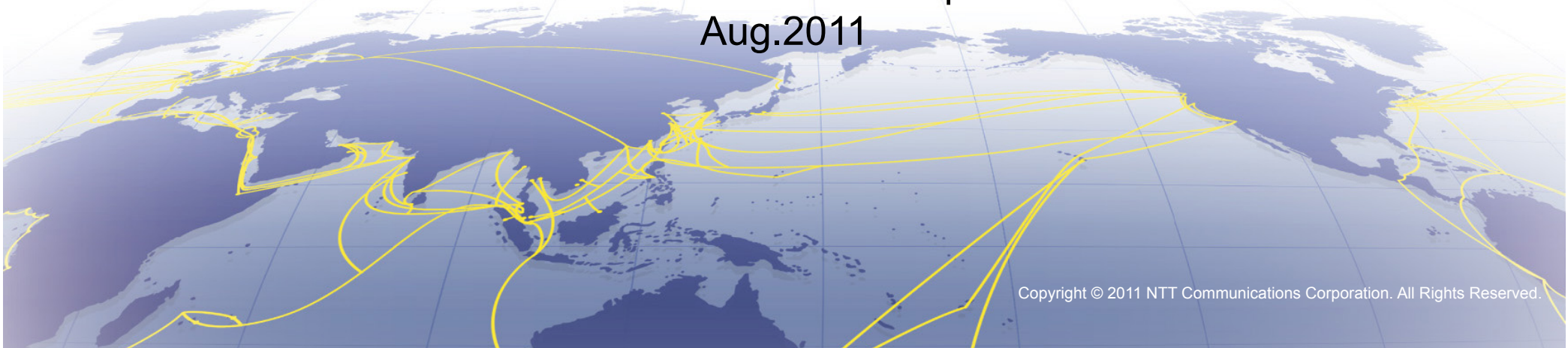# From IPv4 to IPv4/v6 dual stack Internet

APNIC 32
Dr. Shin Miyakawa
NTT Communications Corporation
Aug.2011

IPv4 address shortage

Where IP address comes from ?

IANA (Internet Assigned Number Authority)
- The Origin -

RIR(Regional Internet Registry）
 ARIN: North America
 RIPE NCC: Europe, Middle East, etc
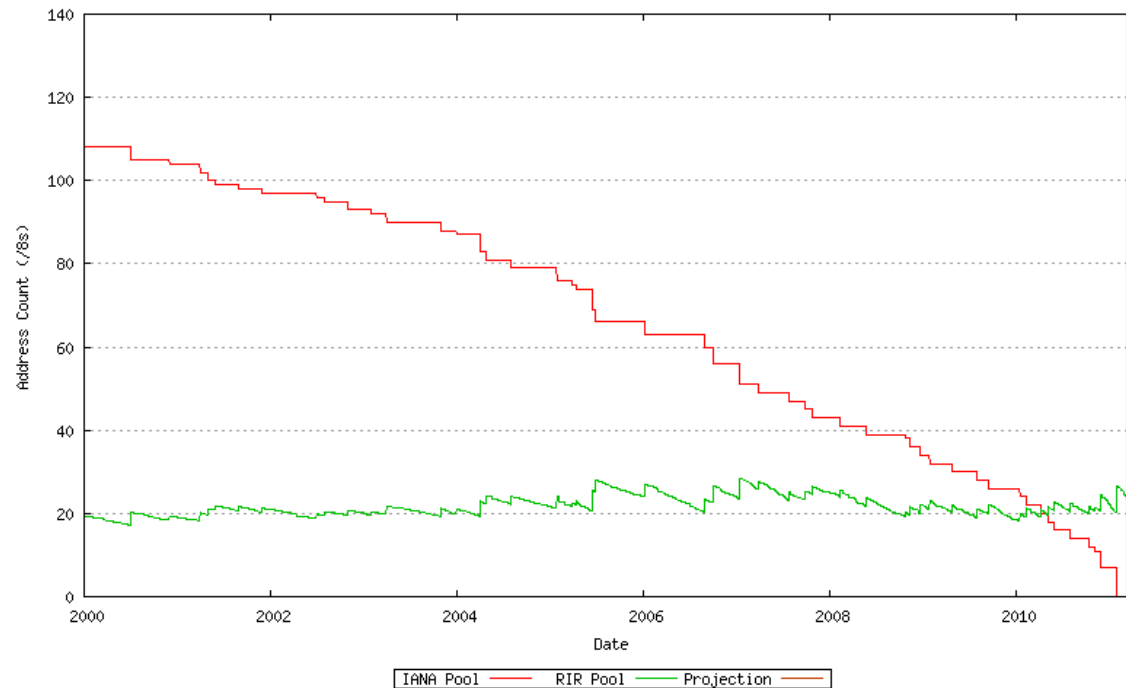APNIC: Asia/Pacific
LACNIC:Latin America, Caribbean
AfriNIC: Africa

ISP, Enterprise…

IPv4 address shortage

- <ins>http://www.potaroo.net/tools/ipv4/index.html</ins>   at 17-May-2011 07:58 UTC.
- IANA Unallocated Address Pool Exhaustion: 01-Feb-2011
- Projected RIR Unallocated Address Pool Exhaustion: 15-Apr-2011

IANA /RIR pools have been EXHAUSTED already.

3

We have to do two things simultaneously

1. IPv4 life time extension

☆ To keep existing assets, we should extend the life of IPv4

☆ However so, there is no new IPv4 address space, we have to modify IPv4 Internet itself.

