인터넷 만들기

고양우

따로 출처 표기가 없는 그림은 Microsoft의 클립, 위키백과의 그림 또는 제가 그림 것입니다.

We reject: kings, presidents and voting.
*We believe in: **rough consensus** and*
***running code**. – David D. Clark*

관리자@오픈넷.KR

RFC6530 / RFC6531 / RFC6532 / RFC6533

RFC5890 / RFC5891 / RFC3743 / RFC4290

THE FIFTY-THIRD
INTERNET ENGINEERING TASK FORCE
Hosted by Cable and Wireless
Minneapolis, Minnesota USA
March 17 - 22, 2002

2.1.18 Keywords Naming Services (kwns) Bof
Current Meeting Report
[kwns BOF]

Co-Chair YangWoo Ko introduces charter, defines "Keywords" for the purpose of this meeting:

- Keywords are defined as internationalized string for internet navigation.

- Charter highlights - direct navigation is very desirable for users -users wish to use keywords as unambiguous addresses

WHO RUNS THE INTERNET?

NO ONE PERSON, COMPANY, ORGANIZATION OR GOVERNMENT RUNS THE INTERNET.

The Internet itself is a globally distributed computer network comprised of many voluntarily interconnected autonomous networks. Similarly, its governance is conducted by a decentralized and international multi-stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities, and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good.

WHO IS INVOLVED:

IAB A C P S R
INTERNET ARCHITECTURE BOARD
Oversees the technical and engineering development of the IEFT and IRTF.
www.iab.org

ICANN C O P V
INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
Coordinates the Internet's systems of unique identifiers: IP addresses, Protocol-Parameter registries, top-level domain space (DNS root zone).
www.icann.org

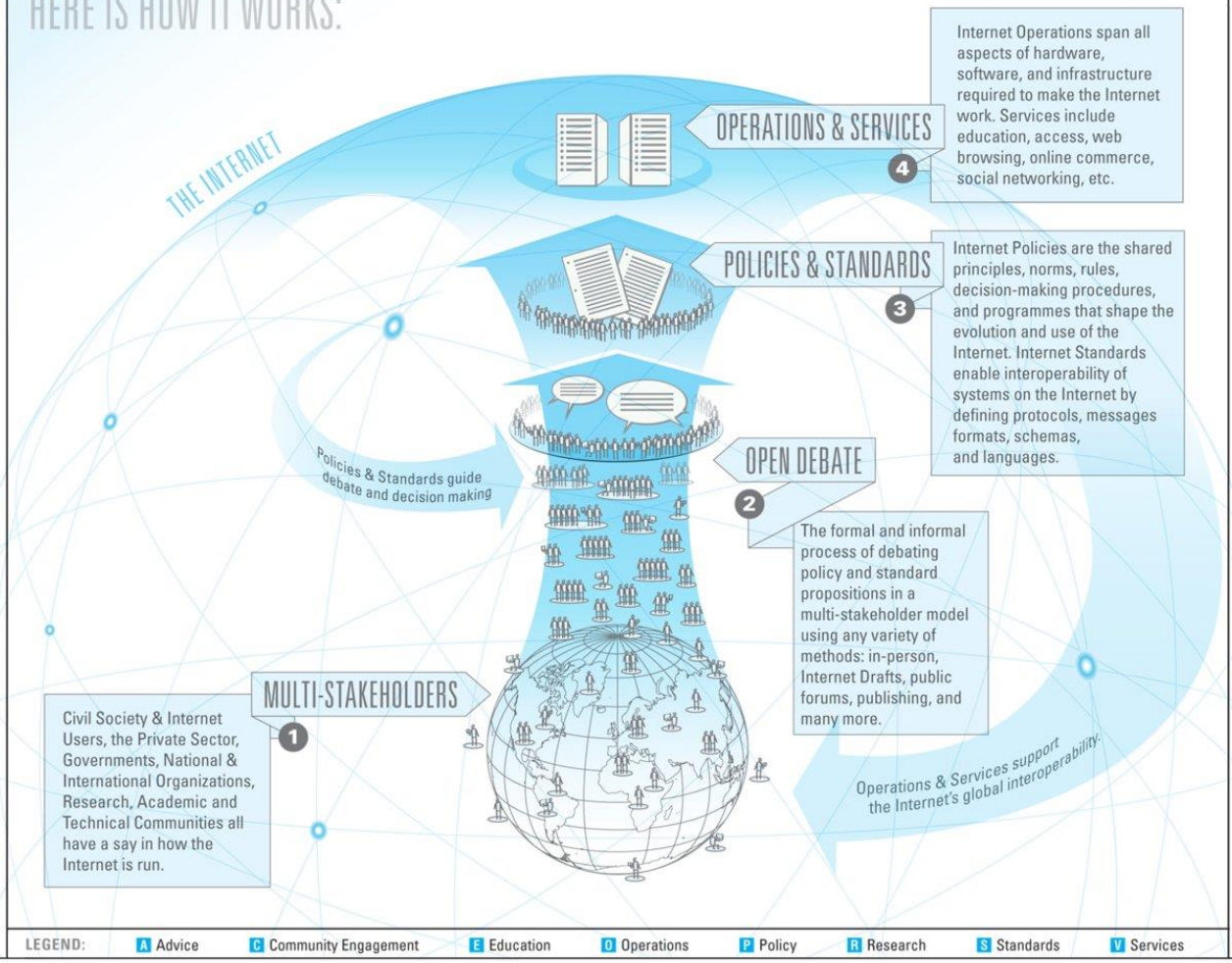
IETF C P S
INTERNET ENGINEERING TASK FORCE
Develops and promotes a wide range of Internet standards dealing in particular with standards of the Internet protocol suite. Their technical documents influence the way people design, use, and manage the Internet.
www.ietf.org

IGF A C P
INTERNET GOVERNANCE FORUM
A multi-stakeholder open forum for debate on issues related to internet governance.
www.intgovforum.org

IRTF R
INTERNET RESEARCH TASK FORCE
Promotes research of the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.
www.irtf.org

GOVERNMENTS AND INTER-GOVERNMENTAL ORGANIZATIONS C P
Develop laws, regulations and policies applicable to the Internet within their jurisdictions; participants in multilateral and multi-stakeholder regional and international fora on Internet Governance.

HERE IS HOW IT WORKS:



WHO IS INVOLVED:

ISO 3166 MA S
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, MAINTENANCE AGENCY
Defines names and postal codes of countries, dependent territories, special areas of geographic significance.
www.iso.org/iso/country_codes.htm

ISOC C E P V
INTERNET SOCIETY
Assure the open development, evolution and use of the Internet for the benefit of all people throughout the world. Currently ISOC has over 90 chapters in around 80 countries.
www.internetsociety.org

RIRs O P V
5 REGIONAL INTERNET REGISTRIES
Manage the allocation and registration of Internet number resources, such as IP addresses, within geographic regions of the world.

www.afrinic.net	Africa
www.apnic.net	Asia Pacific
www.arin.net	Canada & United States
www.lacnic.net	Latin America & Caribbean
www.ripe.net	Europe, the Middle East & parts of Central Asia

W3C S
WORLD WIDE WEB CONSORTIUM
Create standards for the world wide web that enable an Open Web Platform, for example, by focusing on issues of accessibility, internationalization, and mobile web solutions.
www.w3.org

INTERNET NETWORK OPERATORS' GROUPS A O V
Discuss and influence matters related to Internet operations and regulation within informal fora made up of Internet Service Providers (ISPs), Internet Exchange Points (IXPs) and others.

This graphic is a living document, designed to provide a high level view of how the internet is run. It is not intended to be a definitive guide. Please provide feedback at www.xplanations.com/whorunstheinternet

그림 출처: http://thetecnica.com/2013/03/who-runs-the-internet-infographic

인터넷을 왜
만들었을까?

그림 출처:http://www.maximumpc.com/files/u69/IBM_Punch_Card.png

데이터는 무겁고 컴퓨터는 비싸고

나는 1960년대에 예일 대학에 있었는데 그 때의 컴퓨터는 무척 크고, 비싸고 또한 몹시 귀했다. 그래서 전산 센터는 희귀한 자원이 있는 핵심 지점의 역할을 했다. 옛날 마을에서 공동 우물과 같은 역할인 셈이다. 컴퓨터를 이용해야 하는 입장이라면 그 무거운 펀치 카드 박스를 들고 멀리 걸어 다니고 싶진 않았을 것이다. (Mitchell, 2005)

그림 출처:http://www.computescotland.com/images/EfVlPmeK4Y2B6oYEnMl10e30b7.jpg

존 매카시(1961) *컴퓨터는 빠르니 여러 사람이 동시에 쓸 수 있고 이걸 계속 발전시키면 컴퓨터 서비스가 물이나 전기와 같은 서비스가 될 것이다.*

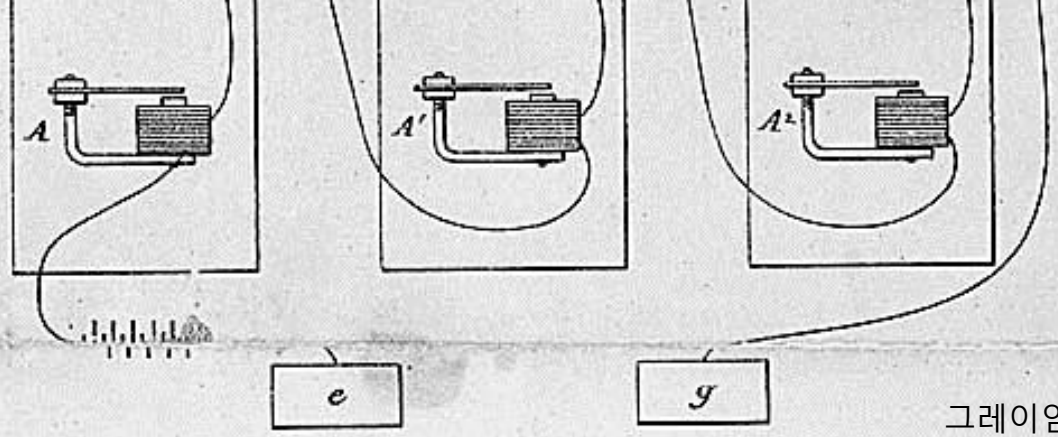
그림 출처:http://en.wikipedia.org/wiki/File:John_McCarthy_Stanford.jpg

AI / Lisp / Algol

릭라이더(1962) 전 세계 어디서나 원하는 프로그램과 자료를 활용할 수 있게 해주는 은하 네트워크 제안

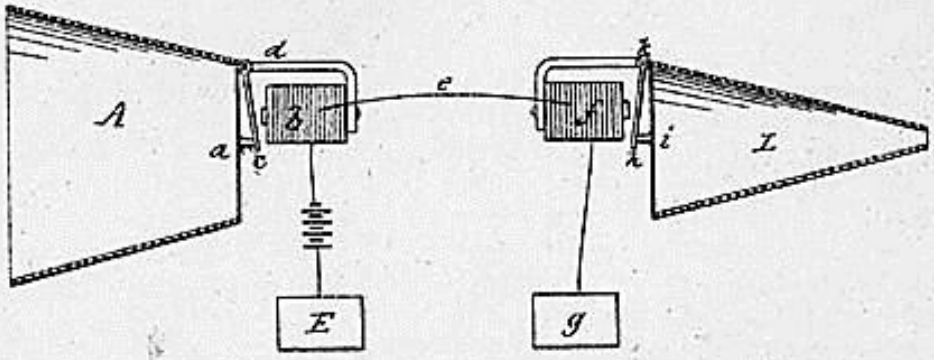
SAGE(1950s) 컴퓨터 기반의 항공 방위 시스템용 사용자 단말

통신의 선구자



그레이엄 벨(1876)
전화 특허 등록

Fig. 7

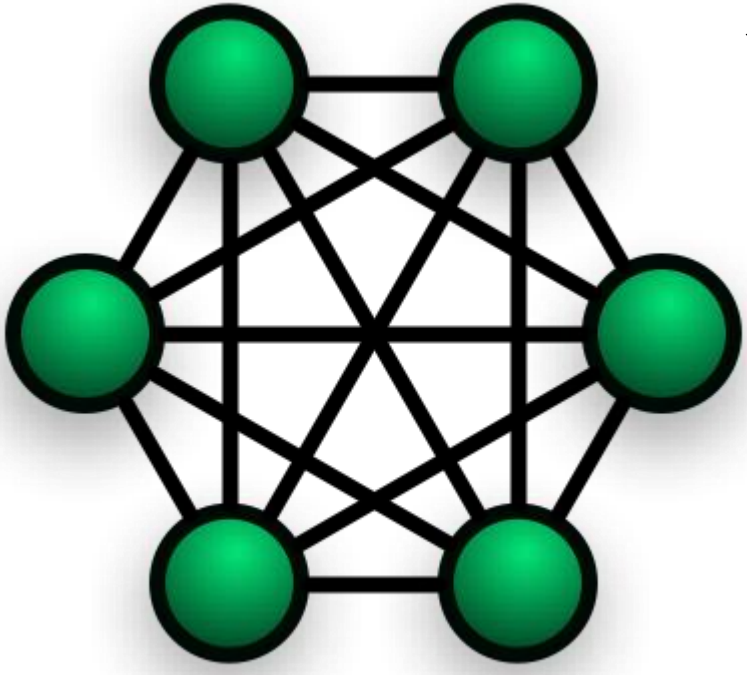


Witnesses
Ewell Strickl.
H. J. Hutchinson

Inventor:
A. Graham Bell
by atty Pollock & Bailey

The Detroit News Timely Topics

Bell's First Telephone



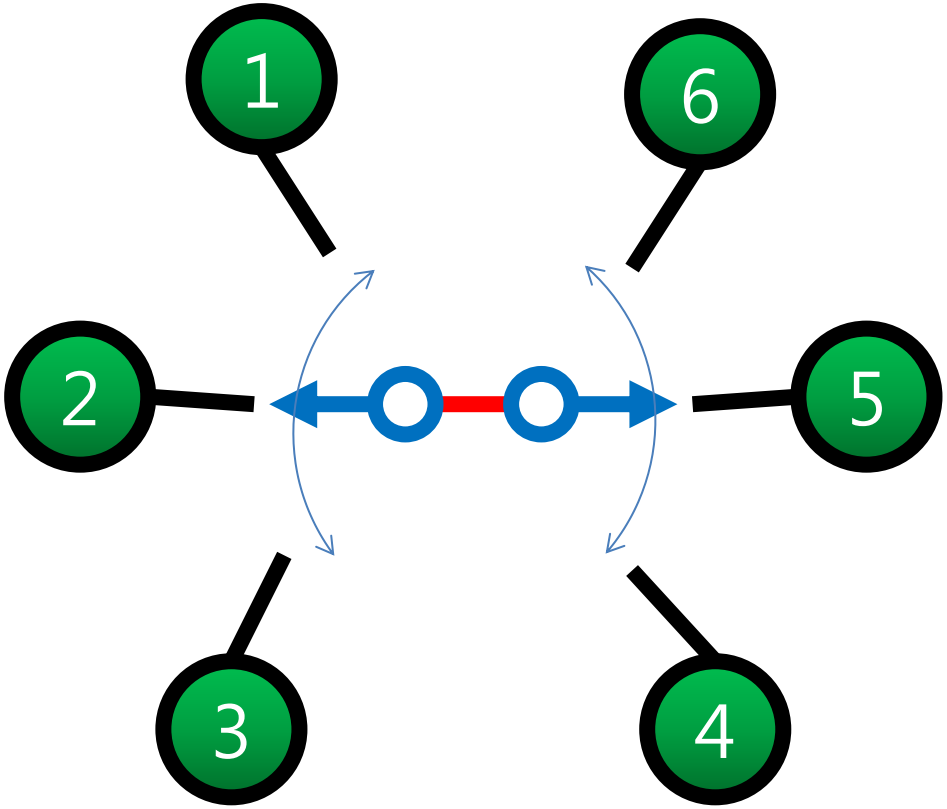
전화기가 늘어나면 어쩌지?

100억대의 컴퓨터를 완전히 연결하려면?

굵기 0.1mm의 회선으로 연결해도
8만 Km 높이로 전 지구를 덮어야 한다.

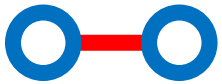
$$n(n-1)/2=$$

$$O(n^2)$$

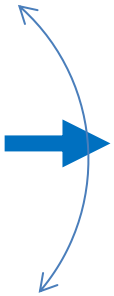


$n+1=$

$O(n)$



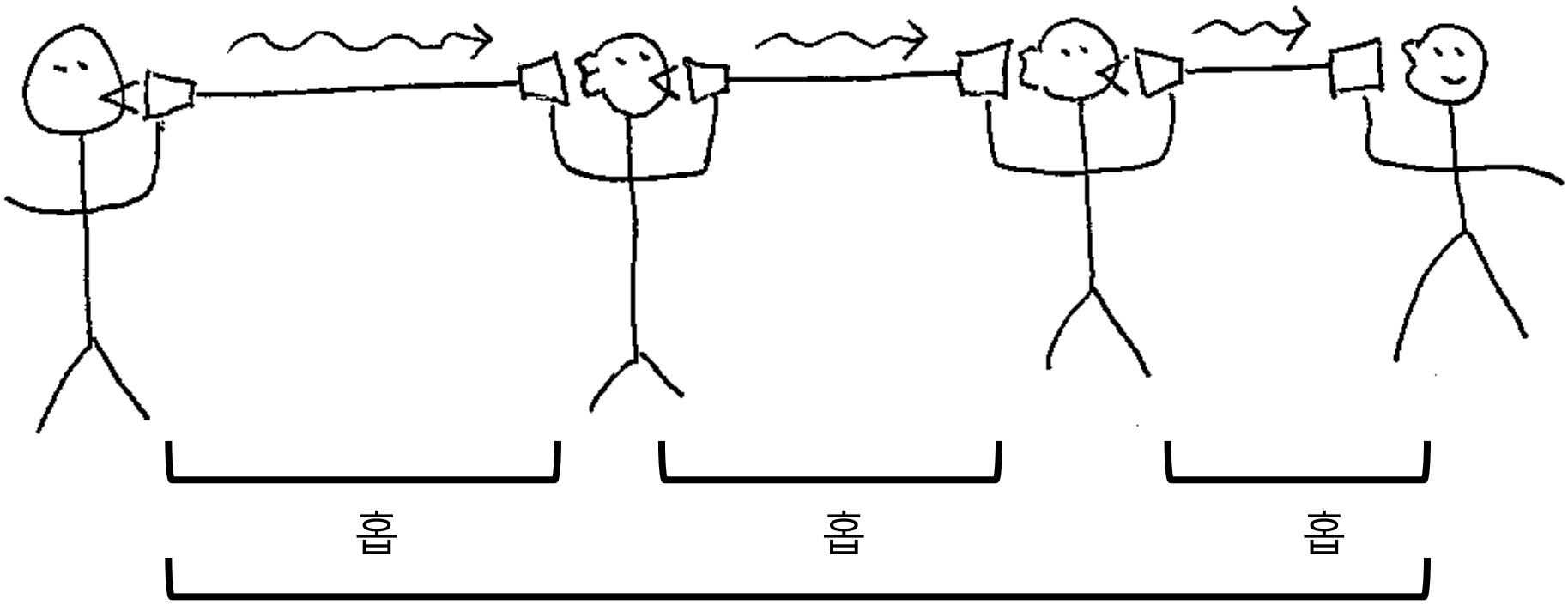
의 갯수가 동시 통화 수를 결정



는 누가하지?

붙어야 통한다

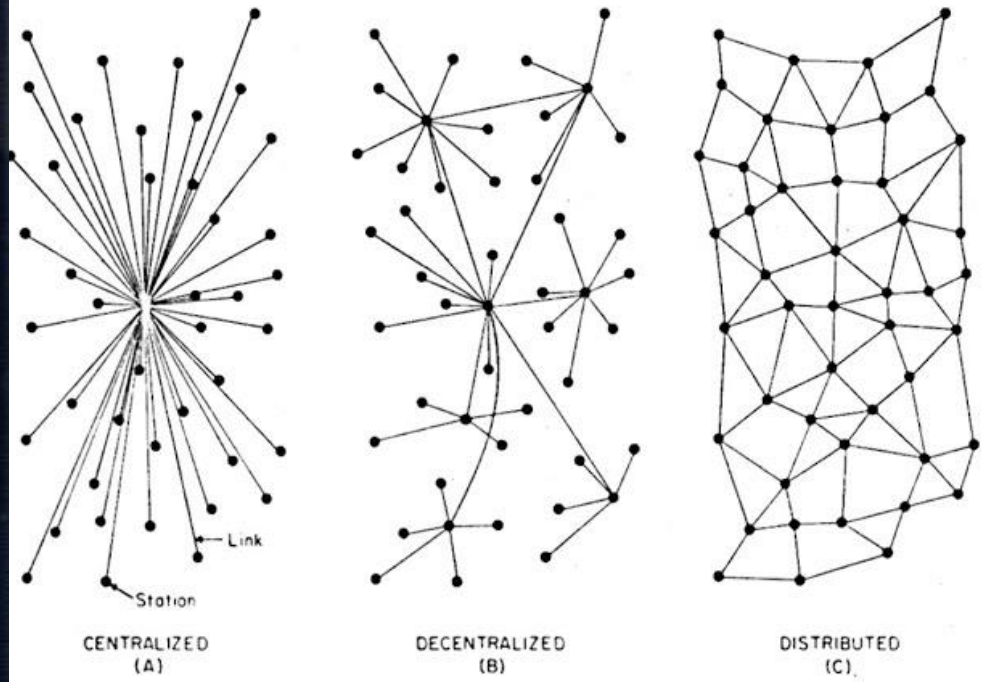
그림 출처: http://tpmdc.talkingpointsmemo.com/2011/07/voters-jam-capitol-phone-lines.php



멀리까지 가려면 **중계**를 해주면 된다.

컴퓨터 통신의 시작

패킷의 탄생



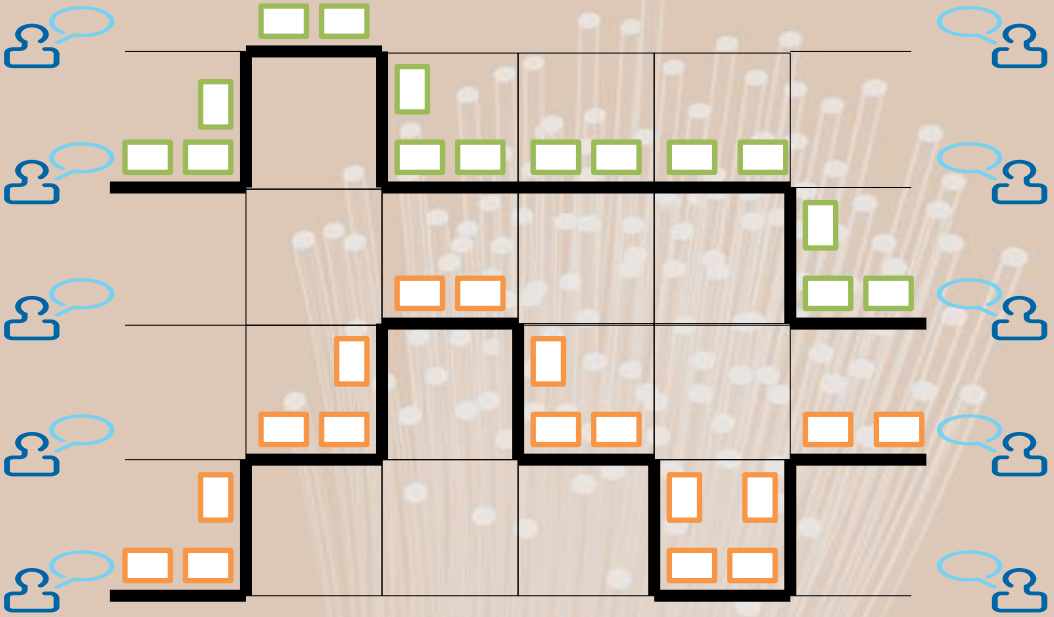
폴 바란@RAND(1960)
핵 무기에도 버티는
생존형 통신 수단 개발

레너드 클라인락 (1962)
컴퓨터를 시간의 축으로
쪼개서 공유할 수 있다면
회선도 같이 하면 안돼?

