Operational Security Capabilities for
IP Network Infrastructure (opsec)
Internet-Draft
Intended status: Informational
Expires: January 4, 2014

F. Gont
UTN/FRH
G. Gont
SI6 Networks
C. Pignataro
Cisco

July 3, 2013

Recommendations for filtering ICMP messages
draft-ietf-opsec-icmp-filtering-04

Abstract

This document document provides advice on the filtering of ICMPv4 and ICMPv6 messages. Additionaly, it discusses the operational and interoperability implications of such filtering.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 4, 2014.

Copyright Notice

Table of Contents

1. Introduction

This document document provides advice on the filtering of ICMPv4 and ICMPv6 messages. Additionaly, it discusses the operational and interoperability implications of such filtering.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Internet Control Message Protocol version 4 (ICMP)

Table 1 summarizes the recommendations with respect to what a device SHOULD do when generating, forwarding, or receiving ICMPv6 messages.

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-unreach-net	Rate-L	Rate-L	Rate-L
ICMPv4-unreach-host	Rate-L	Rate-L	Rate-L
ICMPv4-unreach-proto	Rate-L	Deny	Rate-L
ICMPv4-unreach-port	Rate-L	Deny	Rate-L
ICMPv4-unreach-frag-needed	Send	Permit	Rate-L
ICMPv4-unreach-src-route	Rate-L	Deny	Rate-L
ICMPv4-unreach-net-unknown (Depr)	Deny	Deny	Deny
ICMPv4-unreach-host-unknown	Rate-L	Deny	Ignore
ICMPv4-unreach-host-isolated (Depr)	Deny	Deny	Deny
ICMPv4-unreach-net-tos	Rate-L	Deny	Rate-L
ICMPv4-unreach-host-tos	Rate-L	Deny	Rate-L
ICMPv4-unreach-admin	Rate-L	Rate-L	Rate-L
ICMPv4-unreach-prec-violation	Rate-L	Deny	Rate-L
ICMPv4-unreach-prec-cutoff	Rate-L	Deny	Rate-L
ICMPv4-quench	Deny	Deny	Deny
ICMPv4-redirect-net	Rate-L	Deny	Rate-L
ICMPv4-redirect-host	Rate-L	Deny	Rate-L
ICMPv4-redirect-tos-net	Rate-L	Deny	Rate-L
ICMPv4-redirect-tos-host	Rate-L	Deny	Rate-L
ICMPv4-timed-ttl	Rate-L	Permit	Rate-L
ICMPv4-timed-reass	Rate-L	Permit	Rate-L

ICMPv4-parameter-pointer	Rate-L	Deny	Rate-L
ICMPv4-option-missing	Rate-L	Deny	Rate-L
ICMPv4-req-echo-message	Rate-L	Permit	Rate-L
ICMPv4-req-echo-reply	Rate-L	Permit	Rate-L
ICMPv4-req-router-sol	Rate-L	Deny	Rate-L
ICMPv4-req-router-adv	Rate-L	Deny	Rate-L
ICMPv4-req-timestamp-message	Rate-L	Deny	Rate-L
ICMPv4-req-timestamp-reply	Rate-L	Deny	Rate-L
ICMPv4-info-message (Depr)	Deny	Deny	Deny
ICMPv4-info-reply (Depr)	Deny	Deny	Deny
ICMPv4-mask-request	Rate-L	Deny	Rate-L
ICMPv4-mask-reply	Rate-L	Deny	Rate-L

Legend: "Depr" = Deprecated; "Rate-L" = Rate-Limit

Table 1: Summary Recommendations for ICMPv4

2.1. ICMPv4 Error Messages

[RFC0792] is the base specification for the Internet Control Message Protocol (ICMP) to be used with the Internet Protocol version 4 (IPv4). It defines, among other things, a number of error messages that can be used by end-systems and intermediate systems to report errors to the sending system. The Host Requirements RFC [RFC1122] classifies ICMP error messages into those that indicate "soft errors", and those that indicate "hard errors", thus roughly defining the semantics of them.

Section 3.2.2.1 of [RFC1122] specifies the amount of information to be included in the payload of an ICMP error message, and how ICMP error messages should be demultiplexed to the corresponding transport protocol instance. Additionally, it imposes details some scenarios in which ICMP errors should not be generated.

Section 4.1.3.3 of [RFC1122] states that UDP MUST pass to the application layer all ICMP error messages that it receives from the

IP layer.

Section 4.2.3.9 of [RFC1122] states that TCP MUST act on an ICMP error message passed up from the IP layer, directing it to the connection that created the error.

Section 4.3.2 of [RFC1812] contains a number of requirements for the generation and processing of ICMP error messages, including: initialization of the TTL of the error message, the amount of data from the offending packet to be included in the ICMP payload, setting the IP Source Address of ICMP error messages, setting of the TOS and Precedence, processing of IP Source Route option in offending packets, scenarios in which routers MUST NOT send ICMP error messages, and application of rate-limiting to ICMP error messages.

The ICMP specification [RFC0792] originally defined the ICMP Source Quench message (Type 4, Code 0), which was meant to provide a mechanism for flow control and congestion control. ICMP Source Quench is being formally deprecated by [RFC6633].

[RFC1191] defines a mechanism called "Path MTU Discovery (PMTUD), which makes use of ICMP error messages of Type 3 (Destination Unreachable), Code 4 (fragmentation needed and DF bit set) to allow systems to determine the MTU of an arbitrary internet path.

Appendix D of [RFC4301] provides information about which ICMP error messages are produced by hosts, intermediate routers, or both.

2.1.1. Destination Unreachable (Type 3)

The ICMP Destination Unreachable message is sent by a router in response to a packet which it cannot forward because the destination (or next hop) is unreachable or a service is unavailable. Examples of such cases include a message addressed to a host which is not there and therefore does not respond to ARP requests, and messages addressed to network prefixes for which the router has no valid route. [RFC1812] states that a router MUST be able to generate ICMP Destination Unreachable messages and SHOULD choose a response Code that most closely matches the reason the message is being generated. Section 3.2.2.1 of [RFC1122] states that a Destination Unreachable message that is received MUST be reported to the transport layer, and that the transport layer SHOULD use the information appropriately.