2. Introduction of IPv6

☆ Fundamental treatment with new protocol with 128 bit length address space

☆ Smooth introduction
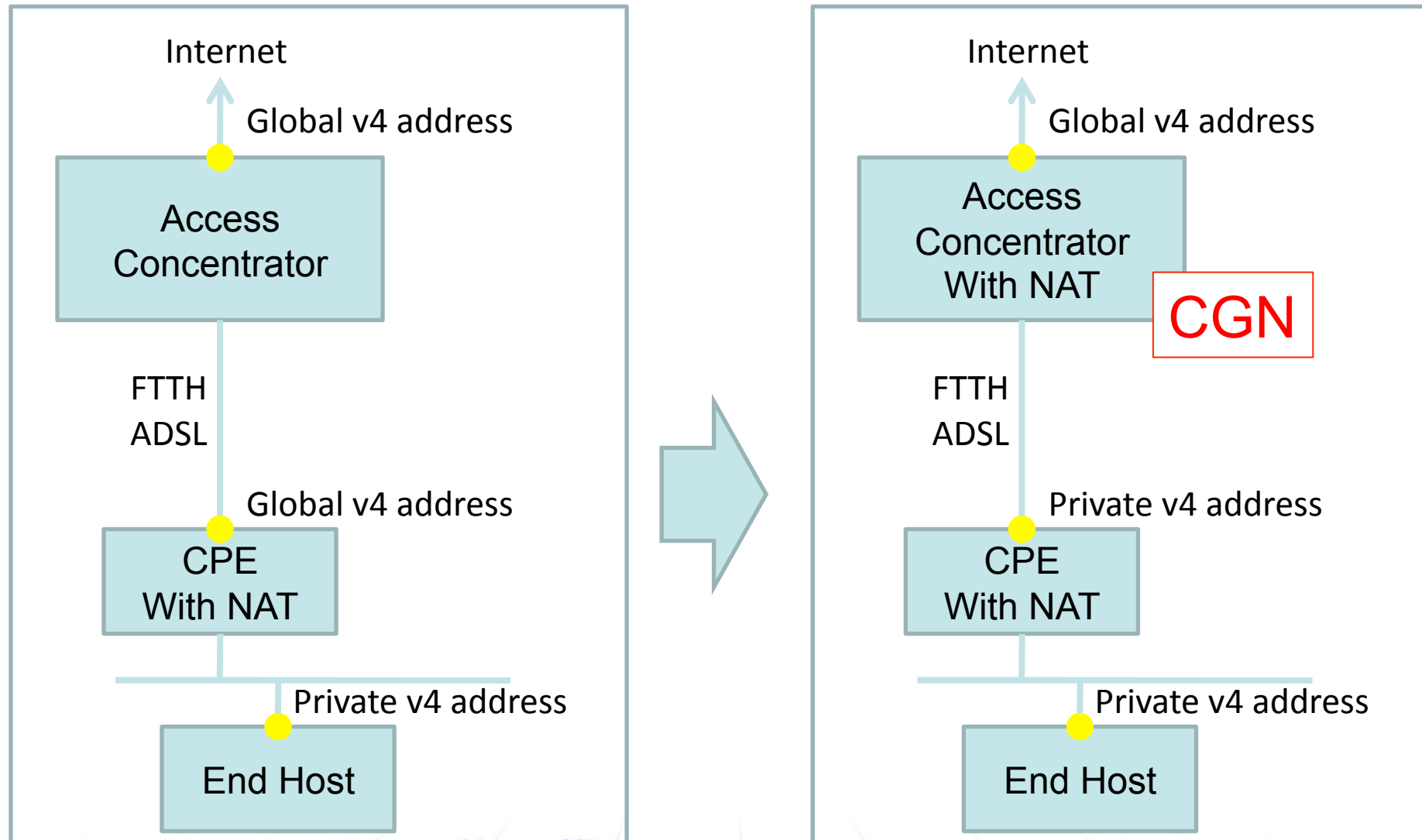
Carrier Grade NAT / Large Scale NAT

Huge NAT (Network Address Translator) introduction into the ISP access concentration to share single global IPv4 address with multiple users

It is called as Large Scale NAT (LSN) or Carrier Grade NAT (CGN)

CGN:Carrier Grade NAT (NAT444)

Internet

Global v4 address

Access
Concentrator

FTTH
ADSL

Global v4 address

CPE
With NAT

Private v4 address

End Host

Internet

Global v4 address

Access
Concentrator
With NAT

CGN

FTTH
ADSL

Private v4 address

CPE
With NAT

Private v4 address

End Host

CGN: It's not enough nor perfect

Sharing IPv4 address means modification of IP communication model

ACL (Access Control List) against for some attack traffic has huge side effect

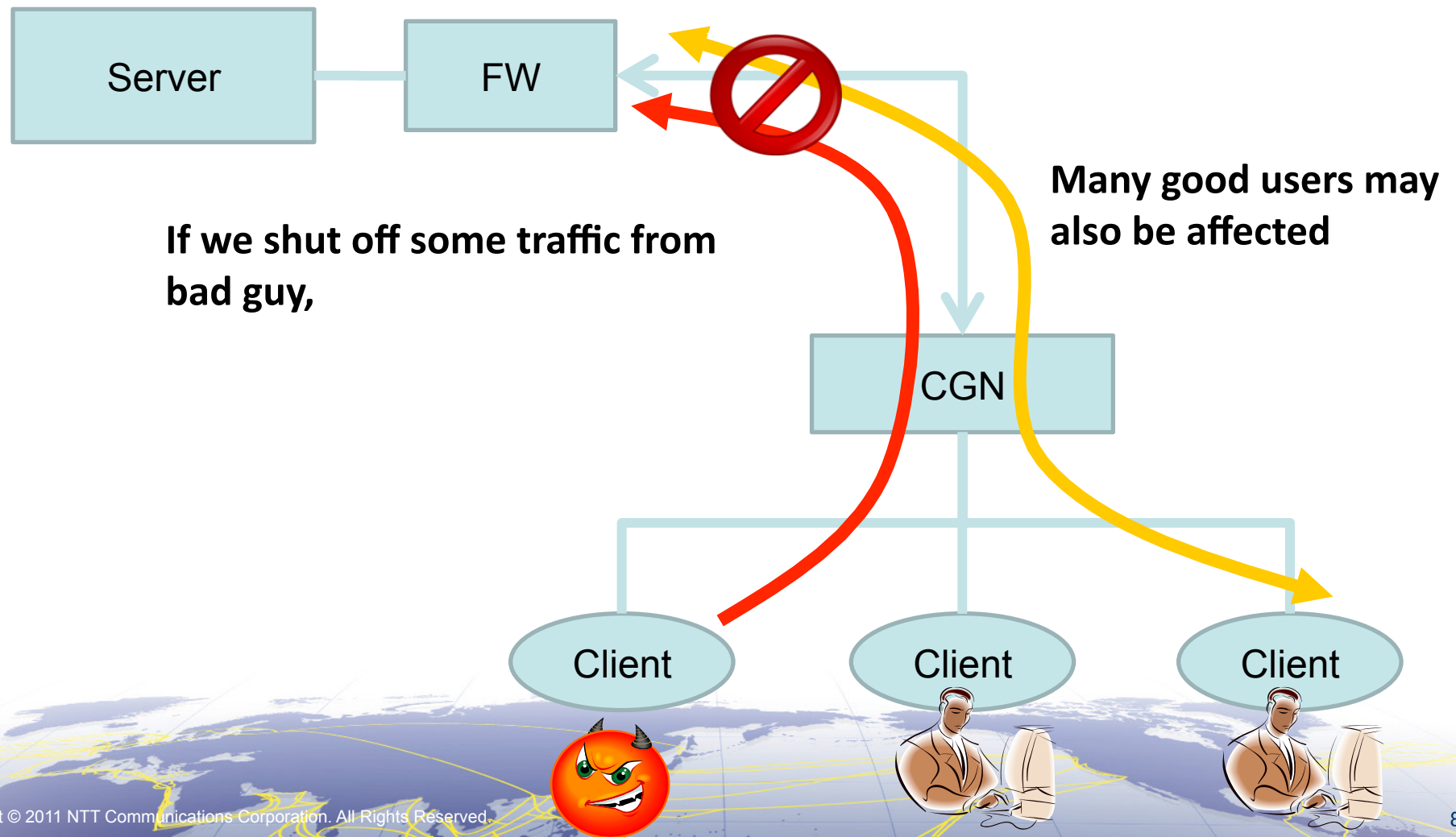Not only IP address but its Port number must be recorded at server to identify who accessed to the service

Can we use SIP for VoIP ? fmmmm

Does P2P work ?????

