CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

ARP SPOOFING 탐지 및 대응 : NAGA

2019. 7. 2

정보보안SW전공

정 재 훈

JOONGBU UNIVERSITY
JBU
충부대학교

Table of Contents

누군가 대화를 엿듣고 있다면????

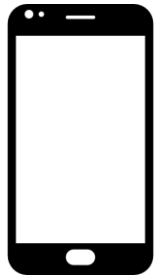
나가!!!!

ARP TABLE

L3 Switch

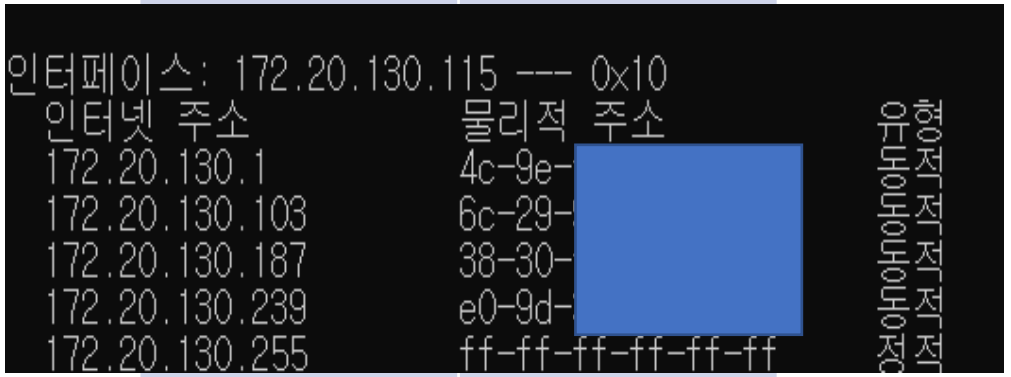
Laptop

Smart Phone

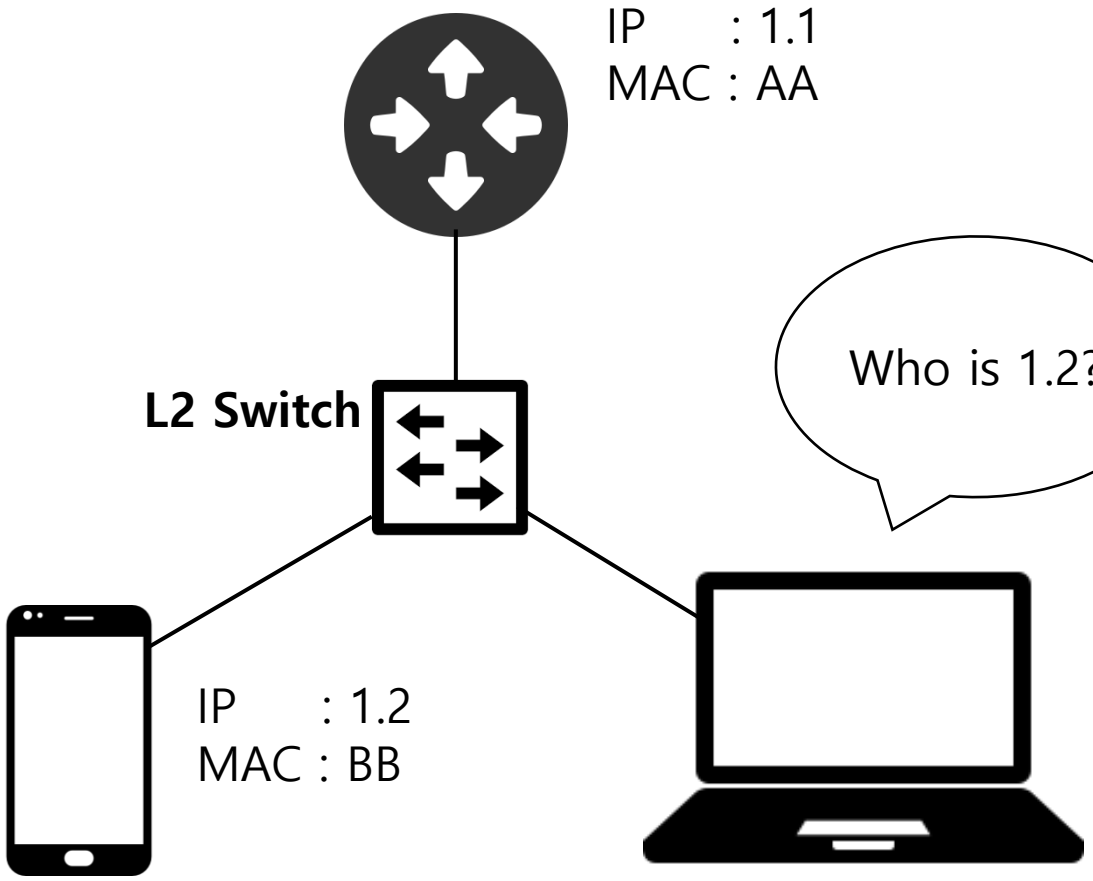


ARP Table

IP	MAC



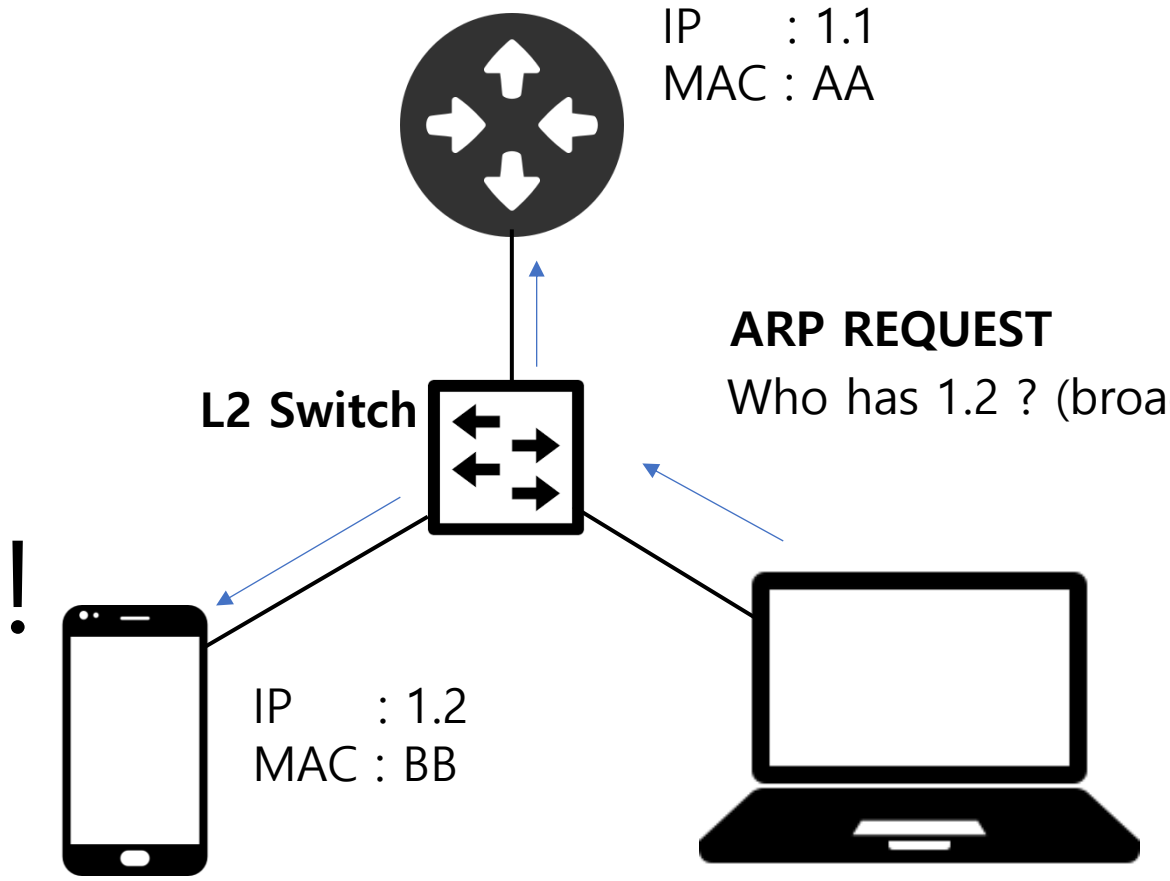
ARP TABLE



Laptop's ARP Table

IP	MAC
1.1	AA
1.2	??

