Securing Server on IPv6 Environment

Shin Shirahata <shin@clara.ad.jp>
Clara Online, Inc.

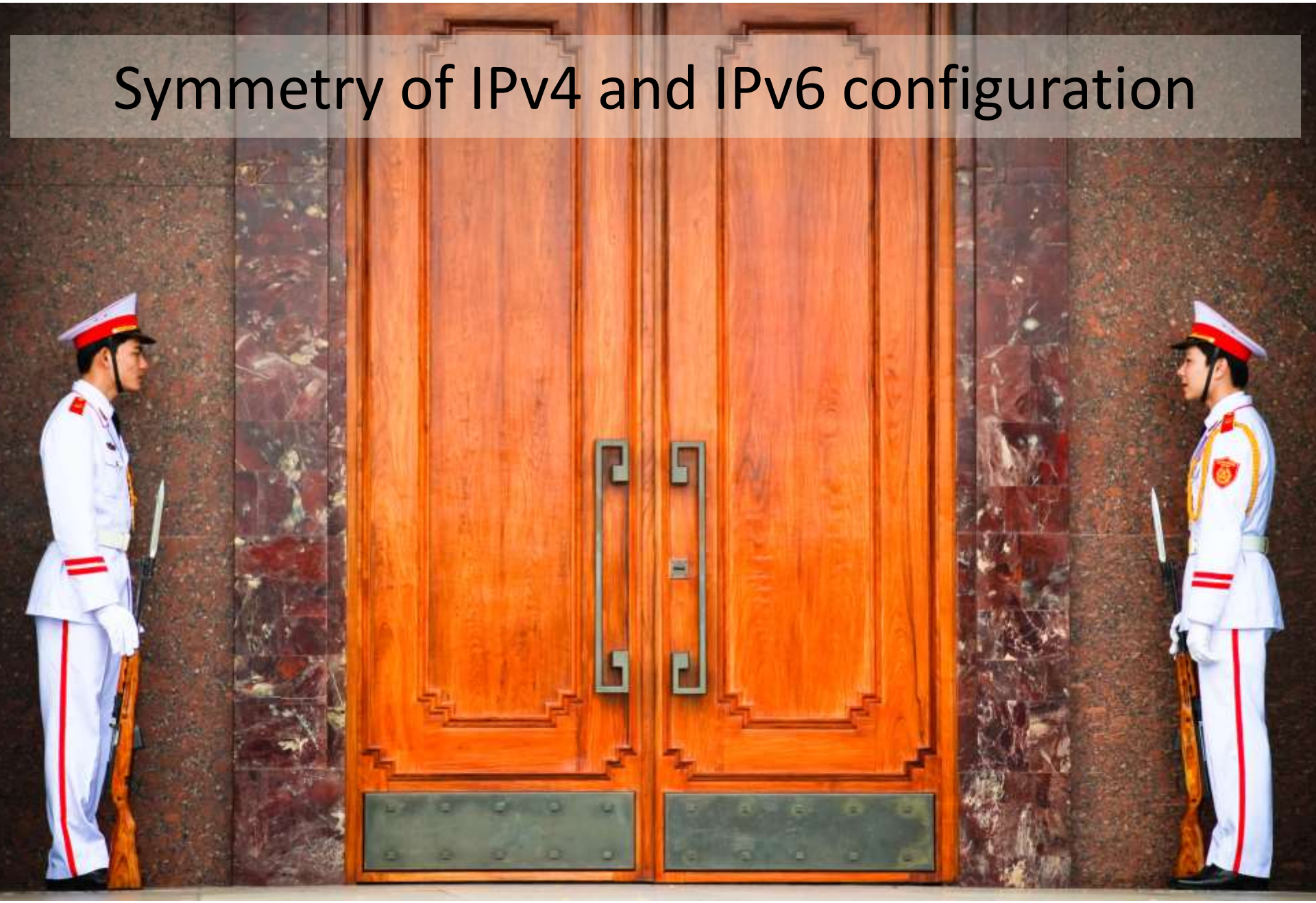
Agenda

- Design principle of dual stack environment
  - Protect IPv6 service as well as IPv4 service
- IPv6 security in Fundamental services
  - IPv6 socket implementation
  - Configuration
- IPv6 Specific issues
  - Privacy Extension
- Quality of protocol stack
  - Operational consideration from statics

DESIGN PRINCIPLE OF DUAL STACK ENVIRONMENT

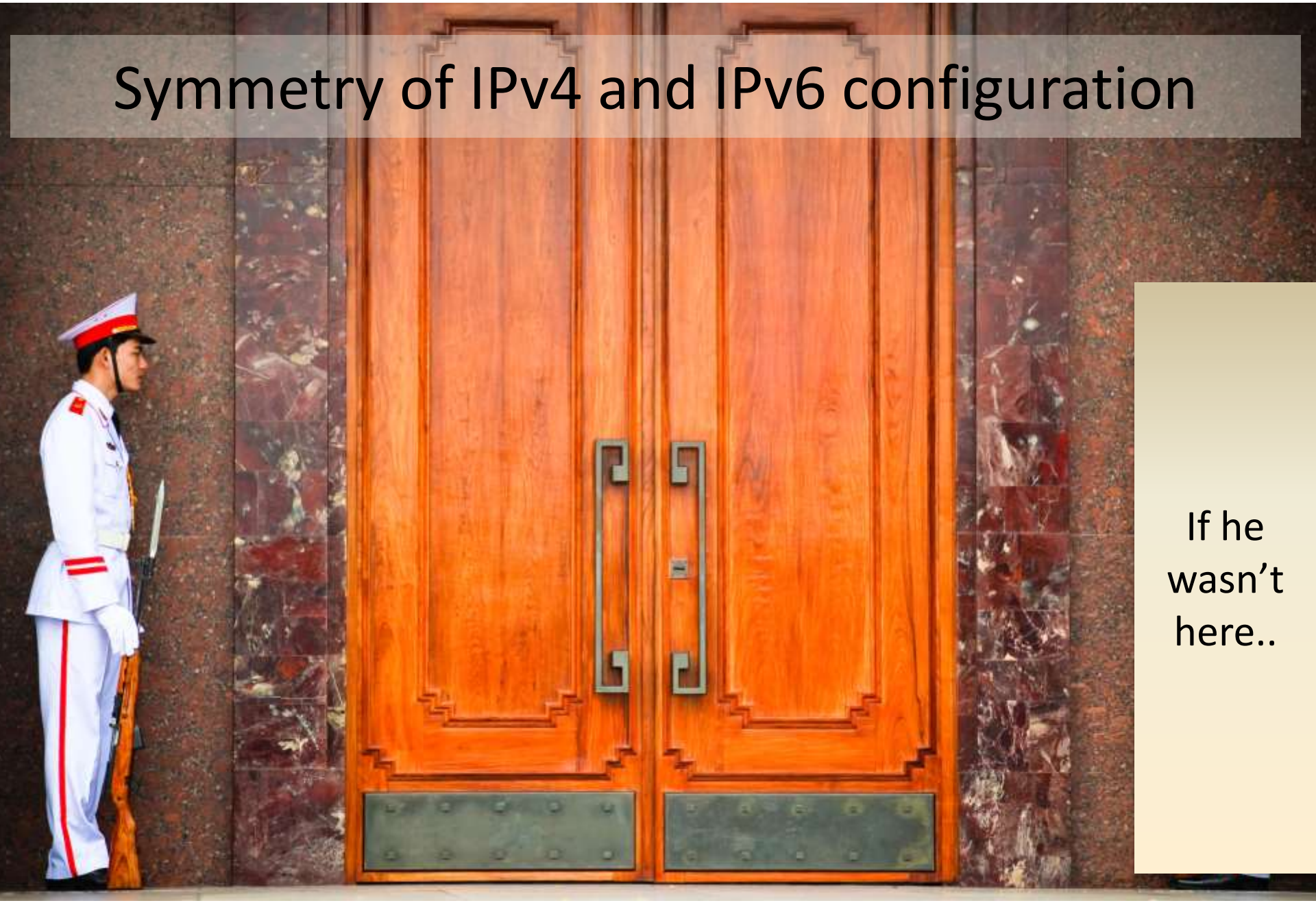
$IPV6_SECURITY_LEVEL = $IPV4_SECURITY_LEVEL (?)