도널드 데이비스@NPL
(1964) 패킷 스위칭!

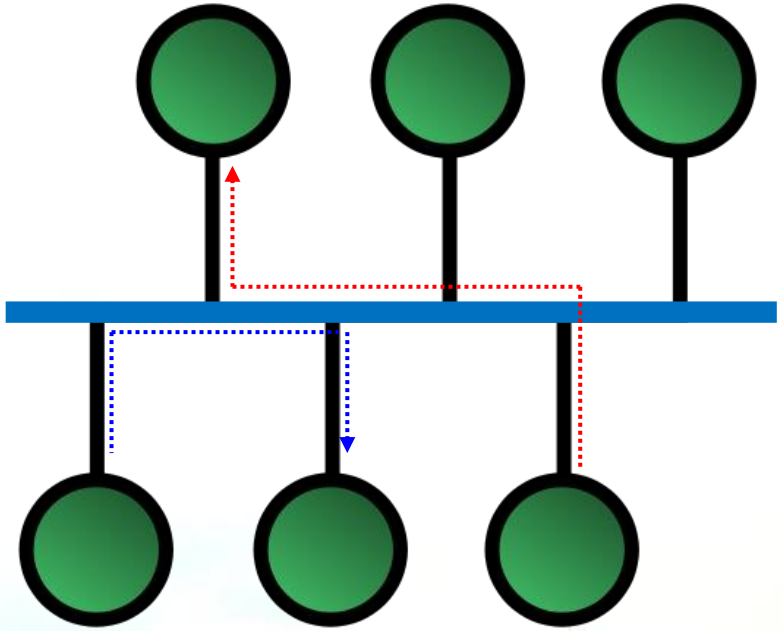
길을 미리 뚫어 놓는다.
통화(세션) 끝까지 전용이다.
회선이 낭비될 수 있다.
품질이 보장된다.
끊기면 끊긴다.

circuit switching



packet switching

패킷을 전달할 때 길을 정한다.
통화(세션) 개념이 없다.
회선을 공유할 수 있다.
품질이 보장되기가 거의 불가능.
끊기면 돌아서라도 간다.



패킷 덕분에 회선의 독점
할당에서 해방되어

버스 탄생

그림 출처: http://upload.wikimedia.org/wikipedia/commons/9/9f/Hands_Across_America_Philadelphia.jpg

그림 출처: http://farm8.staticflickr.com/7267/7113714943_902f956c5b_z.jp

costermk

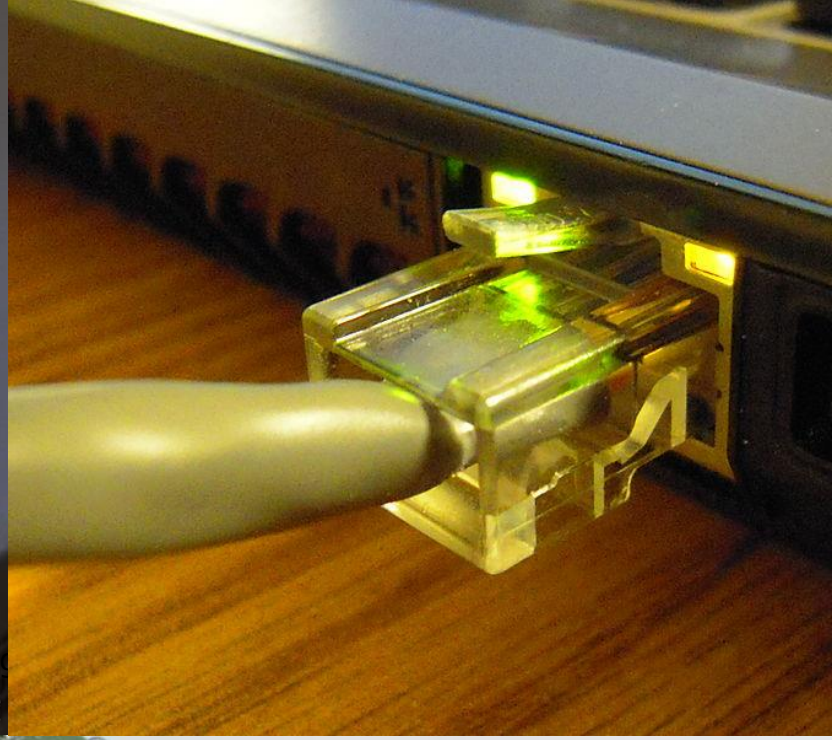


그림 출처: http://hbernstaedt.de/thinethernet.jpg

버스+패킷의 운명: 주소 & 충돌 →

➔ 메트칼프(1973) Ethernet

MAC 주소를 봉투에

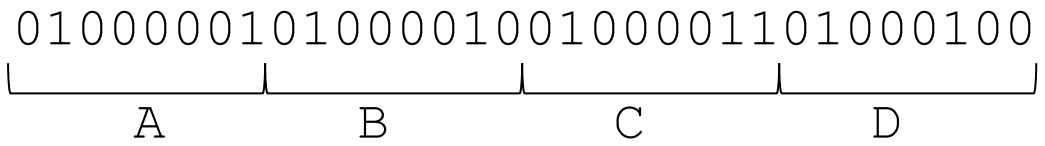
CS: carrier sense 남이 안 보낼 때
MA: multiple access 여럿이 공유
CD: collision detection 충돌 확인
➔ **random** back off

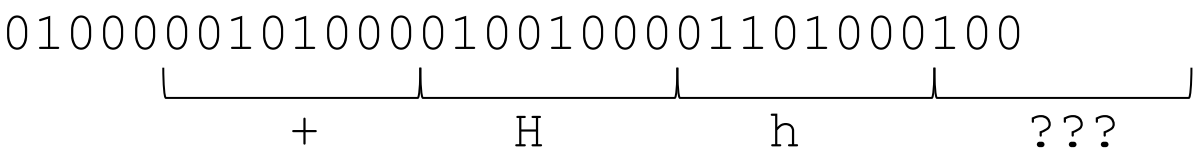
→ 그리고 도청
Promiscuous mode
들리지만 못 듣는 척

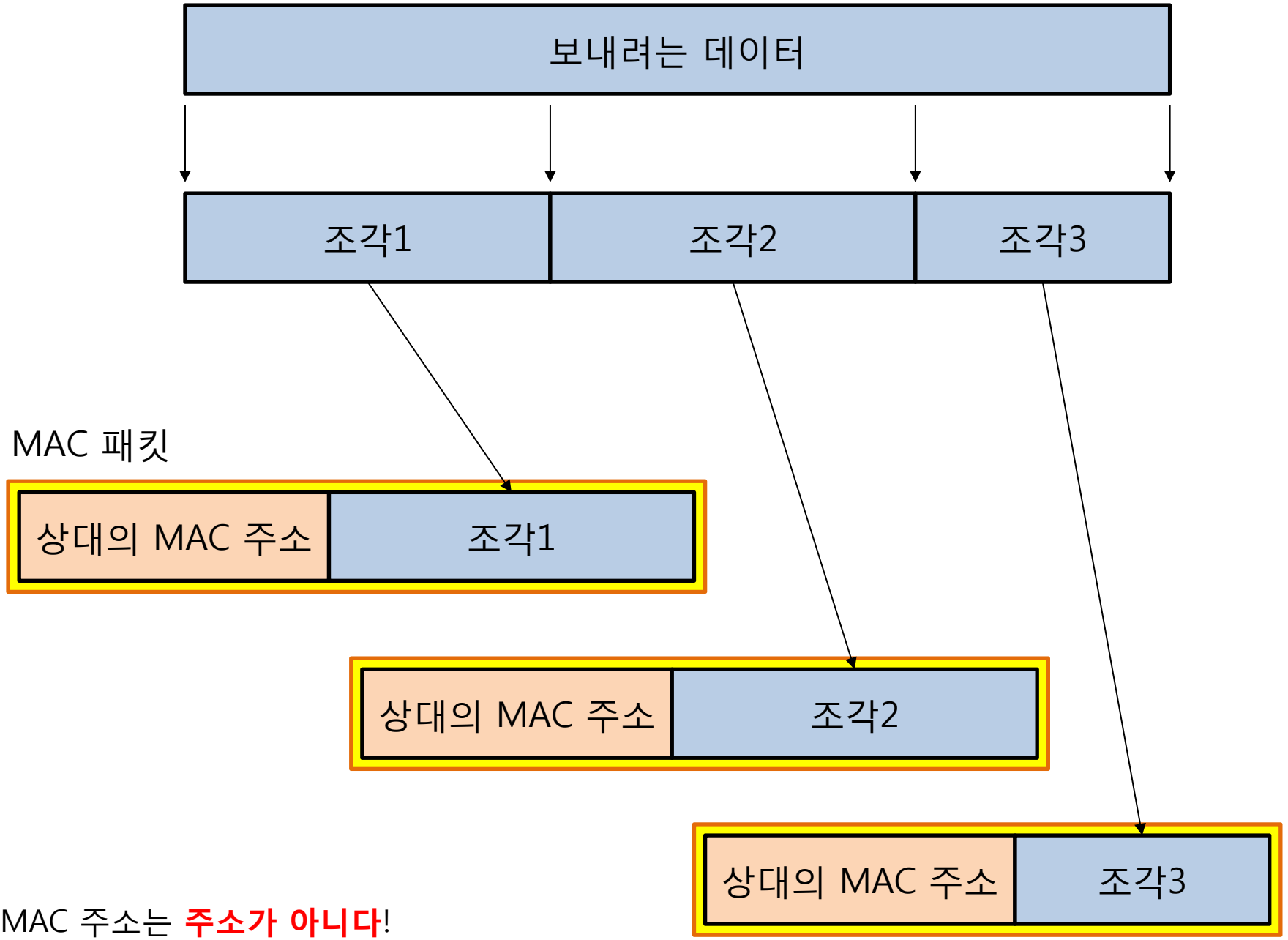
기원전 3세기의 아리스토텔레스는 우주의 중심이 지구이고 그 위로 달, 태양, 행성이 수정 구면 위에 붙어 궤도를 돌고 있다고 주장했다. 세계는 (무거운 순서로) 흙, 물, 공기, 불의 4원소로 구성되어 있어 불완전하(고 땅으로 추락하)지만 우주의 천체는 완벽한 물질인 에테르로 구성되어 있어 완벽하(고 땅으로 추락하지도 않는)다고 했다. 이런 생각은 16세기까지 유럽에서 받아들여졌다. (nasa 홈페이지에서 발췌 번역)

그림 출처: http://elementsunearthed.com/2009/06/

어디가 시작이고 어디가 끝인가?





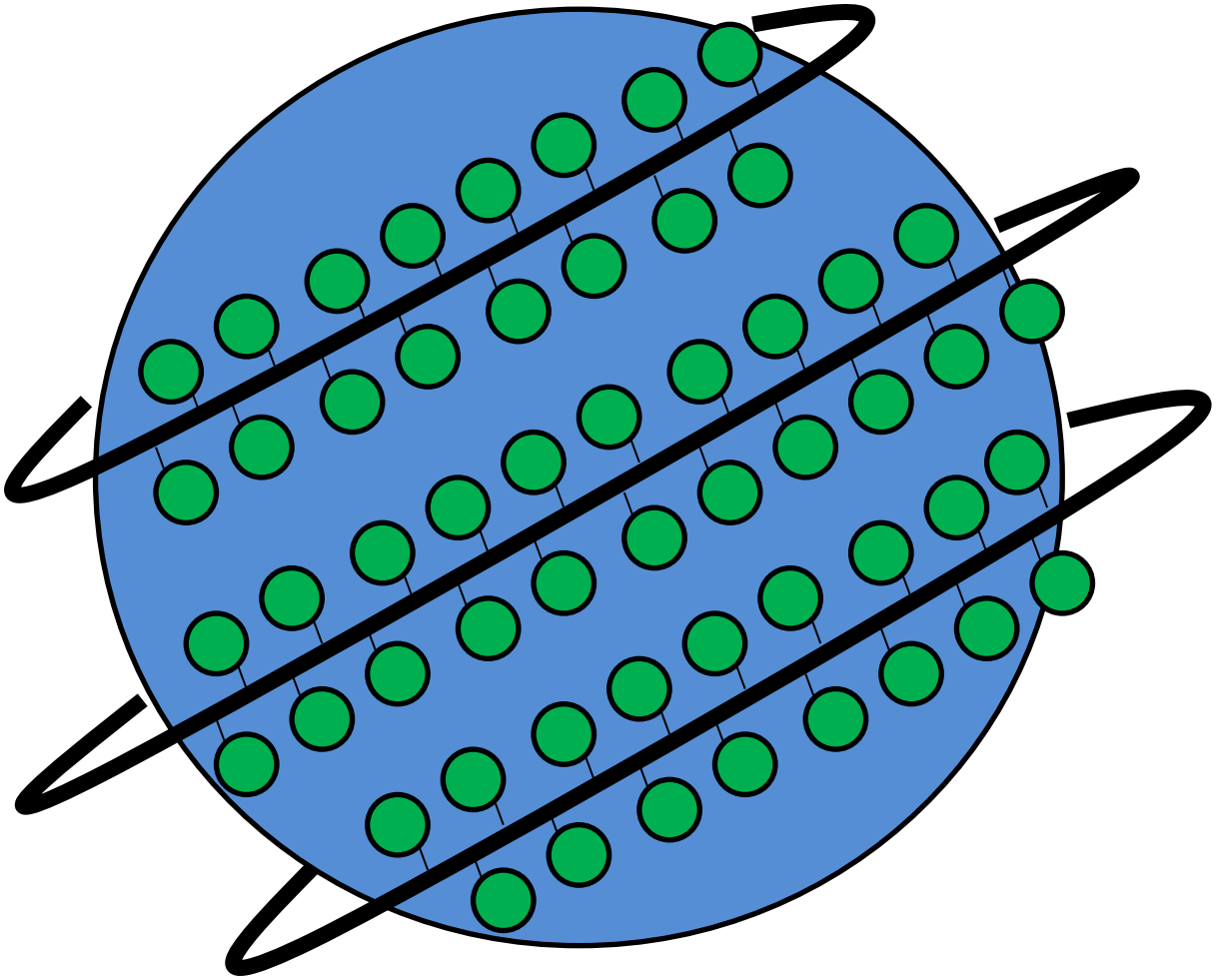


MAC 주소는 **주소가 아니다**!

MAC or L2

직접 연결된 컴퓨터
끼리 데이터를
주고 받을 수
있게 되었다

전 지구 단일 버스 네트워크

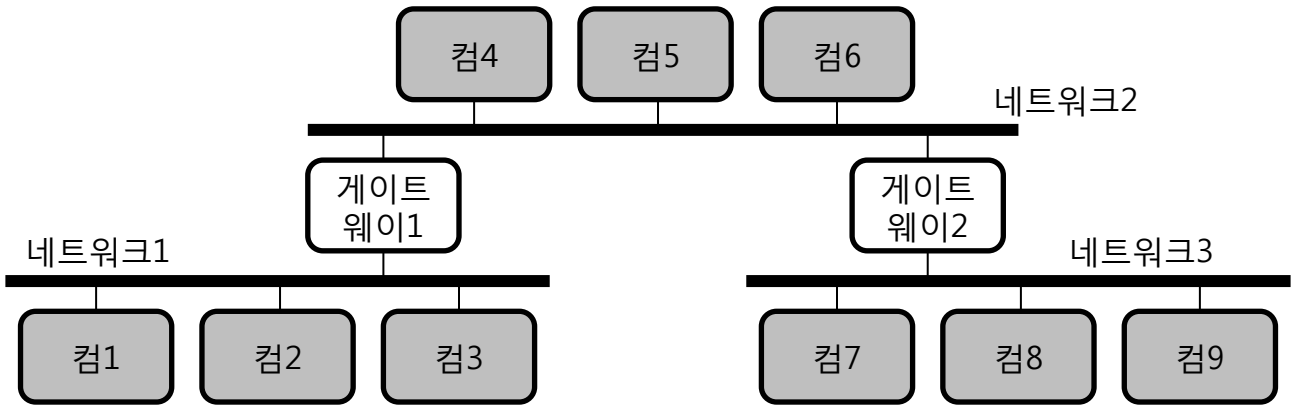


굼벵이 빛 또는 너무 큰 지구

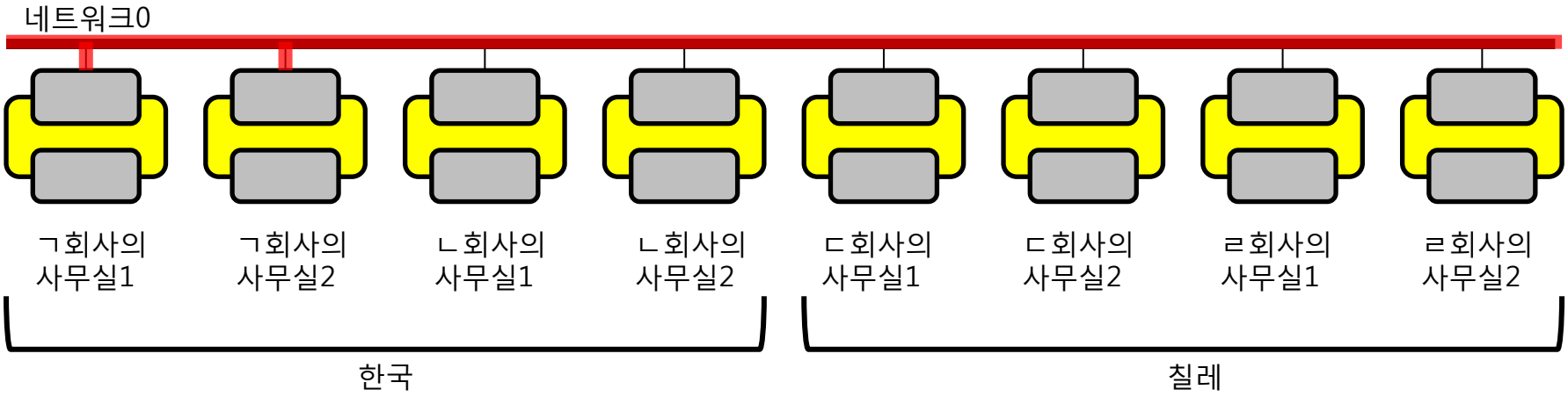
하나로 안 된다 ➔ 여러 네트워크로 쪼개자.
서로 연결은? ➔ 양 다리 걸친 장비를 만들자.

