IP Toy II

aon, leeopop, overmania

IP Toy I

외부 링크

Toy

사용자

사용자

IP Toy I

외부 링크

1. 사용자가 ARP request를 보낸다 (143.248.234.123이 누구냐?)

Toy

사용자

사용자

IP Toy I

외부 링크

2. 장난감이 가짜 응답을 보낸다 (143.248.234.123은 나다!)

Toy

사용자

사용자

IP Toy I

외부 링크

3. 사용자는 143.248.234.123을 쓰는 사람이 있다는 것을 인지하고 아이피 충돌을 감지한다.

Toy

사용자

사용자

IP Toy I

외부 링크

4. 허가된 사용자는 123 IP와 MAC 주소 ABCD를 같이 보낸다.

Toy

사용자

사용자

IP Toy I

외부 링크

5. 장난감이 123 – ABCD 매핑을 DB에서 확인하고 응답을 하지 않는다.

Toy

사용자

사용자

문제점

IP Toy I

외부 링크

1. 나는 라우터 234.1 이고 내 MAC은 EFEF 이다. 234.123으로 데이터가 왔는데 123이 누구냐?

Toy

사용자

사용자

IP Toy I

외부
링크

2. (아니, EFEF가 123의 안부를 묻잖아? – 거부) 내가 MAC ABCD를 가진 234.123이다.

2. 제가 234.123 입니다. MAC은 ABCD이고요

Toy

사용자

사용자

IP Toy I

234.123은
ABCD이다 x 2

외부
링크

라우터 입장에선 응답이 두 번 왔지만 여튼 234.123이란 IP는 ABCD에 대응됨을 안다.

Toy

사용자

사용자

IP Toy I

(스위치) 그래서 ABCD가 1번포트야 3번포트야...

ABCD에게 전송바람

외부 링크

나는 ABCD이다

나는 ABCD이다

Toy

사용자

사용자

그래서 단점들을 요약하면

1. 외부에서 오는 ARP 처리 로직에 문제가 있다 (해결가능한 문제)

2. 스위치 입장에선 일종의 ARP spoofing 공격이 된다.

3. 강제성이 없다
   (IP toy로 인터넷이 차단되는 것은 컴퓨터 본인이 IP 충돌을 감지하고 스스로 차단하는 것이다)
   1. 이 상황에서 IP 충돌이 나면 혼돈이 펼쳐진다.

IP Toy II

배경

- 1/9 휠회의에서 IP 자원 부족에 관한 이야기가 나옴

- DHCP + NAT 를 이용하자는 주장

  Vs public IP를 효율적으로 활용하자

- Public IP를 그대로 쓰면서 남는 IP 자원을 DHCP로 활용하자?

  => 개발 착수

특징

- 모든 트래픽을 관리하는 절대적인 허용/차단/감지 기능

- Passive mode (패킷 생성을 거의 하지 않음, 다만 차단할 뿐…)
  - IP Toy I 은 능동적으로 차단 신호를 보냄

- DHCP 를 통한 자동 IP 배분
  - 기숙사에서 노트북 들고오면 IP 적기 귀찮죠? 그냥 꽂으면 됩니다
    (기숙사에 개인 공유기로 DHCP를 쓰고 있다면 금상첨화)
  - 빈 IP 찾아서 넣기 귀찮다고요? MAC 주소만 등록하면 자동으로 IP를 줍니다.

특징 II

- MAC forwarding
  - 한 IP를 여럿이서 돌려쓰면 라우터의 MAC table을 자주 바꿔야 합니다.
  - 그리고 몇몇 IP는 사용할 수 있는 MAC 주소가 고정되어 있습니다.
  - 이를 한방에 해결하는 솔루션을 탑재하고 있습니다.

