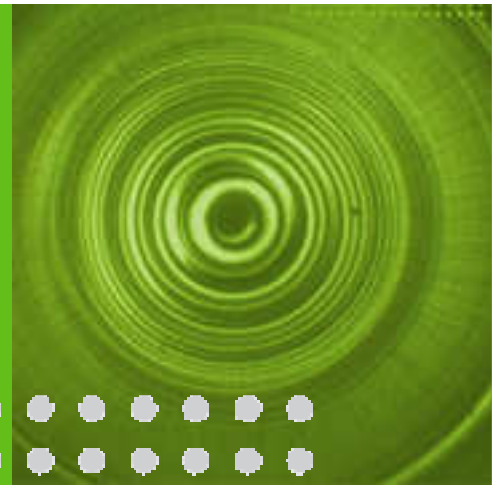
Multiple NSP Architecture for IPv6



David Miles david.miles@alcatel-lucent.com
Tadahisa Okimoto t.okimoto@hco.ntt.co.jp
Satoru Matsushima satoru.matsushima@tm.softbank.co.jp
Jun-ya Kato kato.junya@lab.ntt.co.jp

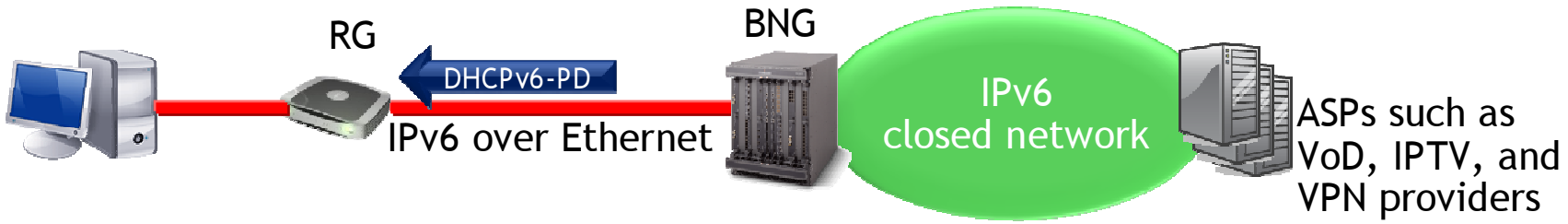
Agenda

1. IPv6 Broadband Service Circumstance in Japan
2. Generalized Problem Statement & Requirements
3. A policy based solution
    - 3.1 Source Address Selection
    - 3.2 Route Selection
    - 3.3 DNS Selection
4. Legacy Host Support
5. Considerations of how to put this model into BBF

1 IPv6 Broadband Service Circumstance in Japan

[Background]
Current IPv6 Service and Next Step toward April 2011.

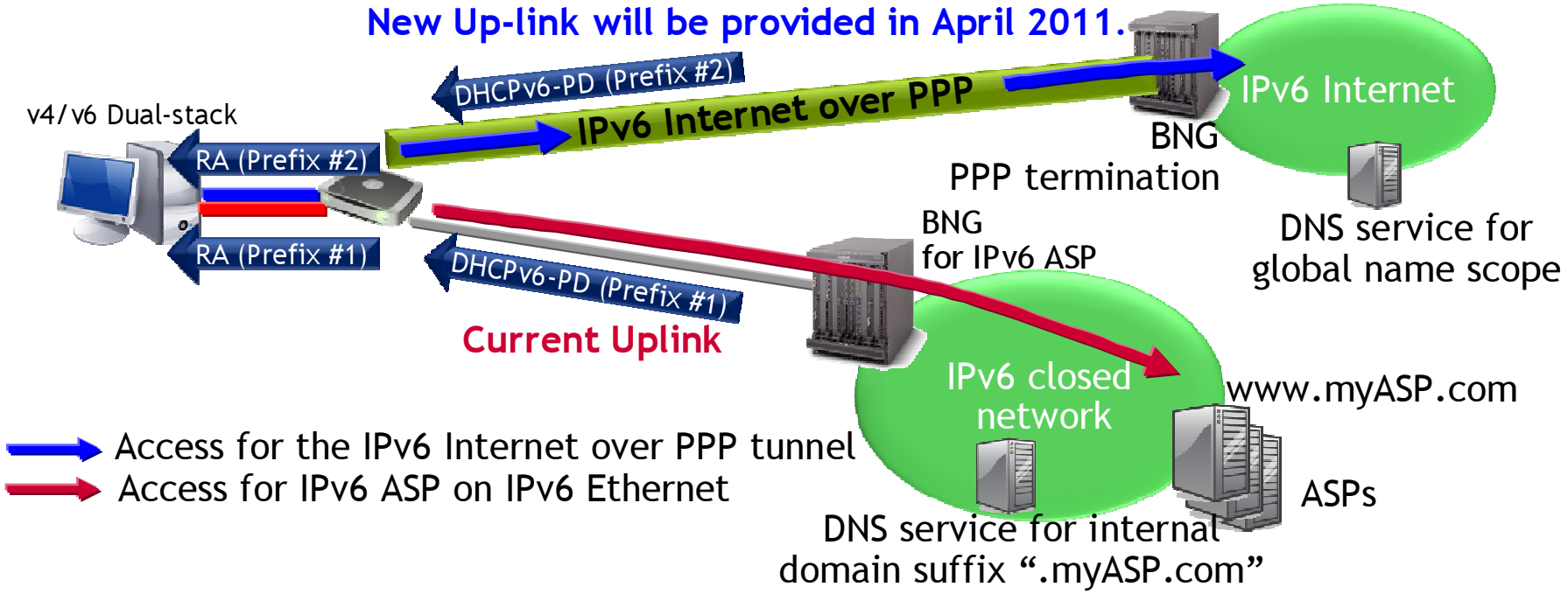
- NTT regional companies hold almost 74.3% FTTH market share in Japan (as of Sep 2009). Their current major service is connectivity to the IPv4 Internet.
- In addition, they already started IPv6 transport services on their FTTH over 6 years ago.
  - Now that many residential gateways have an IPv6 uplink.
  - The network configuration for accessing ASP is almost compatible with architecture defined in WT-177.
  - IPv6 uplink doesn't reach global IPv6 internet.



- However, global IPv4 address will be exhausted in recent days. They decided to launch commercial IPv6 Internet connectivity service by April 2011.
  - Two types of IPv6 Internet connectivity services will be deployed:
    One is PPP tunnel, the other is so-called quasi-native model.

