IPv6 deployment and operation at IIJ (ISP point of view)

Internet Initiative Japan Inc (IIJ)
Jun-ichiro itojun Hagino
itojun@iijlab.net

Who is IIJ, what kind of IPv6 services offered?

- One of the very first commercial ISPs in Japan
  - (and probably one of the biggest)
- Operational since 1992, IPv6 since 1998

- Connectivity services
  - 2001:240::/35, 3ffe:8020::/28
  - IPv6 tunnel service - since 1999
  - IPv6-only leased line service - since 2000
  - IPv4/v6 dual stack leased line service - since 2001
  - Commercial service, not experimental
- Other services
  - Web server hosting, with IPv4/v6 dual stack support
  - Data center with IPv6 connectivity
  - IPv4/v6 router "SEIL"
  - Consultation - help people design IPv6 network
  - Participate/contribute to KAME, IETF and others

Why are we doing it so early

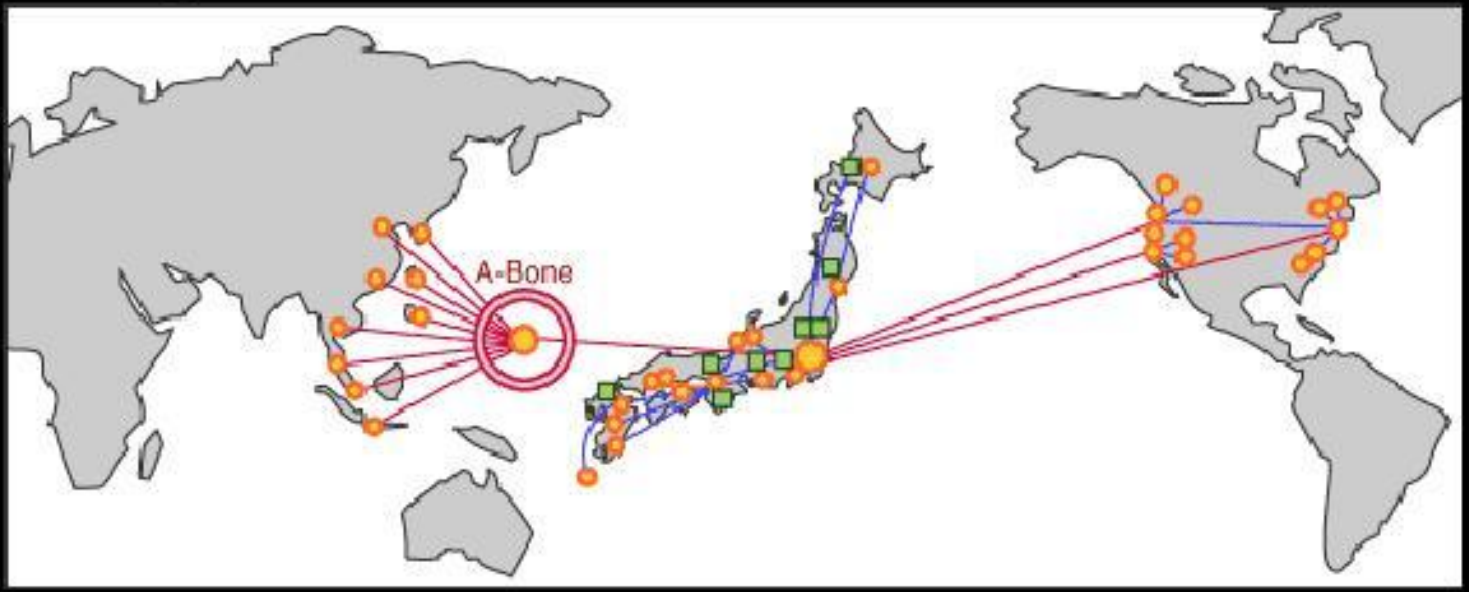
- For us, it is not early at all!
- ISPs need to act proactively
  - By the time customers start asking for IPv6, we need a working backbone - need to be prepared
  - We need to gather operational experiences much earlier than customers
  - Break the chicken-and-egg problem
- Our mission: make IPv6 the default IP protocol
  - Elwood Blues: "We're on a mission from God."

