Problem Statement of Default Address Selection in Multi-prefix Environment : Operational Issues of RFC3484 Default Rules

NTT PF Lab. Arifumi Matsumoto
Tomohiro Fujisaki
Intec NetCore, Inc. Kenichi Kanayama
Ruri Hiromi

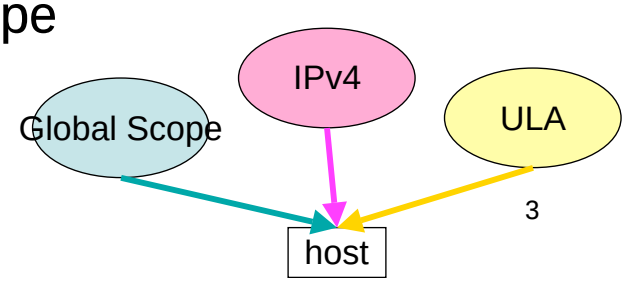
background

- draft-arifumi-v6ops-addr-select-ps-00.txt
  - related 2 documents ;
    - draft-arifumi-ipv6-policy-dist-01.txt
    - draft-fujisaki-dhc-addr-select-opt-02.txt

- proposed the mechanism of providing policy information by dhcpv6 at dhc-wg
- working code & experiment made last year
- what is the problem and what we are trying to solve are described in this Problem Statement

Our scope and multi-prefix environment

- End-host that has multiple IP addresses
- Connect to
  - v4-v6 dual stack network
  - v4 and ULA co-existing network
  - v6 global scope and ULA co-existing network, etc.
  - we called this situation as “multi-prefix environment”
- users possibly encounter problems on default address selection in multi-prefix environment
- Multi-homing is out of scope



What RFC3484 defines

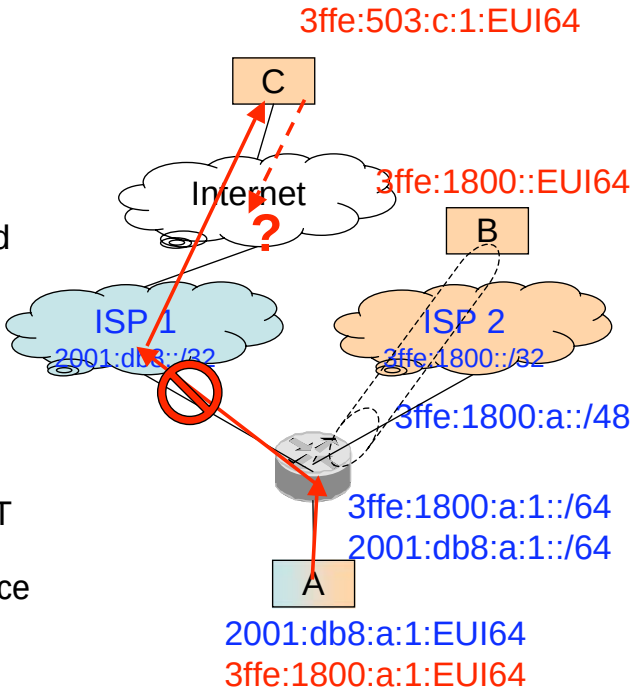
- RFC3484 - Default Address Selection for IPv6
- defines both source and destination address selection algorithms at end-host
  - Rule 1: Avoid unusable destinations
  - Rule 2: Prefer matching scope
  - Rule 3: Avoid deprecated addresses
  - Rule 4: Prefer home addresses
  - Rule 5: Prefer matching label
  - Rule 6: Prefer higher precedence
  - Rule 7: Prefer native transport
  - Rule 8: Prefer smaller scope
  - Rule 9: Use longest matching prefix
  - Rule 10: Otherwise, leave the order unchanged

Considered Problematic cases

- RFC3484 works but these cases are considered
- Source Address Selection
  - Multiple Routers on a Single Interface
  - Ingress Filtering Problem
  - Half-Closed Network Problem
  - Combined Use of Global address and ULA
  - Site Renumbering
  - Multicast Source Address Selection
  - Temporary Address Selection
- Destination Address Selection
  - IPv4 or IPv6 prioritization
  - ULA and IPv4 dual-stack environment
  - ULA or Global Prioritization

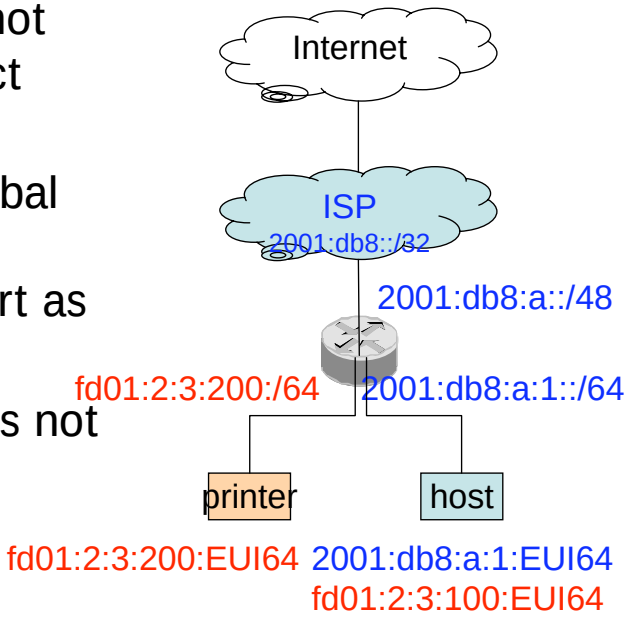
Case1 Half-Closed Network Problem

- HOST-A has addresses from ISP1 and ISP2.
- for the longest matching algorithm of source address selection, Host-A has ISP2 address in the source address field and sends a packet to Host-C then filtered by ingress filter at ISP1.
- Even if the packet is fortunately not filtered by ISP1, a return packet from Host-C cannot be delivered to Host-A because the return address is closed from the Internet.
- source-address-based routing does NOT work at this problem
- each host should choose a correct source address for a given destination address



