Implementation and Deployment of IPv6 in Japan

Tatuya Jinmei

Toshiba Corporation/The KAME Project

IPv6 activities in WIDE

- The WIDE project
  - http://www.wide.ad.jp/
  - the largest research activity on the Internet in Japan
  - committed to IPv6 since 1995 (started a wg)
- The KAME project
  - a joint effort on IPv6 R&D by several companies
  - provided IPv6 referential implementation on *BSDs
  - 3 RFCs, >20 Internet Drafts
- The USAGI Project
  - a similar effort on IPv6 R&D for Linux
  - results have been merged to the mainline kernel

Contents

- IPv6 deployment activities in Japan
  - network and services
  - IPv6 DNS deployment
- Issues on IPv6 deployment
  - DNS, security, and others

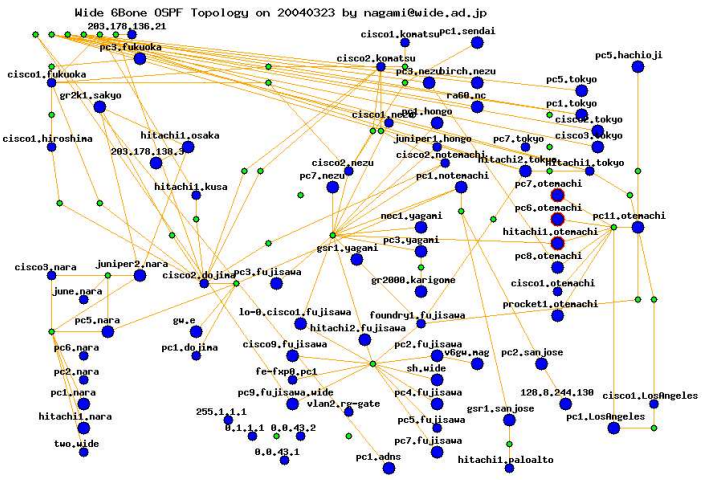
WIDE IPv6 backbone (1)

- Nation wide, large IPv6 network
  - over 50 routers in the backbone
  - more than 60 "/48" sites
  - about 50 EBGP peers
- R&D network, but with "production quality"
  - with commercial routers
    - Hitachi, Cisco, Juniper, Foundry
  - experimental PC routers for advanced researches
    - zebra on BSD PCs (http://www.zebra.org/)

WIDE IPv6 backbone (2)

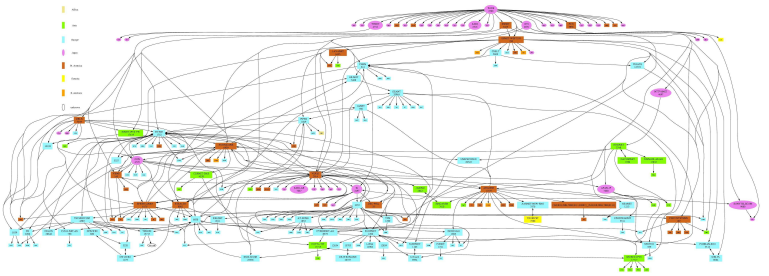
- Routing protocols
  - IGP backbone: OSPFv3
  - Within leaf sites: OSPFv3, RIPng
  - EGP: BGP-4+
  - Multicast: PIM-SM within WIDE
- IPv6 links
  - Ethernet, GbE, (tunnel, ATM)
  - PPP, PPPoE (in some limited places)

WIDE IPv6 backbone as of today



The IPv6 Internet (June 2003)

- Pink: Japan
- Orange: South America
- (http://www.jinmei.org/v6topology.jpg)



IPv6 services

- End hosts
  - servers: (mainly) FreeBSD and NetBSD
  - client hosts: *BSD, Linux, Mac OS-X, Windows XP
    - configure themselves by IPv6 autoconfiguration
- Today's typical Internet applications
  - DNS: BIND9
  - WWW: apache2
  - SMTP: postfix + IPv6 patch, sendmail
  - FTP: BSD's ftpd, wu-ftpd
  - SSH: OpenSSH
- Security tools
  - Firewall: FreeBSD ipfw, OpenBSD pf
  - Filtering at commercial routers

IPv6 deployment and operation in DNS

- IPv6 transport with BIND9
  - most DNS servers in WIDE enable IPv6 transport
    - accept/send DNS queries over IPv6

```
listen-on-v6 { any; };
```

  - same for TLD servers in japan
    - 3 "JP" servers (out of 6)
    - the "M" root server (in addition to B, F, and H)
- AAAA glues for "JP" at the root zone
  - already asked IANA

Summary of our experiences

- Works fine for basic operation
  - backbone routing is stable
  - various routers are interoperable
  - server applications run without troubles
    - and can communicate with clients
    - users are even not aware of IPv6
- We are now trying
  - yet other autoconfiguration
    - DNS server discovery by DHCPv6, multicast DNS
  - deploy new applications
    - home network appliances, IPv6 "toys", ...
    - (shown in tomorrow's presentation)