게이트웨이로 연결된 여러 네트워크

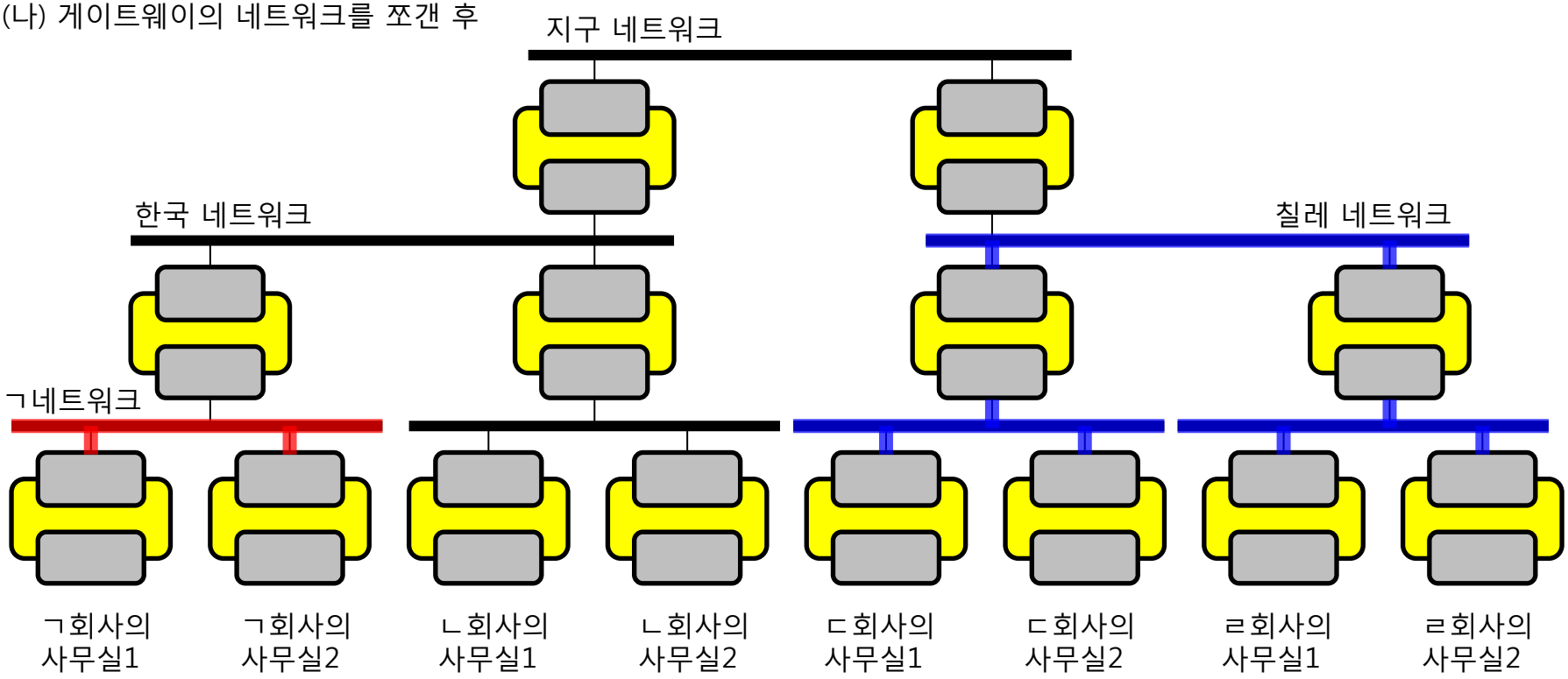
inter - net

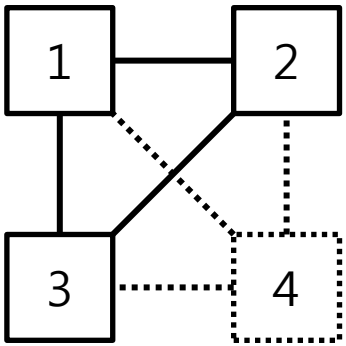


(가) 게이트웨이의 네트워크를 쪼개기 전

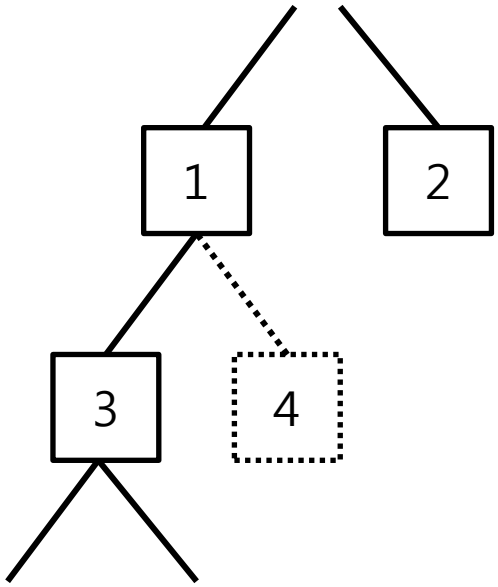


(나) 게이트웨이의 네트워크를 쪼갠 후





(가) 티어-1 네트워크의 경우



(나) 그 이하 네트워크의 경우

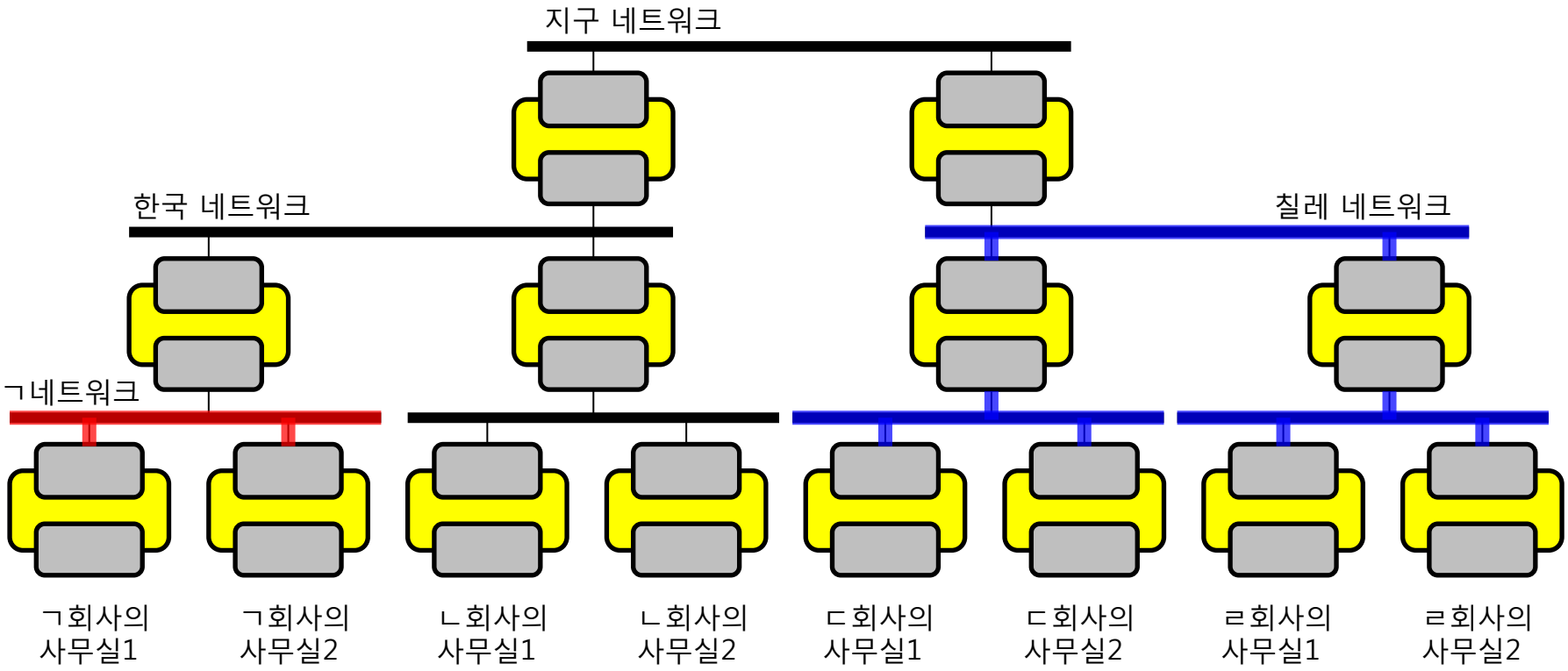
101.211.123.168

네트워크 번호 컴퓨터 번호

게이트웨이의 고민

- 무엇을 퍼 나를지 어떻게 아는가?
- 그것을 알기 위한 비용을 어떻게 줄일 것인가?

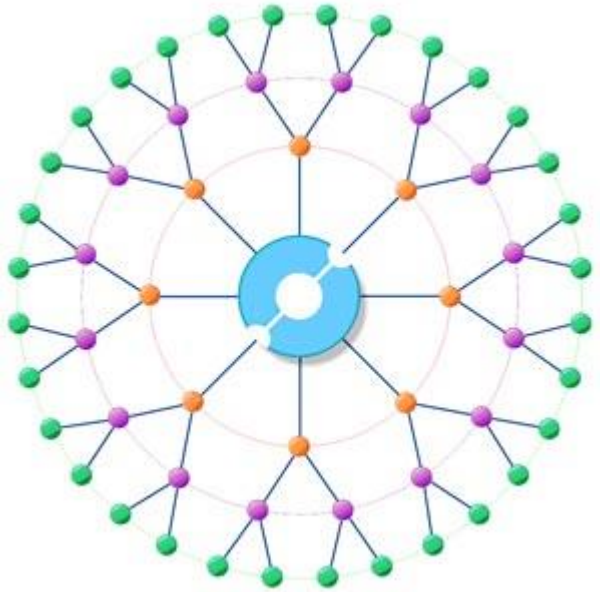
inter - net

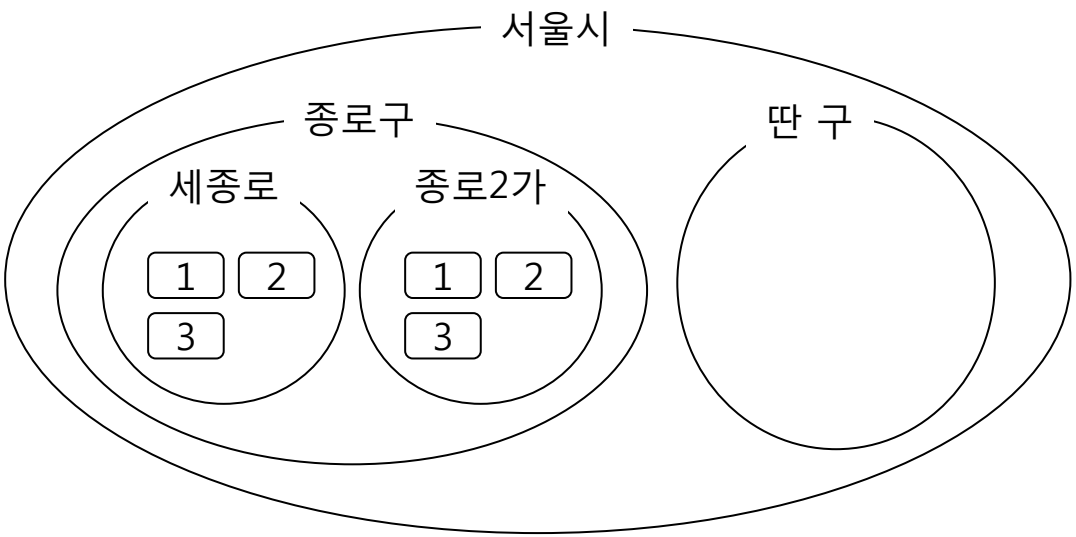


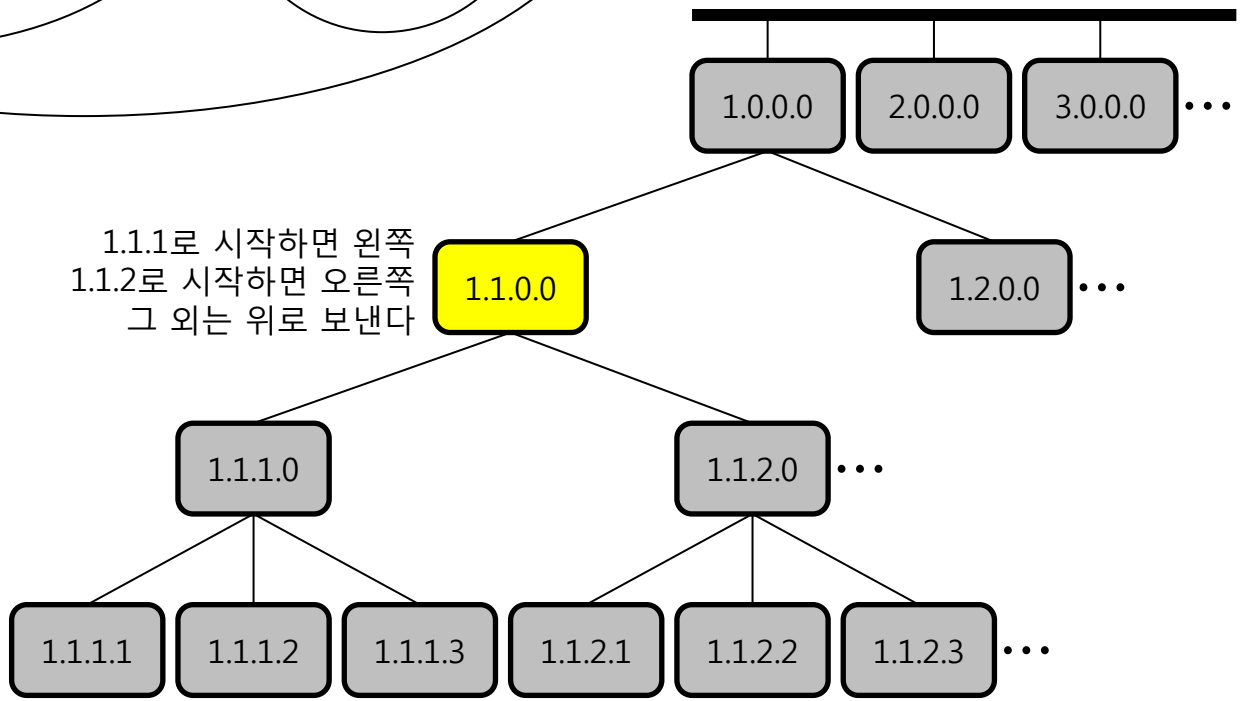
프레데릭 스미스 (1960s)
대학 리포트로 IT 기술을
이용한 당일 배송 시스템
제안 → C학점 ㅠㅠ

1. 모르면 위로 보내라. 고민은 한 곳에서 하자.
2. 주소는 "위치"를 나타내야 한다. (!= MAC)

➔ 컴퓨터 주소 = 네트워크 주소 + 자신을 구별하는 번호
~= "서울시 종로구 세종로" + "1번지"







IP 주소 & 라우팅

IP or L3

전세계 컴퓨터가
어디 있든 찾아갈 수
있게 되었다

계층 구조의 다른 시각

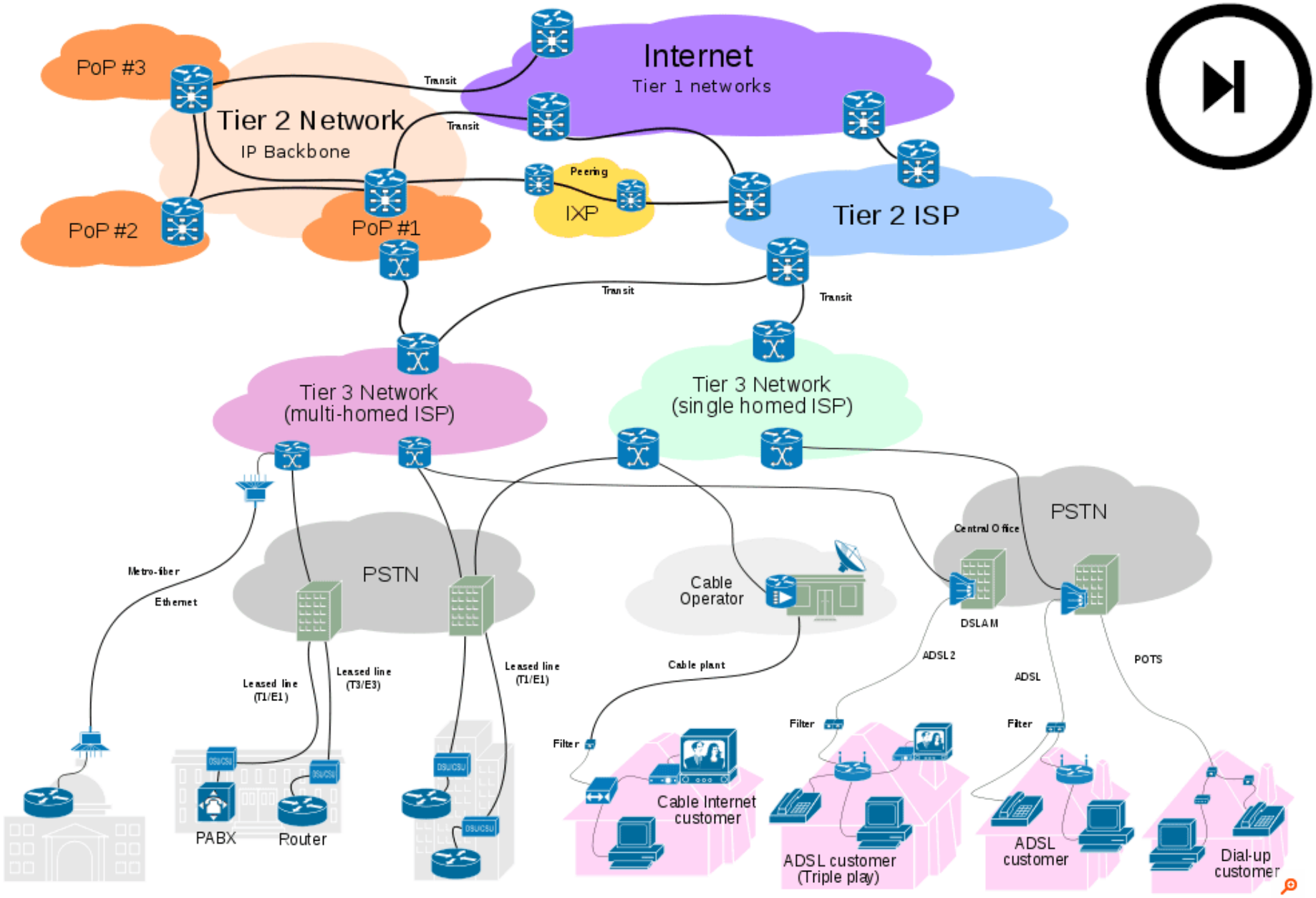
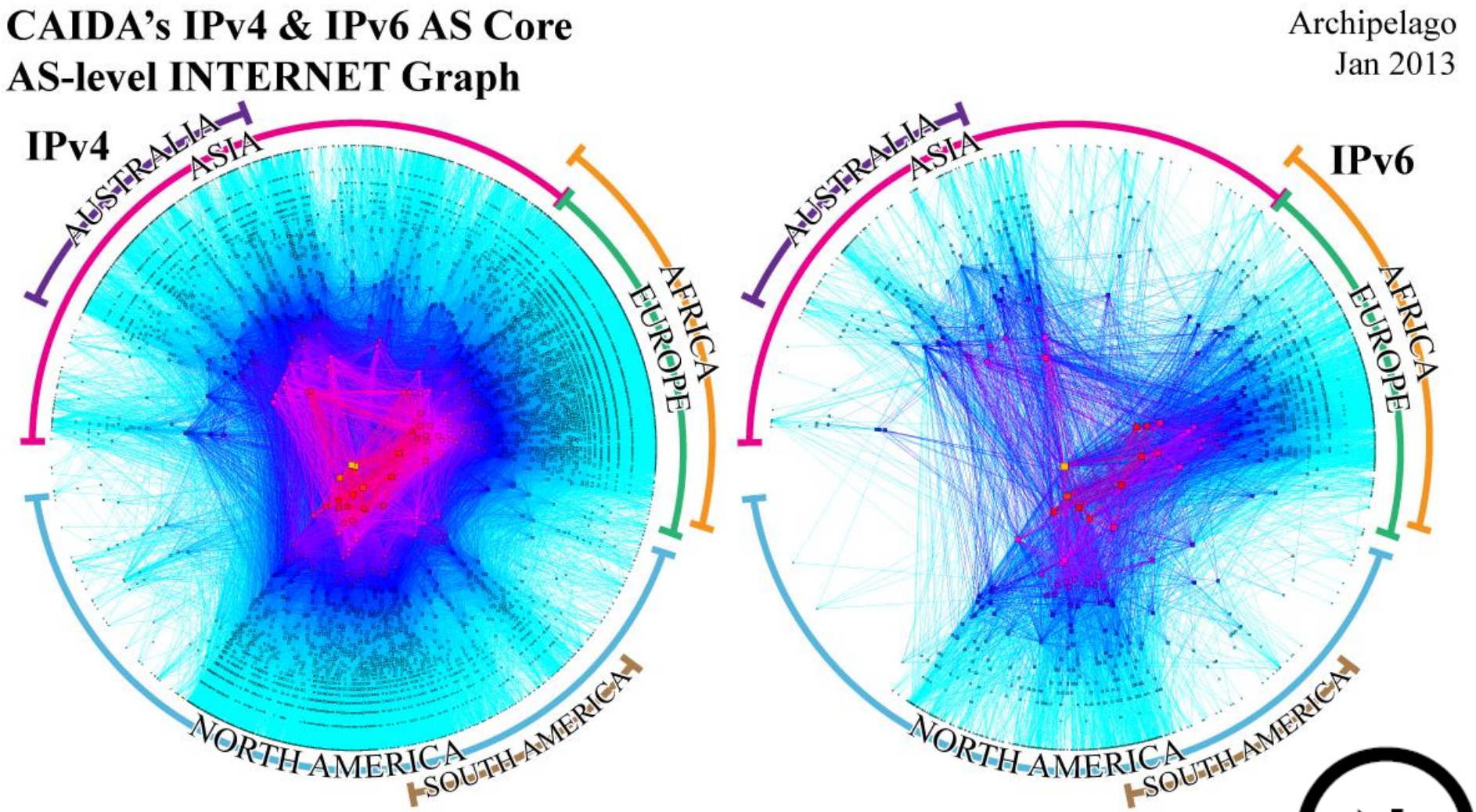


그림 출처:http://arstechnica.com/security/2013/04/can-a-ddos-break-the-internet-sure-just-not-all-of-it/

세상이 평평하지 않다는 증거



앞에서 안 하고 넘어온 이야기
상대의 MAC 주소는 어떻게 알 수 있나?

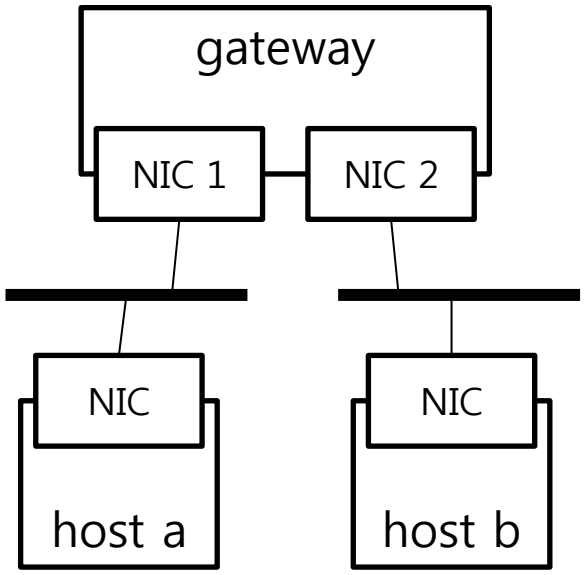
↓

내가 접속하려는 컴퓨터(의 네트워크 연결 장치)

↓

전 세계 어디로든 연결
하려면 IP 주소가 필요
(IP 주소 = 위치 + ID)

?



ARP 요청

브로드캐스트 주소	"IP 주소 X.X.X.X는 누구에요?"

ARP 응답

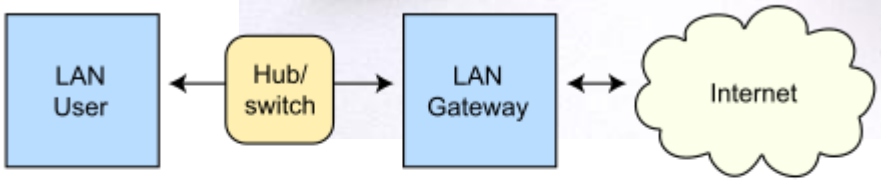
상대의 MAC 주소	"IX.X.X.X의 MAC 주소는 YY:YY:YY:YY:YY:YY 입니다"

ARP의 명과 암

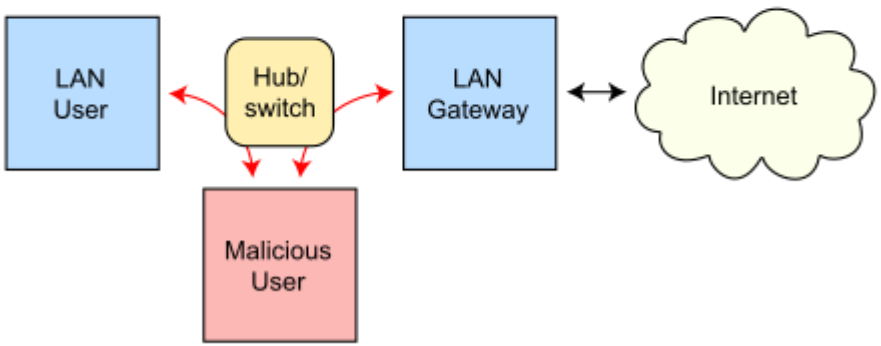
- Man-in-the-middle attack
- Denial of service attack

+ IP 통제

Routing under normal operation



Routing subject to ARP cache poisoning



MAC 패킷

상대의 MAC 주소	보내려는 데이터

같은 버스에서만

IP 패킷

상대의 IP 주소	보내려는 데이터

인터넷 전체

하지만...

패킷을 보내고 받는 양자는 **연결**되어 있어야 한다 → 항상 MAC 패킷으로 보내야

MAC의 탈을 쓴 IP

상대의 MAC 주소	상대의 IP 주소	보내려는 데이터

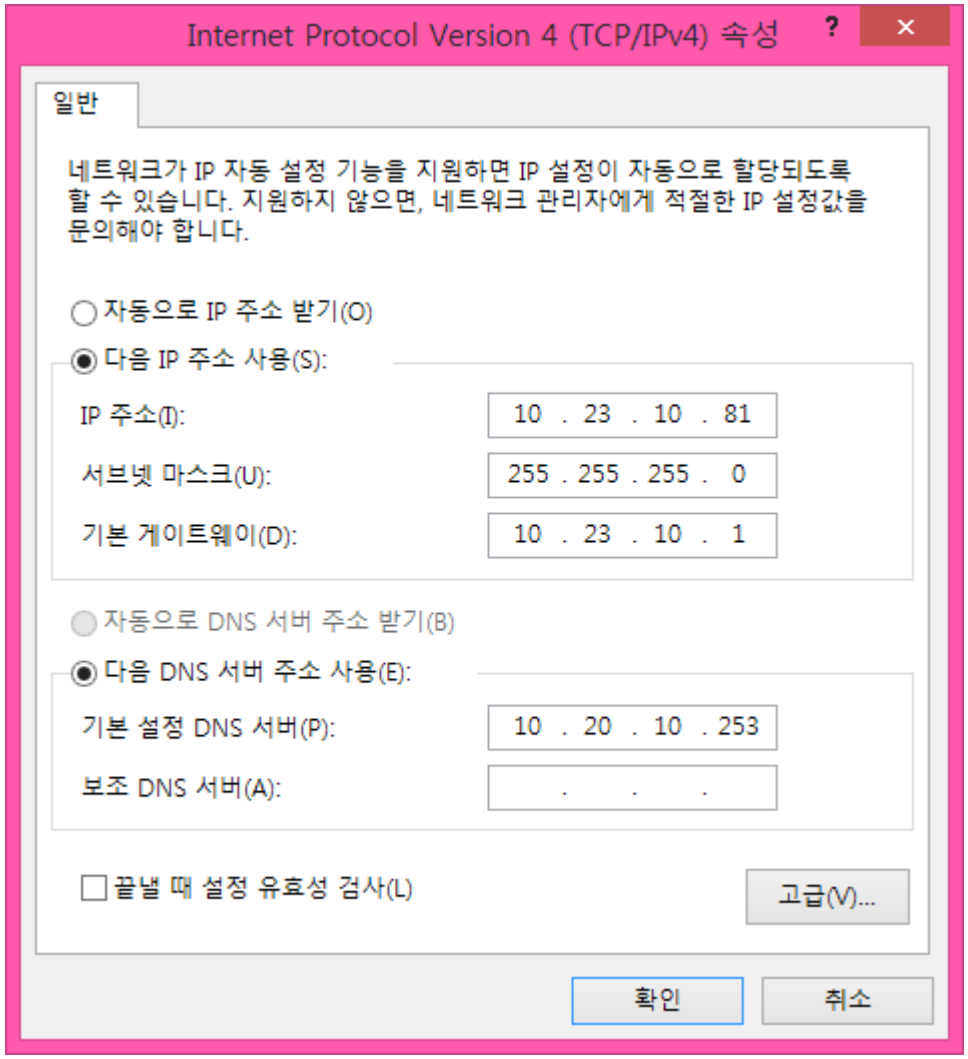
IP 패킷이 생각하는 내용물

MAC 패킷이 생각하는 내용물 = IP 패킷

+ ARP

같은 네트워크에 연결된
컴퓨터의 IP 주소를 알면
MAC 주소를 안다
→ 데이터를 보낼 수 있다.