IPv6 Broadband Service Circumstance after Introduced IPv6 Internet access

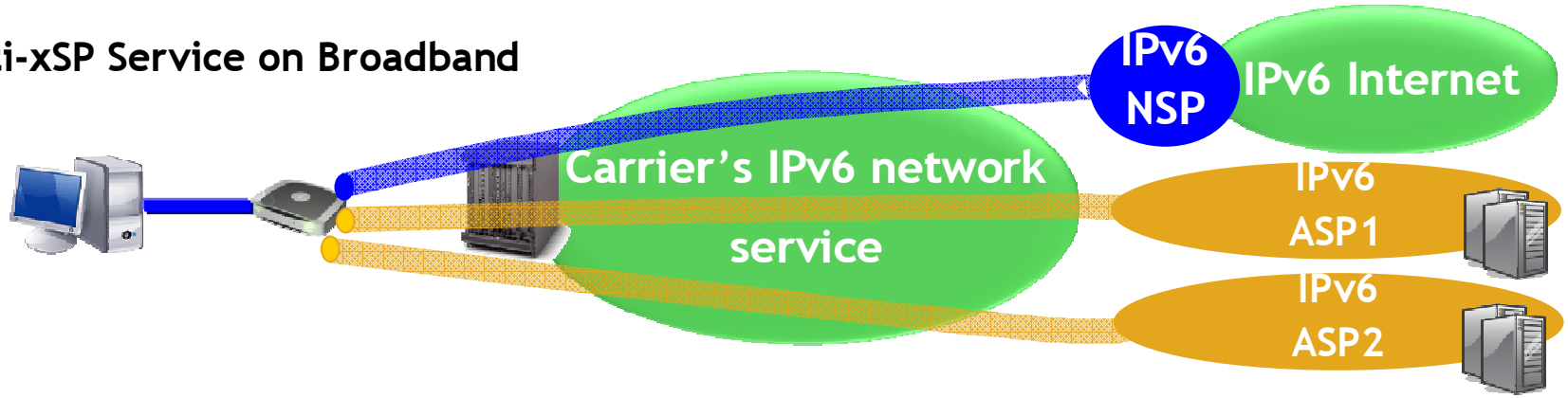
- PPP tunnel that is almost equivalent to WT-187 will be adopted for IPv6 Internet connection. New BNG installation is planned for PPP termination.
- In this configuration, the residential gateway has two IPv6 uplinks when PPP link is established.
- Both BNGs distribute the following three kinds of information to RG.
  1. IPv6 prefixes – prefix #1 for ASP, another #2 for the IPv6 Internet
  2. Route information – RG needs route info for IPv6 packet forwarding
  3. DNS information – DNS address and domain suffix need to be distributed



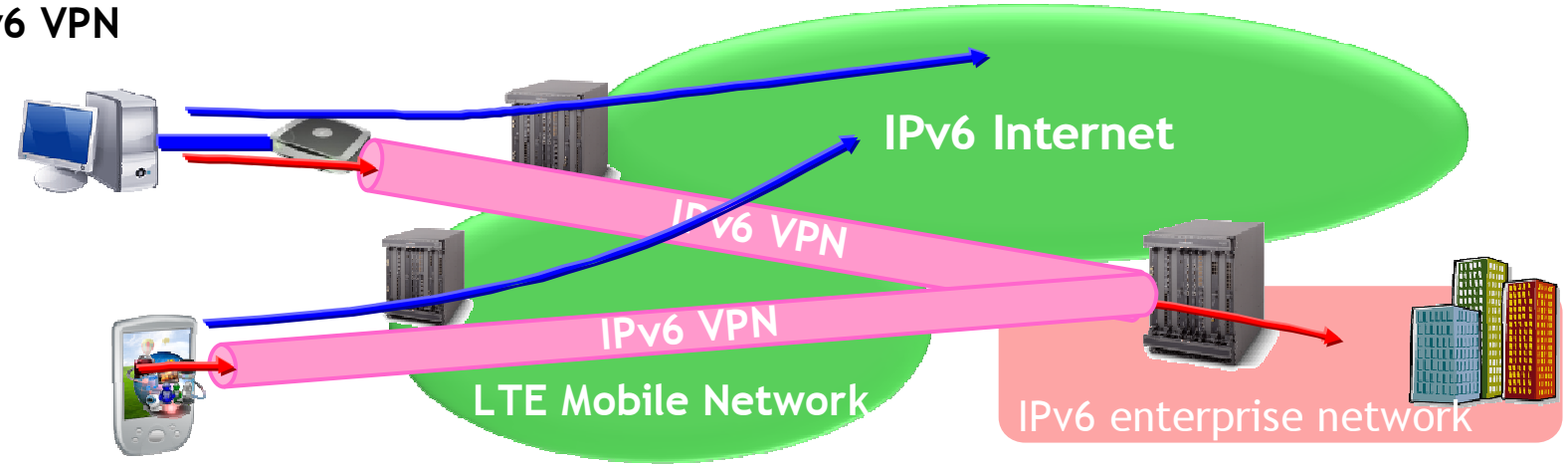
2 Generalized Problem statement & Requirements

