address
 - DHCP Server Identifier

임대



DHCP Acknowledge

- 서버는 클라이언트에게 IP 주소 임대 시간 등의 정보를 담은 승인 메시지를 보냄
- 주요 파라미터
 - Your IP Address
 - Subnet Mask
 - Router
 - DNS
 - IP Lease Time
 - DHCP Server Identifier

사실 패킷을 보면 좋긴한데

Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Length: 1
DHCP: Request (3)
Option: (61) Client Identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC Address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Requested IP Address: 192.168.0.27
Length: 4
DHCP Server Identifier: 192.168.0.1
Length: 4
DHCP Server Identifier: 192.168.0.1
Option: (12) Host Name
Length: 11
Host Name: Windows7-PC
Option: (81) Client Fully Qualified Domain Name
Length: 14
> Flags: 0x00
> Lease: 0
PTA-RA result: 0
Client name: Windows7-PC
Option: (60) Vendor Class Identifier
Length: 8
Vendor class identifier: MSFT 5.0
Option: (55) Parameter Request List
Length: 12
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (3) Router
Parameter Request List Item: (1) Domain Name Server
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (32) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (43) Vendor-Specific Information
Option: (255) End
Option End: 255

Dynamic Host Configuration Protocol (Request)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x7582dac0
Seconds elapsed: 0
> Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Client hardware address padding: 00000000000000000000000000000000
Server host name not given
Boot file name not given

Ethernet II, Src: EFMNetwo_d7:94:61 (00:08:9f:d7:94:61), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68

Magic cookie: DHCP
Option: (53) DHCP Message Type (Release)
Length: 1
DHCP: Release (7)
Option: (54) DHCP Server Identifier (192.168.0.1)
Length: 4
DHCP Server Identifier: 192.168.0.1
Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Option: (255) End
Option End: 255
Padding: 00000000000000000000000000000000...

Dynamic Host Configuration Protocol (Release)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x10c7e93f
> Seconds elapsed: 11
> Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.0.27
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Client hardware address padding: 00000000000000000000000000000000
Server host name not given
Boot file name not given

Ethernet II, Src: IntelCor_36:3a:8a (7c:67:a2:36:3a:8a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67

Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Requested IP Address: 192.168.0.27
Length: 4
Requested IP Address: 192.168.0.27
Option: (12) Host Name
Length: 11
Host Name: Windows7-PC
Option: (60) Vendor Class Identifier
Length: 8
Vendor class identifier: MSFT 5.0
Option: (55) Parameter Request List
Length: 12
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (43) Vendor-Specific Information
Option: (255) End
Option End: 255
Padding: 00000000000000000000000000000000

Ethernet II, Src: EFMNetwo_d7:94:61 (00:08:9f:d7:94:61), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 67, Dst Port: 68

Dynamic Host Configuration Protocol (Offer)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x7582dac0
Seconds elapsed: 0
> Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Client hardware address padding: 00000000000000000000000000000000
Server host name not given
Boot file name not given

Dynamic Host Configuration Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x7582dac0
Seconds elapsed: 0
> Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: PcsCompu_2e:10:f0 (08:00:27:2e:10:f0)
Client hardware address padding: 00000000000000000000000000000000
Server host name not given
Boot file name not given

04

갱신

갱신

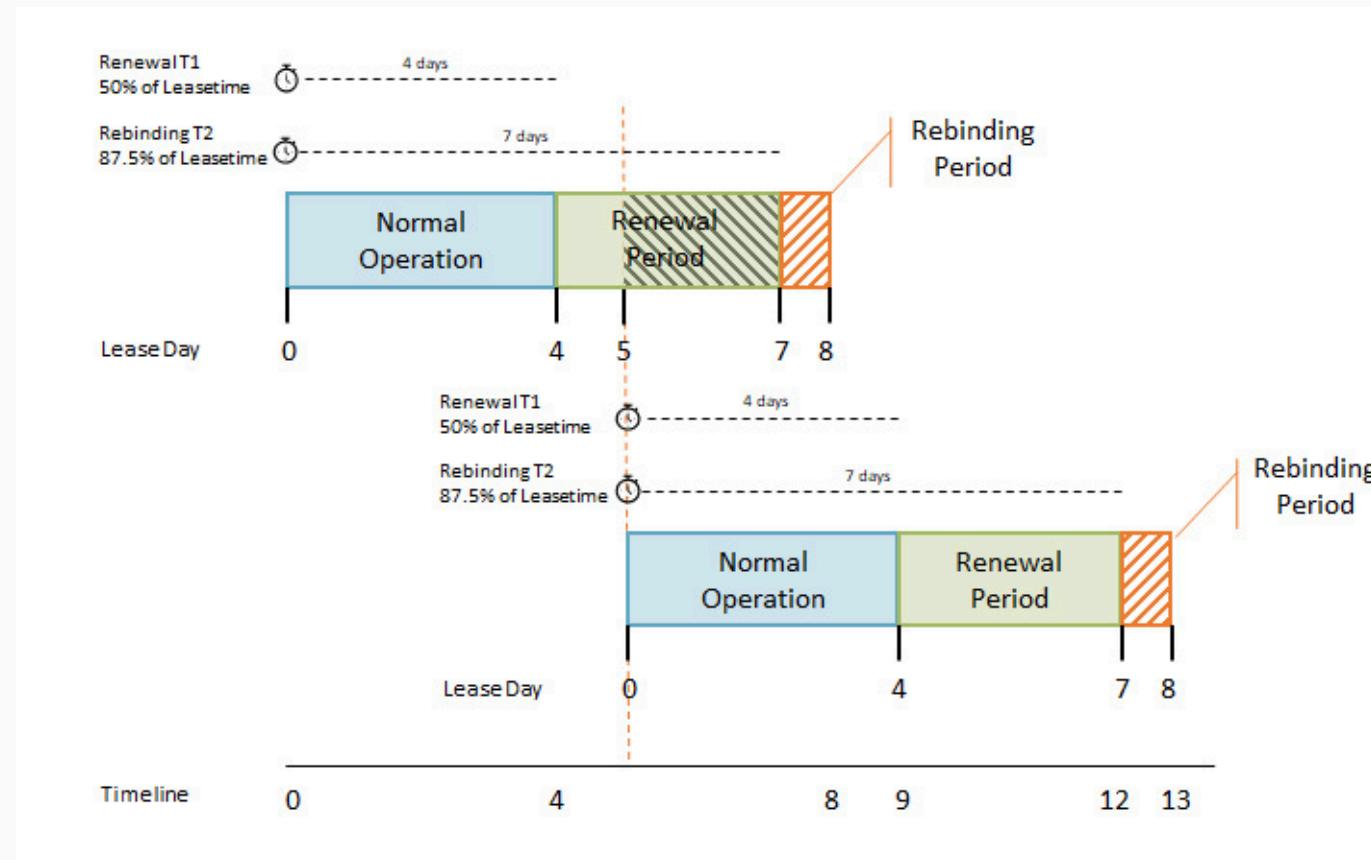


Renewal

- 클라이언트는 임대 시간이 끝나기 전에 서버에 IP 주소를 계속 사용하고 싶다고 요청
- Renewal
- Rebinding

[OSEN=고성환 기자] 말 그대로 미친 액수다. 엘링 홀란(25)이 맨체스터 시티와 10년 재계약을 체결하면서 어마어마한 돈을 벌어들이게 됐다.