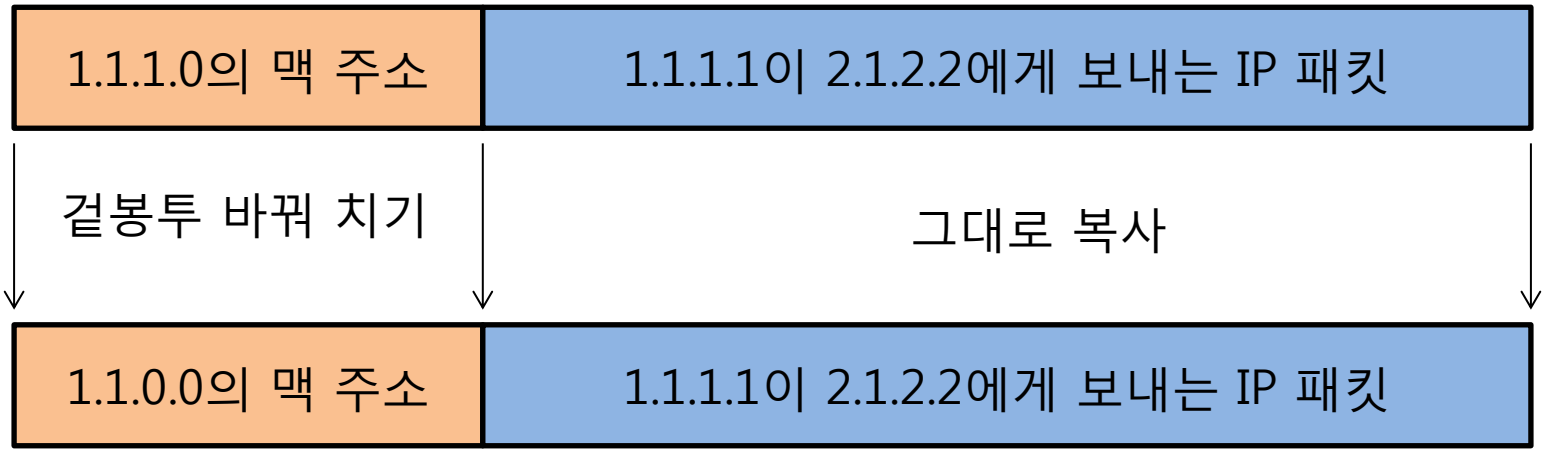
상대가 같은 네트워크면 그냥 데이터를 보내면 되고 다른 네트워크면 네트워크를 연결하는 컴퓨터 즉, 게이트웨이에게 전달해달라고 부탁하면 된다.



같은지 다른지
어떻게 알지?
게이트웨이 주소는
어떻게 알지?

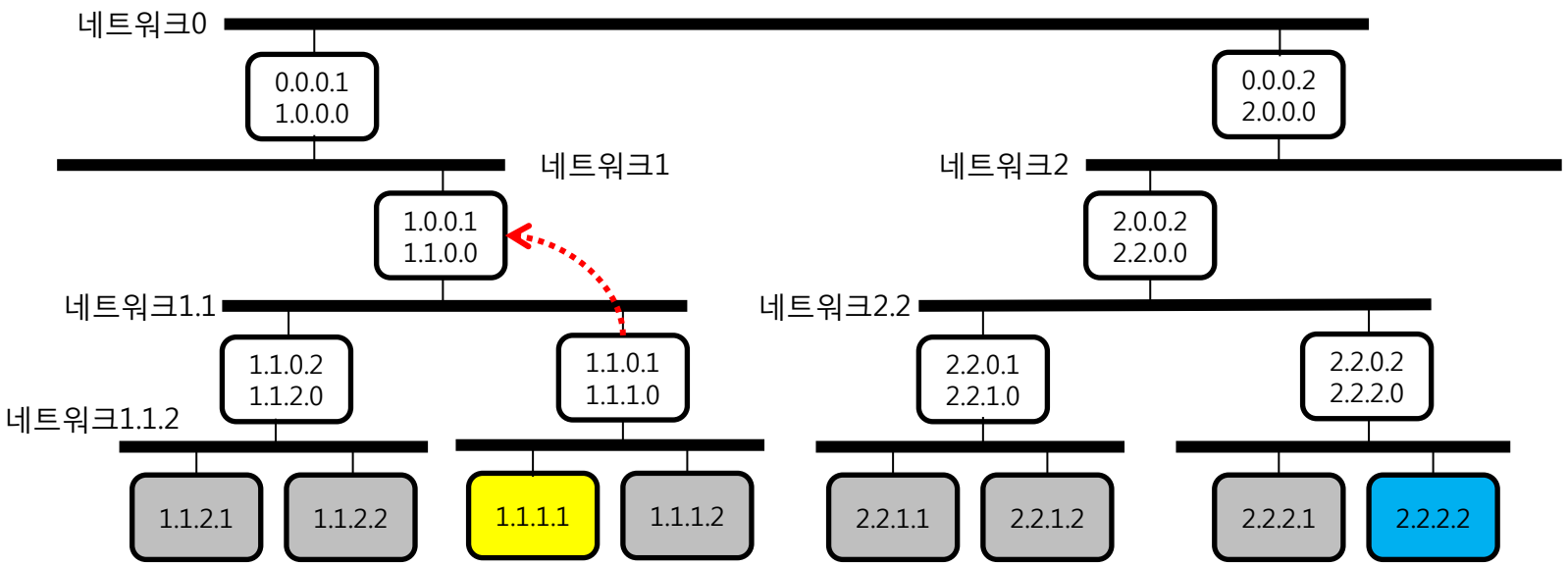
아는 방법 없다!
알려줄 수 밖에

게이트웨이 1.1.1.0이 받은 패킷



게이트웨이 1.1.0.0에게 떠넘긴 패킷

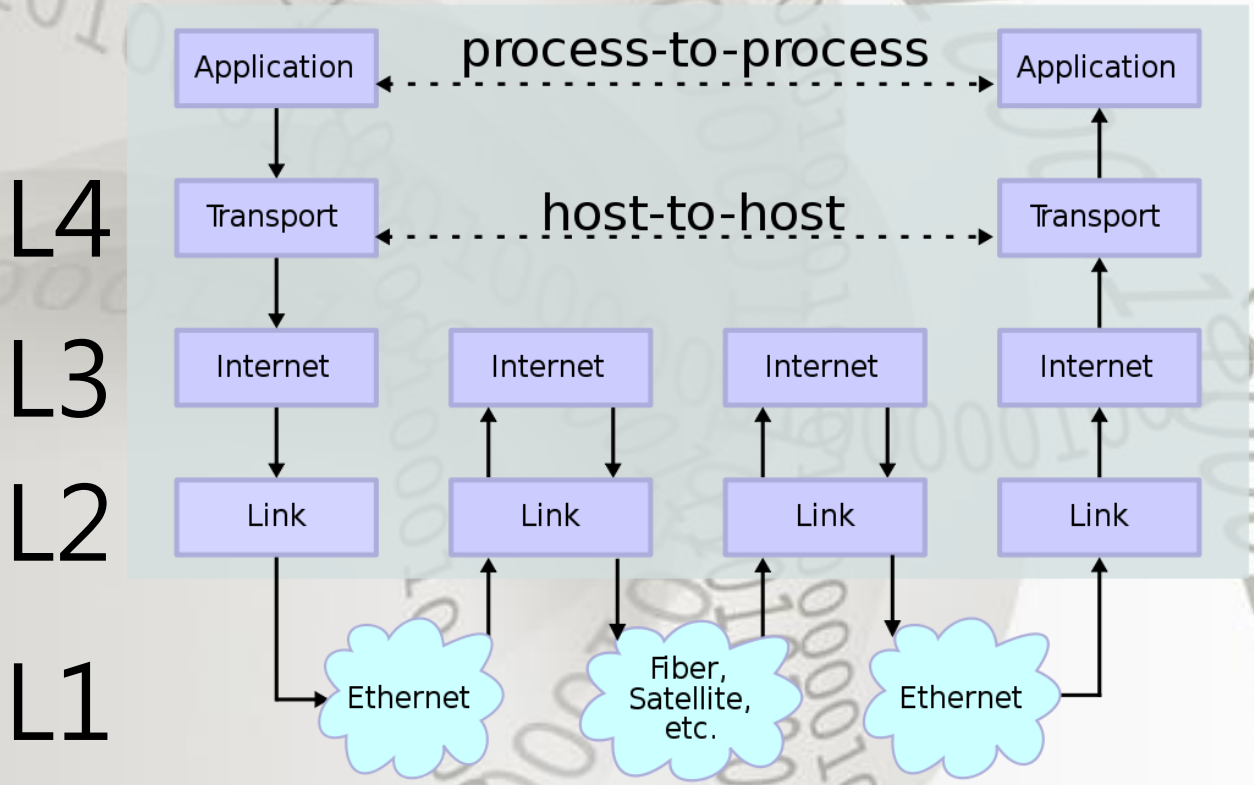
포대갈이



L2 + L3

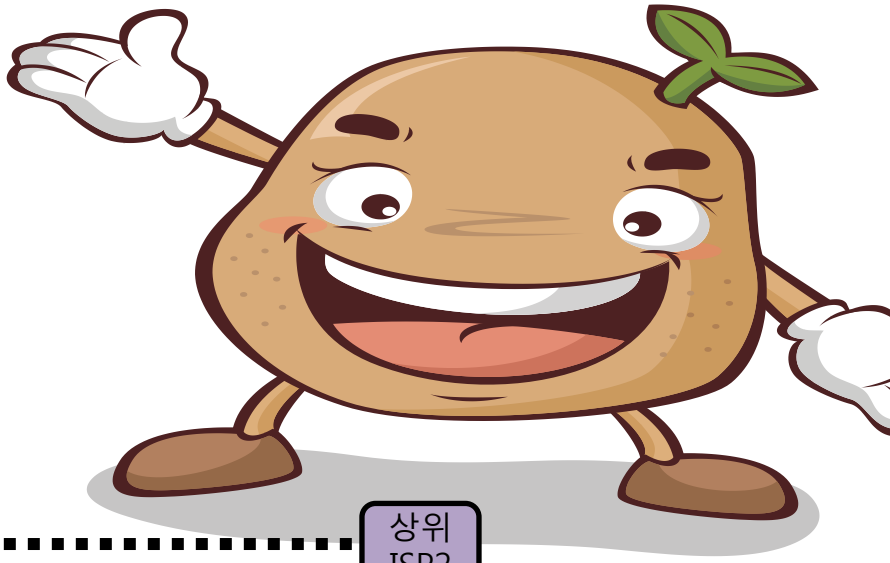
전세계 어느 컴퓨터로나
상대의 IP 주소를 알면
데이터를 보낼 수 있다.

Data Flow

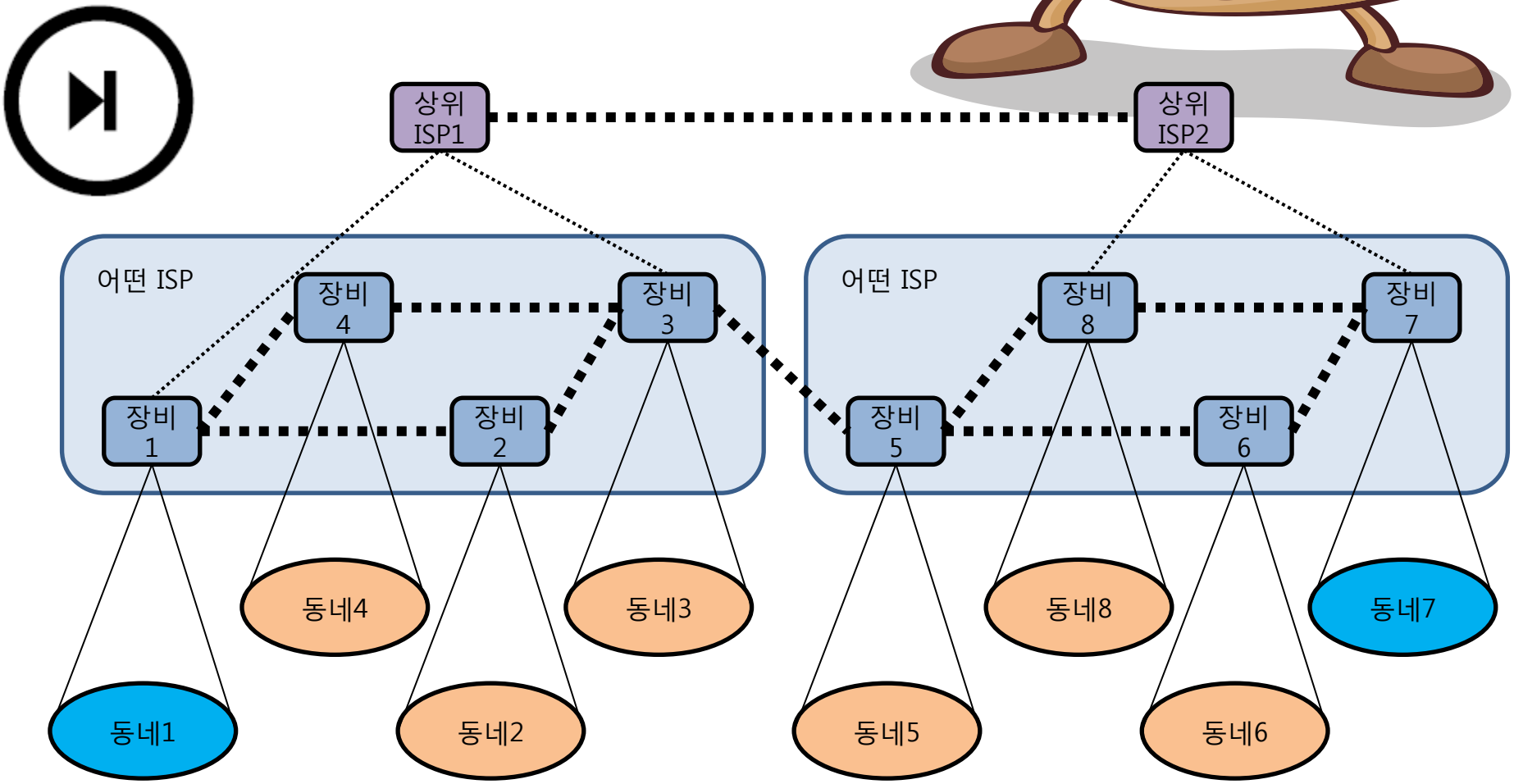


오르락 내리락

동네1 → 장비1 → 상위ISP1 → 상위ISP2 → 장비7 → 동네7
동네1 → 장비1 → 장비2 → 장비3 → 장비5 → 장비8 → 장비7 → 동네7



가는 길은 네트워크 장비의 설정에 따른다.
설정에는 이윤을 최대화하기 위한
여러 가지 요소가 고려된다.

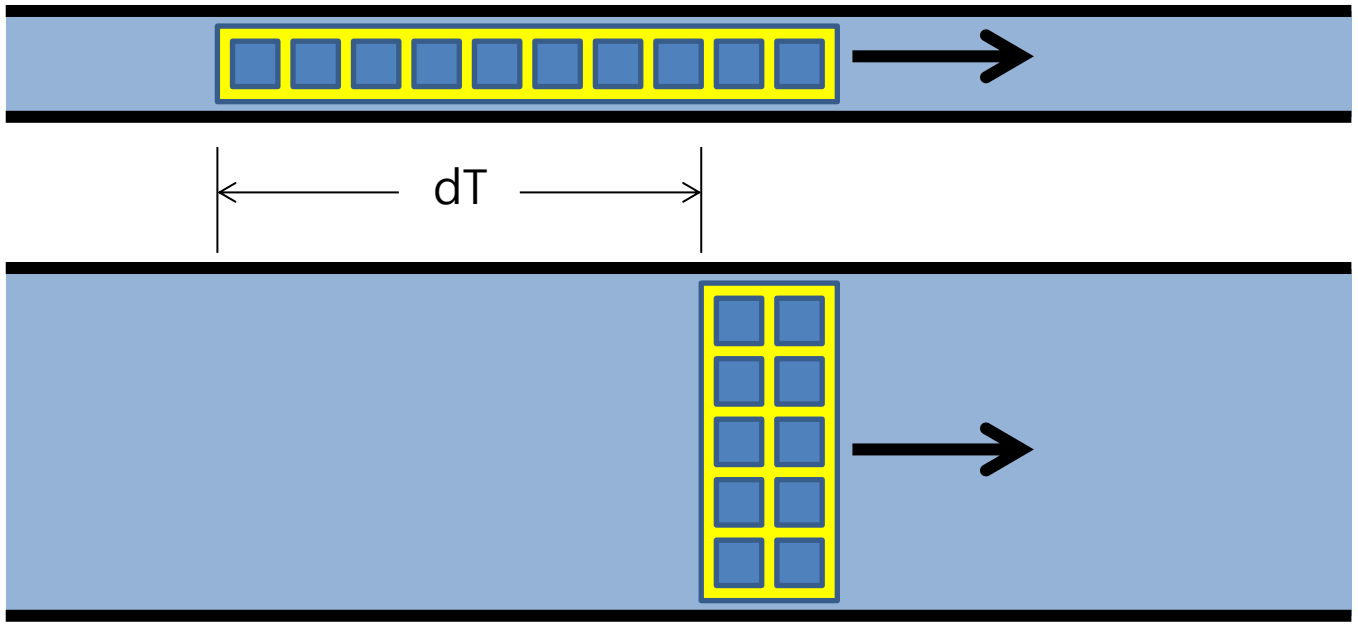


패킷의 전달 속도는 거의 같다. 다만 길이 넓어질 뿐

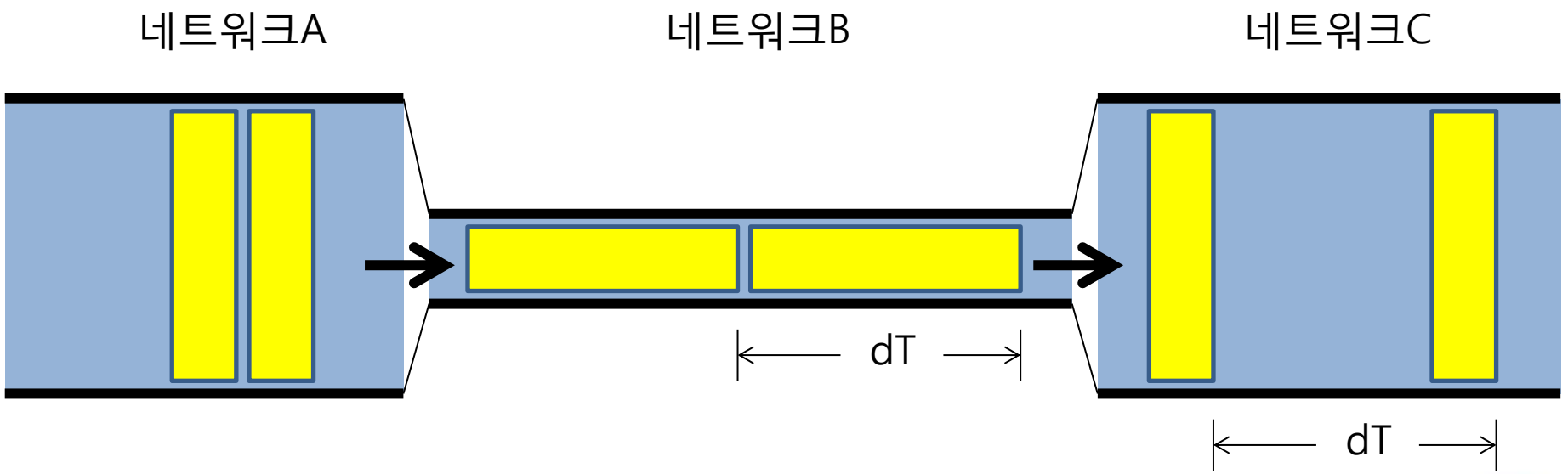
그림 출처:http://702story.blog.me

굵고 짧게 혹은 가늘고 길게

패킷 몇 개 보내서는 樂이 없다.



n개 연달아 보내면 n x dT 만큼 짧아진다!



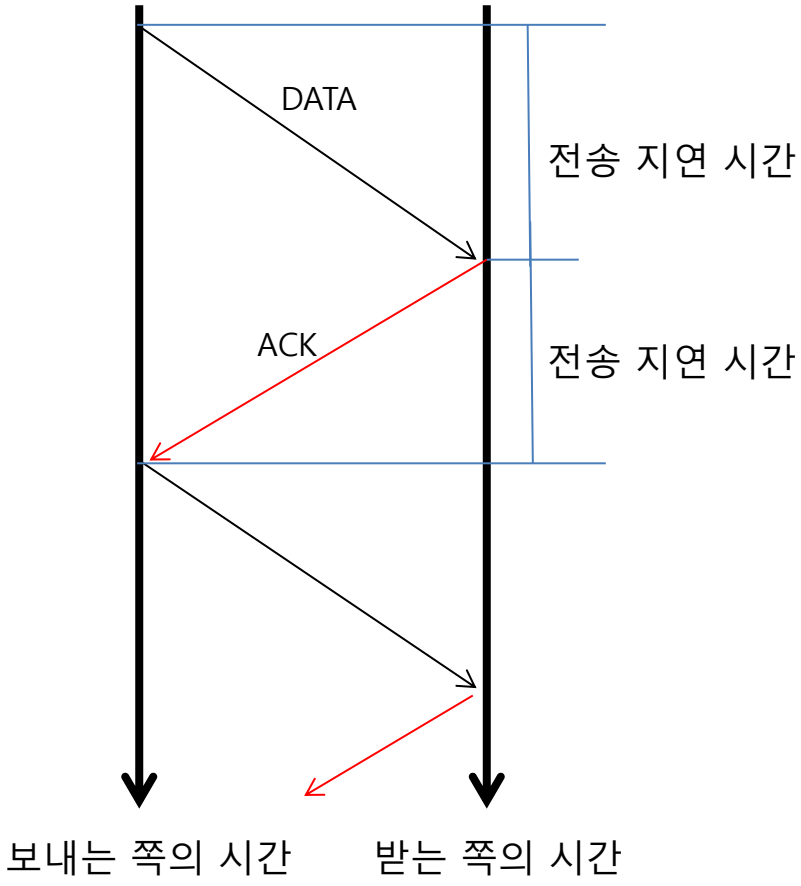
연달아 보낸 것이 무색하다.

그리고 패킷이 **손실** 될 수도...