Use cases

- Multi-xSP Service on Broadband

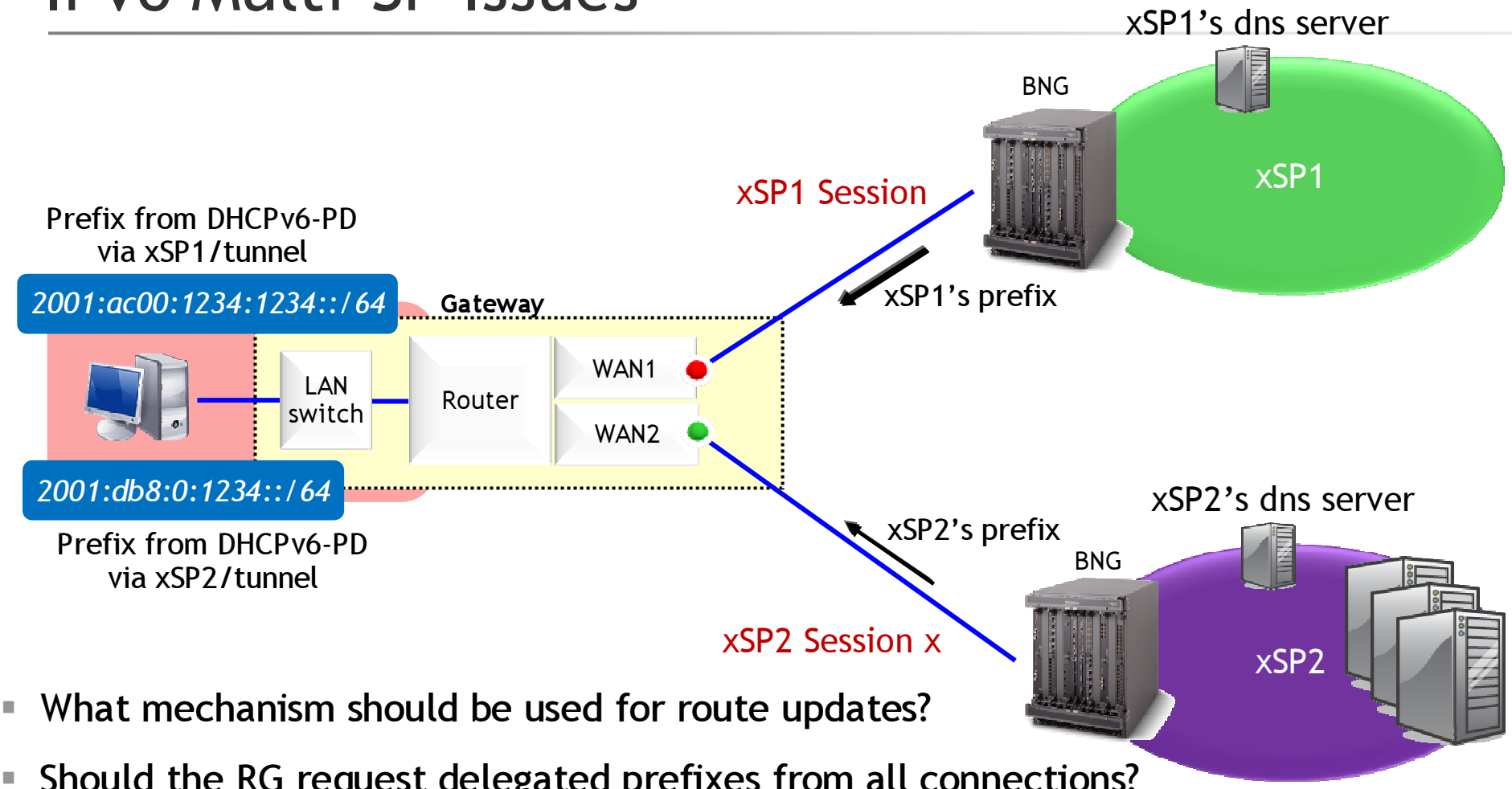


- IPv6 VPN



Multi-Uplink situation will happen in many use case scenarios.

IPv6 Multi-SP Issues

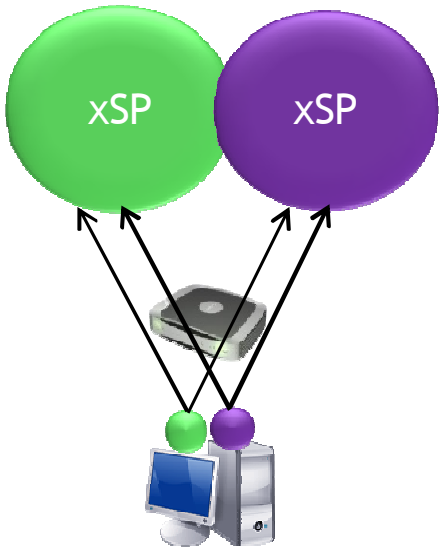


- What mechanism should be used for route updates?
- Should the RG request delegated prefixes from all connections?
- How should DNS servers be configured?
- What about host source address selection?

Why it'll not work without policy

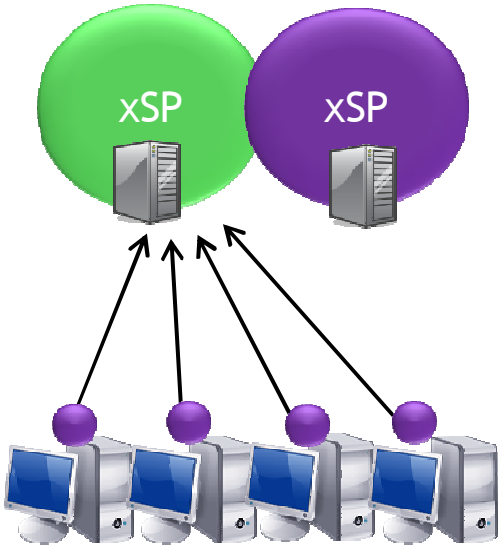
- Without knowledge, end system will connect by try-and-error or try-all-at-once manner.
- However, it raises the following problems.

- Privacy exposure



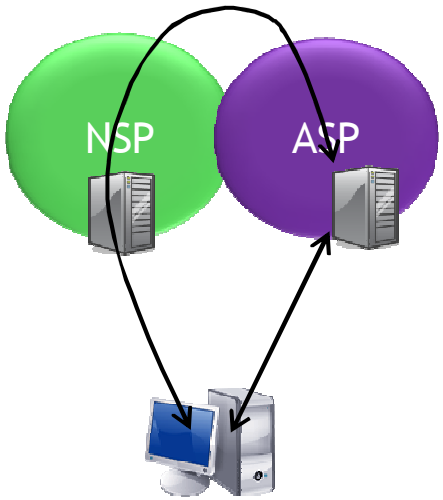
xSP can know which services user's are subscribing

- Unwanted traffic



Unwanted traffic/query goes to xSP's network/server

- DNS view



DNS replies can be different depending on query source. NAT64 is another example.

Simultaneous Internet and ASP Access

The challenge becomes:

- "How do I provide IPv6 multi-SP Access to a single device?"

The Issues we need to solve:

- **How can we implement source address selection policy ?**
- **How can we implement route selection policy ?**
- **How can we implement DNS selection policy ?**

3 A policy-based solution

3.1 Source Address Selection

Source Address Selection Requirement

- When the host has multiple IPv6 addresses on the same interface, a host can dynamically select its own source address based on a selection policy.
- The RG can determine the address selection policy for each uplink, and distribute the policy to the hosts in IPv6 home network.
- Hosts can get the address selection policy from the RG.

IPv6 Policy Table (RFC 3484)

For ***source*** address selection

Prefix	Precedence	Label	Explanation
::1/128	50	0	Loopback
::/0	40	1	Native IPv6 addresses
2002::/16	30	2	6to4
::/96	20	3	IPv4 compatible addresses
::ffff:0:0/96	10	4	IPv4 mapped address
2001::/32	5	5	Teredo (Windows)