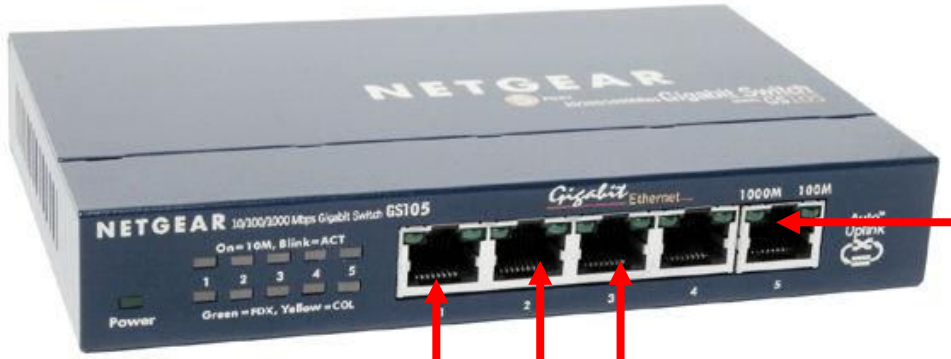
- 절대적 사용량 통계
  - Toy I은 랜선을 새로 꼽을 때에만 접속 여부를 탐지할 수 있습니다
  - 덕분에 sparcs, maru, printer 등은 6개월간 최근 사용시간이 그대롭니다
  - 이제 동아리 내부 인터넷 사용량이 실시간으로 통계가 됩니다.
    (현재는 “누가, 언제” 만 통계를 내지만 사실은 얼마나, 어디로의 통계도 가능합니다)

제원

- 하드웨어: (구)다 본체에 1Gbps NIC 2개를 꽂아서 사용

- 개별 IP 100Mbps 지원(MTU 1500)
- Up/Down 1Gbps 지원
  - 200Mbps 까지는 검증 완료
  - Drop rate 등의 통계는 에어컨 뒤의 콘솔에서 확인하실 수 있습니다.
- 내부 통신은 이 트래픽에 포착되지 않습니다.
  - (ex: 동방에서 마녀사냥 다운로드 등등)

연결 구조



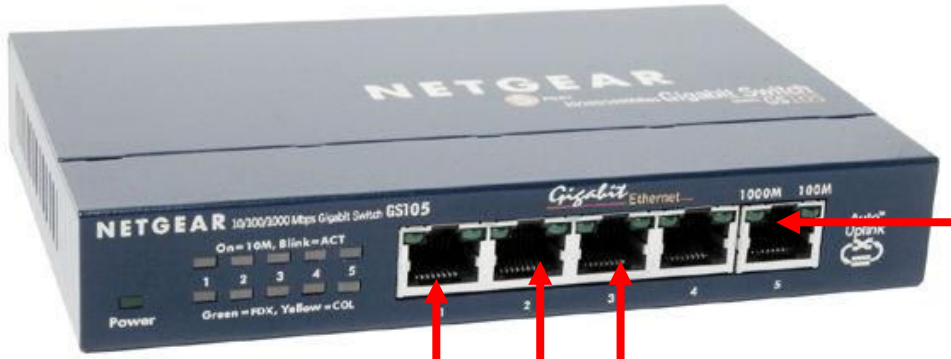
IP Toy II

외부 링크

사용자

사용자

사용자



IP Toy II

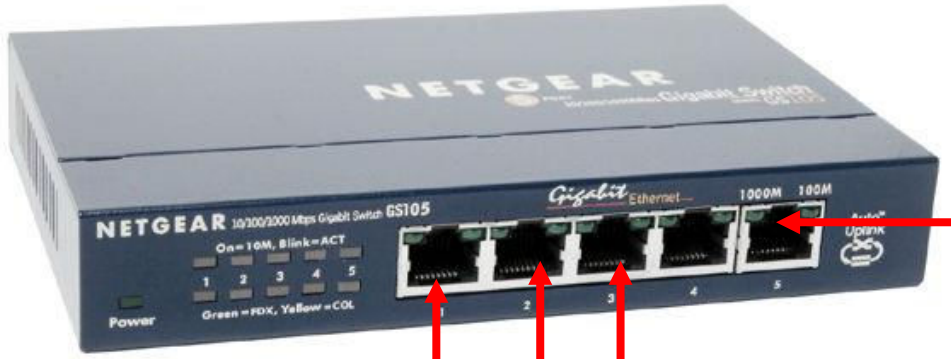
외부 링크

1. 나는 ABCD다, 234.1은 응답하라.