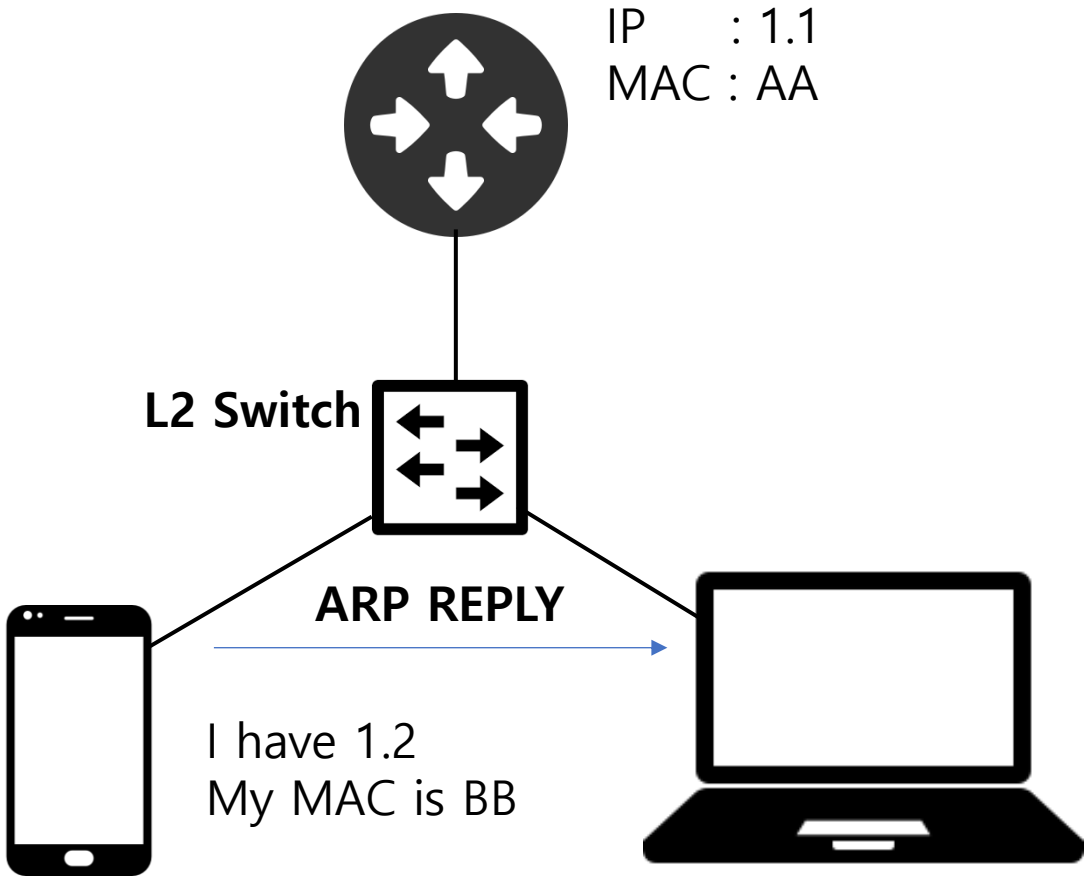
ARP TABLE



Laptop's ARP Table

IP	MAC
1.1	AA
1.2	??

ARP TABLE



Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

ARP SPOOFING

Gateway's ARP Table

IP	MAC
1.1	AA
1.2	BB

IP : 1.1
MAC : AA

Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

L2 Switch

Attacker's ARP Table

IP	MAC
1.1	??
1.2	??