Symmetry of IPv4 and IPv6 configuration



Ho Chi Minh Mausoleum, Hanoi, Vietnem
http://www.flickr.com/photos/aftab/4625751380/

Symmetry of IPv4 and IPv6 configuration



If he wasn't here..

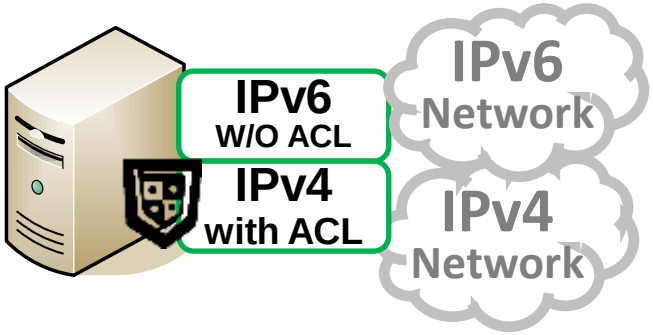
Ho Chi Minh Mausoleum, Hanoi, Vietnem
http://www.flickr.com/photos/aftab/4625751380/

Symmetry of IPv4 and IPv6 configuration

- When service is running on IPv4/IPv6 dual stack, same security level should be implemented on both protocols.
- Example : IPv4 connection is protected by IPS, but IPv6 isn't protected since IPS does not support IPv6.

→Need to confirm IPv6 support status of Firewall, IDS, IPS and Anti-Virus

  - In some equipment, IPv6 feature is not rich as IPv4 feature (e.g. Session sync feature is not possible in HA configuration)



DNS

WWW

Mail

IPV6 SECURITY IN FUNDAMENTAL SERVICES

Assumption

- I assume that you're using RHEL/CentOS 6.
  - Basic concept is also applicable for other operating systems.

Operating System

- Use static address configuration.
  - Do not use SLAAC (Stateless Address Auto Configuration) and DHCPv6 on servers!
  - In case of a server replacement, MAC address of NIC will be altered. It causes IPv6 address changes on auto configuration.4

/etc/sysconfig/network

```
NETWORKING_IPV6=yes
IPV6_DEFAULTGW=<IPv6 Gateway Address>
IPV6FORWARDING=no (default: no)
IPV6_AUTOTUNNEL=no (default: no)
```

/etc/sysconfig/network-scripts/ifcfg-eth<$NUMBER>

```
IPV6INIT=yes
IPV6ADDR=<IPv6 Address>
IPV6_AUTOCONF=no (default: yes if IPV6FORWARDING=no)
IPV6_AUTOTUNNEL=no (default: no)
```

Dirty Hack: Set MTU to 1280

/etc/sysconfig/network-scripts/ifcfg-eth<$NUMBER>

```
MTU=1280
```

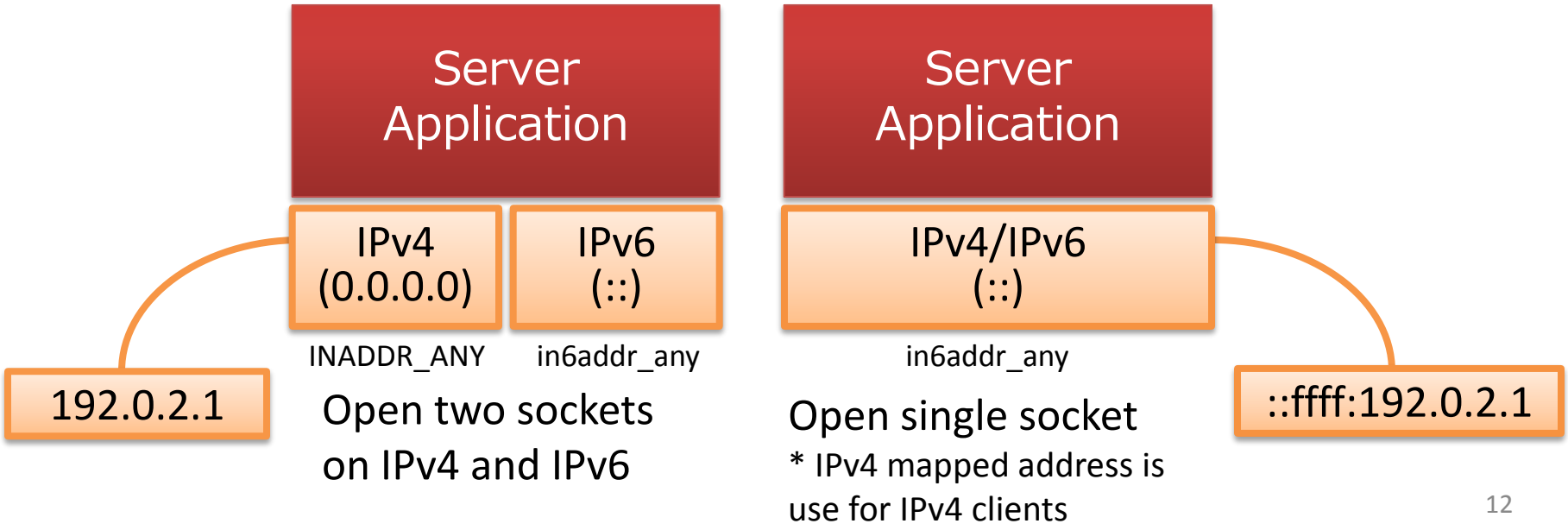
- Why set MTU to 1280
  - Theoretically…

> "IPv6 nodes **SHOULD** implement Path MTU Discovery in order to discover and take advantage of paths with PMTU greater than the IPv6 minimum link MTU."
> RFC 1981: Path MTU Discovery for IPv6

  - But actually it's ***doesn't works*** on significant number of IPv6 network.
    - IPv6 over IPv4 tunnels – MTU is smaller than 1500
    - Site that filters ICMPv6 traffic – Path MTU discovery couldn't be works.
  - 1280 is a minimum MTU of IPv6 network.
    - You avoid reachability issue and save the time for troubleshooting regarding to Path MTU
    - It brings small performance degradation in compare to 1500 or more larger MTU value.