2.1.1.1. Net Unreachable (Code 0)

2.1.1.1.1. Uses

Used to indicate that a router cannot forward a packet because it has no routes at all (including no default route) to the destination specified in the packet. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.1.2. Message Specification

Defined in [RFC0792]. Section 4.3.3.1 of [RFC1812] states that if a router cannot forward a packet because it has no routes at all (including no default route) to the destination specified in the packet, then the router MUST generate a Destination Unreachable, Code 0 (Network Unreachable) ICMP message. Section 3.2.2.1 of [RFC1122] states that this message may result from a routing transient, and MUST therefore be interpreted as only a hint, not proof, that the specified destination is unreachable. For example, it MUST NOT be used as proof of a dead gateway. Section 4.2.3.9 of [RFC1122] states that this message indicates a soft error, and therefore TCP MUST NOT abort the connection, and SHOULD make the information available to the application.

2.1.1.1.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This attack be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.1.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts that could have been avoided by those systems aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.2. Host Unreachable (Code 1)

2.1.1.2.1. Uses

Used to indicate that a router cannot forward a to the intended destination because it is unreachable. A number of systems abort

connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.2.2. Message Specification

Defined in [RFC0792]. Section 3.2.2.1 of [RFC1122] states that his message may result from a routing transient, and MUST therefore be interpreted as only a hint, not proof, that the specified destination is unreachable. For example, it MUST NOT be used as proof of a dead gateway. Section 4.2.3.9 of [RFC1122] states that this message indicates a soft error, and therefore TCP MUST NOT abort the connection, and SHOULD make the information available to the application.

2.1.1.2.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.2.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts that could have been avoided by those systems aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.3. Protocol Unreachable (Code 2)

2.1.1.3.1. Uses

Used by hosts to indicate that the designated transport protocol is not supported.

2.1.1.3.2. Message Specification

Defined in [RFC0792]. [RFC1122] states that a host SHOULD send a protocol unreachable when the designated transport protocol is not supported. Section 4.2.3.9 of [RFC1122] states that this message indicates a hard error condition, so TCP SHOULD abort the connection.

2.1.1.3.3. Threats

Can be exploited to perform connection-reset attacks [RFC5927]. Such attacks need to be mitigated at hosts, as discussed in [RFC5927].

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. These DoS attacks can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.3.4. Operational and Interoperability Impact if Blocked

None.

2.1.1.4. Port Unreachable (Code 3)

2.1.1.4.1. Uses

Used by end-systems to signal the source system that it could not demultiplex the received packet (i.e., there was no listening process on the destination port). Used by UDP-based trace route to locate the final destination (UDP probes are sent to an UDP port that is believed to be unused). Some firewalls respond with this error message when a received packet is discarded due to a violation of the firewall security policy. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.4.2. Message Specification

Defined in [RFC0792]. Section 3.2.2.1 of [RFC1122] states that a host SHOULD send an ICMP port unreachable when the designated transport protocol (e.g., UDP) is unable to demultiplex the datagram but has no protocol mechanism to inform the sender. Additionally, it states that a transport protocol that has its own mechanism for notifying the sender that a port is unreachable MUST nevertheless accept an ICMP Port Unreachable for the same purpose.

Section 4.2.3.9 of [RFC1122] states that this message indicates a hard error condition, so TCP SHOULD abort the connection.

2.1.1.4.3. Threats

Can be exploited to perform connection-reset attacks [RFC5927]. Such attacks need to be mitigated at hosts, as discussed in [RFC5927].

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. These DoS attacks can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.4.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.5. Fragmentation Needed and DF Set (Code 4)

2.1.1.5.1. Uses

Used for the Path-MTU Discovery mechanism described in [RFC1191].

2.1.1.5.2. Message Specification

Defined in [RFC0792]

2.1.1.5.3. Threats

This error message can be used to perform Denial of Service (DoS) attacks against transport protocols. [RFC5927] describes the use of this error message to attack TCP connections.

2.1.1.5.4. Operational and Interoperability Impact if Blocked

Filtering this error message breaks the Path-MTU Discovery mechansim described in [RFC1191].

2.1.1.6. Source Route Failed (Code 5)

2.1.1.6.1. Uses

Signals errors araising from IPv4 source routes.

2.1.1.6.2. Message Specification

Defined in [RFC0792]. Section 3.2.2.1 of [RFC1122] states that his message may result from a routing transient, and MUST therefore be interpreted as only a hint, not proof, that the specified destination is unreachable. For example, it MUST NOT be used as proof of a dead gateway. Section 4.2.3.9 of [RFC1122] states that this message indicates a soft error, and therefore TCP MUST NOT abort the connection, and SHOULD make the information available to the application.

Section 4.2.3.9 of [RFC1122] states that this message indicates a hard error condition, so TCP SHOULD abort the connection.

2.1.1.6.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.6.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.7. Destination Network Unknown (Code 6) (Deprecated)

2.1.1.7.1. Uses

Signal unreachability condition to the sending system. Currently deprecated. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.7.2. Message Specification

Defined in [RFC1122]. [RFC1812] states that this Code SHOULD NOT be generated since it would imply on the part of the router that the destination network does not exist (net unreachable Code 0 SHOULD be used in place of Code 6).

2.1.1.7.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This can be mitigated by not-generating and dropping (rather than forwarding) these messages (since they have been deprecated).

2.1.1.7.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.8. Destination Host Unknown (Code 7)

2.1.1.8.1. Uses

Signal unreachability condition to the sending system. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.8.2. Message Specification

Defined in [RFC1122], and is generated only when a router can determine (from link layer advice) that the destination host does not exist

2.1.1.8.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.8.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.9. Source Host Isolated (Code 8) (Deprecated)

2.1.1.9.1. Uses

Signal unreachability condition to the sending system, but is currently deprecated. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.9.2. Message Specification

Defined in [RFC1122]. [RFC1812] states that routers SHOULD NOT generate this error message, and states that whichever of Codes 0 (Network Unreachable) and 1 (Host Unreachable) is appropriate SHOULD be used instead.

2.1.1.9.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.9.4. Operational and Interoperability Impact if Blocked

Might lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461]. However, this error message is deprecated, and thus systems should not depend on it for any purpose.

2.1.1.10. Communication with Destination Network Administratively Prohibited (Code 9) (Deprecated)

2.1.1.10.1. Uses

Signal unreachability condition to the sending system. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.10.2. Message Specification

This error Code is defined in [RFC1122], and was intended for use by end-to-end encryption devices used by U.S military agencies. [RFC1812] deprecates its use, stating that routers SHOULD use the Code 13 (Communication Administratively Prohibited) if they administratively filter packets.