IP : 1.2
MAC : BB

IP : 1.3
MAC : CC

ARP SPOOFING

Gateway's ARP Table

IP	MAC
1.1	AA
1.2	BB

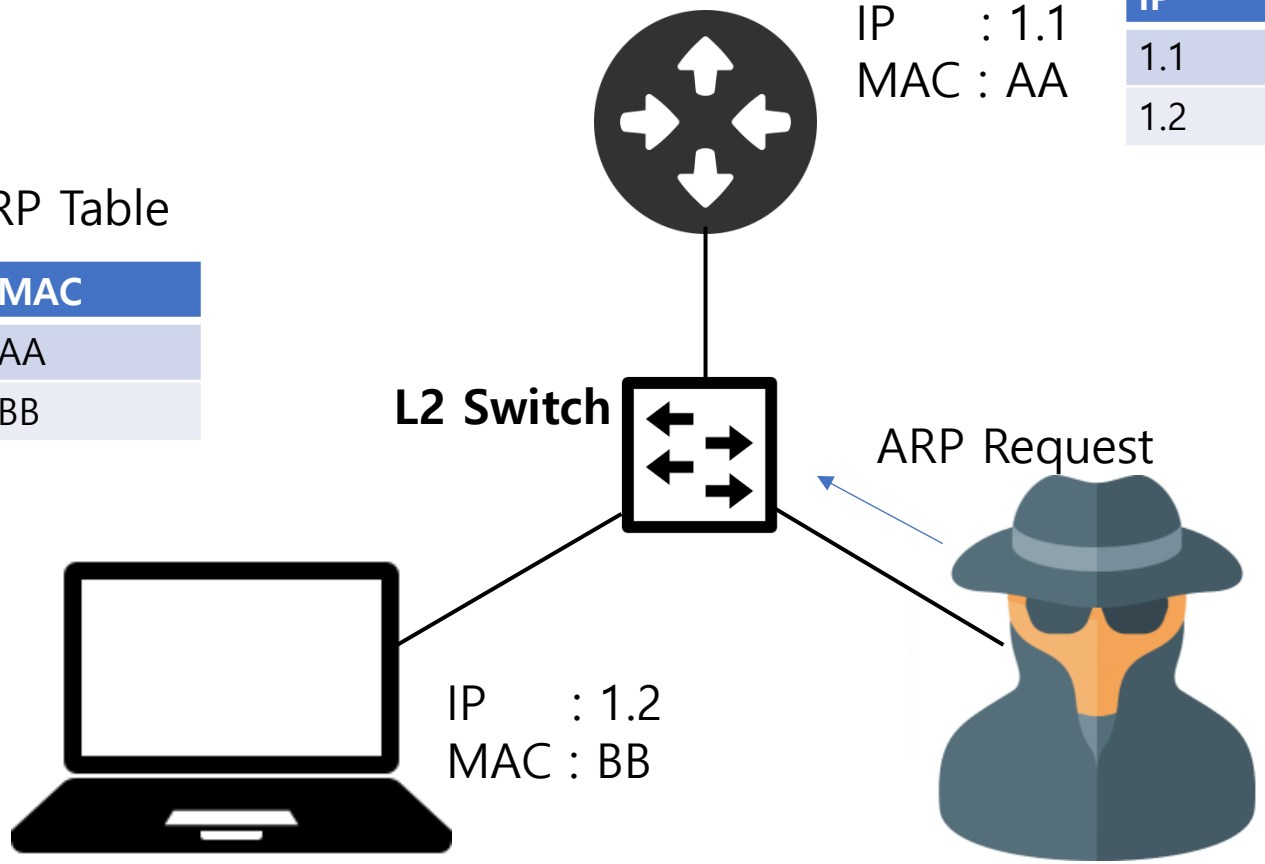
IP : 1.1
MAC : AA

Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

Attacker's ARP Table

IP	MAC
1.1	AA
1.2	BB



ARP SPOOFING

Gateway's ARP Table

IP	MAC
1.1	AA
1.2	CC

IP : 1.1
MAC : AA