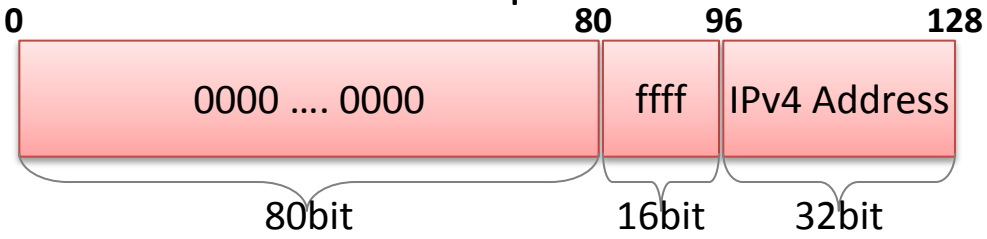
Understanding IPv6 server application and it's socket implementation

- There is a two way to implement IPv4/IPv6 dual stack server
  - Depends on a implementation of OS, server software, and configuration.
  - It is better to know which way is used to the server software.
  - In some cases, different address syntax should be used.



What is IPv4 Mapped address?

- IPv4 Mapped Address:
  - Special IPv6 address that represents IPv4 address



  - E.g. 192.0.2.128
    "::ffff:192.0.2.128" or "::ffff:c000:280"
  - It will be used by IPv4/IPv6 dual stack application with IPv6 sockets ("::") that communicate with IPv4-only node.
    - Limited to use within a node.
    - It will not be used as source and destination address in packets

Socket setting is configurable in some server software
Example: OpenSSH

Recommended

- Two different sockets are bind(2)ed on IPv4 and IPv6.

```
Result of "netstat -an" command:
tcp    0 0 0.0.0.0:22                0.0.0.0:*                   LISTEN
tcp    0 0 :::22                     :::*                        LISTEN
```

Configuration in /etc/ssh/sshd_config
ListenAddress 0.0.0.0
ListenAddress ::

- Sockets is bind(2)ed on IPv6 only

```
Result of "netstat -an" command:
tcp    0 0 :::22                     :::*                        LISTEN
```

Configuration in /etc/ssh/
ListenAddress ::

Default configuration on RHEL6.4

(As of 2013-Apr-20)

Name	Feature	RPM Package	IPv6		IPv4	Remarks
			Dual Stack	IPv6 Only		
Apache	Web Server	httpd-2.2.15-26.el6	X			
BIND	DNS Server	bind-9.8.2-0.17.rc1.el6_4.4		X	X	
postfix	SMTP Server	postfix-2.6.6-2.2.el6_1		X	X	
Dovecot	POP3/IMAP Server	dovecot-2.0.9-5.el6		X	X	
OpenSSH	SSH Server	openssh-5.3p1-84.1.el6		X	X	
ntpd	NTP Server	ntp-4.2.4p8-3.el6		X	X	
vsftpd	FTP Server	vsftpd-2.2.2-11.el6_4.1			X	default
				X		/etc/vsftpd/vsftpd.conf: enable “listen_ipv6=YES” and disable “listen=YES“
xinetd	Super server	xinetd-2.3.14-38.el6	X			

DNS

- BIND 9.8 on RHEL/CentOS 6
  - IPv6 is enabled by default, but query is limited from localhost

/etc/named.conf

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
}
```

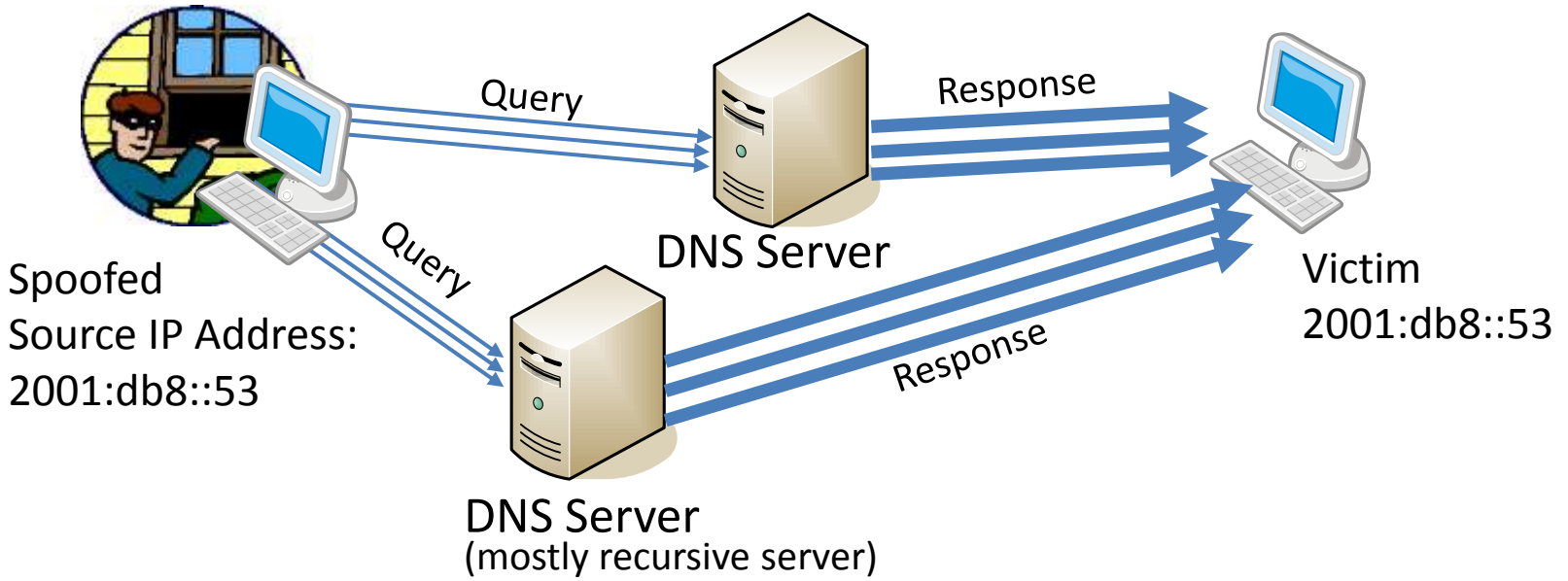
↓

