Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/ICMPv6 Error Messages

(draft-gont-opsec-icmp-ingress-filtering)

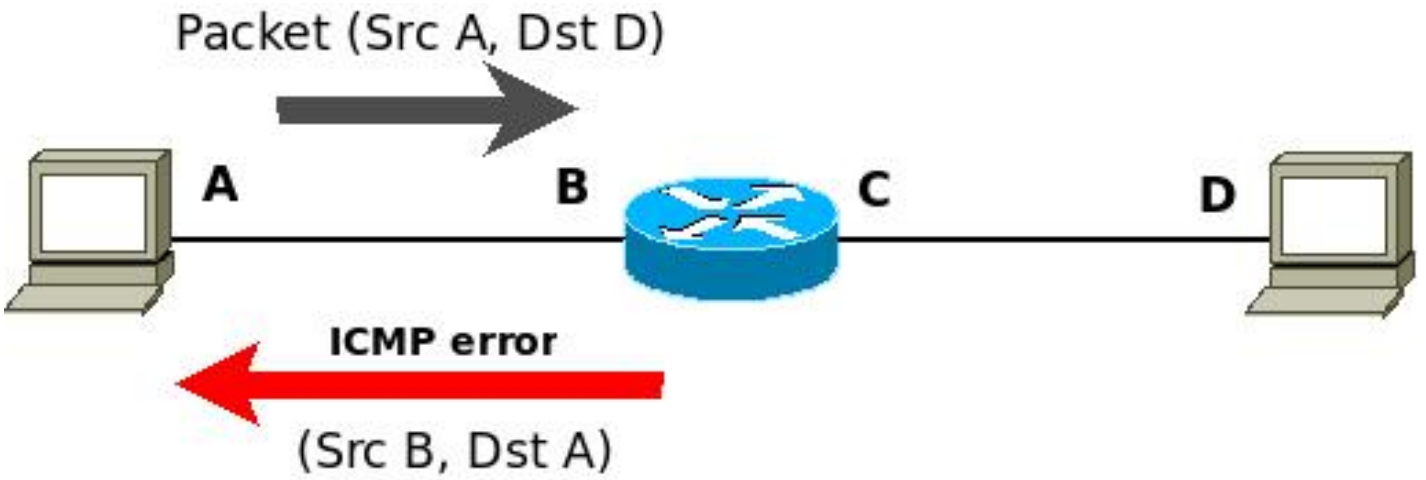
Fernando Gont
Ray Hunter
Jeroen Massar
Will Liu

IETF 95
Buenos Aires, Argentina. April 3-8, 2016

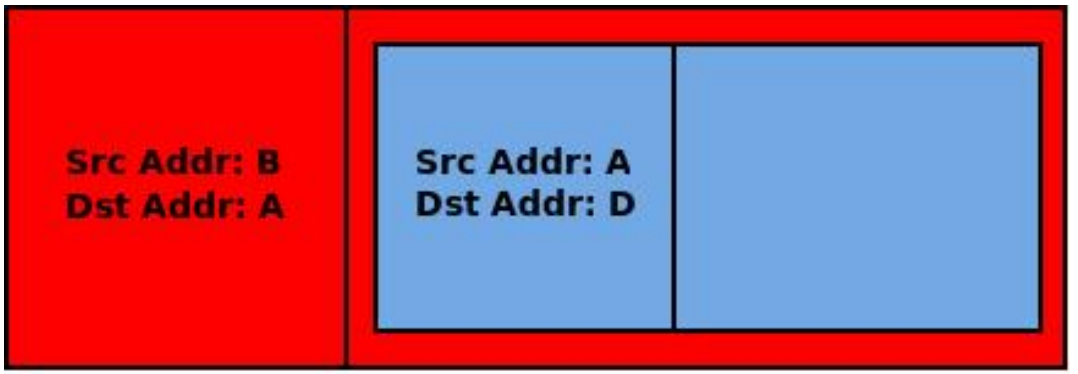
Goal

- Specify filtering policy to mitigate attacks based on spoofed ICMPv6 errors
  - Spoofed ICMPv6 PTB to play with PMTUD or trigger fragmentation
  - Spoofed ICMPv6 errors that might reset connections
  - etc.
- Should be deployed close to users (e.g. CPEs)
- Must never be applied in multihomed scenarios