Longest prefix match → Ignore precedence (dest. addr selection) → Retrieve label

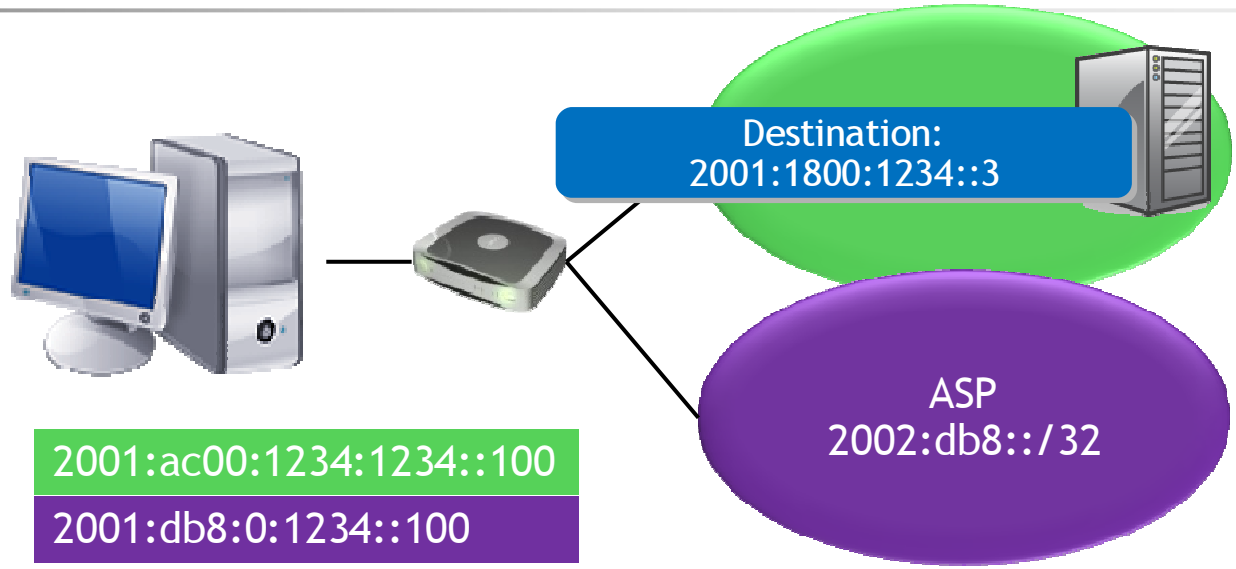
Rule 6: Prefer matching label

Try to match source and dest. address labels

Example use of policy table

For ***source*** address selection

Prefix	Precedence	Label
::1/128	50	0
::/0	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4
2001::/32	5	5

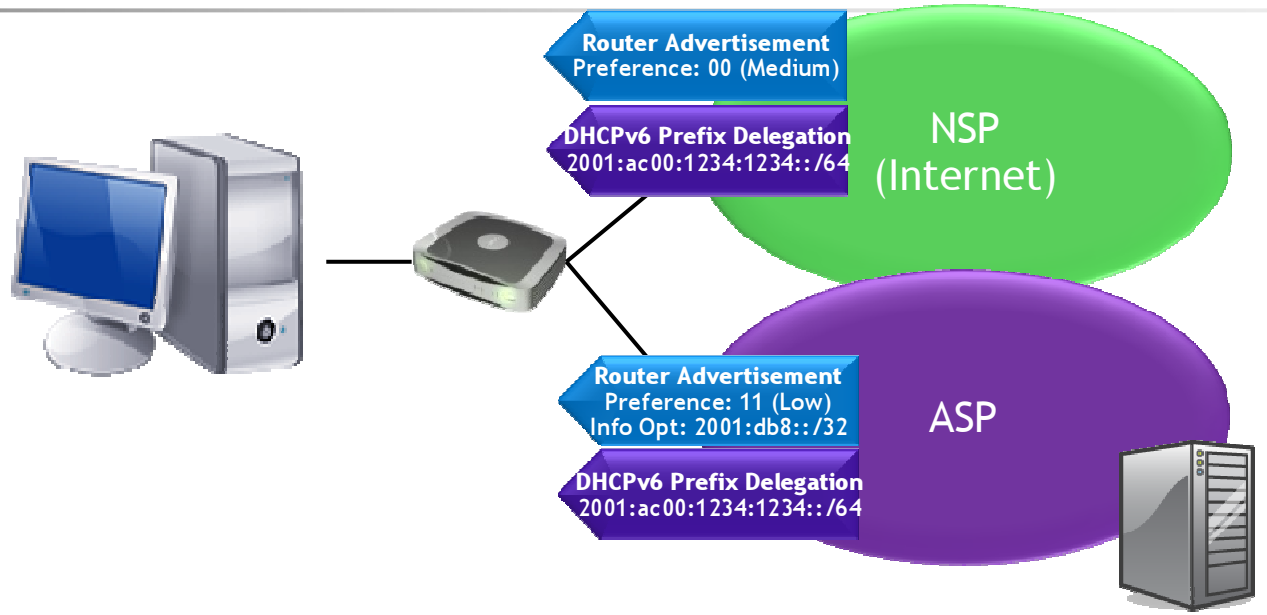


Source	Source Label	Destination	Destination Label
2001:ac00:1234:1234::100	1	2001:1800:1234::3	1
2001:db8:0:1234::100	1	2001:1800:1234::3	1

Automatic Table Generation

For ***source*** address selection

Prefix	Prec	Label
::1/128	50	0
::/0	40	1
2001:ac00:1234:1234::/64	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4
2001::/32	5	5
2001:db8::/32	1	10
2002:db8:0:1234::/64	1	10



RG Route Table

Prefix	Next-Hop
::/0	NSP
2001:db8::/32	ASP

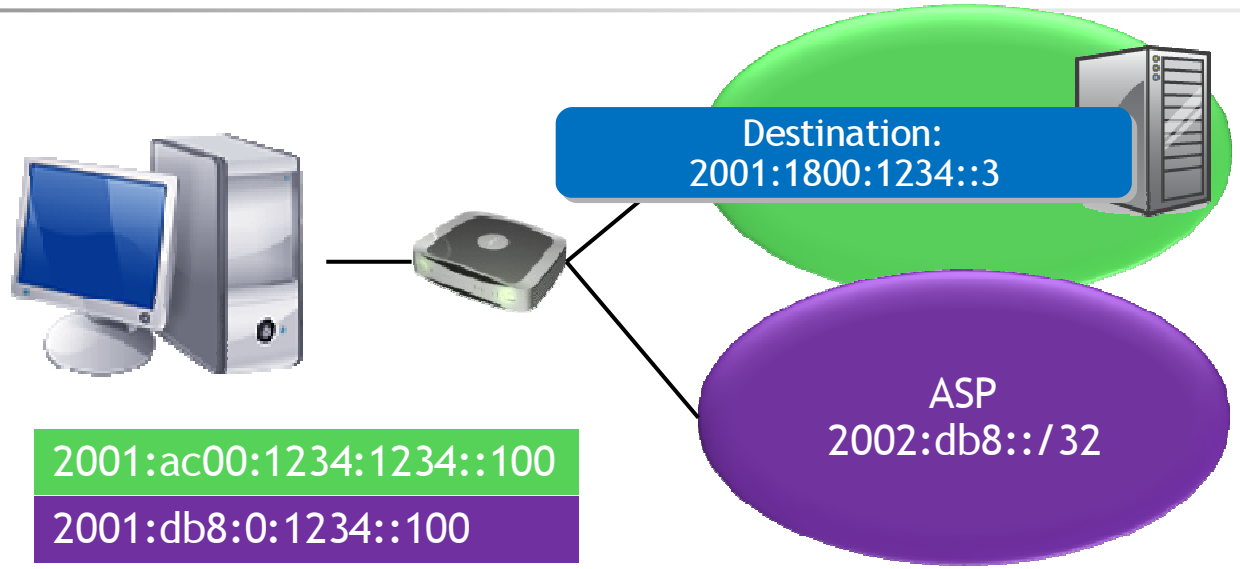
RG Delegated Prefix Table

Delegated Prefix	Origin
2001:ac00:1234:1234::/64	NSP
2002:db8:0:1234::/64	ASP

Example use of policy table

For ***source*** address selection

Prefix	Prec	Label
::1/128	50	0
::/0	40	1
2001:ac00:1234:1234::/64	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4
2001::/32	5	5
2001:db8::/32	1	10
2002:db8:0:1234::/64	1	10

