

# ISP Support for Enterprise Customers during IPv6 Deployment

27<sup>th</sup> August, 2009  
APNIC 28, Beijing, China

Takeshi Tomochika

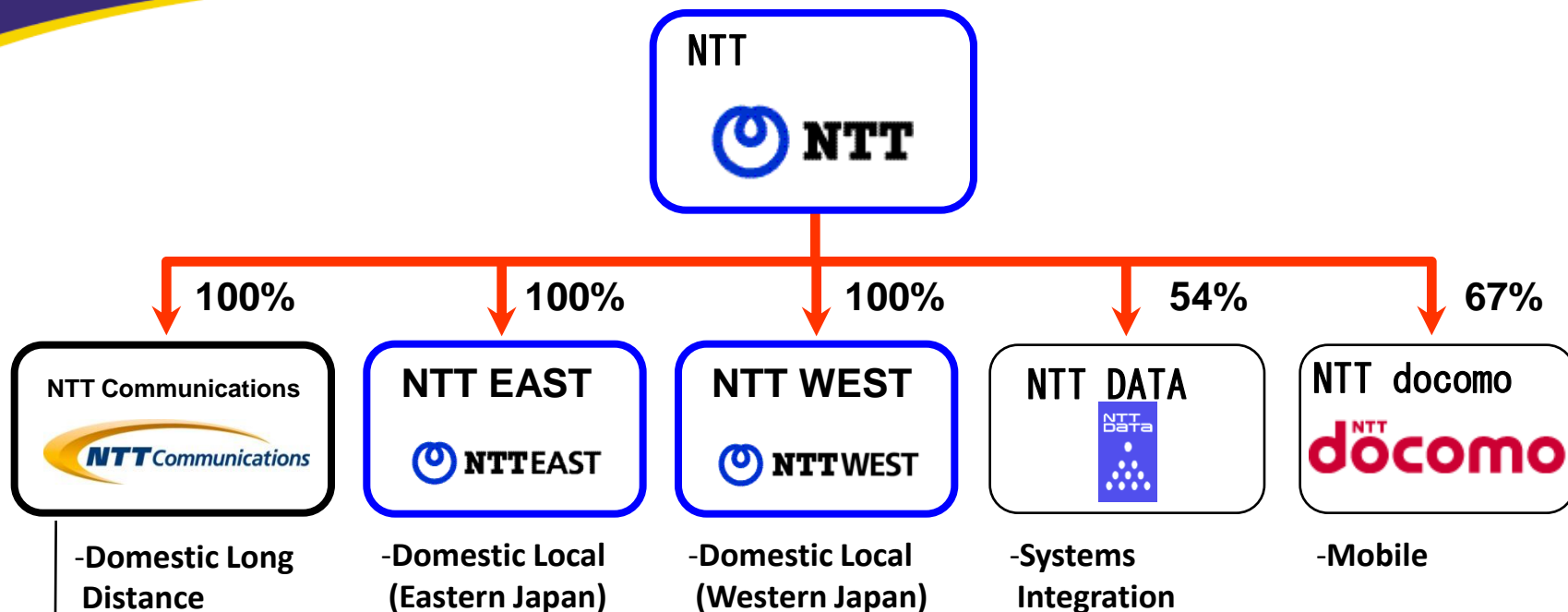
NTT Communications Corporation

# Outline

- Introduction of NTT Com's IPv6 Activities
- 5 Check Points in IPv6 Adoption Plan for Enterprise Networks
- Issues
- Case Study
- Conclusion

# **Introduction of NTT Com's IPv6 Activities**

# Outline of NTT Group



**ntt.net** : International Open IP Service Brand

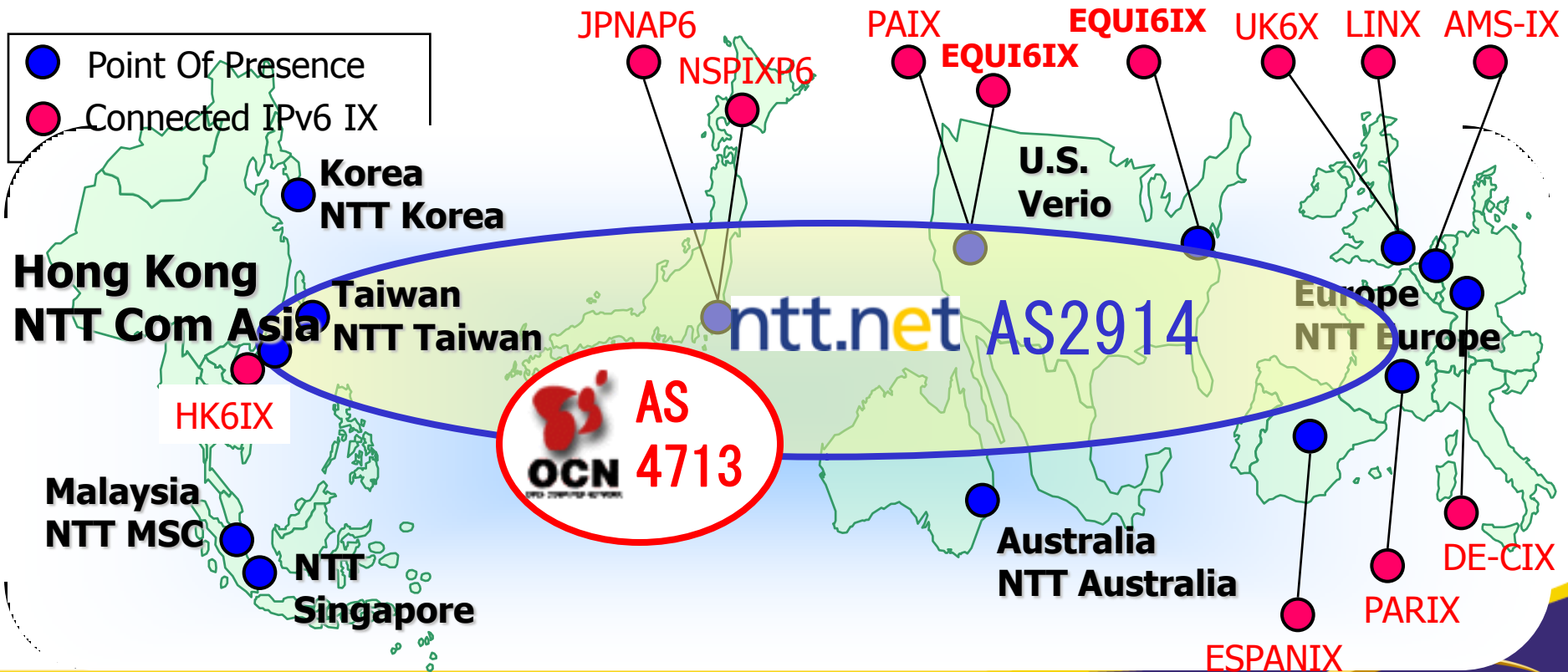
**OCN** : Domestic Open IP Service Brand