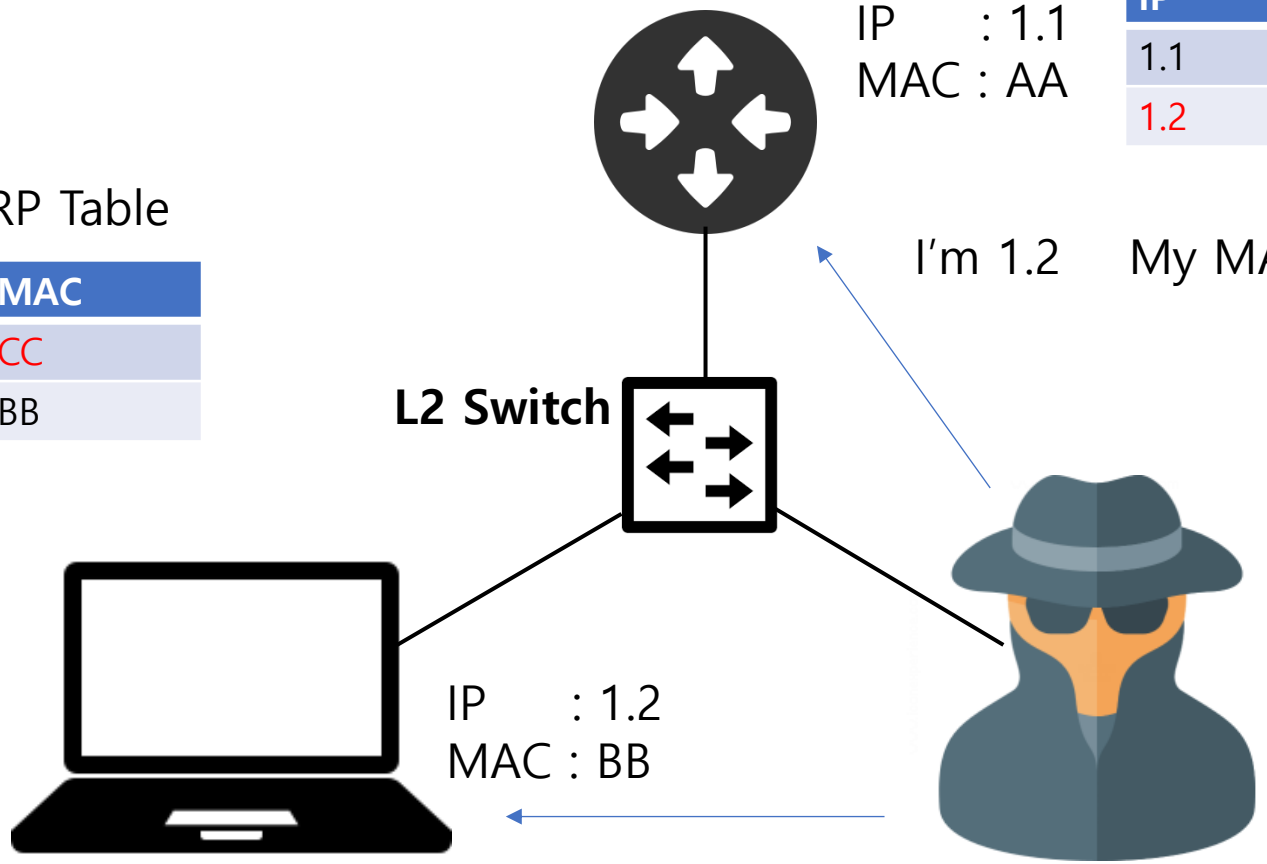
Laptop's ARP Table

IP	MAC
1.1	CC
1.2	BB

I'm 1.2 My MAC is CC

Attacker's ARP Table

IP	MAC
1.1	AA
1.2	BB

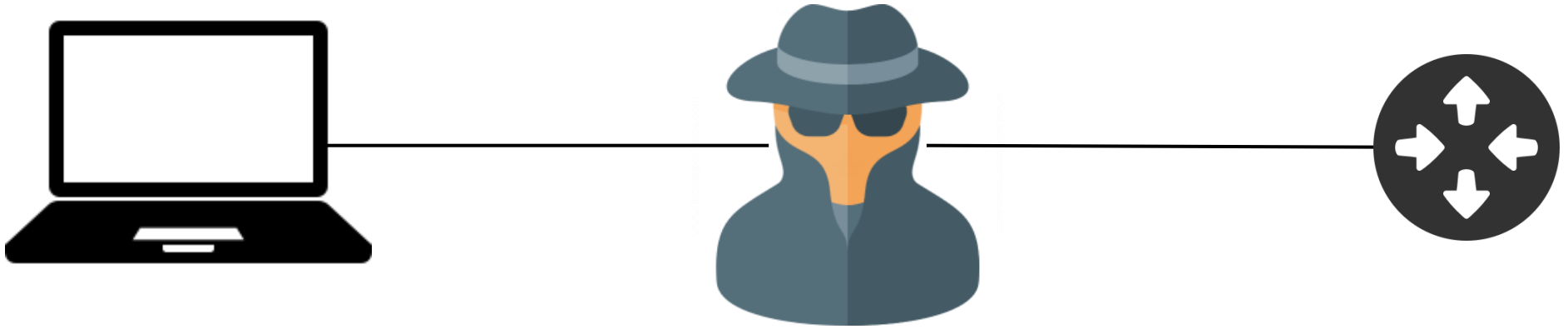


IP : 1.3
MAC : CC

IP : 1.2
MAC : BB

I'm 1.1 My MAC is CC

ARP SPOOFING



도청 공격, 변조 공격

Project NAGA

Gateway IP

Attacker's MAC

I'm 1.1 My MAC is CC

IP : 1.2
MAC : BB

IP : 1.3
MAC : CC

IP : 1.2
MAC : BB

I'm 1.1 My MAC is CC

IP : 1.3
MAC : CC

Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

AA != CC

(3) Gateway와의 연결 복원!

I'm 1.2 My MAC is BB

IP : 1.2
MAC : BB

(1) Gateway의 맥주소 설정변경 요구

I'm 1.1 My MAC is CC

I'm 1.2 My MAC is !@#$%

(2) 너랑 안놀아!

