

# ICMPv6とパケットフィルタの 微妙な関係

JPIX

石田慶樹

2008/4/22

# Abstract

- IPv6で必須となるPMTU discovery(PMTUd)に思わぬ落とし穴があって動かない可能性がないですか？
- BCP38(Source Address Verification)やBCP84(Ingress Filtering for Multihomed Networks)とICMPv6との関係は明確ですか？
- IPv6でIXが使うPrefixの取り扱い

# 関連RFC

- **RFC1981** Path MTU Discovery for IP version 6, Draft Standard, August 1996
- **RFC2827/BCP38** Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, BCP, May 2000
- **RFC3484** Default Address Selection for Internet Protocol version 6 (IPv6), PROPOSED STANDARD, February 2003
- **RFC3704/BCP84** Ingress Filtering for Multihomed Networks, BCP, March 2004
- **RFC4443** Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, Draft Standard, March 2006
- **RFC4890** Recommendations for Filtering ICMPv6 Messages in Firewalls, Informational, May 2007

# はじめに

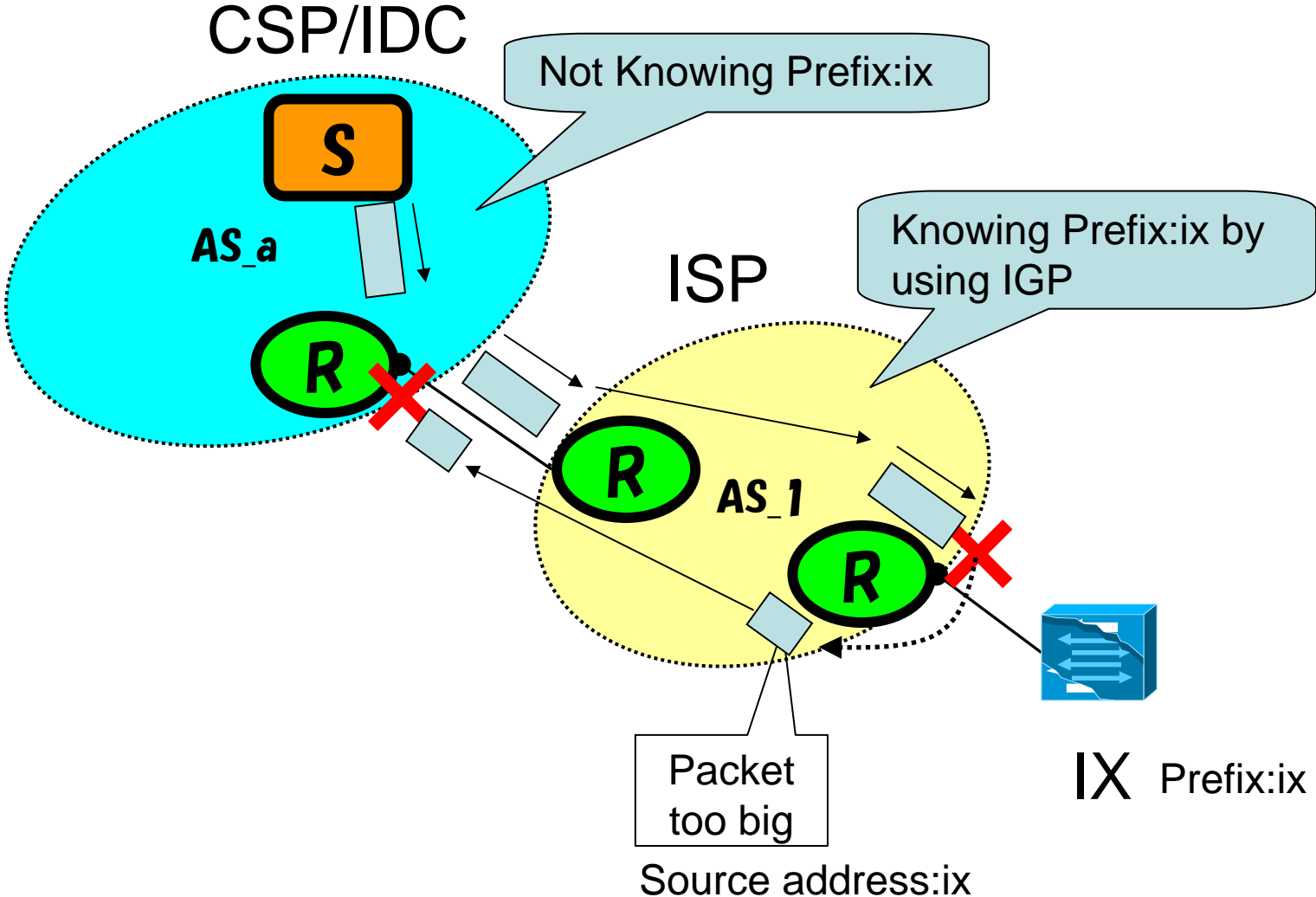
- 今日の議論の前提
  - BCP38/IPv6が当然のこととなっている
  - 技術としてuRPF (strict/feasible/loose)が広く使われている
- 疑問
  - 中間ノードがICMPエラーメッセージを返す場合にそのソースアドレスは何か？  
⇒RFC4443

(b) If the message is a response to a message sent to any other address, such as - a multicast group address, - an anycast address implemented by the node, or - a unicast address that does not belong to the node the Source Address of the ICMPv6 packet MUST be a unicast address belonging to the node. The address SHOULD be chosen according to the rules that would be used to select the source address for any other packet originated by the node, given the destination address of the packet. However, it MAY be selected in an alternative way if this would lead to a more informative choice of address reachable from the destination of the ICMPv6 packet.
  - そのソースアドレスはアナウンスされてるか？
  - ICMPv6とソースアドレス・フィルタリングはどちらを優先するか？  
⇒BCP38 vs RFC4890

# 思考実験

1. IXはIXP用のIPv6アドレスを利用している
2. そのIPv6アドレスはグローバルにアナウンスされていない
3. IXを利用するISPはバックボーンではジャンボフレームを利用している
4. IXでは通常のフレームサイズが利用されている
5. 何が起こるのか？

# Trouble Case



# 解決策

- どれもこれも一長一短
  1. みんなでMTUをジャンボフレームにする
  2. みんなでMTUをオリジナルサイズにする
  3. IXを含めすべての経路をアナウンスする
  4. uRPFを利用しない
- これかな
  5. uRPFを適用する前にICMPv6(特にType=2, Packet too big)は必ず通す

# 会場に聞きたいこと

## 1. ベンダ向け

1. ルータが返すICMPv6のソースアドレスはRFC2463に従うとともに静的にも設定可能ですか？
2. uRPFを適用する前に特定のパケットフィルタ(ICMPv6のみacceptとか)のルールを適用できますか？

## 2. xSPのオペレータ向け

1. IPv6でもuRPFは使いますか／使いたいですか？
2. IXのIPv6 Prefixの経路情報は流れていたほうがいいですか？



# やるべきこと

- IDを書く?
- IETF/NANOGでプレゼンする?
- ICMPv6のRFCのアップデートする?
  - ICMPv6は絶対にパケットフィルタしない...

# エピローグ

- IPv4でもますます増えるんじゃない？
  - JANOGコメントでソースアドレスがプライベートなパケットはエッジで落とすことが推奨
  - v4アドレスが枯渇するとバックボーンのインフラで使っているアドレスを顧客に回す
  - バックボーンのアドレスはv6を使う、もしくはv4のプライベートアドレスを使う