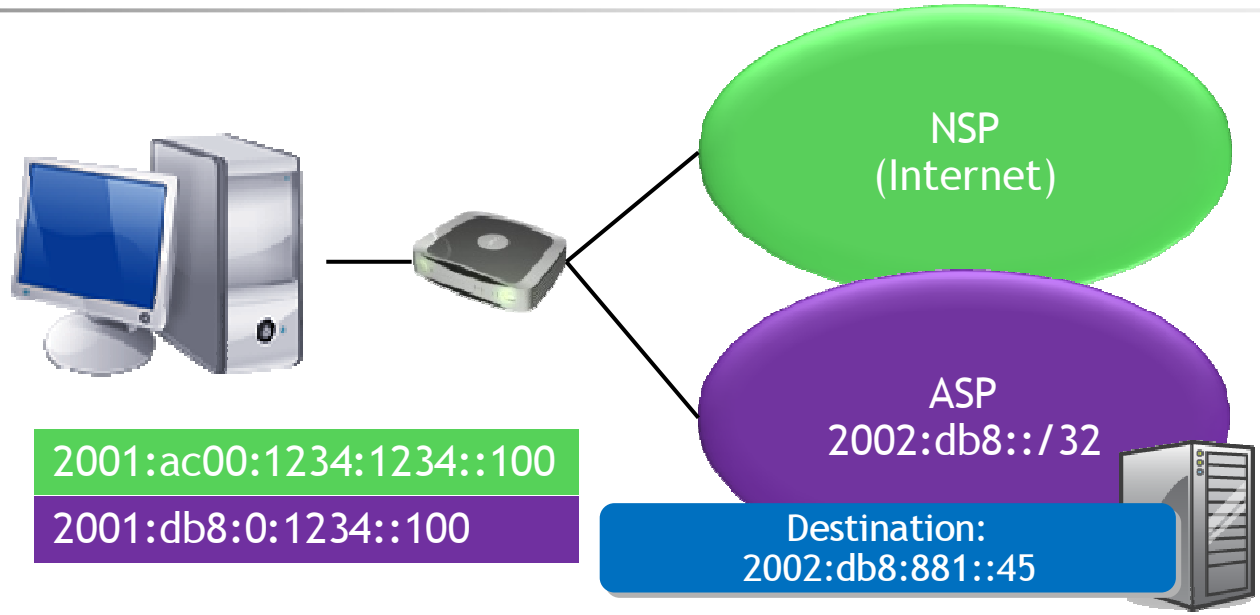


Source	Source Label	Destination	Destination Label
2001:ac00:1234:1234::100	1	2001:1800:1234::3	1
2001:db8:0:1234::100	10	2001:1800:1234::3	1

Example use of policy table

For ***source*** address selection

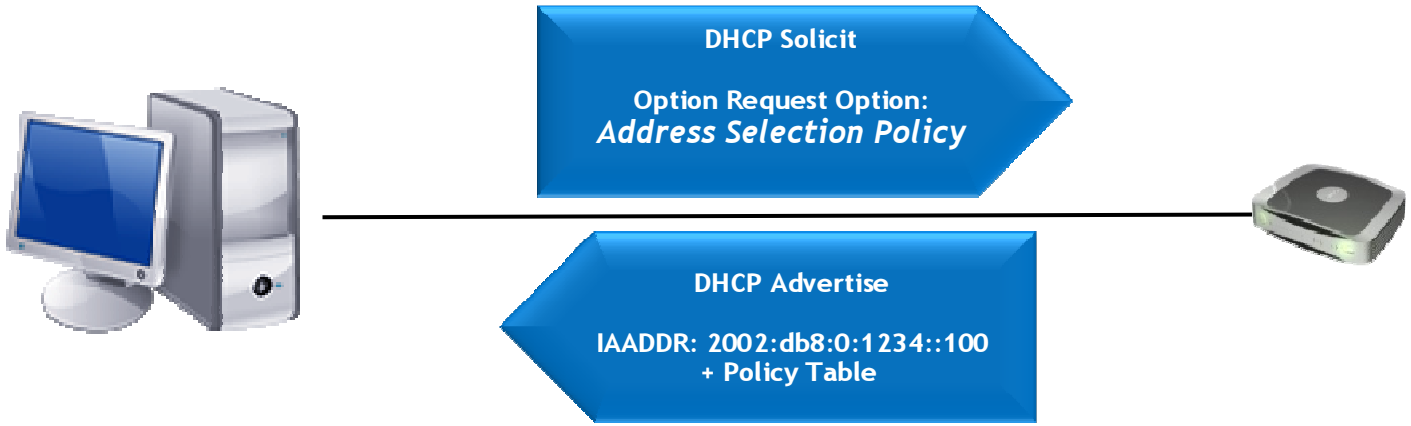
Prefix	Prec	Label
::1/128	50	0
::/0	40	1
2001:ac00:1234:1234::/64	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4
2001::/32	5	5
2001:db8::/32	1	10
2002:db8:0:1234::/64	1	10



Source	Source Label	Destination	Destination Label
2001:ac00:1234:1234::100	1	2002:db8:881::45	10
2001:db8:0:1234::100	10	2002:db8:881::45	10

Conclusion: Source address selection policy

- Can be configured automatically by combining the RG routing table and a table of delegated prefixes: explicit policy table
- A mechanism to pass information to the client is required: "*draft-fujisaki-dhc-addr-select-opt*" is one of the possible solution
- Only hosts which request the Address Selection Policy will be assigned an IPv6 address from the ASP networks and provided the policy



3.2 Route Selection

How to populate routes on the RG?