사용자

사용자

사용자



IP Toy
II

외부
링크

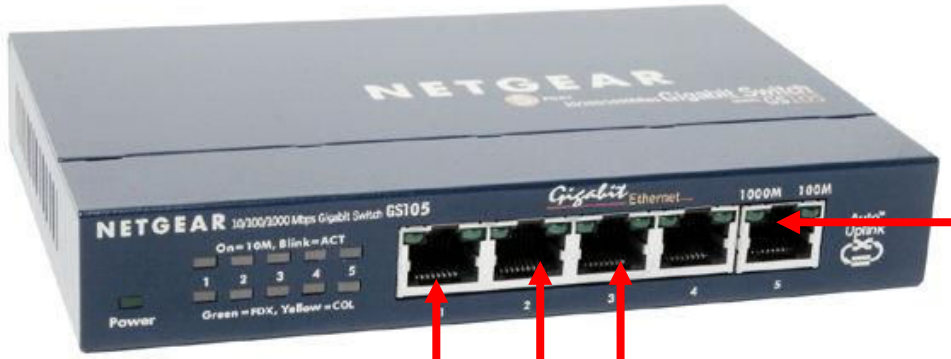
2. 234.123은 ABCD에게 허용된 주소, 바깥에는 DCBA로 보임

1. 나는 234.123에 있는 ABCD 234.1은 누구냐

사용자

사용자

사용자



IP Toy II

외부 링크

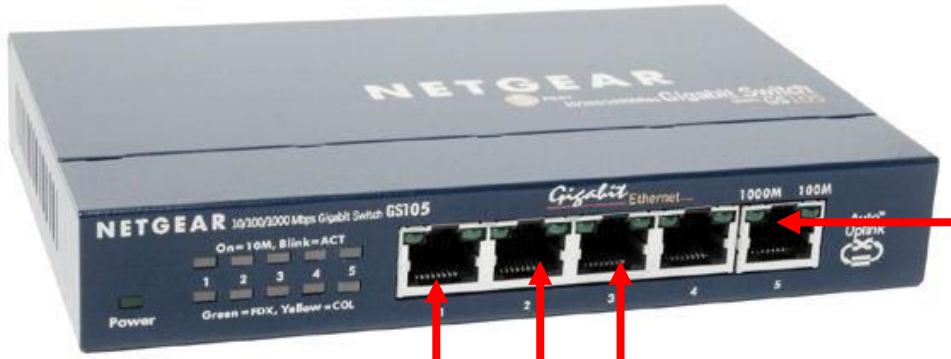
234.123은 ABCD에게 허용된 주소, 바깥에는 DCBA로 보임

1. 나는 234.123에 있는 ABCD 234.1은 누구냐

사용자

사용자

사용자



IP Toy
II

외부
링크

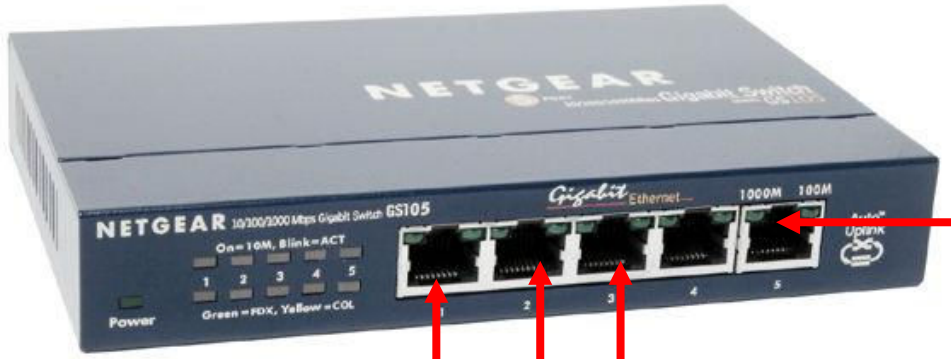
보낸이 MAC: **ABCD**
보낸이 IP: 234.123
받는이 MAC: FFFF
받는이 IP: 234.1
종류: 질문