Many (serious) side effects

We can not use ACL

Server

FW

CGN

Client

Client

Client

Many good users may also be affected

If we shut off some traffic from bad guy,

8

What's going on about security and other issues with CGN ?

- We have to give up to use IP address as user identifies
→ This impacts on firewall and many security device seriously

- We have to log the access with not only IP address but also port number indicates where the user comes from
    - Legally needed to identify the client
    - However so, this means HUGE storage which COSTS A LOT

- We have to define the notion "CGN Friendly", however it is not clear yet
    - What application can be used over CGN and how ?

- Session number limitation problem (see following slides)

Session Number Limitation

Host

Host

Host

NAT

Host

Host

Host
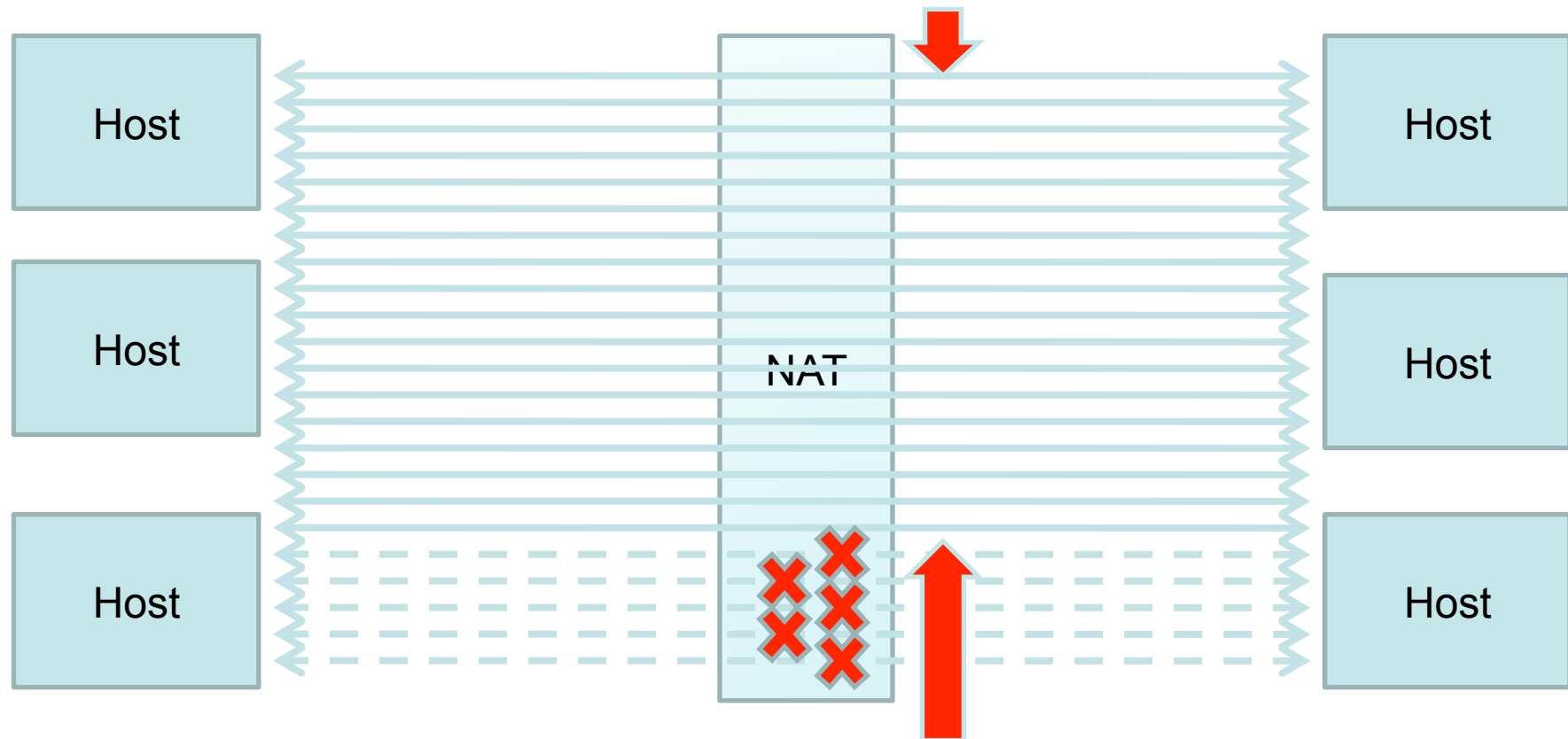
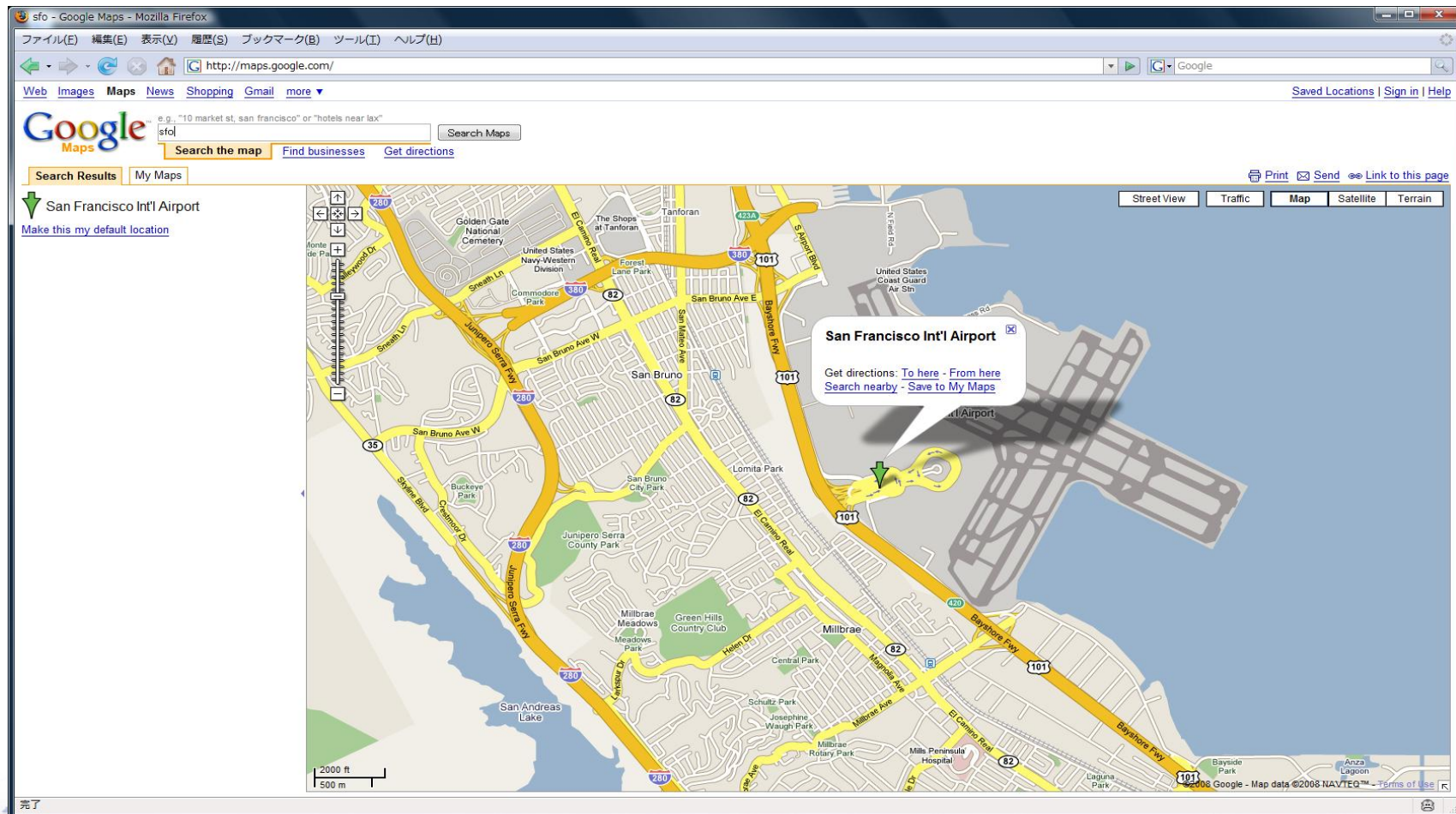Maximum # of sessions

