IPv6 Implementation and Deployment Experiences

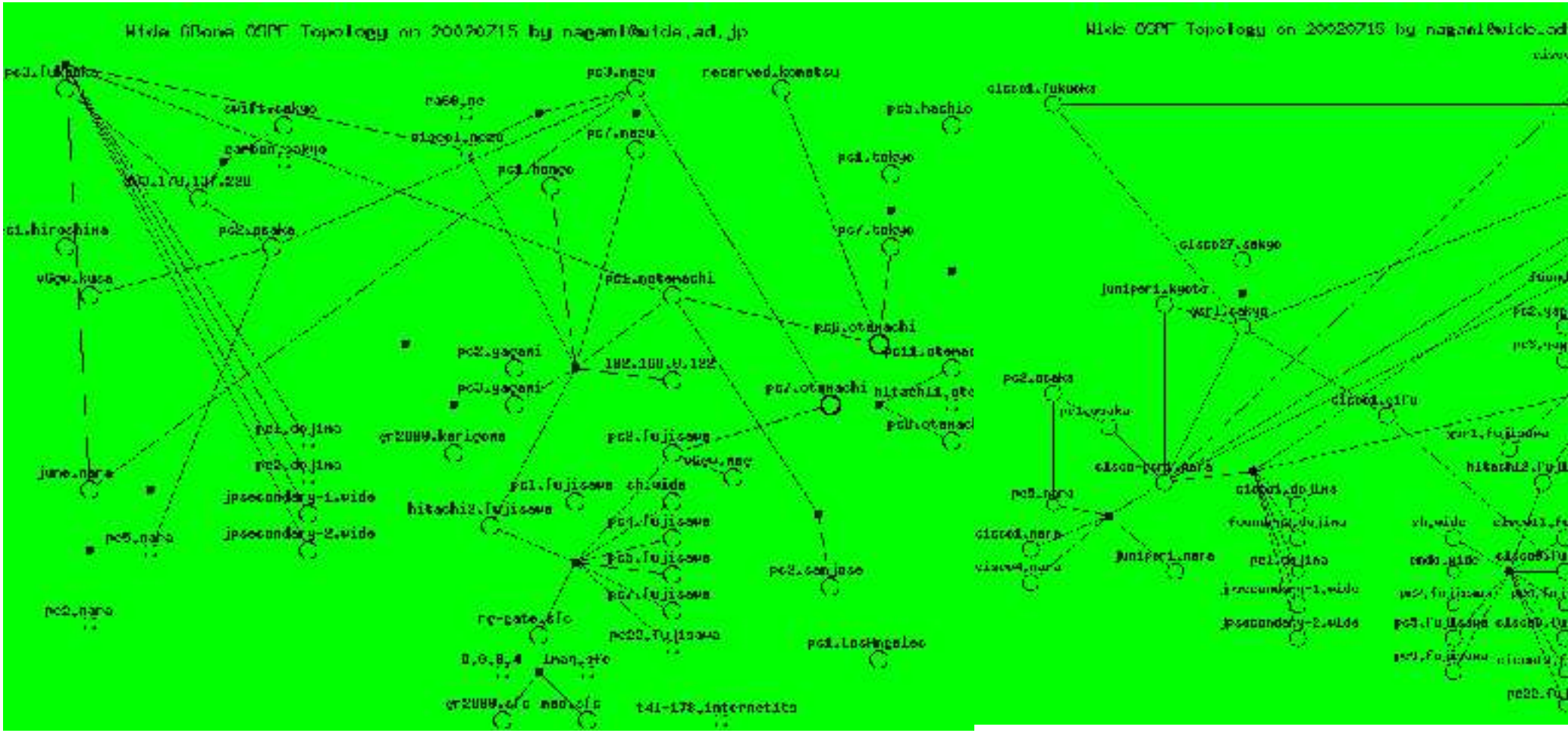
54th IETF, IESG open plenary

JINMEI, Tatuya
Toshiba Corporation, The WIDE/KAME project
jinmei@{isl.rdc.toshiba.co.jp, kame.net}

What's WIDE/KAME wrt IPv6?

- An implementor as well as an operator
- Implementor hat:
  - provide free running code of IPv6 to help deployment
    - fill missing pieces
    - check validity and applicability of specs
- Operator hat:
  - run a nation wide, large IPv6 network in WIDE
    - over 50 routers in the backbone (as large as our IPv4 BB)
    - more than 60 "/48" sites
    - more than 40 EBGP peers

Our IPv6 and IPv4 backbones



What we are using on IPv6 (1):

- Today's typical Internet applications
  - www, mail, FTP, SSH, ...
- Network operation tools
  - DNS, ping, traceroute, firewall
- Routing protocols
  - RIPng, OSPFv3, BGP-4+, (PIM-DM), PIM-SM
- IPsec
  - for end-to-end communication (e.g. POP with IPsec)
  - mainly in transport mode

What we are using on IPv6 (2):

- IPv6-specific stuff
  - Transport Relay Translator
  - node information queries
    - for address-to-hostname resolution
  - site-scope anycast
    - for DNS server discovery
  - privacy extension of stateless autoconf
  - 6to4
    - we are not using it in our backbone, but we've developed it and we know there is a certain amount of users.
- IPv6 links
  - Ethernet, ATM, serial line, tunnel, PPP

