IPv6 via IPv4 Service Provider Networks (6rd)

draft-ietf-softwire-ipv6-6rd-01

IETF 76, Hiroshima

November 8-13, 2009

softwire Working Group

Mark Townsley (townsley@cisco.com)

Ole Trøan, (ot@cisco.com)

6rd - summary

- @IETF75: presented in v6ops, softwire, dhc working groups
- Accepted as a working group item
- Revision -01 changes:
  - Suggestion to use DHCP Inform on PPP links (remove IPCP option from base spec, does not eliminate it to be defined in a separate specification in the future)
  - DHCP option to use v4suffix instead of v4prefix (semantics)
  - Removed "domain-id" – same functionality possible with separate 6rd prefixes
  - Forwarding loop and anti-spoofing rules nailed down (detail in this presentation if we have time and desire to talk about it in the meeting)
  - General text cleanup, thanks for all the great reviews!
- Goal: base 6rd specification ready for WG last call shortly after this IETF meeting

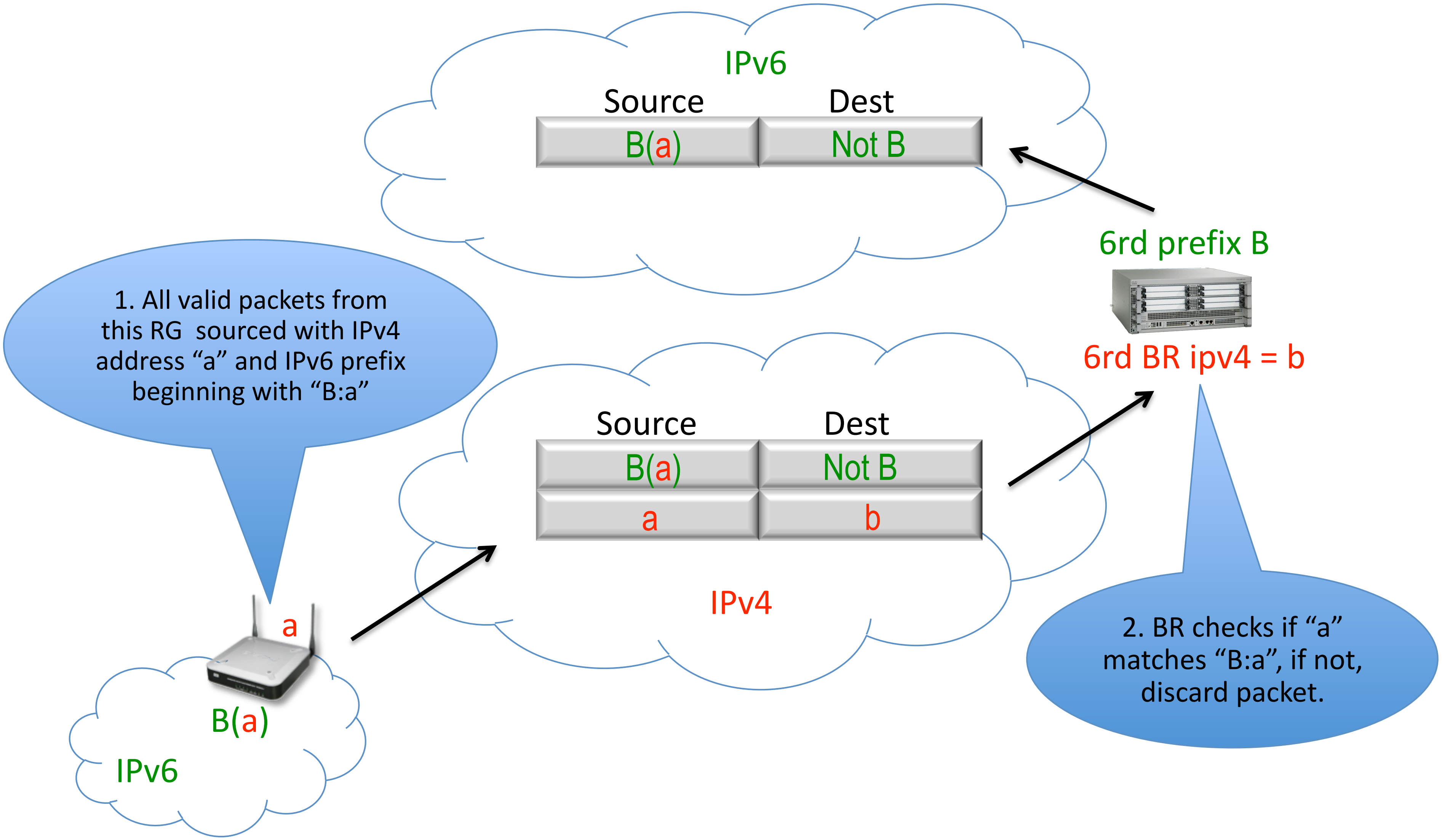
6rd Anti-Spoofing and Loop Protection Border Relay Rules