```
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { any; };
}
```

…. Or specified IPv6 global address.

DNS Reflection Attack

(also known as DNS Amplifier Attack)



*"The DDoS is perpetrated via open DNS resolvers using a **DNS reflection attack**. The current volume of the DDoS is reported to be quite large, topping 140Gbps in some instances, while other reports suggest it may have been as **high as 300+ Gbps.** "*

Cisco Blog - Chronology of a DDoS: SpamHaus
http://blogs.cisco.com/security/chronology-of-a-ddos-spamhaus/

What is Open Resolver

- Cache DNS server that does NOT implement proper access control
  - Could be abused for DNS amplification attacks
  - Note: Some provider offers Open Resolver publicly (e.g. Google Public DNS and OpenDNS), but they implements a rate limiting to mitigates an attack.

- Typical configuration issue
  - Cache DNS feature is unintentionally enabled when Authoritative DNS was installed.
  - Authoritative DNS is not separated from Cache DNS server
  - Broadband router that answer DNS query from WAN Interface

What is the problem?

- DNS server became an attacker thoughtlessly.
- To prevent DNS amplification attacks:

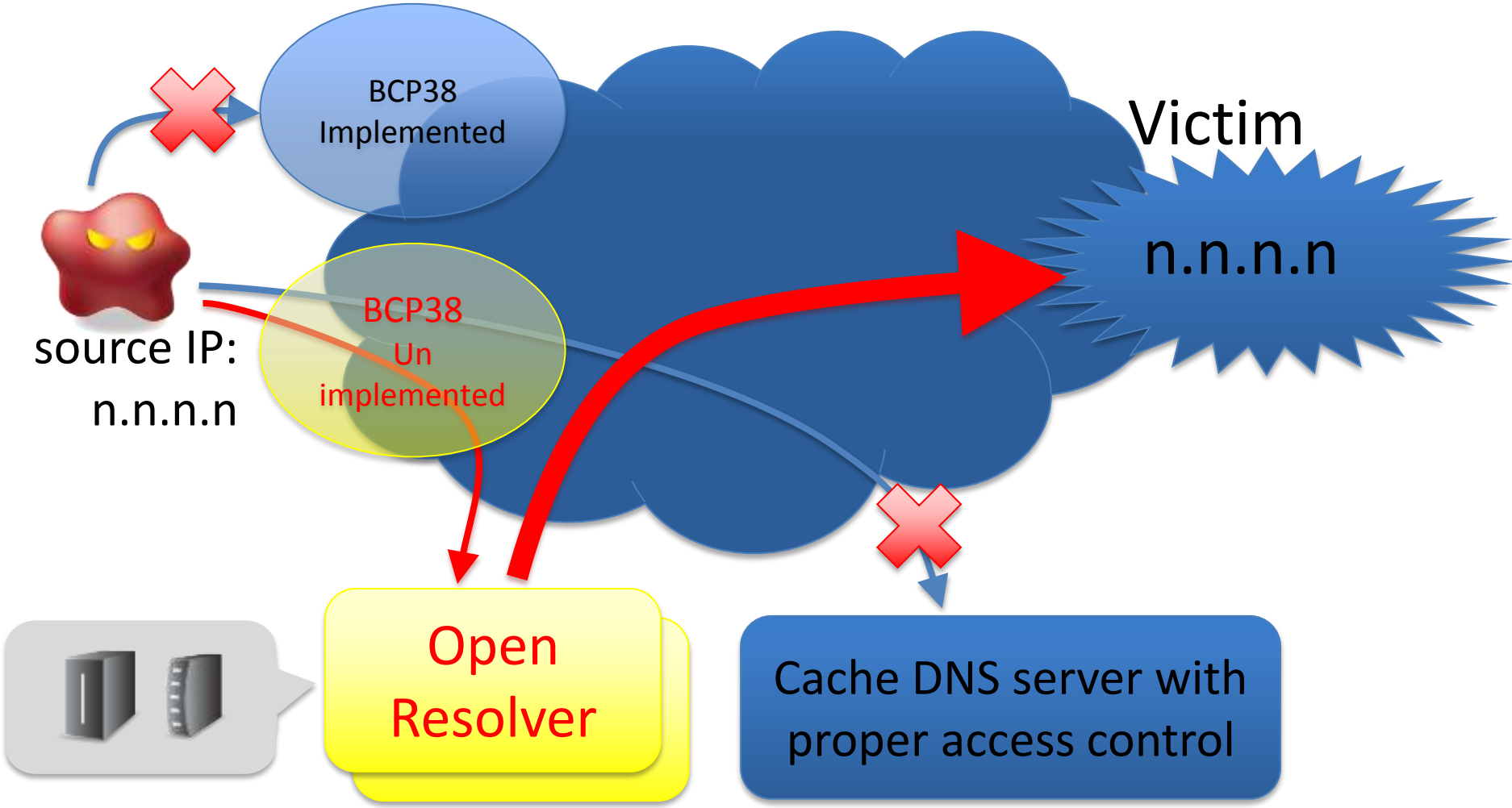
Countermeasure against
Open Resolver

and

BCP38

- Both countermeasures are needed.

Mechanism of DNS amplification attacks



Recursive DNS server

- Separate Recursive DNS server from Authoritative server
  - Or use “views” feature in BIND
- Limit a client IPv4/IPv6 address block for recursion
  - Prevent to used by third party

```
options {
        recursion yes;
        allow-recursion {
                127.0.0.1/32;
                ::1/128;
                192.0.2.0/24;
                2001:db8:cafe::/48;
        };
};
```

←Client's IPv4/IPv6 address block

Response Rate Limiting

- limiting the rate of responses by a DNS server in order to blunt the impact of DNS reflection and amplification attack
- Note: This feature is included on bind-9.8.2-0.17.rc1.el6.3 or later version. Please confirm that bind package is up-to-date.
- bind-9.8.2-0.17.rc1.**el6_4.4** is a latest version as of 2013-Apr-20

```
options {
        rate-limit {
                responses-per-second 5;
                window 5;
        ;
};
```

WWW

- Apache
  - IPv6 is enabled by default - no special configuration is needed.
    - IPv4 is supported by IPv4 mapped address.