What about other ISPs in Japan

- 5+ ISPs are offering commercial services
  - tunnel, leased lines
- 25+ ISPs are offering experimental services
- 5+ IPv6 IXes are operational
  - (both commercial and academic)
  - 44 ISPs are participating NSPIXP6
- at least 1200 to 1500 /48 sites are in Japan
  - We can't count 6to4 sites reliably (so there could be more)

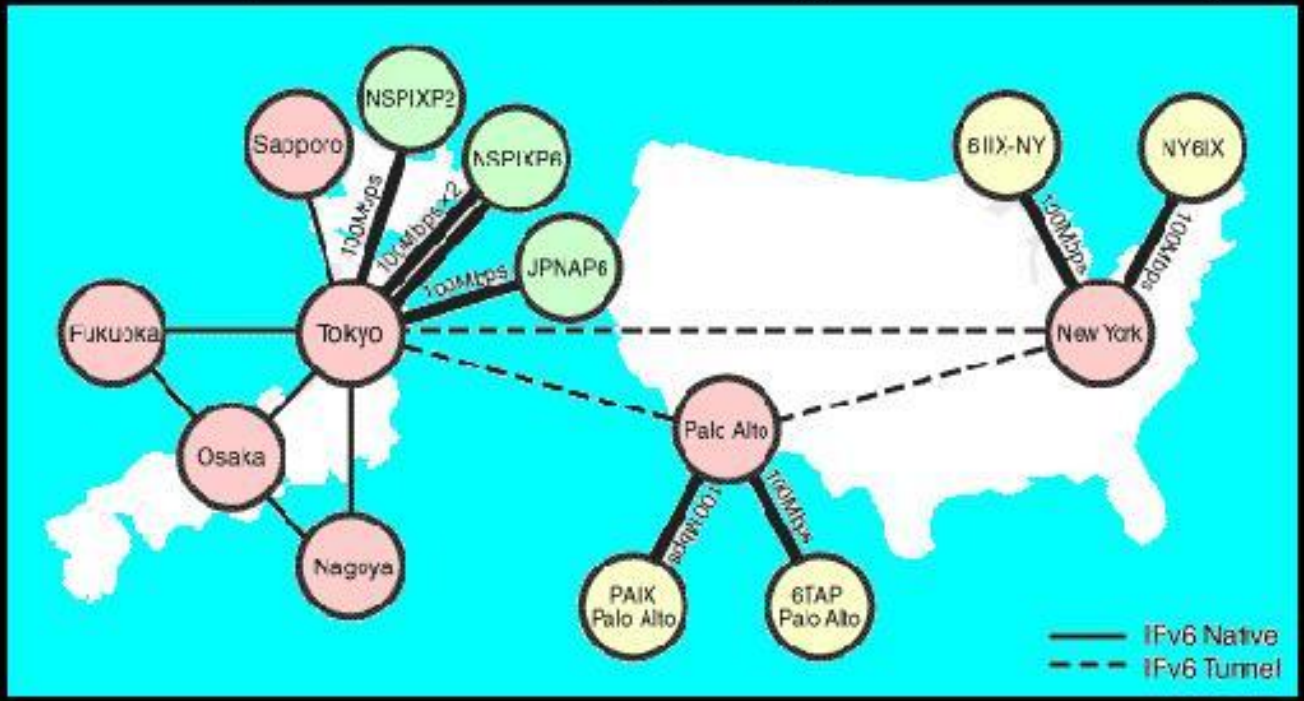
IIJ backbone topology (IPv4)

- Asia, Japan and US (east/west coast)
- Pure IP backbone, no MPLS
- 2.2Gbps between JP-US