1. On tunnel decap, check the source IPv4 address and source IPv6 prefix to ensure that the mapping between matches
2. 6rd (anycast) IPv4 BR addresses should be unreachable from outside the SP
3. IPv4 ACLs on BR routers that prohibit sending or receiving packets to or from other relays within the SP

6rd Anti-Spoofing and Loop Protection Customer Edge (RG) Rules

1. On tunnel decap, check the source IPv4 address and source IPv6 prefix to ensure that the mapping between matches, *or that the packet was sourced from the configured IPv4 Border Relay (anycast) address*
2. Arriving IPv6 packets with a destination address outside the 6rd Delegated Prefix for the RG are discarded

Antispoofing at the BR



1. All valid packets from this RG sourced with IPv4 address “a” and IPv6 prefix beginning with “B:a”

IPv6

Source	Dest
B(a)	Not B

6rd prefix B

6rd BR ipv4 = b

Source	Dest
B(a)	Not B
a	b

IPv4

a

B(a)

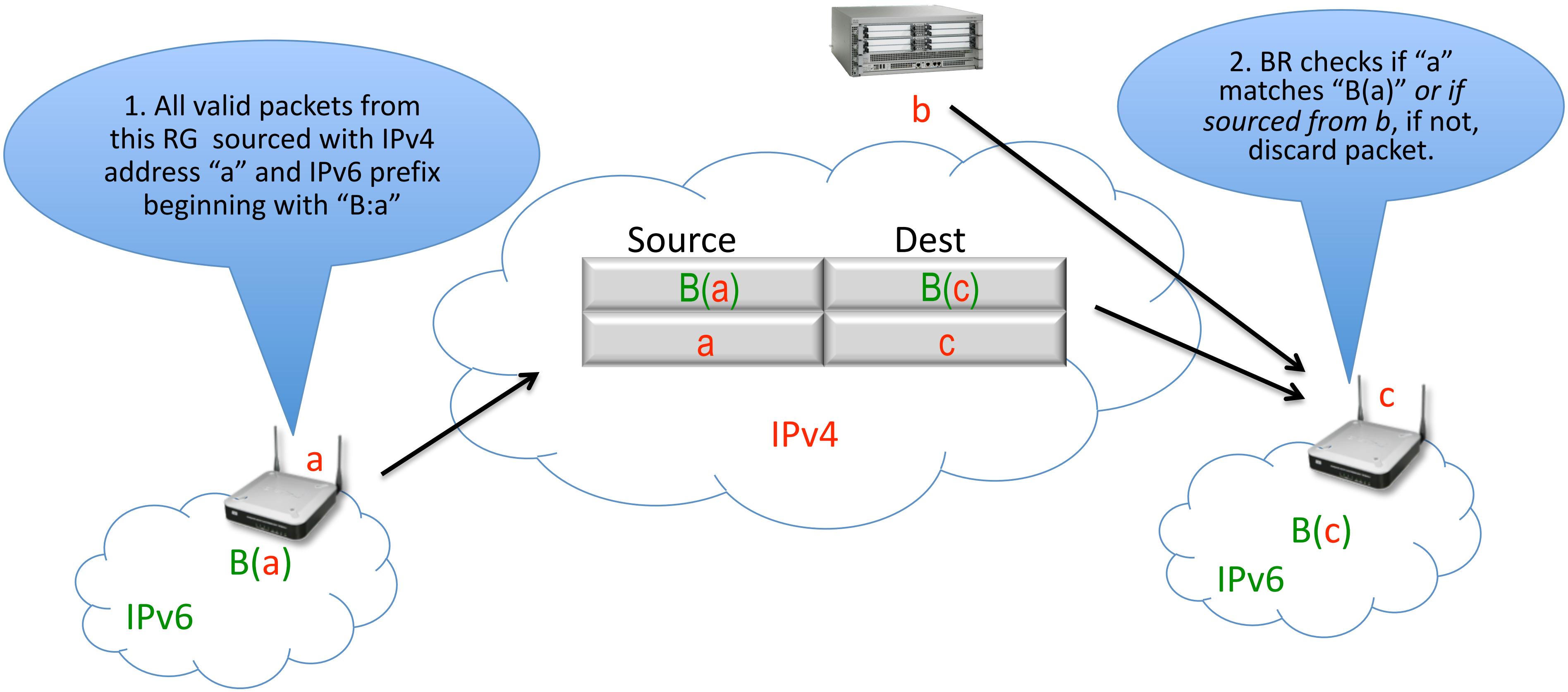
IPv6

2. BR checks if “a” matches “B:a”, if not, discard packet.

IPv6 Prefixes in Green Capital Letters
IPv4 addresses in red lowercase

Antispoofing at the CE

Anti-spoofing rule is the same on the BR as on the RG, except that source address from Border Relay is specifically allowed.



