AlaxalA

Operational Issues in IPv6
— from vendors' point of view —

鈴木 伸介
SUZUKI, Shinsuke
< suz@alaxala.net>

ALAXALA Networks Corporation

1. Introduction
   - Introduction of ALAXALA
   - Dual Stack for the “Guaranteed Network”
2. IPv6-Specific Issues in Network Equipment
3. IPv6 Operational Issues in a Dual-stack Network System

Who is ALAXALA?

Established	2004 October 1st
Mission	High end, Mid range Router and Switches Development, Manufacturing, Sales, Maintenance &Support
Background	Joint Company : Hitachi Ltd., NEC corp., • Long term experiences on Carrier/ISP business • Core Technologies for Mission Critical Systems • **Many Experts and Experiences on IPv6 Area**

HITACHI

NEC

ALAXALA Product Line-up

- All of them support wire-rate IPv6 forwarding/filtering/QoS

AX2400S series

1U Layer2 Switch

10G

AX2430S-48T

AX2430S-24T2X

AX2430S-24T

AX2430S-48T2X

AX3600S series

1U Layer3 Switch

10G

AX3630S-24T2X

AX3630S-24T

AX3630S-24P

AX3630S-48T2XW

AX3630S-48TW

AX3630S-24S2XW

AX6300S series

Enterprise Backbone Switch

10G

AX6308S

AX6304S

AX6700S series

Terabit Switch

10G

AX6708S

AX5400S series

Carrier/ISP Backbone Switch

AX5404S

AX5402S

AX7800S series

Carrier/ISP Backbone Switch

10G

AX7816S

AX7808S

AX7804S

Switch

AX2000R series

Enterprise External Router

AX2002RX

AX2002R

AX2001R

AX7700R series

ISP Router

10G

AX7702R

AX7800R series

Carrier Router

10G

AX7816R

AX7808R

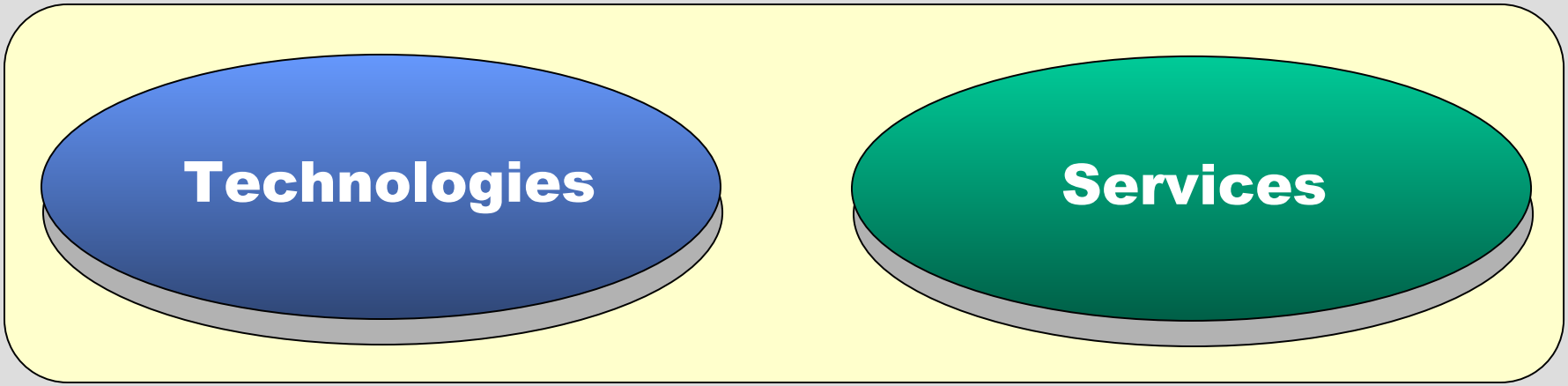
AX7804R

Router

ALAXALA's Philosophy

[Guaranteed Network]

- Contribute to the establishment of a society rich in information and telecommunications.
- Provide user-friendly and security-conscious networks for the customers all over the world.
- Highly Reliable, Stable, and Secure Guaranteed Networks in IP/Ethernet Environments.