보낸이 MAC: **DCBA**
보낸이 IP: 234.123
받는이 MAC: FFFF
받는이 IP: 234.1
종류: 질문

사용자

사용자

사용자



IP Toy
II

외부
링크

234.123은 ABCD에게 허용된
주소, 바깥에는 DCBA로 보임

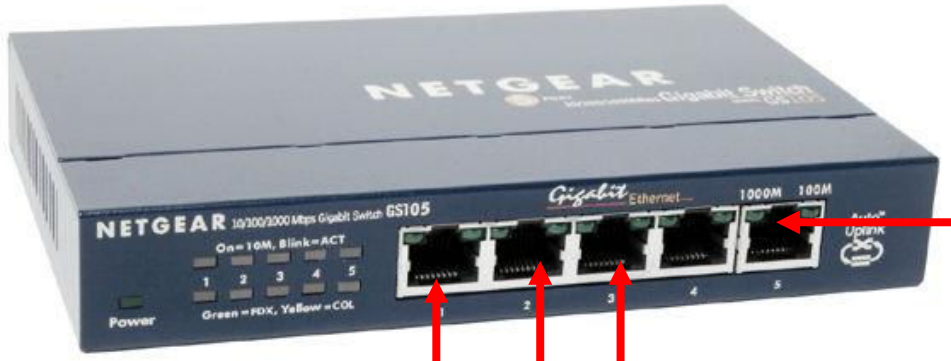
외부 링크의 눈으로는

1. 나는 234.123에 있는 **DCBA**
234.1은 누구냐

사용자

사용자

사용자



IP Toy
II

외부
링크

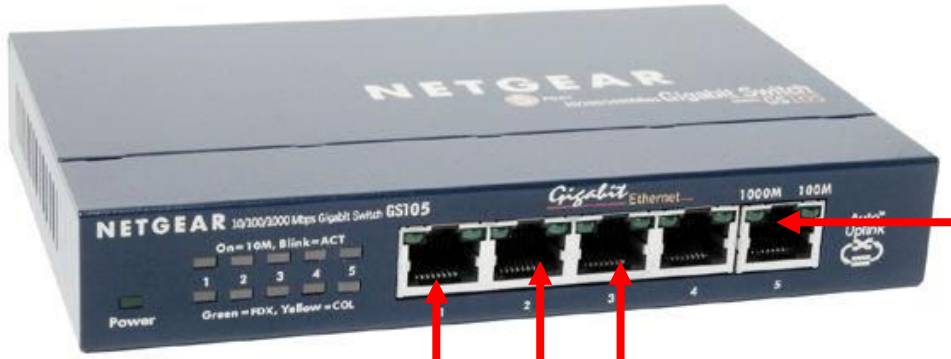
234.123 IP와, DCBA MAC을 가진 패킷은 ABCD로 간다.

2. 234.123에 있는 DCBA여, 234.1은 EFEF에 있다.