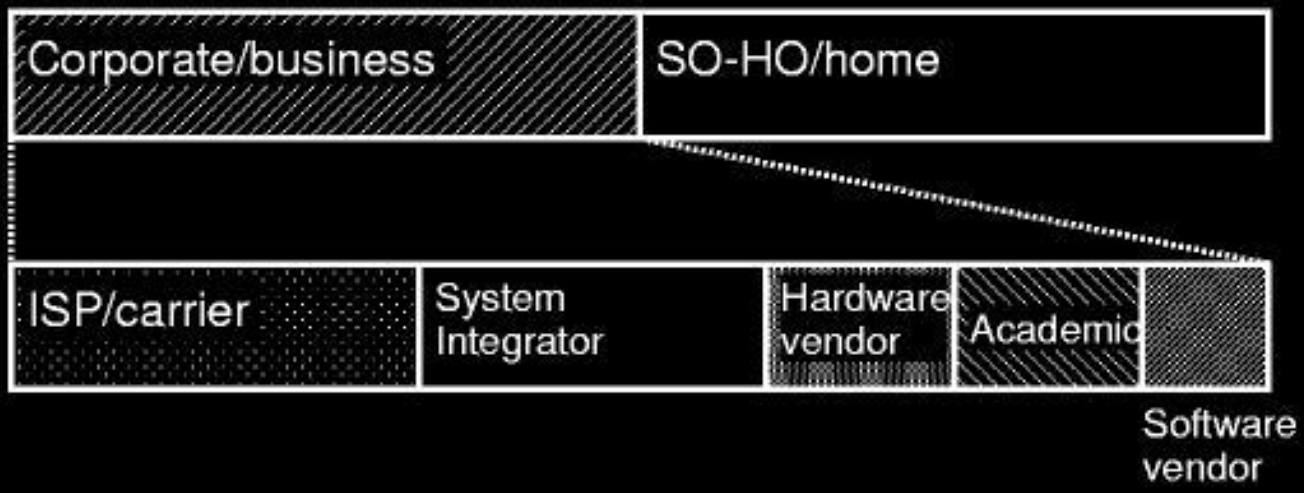
IIJ backbone topology (IPv6)

- 7 IXes, native peerings with 45 ASes
- Why deploy a separate backbone?
  - Can't compromise IPv4 SLA (stability of IPv4/v6 router)



Who are the IPv6 customers?

- A couple of /40 delegations
  - Smaller ISPs
- 200+ /48 customers already
  - 10% are leased lines, 90% are tunnels to IPv4 customers



Techs IIJ is using

- Well, pretty simple and standard stuffs

- BGP4+ over IPv6 for IBGP/EBGP
- RIPng
- RFC2893 configured tunnels (within our AS only)
- IPv6 PPP on leased lines
- Stateless autoconf
- RFC2772-based route filters at EBGP router
  - Avoids junk routes from injected into our cloud

Techs IIJ is not using, and plan to use

- Obstacles: vendors support, RFC delays
- Multicast by IPv6 PIM
  - Waiting for vendor routers support, as we need all routers to speak PIM
- OSPFv3, eventually
  - Again, waiting for vendors to ship/stabilize it
- IPsec for protecting routing protocols
  - No vendor support at all at this point
  - Details are lacking in RFC - "use IPsec" is too vague

Techs IIJ is not using, and no plans on using

- Site-locals in general/for IBGP
  - Tried it but benefit was too low
  - It is nontrivial for us to return the current sTLA to RIR - we handed them out to the customers
- Router renumbering (for backbone)
  - Again, we'll use 2001:240::/35 anyways
  - Renumbering an ISP is non-trivial (if possible at all)
- EBGP over tunnels/tunnels across AS border
  - We peer over IPv6-native only (at IXes, cross-connect)
  - With tunnels it's difficult to track down problems/keep quality
    - Routes from tunnel peer are unstable
  - Most of tunnel-based peers are not that serious about IPv6
    - Peers disappear without notice
- All translators and transition tools as service
  - (next page)