- We installed a machine that has two Ethernet interfaces and acts as a Ethernet bridge in front of a normal PC client runs Windows and Internet Explorer.

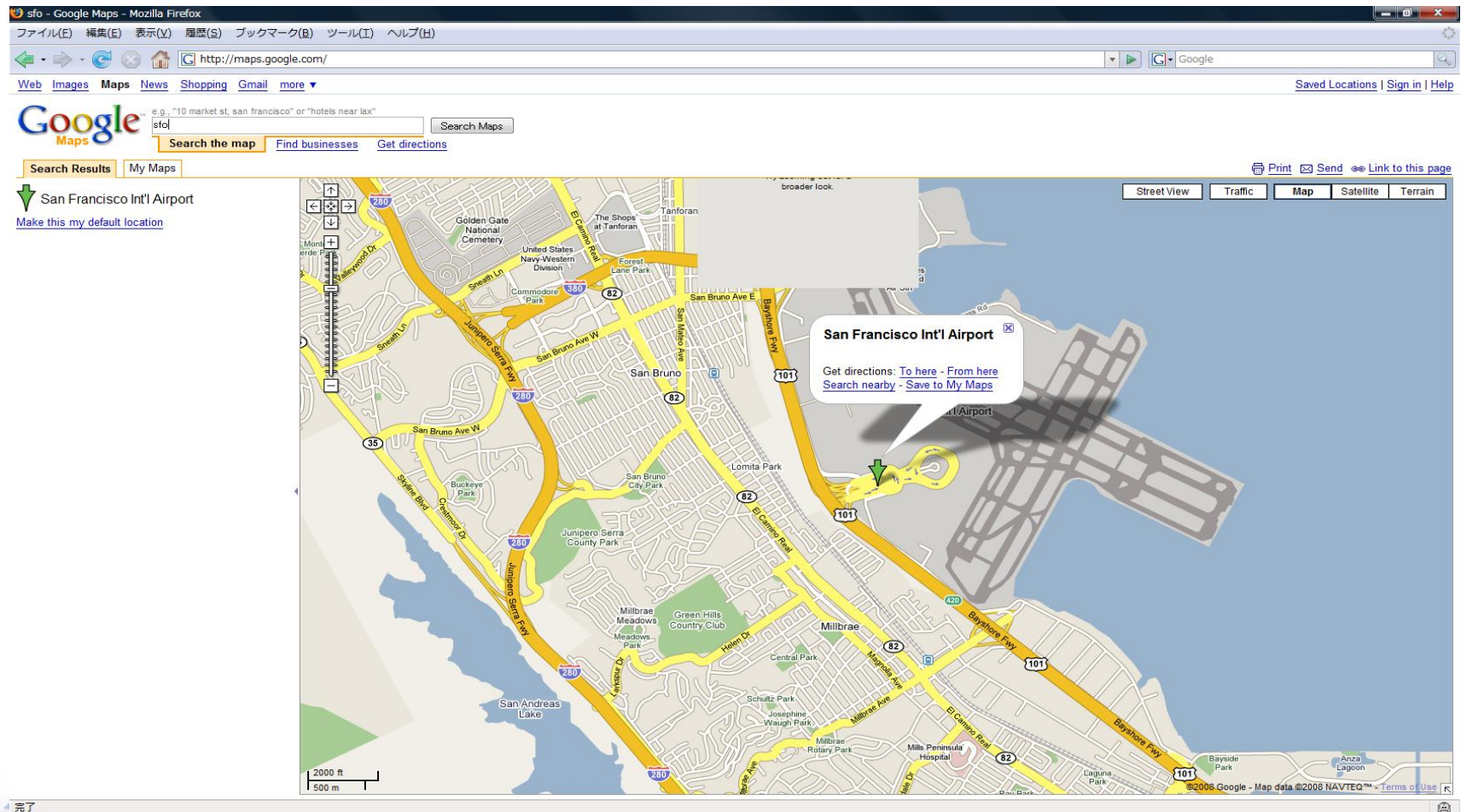- That machine can limit the number of simultaneous TCP sessions through it.