사용자

사용자

사용자



IP Toy
II

외부
링크

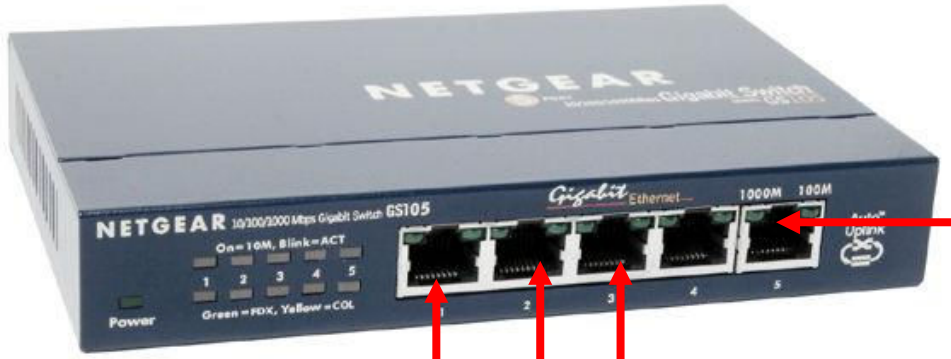
보낸이 MAC: EFEF
보낸이 IP: 234.1
받는이 MAC: **ABCD**
받는이 IP: 234.123
종류: 응답

보낸이 MAC: EFEF
보낸이 IP: 234.1
받는이 MAC: **DCBA**
받는이 IP: 234.123
종류: 응답

사용자

사용자

사용자



IP Toy
II

외부
링크

234.123 IP와, DCBA MAC을 가진 패킷은 ABCD로 간다.

2. 234.123에 있는 **ABCD**여, 234.1은 EFEF에 있다.