And we also provides  
Network consulting,  
integration and solution.

恩梯梯通信設備(上海)有限公司 (NTT Communications China Co., Ltd.)  
100% <http://www.ntt.com.cn/en/>

# NTT Com's two IP Backbones

- Operate the world's largest IPv6/IPv4 Dual Stack Backbone, spanning Asia/Pacific, North America and Europe.
- Global coverage of IPv6 network (7 Asia/Pacific Countries, US, 5 European Countries)
- Worldwide IPv6-IX Connectivity (JP, HK, U.S, UK, NL, DE, FR, ES)



# NTT Com's IPv6 History

**1996:** NTT Labs started one of the world's largest global IPv6 research networks

**1998:** Verio begins participation in PAIX native IPv6 IX

**1999:** NTT Com begins IPv6 tunneling trial for Japanese customers

**2000:** Verio obtains IPv6 sTLA from ARIN

**2001:** NTT Com pioneers world's first IPv6 connectivity services on a commercial basis

**2002:** World Communications Awards (WCA) awards NTT Communications with "Best Technology Foresight" for its IPv6 Global products

**2003:** NTT/VERIO launches IPv6 Native, Tunneling, and Dual Stack commercial service in North America

**2003:** Communications Solutions magazine names NTT/VERIO IPv6 Gateway Services "Product of the Year"

**2004:** NTT IPv6 Native and Dual Stack services available around the globe

**2004:** NTT Com wins the World Communications Awards "Best New Service" award for IPv6/IPv4 Global Dual Service

**2005:** Dual stack Virtual Private Server released. First ISP to offer an IPv6 managed firewall service

**10/2006 –** Launched the NTT Communications IPv6 Transition Consultancy

**2/2007 –** Awarded GSA Schedule 70 contract for IPv6 IP transit



# NTT Com's IPv6 Services & Solutions

## Internet Transit & Access

*High quality Internet transit & access services based on our Global Tier 1 provider status*

- Global IP Network IPv6 transit.
- "OCN IPv6" is for consumers use.
- "Super OCN IPv6 Dual Ethernet Access"
- "OCN IPv6 Transit" for Colo Customers
- "OCN ADSL IPv6/IPv4 Dual Stack Access"
- "OCN IPv6 Configured Tunnel Access"

## VPN

*IP Private Network Services: Stable, Secure, and High speed*

- 「Arcstar IP-VPN」

## Services & Outsourcing

*Suitable services for your needs*

- Verio VPS (IPv4/IPv6 Dual Stack Housing/Hosting Service)
- Earthquake Early warning system
- Contents Delivery with IPv6 Multicast (Remote lesson)
- HTTP Application Level Gateway. (OCN IPv6 Mobile )

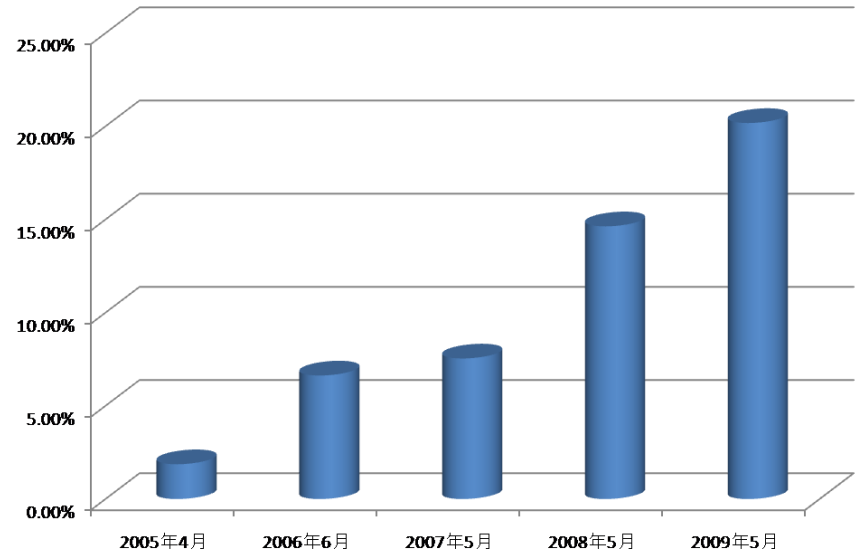
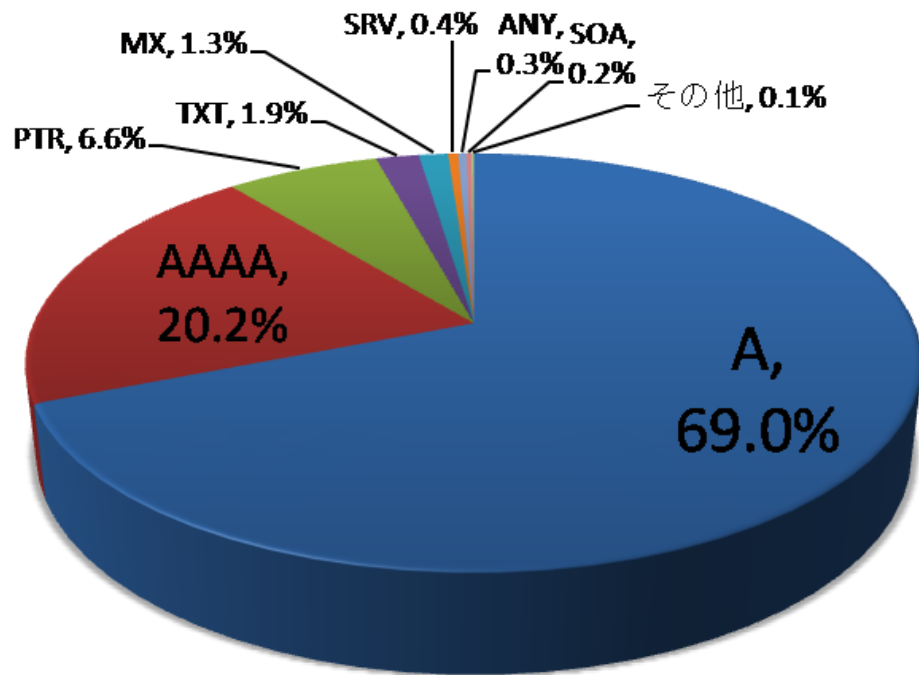
## Solutions