```
Listen 80
```

  - To serve a different content by protocol, or take a log in separate file, set up a virtual host for IPv4 and IPv6.

VirtualHost for IPv4

```
<VirtualHost 192.0.2.1:80>
 ServerName ipv4.example.vn
 DocumentRoot /var/www/html/ipv4
...
</VirtualHost>
```

VirtualHost for IPv6

```
<VirtualHost [2001:db8:cafe:6::80]:80>
 ServerName ipv6.example.vn
 DocumentRoot /var/www/html/ipv6
...
</VirtualHost>
```

Tips: IPv6 address syntax in configuration

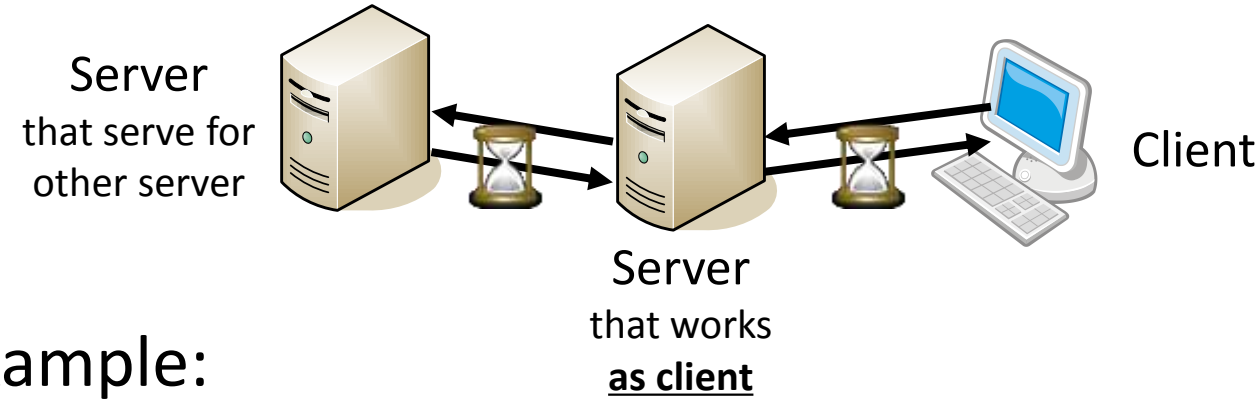
- IPv6 address syntax may vary according to software or configuration part.
  - Example: Apache
    - In VirtualHost configuration, bracket ('['and ']') are needed for IPv6 address.

```
<VirtualHost [2001:db8:cafe:6::80]:80>
ServerName ipv6.example.vn
DocumentRoot /var/www/html/ipv6
...
</VirtualHost>
```

    - No bracket is needed to specify IPv6 address to configure ACL.

```
<Directory "/var/www/html/ipv6/">
Order deny,allow
Deny from all
Allow from 127.0.0.1/32 ::1/128 2001:db8:cafe:1::/64
</Directory>
```

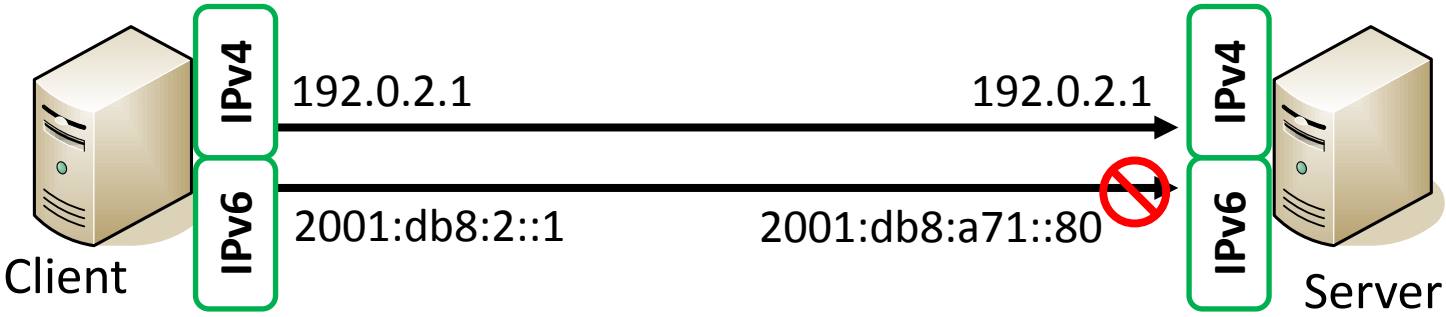
A Server is a Client (sometimes)



- Example:
  - DNS Cache server is works as DNS resolver (client)
  - HTTP Proxy server is works as a HTTP client
  - SMTP Server is works as a SMTP Client to connect other server

Problem of a client part of communication may be a issue of the server

Case: Web API



- Web API HTTP server
  - Originally, a Web API server supports IPv4 only.
    - Access control was properly implemented on IPv4.
  - When the Web API server started IPv6 support, client couldn't connect the server.
    - Access control on IPv6 wasn't configured properly.

SMTP

- Postfix
  - postfix-2.6.6-2.2.el6_1
  - IPv6 is enabled by default
    - But connection is accepted only from localhost

/etc/postfix/main.cf

```
inet_protocols = all
```

```
inet_interfaces = localhost
```

↓

```
inet_interfaces = all
```

DNSBL and IPv6

- If blacklisted...
  - On IPv4 DNSBL, single IP (=/32) was blacklisted in common case. Some aggressive DNSBL listed /24 or more largeer address blocks.
  - On IPv6 era, /64 is a minimum choice because /128 is not suitable for identify malicious client (e.g. Privacy Extension)
- Spamhaus, major DNSBL operator says:

IPv6 Blocklist minimum range
"Based on how we view the specifications for allocation of IPv6 addresses, all Spamhaus blocklists will list IPv6 ranges no smaller than a /64.“

Spamhaus IPv6 Blocklists Strategy Statement
http://www.spamhaus.org/organization/statement/12/

Strategy for traceback

- With IPv6 auto-configuration, traceback is a tough process.
  - Its difficult to find what IPv6 address were used before without having a MAC address and IPv6 address mapping record.
- Solution: Record an IPv6 address usage
  - Monitoring NDP entries
    - NDPMon http://ndpmon.sourceforge.net/
    - NDPMon also maintains up-to-date a list of neighbors on the link and watches all advertisements and changes. It permits to track the usage of cryptographically generated interface identifiers or temporary global addresses
  - Use Stateful DHCPv6
    - Stateful DHCPv6 gives more control over exact address assignment ; DHCPv6 server have a client information including DHCP Unique Identifier (DUID; which includes link layer address), Identity Association for Prefix Delegation (IA_PDs), prefixes, and preferred and valid lifetimes.
    - Note: DHCPv6 is supported since Windows Vista, but free DHCPv6 client called "Dibbler" could be used for Windows XP/2003 platforms. http://klub.com.pl/dhcpv6/#DOWNLOAD

Sender Policy Framework (SPF)

- E-mail's sender validation system
  - SPF allows administrators to specify which hosts or networks are allowed to send mail from a given domain by SPF (or TXT) record
- Some mechanisms in SPF records are protocol depend parameter.
  - If you are publishing SPF record and supports IPv6 on mail server, don't forget to specify IPv6 related setting.

mechanisms	
A	If the domain name has an address record (A or **AAAA**) that can be resolved to the sender's address, it will match.
IP4	If the sender is in a given IPv4 address range, match.
IP6	If the sender is in a given **IPv6 address range**, match.

Source: http://en.wikipedia.org/wiki/Sender_Policy_Framework

Example of SPF record

- Example: iij.ad.jp