IPv6 influence to the Guaranteed Network

To provide the Guaranteed IPv6 Network... ALAXALA

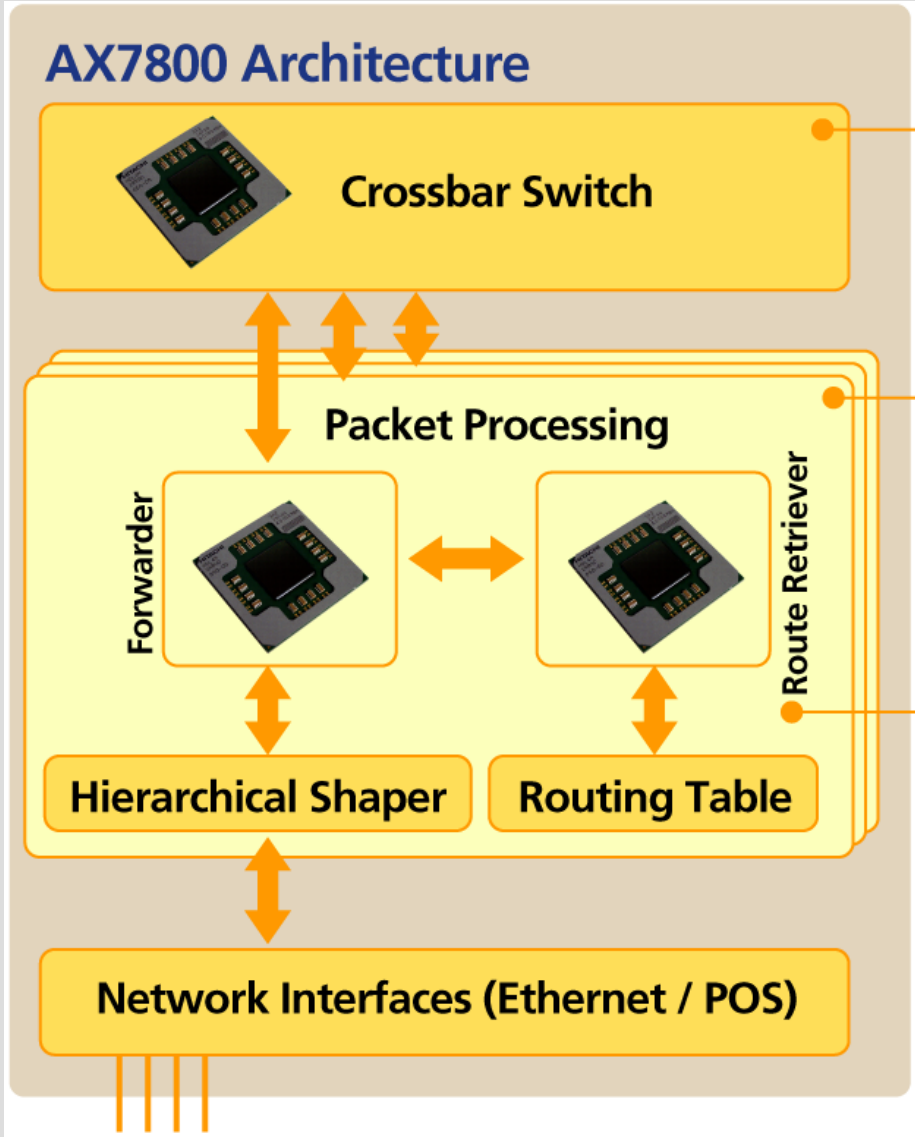
- IPv6 Forwarding Speed
  - Wire-rate packet forwarding over 10G-Ethernet
  - Very short latency : about 10 μ sec
- IPv6-aware ACL & QoS without performance degradation
  - Layer 2: MAC address, protocol, VLAN-ID (IEEE802.1q), User priority (IEEE802.1p)
  - Layer 3: Address, Protocol, Traffic class, …
  - Layer 4: TCP/UDP port number, TCP flags, ICMP(v6) type/code
  - Even in L2 forwarding, ACL and QoS can work based on L2, L3 & L4 rules
- Protocol Stability & Redundancy
  - IPv6 Protocol Line-up congruent to IPv4
    - routing protocol (rip, ospf, bgp, isis, pim …)
    - management protocol (telnet, ftp, ssh, snmp, …)
    - redundancy protocol (vrrp)
    - …
  - Stable IPv6 implementation based on KAME
- Small number of electronic components
  - (will be discussed later)