*NTT-Com's solutions are designed to meet your needs and turn your challenges into competitive business advantages.*

- Building Management service (BAS) via the IPv6 Network
- Data Distribution network with IPv6 Multicast
- Sensors network with RFID

# Ranking of Query Types

- Ranking of query type from end users (2009/05) and growth of AAAA





# AAAA record

- The rate of IPv6 response when querying AAAA in May, 2009 :

**0.19%**

- Only one of 500 queries
- Few servers have configured AAAA for FQDN
- Few servers have supported IPv6

# **5 Check Points in IPv6 Adoption Plan for Enterprise Networks**

# Impacts of IPv4 Address Exhaustion for Enterprise Networks

IPv4 address exhaustion will cause

1: difficulty in getting new IPv4 addresses for

1-1: additional public servers.

1-2: additional Internet VPN (IPsec VPN) edge sites.

2: growing use of IPv6 that requires

2-1: way to communicate with external IPv6-only users

2-2: way to communicate with external IPv6-only servers

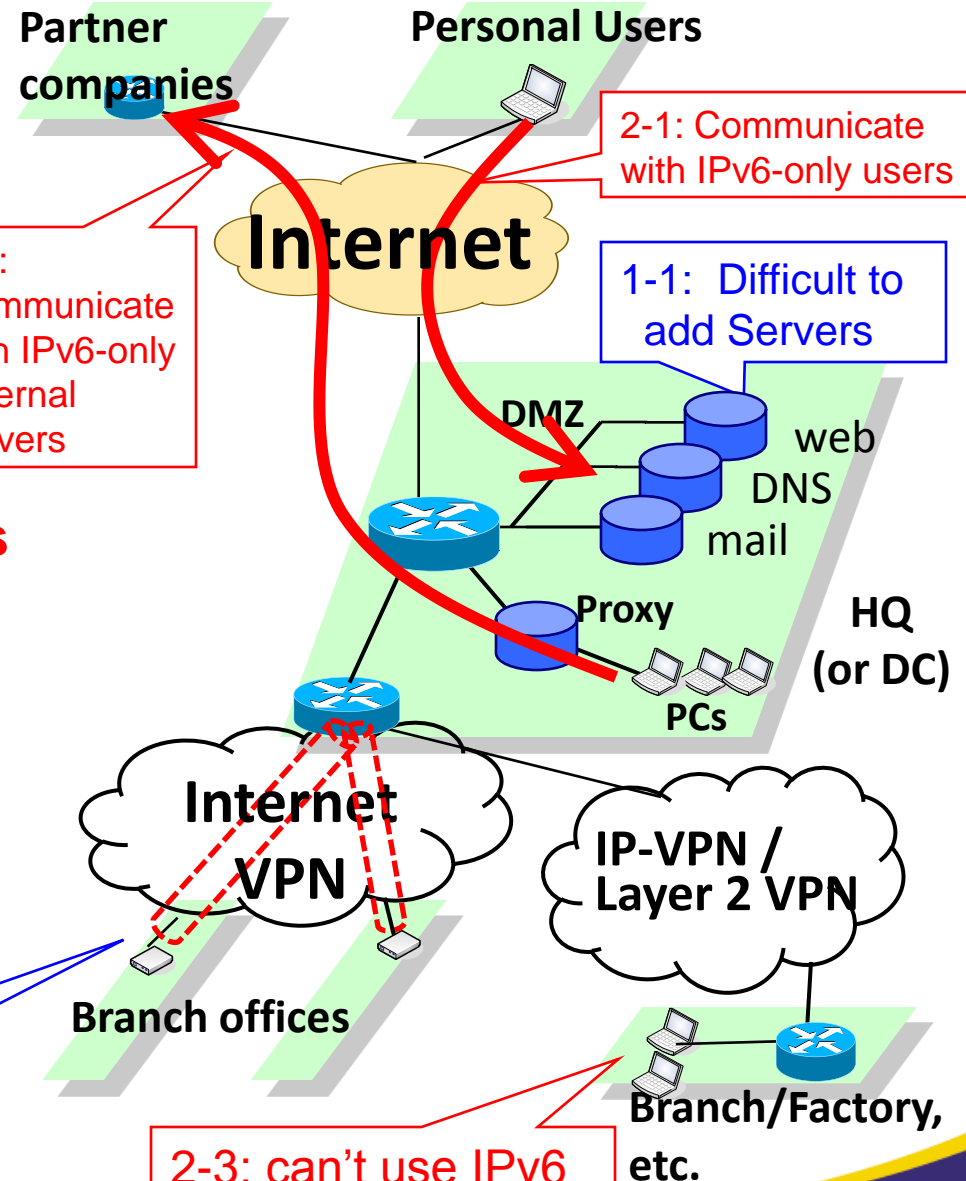
2-3: way to use IPv6-based applications and equipment in the future.