사용자의 눈으로는

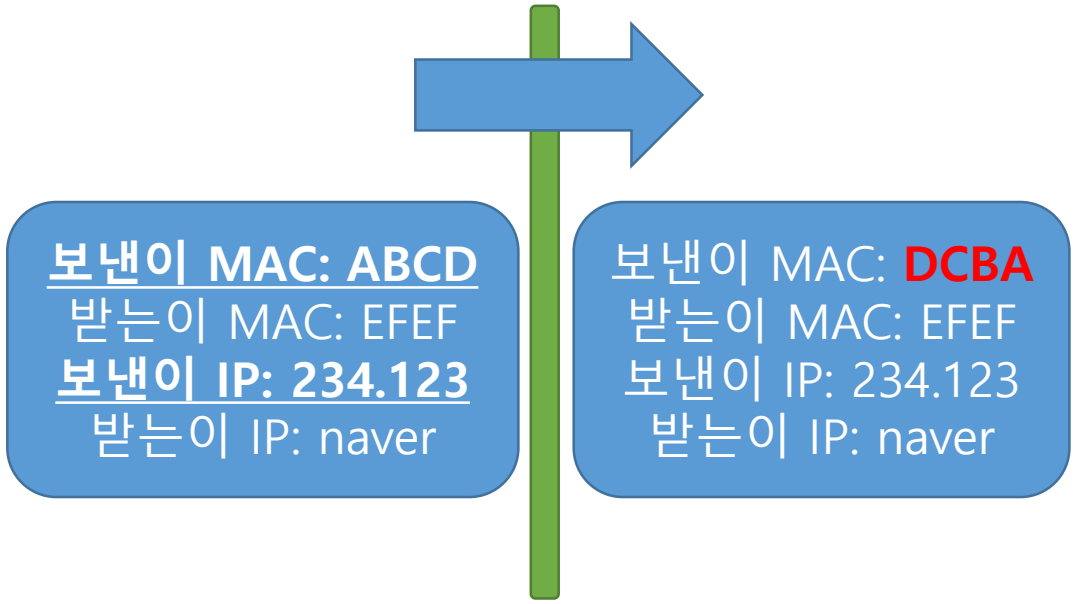
사용자

사용자

사용자

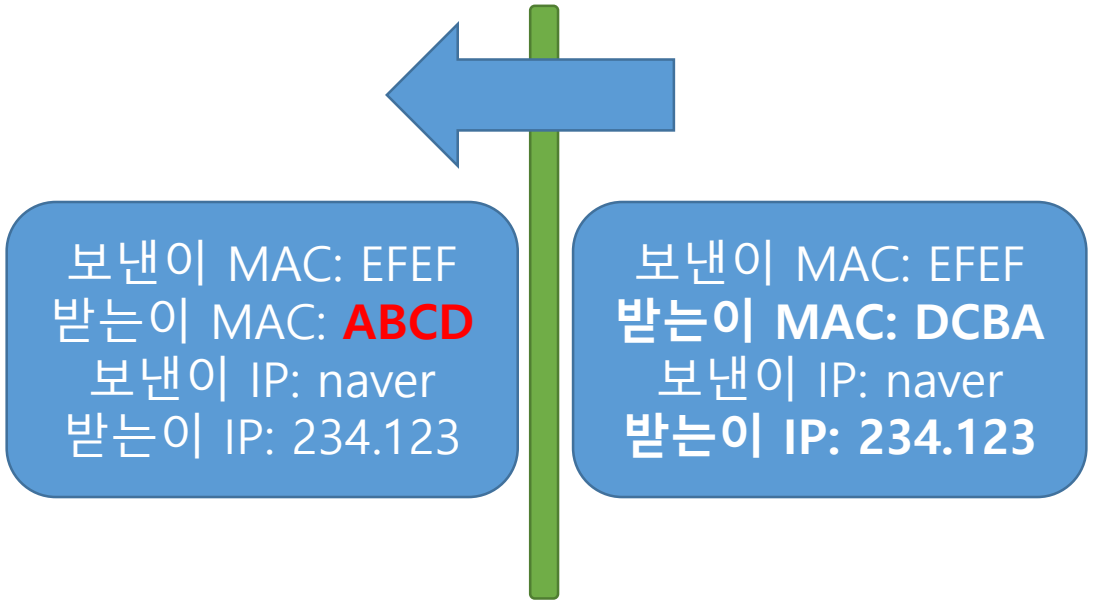
IP 패킷 처리

패킷이 나갈 때



보낸이 MAC과 **보낸이 IP**를 보고 Table에서 검색을 하여 **보낸이 MAC**을 치환하여 바깥으로 보낸다.

패킷이 들어올 때



받는이 MAC과 **받는이 IP**를 보고 Table에서 검색을 하여 **받는이 MAC**을 치환하여 안쪽으로 보낸다.

그 외…

- DHCP 요청은 따로 필터링하여 바깥으로 내보내지 않고 내부 로직에 따라 응답을 생성하여 보내준다.

- 만일 게이트웨이의 MTU 크기보다 큰 패킷을 전송하려 하면 MTU discover를 따라 적절한 ICMP응답을 보내준다.

- 모든 검색은 in-memory hash table에서 이루어지며 매 패킷을 검사할 수 있을 정도로 빠르다.
- DB 검색 요청은 asynchronous 하게 이루어진다.

만일 인터넷이 되지 않는다…

1. Sparcs.org 에서 mysql –u gateway –p –h 143.248.234.136 에서 `gateway`.`static_ip` 에 적힌 IP가 맞는지 본다.
2. `gateway`.`user` 테이블에 자신의 IP와 자신의 local MAC이 제대로 적혀 있는지 확인한다.
3. `gateway`.`static_ip` 에 IP가 없다면 게이트웨이는 아무 일을 하지 않는다.
4. 만일 3의 조건을 만족하는데 인터넷이 되지 않으면 재부팅을 시도해본다(MAC table에 혼란이 와서 인터넷이 멈추는 경우가 있습니다.)

만일 인터넷이 이미 잘 된다...

1. `gateway`.`user` 테이블에 자신의 IP와 자신의 local MAC이 제대로 적혀 있는지 확인한다.
2. 혹시 만약에 MAC 주소 고정을 정통팀에 신청했다면 `gateway`.`static_ip` 에 있는 MAC이 그 MAC인지 확인한다. (현재는 내부-외부 MAC을 모두 동일한 것으로 설정)
3. 1,2 가 만족한다면 네트워크 설정을 자동 IP로 바꾸어보자
4. IP 설정이 자동으로 이루어질 것이다.