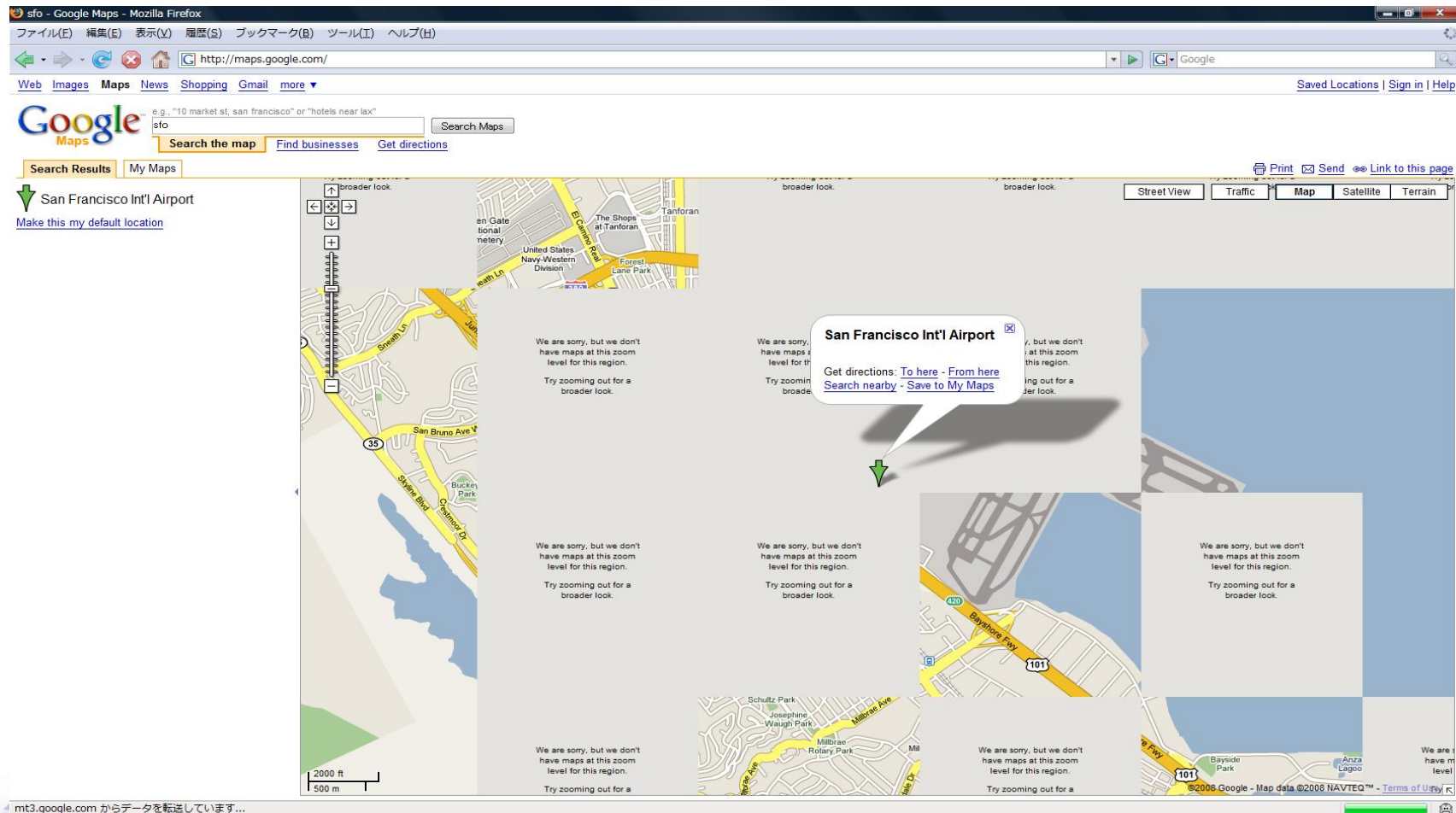| PC

Web browser | → | TCP session limiter | → | The Internet |
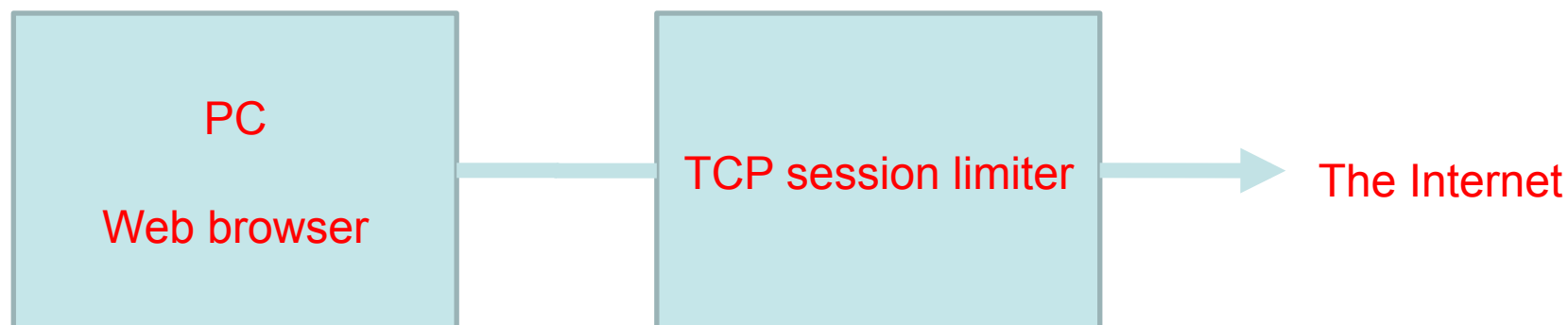
Max 30 Connections with Google MAP