Blue: IPv4

Red: IPv6

1-2: Difficult to add new branches to their Internet VPN

2-3: can't use IPv6 based applications



# 5 Check Points in IPv6 Adoption Plan for Enterprise Networks

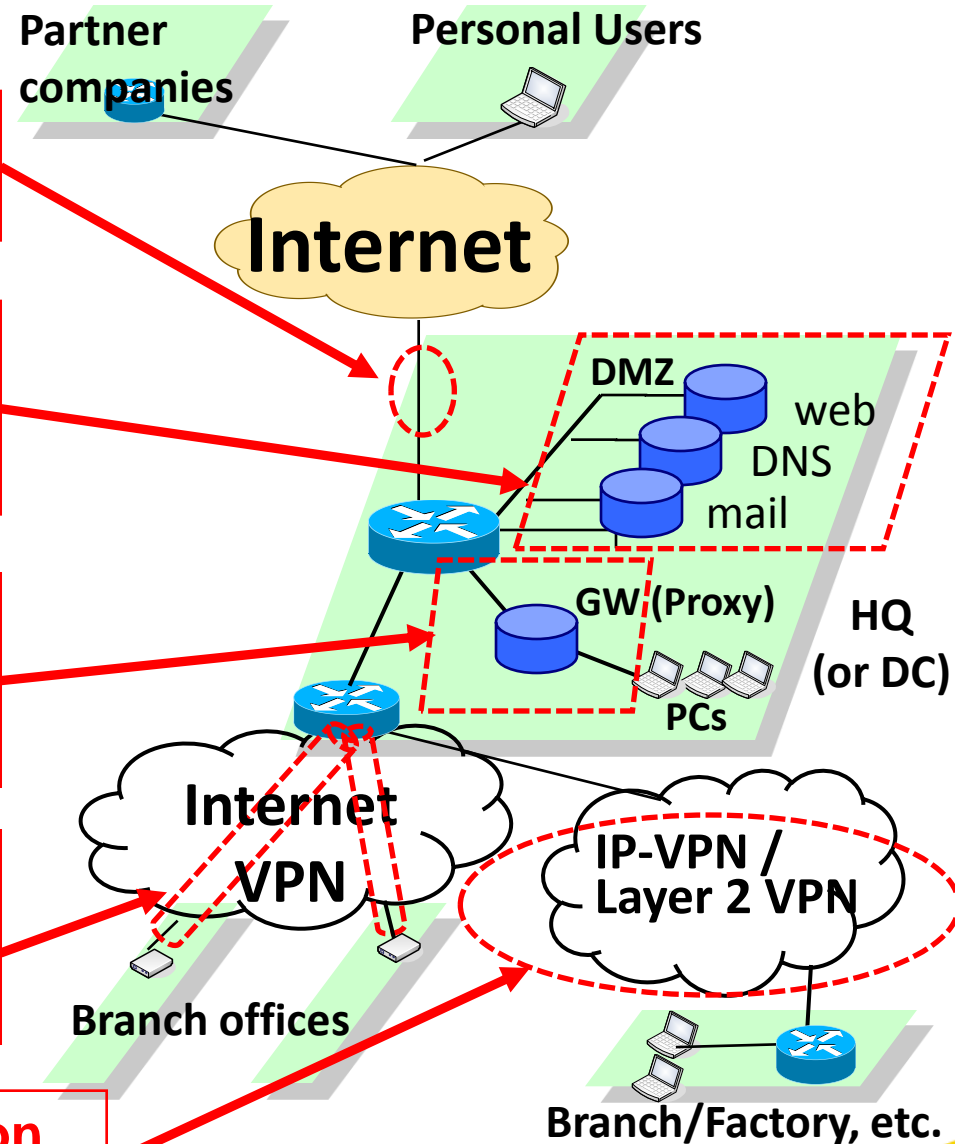
**A: External connectivity**  
- for IPv6 Internet connection

**B: Public servers**  
- for incoming access from external IPv6-only users

**C: GW (proxy)**  
- for outgoing access to external IPv6-only servers

**D: IPsec VPN connection**  
- for additional Internet VPN (IPsec VPN) edge sites

**E: IP-VPN/ Layer 2 VPN connection**  
- for using IPv6-based applications



# Mapping between Check Points and impacts

Considering these 5 points will solve impacts of IPv4 address exhaustion

## 5 check points

**A: External connectivity**  
( B and C are based on A)

**B: Public servers**

**C: GW (proxy)**

**D: IPsec VPN connection**

**E: IP-VPN/ Layer 2 VPN connection**

IPv4 address exhaustion will cause

**1: difficulty in getting new IPv4 addresses for**

**1-1: additional public servers.**

**1-2: additional Internet VPN (IPsec VPN) edge sites.**

**2: growing use of IPv6 that requires**

**2-1: way to communicate with external IPv6-only users**

**2-2: way to communicate with external IPv6-only servers**

**2-3: way to use IPv6-based applications and equipment in the future.**

# A: External Connectivity

- External connectivity for IPv6 Internet connection
  - > IPv6 capable ISP connectivity services
    - Many ISPs already offer connectivity service for enterprises
    - 3 Types of connections