```
% dig txt iij.ad.jp
(snip)
;; ANSWER SECTION:
iij.ad.jp.          3600    IN      TXT     "v=spf1 ip4:202.232.30.145 ip4:202.232.30.71
ip4:210.138.145.126 ip4:210.148.162.32/28 ip4:210.148.162.48 ip4:202.32.219.46
ip4:210.138.175.224/28  include:v6spf.iij.ad.jp  -all“
;; MSG SIZE  rcvd: 340
```

```
v6spf.iij.ad.jp.        3600    IN      TXT     "v=spf1 ip6:2001:240:11e:6000::1:145
      ip6:2001:240:11e:6300::1:71 ip6:2001:240:bb42:8010::1:126
      ip6:2001:240:bb41:8003::1:46 ~all“
;; MSG SIZE  rcvd: 299
```

POP3 and IMAP

- Dovecot
  - IPv6 is Enabled by default
  - If you are still using POP before SMTP, please make sure that is supporting IPv4 address.
    - As far as I know, most of the implementation doesn't support IPv6 or IPv4-mapped address by default . Need to update regexp in the code.
    - Its better to use SMTP AUTH since deployment of NAT may cause security issue.

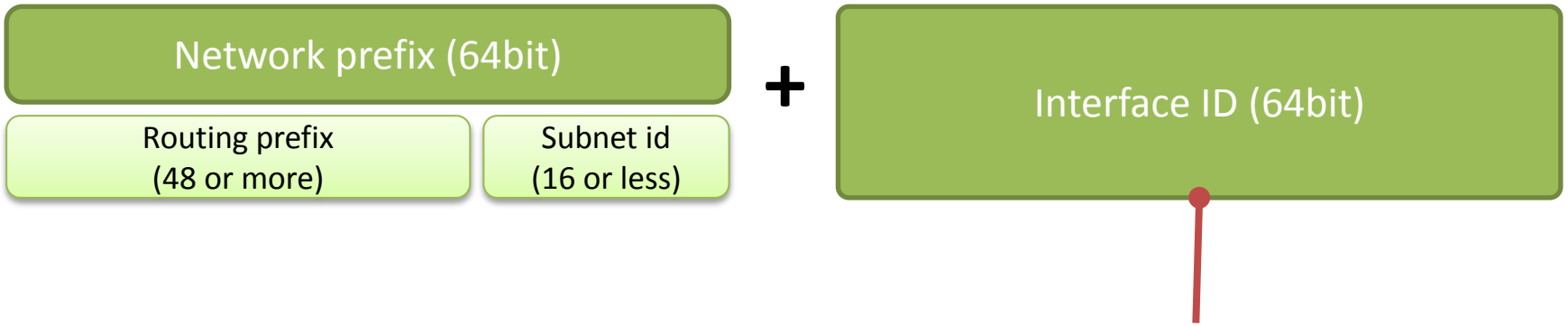
Conclusion

- Major service on CentOS6 is supports IPv6 by default.
- It is strongly suggested to use recent version for feature enhancement for IPv6 and bug fix.

IPV6 SPECIFIC ISSUES

Privacy Extensions and its issue

IPv6 address assignment via SLAAC



- Background
  - Static MAC address gives a opportunity to **track user equipment across time** and network prefix.
  - E.g. Someone knows the interface ID of the my laptop at this conference network, an he/she can track my laptop by observing the interface ID in another place.

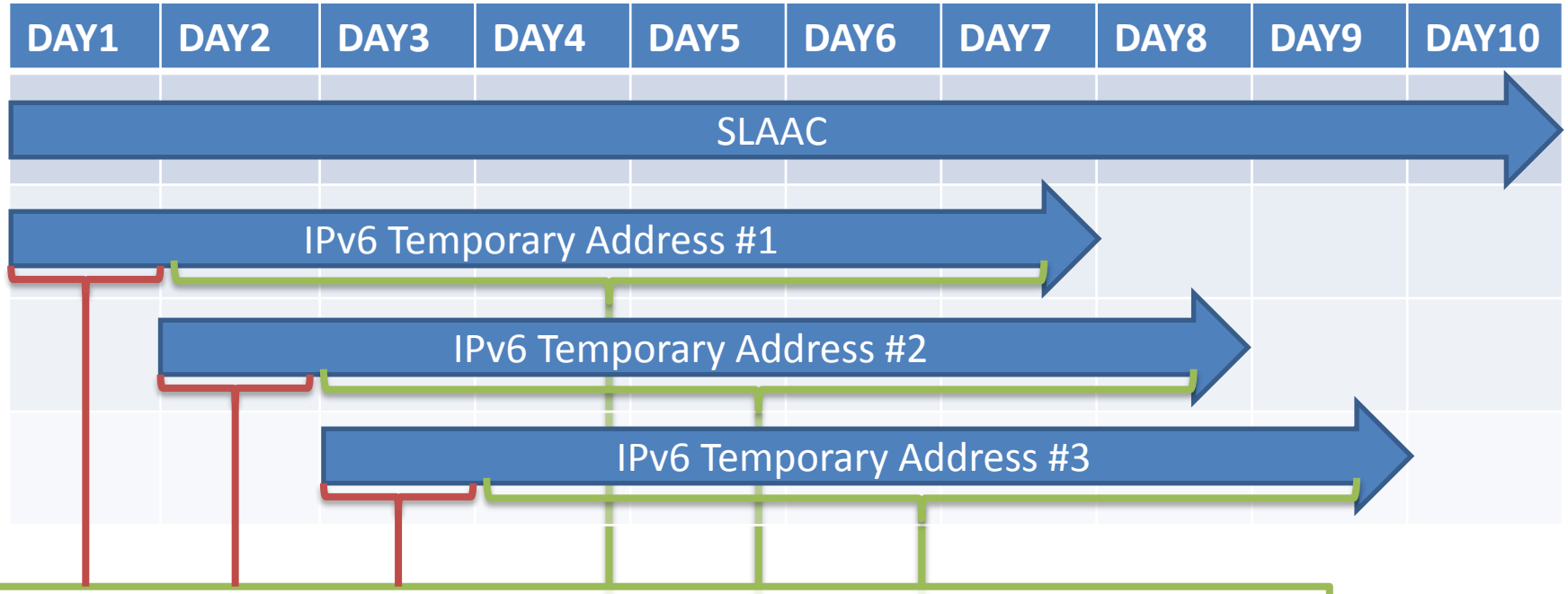
Privacy Extensions and its issue

RFC4941 : Privacy Extensions for Stateless Address Autoconfiguration in IPv6
*"Use of the extension causes nodes to generate global scope addresses from interface identifiers that **change over time** …"*