IP : 1.3
MAC : CC

Laptop's ARP Table

IP	MAC
1.1	AA
1.2	BB

AA != CC

NAGA

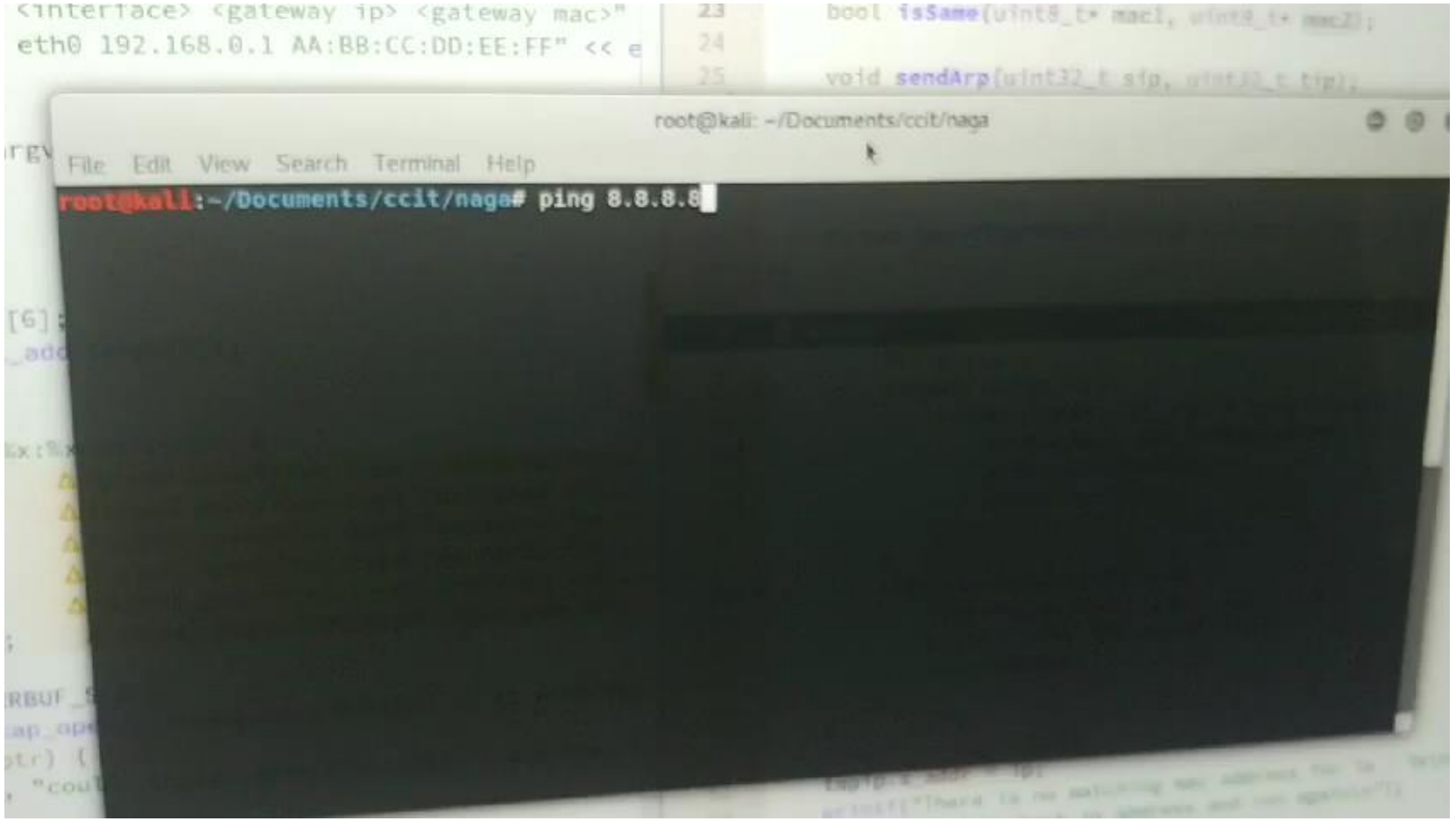
1. 초기 네트워크 연결시 Gateway의 맥 주소를 저장

2. ARP spoofing 공격 탐지....
 - Gateway의 맥주소 설정 변경을 요구 받으면 공격으로 판단

3. 공격자와의 통신을 끊음
 - 공격자에게 내 맥주소를 쓰레기 값으로 보냄

4. Gateway와의 연결 복원
 - 원래의 내 맥주소를 다시 홍보

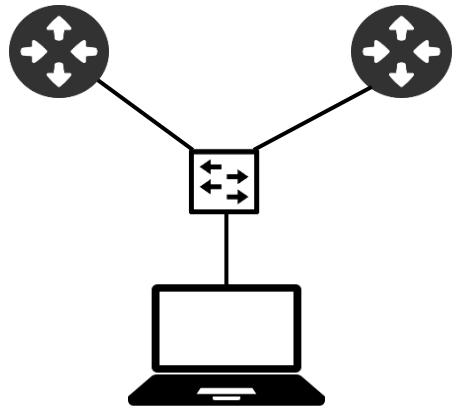
DEMO


root@kali: ~/Documents/ccit/naga
File Edit View Search Terminal Help
root@kali:~/Documents/ccit/naga# ping 8.8.8.8