Translation/Transition mechanisms

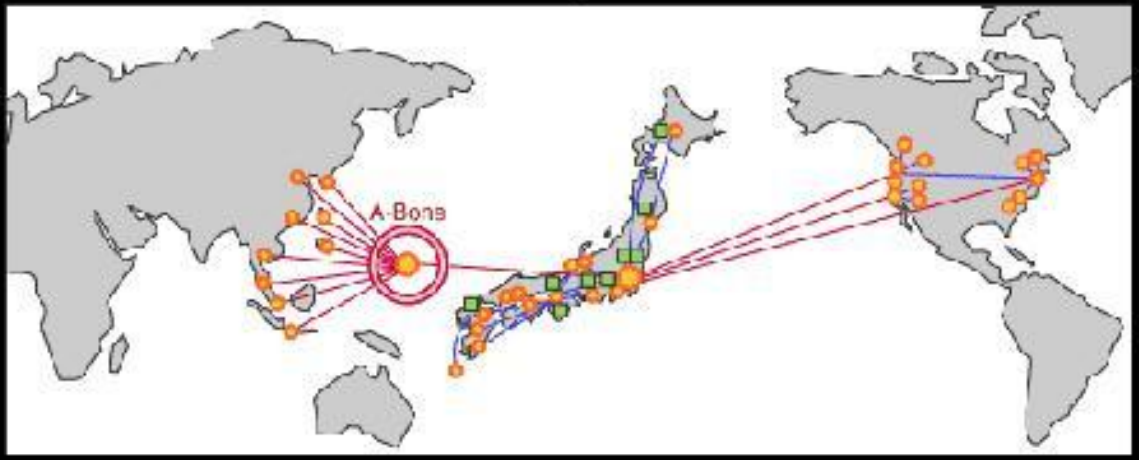
- We don't provide transition mechanisms as services
  - Our job is to provide big fat pipe for IPv4 and IPv6, that's all
- Translators/transition tools are "open relay of packets"
  - Anonymizer/malicious traffic generator
  - We're VERY worried, given the amount of abuses/attacks against our http proxy/smtp relay/IRC server
  - Not suitable to be operated at the core
  - draft-itojun-ipv6-transition-abuse-01.txt
- We provide transition technology to the customer
  - Sell translator products (routers with translator inside)
  - Customers are free to set it up on their own

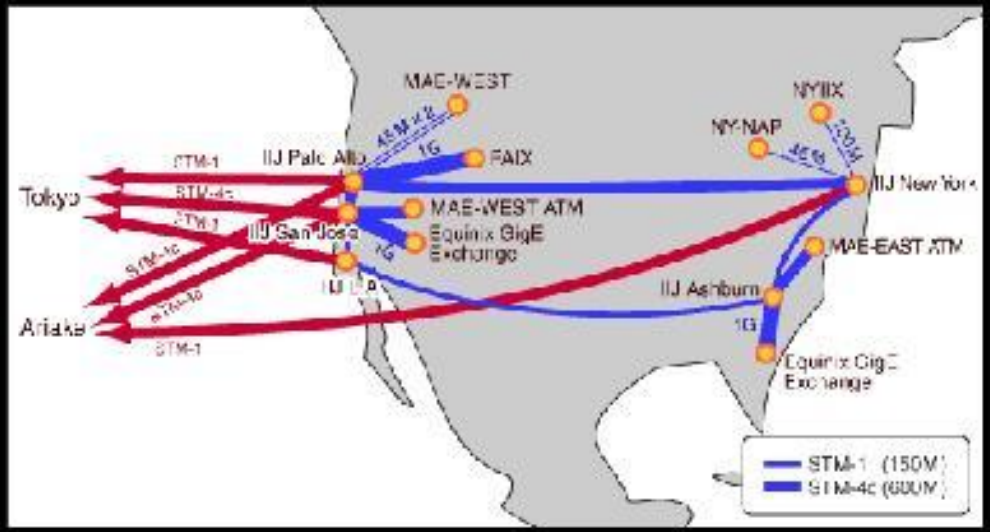
Which specs should be augmented/revisited?