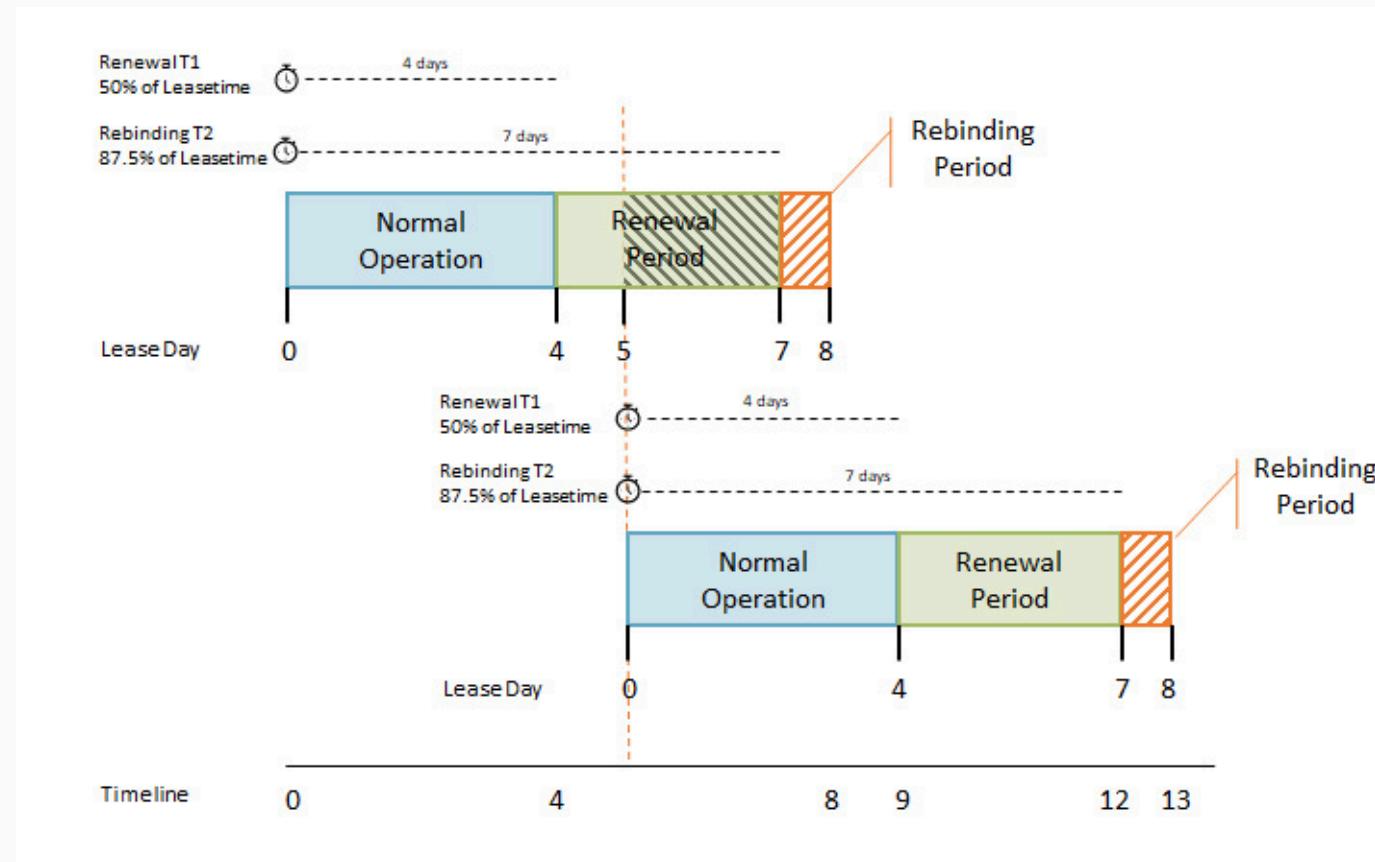
갱신



Renewal (T1)

- IP 주소 할당 후 50% 지나면 갱신 과정 수행
- Request, ACK로 갱신 과정 진행
- 유니캐스트로 진행
- 서버가 응답하면? 갱신 끝