01-000280,01-000307

Treat IPv6 equally to IPv4 to provide a true dual-stack

Example. AX7800 Architecture

AlaxalA



IPv4/IPv6 symmetric design based on proprietary ASIC

- 320Gbps throughput
- Smaller Pin counts
- 1+1 Redundancy

Distributed Packet Processor

- Wire-speed Packet Forwarding
- Wire-speed Packet Filtering
- Classified QoS/Queuing

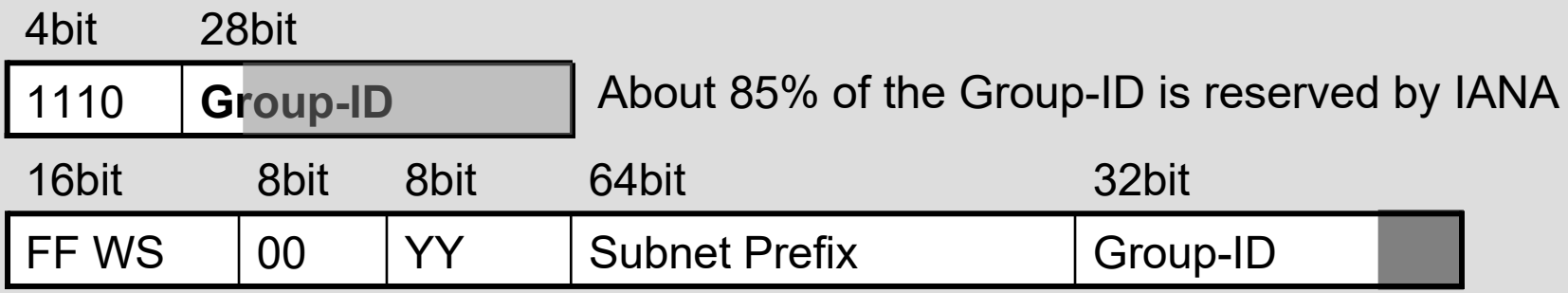
Single Engine for Multiple Forwarders

- 20Gbps/chip
- IPv6/v4 + Ethernet
- Filter/QoS

- Introduction
- IPv6-specific Issues in Network Equipment
  - Benefit of IPv6 from vendors' point of view
  - Hardware Issues
    - Number of FIB entries
    - Filtering Capabilities
    - Tunnel I/F
  - Software Issues
    - Link-local address handling
- IPv6 Operational Issues in a Dual-stack Network System

Benefit of IPv6 from vendors' point of view

- No NAT
  - Makes an implementation simpler
- Smaller number of routing entries
  - Although IPv6 address is 4times larger than IPv4, the aggregation efficiency still wins.
- Simpler automatic address allocation
  - DHCPv4(src=0.0.0.0,dst=255.255.255.255) has to be treated specially
  - No special treatment is required in IPv6, thanks to link-local address.
- Free from a solution to cope with address confliction
  - Private Address → Unique Local Address
  - Multicast Address → Unicast-Prefix-based Multicast Address



Number of FIB entries

- FIB = Forwarding Information Base
  - Information necessary to forward an incoming packet
  - FIB-search speed determines packet-forwarding speed
    - CAM (Contents-Addressable Memory) is adopted to store a FIB

2001:db8:1:2:3:9:8:9

2001:db8:1::/48	fe80::1	eth00
2001:db8:2::/48	fe80::2	eth01
...		