2.1.1.10.3. Threats

May reveal filtering policies. In orther to mitigate this issue, a node could deny the generation of these error messages. However, we note that this would also have a negative impact on network troubleshooting.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. These DoS attacks can be mitigated by rate-limiting the rate of IMCP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.10.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461]. However, this error message is deprecated, and thus system should not depend on it for any purpose.

2.1.1.11. Communication with Destination Host Administratively Prohibited (Code 10) (Deprecated)

2.1.1.11.1. Uses

Signal unreachability condition to the sending system, but is currently deprecated. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.11.2. Message Specification

This error Code is defined in [RFC1122], and was intended for use by end-to-end encryption devices used by U.S military agencies. [RFC1812] deprecates its use, stating that routers SHOULD use the Code 13 (Communication Administratively Prohibited) if they administratively filter packets.

2.1.1.11.3. Threats

May reveal filtering policies. In orther to mitigate this issue, a node could deny the generation of these error messages. However, we note that this would also have a negative impact on network troubleshooting.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages.

This can be mitigated by rate-limiting the rate of ICMP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.11.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461]. However, this error message is deprecated, and thus system should not depend on it for any purpose.

2.1.1.12. Network Unreachable for Type of Service (Code 11)

2.1.1.12.1. Uses

Signal unreachability condition to the sending system when TOS-based routing is implemented, because the TOS specified for the routes is neither the default TOS (0000) nor the TOS of the packet that the router is attempting to route. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.12.2. Message Specification

Defined in [RFC1122]. Section 4.3.3.1 of [RFC1812] states that if a router cannot forward a packet because the TOS specified for the routes is neither the default TOS (0000) nor the TOS of the packet that the router is attempting to route, then the router MUST generate a Destination Unreachable, Code 11 (Network Unreachable for TOS) ICMP message.

2.1.1.12.3. Threats

May reveal routing policies.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. This can be mitigated by rate-limiting the rate of ICMP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.12.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.13. Host Unreachable for Type of Service (Code 12)

2.1.1.13.1. Uses

Signal unreachability condition to the sending system, when TOS-based routing is implemented, because the TOS specified for the routes is neither the default TOS (0000) nor the TOS of the packet that the router is attempting to route. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.13.1.1. Message Specification

Defined in [RFC1122]. Section 4.3.3.1 of [RFC1812] states that this message is sent if a packet is to be forwarded to a host that is on a network that is directly connected to the router and the router cannot forward the packet because no route to the destination has a TOS that is either equal to the TOS requested in the packet or is the default TOS (0000).

2.1.1.13.2. Threats

May reveal routing policies.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. This can be mitigated by rate-limiting the rate of ICMP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.13.3. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.14. Communication Administratively Prohibited (Code 13)

2.1.1.14.1. Uses

Signal unreachability condition (due to filtering policies) to the sending system. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.14.2. Message Specification

Defined in [RFC1812], and is generated if a router cannot forward a packet due to administrative filtering.

2.1.1.14.3. Threats

May reveal filtering policies.

Given that the semantics of this error message are not accurately specified, some systems might abort transport connections upon receipt of this error message. [RFC5927].

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. This can be mitigated by rate-limiting the rate of ICMP messages generated. For rate-limiting ICMPv4 messages see Section

4.3.2.8 of [RFC1812].

2.1.1.14.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.15. Host Precedence Violation (Code 14)

2.1.1.15.1. Uses

Signal unreachability condition to the sending system. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.15.2. Message Specification

Defined in [RFC1812], and is sent by the first hop router to a host to indicate that a requested precedence is not permitted for the particular combination of source/destination host or network, upper layer protocol, and source/destination port

2.1.1.15.3. Threats

May reveal routing policies.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. This can be mitigated by rate-limiting the rate of ICMP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.15.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.1.16. Precedence Cutoff in Effect (Code 15)

2.1.1.16.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.1.16.2. Message Specification

Defined in [RFC1812], and is sent when the network operators have imposed a minimum level of precedence required for operation, and a datagram was sent with a precedence below this level.

2.1.1.16.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMP messages. This can be mitigated by rate-limiting the rate of ICMP messages generated. For rate-limiting ICMPv4 messages see Section 4.3.2.8 of [RFC1812].

2.1.1.16.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.2. Source Quench (Type 4, Code 0)

2.1.2.1. Uses

Originally meant to aid in congestion-control and flow-control. Currently ignored by most end-system implementations, because of its security implications (see [RFC5927]. It is being formally deprecated by [RFC6633].

2.1.2.2. Message Specification

The Source Quench message was originally specified in [RFC0792]. It is being formally deprecated by [RFC6633].

2.1.2.3. Threats

Can be exploited for performing throughput-reduction attacks [RFC5927].

2.1.2.4. Operational and Interoperability Impact if Blocked

None.

2.1.3. Redirect (Type 5)

Section 3.2.2.2 of [RFC1122] states that SHOULD NOT send an ICMP Redirect message, and that a host receiving a Redirect message MUST update its routing information accordingly, and process the ICMP redirect according to the rules stated in Section 3.3.1.2 of [RFC1122]. ICMP redirects that specify a a gateway that is not on the same connected (sub-) net through which the Redirect arrived, or that are received from a source other than the first-hop gateway SHOULD be silently disacarded.

Section 4.3.3.2 of [RFC1812] states that a router MAY ignore ICMP Redirects when choosing a path for a packet originated by the router if the router is running a routing protocol or if forwarding is enabled on the router and on the interface over which the packet is being sent.

2.1.3.1. Redirect Datagrams for the Network (Code 0)

2.1.3.1.1. Uses

Used by routers to communicate end-systems a better first-hop router for a particular network. Currently ignored by a large number of stacks.

2.1.3.1.2. Message Specification

Defined in [RFC0792].

2.1.3.1.3. Threats

Can be abused by an attacker to redirect all or some traffic to himself and/or to perform a DoS attack.

This issue could be mitigated by disabling reaction to ICMP Redirect messages at hosts and/or dropping these messages at the network.

2.1.3.1.4. Operational and Interoperability Impact if Blocked

If the ICMP redirect was originated in some network segment other than the one it should be forwarded on, there is no operational impact, as the message is bogus or part of an attack. If an ICMP Redirect that was locally generated is blocked, the end-system will not be informed of the better first-hop for reaching the target

network, and thus this would result in less-optimum routes being used to get the target network.