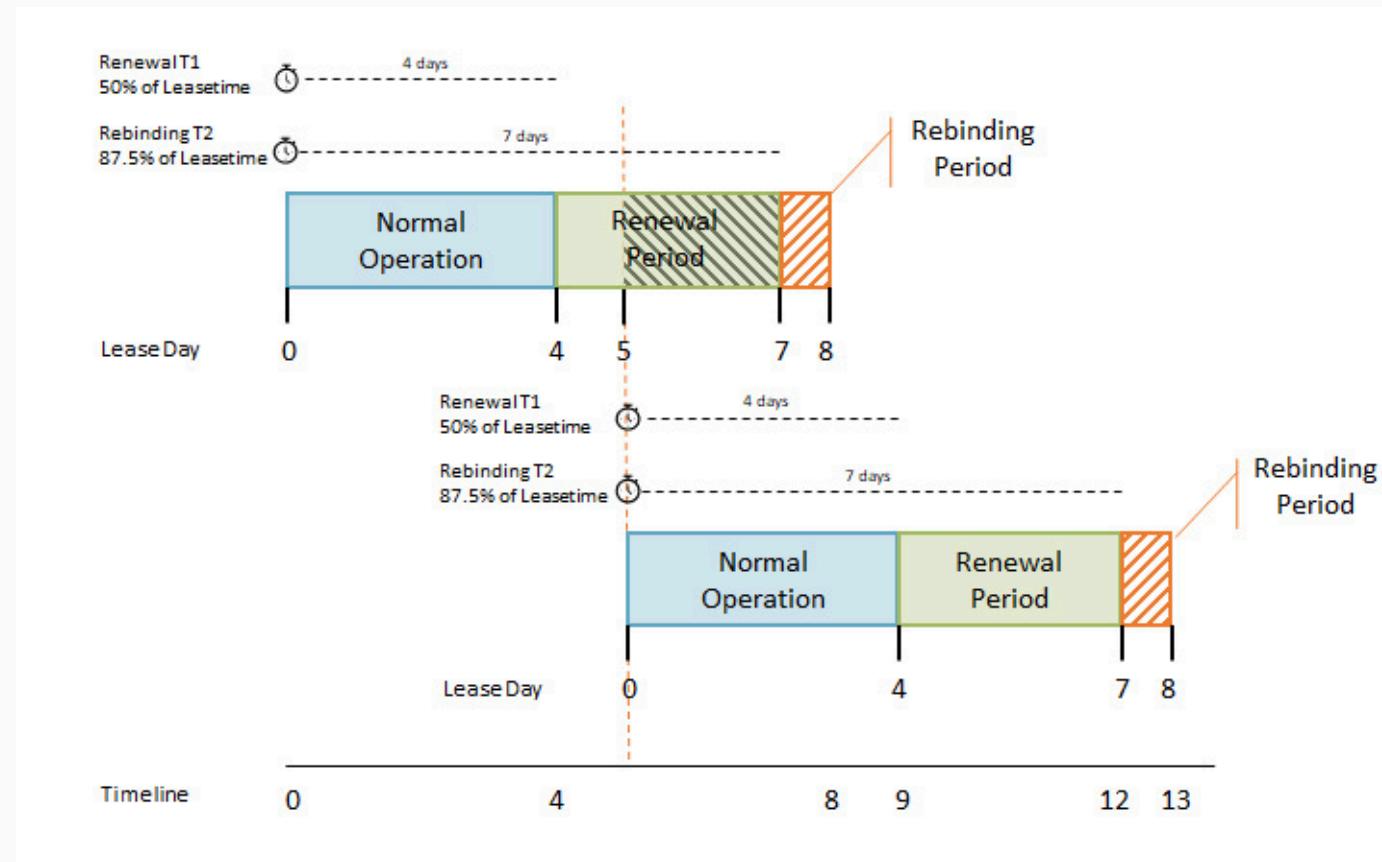
갱신



Rebinding (T2)

- T1에서 서버가 응답을 하지 않은 경우
- IP 주소 할당 후 87.5% 지나면 갱신 과정 수행
- Request, ACK로 갱신 과정 진행
- 브로드캐스트로 진행