1. All valid packets from this RG sourced with IPv4 address “a” and IPv6 prefix beginning with “B:a”

2. BR checks if “a” matches “B(a)” *or if sourced from b*, if not, discard packet.

Source	Dest
B(a)	B(c)
a	c

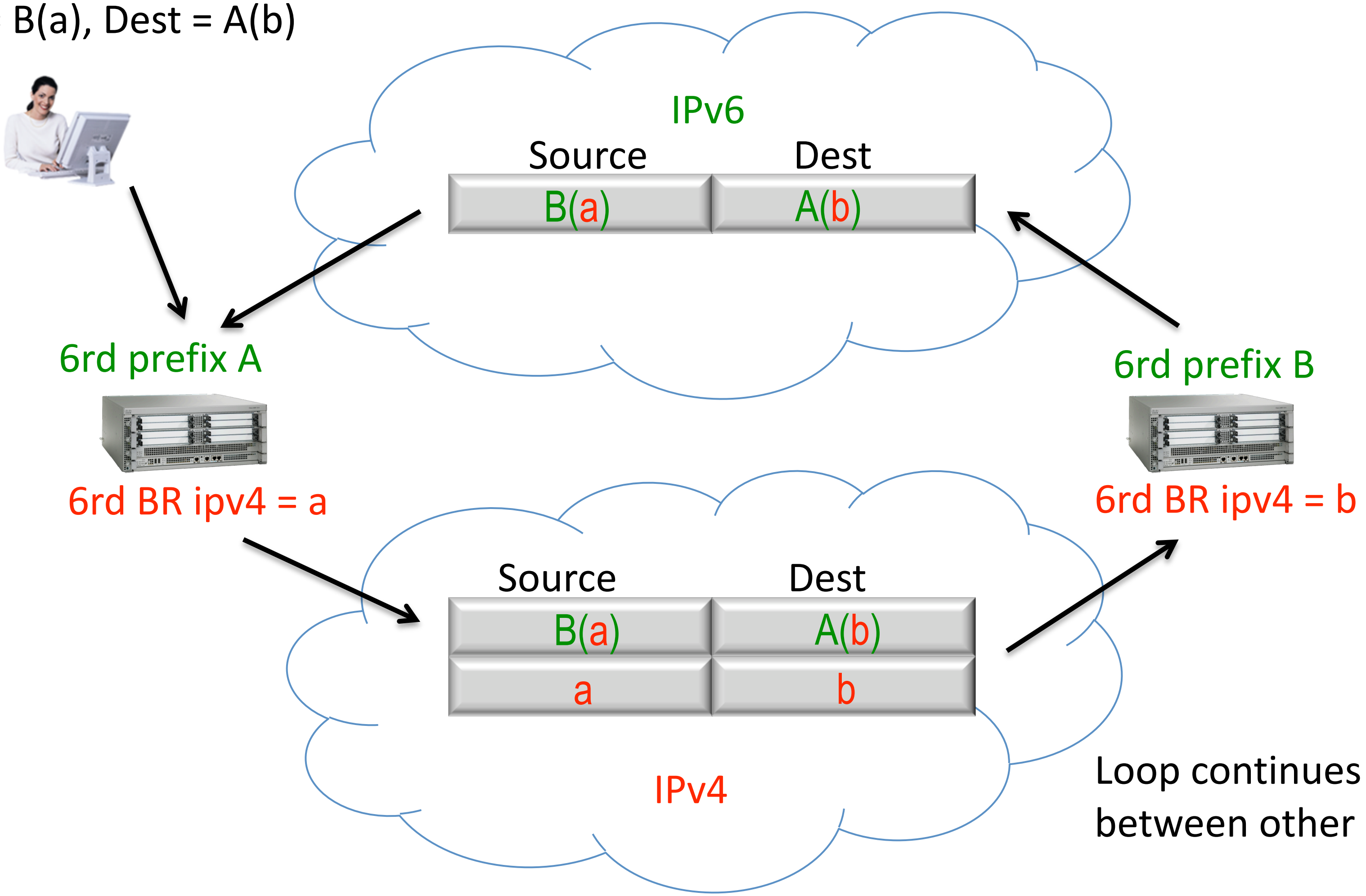
IPv6 Prefixes in Green Capital Letters
IPv4 addresses in red lowercase

Looping – 2 Cases

1. Concerned with amplification attacks where a 3rd party can cause packets to loop between two other nodes.
2. Not concerned with looping between an attacker's own equipment and a relay

1. Amplification DOS Attack

Hacker launches first packet
src = B(a), Dest = A(b)



IPv6

Source	Dest
B(a)	A(b)