Not implemented, but have a plan (including ongoing ones):

- Necessary for IPv6 deployment
  - mDNS (LLMNR), IPv6 prefix delegation, "killer applications"
- Missing pieces
  - SSM
  - mobile IPv6
    - worried about the standardization status and procedure, though:
    - more and more revises
    - tend to require ALL nodes "support mobile nodes this way".
- Need to check how it works:
  - SCTP, VRRP, ISATAP, multi-sited node

Implemented, but not used:

- Router renumbering
  - we were not convinced that it was effective
- NAT-PT
  - Transport Relay Translator is enough for us
- DHCPv6 for DNS server discovery
  - we could not (always) assume multicast routing
- Some DNS extensions
  - A6/DNAME/bit labels (they were just deprecated.)

Not implemented, and no plans:

- Stateful address autoconf (by DHCPv6)
- Some of transition mechanisms
  - including SIIT, DSTM, and Teredo
- Why not?
  - we’ve not seen real need for them.
  - (see the next slide as for transition tools)

Translation/Transition mechanisms

- We are only using simple transition mechs:
  - configured v6 over v4 tunneling
    - but only when the benifit outweighs the overhead much.
    - esp. for BGP peering.
  - transport-relay (v6 to v4) translator
    - to browse IPv4-only web sites from an IPv6-only network.
- Perhaps these are enough;
  - we can even avoid translators when v4NAT is available.
  - if we really need complicated tools, users may reject the transition.
    - we may be wrong, of course, but we've been operating our network thi way.
- No clear image on tools after IPv6 is fully deployed

IPv6 scoped addresses

- Link-locals
  - necessary for operation, and in some cases very useful
- Site-local unicast/anycast
  - using site-local anyast for DNS server discovery
  - using site-local unicast for IBGP peerings
  - we can live *without* them and have not seen real need, though
  - no experiences on multi-site node
- Scoped multicast (other than link-local)
  - in use for multicast streaming
  - experimentally tried for DHCPv6 and router renumbering
  - do not have an essential reason for narrower scopes

Network configuration and management

- Dual stack env. may introduce confusion
  - "telnet localhost" does not work, when the client only tries 127.0.0.1 and the server only accepts ::1.
- source address selection is more complicated
  - (e.g.) mismatches of BGP peer addresses can happen.
- DNS PTR RRs
  - we cannot pre-register all IPv6 addresses in a subnet;
  - "dhcp101.kame.net" doesn't work for IPv6.
- Scoped addresses
  - (e.g.) link-locals are very useful for operation, but the notion is very confusing;
  - novice operators often forget disambiguating the link.

IPv6 security

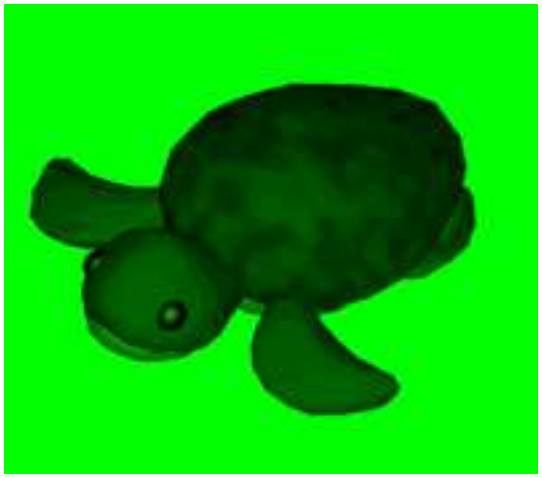
- Firewalls will remain, but the model needs a change;
  - we cannot just drop incoming SYNs.
    - IPv6 will introduce many bi-directional communications
  - per-host security will be more and more important.
- Applicability of IPsec should change
  - today (for IPv4): mainly for VPN, thus tunnel mode
  - for IPv6: more and more end-to-end usage will come.
    - mainly transport mode.
    - key management can be much harder
    - an "ad-hoc", easy-to-use secure pipe will meet the requirement, rather than a solid security infrastructure.
    - c.f. ssh

What is missing that really hurts?

- "Killer applications"
  - IPv6 will only be for geeks without apps appealing mass users.
  - P2P apps can be the ones, but most of them only support IPv4.
    - some of the implementation highly depend on IPv4.
    - educational issues may exist.
- Solid APIs
  - lack of portability wrt the basic API
  - loss of compatibility of the advanced API
- Security products
  - corporate operators tend to use commercial products.
  - all-in-one boxen are necessary for "home" users.

IPv6-only fun things

- Dancing turtles:-)



- Basically v4 and v6 provide the same stuff
  - however, IPv6 can enlarge the opportunity;
    - everyone can enjoy the apps
    - no upper limitation on the number of nodes

Apps demonstrated in N+I Tokyo 2002

- Cameras, TVs, games, cars, PDAs, home appliances, ...

And we'll try

- to provide applications that can be more effective in IPv6.
  - P2P or multicast apps are examples
- to encourage developers of such apps to support IPv6 in their products.
  - free software programmers, game/appliance vendors...