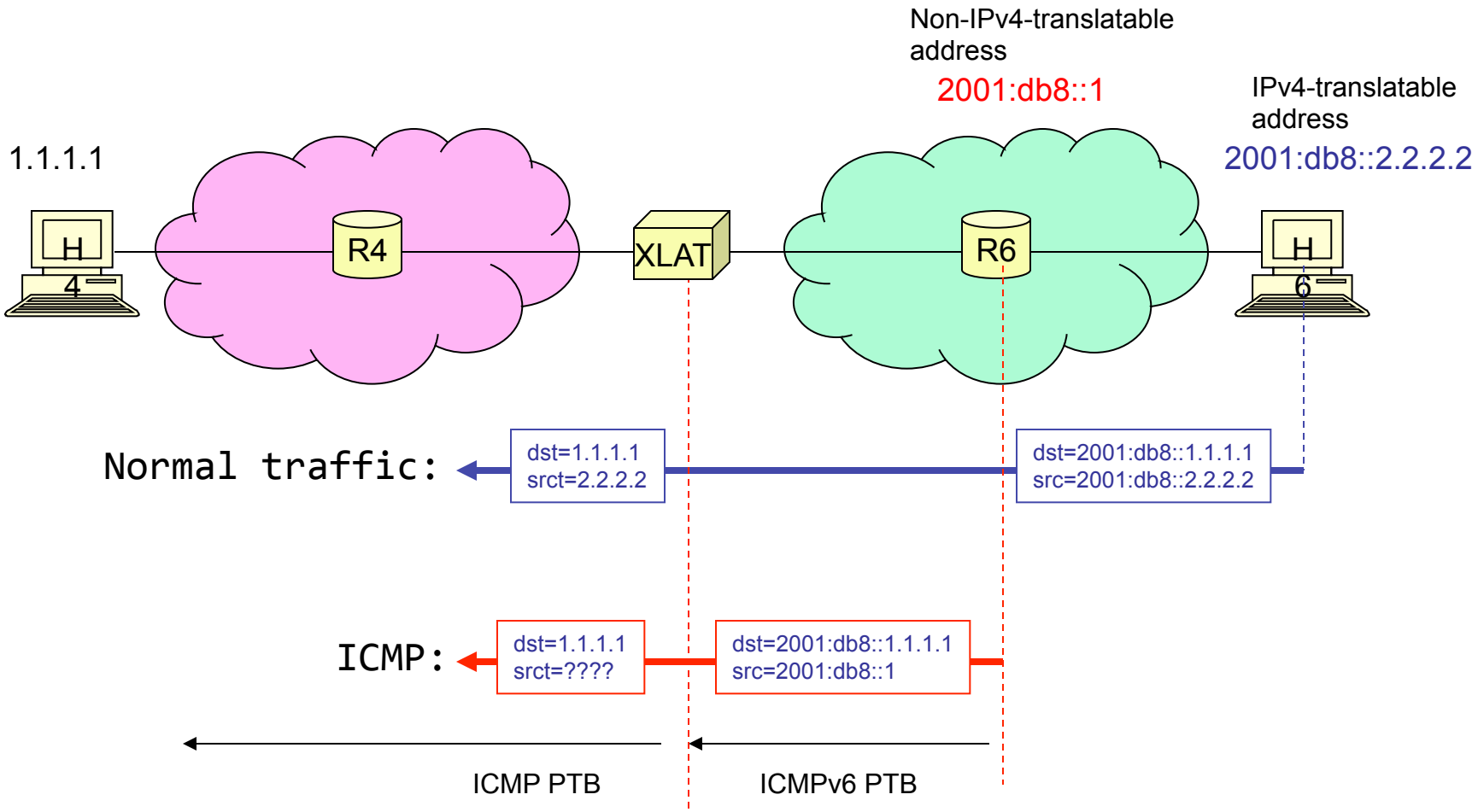
Stateless Source Address Mapping for ICMPv6 Packets