갱신



임대 만료

- T2에서 서버가 응답을 하지 않은 경우
- IP 주소를 더 이상 사용 할 수 없음
- Discover부터 다시 시작

05

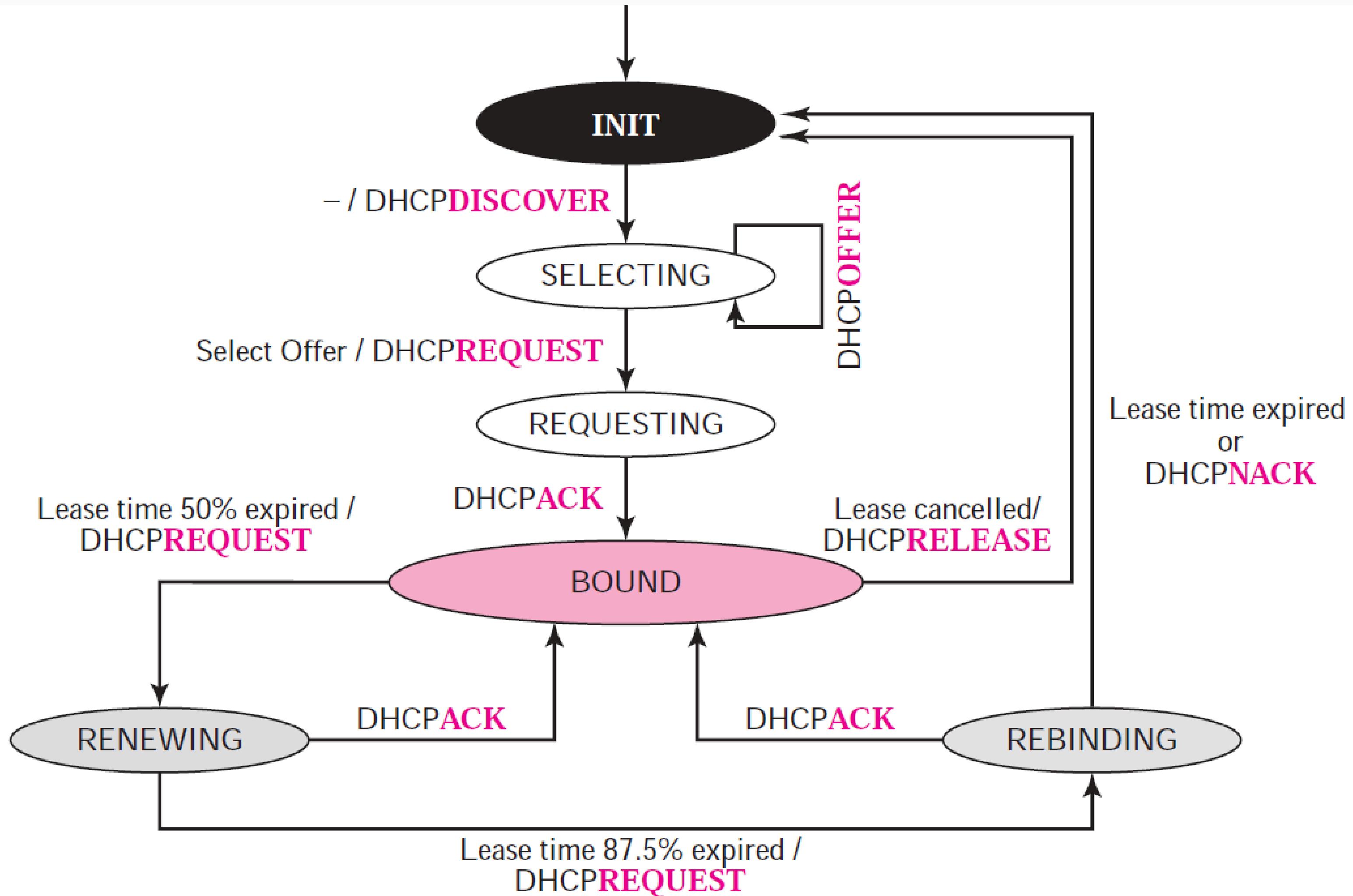
반환

반환



Release

- 갱신 과정에 모두 실패하여 만료된 경우
- IP 주소를 더 이상 사용하지 않는 경우
- 할당 받았던 IP 주소를 반환



06

DHCP Spoofing

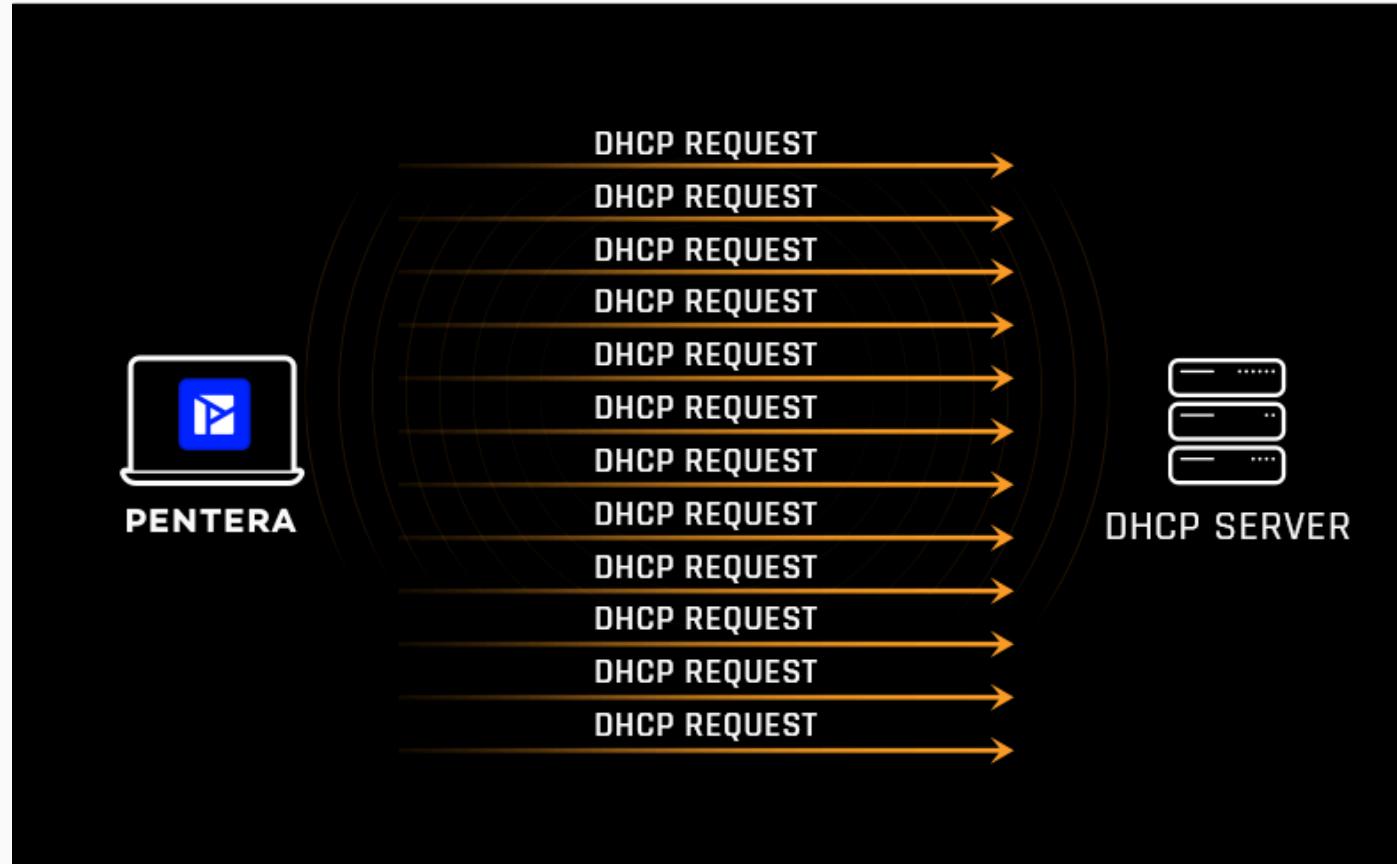