6rd prefix A

6rd BR ipv4 = a

6rd prefix B

6rd BR ipv4 = b

Source	Dest
B(a)	A(b)
a	b

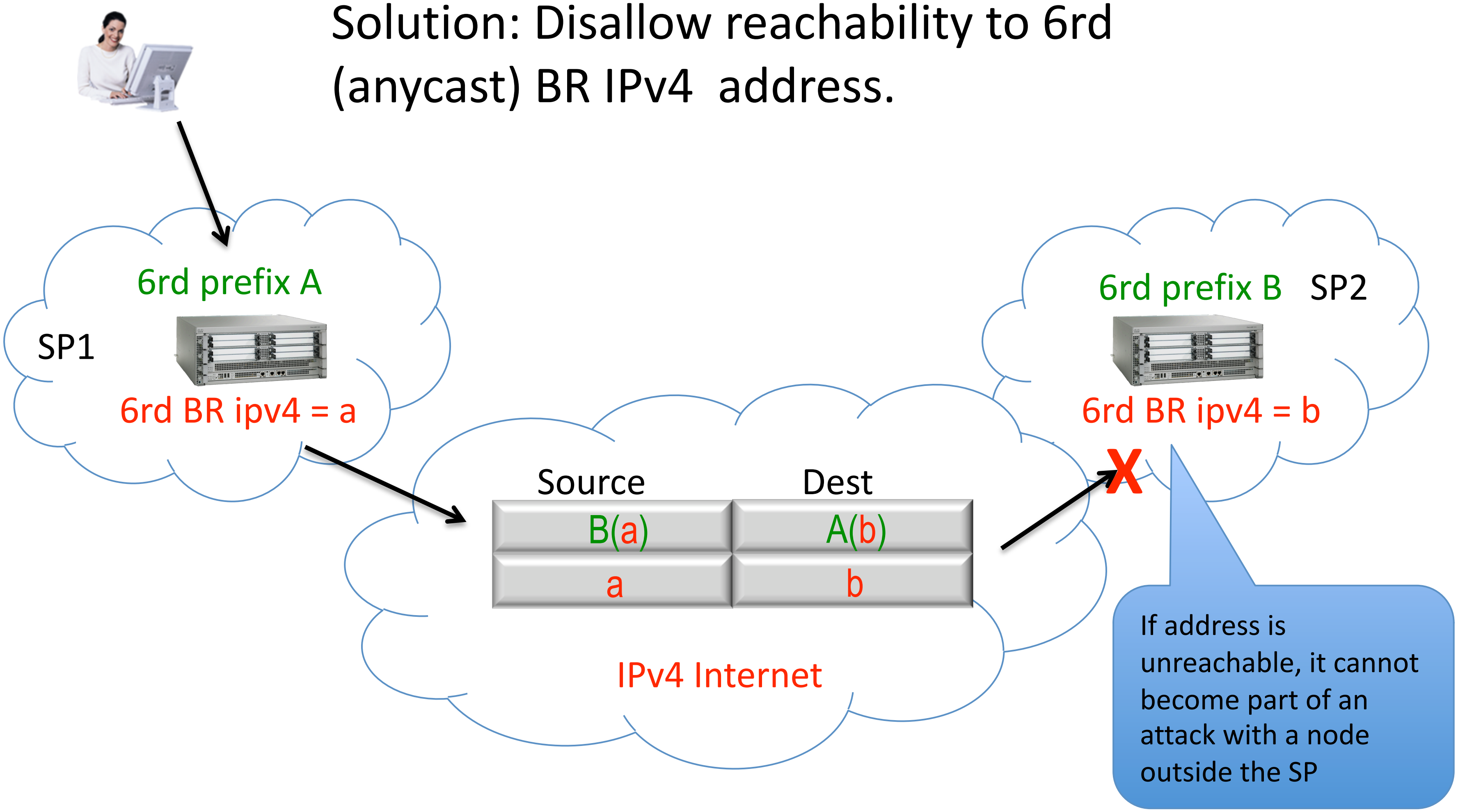
IPv4

Loop continues
between other nodes

IPv6 Prefixes in Green Capital Letters
IPv4 addresses in red lowercase

Looping between relays outside SP

Solution: Disallow reachability to 6rd (anycast) BR IPv4 address.