X. Li, C. Bao, D. Wing,
R. Vaithianathan, G. Huston

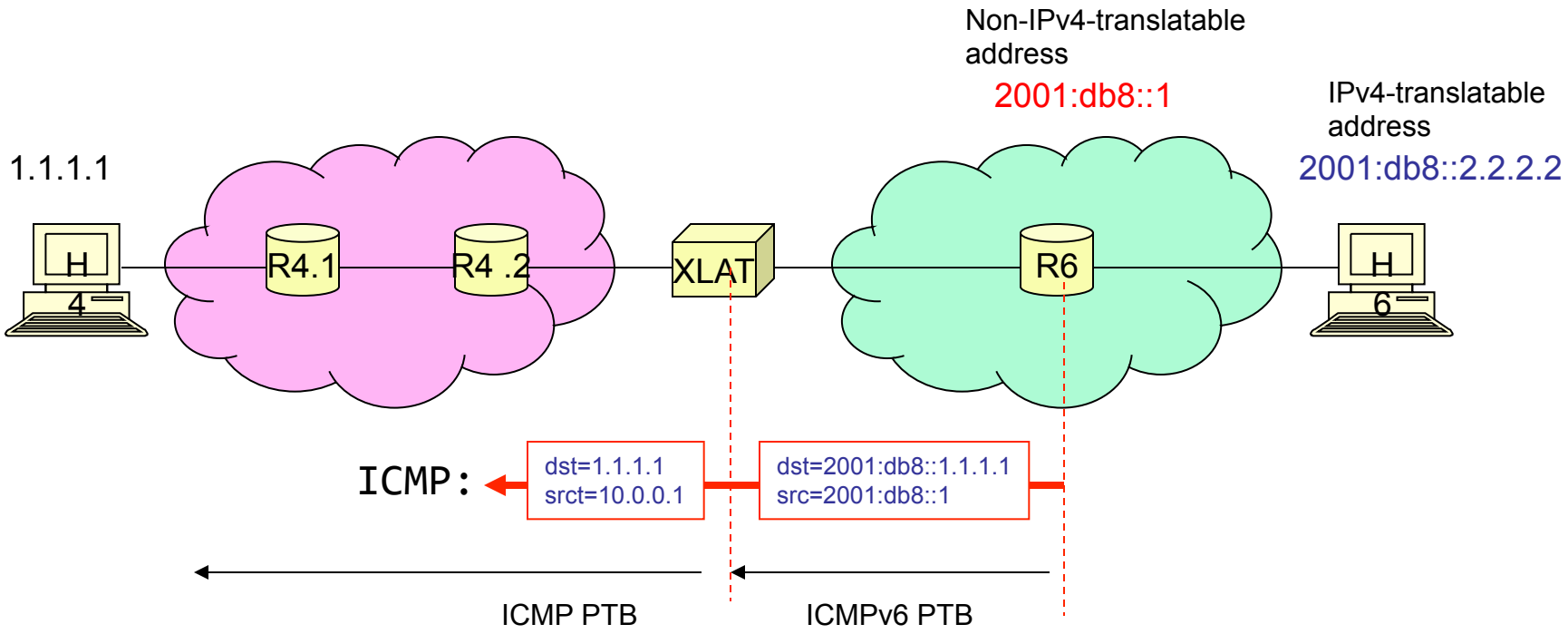
2011-11-12

Introduction



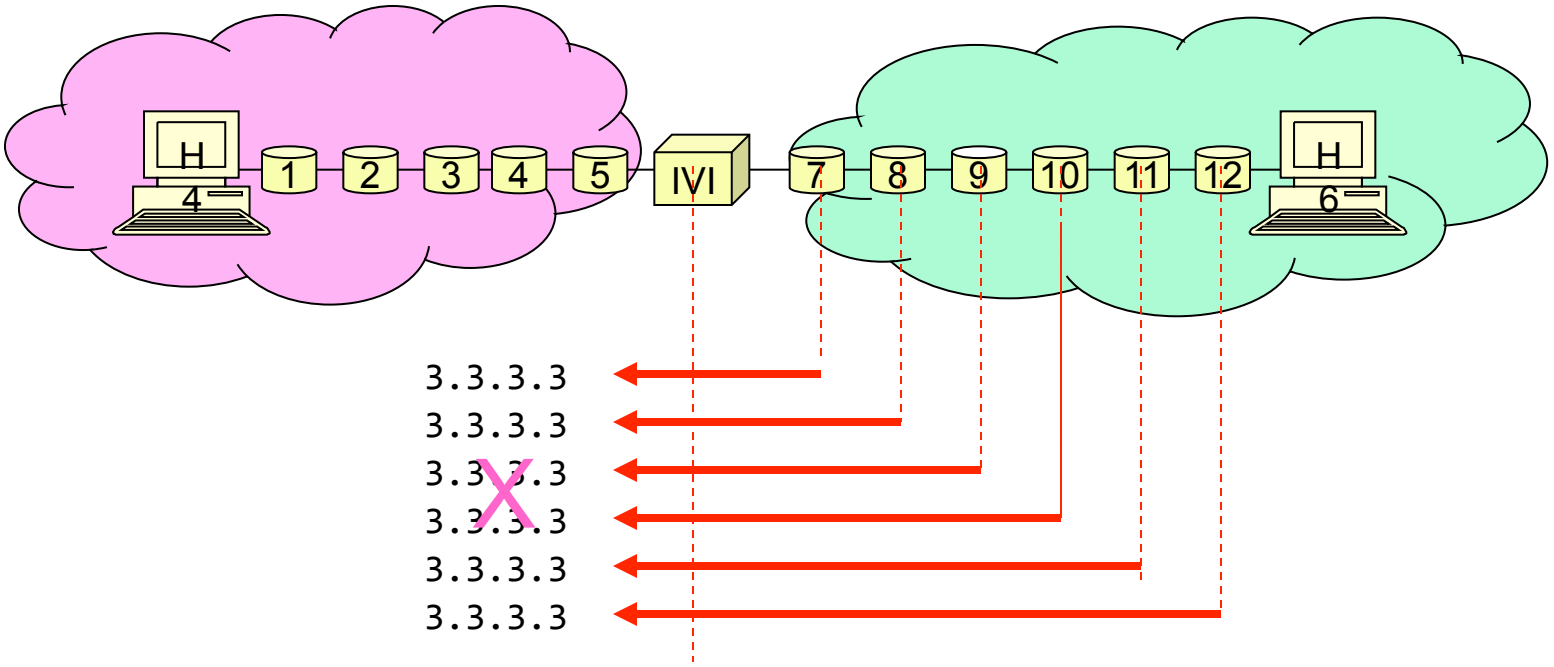
RFC6145: The IPv6 addresses in the ICMPv6 header may not be IPv4-translatable addresses. … A mechanism by which the translator can instead do stateless translation is left for future work.

Requirements (1)



- uRPF → cannot use RFC1918 addresses
- IPv4 address depletion → hard to use public IPv4 addresses

Requirements (2)



- IPv4 recipient of the ICMP message should be able to distinguish between different IPv6 ICMPv6 origination → needs a pool

Recommendation

- Recommend to drawing an IPv4 /24 prefix from the IANA Special Purpose Address Registry as a "Well-Known Prefix" for use by IPv4/IPv6 translators for the purpose of mapping otherwise untranslatable IPv6 source addresses of ICMPv6 messages to IPv4 ICMP messages.
- These addresses are for use
  - As the source address of ICMP packets
  - Not as a destination address for any packets

Mapping Algorithms

- When an IPv4 /24 prefix is allocated to represent the source address of ICMP, the least-significant byte can be generated using one of the following algorithms.
  - Randomly
  - Copy the "Hop Count" in the IPv6 header of the ICMPv6
  - Hashing of the IPv6 address
- The selection of the algorithm SHOULD be a configuration function in the IPv4/IPv6 translator.
  - May not generate subnet identifier or broadcast addresses