공격 위험



취약점 발생 원인

- 사용자는 DHCP에 대한 정보를 저장하지 않음
- 인증과 암호화 매커니즘이 없음

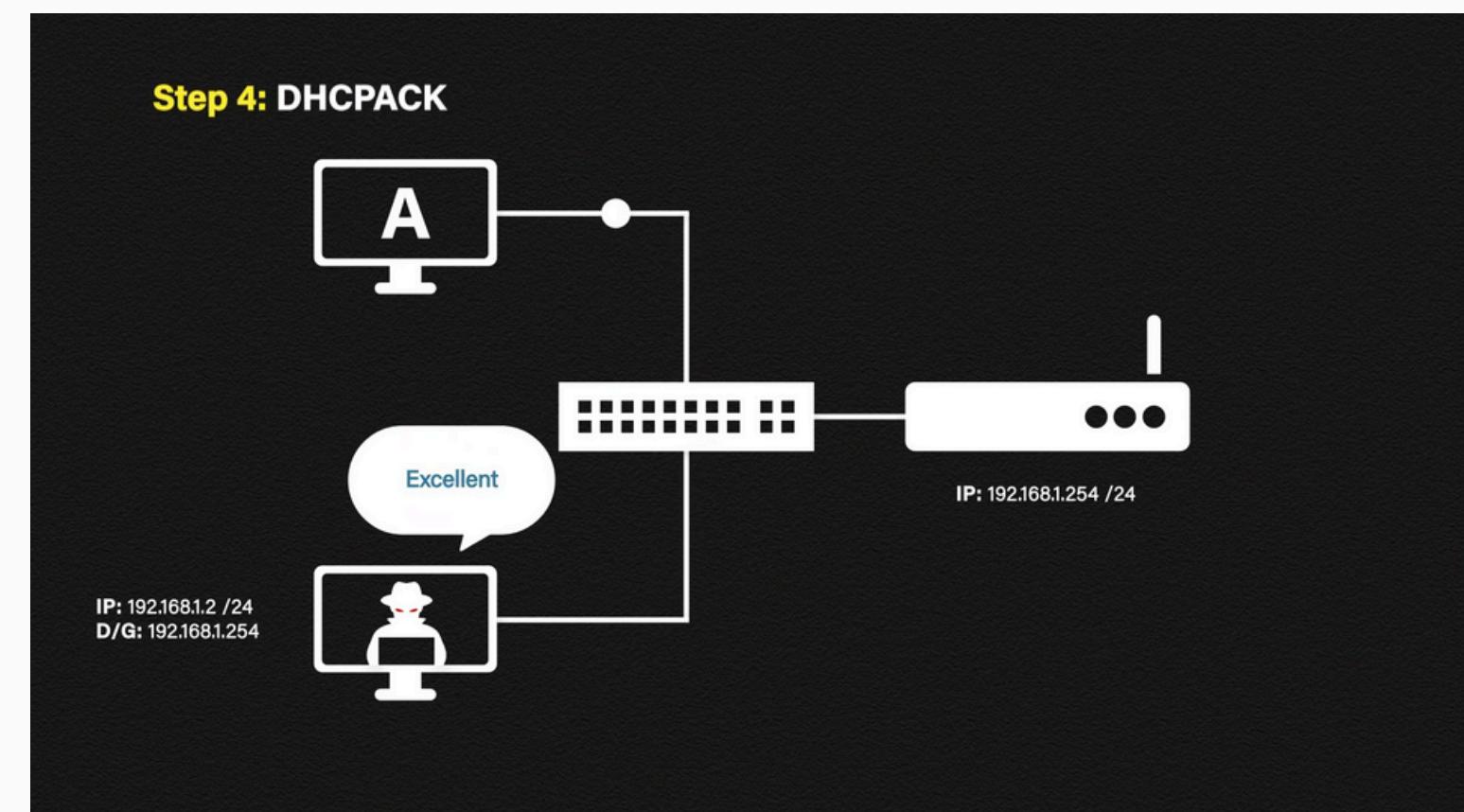
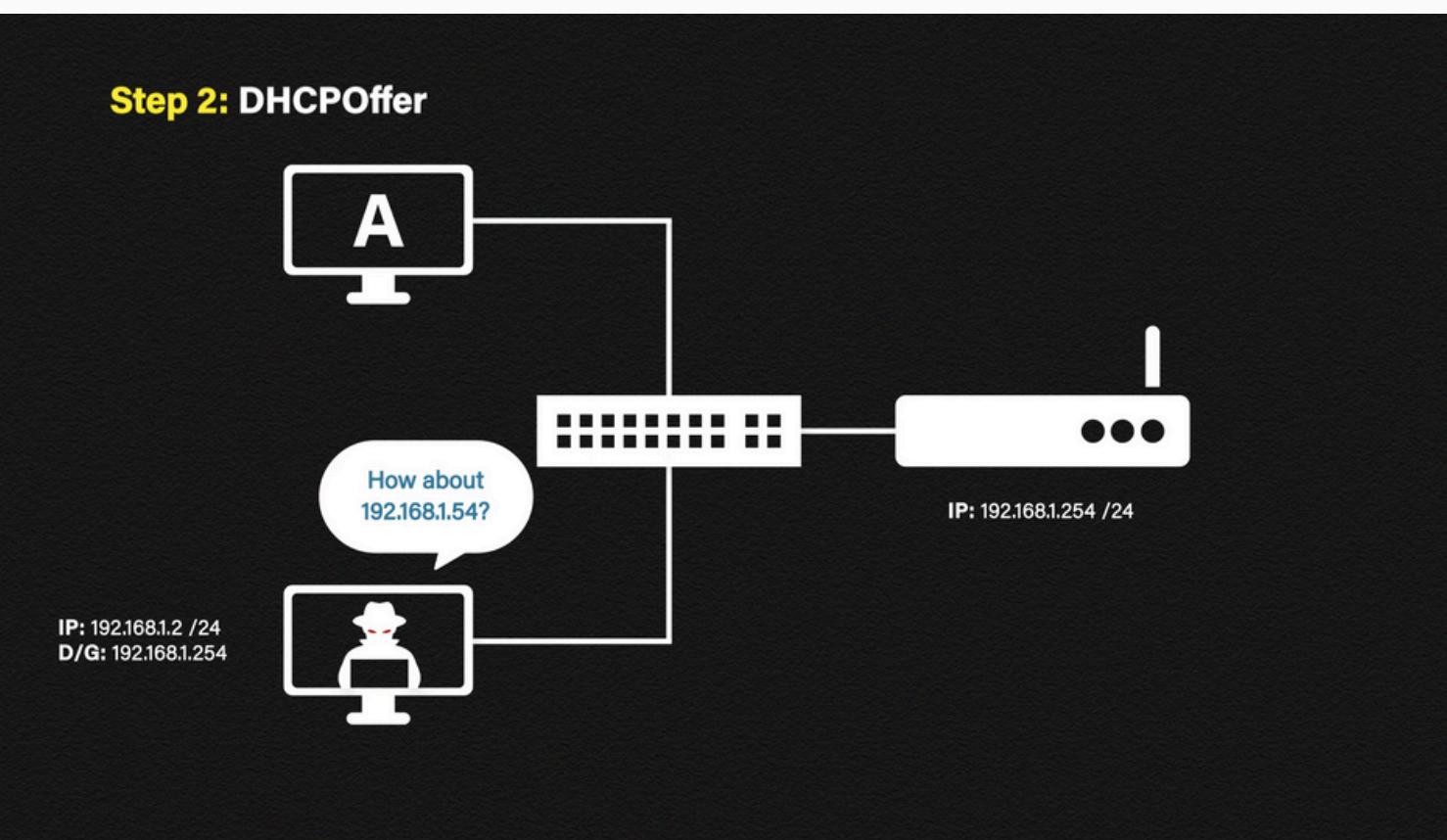
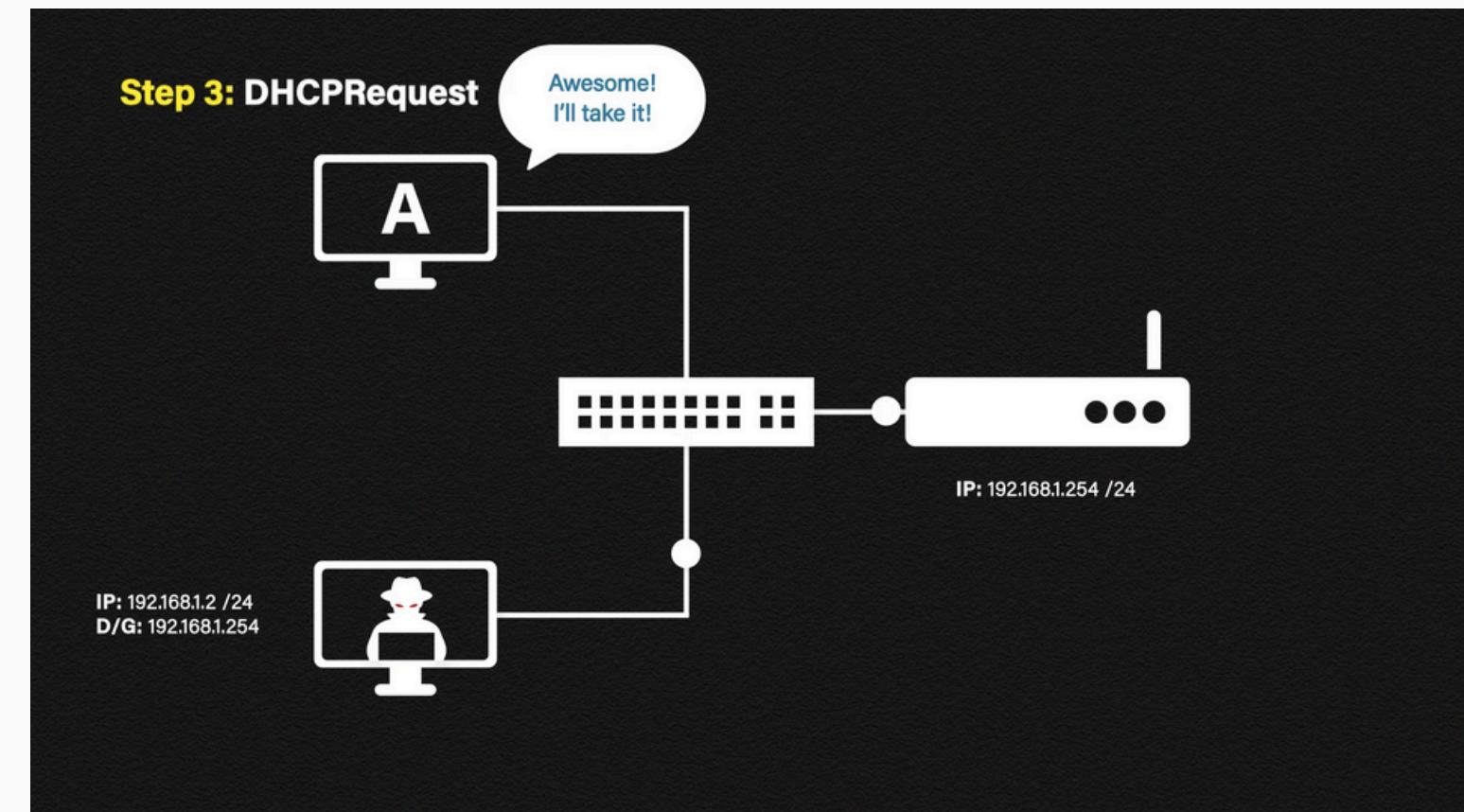
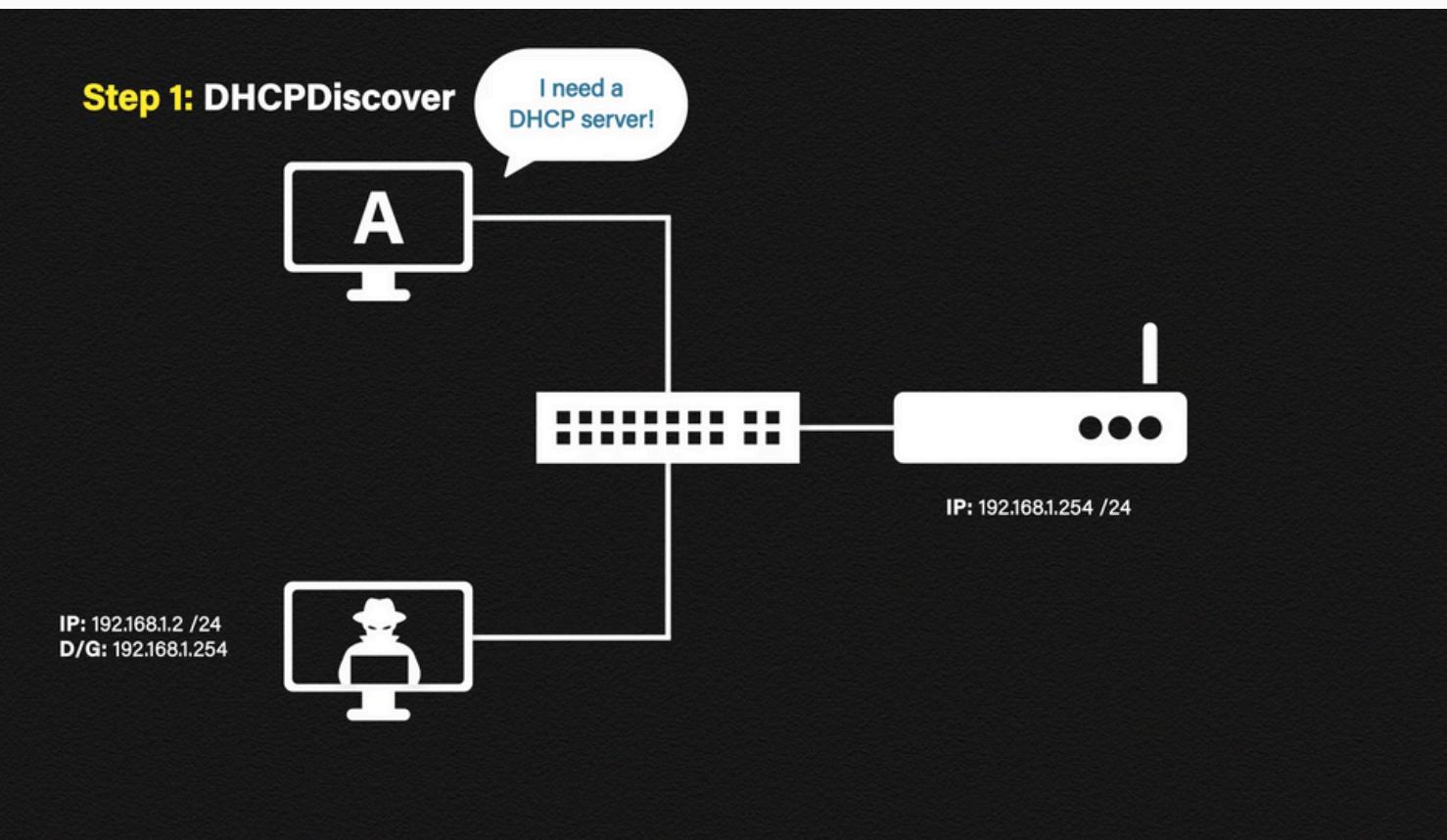
공격 위험