2.1.3.2. Redirect Datagrams for the Host (Code 1)

2.1.3.2.1. Uses

Used by routers to communicate end-systems a better first-hop for a particular host. Currently ignored my a large number of stacks.

2.1.3.2.2. Message Specification

Defined in [RFC0792].

2.1.3.2.3. Threats

Can be abused by an attacker to redirect all or some traffic to himself and/or to perform a DoS attack.

This issue could be mitigated by disabling reaction to ICMP Redirect messages at hosts and/or dropping these messages at the network.

2.1.3.2.4. Operational and Interoperability Impact if Blocked

If the ICMP redirect was originated in some network segment other than the one it should be forwarded on, there is no operational impact, as the message is bogus or part of an attack. If an ICMP Redirect that was locally generated is blocked, the end-system will not be informed of the better first-hop for reaching the target network, and thus this would result in less-optimum routes being used to get the target network.

2.1.3.3. Redirect datagrams for the Type of Service and Network (Code 2)

2.1.3.3.1. Uses

Used by routers to communicate end-systems a better first-hop router for a particular network. Currently ignored my a large number of stacks.

2.1.3.3.2. Message Specification

Defined in [RFC0792].

2.1.3.3.3. Threats

Can be abused by an attacker to direct all or some traffic to himself and/or to perform a DoS attack.

This issue could be mitigated by disabling reaction to ICMP Redirect messages at hosts and/or dropping these messages at the network.

2.1.3.3.4. Operational and Interoperability Impact if Blocked

If the ICMP redirect was originated in some network segment other than the one it should be forwarded on, there is no operational impact, as the message is bogus or part of an attack. If an ICMP Redirect that was locally generated is blocked, the end-system will not be informed of the better first-hop for reaching the target network, and thus this would result in less-optimum routes being used to get the target network.

2.1.3.4. Redirect Datagrams for the Type of Service and Host (Code 3)

2.1.3.4.1. Uses

Used by routers to communicate end-systems a better first-hop for a particular host. Currently ignored my a large number of stacks.

2.1.3.4.2. Message Specification

Defined in [RFC0792].

2.1.3.4.3. Threats

Can be abused by an attacker to redirect all or some traffic to himself and/or to perform a DoS attack.

2.1.3.4.4. Operational and Interoperability Impact if Blocked

If the ICMP redirect was originated in some network segment other than the one it should be forwarded on, there is no operational impact, as the message is bogus or part of an attack. If an ICMP Redirect that was locally generated is blocked, the end-system will not be informed of the better first-hop for reaching the target network, and thus this would result in less-optimum routes being used to get the target network.

2.1.4. Time Exceeded (Type 11)

Section 3.2.2.4 of [RFC1122] states that an incoming Time Exceeded message MUST be passed to the transport layer.

Section 4.3.3.4 of [RFC1812] states that when the router receives (i.e., is destined for the router) a Time Exceeded message, it MUST comply with [RFC1122].

2.1.4.1. Time to Live Exceeded in Transit (Code 0)

2.1.4.1.1. Uses

Used for the traceroute troubleshooting tool. Signals unreachability condition due to routing loops. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.4.1.2. Message Specification

Defined in [RFC0792].

[RFC1812] states that a router MUST generate a Time Exceeded message Code 0 (In Transit) when it discards a packet due to an expired TTL field. Section 4.2.3.9 of [RFC1122] states that this message should be handled by TCP in the same way as Destination Unreachable codes 0, 1, 5.

2.1.4.1.3. Threats

Can be used for network mapping.

2.1.4.1.4. Operational and Interoperability Impact if Blocked

Breaks the traceroute tool. May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.4.2. Fragment Reassembly Time Exceeded (Code 1)

2.1.4.2.1. Uses

Signals fragment reassembly timeout. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.4.2.2. Message Specification

Defined in [RFC0792]. [RFC0792] states this message may be sent by a host reassembling a fragmented datagram if it cannot complete the reassembly due to missing fragments within its time limit. Section 4.2.3.9 of [RFC1122] states that this message should be handled by

TCP in the same way as Destination Unreachable codes 0, 1, 5.

2.1.4.2.3. Threats

May reveal the timeout value used by a system for fragment reassembly, and thus aid in evading NIDSs and fingerprinting the operating system in use by the sender of this error message.

2.1.4.2.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.5. Parameter Problem (Type 12)

Section 3.2.2.5 of [RFC1122] states that a host SHOULD generate Parameter Problem messages. An incoming Parameter Problem message MUST be passed to the transport layer, and it MAY be reported to the user. Section 4.2.3.9 of [RFC1122] states that this message should be handled by TCP in the same way as Destination Unreachable codes 0, 1, 5.

Section 4.3.3.5 of [RFC1812] states that a router MUST generate a Parameter Problem message for any error not specifically covered by another ICMP message. The IP header field or IP option including the byte indicated by the pointer field MUST be included unchanged in the IP header returned with this ICMP message. Section 4.3.2 of the same document defines an exception to this rule.

2.1.5.1. Pointer Indicates the Error (Code 0)

2.1.5.1.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

2.1.5.1.2. Message Specification

Defined in [RFC0792].

2.1.5.1.3. Threats

May be used to fingerprint the operating system of the host sending this error message.

2.1.5.1.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

2.1.5.2. Required Option is Missing (Code 1)

2.1.5.2.1. Uses

This ICMP Parameter Problem message Code is sent whenever a received IP packet should have contained a particular IP Option but the actual received IP packet did not contain that IP option. At present, a common situation in which this is ICMP Parameter Problem message Type is likely to arise is in certain high-security IP deployments where one or more IP Security options (e.g. RFC-1108, CIPSO) are deployed, and a packet is missing one of those security options. Other similar situations might also exist now, or in future.

2.1.5.2.2. Message Specification

Defined in Section 3.2.2.5 of [RFC1122].

2.1.5.2.3. Threats

None.

2.1.5.2.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

Additionally, blocking this ICMP message would make network trouble-shooting difficult or impossible in networks where IP Security Options (e.g. CIPSO, IPSO) are deployed. So blocking these ICMP messages could lead to a kind of denial-of-service attack on such deployments.

2.2. ICMPv4 Informational Messages

2.2.1. Echo or Echo Reply Message

2.2.1.1. Echo Message (Type 8, Code 0)

2.2.1.1.1. Uses

Used by the ping troubleshooting tool.