Max 20 Connections

Max 15 Connections

Max 10 Connections
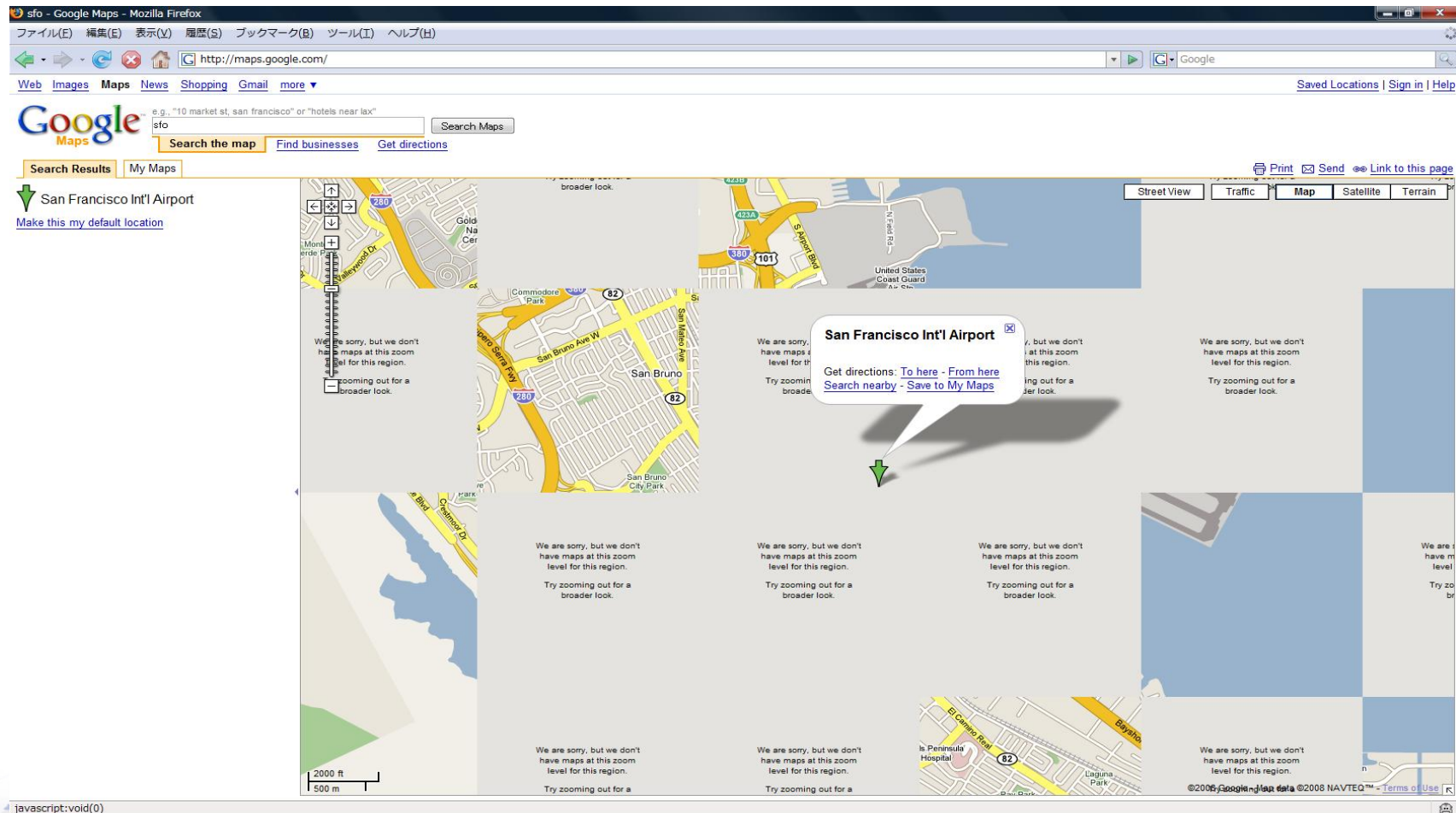
Max 5 Connections

- Use of AJAX (Asynchronous JavaScript + XML) provides users with quite good quality of operation

- Because AJAX allows an application to communicate with a server by its JAVA based communication channels, the application can be escaped from the max connection limitation opposed by the browser so that it can use many TCP sessions as much as possible to accelerate data transmission.

- In short, AJAX application is moving quickly and is able to show the results faster.

- Therefore, so many web applications use AJAX which means that so many applications use many simultaneous TCP sessions which would stress CGN a lot.

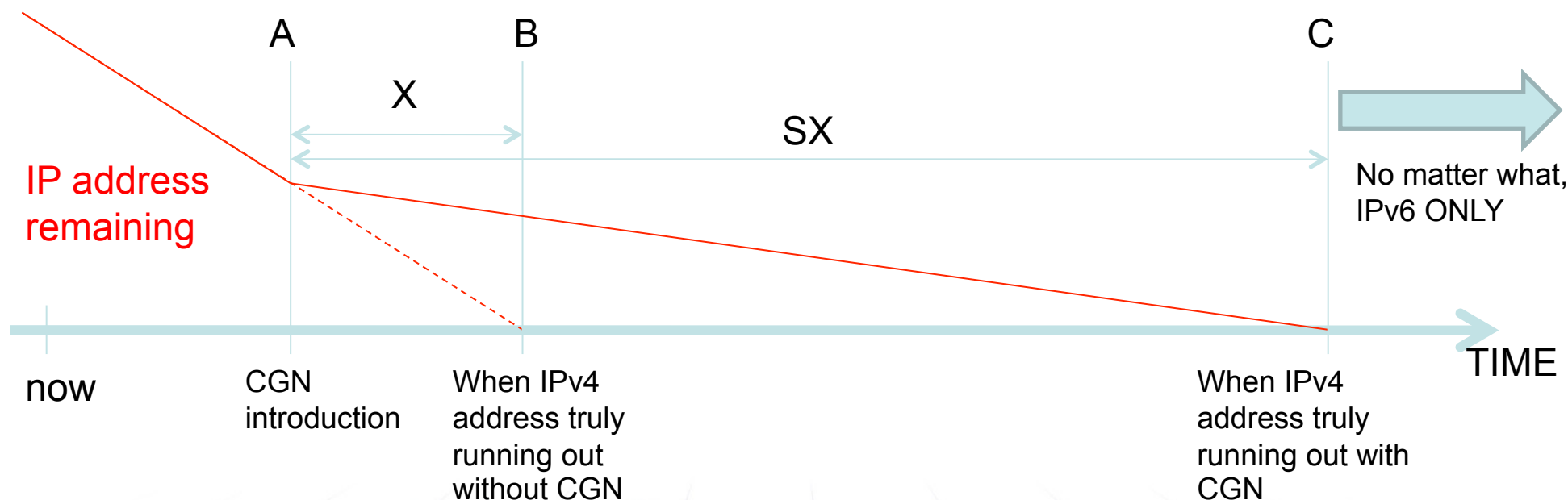| Webpage	# of TCP sessions
No operation	5〜10
Yahoo top page	10〜20
Google image search	30〜60
Nico Nico Douga	50〜80
OCN photo friend	170〜200+
iTunes	230〜270
iGoogle	80〜100
Rakuten	50〜60
Amazon	90
HMV	100
YouTube	90

How many session should we allow to a user ?

- TCP has only 2 bytes (16 bits) for its port range. This means that with usual implementation, we can use only up to 64K (2^16 or 65536) sessions with single global IP address as source address theoretically. Because of security and other reasons, we should use upper 32K ports as source address towards servers, if we need to share single IPv4 address with 1000 customers, one customer can use only 32 ports at the maximum.

- However so, the previous slide shows our survey about how many sessions are used in popular web applications and it tells that we should assign at least 1000 or maybe 3000 ports per customer to assure good performance of IPv4 applications with CGN. This means we can slow down the consumption speed of IPv4 address only 10 times slower.

CGN can only slow catastrophe, can not prevent it

- S (Slow down ratio) can be defined as the number of customers who share a single global IP address and is likely 10 according to the previous discussion.

- If X is defined as the duration between A: when CGN introduction and B: whenIPv4 address running out without CGN （X=AB), the catastrophe: C can be postponed until SX later （C=AC).

- Then, because we'd like to C be year 2025, if B could be year 2015, A must be 2014 or 2013 at least.

A   B   C

X

SX

IP address
remaining

No matter what,
IPv6 ONLY

now   CGN   When IPv4   When IPv4
               introduction   address truly   address truly
                                running out   running out with
                                without CGN   CGN

TIME

- CGN is quite expensive… (Please help!)