- All translator/transition technology documents
  - Applicability is limited to leaf sites
  - Security worries in packet open relay, abuse
- All routing protocol documents
  - "use IPsec to secure it" is not enough
  - Must talk about gory details
  - IPsec over link-local multicast is A Difficult Problem
- Site-locals - we do not need it, from our POV
  - Big debate on ipv6wg mailing list
- Router renumbering
  - Applicability is limited to leaf sites, IMHO
  - Site-local multicast with IPsec - difficult
- Mobile-IPv6 draft 18
  - Need to remove "MUST" for HAO/binding error handling
  - Implementations without any HAO support are already deployed, need to make MN intereoperate with them

How the future IIJ IPv6 backbone will look like

- Unified IPv4/v6 backbone (router vendors, hurry up!)





Which specs need to be pushed to RFC ASAP?

- Prefix delegation - for "plug-and-play" DSL services
  - ntt.com will provide services starting Aug 2002
- DNS/whatever server discovery - ditto
- IPv6-ready root/ccTLD/gTLD DNS servers
  - To allow deploying IPv6-dominated/IPv6-only network

What we need ASAP from vendors

- IPv6 PIM support in all routers
- MLD-snooping L2 switches
  - We plan to do high-volume multicast streaming, so "flood-to-all-ports" switch is a big problem
- Stabilized IPv4/v6 dual stack routers from vendors
  - Please make our operators happy with dual stack operation
- IPv6 support at wholesale xDSL/L2 providers
- More educational materials for IPv6
- New security model/tool for IPv6, something better than firewall
  - (next page)

- http://www.kame.net/newsletter/20010615/

IPv6 security

- We need a new model for security for leaf sites, which is much more flexible than the firewalls nowadays
  - Otherwise most of the corporate IPv6 networks will continue to implement outgoing-only limitation (like one-way TCP filter), and there'll be no p2p apps deployment
- Firewall model really needs to be revisited anyways
  - Does not solve email viruses and/or abuse from inside
- Every nodes need to be secure by its own
  - OS vendors must take a security stance

Summary

- ISPs should deploy IPv6 now, if not yesterday
  - Or you will lose your potential customers
- No need to deploy fancy IPv6 network
  - Keep it simple and robust, that's what the Internet is about
- ASP/Integration services may be an interesting field
  - Translators, IPv6 network consultation and such
- There are drafts/RFCs need to be revisited
- Vendors need to do more
  - Security, stability, follow recent RFCs
- We hope to deploy IPv4/v6 integrated backbone sooner