DHCP Spoofing

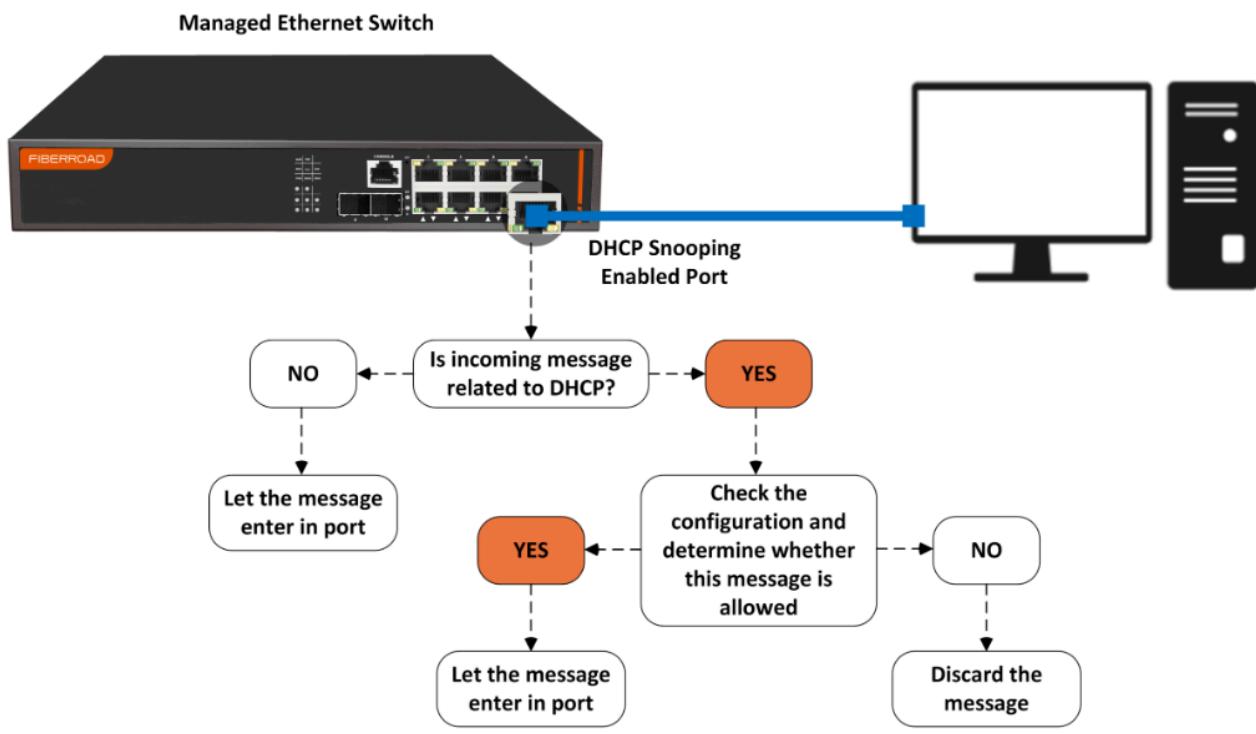
- UDP로 동작하기 때문에 인증을 수행하지 않음
- DHCP 프로토콜이 제공하는 정보를 조작해서 타켓 PC를 속임
- 조작된 게이트웨이 주소, DNS 주소 정보를 전달하여 공격을 수행
- 주요 위험 요소
 - MITM(Man-In-The-Middle)
 - 서비스 거부 공격(Dos)
 - 네트워크 혼란

공격 위험



공격 위험

How DHCP Snooping Works?