2.2.1.1.2. Message Specification

Defined in [RFC0792].

Section 3.2.2.6 of [RFC1122] states that every host MUST implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies. A host SHOULD also implement an application-layer interface for sending an Echo Request and receiving an Echo Reply, for diagnostic purposes. Section 3.2.2.6 of [RFC1122] includes a number of requirements for the processing of ICMP Echo messages and the generation of the corresponding replies.

Section 4.3.3.6 of [RFC1812] contains a number of requirements with respect to the generation and processing of ICMP Echo or Echo Reply messsages, including: maximum ICMP message size all routers are required to receive, a number of factors that may determine whether a router responds (or not) to an ICMP Echo message, the implementation of a user/application-layer interface, and the processing of Record Route, Timestamp and/or Source Route options that might be present in an ICMP Echo message.

2.2.1.1.3. Threats

Can be used for network mapping [icmp-scanning]. This vector could be partially mitigated by applying rate-limit to this traffic.

Has been exploited to perform Smurf attacks [smurf]. A router could mitigate this by dropping ICMP echor request messages directed to any of its directly-connected subnets.

2.2.1.1.4. Operational and Interoperability Impact if Blocked

Filtering this error message will break the ping tool. The best current practice is to rate-limit this ICMP message.

2.2.1.2. Echo Reply Message (Type 0, Code 0)

2.2.1.2.1. Uses

Used by the ping troubleshooting tool.

2.2.1.2.2. Message Specification

Defined in [RFC0792].

Section 3.2.2.6 of [RFC1122] states that every host MUST implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies. A host SHOULD also implement an application-layer interface for sending an Echo Request and receiving an Echo Reply, for diagnostic purposes. Section 3.2.2.6 of [RFC1122] includes a number of requirements for the processing of ICMP Echo messages and the generation of the corresponding replies.

Section 4.3.3.6 of [RFC1812] contains a number of requirements with respect to the generation and processing of ICMP Echo or Echo Reply messsages, including: maximum ICMP message size all routers are required to receive, a number of factors that may determine whether a router responds (or not) to an ICMP Echo message, the implementation of a user/application-layer interface, and the processing of Record Route, Timestamp and/or Source Route options that might be present in an ICMP Echo message.

2.2.1.2.3. Threats

Can be used for network mapping [icmp-scanning]. Has been exploited to perform Smurf attacks [smurf].

2.2.1.2.4. Operational and Interoperability Impact if Blocked

Filtering this error message will break the ping tool. The best current practice is to rate-limit this ICMP message.

2.2.2. Router Solicitation or Router Advertisement message

2.2.2.1. Router Solicitation Message (Type 10, Code 0)

2.2.2.1.1. Uses

Used by some systems as form of stateless autoconfiguration, to solicit routers on a network segment.

2.2.2.1.2. Message Specification

Defined in [RFC1256]

Section 4.3.3.10 of [RFC1812] states that an IP router MUST support the router part of the ICMP Router Discovery Protocol on all connected networks on which the router supports either IP multicast or IP broadcast addressing. The implementation MUST include all the

configuration variables specified for routers, with the specified defaults.

2.2.2.1.3. Threats

Can be used for network mapping (e.g., learning about routers on a network segment.).

2.2.2.1.4. Operational and Interoperability Impact if Blocked

This mesages should not be routed. Therefore, there is no operational/interoperability impact if blocked.

2.2.2.2. Router Advertisement Message (Type 9, Code 0)

2.2.2.2.1. Uses

Used to advertise routers on a network segment.

2.2.2.2.2. Message Specification

Defined in [RFC1256]

Section 4.3.3.10 of [RFC1812] states that an IP router MUST support the router part of the ICMP Router Discovery Protocol on all connected networks on which the router supports either IP multicast or IP broadcast addressing. The implementation MUST include all the configuration variables specified for routers, with the specified defaults.

2.2.2.2.3. Threats

Can be spoofed by an attacker to direct all traffic sent on a network segment to itself and/or to perform a DoS attack.

2.2.2.2.4. Operational and Interoperability Impact if Blocked

This mesages should not be routed. Therefore, there is no operational/interoperability impact if blocked.

2.2.3. Timestamp or Timestamp Reply Message

2.2.3.1. Timestamp Message (Type 13, Code 0)

2.2.3.1.1. Uses

May be used as a fall-back mechanism when NTP fails (?).

2.2.3.1.2. Message Specification

Defined in [RFC0792].

Section 3.2.2.8 of [RFC1122] states that a host MAY implement Timestamp and Timestamp Reply. For hosts that implement these messages, a number of requirements are stated.

2.2.3.1.3. Threats

Can be used for network mapping, and device fingerprinting.

2.2.3.1.4. Operational and Interoperability Impact if Blocked

None.

2.2.3.2. Timestamp Reply Message (Type 14, Code 0)

2.2.3.2.1. Uses

May be used as a fall-back mechanism when NTP fails (?).

2.2.3.2.2. Message Specification

Defined in [RFC0792].

2.2.3.2.3. Threats

Can be used for network mapping and device fingerprinting.

2.2.3.2.4. Operational and Interoperability Impact if Blocked

Systems will not be able to use ICMP timestamps as a fall-bak mechanism when NTP fails.

2.2.4. Information Request or Information Reply Message (Deprecated)

These messages are described in [RFC0792] as "a way for a host to find out the number of the network it is on". Section 3.2.2.7 of [RFC1122] and Section 4.3.3.7 of [RFC1812] deprecate the use of these messages.

2.2.4.1. Information Request Message (Type 15, Code 0)

2.2.4.1.1. Uses

These messages originally provided a basic and simple mechanism for dynamic host configuration. However, they have been deprecated.

2.2.4.1.2. Message Specification

Defined in [RFC0792].

These messages are described in [RFC0792] as "a way for a host to find out the number of the network it is on". Section 3.2.2.7 of [RFC1122] and Section 4.3.3.7 of [RFC1812] deprecate the use of these messages.

2.2.4.1.3. Threats

Allows for OS (Operating Sytem) and device fingerprintng. Since this messages have been deprecated, the best possible mitigation is to not generate and to drop any received Information Request messages.

2.2.4.1.4. Operational and Interoperability Impact if Blocked

None.