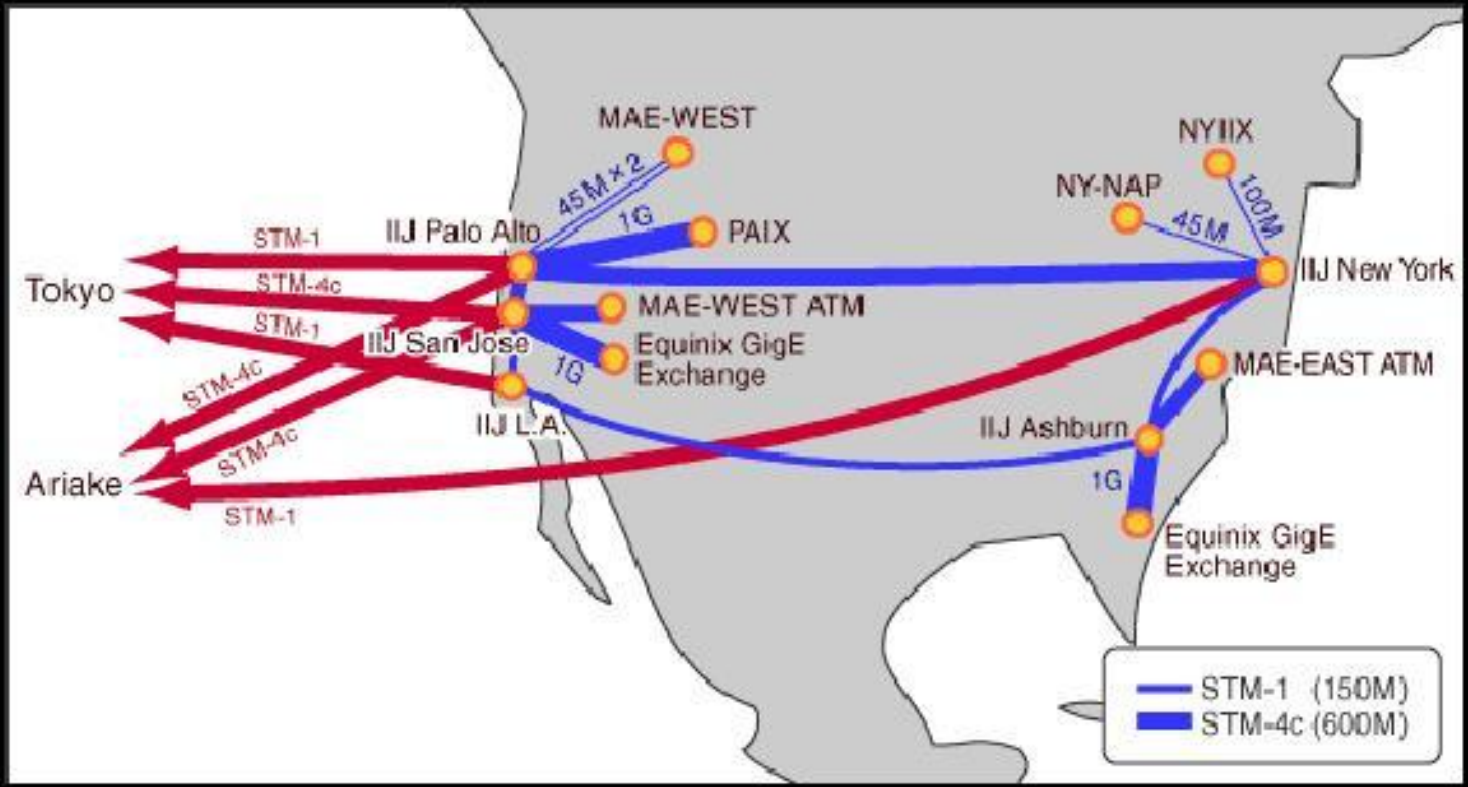
What we should be doing

- Filter packets with site-locals leaking from EBGP peers/customers
  - Just like avoiding "net 10" leaks
- Ingress filter?
  - Not sure if it is 100% okay to do it
  - Conflicts with multihoming with "multiple prefixes from multiple upstream ISPs"
- How should we really use multicast scope zone #s (ff01:: to ff0e::)

Customers are using...

- Honestly we don't know what they are using, really!
- SSH/FTP/IRC/HTTP/SMTP/NNTP are very common
  - People are using those without even noticing
- They could be trying more exotic stuffs
  - Site-locals
  - Router renumbering
  - IPsec
  - Site-local anycast
  - Translators, other transition tools
    - Note all of the current customers are dual-stack sites, otherwise they won't be able to query DNS

IIJ backbone topology (IPv4)



Far future...

- When attractive IPv6-only services appear, IPv4-only nodes will disappear

- Exit strategy is needed
- When IPv4 start to cease -
  - How can we support "legacy" IPv4 networks/nodes?
  - How much support do we need to provide?

- Think about fidonet/uucp/bitnet/decnet support today