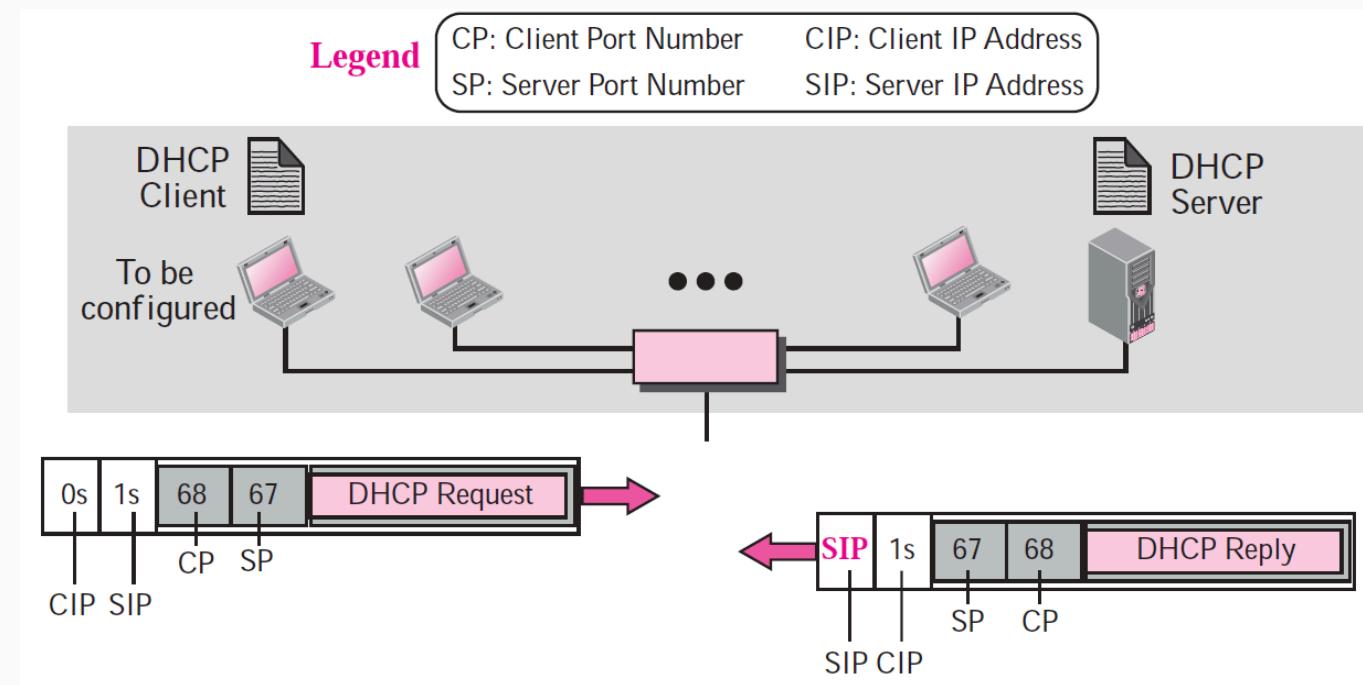
DHCP Snoofing

- 네트워크 포트를 신뢰된 포트와 비신뢰된 포트로 구분하여 DHCP 패킷을 필터링
- 신뢰된 포트
 - 공식적인 DHCP 서버에서 제공하는 응답 허용
- 비신뢰 포트
 - DHCP 서버 역할을 하려는 장치 차단

07

Relay Agent

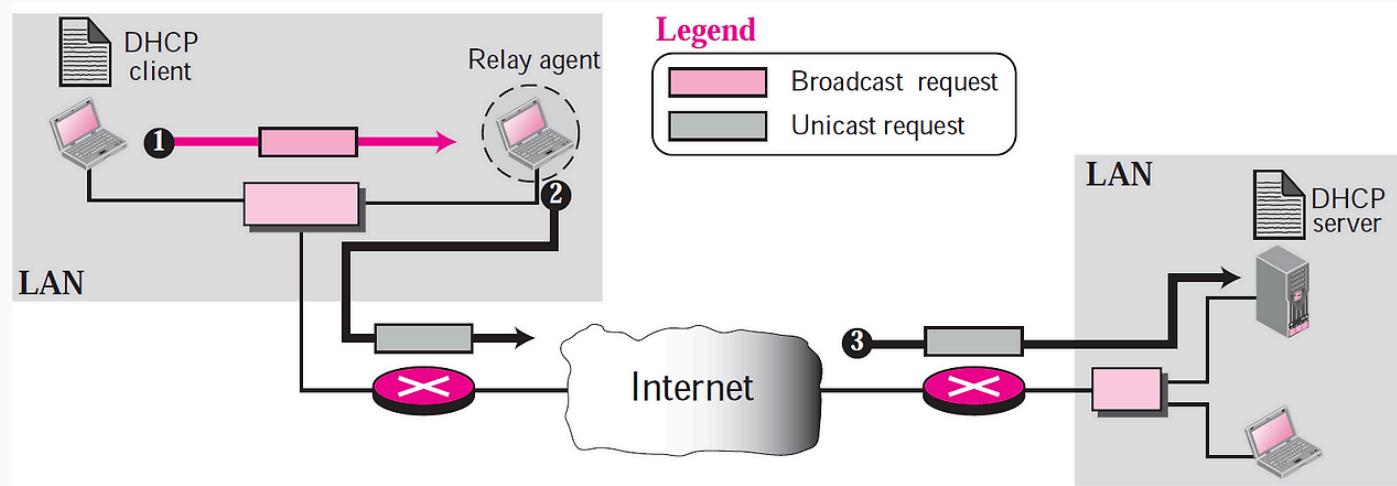
Relay Agent



같은 망에서의 DHCP

- 클라이언트는 자신의 IP 주소와 서버의 IP 주소를 모른채로 브로드캐스팅으로 전송
- 서버는 브로드캐스팅 혹은 유니캐스팅 방식으로 클라이언트에게 reply 전송