Case2 Combined use of Global and ULA

- the longest match rule will not be able to choose the correct address in the future
- the assignment of those Global Unicast Addresses whose beginning bit is 1 will be start as RFC 4291 described.
- when it starts, end host does not know its scope, routing information is needed.

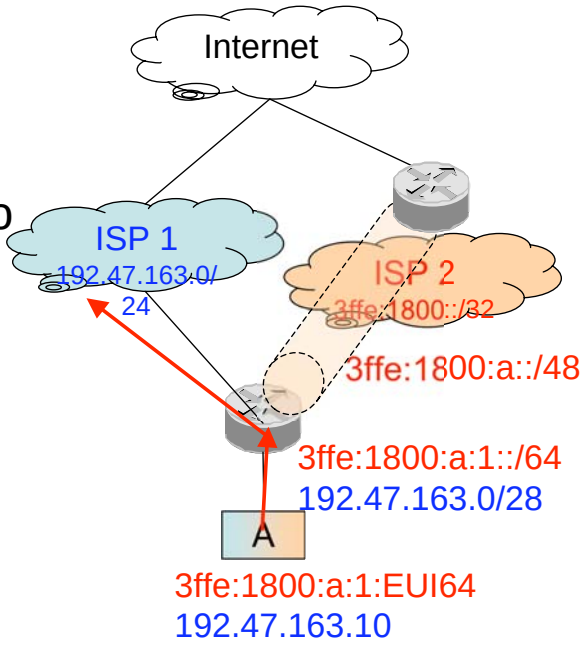


Case3 site reumbering

- An auto-configured address has a lifetime, there is possibility to take a long time in invalidation and long lasting routing caused by long-lived TCP or UDP session that uses the old prefix.
- RFC3484 maybe solve this case
- compare with manual configuration for RFC3484, it might be smooth using by policy distribution

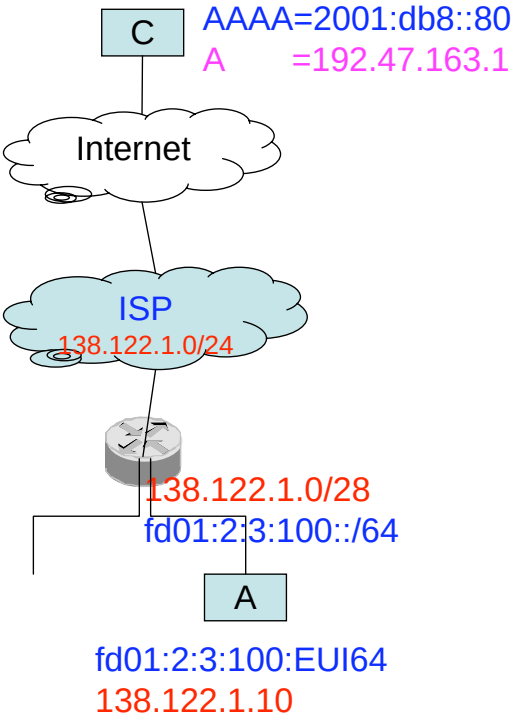
Case4 IPv4 or IPv6 prioritization

- a site has native IPv4 and tunneled IPv6 connectivity.
- the administrator may want to set a higher priority for using IPv4 than using IPv6 because the quality of the tunnel network seems to be worse than that of the native IPv4 transport.



Case5 ULA and IPv4 dual-stack environment

- HOST-A has both an IPv4 global address and a ULA.
- HOST-C has A and AAAA records in DNS
- if host-A chooses AAAA of HOST-C for destination and ULA for the source address, it will clearly make connection failure.



Case6 ULA or global prioritization

- If ULA and IPv6 global address both have global scope, the default rules do not specify which address should be given higher priority.
- This point makes IPv6 implementation of address-based service differentiation a bit harder
- (ex) if a user wants to access internal web server with ULA and external web server with global scope address, it might be problem.

solutions

- Manually configuring the policy table at each end-hosts
  - it is hard for averaged PC users
- policy distribution from the network, using with the form of ND(DHCPv6 option, RA)
  - need to adopt this implementation
  - draft-arifumi-ipv6-policy-dist-01.txt
- something else?

experiments & implementation

- already made working code with DHCPv6 & verified it to solve these problems
- why dhcpv6?
  - might be needed centralized management type of protocol
  - might be better than RA
  - (RA type implementation and test was also done, not evaluated yet)

Conclusion & Next step

- There are some trouble case for address selection at end nodes in MULTI-PREFIX environment
  - There are also several solutions for this
  - we think ‘policy distribution with dhcpv6’ can solve better in working with RFC3484
- Can v6ops support?
  - Q1. Is this information useful? Worth sharing?
  - Q2. support distribution of policy info to each node?
  - Q3. support to use dhcpv6?(draft-arifumi-ipv6-policy-dist-01.txt)

That’s all, thank you