그림 출처: http://dorrys.com/chain-strong-link/

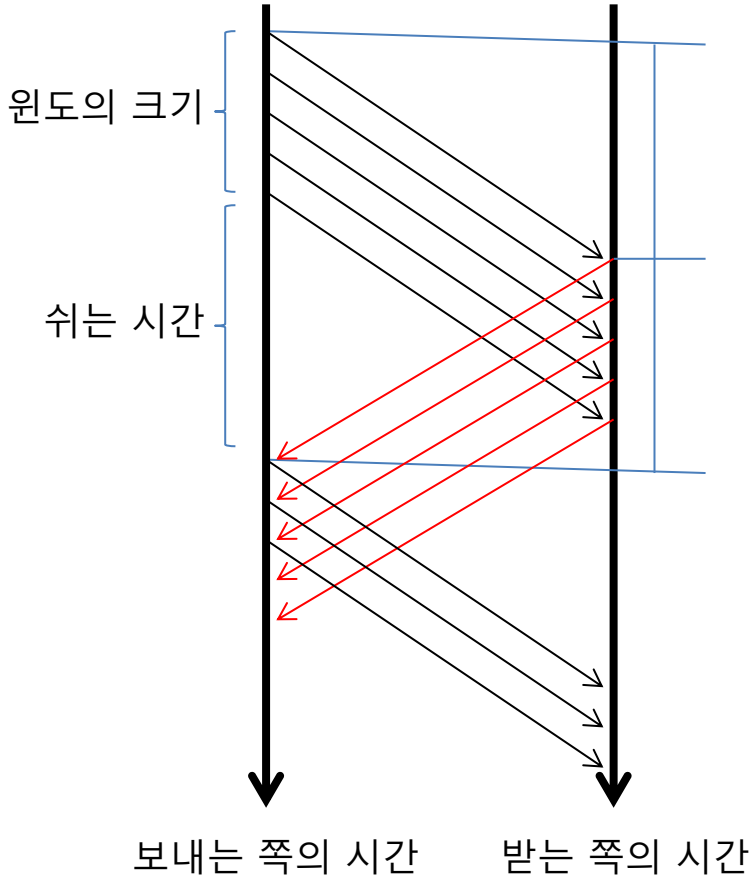
순진한 ARQ

전달을 확인할 수 있지만 연달아 보낼 수 없다.
패킷 손실을 확인하는데 오래 걸린다.



윈도 개념 적용

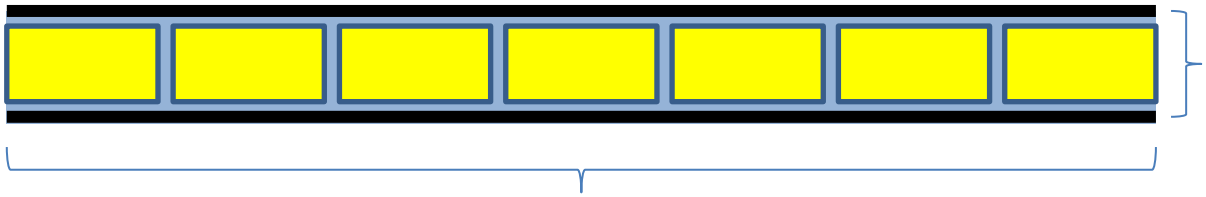
답이 안 와도 몇 개는 믿고 보내자.
패킷 손실도 더 빨리 알 수 있다. 왜?

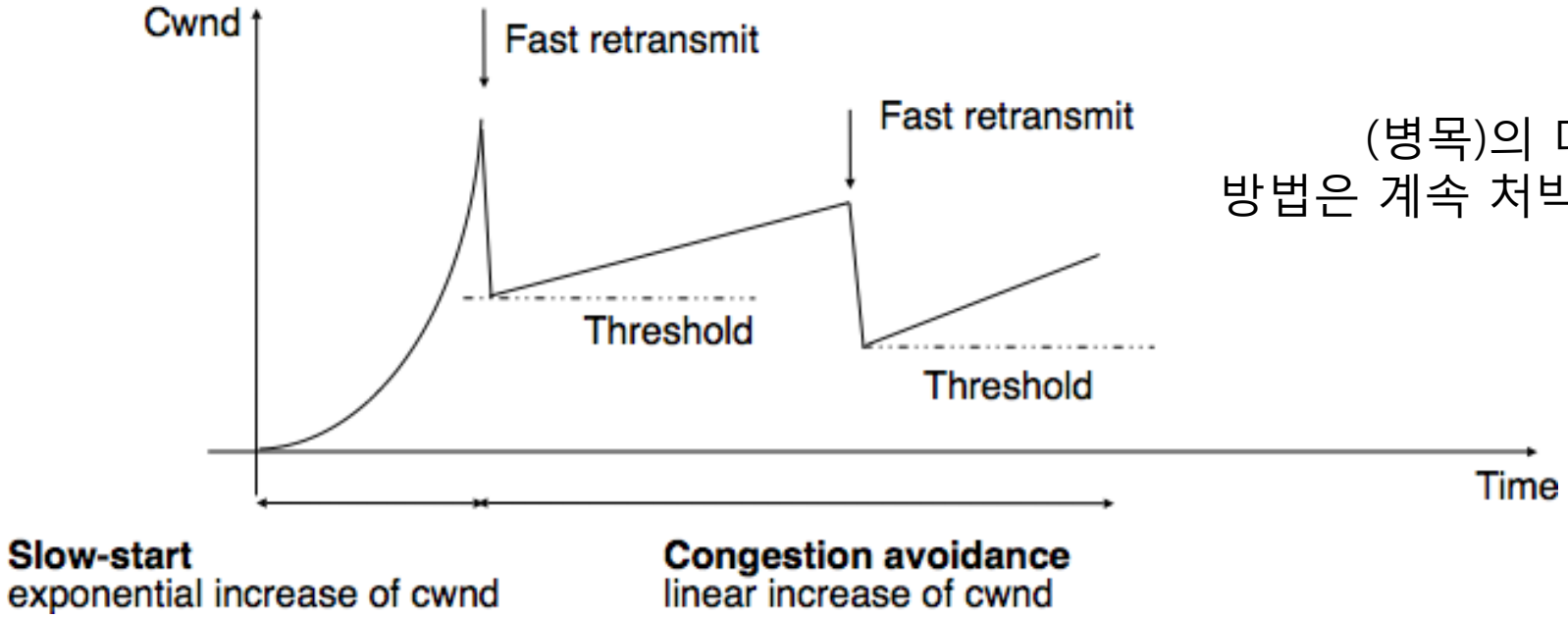


전송 계층 프로토콜의 목표는

Bandwidth x Delay

만큼의 패킷을 네트워크에 흐르게 하는 것!





(병목)의 대역을 아는 방법은 계속 처박는 수 밖에
→ AIMD

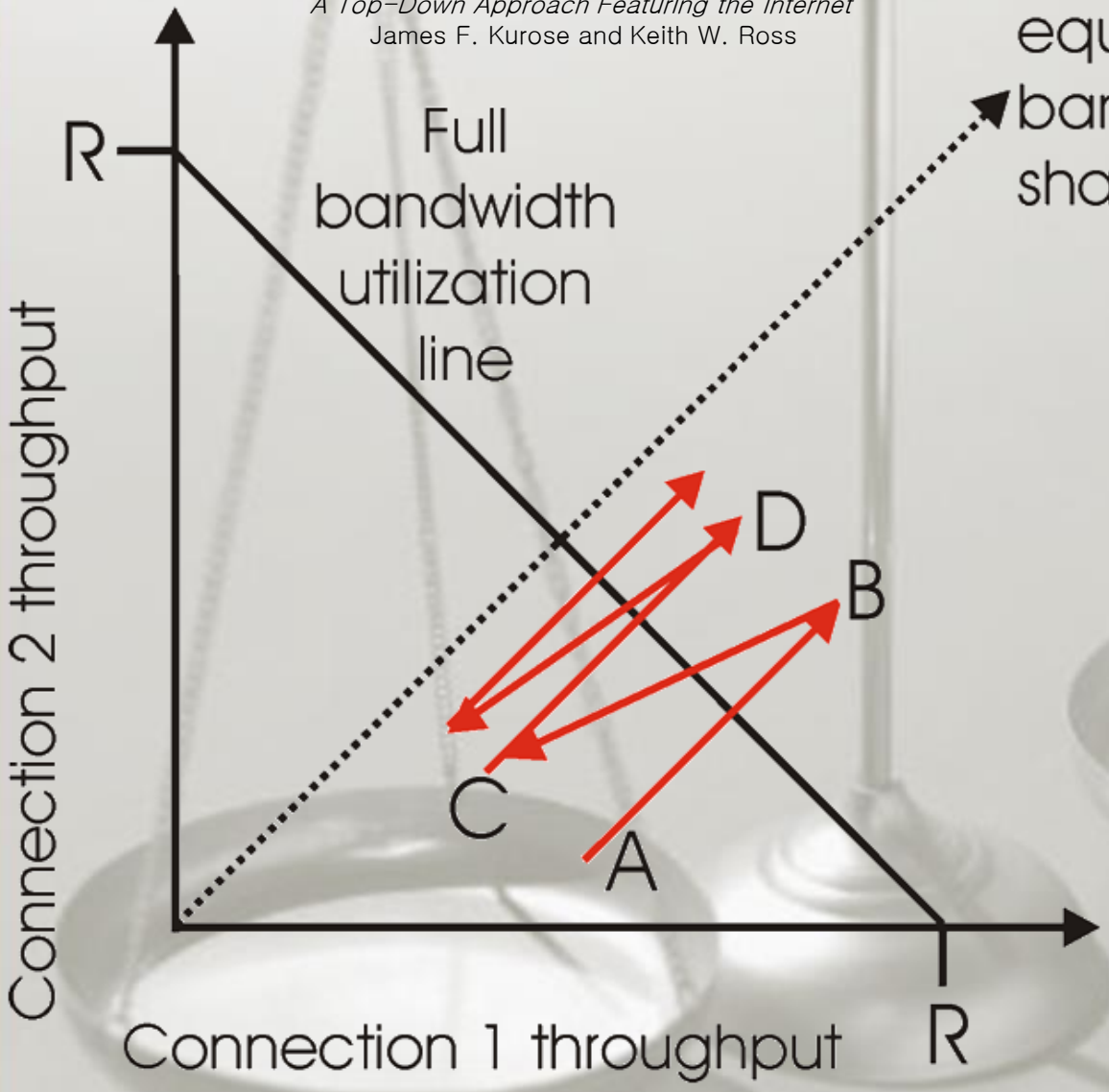
그림 출처: http://cnp3book.info.ucl.ac.be/transport/tcp/

TCP or L4

전세계 어느 컴퓨터로나
데이터를 빨리 그리고
깨지지 않게 보낼 수 있다.

Computer Networking
A Top-Down Approach Featuring the Internet
James F. Kurose and Keith W. Ross

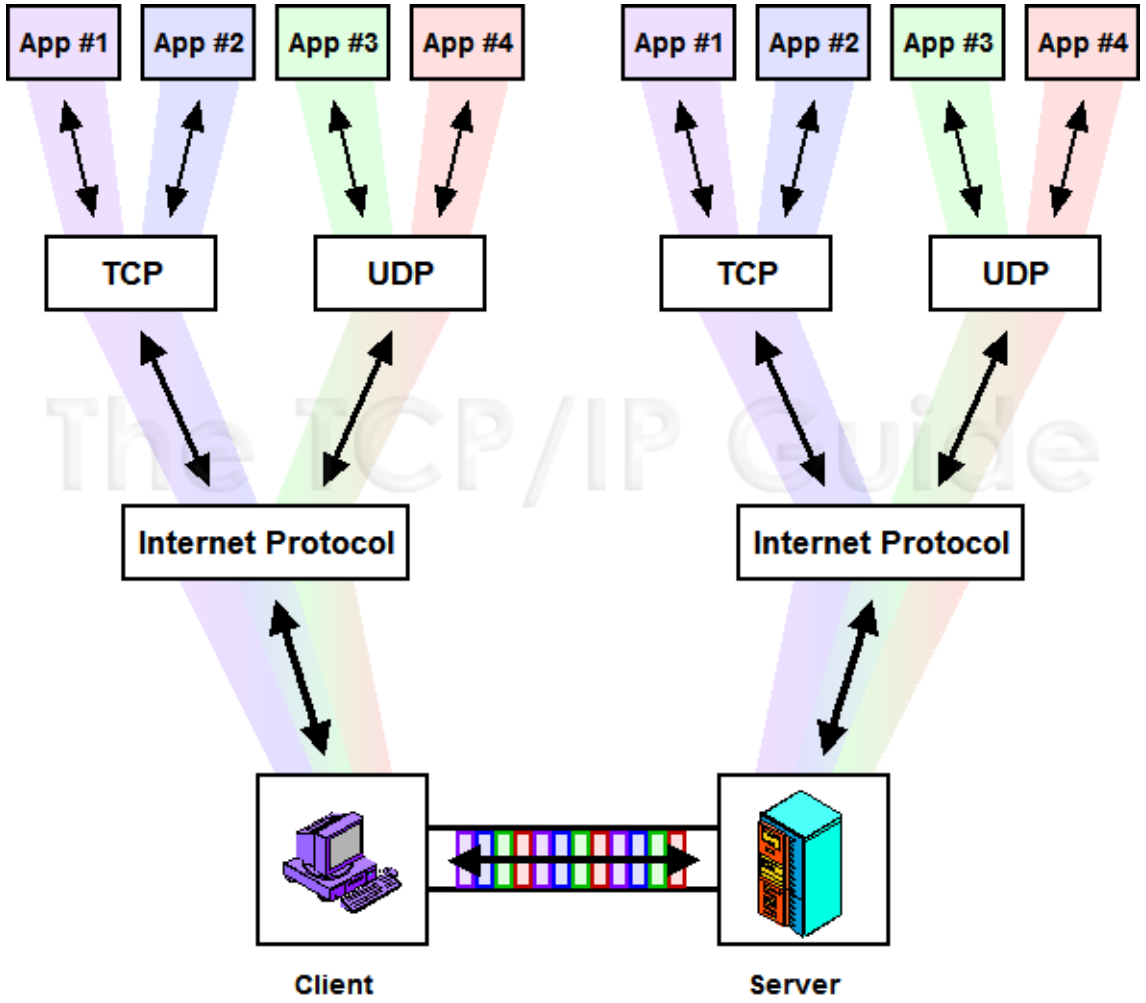
밥 칸 & 빈트 서프(1974)
NCP를 싹 엎어서 TCP를 제안함



tail drop vs.
random early drop vs.
any others

네트워크에서의 **의도적 간섭**은
언제 얼마나 허용되어야 하는가?

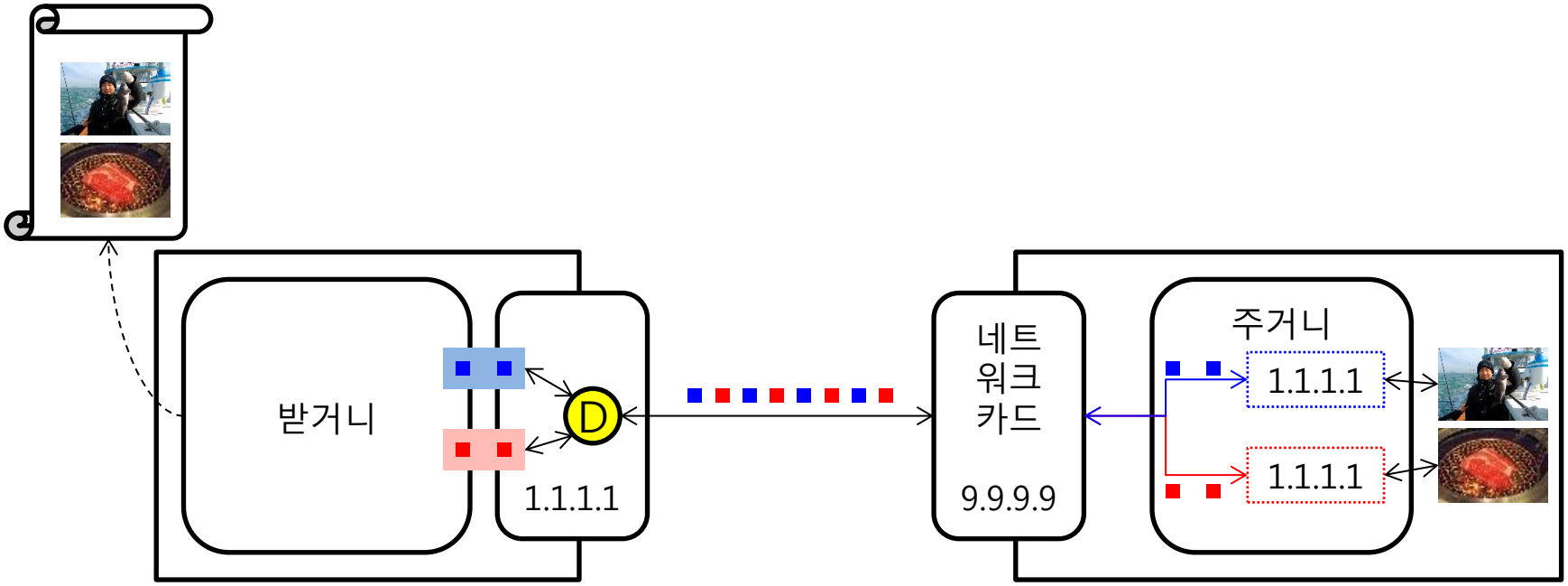
그림 출처: http://www.tcpipguide.com/free/t_TCPIPProcessesMultiplexingandClientServerApplicati-2.htm



ports

공존을 허용하는 비밀 병기

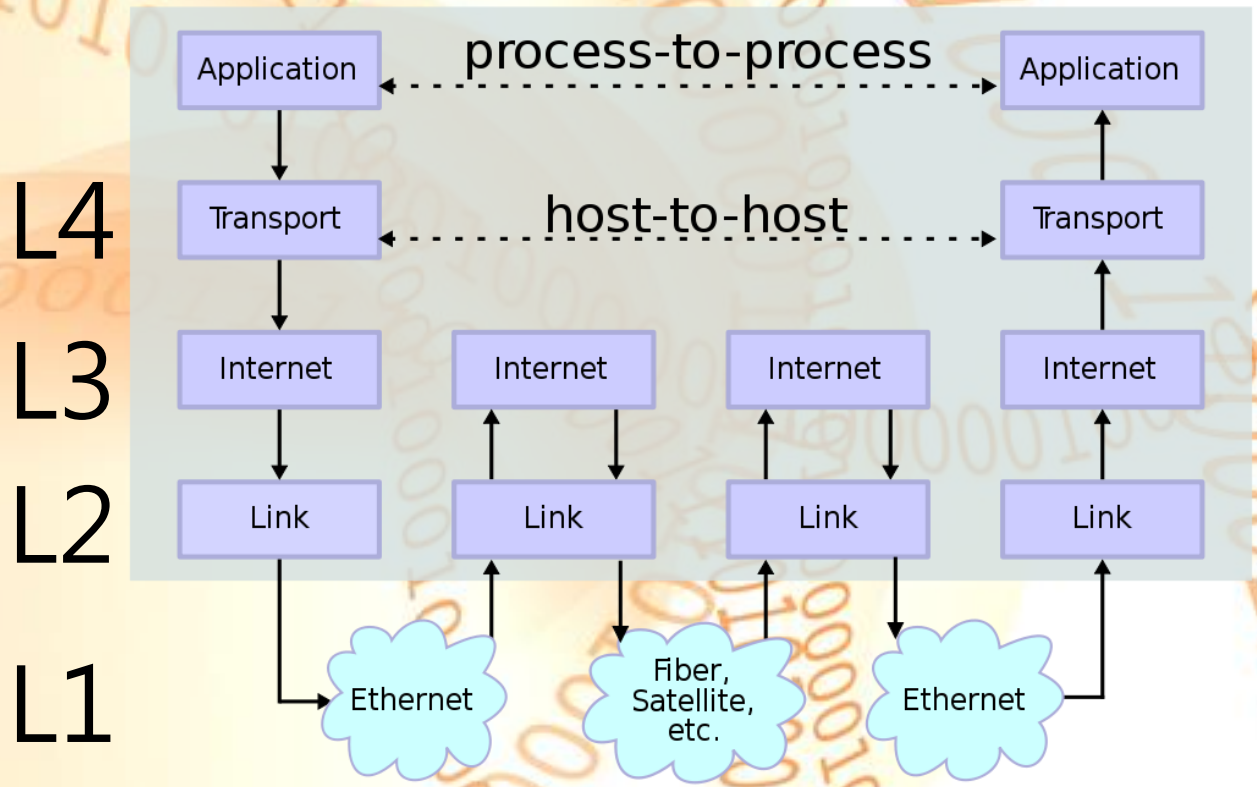
(src ip, src port, dest ip, dest port)


받거니
D
1.1.1.1
네트
워크
카드
9.9.9.9
주거니
1.1.1.1
1.1.1.1

+ port

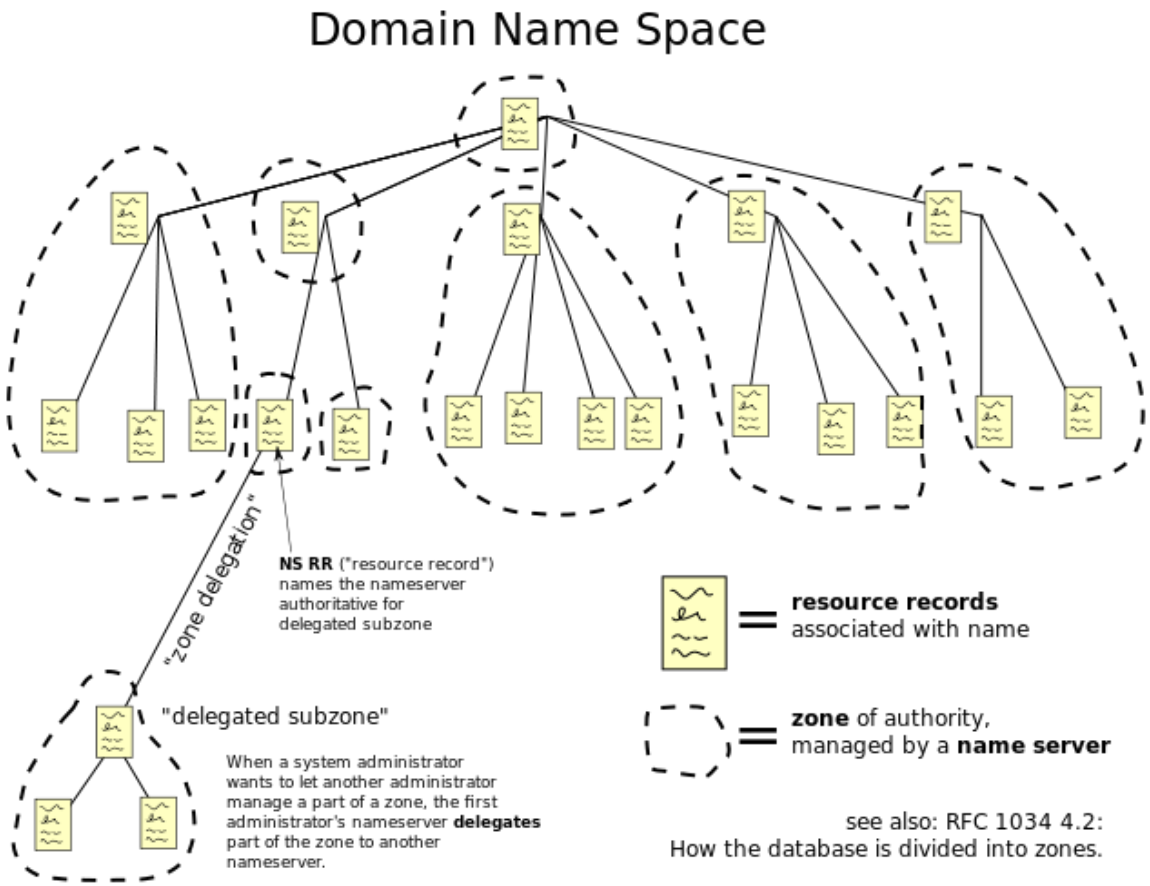
여러 대의 컴퓨터에서
여러 개의 응용 프로그램이
동시에 서로 통신을 해도
꼬이지 않는다.