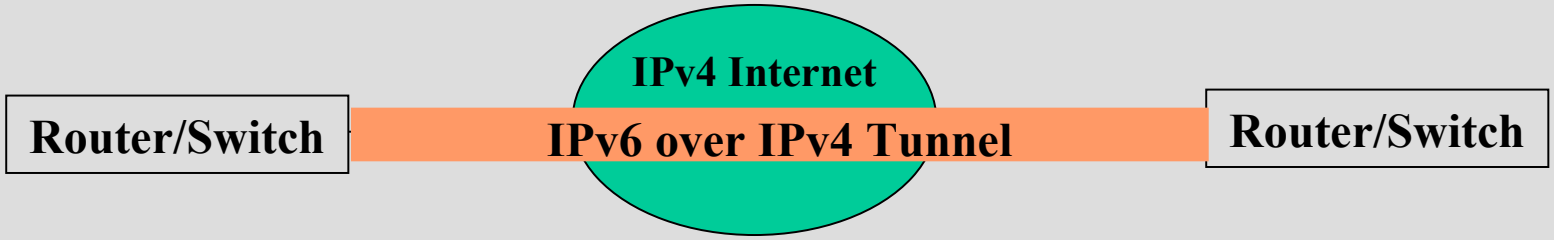
- CAM has too week points = cost & energy consumption
  - It is important to estimate the number of FIB entries.
  - but it is quite difficult to guess...
    - Created a mode to control the amount of CAM entries for IPv4 and IPv6 (and other features)

Filtering Capabilities

- What kind of information can be a filtering condition without a degradation of packet forwarding speed?
  - Address
  - Protocol Type
  - Port Number
  - Packet Length
  - Dynamic Filtering Condition
    - e.g. uRPF (Unicast Reverse Path Forwarding)
- Normally depends on the FIB design.
  - Difficult to append IPv6 to the legacy (=IPv4-only hardware) implem entation.

Tunnel I/F

- Tunnel I/F is often required in the transition phase to bypass non-IPv6-ready routers

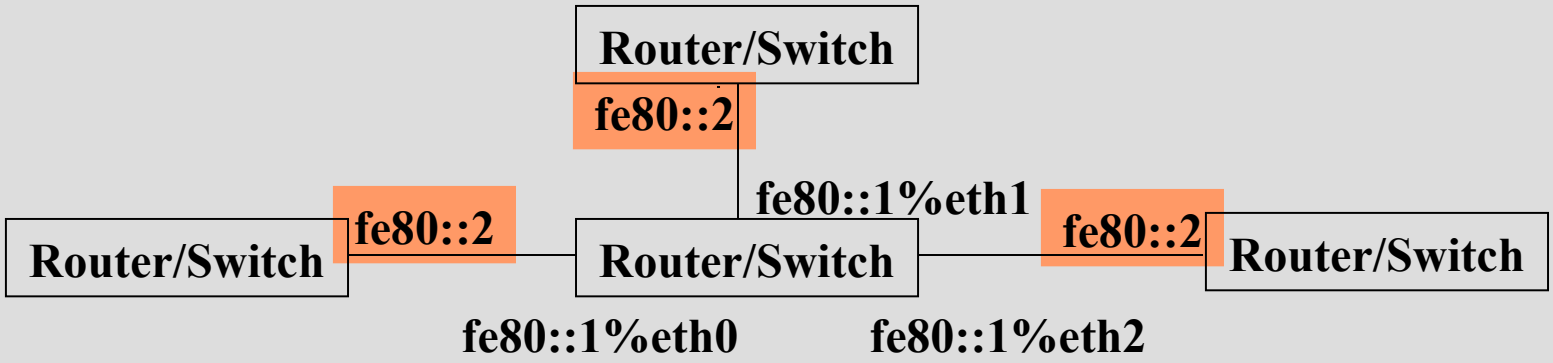


- But there are several problems in tunnel operation:
  - Difficult to guarantee a network quality/speed
  - Difficult to manage the link-connectivity
  - People may misunderstand “IPv6 protocol is slower than IPv4”.