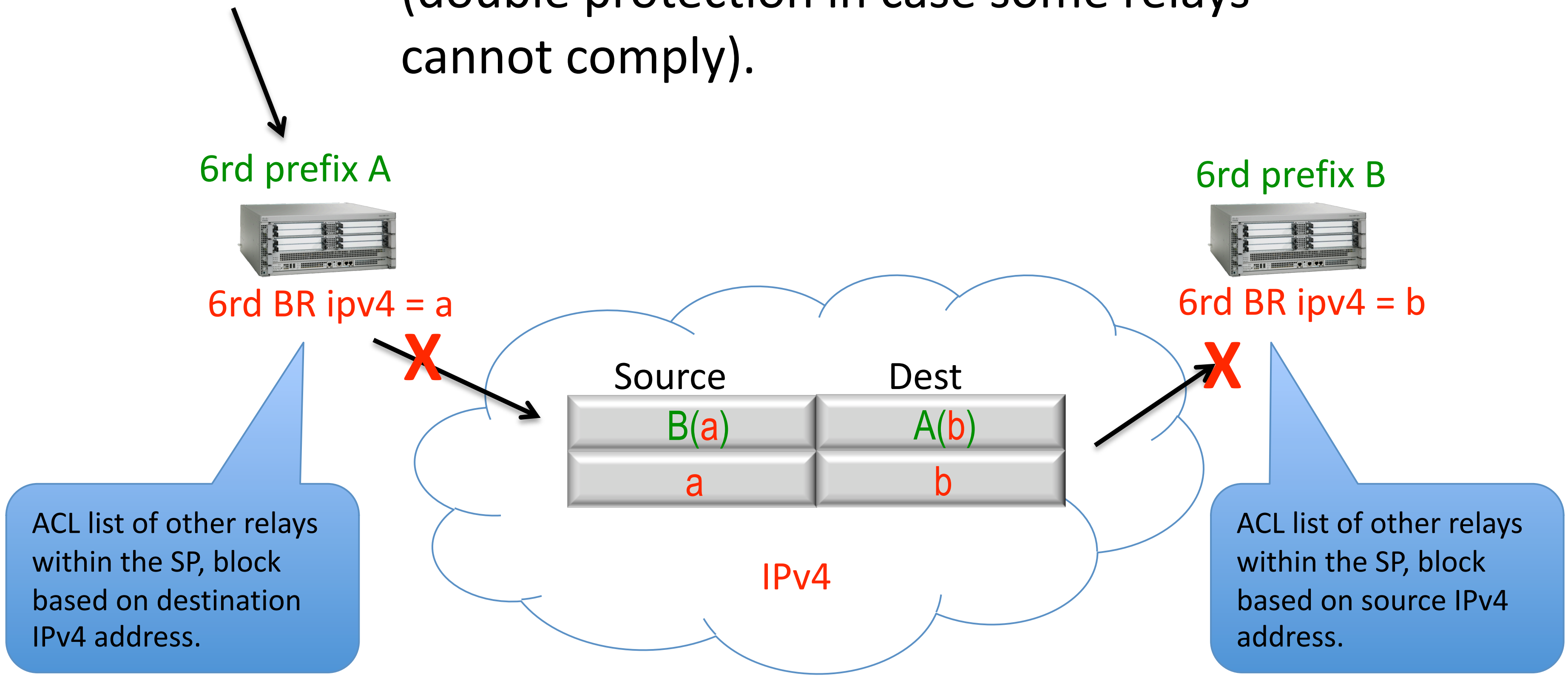
Source	Dest
B(a)	A(b)
a	b

If address is unreachable, it cannot become part of an attack with a node outside the SP

IPv6 Prefixes in Green Capital Letters
IPv4 addresses in red lowercase

Looping between relays inside single SP

Block packets to and from other relays (double protection in case some relays cannot comply).