Data Flow

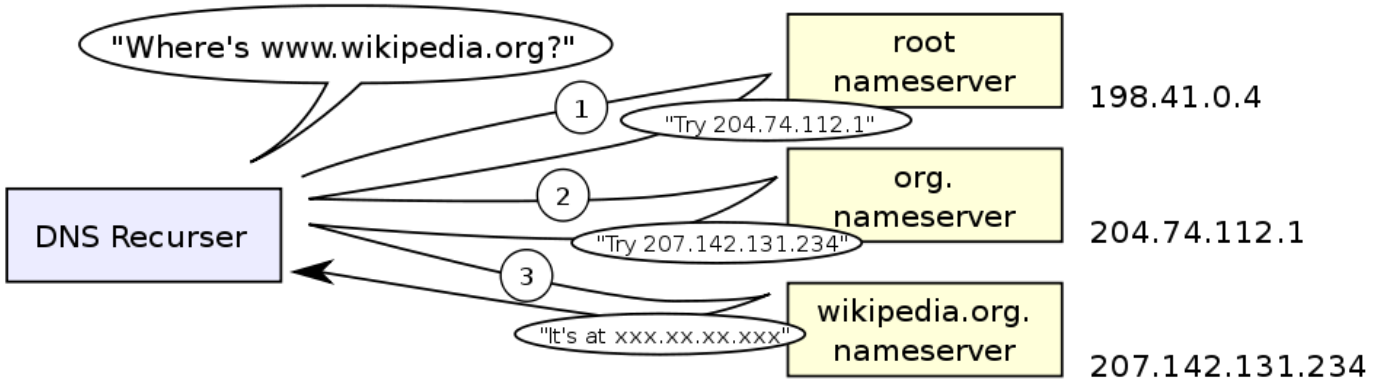


L4는 e2e

폴 모카페트리스(1983)
hosts 파일 관리를 분산 시키자.



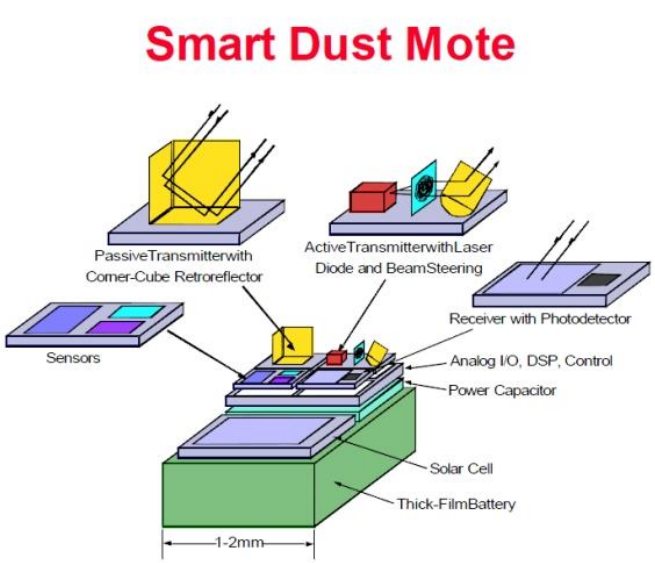
HOSTS.TXT



+ DNS

상대방의 IP 주소 대신
이름을 알면 통신을
할 수 있게 되었다.

zeroconf



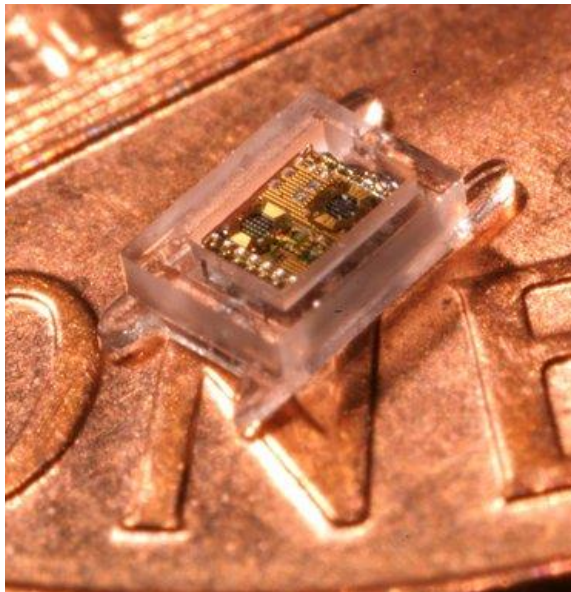
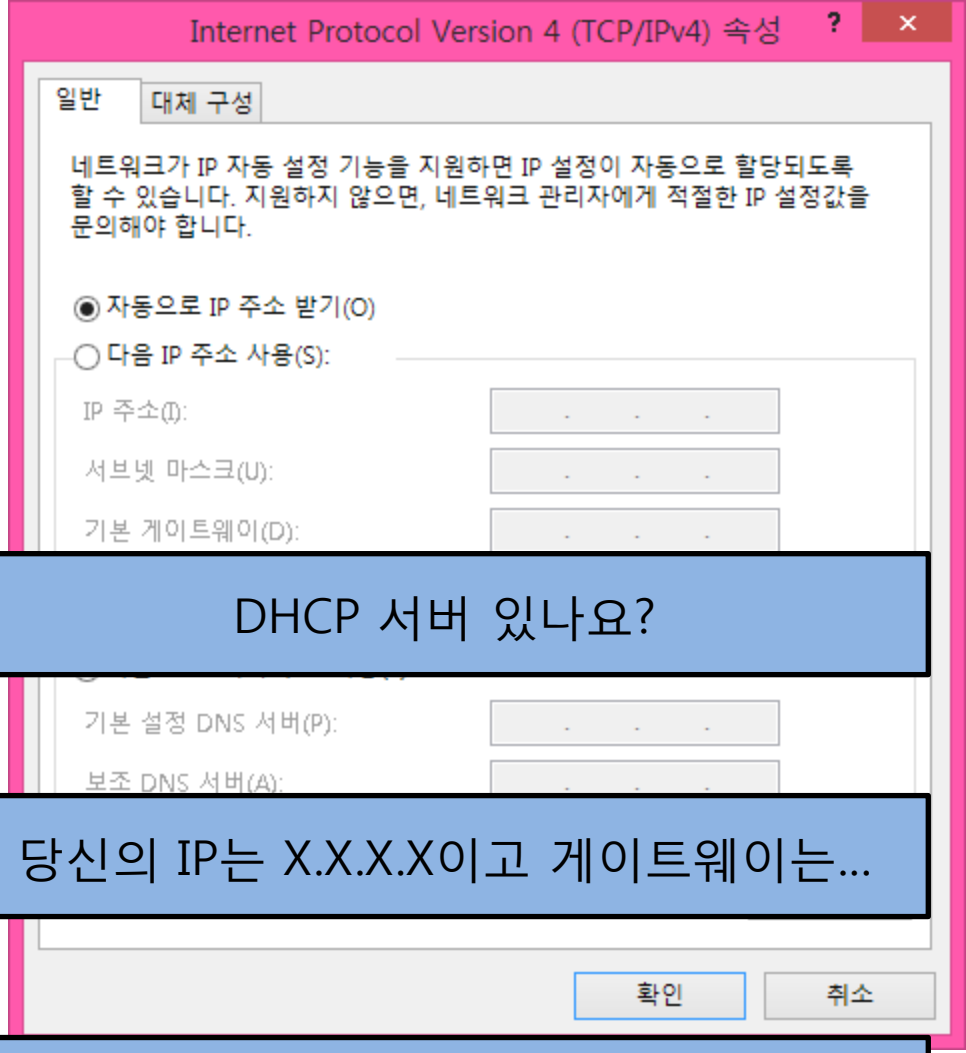


그림 출처: http://inteldigitalreport.com

그림 출처: http://binarydissent.com

DHCP



DHCP 발견

브로드캐스트 주소	궁금이의 맥 주소	DHCP 서버 있나요?

DHCP 제시

브로드캐스트 주소	궁금이의 맥 주소	당신의 IP는 X.X.X.X이고 게이트웨이는...

DHCP 요청

브로드캐스트 주소	궁금이의 맥 주소	알려주신 IP 주소 등 설정 정보 쓸래요

DHCP 확인

브로드캐스트 주소	궁금이의 맥 주소	그러세요


정보 보안 입문

가용성

기밀성

무결성

Confidentiality

- 기밀성, 비밀성
- 허가되지 않은 자에게 정보가 노출되는 것을 막는 것
- 암호화

무결성

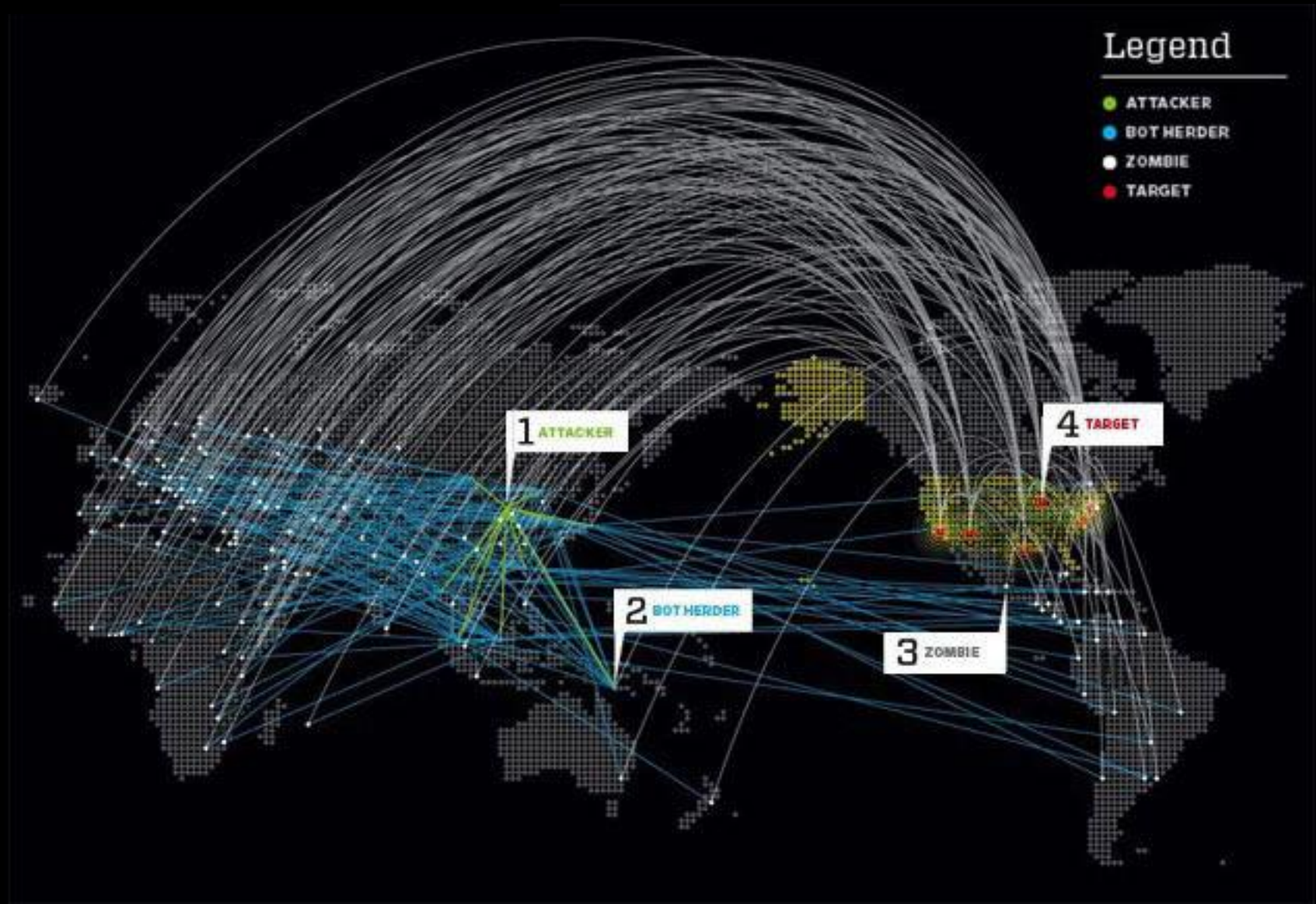
자료의
정확성과
일관성을
보장하는 것

Availability(가용성)

필요할 때 사용할 수 있도록 하는 것

vs. DDoS 공격

디도스 공격의 꼴


Legend
ATTACKER
BOT HERDER
ZOMBIE
TARGET
1 ATTACKER
2 BOT HERDER
3 ZOMBIE
4 TARGET

http://www.ibk.co.kr/X

보안프로그램 설치

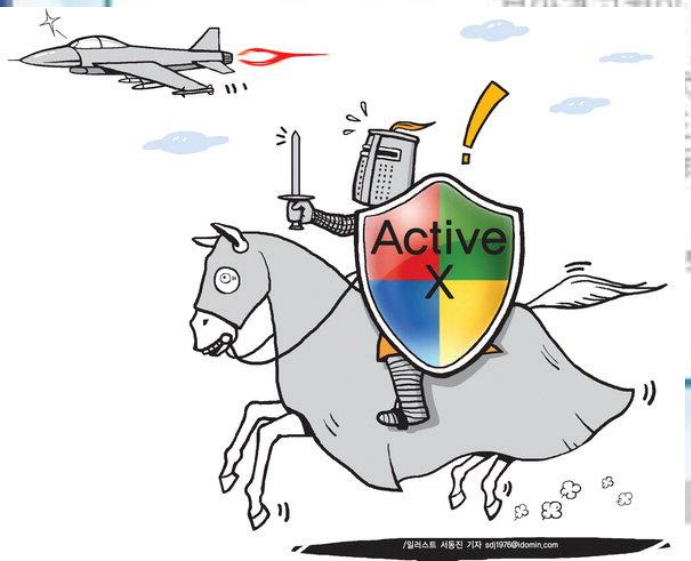
보안 프로그램 확인중

잠시만 기다려주세요

안전한 금융거래를 위해 보안 프로그램 확인중입니다

최초 접속하신 고객님께서는 PC환경에 따라 10초에서 최대 3분까지 소요될 수 있습니다.
나오면 반드시 "예"를 선택하여 주시기 바랍니다.
보이면 보안 프로그램 다운받기를 클릭 하십시오.
이 화면이 계속 보이면 여기를 클릭 하시어
" 하십시오.

보안 프로그램 다운받기



한국은 해커의 놀이터

Authenticity

진정성

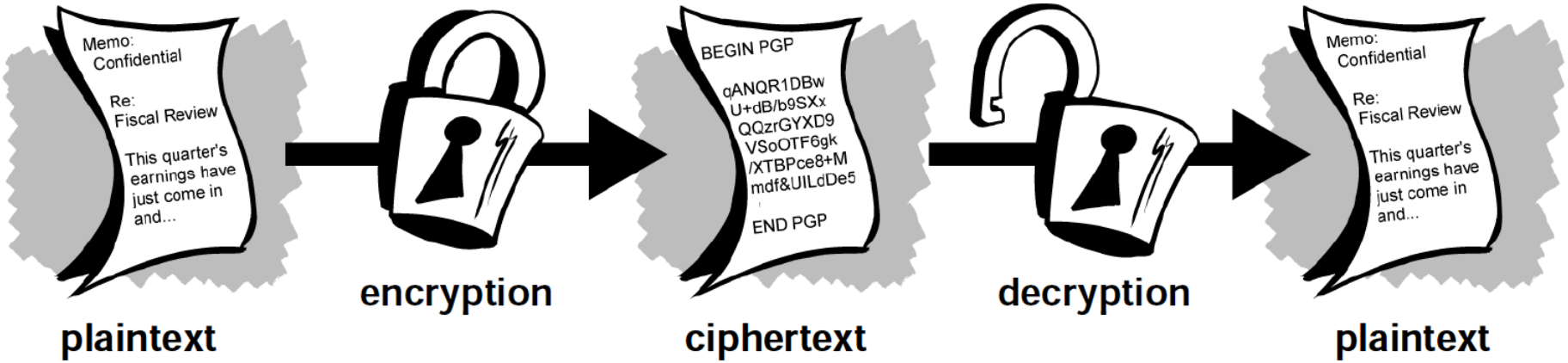
어떤 자료, 거래, 통신, 문서 등이 진짜라는 것을 보증하는 것 (예, 사인)

부인 방지

- Non-repudiation
- 거래의 일방이 그 거래가 있었다는 사실을 부인할 수 없게 하는 것
- 공인인증서를 이용한 은행 거래

HOW?

어떻게 보안을 해냄?



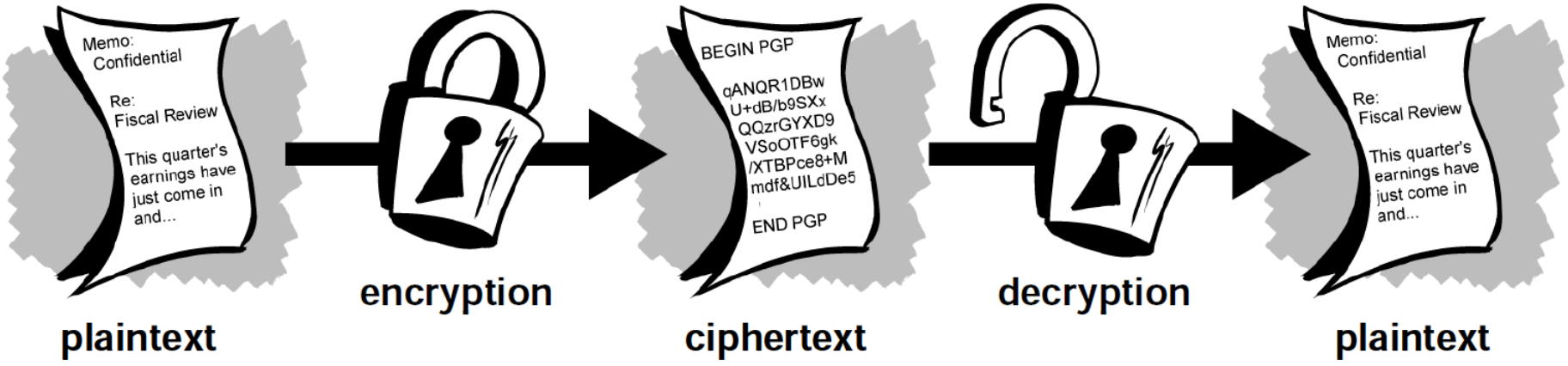
plaintext 평문

encryption 암호화

ciphertext 암호문

decryption 암호풀기

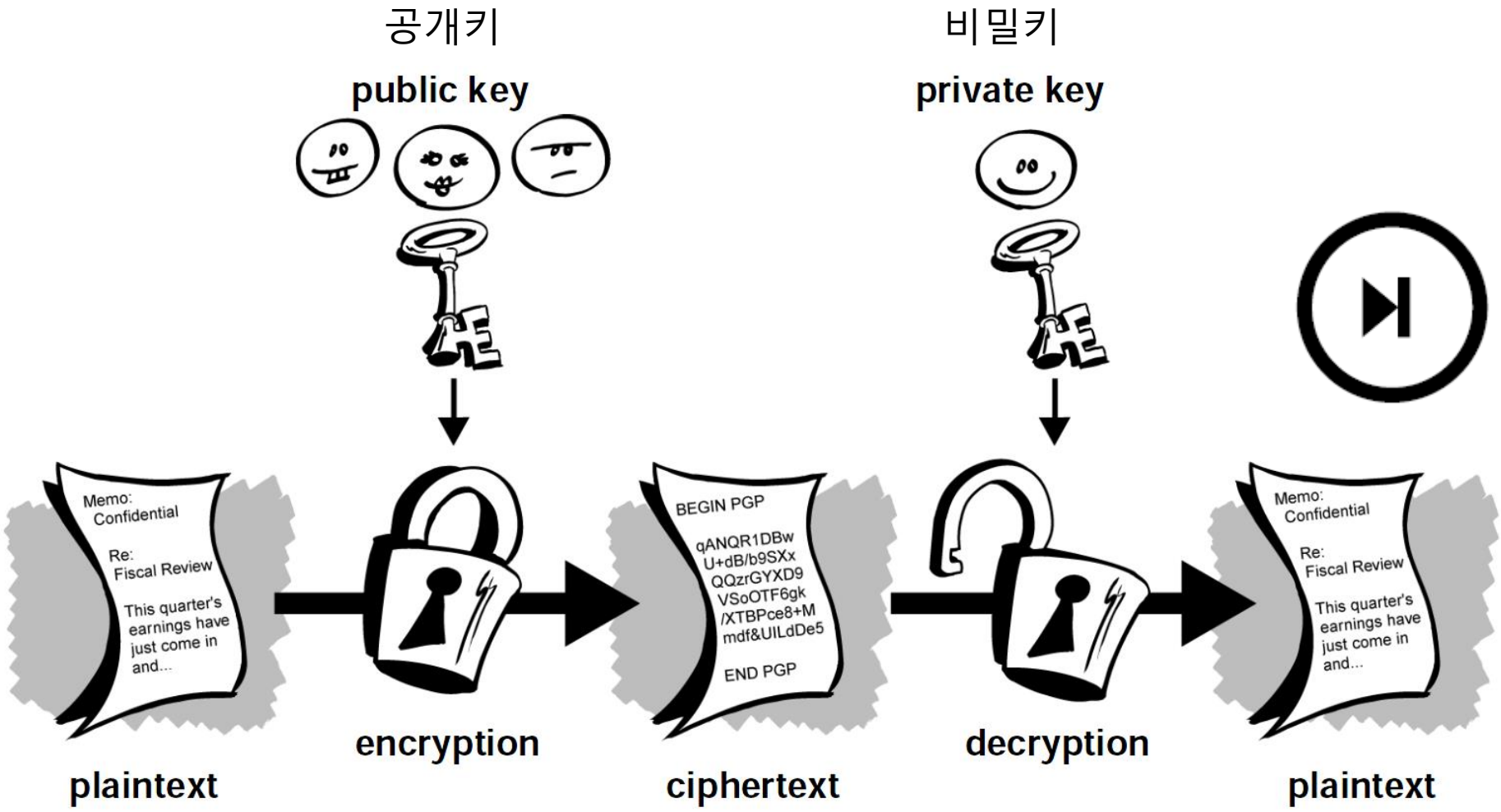
plaintext 평문



평문 암호화 암호문 암호풀기 평문

공유키 암호화 = 대칭키 암호화

공개키 암호화 = 비대칭키 암호화



공개키 암호화

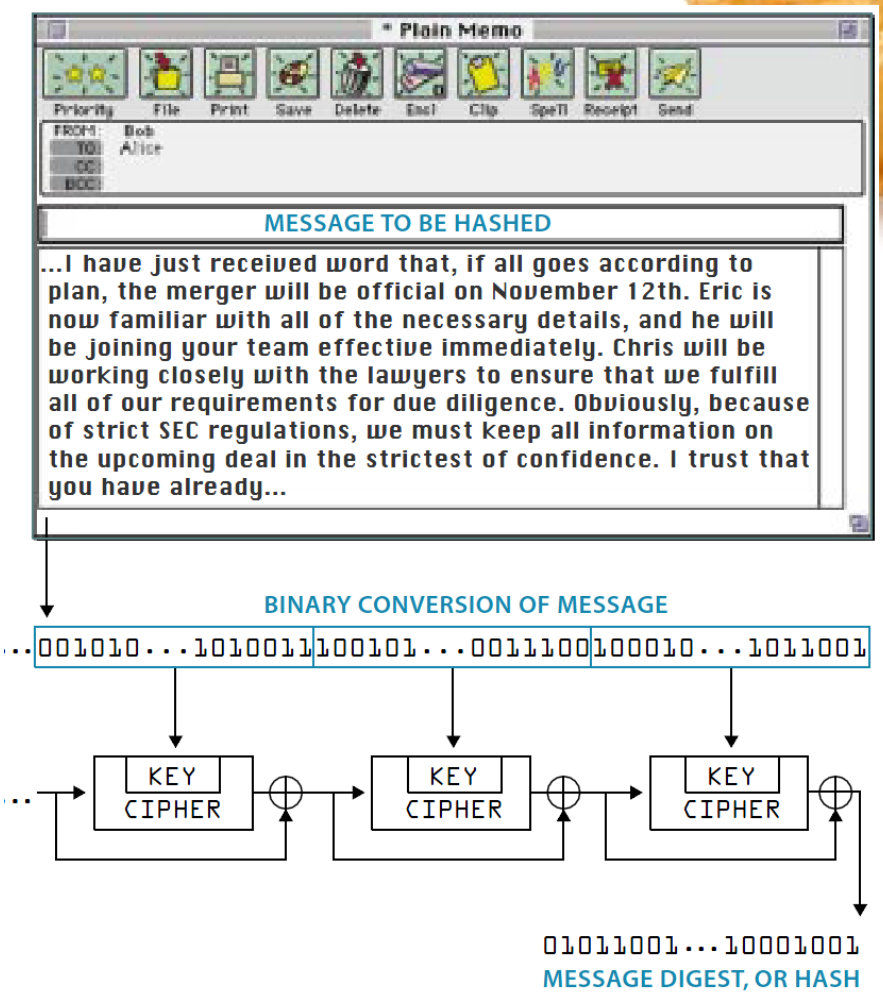
응용

Q1. 내가 내 비밀키로 어떤 문서를
암호화해서 게시판에 올린다면?