- Well suited for a temporarily use, but not for a production use.
  - Is it really worth providing a wire-rate tunnel I/F (with a huge amount of investment)?

Link-Local Address Handling

- Link-local address
  - An IP address which is unique only within a link
  - There may be the same link-local address in different links.
    - Normally link information is followed by a link-local address



- Expected Problems
  - Lack of space to insert link information
    - Protocol, User Interface, …
  - Vague Notation “fe80::1%ethernet0/10”
    - IPv6 address fe80::1 at interface ethernet0 with prefix-length 10
    - IPv6 address fe80::1 at interface ethernet0/10

1. Introduction
2. IPv6-specific Issues in Network Equipment
3. IPv6 Operational Issues in a Dual-Stack Network System
   - Philosophical Issues
   - Operational Issues

Philosophical Issues in Dual-stack Networks

- Should IPv6 network be completely equivalent to IPv4's one?
  - If so, what is the benefit of IPv6 compare to IPv4?
  - If not so, you should provide two different policies for the same network.
    - lead to an increase of operation cost
- Considering the above, the easiest way is
  - use IPv6 for a new service
  - use IPv4 for a legacy service

Operational Issues in Dual-stack Networks

- Each equipment can be dual-stack, but the whole network system cannot always be.
  - Layer3 Routers/Switches without IPv6
    - Different topology between IPv6 and IPv4, which can increase th e operational cost

Avoidable by a redesign or a renewal

  - Layer3 Routers/Switches with IPv6 (but by software)
    - People hates IPv6 because it is slower than IPv4 ☹

Not so serious unless multicast streaming is used

  - Layer2 Switches without IPv6
    - Lack of MLD snooping makes it difficult to deploy IPv6 multicast

Difficult to be handled…

  - Management Servers
    - There are several commercial IDS's and IPS's, but most of them are not IPv6-ready yet.
    - Even when network equipment supports sFlow or NetFlow for IP v6, flow-collectors cannot handle IPv6 traffic.

Conclusion

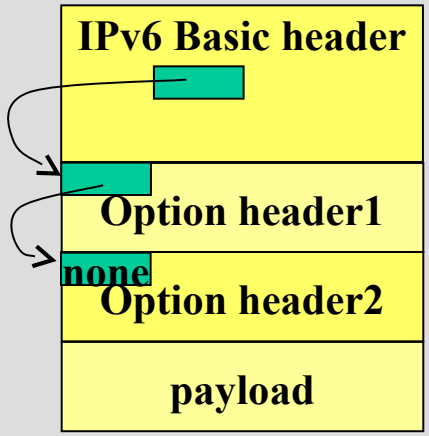
- To guarantee network service in IPv6 as well as in IPv4, network equipment MUST
  - Completely treat IPv6 in the same manner as in IPv4
    - Protocol, ACL, User-Interface, …
  - Equipment MUST be designed taking IPv6 into consideration from the beginning
- Huge amount of IPv6 address space contributes to a simpler implementation of network equipment
  - No need for NAT, Better Aggregation, No address confliction, …
- Even when a network equipment is IPv6-ready, the whole network may be non-IPv6-ready due to a lack of helpful management services.
  - Flow collector
  - IDS/IPS

Thank you !

http://www.alaxala.com/

A myth in IPv6 Specification

- One of the benefit of IPv6 is supposed to be “Improved Sup port for Extensions and Options“.