2.2.4.2. Information Reply Message (Type 16, Code 0)

2.2.4.2.1. Uses

These messages originally provided a basic and simple mechanism for dynamic host configuration. However, they have been deprecated.

2.2.4.2.2. Message Specification

Defined in [RFC0792].

These messages are described in [RFC0792] as "a way for a host to find out the number of the network it is on". Section 3.2.2.7 of [RFC1122] and Section 4.3.3.7 of [RFC1812] deprecate the use of these messages.

2.2.4.2.3. Threats

Allow for OS and device fingerprintng.

2.2.4.2.4. Operational and Interoperability Impact if Blocked

None.

2.2.5. Address Mask Request or Address Mask Reply

2.2.5.1. Address Mask Request (Type 17, Code 0)

2.2.5.1.1. Uses

Was originally defined as a means for system stateless autoconfiguration (to look-up the address mask).

2.2.5.1.2. Message Specification

Defined in RFC0950. Section 3.2.2.9 of [RFC1122] includes a number of requirements regarding the generation and processing of this message.

Section 3.2.2.9 of [RFC1122] states that a host MAY implement sending ICMP Address Mask Request(s) and receiving ICMP Address Mask Reply(s). Section 4.3.3.9 of [RFC1812] states that a router MUST implement support for receiving ICMP Address Mask Request messages and responding with ICMP Address Mask Reply messages.

2.2.5.1.3. Threats

Can be used for network mapping, and OS fingerprinting.

2.2.5.1.4. Operational and Interoperability Impact if Blocked

None.

2.2.5.2. Address Mask Reply (Type 18, Code 0)

2.2.5.2.1. Uses

Was originally defined as a means for system stateless autoconfiguration (to allow systems to dynamically obtain the address mask). While they have not been deprecated, they are not used in practice.

2.2.5.2.2. Message Specification

Defined in RFC0950. Section 3.2.2.9 of [RFC1122] includes a number of requirements regarding the generation and processing of this message.

Section 3.2.2.9 of [RFC1122] states that a host MAY implement sending ICMP Address Mask Request(s) and receiving ICMP Address Mask Reply(s). Section 4.3.3.9 of [RFC1812] states that a router MUST implement support for receiving ICMP Address Mask Request messages and responding with ICMP Address Mask Reply messages.

2.2.5.2.3. Threats

Can be used for network mapping, and OS fingerprinting.

2.2.5.2.4. Operational and Interoperability Impact if Blocked

None.

3. Internet Control Message Protocol version 6 (ICMPv6)

Table 2 summarizes the recommendations with respect to what a device SHOULD do when generating, forwarding, or receiving ICMPv6.

ICMPv6 Message	Sourced from Device	Through Device	Destined to Device
ICMPv6-unreach	N/A	N/A	N/A
ICMPv6-unreach-no-route	Rate-L	Permit	Rate-L
ICMPv6-unreach-admin-prohibited	Rate-L	Permit	Rate-L
ICMPv6-unreach-beyond-scope	Rate-L	Deny	Rate-L
ICMPv6-unreach-addr	Rate-L	Permit	Rate-L
ICMPv6-unreach-port	Rate-L	Permit	Rate-L
ICMPv6-unreach-source-addr	Rate-L	Deny	Rate-L
ICMPv6-unreach-reject-route	Rate-L	Permit	Rate-L
ICMPv6-too-big	Send	Permit	Rate-L
ICMPv6-timed	N/A	N/A	N/A
ICMPv6-timed-hop-limit	Send	Permit	Rate-L
ICMPv6-timed-reass	Send	Permit	Rate-L
ICMPv6-parameter	Rate-L	Permit	Rate-L
ICMPv6-parameter-err-header	Rate-L	Deny	Rate-L
ICMPv6-parameter-unrec-header	Rate-L	Deny	Rate-L

ICMPv6-parameter-unrec-option	Rate-L	Permit	Rate-L
ICMPv6-err-private-exp-100	Send	Deny	Rate-L
ICMPv6-err-private-exp-101	Send	Deny	Rate-L
ICMPv6-err-expansion	Send	Permit	Rate-L
ICMPv6-echo-message	Send	Permit	Rate-L
ICMPv6-echo-reply	Send	Permit	Rate-L
ICMPv6-info-private-exp-200	Send	Deny	Rate-L
ICMPv6-info-private-exp-201	Send	Deny	Rate-L
ICMPv6-info-expansion	Send	Permit	Rate-L

Legend: "Rate-L" = Rate-Limit

Table 2: Summary Recommendations for ICMPv6

3.1. ICMPv6 Error Messages

The ICMPv6 specification leaves it up to the implementation the reaction to ICMP error messages. Therefore, the ICMP attacks described in [RFC5927] might or might not be effective.

3.1.1. Destination Unreachable (Type 1)

3.1.1.1. No route to destination (Code 0)

3.1.1.1.1. Uses

Used to indicate that the ofending packet cannot be delivered because there is no route towords the destination address. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.1.1.2. Message Specification

Defined in [RFC4443].

3.1.1.1.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.1.1.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.1.2. Communication with destination administratively prohibited (Code 1)

3.1.1.2.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.1.2.2. Message Specification

Defined in [RFC4443].

3.1.1.2.3. Threats

May reveal filtering policies.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.1.2.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.1.3. Beyond scope of source address (Code 2)

3.1.1.3.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.1.3.2. Message Specification

Defined in [RFC4443].

3.1.1.3.3. Threats

3.1.1.3.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.1.4. Address unreachable (Code 3)

3.1.1.4.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.1.4.2. Message Specification

Defined in [RFC4443].

3.1.1.4.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMPv6 Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.1.4.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.1.5. Port unreachable (Code 4)

3.1.1.5.1. Uses

Used to identicate that there is no listening process on the target transport protocol port.

3.1.1.5.2. Message Specification

Defined in [RFC4443].

3.1.1.5.3. Threats

This error message might used to perform Denial of Service (DoS) attacks against transport protocols. [RFC5927] describes the use of this error message to attack TCP connections.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMPv6 Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.1.5.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.1.6. Source address failed ingress/egress policy (Code 5)

3.1.1.6.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.1.6.2. Message Specification

Defined in [RFC4443].

3.1.1.6.3. Threats

May reveal filtering policies.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.1.6.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.1.7. Reject route to destination (Code 6)

3.1.1.7.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.1.7.2. Message Specification

Defined in [RFC4443].