  – It would be "de-graded" IPv4 service if we introduce CGN, so we can not charge more to the users…

  – Rather than that, we could charge LESS…

  – There is no hope to cover the cost of CGN in this case.

- Not only for ISP but Server Operators too

  – You must have massive log for servers…

    - Every single TCP sessions at the server must be logged to identify who access the service.

So…. Even we should extend IPv4 life time…

Only with IPv4 life time extension like CGN,

it costs a lot and there's no hope eventually

Migrating to the IPv6 is quite low cost and better way to keep the Internet business growing for long time

IPv6 Introduction

- Moving to IPv4 / IPv6 dual stack
- Modify applications and services to be compatible with IPv6
    - Google has been finished already
- IPv4 can not be vanished instantly
    - Windows XP DNS query needs IPv4 transport, for example
- Carrier Grade NAT or similar technologies are also needed
- Brand new application should use IPv6 from the beginning to prevent unnecessary cost to be upgraded
    - Sensor network for energy saving, for example
- IPv6 introduction started widely in Japan
- IPv4 should be withdrawn after 2025 or so
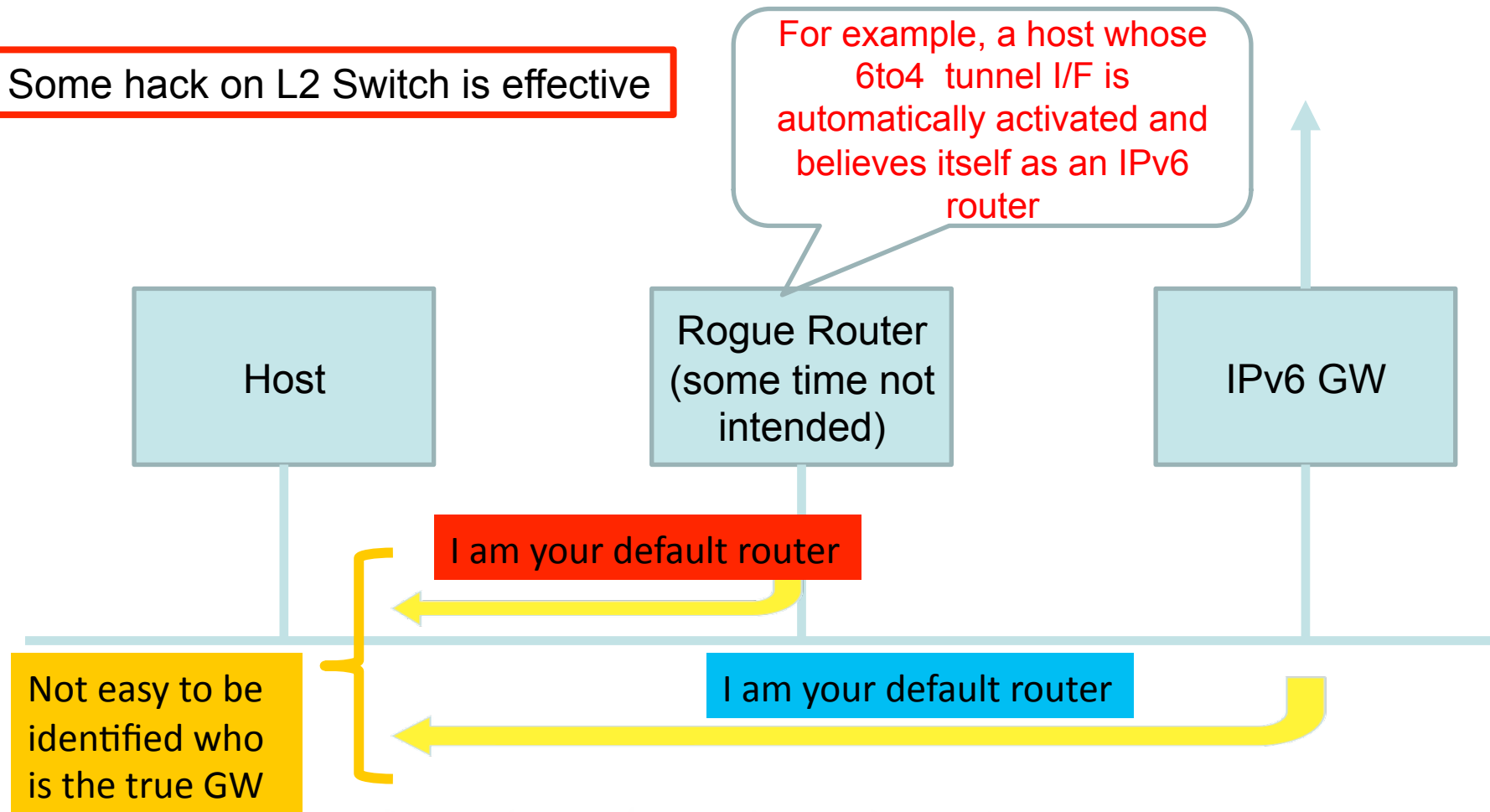
Operation and Security on IPv6 ?

Basically same as v4, but there are certain differences.
We have to think about operation and security from basics.