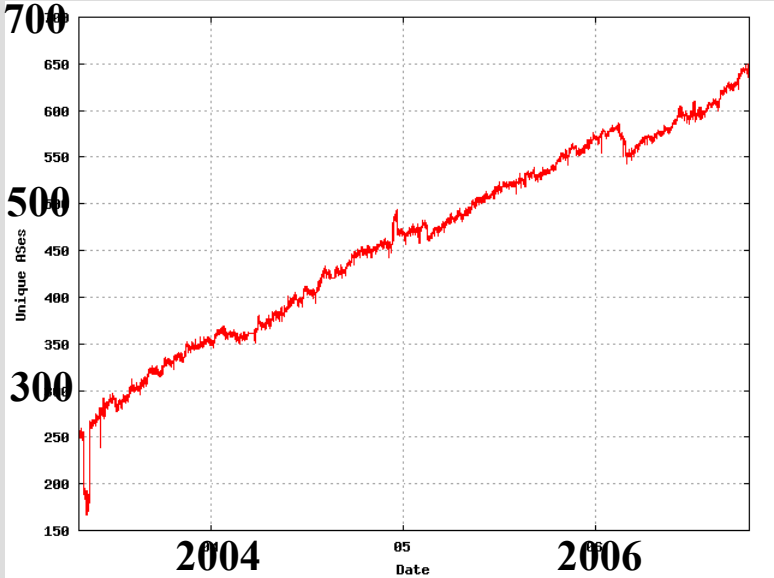
Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future. (RFC2460 “Internet Protocol, Version 6 Specification)

- But it does not contribute to an efficient forwarding from the hardware implementer’s point of view.
  - parallel processing is difficult, because of a uncertain number of ch ain-header look-ups (i.e. uncertain time for packet forwarding)
  - It was a myth in the ATM-era (before the birth of IP-forwarding-ASI C)