Type	Tunnel	Native (IPv6 only)	IPv6 / IPv4 Dual Stack
Throughput	<ul style="list-style-type: none"><li>- capsulation overhead may have impact</li><li>- too much v4 traffic may affect v6 throughput</li></ul>	<ul style="list-style-type: none"><li>- same level as IPv4</li></ul>	<ul style="list-style-type: none"><li>- same level as IPv4</li><li>- too much v4 traffic may affect v6 throughput</li></ul>
Reliability	<ul style="list-style-type: none"><li>- depends on reliability of IPv4 connection</li></ul>	<ul style="list-style-type: none"><li>- independent from IPv4 both physically and logically</li></ul>	<ul style="list-style-type: none"><li>- v6/v4 depends on the same physical line, while logically independent</li></ul>
Price	<ul style="list-style-type: none"><li>- Low</li></ul>	<ul style="list-style-type: none"><li>- High</li></ul>	<ul style="list-style-type: none"><li>- Moderate</li></ul>

- Price and Impacts on existing network are most sensitive
- Most enterprise customers request “Tunnel” connection for price
- Typically, they want physically independent connection from existing one in order not to affect existing network
- ISP customers tend to request “Dual stack”

# B: Public Servers

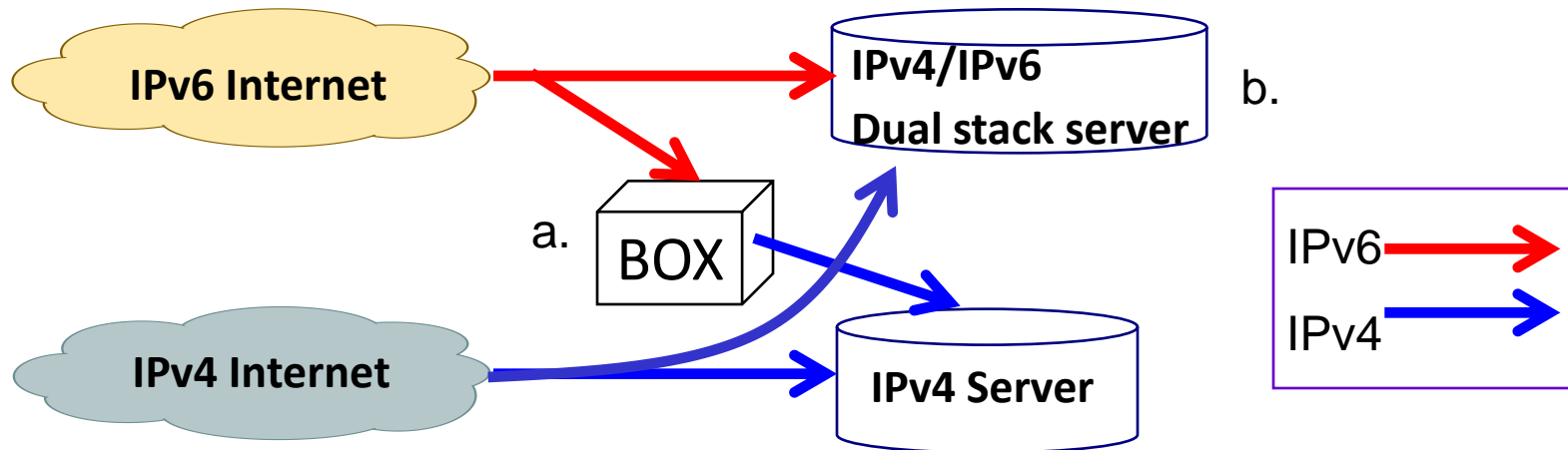
## ■ Make public servers accessible from IPv6 users

> 2 purposes:

1. Solve the difficulty in getting new IPv4 address for additional public servers
2. Achieve the way to communicate with external IPv6-only users

> 2 solutions:

- a. Use v6 to v4 translation box, such as 64 Server Load Balancer (translate IPv6 access into IPv4) and reverse proxy
- b. Make the servers IPv6 capable (Dual stack)



Translation box is useful in many cases; however, in some cases, it's better to make the servers IPv6 capable because of type of servers, logging and operational cost.

# C: GW (Proxy)

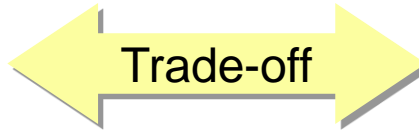
## ■ to communicate with external IPv6-only servers

> 2 solutions:

- a. Use translators, such as proxy servers, for IPv6 external contents

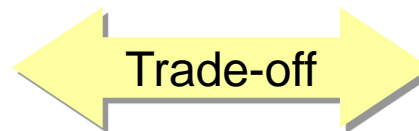
Can keep current structure,  
therefore Implementation is  
relatively easy

Additional Cost (of new devices,  
operation) of proxy / translator



- b. Implement IPv6 (Dual stack) in enterprise network including PCs

Additional Cost (of new  
network, operation,  
management tools, etc.)