Q2. 누군가 내 공개키로 어떤 문서를
암호화해서 게시판에 올린다면?

Q3. 내 비밀키로 암호화한 문서를
누군가의 공개키로 암호화해서
게시판에 올린다면?

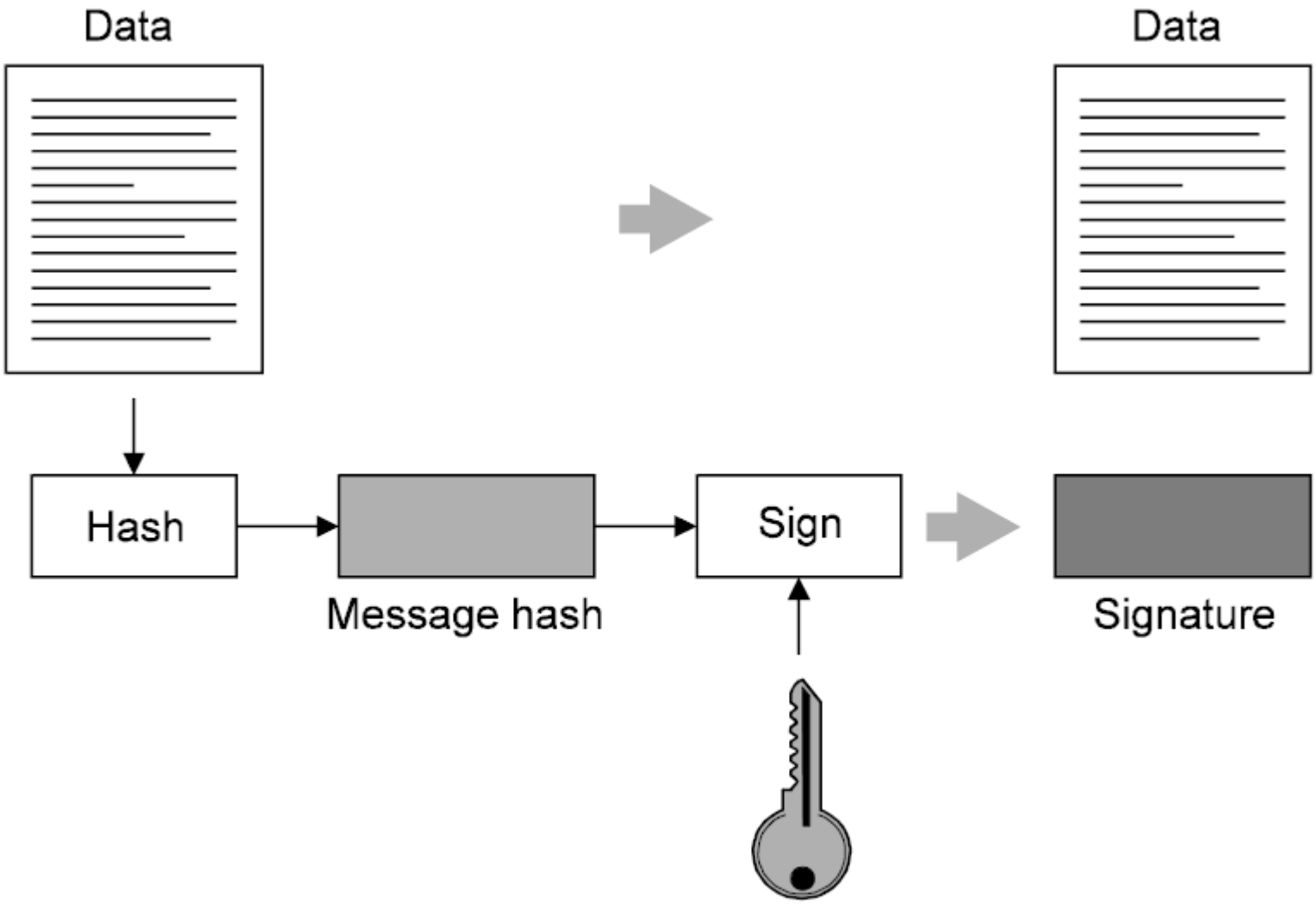
해시브라운



해시에서 원본 복구 불가!
원본이 같으면 해시는 같다.

응용

암호는 해시로 저장해라!
해시는 문서의 지문이다!


Data
Data
Hash
Message hash
Sign
Signature
Senders
private key

해시 + 비밀키 =

디지털 사인

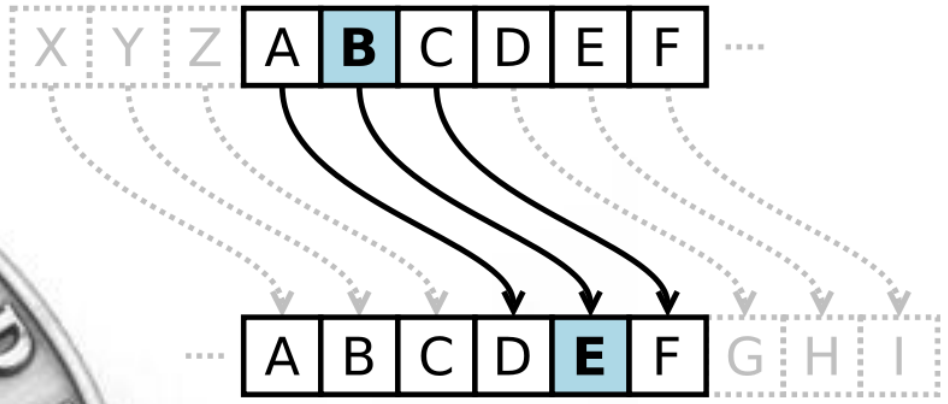
KEYS?

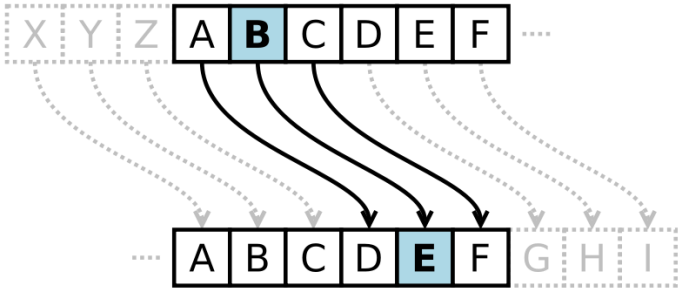
키를 이용한 암호화?


Sworn Fell

스키테일

로마 황제 줄리어스 시저의 암호





Q1. 이들 암호의 단점은?

바꿔 치기 기법

모든 알파벳을
각기 다른 규칙으로
바꿔 치기

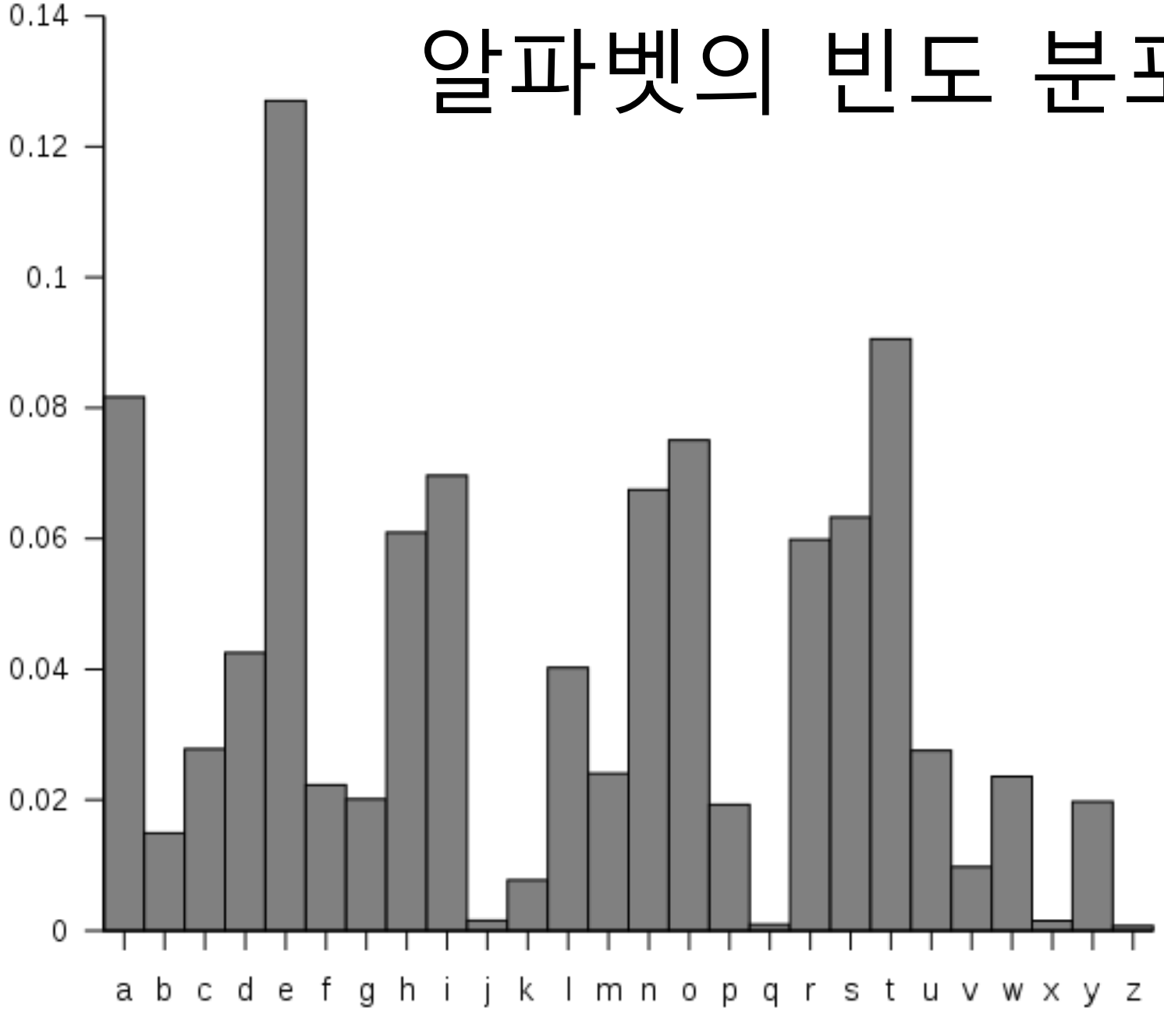
26 x 25 x 24 x … x 2 x 1 가지
그 중 하나를 내 KEY로 선택

GRAY FOX HAS ARRIVED
UKQN YGB IQL QKKOCTR

G	R	A	Y	공백
0 1 0 0 0 1 1 1	0 1 0 1 0 0 1 0	0 1 0 0 0 0 0 1	0 1 0 1 1 0 0 1	0 0 1 0 0

0 1 0 0 0 1 1 1 0 1 0	1 0 0 1 0 0 1 0 0 0 0	0 1 0 1 0 1 1 0 0 1 0	0 1 0 0

알파벳의 빈도 분포



자리 바꾸기 기법

스키테일의 부활

Message: JAMESBONDNEEDSBACKUP
Code: JEONDAUASNESCPMBDEBK

J	E	O	N	D	A	U
A	S	N	E	S	C	P
M	B	D	E	B	K	

공유키(대칭키) 암호화

- 바꿔 치기 기법과 자리 바꾸기 기법을 뒤섞어서 쉽게 풀지 못하게 만듬
- 내가 입력한 키는 각 기법에서 사용할 변환표를 선택하는 역할
- 키가 같으면 변환표가 같고 변환표를 반대로 적용하면 풀린다.

공개키 암호화

- 수학적 기초
  - 연산의 비대칭성
    - 예, 큰 소수 두 개를 찾아서 곱하기

      vs. 곱으로 나온 숫자를 소인수 분해 하기
    - 두 소수의 곱으로 된 129자리 숫자를 소인수분해 하는 데에는 1,600 대의 컴퓨터를 연결해서 8개월 걸림

RSA 공개키 알고리즘

p, q

$n = pq \qquad \phi(n) = (p-1)(q-1)$

$e, \qquad 1 < e < \phi(n) \qquad \gcd(e, \phi(n)) = 1$

$d = e^{-1} \bmod \phi(n)$

$C = M^e \bmod n$

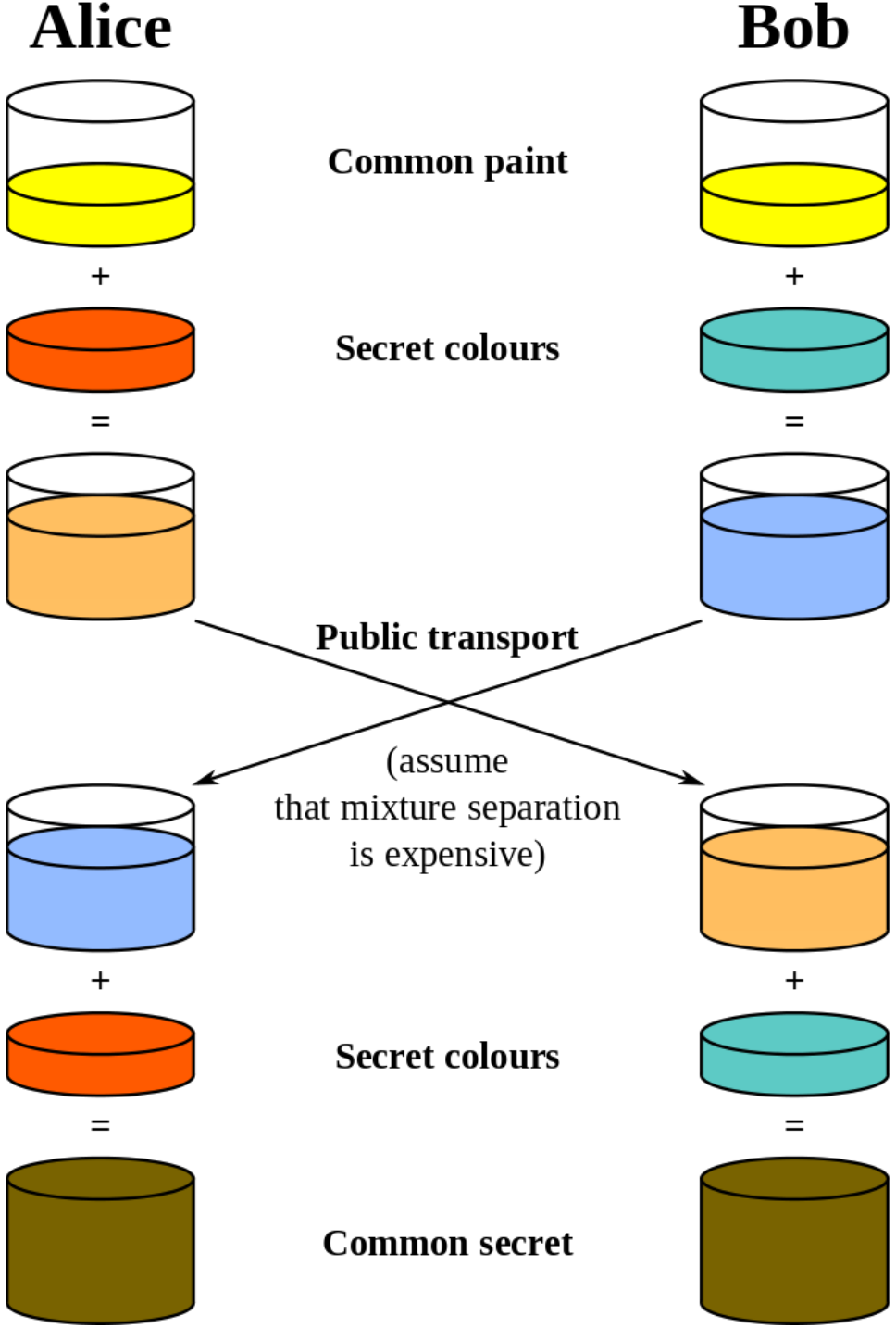
$M = C^d \bmod n$

큰 소수 p, q를 구한다. 이 두수의 곱을 n 이라 할 때 *Φ(n)* 과 서로 소인 e를 구하고 *Φ(n)* 모듈라 산수에서 e의 역수인 d를 구한다. (그리고, p, q는 없애버린다.)

임의의 수를 d제곱한 것을 e제곱하면 원래 수로 돌아오므로 둘 중 하나를 공개키 나머지 하나를 비밀키로 하면 된다.

이 암호를 깨려면 p, q를 알아야 하는데 n을 알아도 이 둘을 알아내는데 충분히 긴 시간이 걸리는 것이 핵심.

물감 섞기로 이해하는 공개키 알고리즘의 비밀



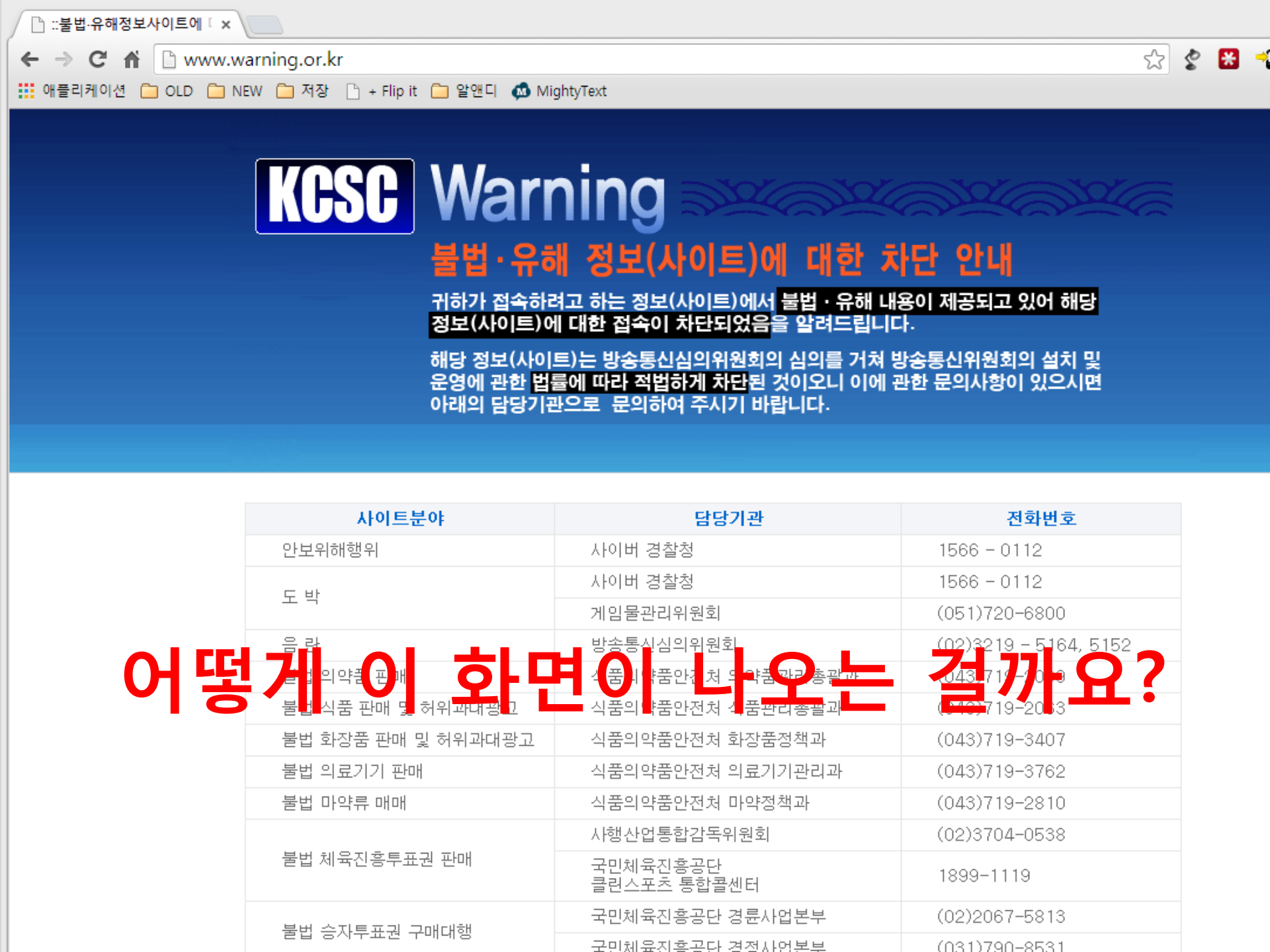
창과 방패

warning.or.kr

방화벽

tor, freenet, & ...