Issues on IPv6 deployment

DNS issues (1): IPv6 reverse maps

- Difficulties to configure IPv6 reverse zones
  - addresses that are not in the DNS
    - scoped addresses (e.g. link-local)
    - RFC3041 privacy extension
  - transition from ip6.int to ip6.arpa (RFC3152)
    - tend to cause lame delegation, communication delay
    - need to manage both for now
- Two approaches to manage both int and arpa
  - share the zone file
    - intuitive, but with some restrictions
  - trick with DNAME RR (for advanced users)
  - http://www.isc.org/tn/isc-tn-2002-1.html

Sharing zone file for int and arpa (1)

- named.conf at primary server

```
zone "9.1.8.4.0.0.0.0.0.0.2.0.1.0.0.2.ip6.int." {
    type master;
    file "2001:200:0:4819::.zone";
};
zone "9.1.8.4.0.0.0.0.0.0.2.0.1.0.0.2.ip6.arpa." {
    type master;
    //shared with ip6.int.
    file "2001:200:0:4819::.zone";
};
```

- zone file at primary server (2001:200:0:4819::.zone)

```
;;$ORIGIN 9.1.8.4.0.0.0.0.0.0.2.0.1.0.0.2.ip6.int.
;;-->!!!doesn't work
c.f.1.8.1.7.e.f.f.f.d.a.0.8.2.0 IN PTR www.kame.net.
```

Sharing zone file for int and arpa (2)

- named.conf at secondary server

```
zone "9.1.8.4.0.0.0.0.0.0.2.0.1.0.0.2.ip6.int." {
    type slave;
    file "bak/2001:200:0:4819::.int.zone";
    masters ...
};
zone "9.1.8.4.0.0.0.0.0.0.2.0.1.0.0.2.ip6.arpa." {
    type slave;
    //unshared with ip6.int.
    file "bak/2001:200:0:4819::.arpa.zone";
    masters ...
};
```

DNS issues (2): packet size limitation

- Max UDP message size of 512 bytes
  - -> upper limit of # of addrs of TLD servers
    - 13 for root and "com/net"
  - draft-ietf-dnsop-respsize-00.txt (expired)
  - be careful to add server addresses
    - whether it's IPv4 or IPv6
    - 5 or 6 are safe and typically enough
- EDNS0: complete solution
  - BIND 8 and 9 already use it by default
  - there is no reason to deny EDNS0
    - many deployed implementations support for it
    - providing backward compatibility
  - "deploy EDNS0, and then add IPv6 addresses for your DNS servers"

DNS issues (3)

- Broken DNS servers regarding AAAA
  - draft-ietf-dnsop-misbehavior-against-aaaa-00.txt
  - some load balancers behave badly for AAAA queries
- Most problematic cases
  - return NXDOMAIN for AAAA queries
    - fatal error on name resolution
    - NXDOMAIN will be cached
  - ignore AAAA queries
    - very long delay to make a connection
- No easy way out
  - if you use a load balancer, check it and complain to the vendor if it's buggy

Other pitfalls (1)

- AAAA exists, but no IPv6 service
  - due to lack of server config, no/poor IPv6 reachability, etc
  - some web browsers give up if a web server has AAAA but is unreachable over IPv6
  - once you add AAAA, be sure to provide complete IPv6 service with good reachability
  - a tip at the trial stage: use different name space
    - we used to use "v6.wide.ad.jp"

Other pitfalls (2)

- Path MTU discovery blackhole
  - ICMP too big is filtered, and hosts keep sending large packets
  - more serious in IPv6
    - PMTU discovery is a basic assumption
  - do not filter ICMPv6 errors at FWs
- Rogue router advertisements
  - often happen from Windows XP with 2002::/16
  - just as bad as rogue DHCP servers
  - -> disable "network sharing" on XP machines

Security issues (1)

- Typical myths
  - "The e2e property (and IPv6) weakens firewall, it's bad for security."
  - "IPv6 is secure enough because it mandates IPsec."
- The facts
  - firewall is not perfect even today
    - virus mail, web bug, bringing infected PCs to the office...
    - regardless of the use of IPv6, security at end hosts is necessary
  - IPsec is very hard to use for novice users
    - no easy way of key management

Security issues (2)

- New security model for e2e communication is necessary
  - still under discussion...
  - WIDE started "secure6" wg for this purpose
  - draft-kondo-quarantine-overview-00.txt
- "m2m-x" by NTT Communications
  - an attempt of deployable IPv6 security
    - by embedding certificate to devices and authenticating them in the ISP
  - (by a proprietary protocol, though...)
  - http://www.ipv6style.jp/en/apps/latest.shtml

Summary

- IPv6 activities in WIDE
  - KAME/USAGI: provide referential implementation
  - WIDE IPv6 network
    - "production quality" by commercial routers
    - as well as experimental trial
  - commodity network service over IPv6
    - Mail, WWW, FTP, SSH,...
  - now working on next steps
- Identified issues
  - DNS reverse map: ip6.int and ip6.arpa
  - packet size and EDNS0
  - misbehavior against IPv6 queries
  - security issues (need more work)

Contact Points

- The KAME Project
  - http://www.kame.net/
- The USAGI Project
  - http://www.linux-ipv6.org/
- HS247: IPv6 News&Links
  - http://www.hs247.com/
- FreeBSD ports
  - http://www.freebsd.org/ports/ipv6.html
- NetBSD pkgsrc
  - ftp://ftp.netbsd.org/pub/NetBSD/packages/