Treatment of ICMP, fragmentation at firewall, rogue router…
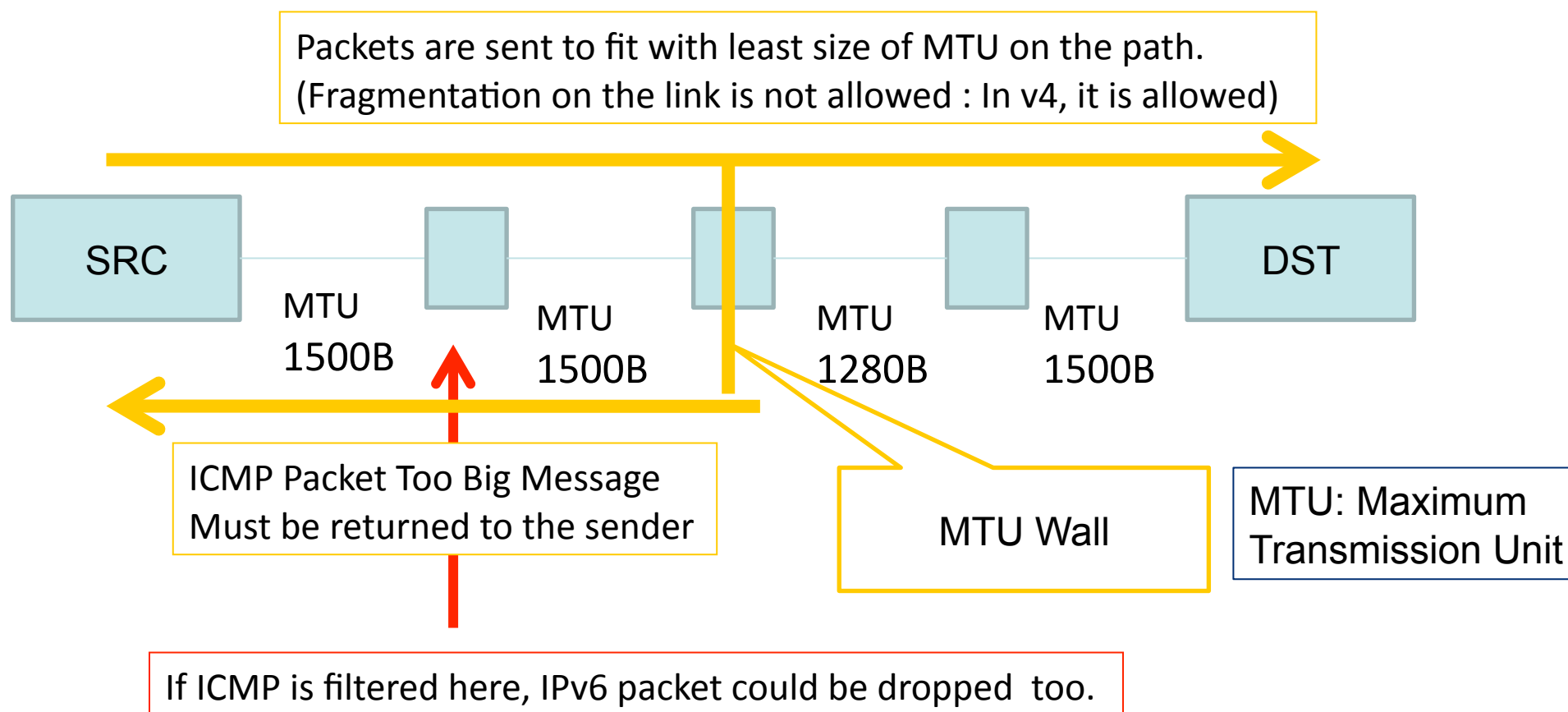High technical skills are required to the ISP

Rogue Router Advertisement

Some hack on L2 Switch is effective

For example, a host whose 6to4 tunnel I/F is automatically activated and believes itself as an IPv6 router

Host

Rogue Router (some time not intended)

IPv6 GW

I am your default router

Not easy to be identified who is the true GW

I am your default router

ICMP is important - Example: Path MTU Discovery

Packets are sent to fit with least size of MTU on the path.
(Fragmentation on the link is not allowed : In v4, it is allowed)

SRC   DST

MTU
1500B

MTU
1500B

MTU
1280B

MTU
1500B

ICMP Packet Too Big Message
Must be returned to the sender

MTU Wall

MTU: Maximum
Transmission Unit

If ICMP is filtered here, IPv6 packet could be dropped too.

Caution on the (hop by hop option) header

Heavy load maybe !

SRC

DST
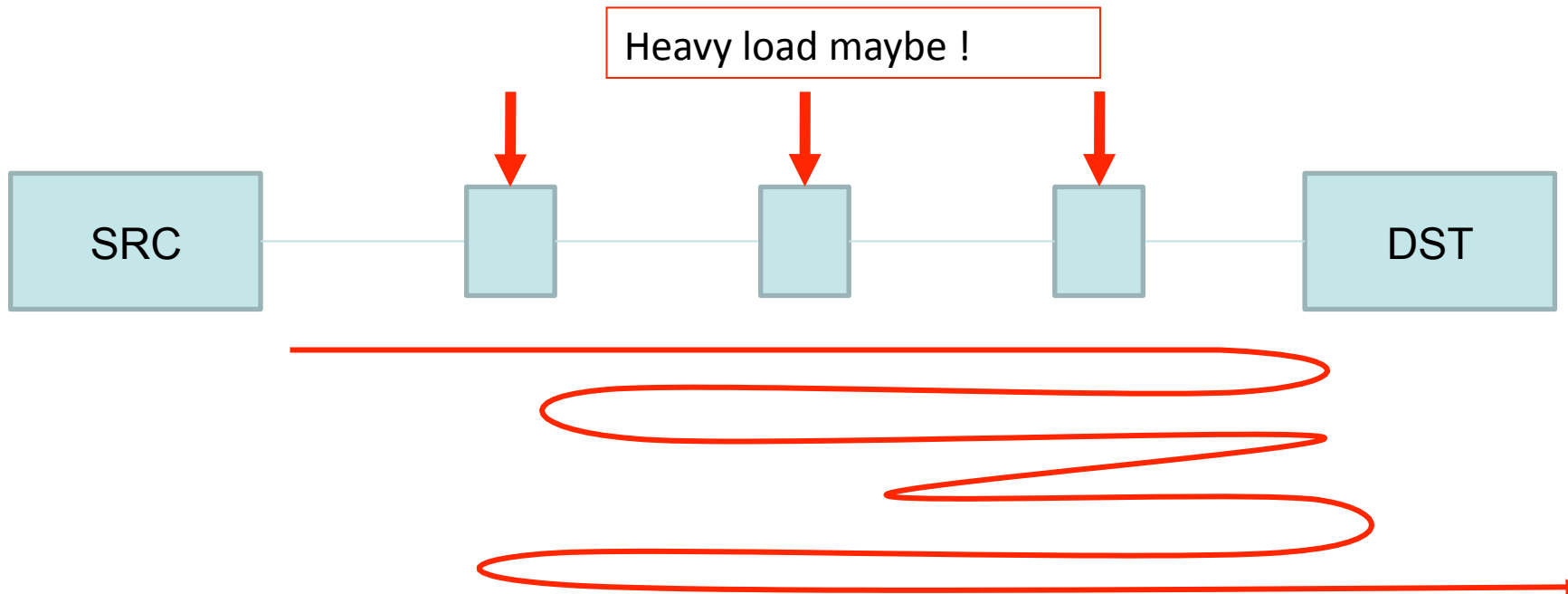
IPv6 can have multiple header.
If hop by hop option header is used , routers in between source and destination could be heavily loaded.
Proper filter must be applied.

Access Control List on Firewall to control the packet forwarding

FIREWALL

If a packet is fragmented,

Put it in the queue and re-assemble to identify this packet can be go through or not

Same fragmentation is required in IPv6 (It's difficult!!)

In IPv4 , this re-assembled packet can be placed to the our going Interface. If needed, out going I/F will fragment as it needs. However so, in IPv6, because of Path MTU Discovery, It must be fragmented as it comes into the firewall.

Can be sent as re-assembled in IPv4

Many Firewall implementation can not do this or, even it can do so, often it consumes CPU power a lot.

At the end

- IPv4 address is running out
- Still many people do not understand about v6
- Seeing is believing. Use it.

- We continues on R&D on these topics to realize smooth migration