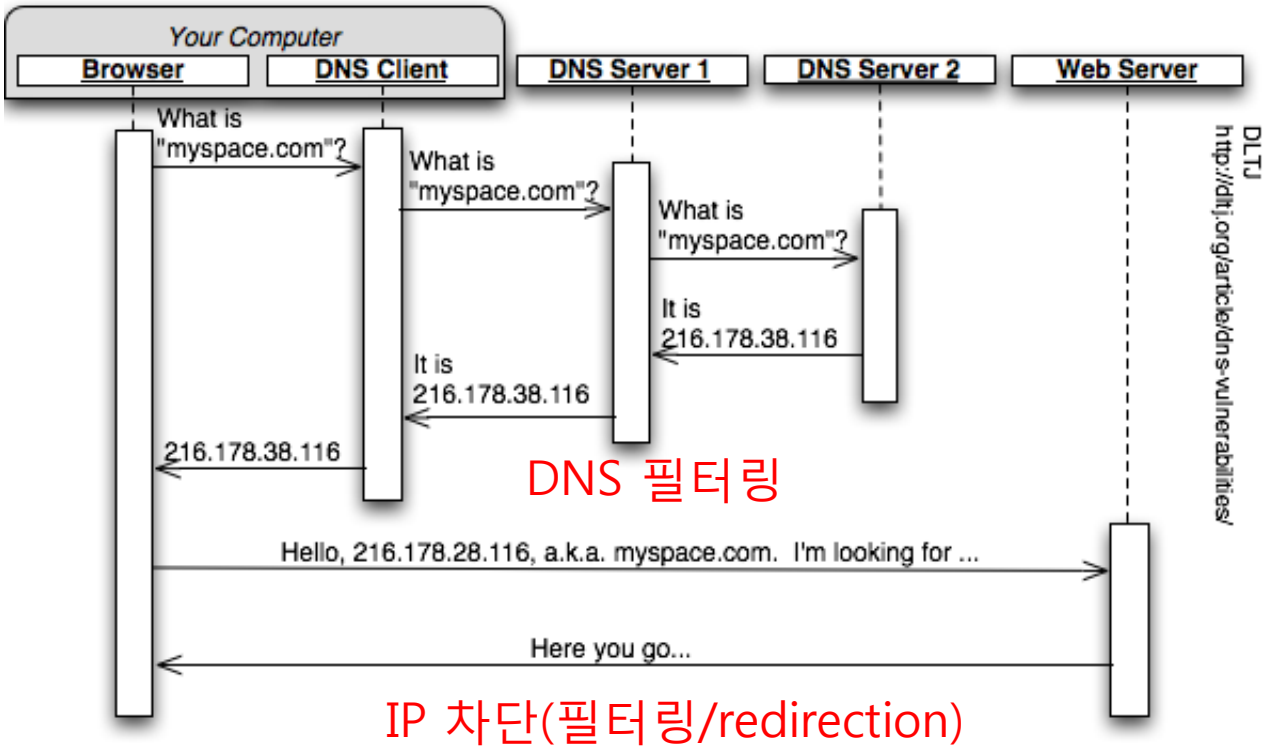
정보보안 기본 개념

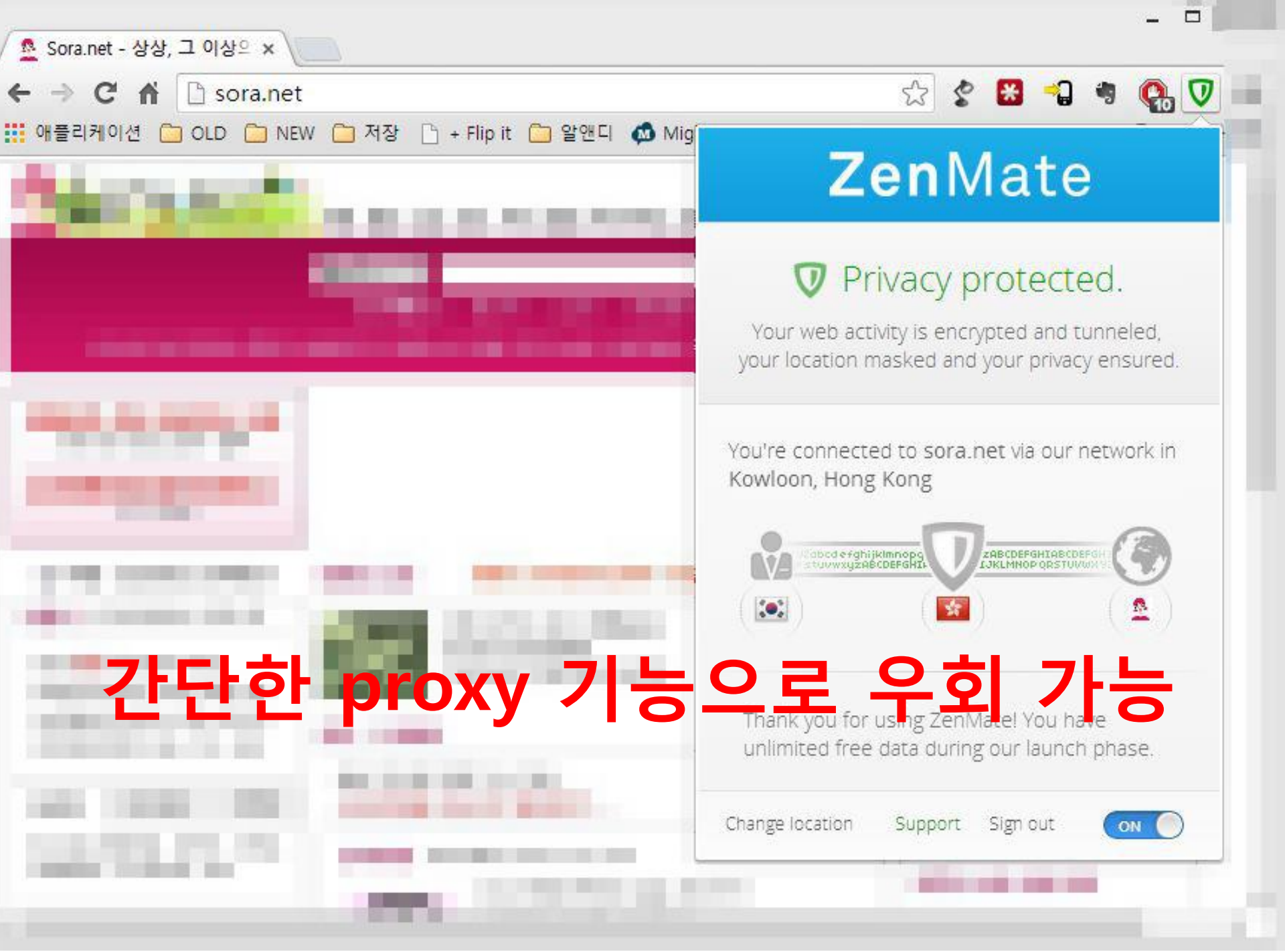

::불법·유해정보사이트에
www.warning.or.kr
애플리케이션
OLD
NEW
저장
+ Flip it
알앤디
MightyText
KCSC
Warning
불법·유해 정보(사이트)에 대한 차단 안내
귀하가 접속하려고 하는 정보(사이트)에서 불법 · 유해 내용이 제공되고 있어 해당 정보(사이트)에 대한 접속이 차단되었음을 알려드립니다.
해당 정보(사이트)는 방송통신심의위원회의 심의를 거쳐 방송통신위원회의 설치 및 운영에 관한 법률에 따라 적법하게 차단된 것이오니 이에 관한 문의사항이 있으시면 아래의 담당기관으로 문의하여 주시기 바랍니다.
사이트분야
담당기관
전화번호
안보위해행위
사이버 경찰청
1566 - 0112
도 박
사이버 경찰청
1566 - 0112
게임물관리위원회
(051)720-6800
음 란
방송통신심의위원회
(02)3219 - 5164, 5152
불법 식품 판매 및 허위과대광고
식품의약품안전처 식품관리총괄과
(043)719-2063
불법 화장품 판매 및 허위과대광고
식품의약품안전처 화장품정책과
(043)719-3407
불법 의료기기 판매
식품의약품안전처 의료기기관리과
(043)719-3762
불법 마약류 매매
식품의약품안전처 마약정책과
(043)719-2810
불법 체육진흥투표권 판매
사행산업통합감독위원회
(02)3704-0538
국민체육진흥공단 클린스포츠 통합콜센터
1899-1119
불법 승자투표권 구매대행
국민체육진흥공단 경륜사업본부
(02)2067-5813
어떻게 이 화면이 나오는 걸까요?

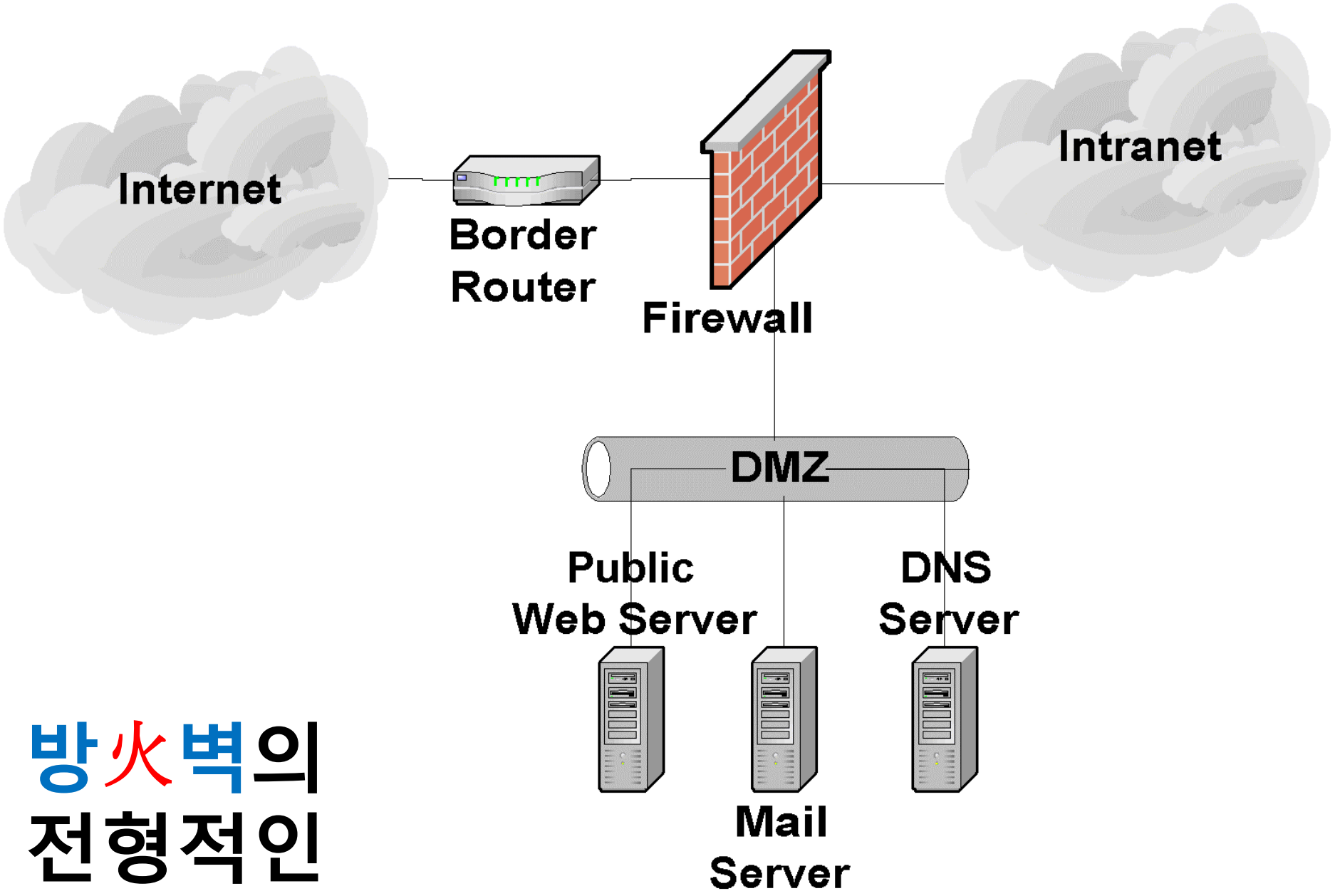
왜 우리는 언니들을 만날 수 없나?

```
$ dig sora.net

; <<>> DiG 9.8.1-P1 <<>> sora.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7406
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;sora.net.                      IN      A

;; ANSWER SECTION:
sora.net.               100     IN      A       69.197.27.194

;; Query time: 210 msec
;; SERVER: ????????????????????
;; WHEN: Sat Jan 11 17:09:52 2014
;; MSG SIZE  rcvd: 42
```

```
$ telnet  69.197.27.194 80
Trying 69.197.27.194...
Connected to 69.197.27.194.
Escape character is '^]'.
GET / HTTP/1.1
Host: sora.net
HTTP/1.0 302 Redirect
Location: http://www.warning.or.kr

Connection closed by foreign host.
```




Sora.net - 상상, 그 이상으
sora.net
애플리케이션
OLD
NEW
저장
+ Flip it
알앤디
ZenMate
Privacy protected.
Your web activity is encrypted and tunneled, your location masked and your privacy ensured.
You're connected to sora.net via our network in Kowloon, Hong Kong
Thank you for using ZenMate! You have unlimited free data during our launch phase.
Change location
Support
Sign out
ON
간단한 proxy 기능으로 우회 가능



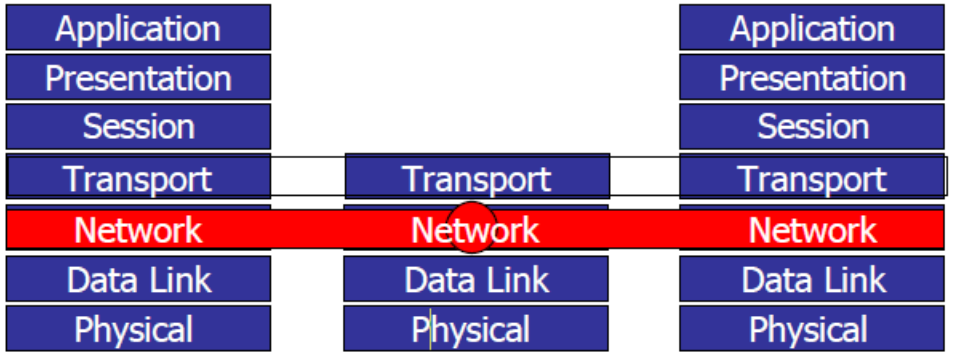
방火벽의 전형적인 構成방식

그림 출처: http://www.totalroute.net/cgi-web-hosting/CGI-Web-Hosting-Guidelines0080.htm

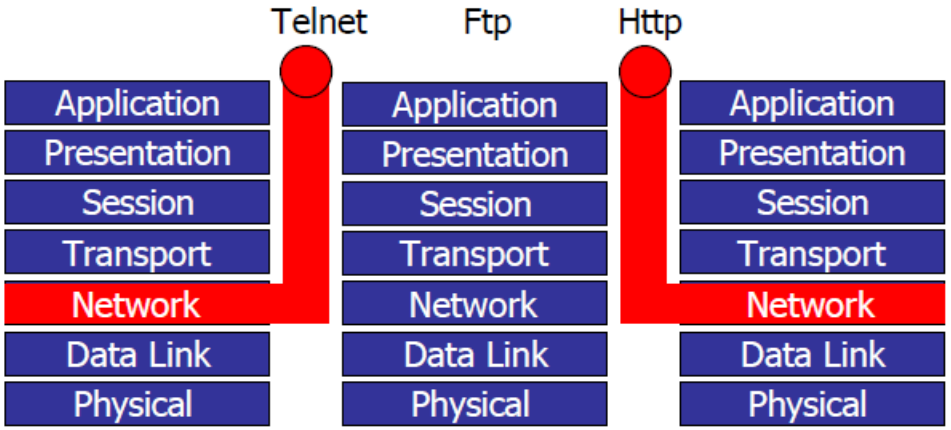
POL34CERT
COMPUTER SECURITY INCIDENTS RESPONSE TEAM OF POL34 NATIONAL NETWORK

Firewall systems

Types and operation



Packet level filtering



Application level filtering

방火벽의
動作방식

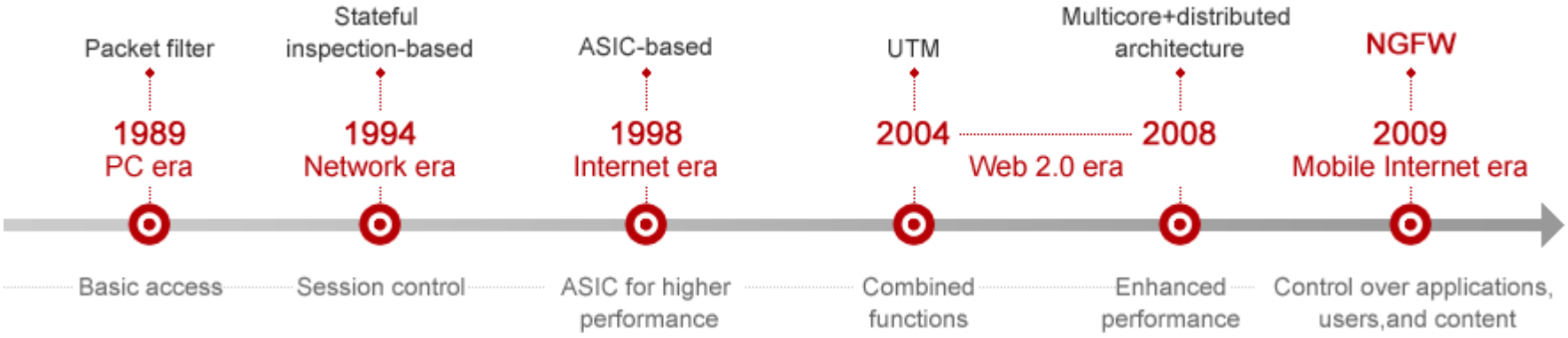
유생전(劉生展) 作, 현대 중국, <유비·관우·장비 삼 형제와 싸우는 여포>

방화벽 공격기법

Packet fragmentation
Source porting
Source routing
Vulnerabilities in TCP/IP stack
FTP PASV
External(e.g. outsourced) systems
Content (e.g. email–borne trojan horse)
Man in the middle attacks
(e.g. compromised DNS)
출처: POL34CERT

방화벽의 진화

그림 출처: http://enterprise.huawei.com/topic/2013_Firewall_en/index.html



theguardian

Google™ Custom

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment

News › World news › Edward Snowden › The NSA files

Edward Snowden

RSS

Latest on the computer analyst whistleblower who provided the Guardian with top-secret NSA documents leading to revelations about US surveillance on phone and internet communications

Top story

Mass surveillance by security services should be reviewed, say Lib Dems

8 Jan 2014: Party's motion, in wake of Snowden whistleblowing, covers agencies' accountability, data collection and bill of rights

191 comments

The NSA files whistleblower

'They will say I aided our enemies'

Video (7min 07sec): The

Most recent

Liberal Democrats: digital drumbeat

9 Jan 2014: Editorial: Two senior Liberal Democrats call for judicial oversight of state surveillance and regular releases of statistics on UK security service data requests

41 comments

European parliament invites Edward Snowden to testify via video

9 Jan 2014: Not yet clear if NSA whistleblower will accept invitation from European parliament committee investigating surveillance

Mass surveillance by security services should be reviewed, say Lib Dems

8 Jan 2014: Party's motion, in wake of Snowden whistleblowing, covers agencies' accountability, data collection and bill of rights

191 comments

2014
or
1984

인터넷에서의 익명성

Tor
Freenet
I2P
GNUnet
nightweb

Home About Tor Documentation

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac Li

Download Tor

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Learn more about Tor »

Why Anony

Tor protects you by b
communications arou
relays run by volunte
prevents somebody v
connection from learr
and it prevents the si
your physical locatio

Freenet

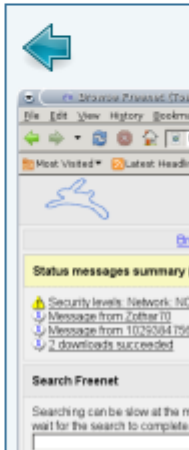
THE FREE NETWORK

Home Download About Help

Share, Chat, Browse. Anonymously. On the I

Share files, chat on forums, browse and publish, anonymously and without fear of blocking or censorship! Then connect to your friends for even better security!
Learn more!

Freenet
Download
0.7.5 for Windows



못다한 이야기


문의 : 1600-4534
2012 CONCERT
still mosdahan song
아직도 못다한 노래...
still mosdahan song
남진

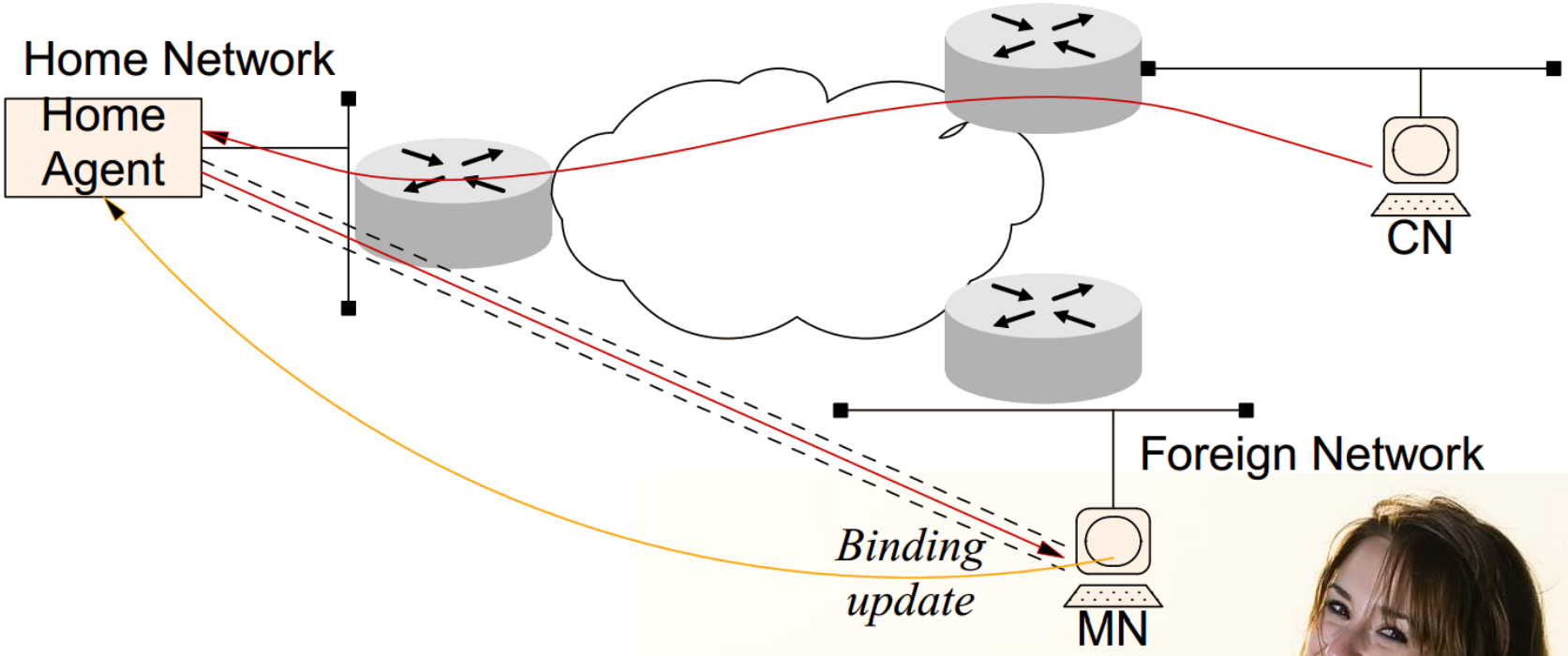
NAT

Public address vs. Private address

10.0.0.0/8 (255.0.0.0)
172.16.0.0/12 (255.240.0.0)
192.168.0.0/16 (255.255.0.0)

그림 출처: http://danawa.com

ISP (ingress) filtering
127.0.0.1 해킹하지 마세요 ^^



IP tunneling
Triangular routing
Binding update

그림 출처: http://www.hznet.de/ipv6/mipv6-intro.pdf

semantic overload

IP address = Locator + Identifier

스마트폰(WIFI+4G) : 같은 기계 다른 주소
DHCP, NAT, proxy : 다른 기계 같은 주소
Mobile IP / Multi homing : 같은 카드 다른 주소

route aggregation

efficiency vs. flexibility

Provider independent address block


25%
북미 ISP의 총 트래픽중 ¼은 구글과 연결되는 것
구글이 소모하는 전기는 원자력 발전소 1기 발전량의 ¼
패킷?
fiber
평평한 인터넷
Backbone vs. Google & CDN
Goodbye hosts!
computing → data → contents
pull → push
인터넷이 필요한지?
facebook / kakao
많은 인터넷?
clean slates / openflow