한계점

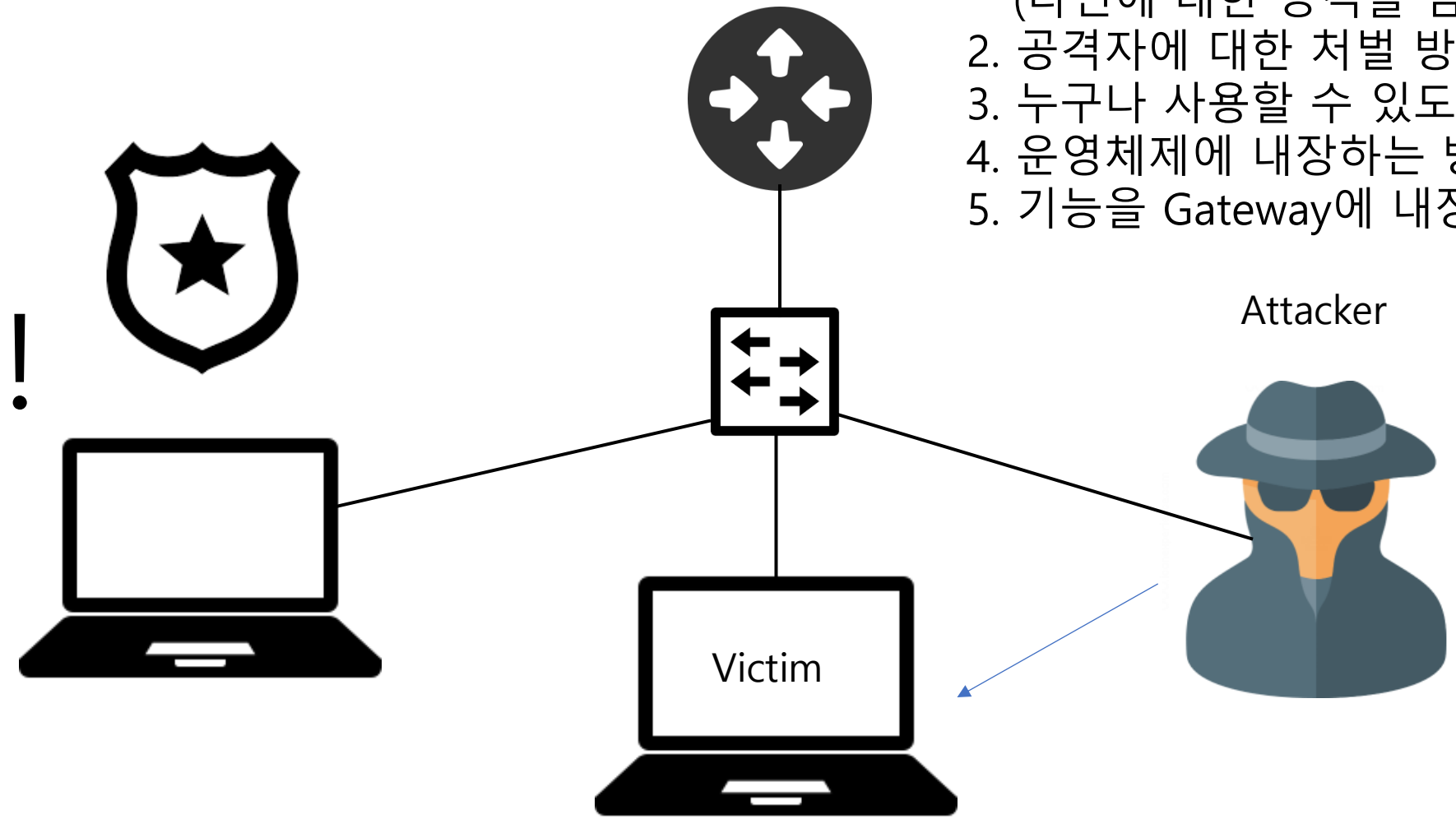
1. 그냥 MAC주소를 고정시키는 방법이 있지 않을까?
   -> 보통 arp스푸핑은 Wireless 환경에서 자주 일어나게 된다. 따라서 게이트웨이가 변하지 않는 환경이라면 고정시켜 놓는 것이 최선이다. 하지만 게이트웨이가 자주 변하는 Wireless 환경에서는 변할 때 마다 고정시켜 놓을 수 없기 때문에 (굉장히 귀찮기 때문에) NAGA가 꼭 필요하다.

2. 게이트웨이가 다중화 되어있을 때 게이트웨이 맥주소의 변화를 어떻게 arp 스푸핑과 다르게 탐지할 수 있을까?
   -> 두개 이상의 게이트웨이가 변화하면서 통신하는 환경이다. N개의 게이트웨이의 맥주소를 관리하는 방법밖에는...ㅠㅜ



발전방향

1. 로컬 네트워크의 경찰관 역할?
   (타인에 대한 공격을 탐지)
2. 공격자에 대한 처벌 방법
3. 누구나 사용할 수 있도록 tool 공개
4. 운영체제에 내장하는 방안
5. 기능을 Gateway에 내장한 제품 개발



감사합니다