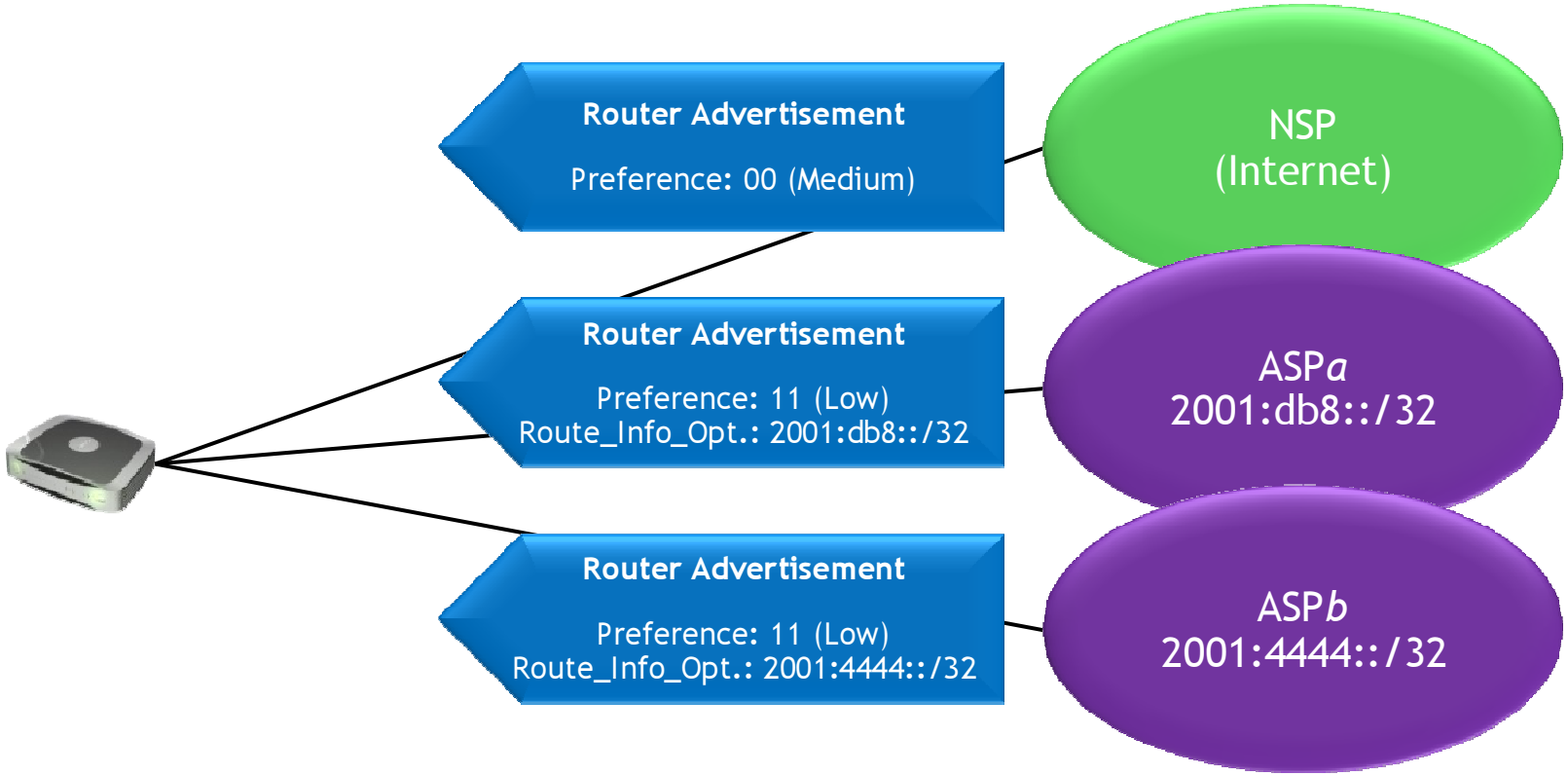
<Requirement>

- RG can select the route for each uplink

<Possible solutions>

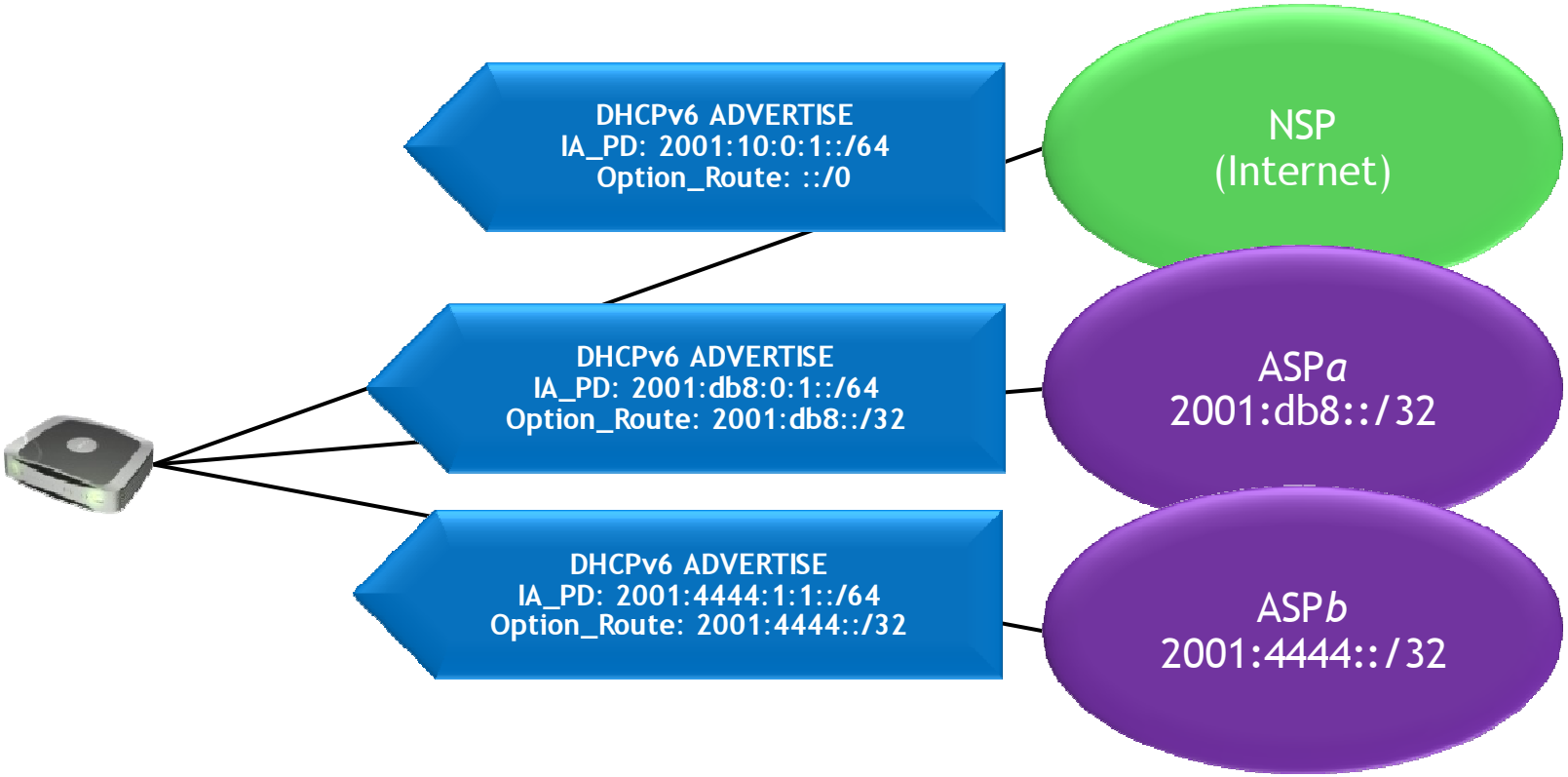
- RFC 4191 - Default Router Preference and More Specific Routes
- DHCPv6 - Route Option (*draft-dec-dhcpv6-route-option-02)*
- Static Configuration
- TR-069
- RIPng