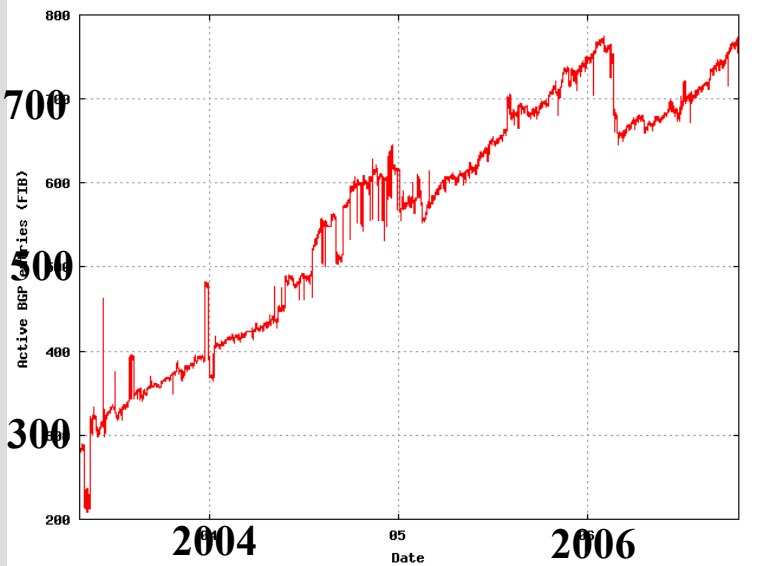
c.f.) Related Statistics

Cited from http://www.potaroo.net/

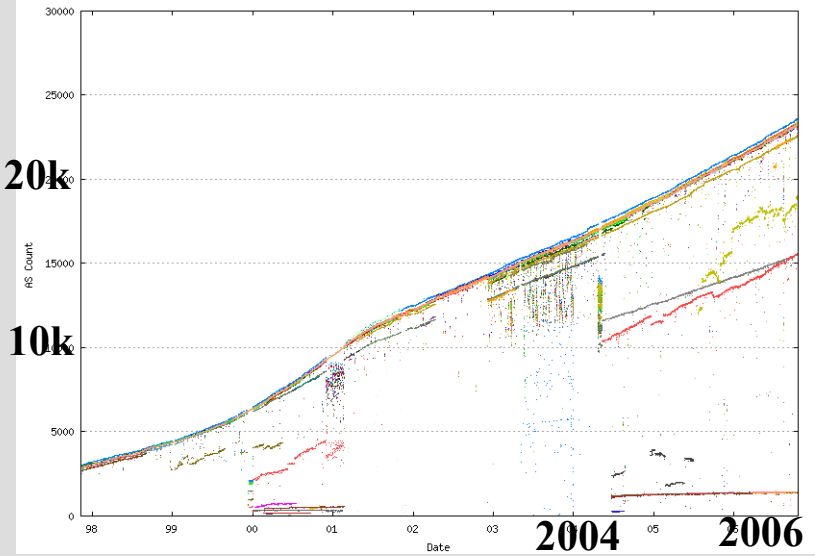
Number of ASes announcing IPv6 prefixes



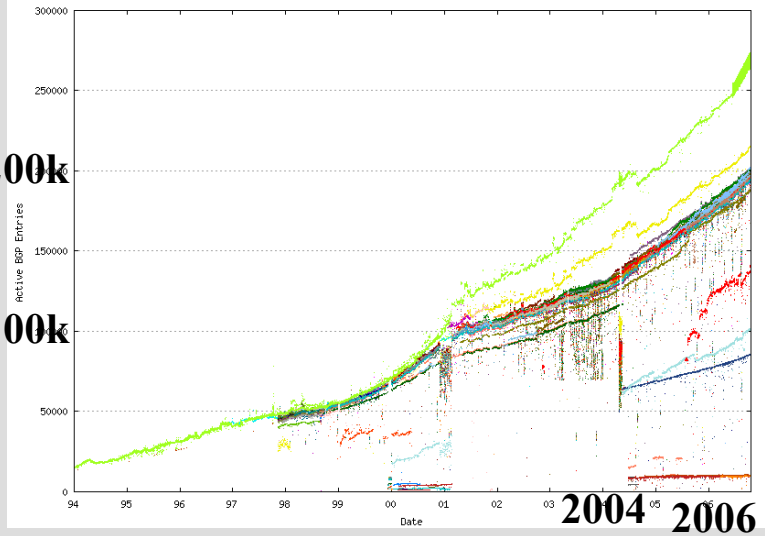
Number of IPv6 FIB entries at 6Net



Number of ASes announcing IPv4 prefixes



Number of IPv4 FIB entries



Appendix. Tips in IPv6 network operation

Manual Link-local Assignment

- Normally, link-local address is automatically generated from MAC address
- However, the automatic generation is not always appropriate for routers/ switches, because
  - Change of interface card leads to an unnecessary change of link-local address
  - Protocol behavior sometimes changes depending on the IPv6 address itself. So a protocol behavior might change between IPv4 and IPv6.

    e.g.)
    - PIM Designated Router in a link = a router with the largest IPv4 address/IPv6 link-local address in the link
    - MLD Querier in a link = a router with the smallest IPv4 address/IPv6 link-local address in the link
  - Operators have difficulty in the management of routing table.

    e.g.)
    - 2001:db8::/32 fe80::200:87ff:fe8a:97ab%eth00

- Proposal = IPv4-address embedded link-local address
  - IPv4:192.168.1.4 → IPv6 link-local fe80::192:168:1:4

Stop Bogus IPv6 Routers

- A Windows-XP PC may become an IPv6 router when it has multiple interfaces and a global IPv4 address on one of the interfaces.
  - Normally by mistake
  - But attackers can make use of this feature for wire-tapping, spoofing, …
  - (This is not an IPv6-specific attack; using a bogus DHCPv4 server, you can do the same thing)
- Several measures can be taken in network equipment
  - Router Preference
  - RA packet filtering by Layer2 switches
  - Private-VLAN