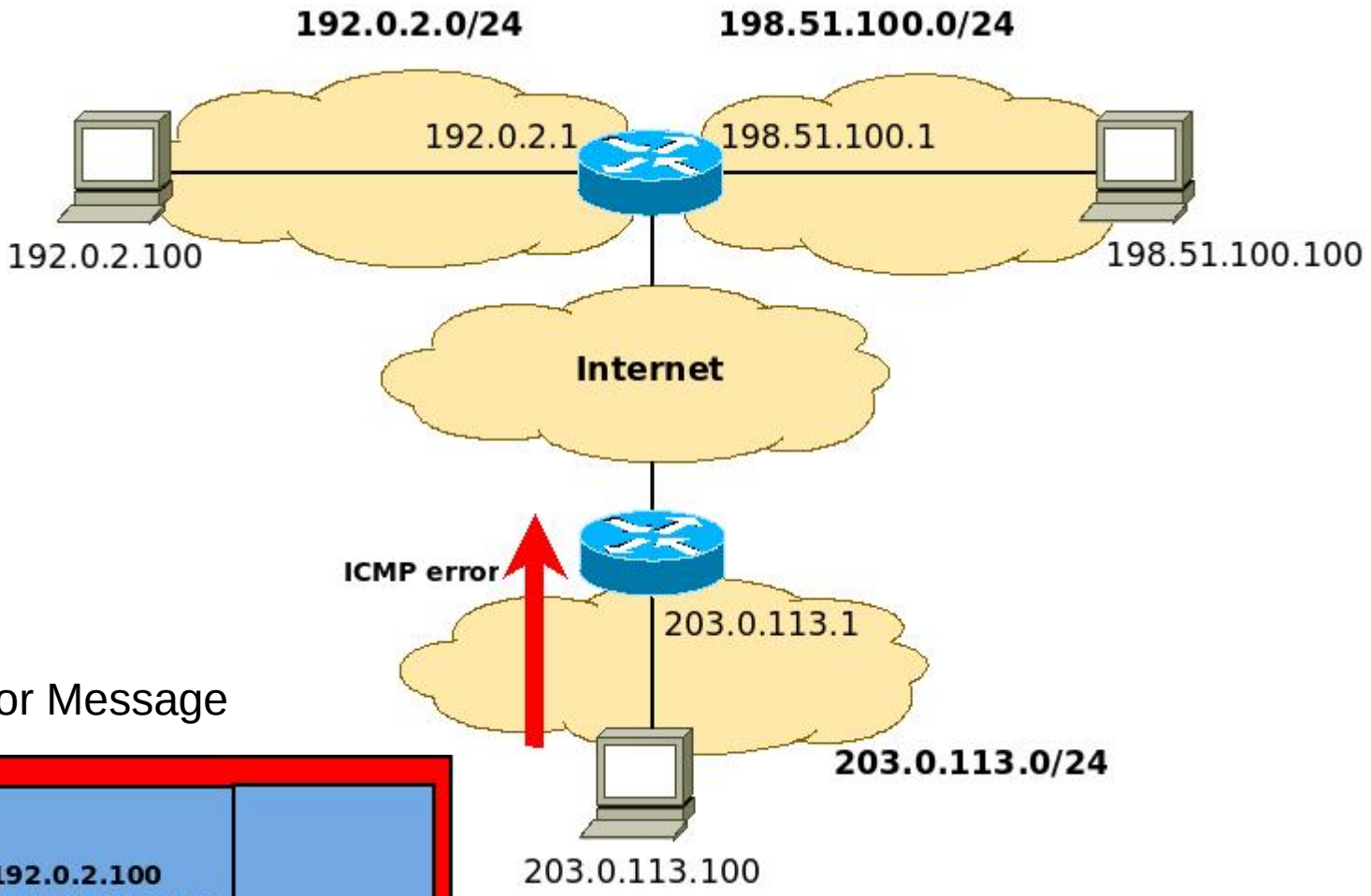
Background on ICMP Error Generation



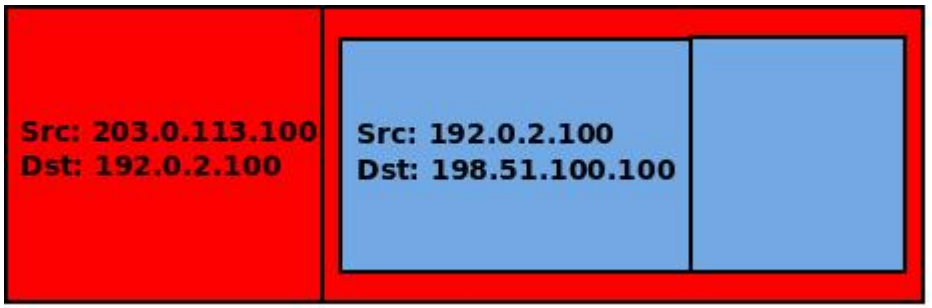
ICMP error



ICMP-based Attack Scenario



ICMP Error Message



draft-gont-opsec-icmp-ingress-filtering

- IF embedded packet's Destination Address is from within my network

  THEN forward as appropriate

- IF embedded packet's Destination Address is anything else

  THEN deny packet

Moving forward

- Adopt as opsec wg item?