3.1.1.7.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Destination Unreachable messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.1.7.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.2. Packet Too Big Message (Type 2, Code 0)

3.1.2.1. Uses

Used for the Path-MTU discovery mechanism for IPv6 defined in [RFC1981].

3.1.2.2. Message Specification

Defined in [RFC4443].

3.1.2.3. Threats

This error message can be used to perform Denial of Service (DoS) attacks against transport protocols. [RFC5927] describes the use of this error message to attack TCP connections.

3.1.2.4. Operational and Interoperability Impact if Blocked

Filtering this error message will break the Path-MTU Discovery mechanism defined in [RFC1981], which could lead to a Denial of Service (unless the sending node implements some for of Path-MTU blackhole detection).

3.1.3. Time Exceeded Message (Type 3)

3.1.3.1. Hop limit exceeded in transit (Code 0)

3.1.3.1.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.3.1.2. Message Specification

Defined in [RFC4443].

3.1.3.1.3. Threats

May be used for network mapping.

3.1.3.1.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.3.2. Fragment reassembly time exceeded (Code 1)

3.1.3.2.1. Uses

Used to signal a timeout in fragment reassembly. A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.3.2.2. Message Specification

Defined in [RFC4443].

3.1.3.2.3. Threats

May reveal the timeout value used by a system for fragment reassembly, and thus help to perform remote OS fingerprinting. Additionally, revealing the fragment reassembly timeout value may help an attacker to evade a NIDS.

3.1.3.2.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.4. Parameter Problem Message (Type 4)

3.1.4.1. Erroneous header field encountered (Code 0)

3.1.4.1.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.4.1.2. Message Specification

Defined in [RFC4443].

3.1.4.1.3. Threats

This error message might used to perform Denial of Service (DoS) attacks against transport protocols. [RFC5927] describes the use of this error message to attack TCP connections.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP

Parameter Problem messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.4.1.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.4.2. Unrecognized Next Header Type encountered (Code 1)

3.1.4.2.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.4.2.2. Message Specification

Defined in [RFC4443].

3.1.4.2.3. Threats

This error message might used to perform Denial of Service (DoS) attacks against transport protocols. [RFC5927] describes the use of this error message to attack TCP connections.

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Parameter Problem messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.4.2.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.4.3. Unrecognized IPv6 option encountered (Code 2)

3.1.4.3.1. Uses

A number of systems abort connections in non-synchronized states in response to this message, to avoid long delays in connection establishment attempts [RFC5461].

3.1.4.3.2. Message Specification

Defined in [RFC4443].

3.1.4.3.3. Threats

An attacker can potentially perform a Denial of Service (DoS) attack against the router by forcing it to generate a high volume of ICMP Parameter Problem messages. This can be done by flooding the router with packets which the attacker knows will result in the router spending resources in generating a high volume of ICMPv6 messages. This can be mitigated by rate-limiting the rate of ICMPv6 messages generated. For rate-limiting ICMPv6 messages see Section 2.4, paragraph (f), of [RFC4443].

3.1.4.3.4. Operational and Interoperability Impact if Blocked

May lead to long delays between connection establishment attempts or long response times that could have been avoided by aborting non-synchronized connections in response to ICMP soft errors [RFC5461].

3.1.5. Private experimentation (Type 100)

3.1.5.1. Uses

Used for performing controlled experiments with ICMPv6 messages before a specific ICMPv6 Type is formally assigned by IANA.

3.1.5.2. Message Specification

Defined in [RFC4443].

3.1.5.3. Threats

The security implications of this message Type will depend on the specific experiment the message is being used for and whether the node this message is destined to implements the aforementioned "experiment".

3.1.5.4. Operational and Interoperability Impact if Blocked

None (this message Type is meant for experimentation rather than "production").

3.1.6. Private experimentation (Type 101)

3.1.6.1. Uses

Used for performing controlled experiments with ICMPv6 messages before a specific ICMPv6 Type is formally assigned by IANA.

3.1.6.2. Message Specification

Defined in [RFC4443].

3.1.6.3. Threats

The security implications of this message Type will depend on the specific experiment the message is being used for and whether the node this message is destined to implements the aforementioned "experiment".

3.1.6.4. Operational and Interoperability Impact if Blocked

None (this message Type is meant for controlled experimentation rather than "production").

3.1.7. Reserved for expansion of ICMPv6 error messages (Type 127)

3.1.7.1. Uses

Type value 127 is reserved for future expansion of the type value range if there is a shortage in the future.

3.1.7.2. Message Specification

Defined in [RFC4443].

3.1.7.3. Threats

None.

3.1.7.4. Operational and Interoperability Impact if Blocked

It would prevent expansion of the Type value range, and hence prevent extension of the ICMPv6 protocol.

3.2. ICMPv6 Informational messages

3.2.1. Echo Request or Echo Reply Message

3.2.1.1. Echo Request message (Type 128, Code 0)

3.2.1.1.1. Uses

Used by the ping tool to test reachability.

3.2.1.1.2. Message Specification

Defined in [RFC4443].

3.2.1.1.3. Threats

Can be used for network mapping [icmp-scanning] and for performing Smurf DoS attacks [smurf].

3.2.1.1.4. Operational and Interoperability Impact if Blocked

Filtering this error message will break the ping tool. The best current practice is to rate-limit this ICMP message.

3.2.1.2. Echo reply message (Type 129, Code 0)

3.2.1.2.1. Uses

Used by the ping tool to test reachability.

3.2.1.2.2. Message Specification

Defined in [RFC4443].

3.2.1.2.3. Threats

Can be used for network mapping [icmp-scanning] and for performing Smurf DoS attacks [smurf].

3.2.1.2.4. Operational and Interoperability Impact if Blocked

Filtering this error message will break the ping tool. The best current practice is to rate-limit this ICMP message.

3.2.2. Multicast Listener Discovery (MLD)

3.2.2.1. Multicast Listener Query (Type 130)

3.2.2.1.1. Uses

3.2.2.1.2. Message Specification

Defined in [RFC2710].

3.2.2.1.3. Threats

3.2.2.1.4. Operational and Interoperability Impact if Blocked

3.2.2.2. Multicast Listener Report (Type 131)

3.2.2.2.1. Uses

3.2.2.2.2. Message Specification

Defined in [RFC2710].