Source	Dest
B(a)	A(b)
a	b

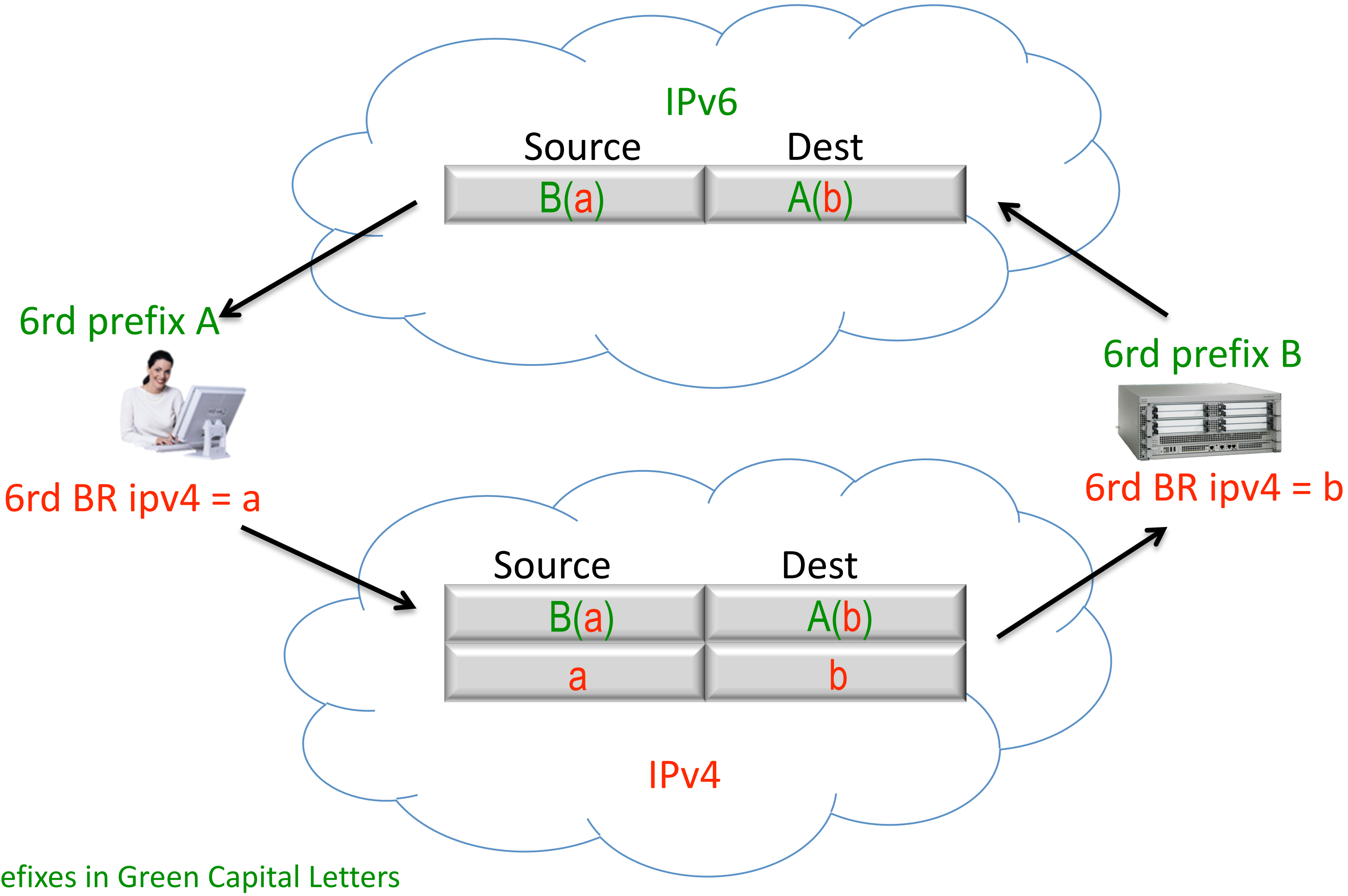
ACL list of other relays within the SP, block based on destination IPv4 address.

ACL list of other relays within the SP, block based on source IPv4 address.

IPv6 Prefixes in Green Capital Letters
IPv4 addresses in red lowercase

2. Loop between BR and attacker

Uses no more resources than normal traffic traversing the BR.
No amplification, no more DOS than legitimate IPv6 traffic.



IPv6

Source	Dest
B(a)	A(b)

6rd prefix A

6rd BR ipv4 = a

6rd prefix B

6rd BR ipv4 = b

Source	Dest
B(a)	A(b)
a	b

IPv4

IPv6 Prefixes in Green Capital Letters
IPv4 addresses in red lowercase

Next Steps

- Implementations exist and code is running
- Draft has received significant review
- Ready for WG Last Call and advancement just this meeting?