Routing Considerations

- As packets passing through the public network need to pass through conventional packet filters, including uRPF filters [RFC3704]
  - The assigned address may be used in routing advertisements
  - Such routing advertisements are non-exclusive and should be accepted from any originating AS in an anycast fashion

Security Considerations

- The use of an address for source addresses in ICMP error packets is considered "safe" in so far as ICMP packets are not intended to generate responses directed to the source address.
- However it is possible to use this address as a means of gaining anonymity when launching a denial of service attacks by using this address as the source address for other forms of malicious traffic.
- Packet firewall filters should be configured discarding
  - All non-ICMP packets that use the IANA-assigned /24 network as a source address
  - All packets that use the IANA-assigned /24 network as a destination address.

IANA Considerations

- Prefix 192.70.192.0/24
- Description: To be used in the context of generating an IPv4 source address for mapped ICMPv6 packets being passed through a stateless IPv4/IPv6 translator.
- Begin: 2011-06-01
- End: Never
- Purpose: Stateless ICMPv6/ICMP translation
- Scope: Addresses from the assigned address prefix are

  network.

Additional discussions

Why not use RFC1918?

- draft-kirkham-private-ip-sp-cores-07 (Issues with Private IP Addressing in the Internet) discussed a similar situation
  - Conservation of Address Space
  - Effects on Traceroute
  - Effects on Path MTU Discovery
  - Unexpected interactions with some NAT implementations
  - Interactions with edge anti-spoofing techniques
  - Peering using loopbacks
  - DNS Interaction
  - Operational and Troubleshooting issues
  - Security Considerations
- Which shows that RFC1918 will results in difficulties.

How to handle the DDOS?

- When setting up the ACL correctly,
  - The network only allows ICMP packets using this block as the source address.
  - No responses will be generated from any network device in the network.
- However, the ICMP packets using this block as the source address may target some hosts for DDOS attack.
  - Does the anycast root server’s addresses have similar problem?
  - The rate-limit configuration should be used.

It is not traceable

- Two cases:
  - The attacker is in IPv6 and behind a real IPv4/ IPv6 translator
    - Handled in the translator by rate-limiting
  - The attacker is in IPv4 generating ICMP packets using the special block as the source

ISPs need to update their ACLs

- This methods provides more control for the network administrator.
  - We believe it is worth the effort for the transition
- If we can move forward, there will be enough time for ISPs to update the filters.
  - No updating is required for “non-default-free” network.
- The operators still lack the experience of handling a "one-way" special purpose packet that is allowed to leave the link, never mind the AS.
  - We should try.

Alternatives

- A privately assigned block of public IPv4 addresses from existing space, which can be shared between operators
  - Similar to this
- Why not use a “global IPv4 unicast address” bound to the translator
  - IPv4 address depletion problem makes it difficult

NAT and looking-glass

IPv4 firewall schema, but in stateless IPv4-IPv6 Schema, it maybe happen in somewhere IPv4-IPv6 edge of ISP (in middle of end hosts).

- Adding publicly-accessible out-of-band "looking glass" web-server to the IPv6/IPv4 translator
  - May not be easy.

glass" web-server to the IPv6/IPv4 translator
– May not be easy.

To do

- Add recommendation for filtering to an
  - Allow ICMP type 11 - Time Exceeded
  - My Allow ICMP type 12 - Parameter Problem
    - SHOULD NOT allow any of the various ICMP request messages
- Add recommendation for rate limiting of traffic from the prefix as additional countermeasure against abuse of this prefix
- Reverse DNS considerations
  - Help mortal Internet users when they traceroute through an IPv6/v4 translator.

PTB)
against abuse of this prefix
- Reverse DNS considerations
  - Help mortal Internet users when they traceroute through an IPv6/v4 translator.