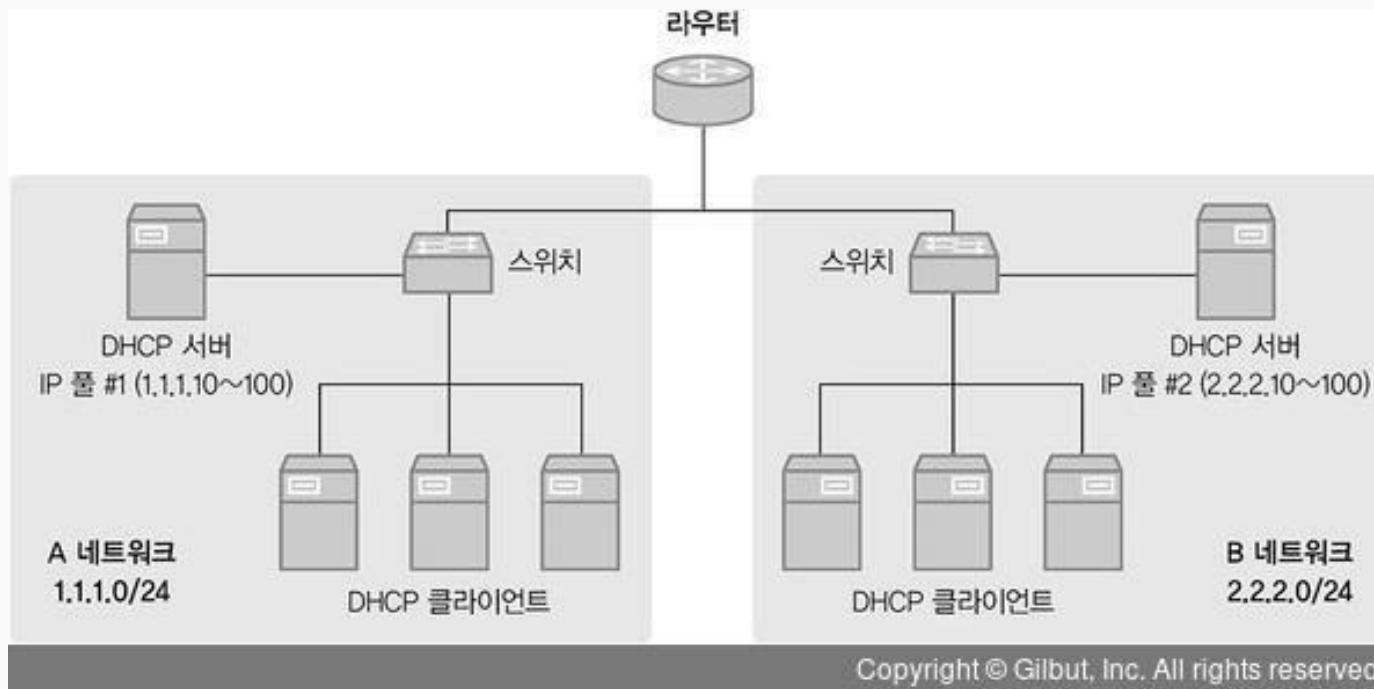
Relay Agent



다른 망에서의 DHCP

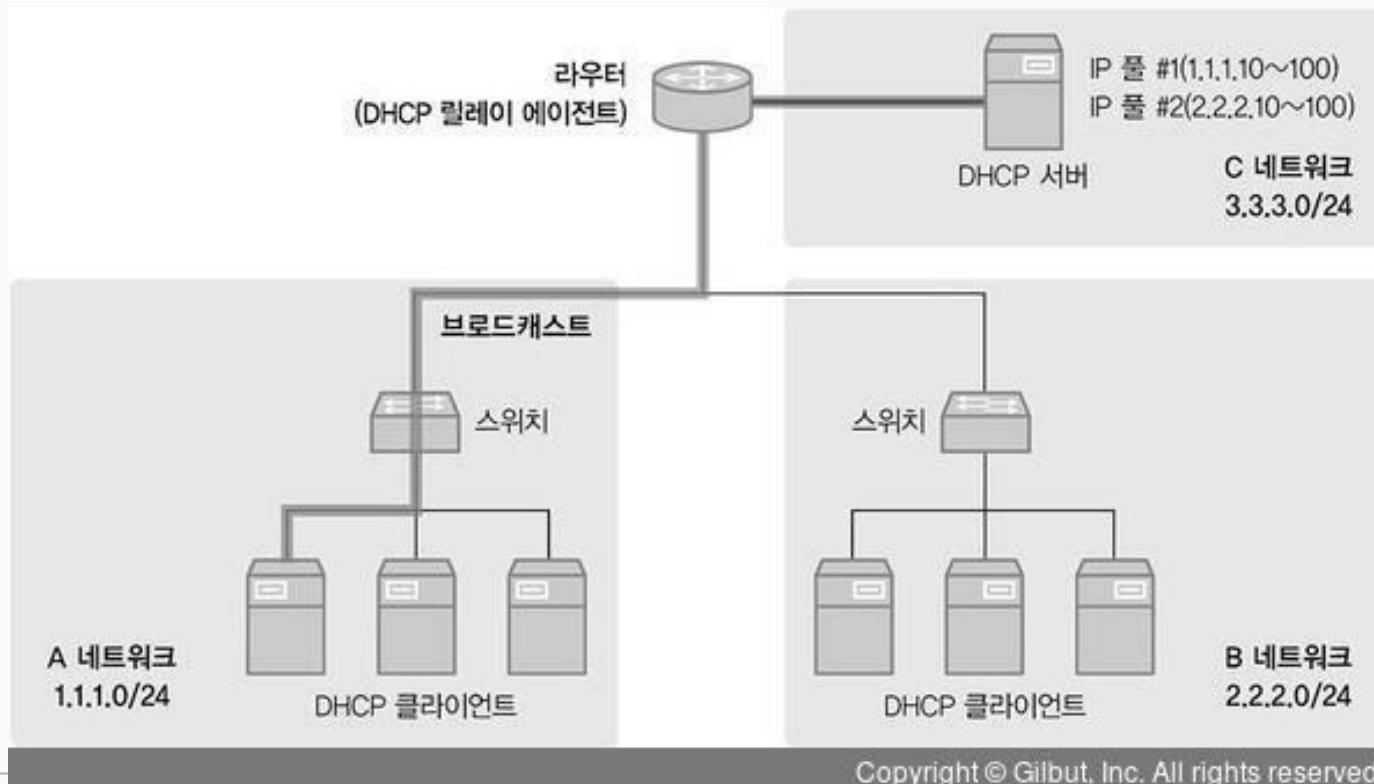
- 클라이언트가 Request를 브로드캐스팅
- Reply Agent가 Request를 서버까지 유니캐스팅
- 서버는 reply를 Reply Agent에게 유니캐스팅
- Reply Agent는 클라이언트에게 전송

Relay Agent



다른 망에서의 DHCP

- 각 네트워크 환경 별로 DHCP 서버를 구축해야 하나?



- Reply Agent를 사용한다면 서버 한 대로도 충분함
- A 네트워크와 B 네트워크에 대한 IP 풀을 C 네트워크에서 관리함

감사합니다

network