  - Most of IPv6 stacks enables privacy extension by default
    - Windows Vista or later, Mac OS X Lion or late
    - Note: Privacy extension doesn't work on static address configuration
- If the same clients access to a server, the source IPv6 address will never be the same.

  →It makes difficult to track the equipment by IPv6 address
  - A Network prefix (usually /64) will remain same, so it can be used for tracking.

Temporary addresses and its lifetime



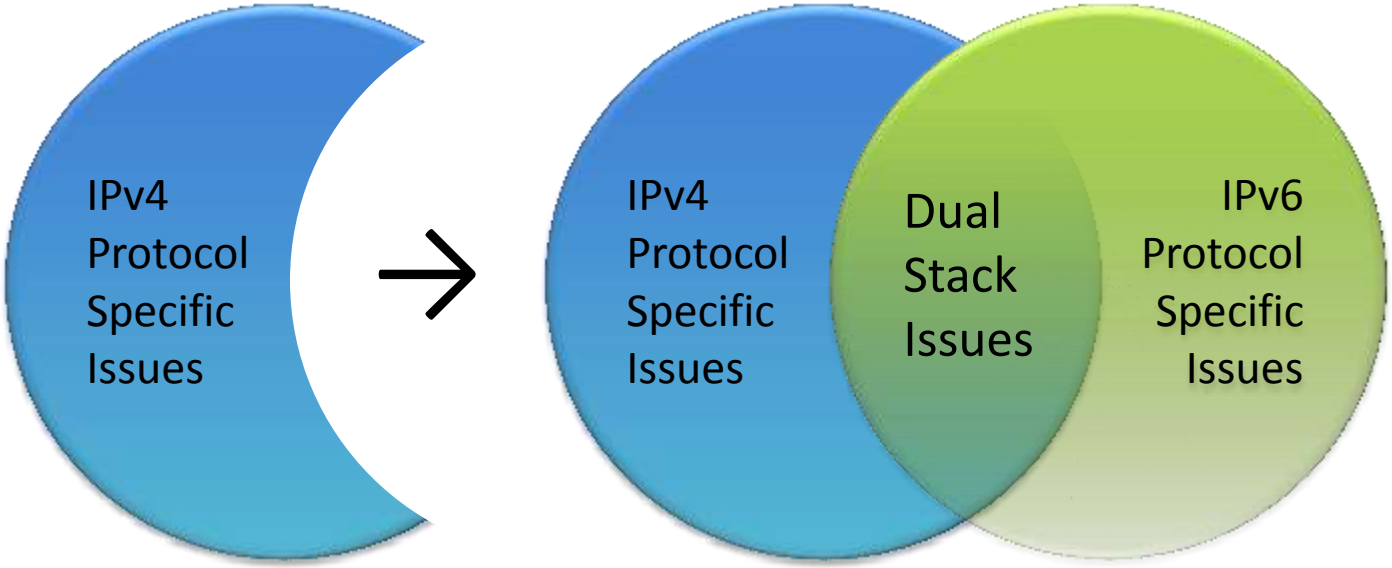
Temporary addresses is used as **source address** for originating connections

Not used for originating connections

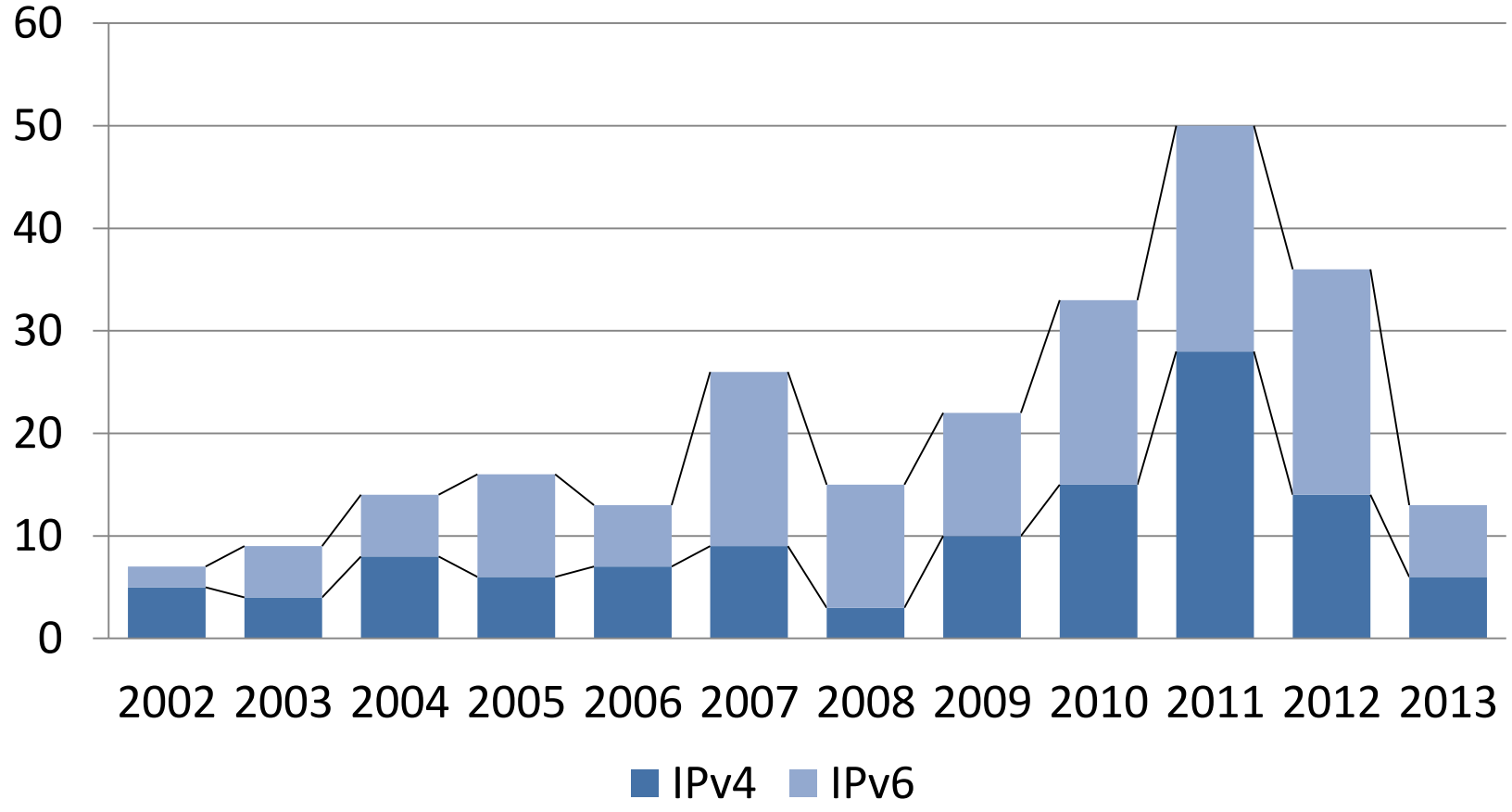
AN INCONVENIENT TRUTH OF DUAL STACK

Quality of implementation

- IPv6 protocol stack has not reach equal maturity as IPv4
  - It has potential security holes



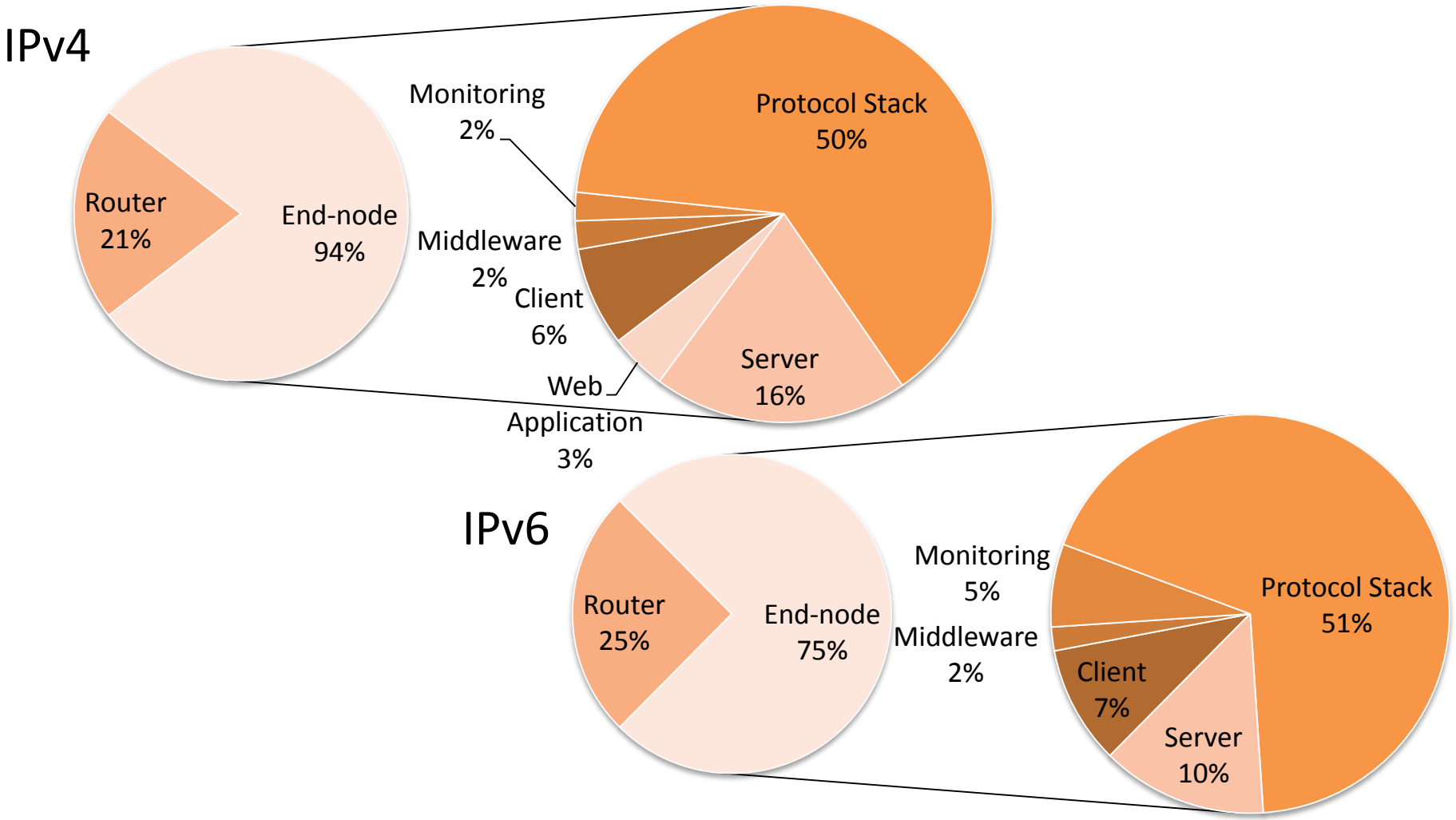
Number of IPv4/IPv6 Protocol specific vulnerability on CVE Database



Source: MITRE's CVE Database; Counted by Author

Need to care for IPv4+IPv6 security issue other than IPv4 only

Breakdown of the security hole



- Almost half of the issues are “protocol stack” related

Source: MITRE’s CVE Database 2002-2012; Counted by Author

IPv6 Specific security hole

- Defect of protocol specification
  - IPv6 Type 0 Routing Header Vulnerability (CVE-2007-2242)
  - → Fixed by RFC 5095 “Deprecation of Type 0 Routing Headers in IPv6”
- Defect of protocol implementation
  - IPv6 Neighbor Discovery Protocol Neighbor Solicitation Vulnerability (CVE-2008-2476)
- It does NOT means IPv6 is a unsecure protocol.
  - IPv4 protocol stack has a same history – In the past, very critical security holes were found in IPv4 protocol stack!