3.2.2.2.3. Threats

3.2.2.2.4. Operational and Interoperability Impact if Blocked

3.2.2.3. Multicast Listener Done (Type 132)

3.2.2.3.1. Uses

3.2.2.3.2. Message Specification

Defined in [RFC2710].

3.2.2.3.3. Threats

3.2.2.3.4. Operational and Interoperability Impact if Blocked

3.2.2.4. Version 2 Multicast Listener Report (Type 143)

3.2.2.4.1. Uses

3.2.2.4.2. Message Specification

Defined in [RFC3810].

3.2.2.4.3. Threats

3.2.7.1.2. Message Specification

Defined in [RFC6275].

3.2.7.1.3. Threats

3.2.7.1.4. Operational and Interoperability Impact if Blocked

3.2.7.2. Home Agent Address Discovery Reply Message (Type 145)

3.2.7.2.1. Uses

3.2.7.2.2. Message Specification

Defined in [RFC6275].

3.2.7.2.3. Threats

3.2.7.2.4. Operational and Interoperability Impact if Blocked

3.2.7.3. Mobile Prefix Solicitation (Type 146)

3.2.7.3.1. Uses

3.2.7.3.2. Message Specification

Defined in [RFC6275].

3.2.7.3.3. Threats

3.2.7.3.4. Operational and Interoperability Impact if Blocked

3.2.7.4. Mobile Prefix Advertisement (Type 147)

3.2.7.4.1. Uses

3.2.7.4.2. Message Specification

Defined in [RFC6275].

3.2.7.4.3. Threats

3.2.7.4.4. Operational and Interoperability Impact if Blocked

3.2.10.1.2. Message Specification

Defined in [RFC4286].

3.2.10.1.3. Threats

3.2.10.1.4. Operational and Interoperability Impact if Blocked

3.2.10.2. Multicast Router Solicitation (Type 152)

3.2.10.2.1. Uses

3.2.10.2.2. Message Specification

Defined in [RFC4286].

3.2.10.2.3. Threats

3.2.10.2.4. Operational and Interoperability Impact if Blocked

3.2.10.3. Multicast Router Termination (Type 153)

3.2.10.3.1. Uses

3.2.10.3.2. Message Specification

Defined in [RFC4286].

3.2.10.3.3. Threats

3.2.10.3.4. Operational and Interoperability Impact if Blocked

3.2.11. FMIPv6 Messages (Type 154)

3.2.11.1. Uses

3.2.11.2. Message Specification

Defined in [RFC5568].

3.2.11.3. Threats

3.2.11.4. Operational and Interoperability Impact if Blocked

3.2.12. RPL Control Message (Type 155)

3.2.12.1. Uses

3.2.12.2. Message Specification

Defined in [RFC6550].

3.2.12.3. Threats

3.2.12.4. Operational and Interoperability Impact if Blocked

3.2.13. Private experimentation (Type 200)

3.2.13.1. Uses

Used for performing controlled experiments with ICMPv6 messages before a specific ICMPv6 Type is formally assigned by IANA.

3.2.13.2. Message Specification

Defined in [RFC4443].

3.2.13.3. Threats

The security implications of this message Type will depend on the specific experiment the message is being used for and whether the node this message is destined to implements the aforementioned "experiment".

3.2.13.4. Operational and Interoperability Impact if Blocked

None (this message Type is meant for controlled experimentation rather than "production").

3.2.14. Private experimentation (Type 201)

3.2.14.1. Uses

Used for performing controlled experiments with ICMPv6 messages before a specific ICMPv6 Type is formally assigned by IANA.

3.2.14.2. Message Specification

Defined in [RFC4443].

3.2.14.3. Threats

The security implications of this message Type will depend on the specific experiment the message is being used for and whether the node this message is destined to implements the aforementioned "experiment".

3.2.14.4. Operational and Interoperability Impact if Blocked

None (this message Type is meant for controlled experimentation rather than "production").

3.2.15. Reserved for expansion of ICMPv6 informational messages (Type 255)

3.2.15.1. Uses

Type value 255 is reserved for future expansion of the type value range if there is a shortage in the future.

3.2.15.2. Message Specification

Defined in [RFC4443].

3.2.15.3. Threats

None.

3.2.15.4. Operational and Interoperability Impact if Blocked

It would prevent expansion of the Type value range, and hence prevent extension of the ICMPv6 protocol.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

This document does not introduce any new security implications. It attempts to help mitigate security threats that rely on ICMP or ICMPv6 messages, through packet filtering and rate-limiting.

6. Acknowledgements

The authors would like to thank (in alphabetical order) Steinthor Bjarnason, Alfred Hoenes, and Panos Kampanakis, for their valuable feedback on earlier versions of this document.

The survey of ICMP specifications is based on a yet-to-be-published internet-draft on ICMP by Fernando Gont and Carlos Pignataro. This document borrows its structure from the "ICMP filtering" wiki started by George Jones.

7. References

7.1. Normative References

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC1256] Deering, S., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC3122] Conta, A., "Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification", RFC 3122, June 2001.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure

Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4065] Kempf, J., "Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations", RFC 4065, July 2005.

[RFC4286] Haberman, B. and J. Martin, "Multicast Router Discovery", RFC 4286, December 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4620] Crawford, M. and B. Haberman, "IPv6 Node Information Queries", RFC 4620, August 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

7.2. Informative References

[RFC5461] Gont, F., "TCP’s Reaction to Soft Errors", RFC 5461, February 2009.

[RFC5927] Gont, F., "ICMP Attacks against TCP", RFC 5927, July 2010.

[RFC6633] Gont, F., "Deprecation of ICMP Source Quench Messages", RFC 6633, May 2012.

[icmp-scanning] Arkin, 0., "ICMP Usage in Scanning: The Complete Know-How", http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf, 2001.

[smurf] CERT, "CERT Advisory CA-1998-01: Smurf IP Denial-of-Service Attacks", http://www.cert.org/advisories/CA-1998-01.html, 1998.

Authors' Addresses

Fernando Gont
Universidad Tecnologica Nacional / Facultad Regional Haedo
Pueyrredon 76, 3A
Ramos Mejia, Provincia de Buenos Aires 1704
Argentina

Phone: +54 11 4650 8472
Email: fernando@gont.com.ar
URI: http://www.gont.com.ar

Guillermo Gont
SI6 Networks
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: ggont@si6networks.com
URI: http://www.si6networks.com

Carlos Pignataro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: cpignata@cisco.com