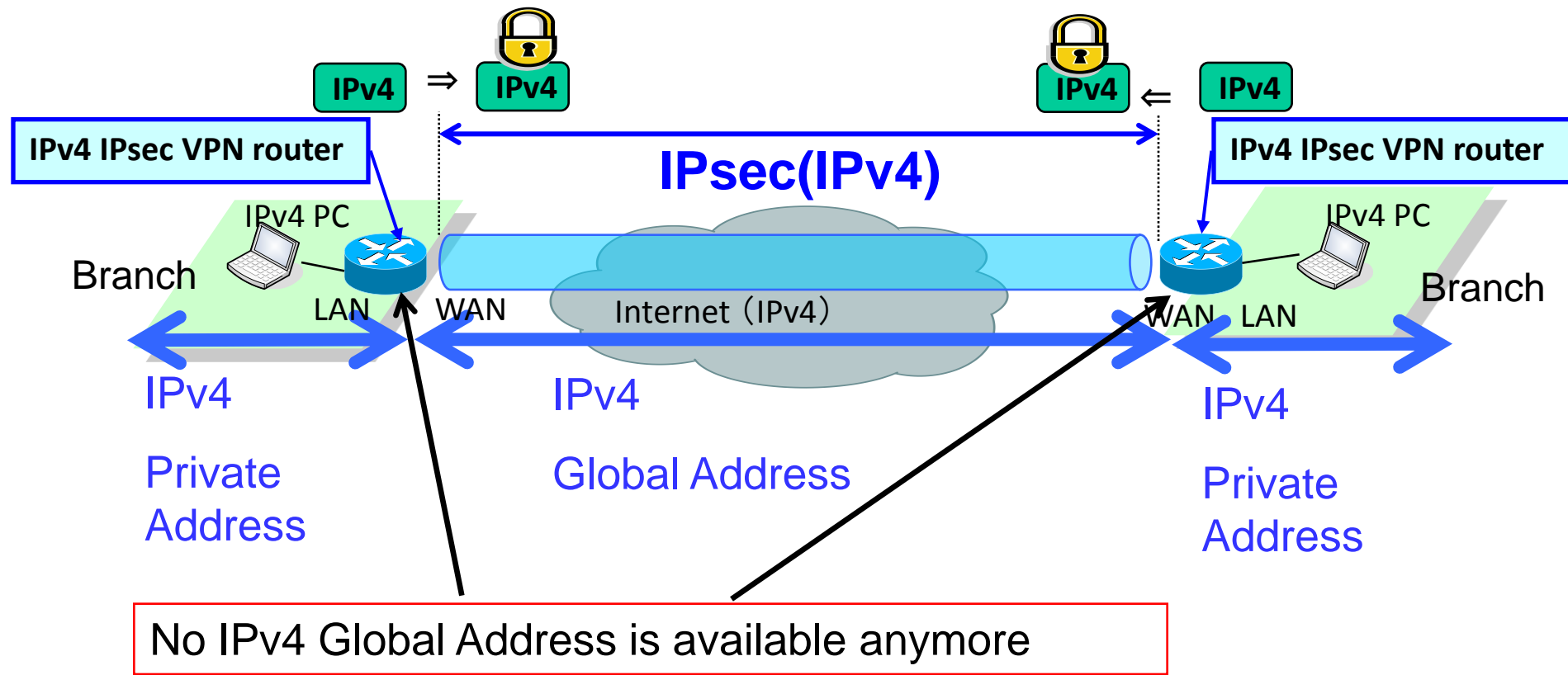
Flat network, multicast





# D: IPsec VPN Connection

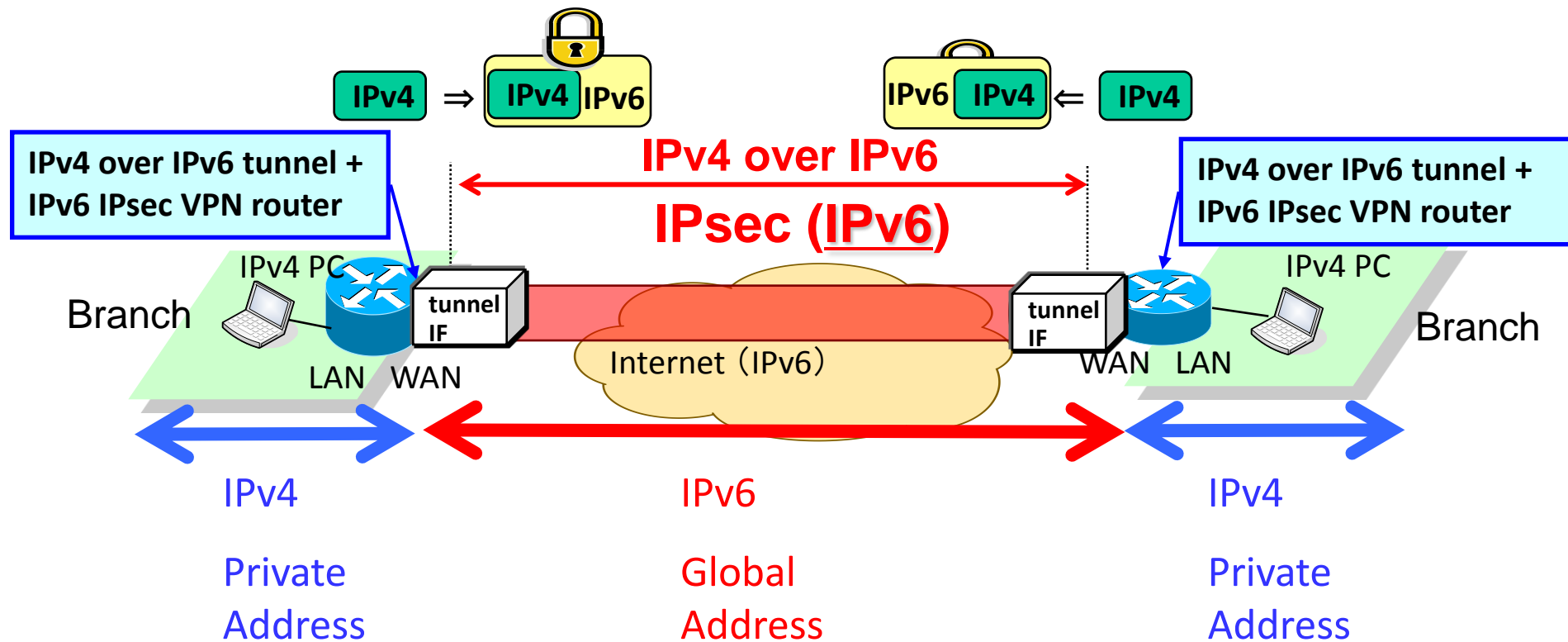
- How can enterprise users add new branches with IPsec VPN after IPv4 global address exhaustion ?