  - Examples: Ping of Death Attack (1996), Path MTU Discovery Attack (2004)

IPv4/IPv6 Dual Stack environment specific security hole

- CVE-2008-1153
  - Cisco IOS 12.1, 12.2, 12.3, and 12.4, with IPv4 UDP services and the IPv6 protocol enabled, allows remote attackers to cause a denial of service (device crash and possible blocked interface) via a crafted IPv6 packet to the device.
- CVE-2006-6263, CVE-2006-6266, CVE-2007-3038
  - Teredo clients, when source routing is enabled, recognize a Routing header in an encapsulated IPv6 packet and send the packet to the next hop, which might allow remote attackers to bypass policies of certain Internet gateways that drop all source-routed packets.
- CVE-2007-1338
  - The default configuration of the AirPort utility in Apple AirPort Extreme creates an IPv6 tunnel but does not enable the "Block incoming IPv6 connections" setting, which might allow remote attackers to bypass intended access restrictions by establishing IPv6 sessions that would have been rejected over IPv4.

Conclusion

- Keep up-to-date a software of a network equipment and servers
  - Migration from *Single* stack to *Dual* stack means almost double amount of risks.
- It’s better to use latest OS or software
  - Specifications are updated often in compare to IPv4. Older version couldn’t catch up them.

Summary

- Design principle of dual stack environment
  - Protect IPv6 service as well as IPv4 service
- IPv6 security in Fundamental services
  - IPv6 is enabled by default
  - How IPv6 socket is works
- IPv6 Specific issues
  - Concept of an IPv6 addressing is different from IPv4 - IPv6's /128 is not same meaning as IPv4's/32
- Quality of protocol stack