BCP for Filtering ICMPv6 Messages in Firewalls

draft-davies-v6ops-icmpv6-filtering-bcp-00

Elwyn Davies
János Mohácsi

IETF-63, Paris, 1 August 2005

New draft

- Suggested by
  - Work in EU 6Net project
    - E.g., http://www.terena.nl/conferences/tnc2004/programme/sessions/show.php?sess_id=68
  - Section in earlier versions of security overview draft

Motivation

- ICMPv6 is a fundamental component of IPv6 networks
  - Some parts of ICMPv6 have an essential role in establishing communications
  - Less of an 'auxiliary' than ICMP in IPv4
- Some ICMPv6 messages can be a threat to open networks
  - IPsec not generally applicable
- Firewall filtering important for maintaining security.. Hence..
- Need to balance effective IPv6 communications against security needs

ICMPv6 Functions

- Error messages (4 types)
- Echo Request and Response
- Neighbor finding (NS, NA, RS, RA)
  - Duplicate Address Detection
  - IP and Link Layer Address exchange
  - Router Identification
  - Stateless Address Auto-configuration
- Network renumbering (NS, NA + renumber)
- Path MTU determination (Packet Too Big)
- Multicast Listener Discovery (4 messages)
- Mobile IPv6 support (4 messages)
- Node information lookup (2 messages)

Classifying ICMPv6 Functions and Messages

- Error and Informational Messages
- Addressing
  - Lots of different possibilities
- Network Topology and Address Scopes
  - Intra-link
  - End-to-end
  - ‘Any-to-end’ (borrowed from Jari Arkko)
- Role in Establishing Communications

Security Issues

- Denial of Service possibilities
- Use in network probing
- Redirection attacks
- Renumbering attacks

Example functions of messages

- Cannot blindly filter these messages!

	Echo request/reply	Debug
	No route to destination	Debug – better error indication
	TTL exceeded	Error report
IPv6 specific	Parameter problem	Error report
required	NS/NA	Required for normal operation – except static ND entry
required	RS/RA	For Stateless Address Autoconfigration
required	Packet too big	Path MTU discovery
IPv6 specific	MLD	Limited requirements for Neighbor Functions

Common Considerations

- Need to filter on
  - ICMPv6 type
  - Address types and scopes
- If possible: deep packet inspection
  - ICMPv6 Code field
  - Stateful mechanisms may be able to
    - Match incoming and outgoing packets
    - Allow max one error packet per original packet
- Messages for communications establishment need fixed rules
- Others can be subject to local policy

Missing pieces…

- Inverse Neighbor Discovery messages (#141/142)
- No mention of SEND
  - Role in securing Intra-link messages
  - Certification Path messages (#148/149)
- Implications of ND Proxy solution
- Seamoby message (#150)
- Multicast Router Discovery messages (#151/152/153)
- Acknowledgement of 6Net work

Next steps

- Ask the working group to make this a WG document/task
- Encourage comments especially from firewall configurers!
- Generate a new version to fill in the gaps

- Authors:
  - Elwyn Davies – elwynd@dial.pipex.com
  - János Mohácsi - mohacsi@niif.hu