# D: IPsec VPN Connection (cont.)

## Solution: Tunneling (IPv4 over IPv6) + IPv6 IPsec

- Encapsulate IPv4 Packet with IPv6, and Encrypt IPv6 IPsec



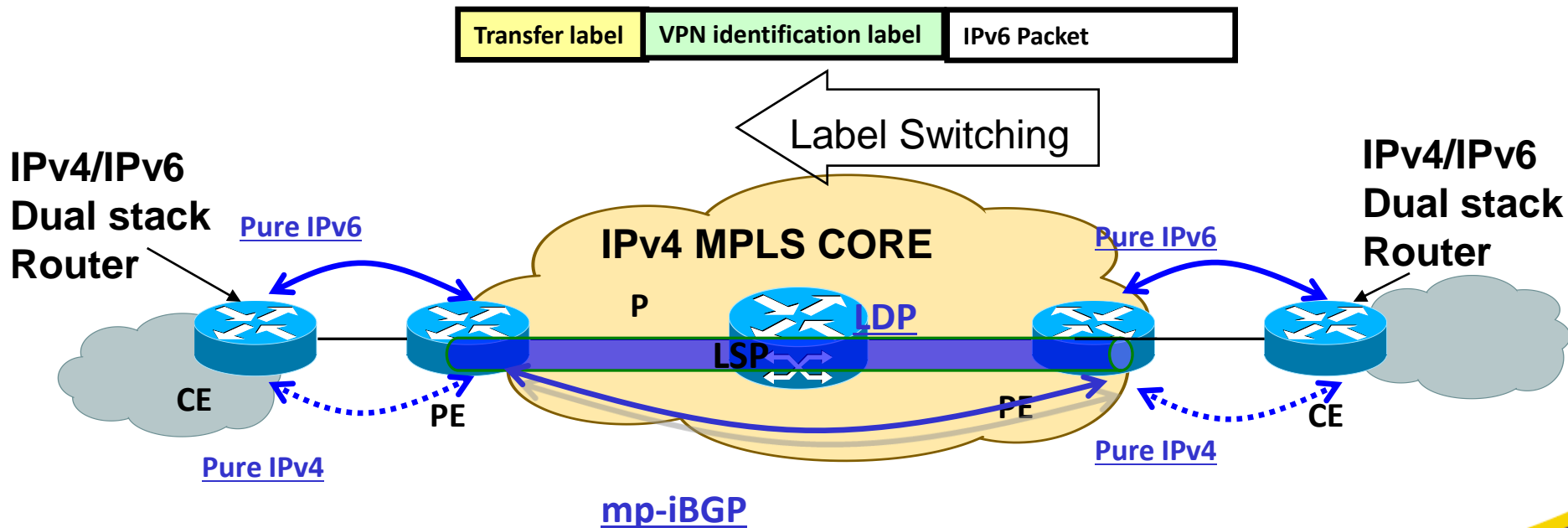
# E: IP-VPN / Layer 2 VPN connection

- IP-VPN / Layer 2 VPN connection for using IPv6-based applications
  - > solution: IPv6-supported VPN
    - in the future, there should be a lot of IPv6-based applications; so, enterprise will need IPv6-supported VPN
- IP-VPN
  - Requires IPv6 capable service since it's layer 3 aware service
  - “IPv6 over IPv4 tunneling” could help when the service provider doesn't support IPv6
- Layer 2 VPN
  - Layer 3 and above doesn't matter
  - Key device is Customer Premises
  - Exception: MLD snooping
- Leased Line
  - Key device is Customer Premises

# E': Model of IPv6 capable IP-VPN

## 6VPE model

- RFC 4659 (2006)
- Only upgrade of edge routers (OS) are required.
- MPLS core devices are NOT affected for IPv6 adoption
- No regression in throughput (different from IPv6 over IPv4 tunneling)
- MPLS technologies such as Fast Re-Route are NOT affected