RFC 4191 Example



Prefix	Next-hop
::/0 (default)	NSP
2001:db8::/32	ASP*a*
2001:4444::/32	ASP*b*

DHCPv6 – Route Option Example



Prefix	Next-hop
::/0 (default)	NSP
2001:db8::/32	ASP*a*
2001:4444::/32	ASP*b*

Conclusion: Routing Policy

Distributing routing policy to the RG allows for the simple routing of packets based on destination IP

Avoids a need to track remote destinations

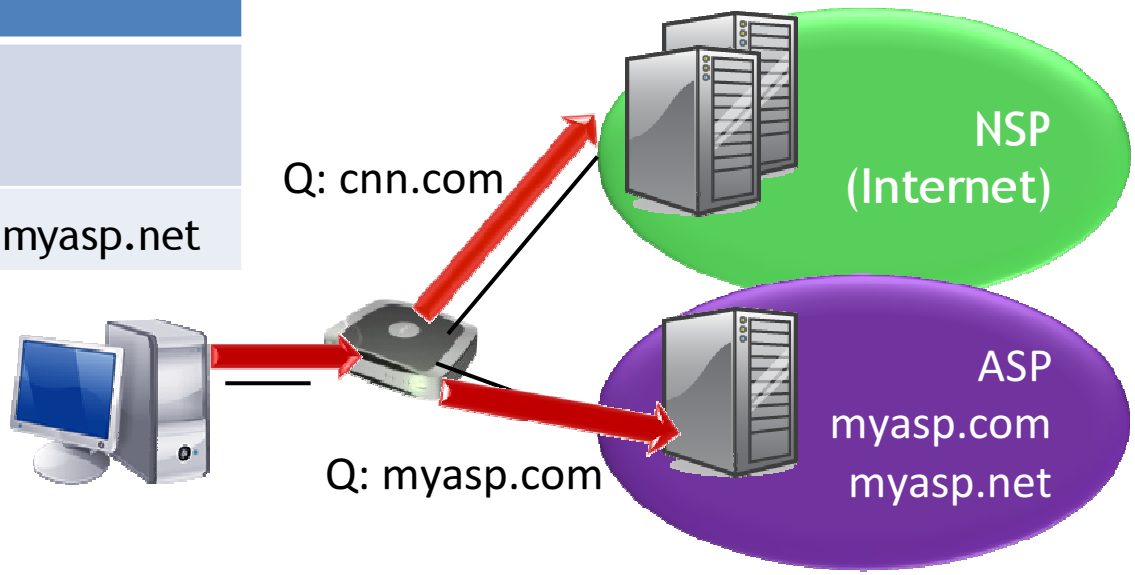
Policy gives operators and users the ability to influence behavior to suit their needs (such as with VPN access)

3.3 DNS Selection

DNS selection requirements

- "A user can resolve a FQDN from the qualified ASP's DNS server(s)."
  - Domain Name can be used to represent "qualification".
  - An ASP can have multiple DNS servers and Domain Name.
  - For NSP's case , an ASP can be qualified for ANY domains.

DNS Server	Domain Name
2001:db8:1::53 fd00:1:1:1:1::53	[ANY]
2001:db8:2::53	.myasp.com, .myasp.net



DNS selection possible solutions

1) Distribute Domain Name to DNS Server mapping information

- By DHCP or RA.
- "***draft-savolainen-mif-dns-server-selection***" shows the solution.

DNS Server	Domain Name
2001:db8:1::53 fd00:1:1:1:1::53	[ANY]
2001:db8:2::53	.myasp.com, .myasp.net

2) Send DNS queries to every possible DNS servers:

- Clear drawbacks are extra-load on DNS servers.
- Also when multiple replies are returned, it's hard to tell which answer is qualified.

Conclusion: DNS selection policy

Hosts themselves do not require DNS policy: the RG acts as a DNS relay/proxy

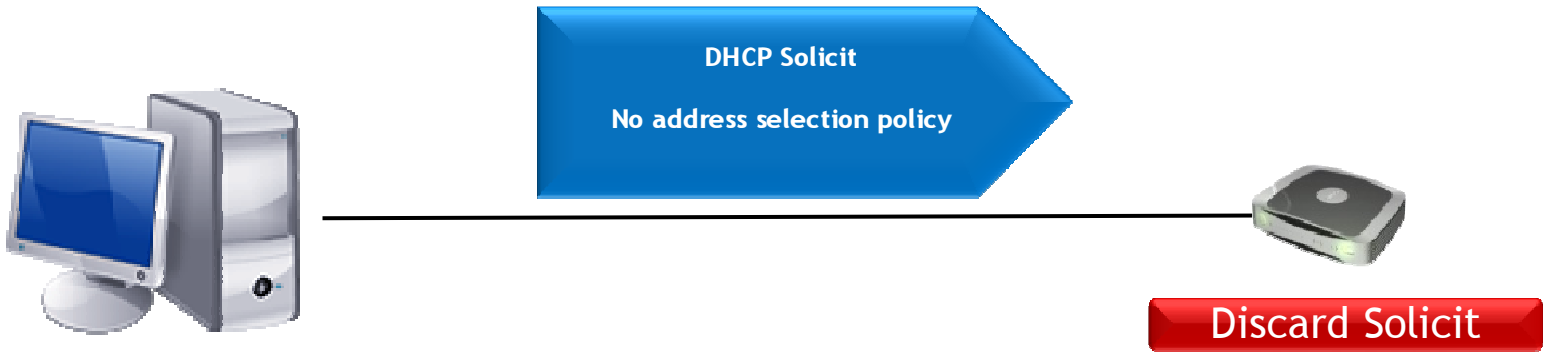
The RG DNS proxy will direct the DNS query to the appropriate name server

4 Legacy Host Support

DHCPv6 without Address Selection Policy

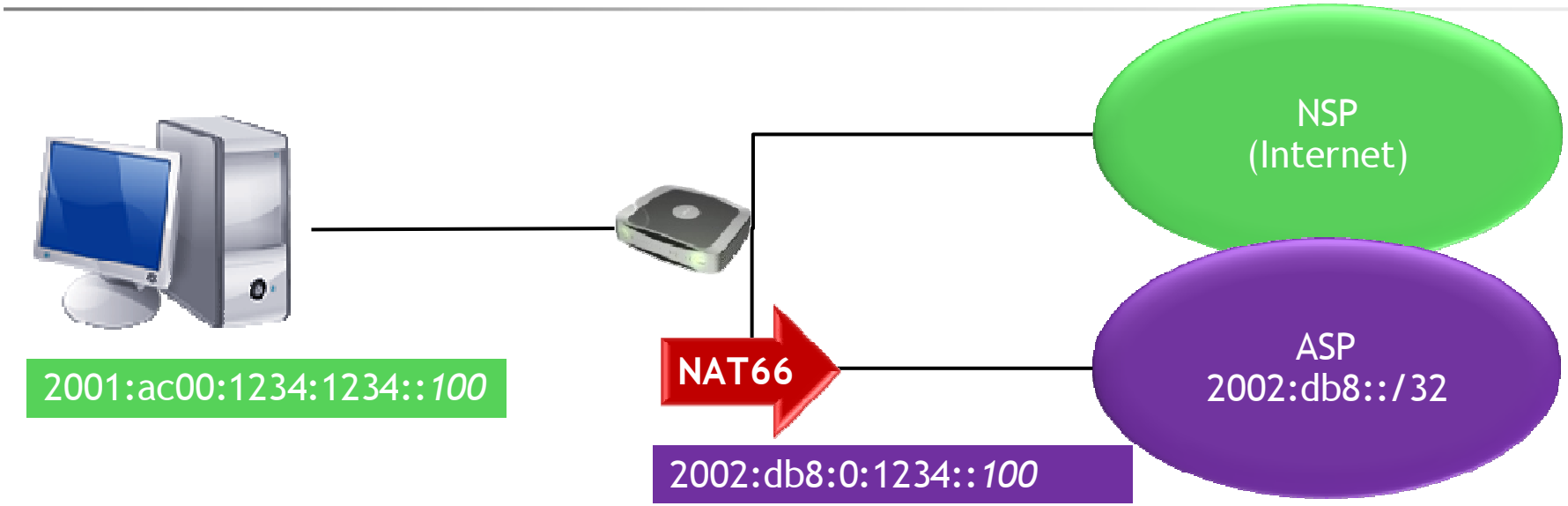
- We should not give multiple addresses to hosts which cannot support address selection policy, if a request is sent we discard the Solicit (per RFC)

- DNS and routing are provided by the RG, so legacy hosts can access ASP services via NAT66



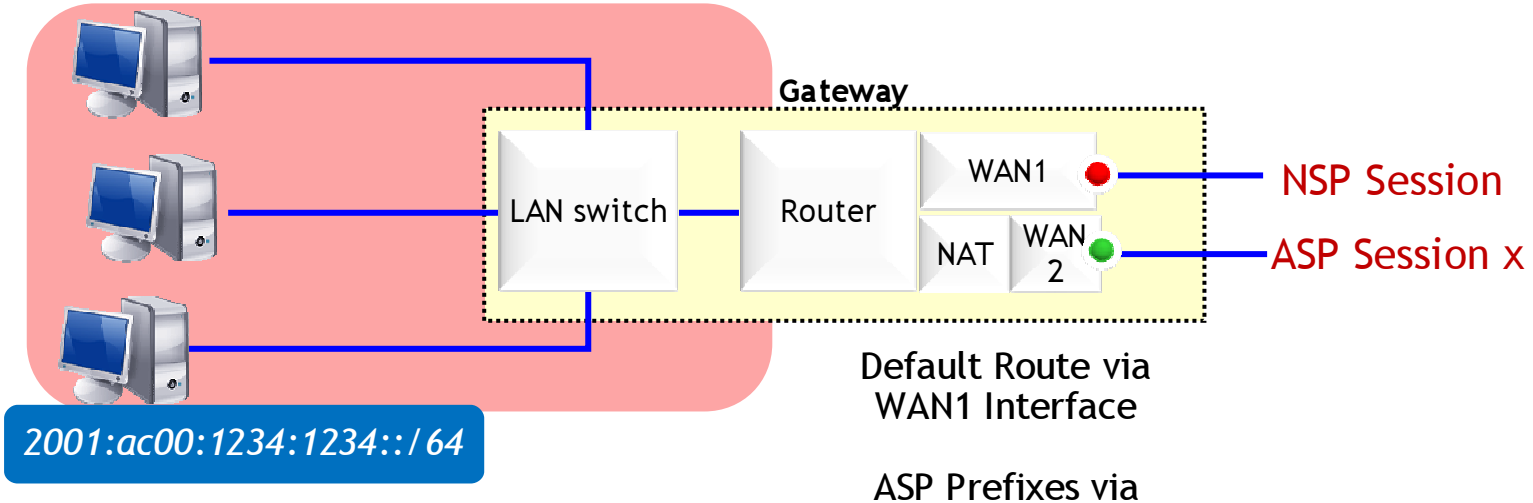
Hosts without policy table

For ASP access



- ***Stateless*** 1:1 NAT66
  2001:ac00:1234:1234:w:x:y:z <-> 2002:db8:0:1234:w:x:y:z
- NAT66 should be the option of last resort for hosts which don't support policy.

Gateway Routing Table



Prefix	Next-hop
::/0 (default)	WAN1
2002:db8::/32	WAN2 (NAT)

5 Considerations of How to put this model into BBF

Recommendations

- TR-124 expanded to include gateway operation for multiple links (IPv6)
- WT-187 normative reference to TR-124bis multi-link operation for PPPoE and L2TP Softwires
- WT-177 normative reference to TR-124bis multi-link operation for IPv6oE

- Solicit operator input and advance IETF drafts in the various WG

Related I-Ds

- ***draft-fujisaki-dhc-addr-select-opt-08*** **@6man wg**
  - October 13, 2009
  - http://tools.ietf.org/html/draft-fujisaki-dhc-addr-select-opt-08
  - Distributing Address Selection Policy using DHCPv6
  - Intended status: Standards Track
  - T. Fujisaki, A. Matsumoto NTT, R. Hiromi Intec Netcore
- ***draft-dec-dhcpv6-route-option-02*** **@dhc wg**
  - October 19, 2009
  - http://tools.ietf.org/html/draft-dec-dhcpv6-route-option-02
  - DHCPv6 Route Option
  - Intended status: Informational
  - W. Dec, R. Johnson Cisco Systems
- ***draft-savolainen-mif-dns-server-selection-01*** **@mif wg**
  - October 20, 2009
  - http://tools.ietf.org/html/draft-savolainen-mif-dns-server-selection-01
  - DNS Server Selection on Multi-Homed Hosts
  - Intended status: Informational
  - T. Savolainen Nokia

Thank You