\* NTT Com “Arcstar IP-VPN IPv6 Dual” uses this mechanism

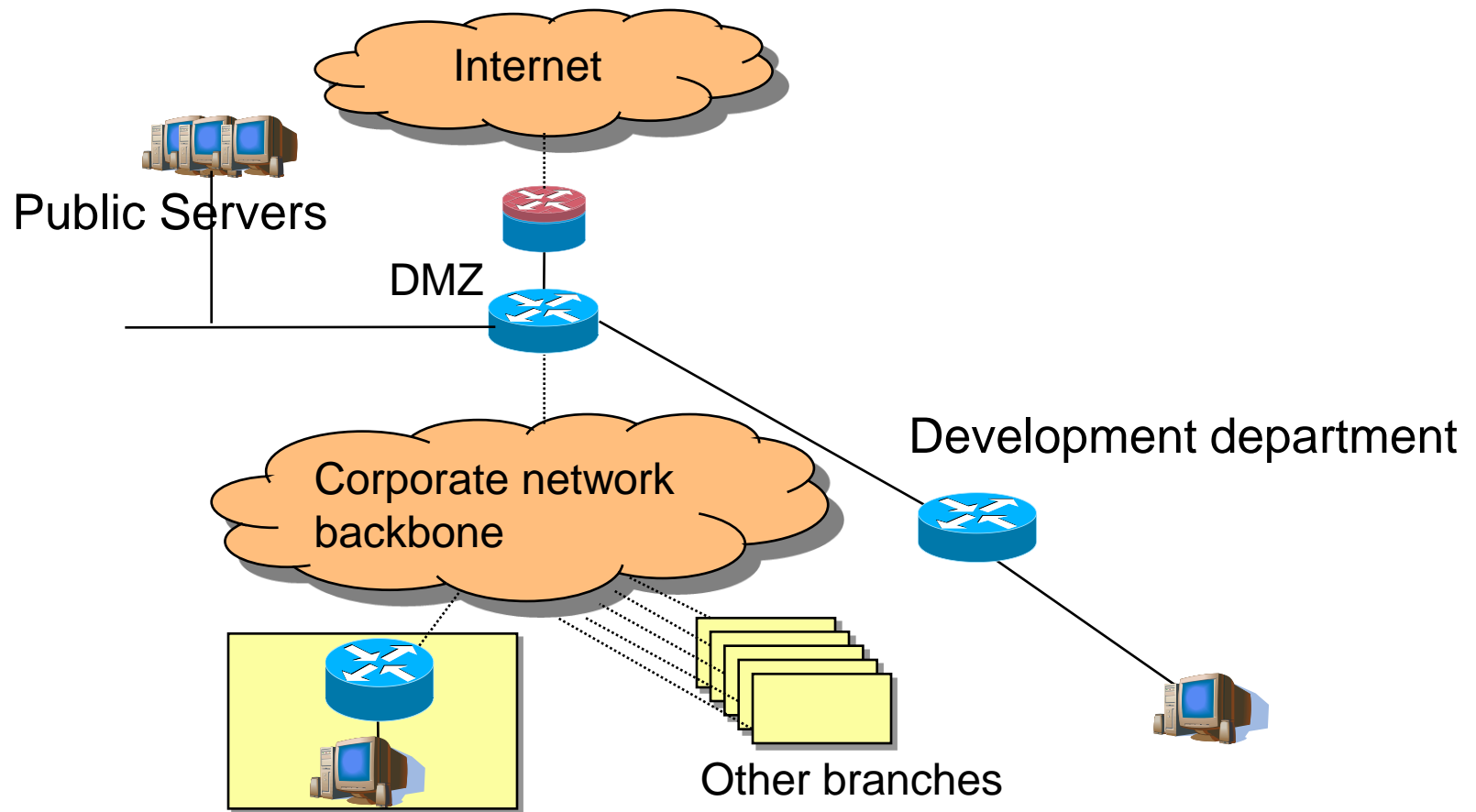
# Issues

# Issues

- Implementation of easy Multi-homing
  - BGP multi-homing is tough for small and medium enterprise customers
  - NAT multi-homing using famous appliances such as linkproof and isurf is popular; however, NAT66 hasn't standardized yet.
- Addressing for closed Network
  - When using ULA (Unique local address; FD00::/8), designers tend to choose easily memorable address; however, ULA MUST be generated with a pseudo-random algorithm according to RFC4193
  - ULA-central (FC00::/8) is not available, yet
- Firewall: immature
  - Management functions, such as logging, may not be sufficient yet
  - Performance may not be sufficient. Especially, IPv6 has extension header, and they are processed by Software, that causes low performance.
  - Transparent firewall may not work yet
  - Redundancy might not work well, yet
  - So, firewall function is usually implemented with packet filtering of routers.
- Operation System (OpS), Network Management System
  - Making enterprise OpS and NMS IPv6-capable might be costly
- Management of address assignment for clients
  - RA itself is OK, but different management from IPv4 only NW may be necessary
  - Sometimes, RA without intention happens.

# Case Study

# Case of XYZ Corporation





# Case of XYZ Corporation (cont.)

- **Inquiries:**
  - IPv4 exhaustion must come, but what impacts would they have?
    - We explained slide #11 “Impacts of IPv4 Address Exhaustion for Enterprise Networks”
- **Requirements:**
  - They wanted to achieve the same activities with IPv6 as they did with IPv4.
  - They required that public servers can be accessed by IPv6.
  - In addition to corporate backbone, their development department wanted another connectivity for evaluation and testing IPv6.

# Case of XYZ Corporation (cont.)

## **A: External connectivity - for IPv6 Internet connection**

### Solutions:

Tunnel	Native (IPv6 only)	IPv6 / IPv4 Dual Stack
--------	--------------------	------------------------

- This customer was most sensitive to the price
  - We offered “Tunnel” service for business (around \$100/month) for existing network
  - For development department, we offered another cheap FTTH connectivity (Flets: about \$70/month) with cheap Tunnel service called “OCN IPv6” (\$3/month) in order not to affect existing network.

# Case of XYZ Corporation (cont.)

## **B: Public servers**

**- for incoming access from external IPv6-only users**

Solutions:

- a. Use v6 to v4 translation box, such as 64 Server Load Balancer (translate IPv6 access into IPv4) and reverse proxy
  - b. Make the servers IPv6 capable (Dual stack)
- This customer didn't want to make any change in servers
    - We offered v6 to v4 Server Load Balancer
    - Attention:
      - Translators have difficulty in handling embedded IP addresses in payload (e.g. HTML documents). Therefore, checking and test or modification for contents was required.

# Case of XYZ Corporation (cont.)

## **C: GW (proxy)**

**- for outgoing access to external IPv6-only servers**

2 solutions:

- a. Use translators, such as proxy servers, for IPv6 external contents
  - b. Implement IPv6 (Dual stack) in enterprise network including PCs
- 
- This customer didn't want to make any changes in enterprise network including PCs
    - We offered proxy server
    - Attention:
      - Regarding proxy server, many of open source softwares have already supported IPv6; while, appliance products try to support IPv6 now.

# Case of XYZ Corporation (cont.)

## **D: IPsec VPN connection**

**- for additional Internet VPN (IPsec VPN) edge sites**

## **E: IP-VPN/ Layer 2 VPN connection**

**- for using IPv6-based applications**

- Check Point D and E were out of scope for this customer

## **Another motivation to use IPv6 for VPN:**

- Some of other customers want to merge branches.
- In this case, IPv4 private address sometimes overlap.
- Using NAT boxes can solve this problem, even though it will make complicated network and can't ping to nodes beyond NAT.
- In this case, we recommend to use IPv6, which introduce future-ready network, clear view on the network with IPv6 flat addressing, and IPv6 multicast supported network.

# Conclusion

- IPv4 address exhaustion has large impacts on enterprise network
  - IPv4 address exhaustion affects not only the company setting up new network, but also the one having their existing IPv4 network
  - IT Cycle, from planning to implementation may take approximately 2 years; consequently, enterprise users should consider IPv6 deployment right now.
- Remaining Issues
  - Keep your eyes on remaining issues
- 5 Check Points in IPv6 Adoption Plan for Enterprise Networks
  - ISPs and System Integrators can support enterprise customers' IPv6 adoption plan by consideration of the 5 check points.

# Thank you for your attention



*Thank you for your attention*

謝謝

[http://www.v6.ntt.net/index\\_e.html](http://www.v6.ntt.net/index_e.html)