ICMP Message Types in Response to SNMP Requests

This document describes the ICMP messages types and responses to SNMP traffic. This information if relevant to SNMP polling and can be used for determining actions on SNMP error outcomes. You would use this information when writing designing NerveCenter Alarms and Polls.

Table 1 shows the set of defined set of ICMP message types. Messages are encoded using Type and Code values as shown. While the Type field usually serves as the primary key for a particular group of ICMP messages, this has not always been the case. The Echo or Echo Reply group, for example, uses two Type values: one for the request and one for the reply.

While some message groups form a response/reply set, other do not. The Destination Unreachable group, for example, can be issued in response to any IP-based message on the network; there is no explicit 'request' message for this group. On the other hand the Echo group has a clearly defined 'request' and 'reply' message pair. The same is true of the Timestamp and Information groups.

The table's Origin columns show which network nodes could generate such a message. Src Host is typically a management station, sending an ICMP or other IP-based request message to a specified Dest Host. An ICMP reply message is potentially generated either by the Dest Host or else by a gateway along the route taken by the request message.

Several of the groups can be considered Historic - meaning here that they are defined by their respective RFCs but are not known to have been implemented.[i] These are the groups Conversion Failed, Domain Name and Security Failures. For the sake of completeness, they are covered throughout this document; however, the likelihood of ever encountering them would be highly unlikely.

Table 1: ICMP Message Types with IPv4 (Organized by group - usually the Type label)

Message				**Origin**			**Description**	**Reference**
Type		**Code**		**src host**	**gateway**	**dest host**		
#	**Label**	**#**	**Label**					
3	Destination Unreachable	0	net unreachable	-	yes	no	The specified network is unreachable.	RFC792
		1	host unreachable	-	yes	no	The specified host is unreachable.	RFC792
		2	protocol unreachable	-	no	yes	The indicated protocol module is not active.	RFC792
		3	port unreachable	-	no	yes	The indicated process port is not active.	RFC792
		4	fragmentation needed and DF set	-	yes	no	The datagram must be fragmented in order to be forwarded; however, the Don't Fragement flag is on.	RFC792 RFC1191
		5	source route failed	-	yes	no	Datagram cannot be route under current (transient) routing state	RFC792
		6	destination network unknown	-	yes	no	no route (include default route) is valid for this datagram's target	RFC1122
		7	destination host unknown	-	yes	no	no known host matches this datagram's target.	RFC1122
		8	source host isolated	-	no	yes	Source host isolated.	RFC1122
		9	communication with destination	-	no	yes	(for use by end-to-end encryption devices used by U.S	RFC1108

Table 1: ICMP Message Types with IPv4 (Organized by group - usually the Type label)

Message				Origin			Description	Reference
Type		Code		src host	gateway	dest host		
#	Label	#	Label					
			network is administratively prohibited				military agencies)	RFC1812
		10	communication with destination host is administratively prohibited	-	no	yes	(for use by end-to-end encryption devices used by U.S military agencies)	RFC1108 RFC1812
		11	destination network unreachable for Type of Service	-	yes	no	The TOS specified for a defined route is neither the default TOS nor the TOS of the datagram that the gateway is attempting to route.	RFC1122
		12	destination network unreachable for Type of Service	-	yes	no	The TOS specified for a directly connected host is neither the default TOS nor the TOS of the datagram that the gateway is attempting to route.	RFC1122
		13	communication administratively prohibited	-	yes	no	Administrative filtering prohibits gateway from forwarding datagram.	RFC1812
		14	host precedence violation	-	yes	no	The datagram's requested precedence is not permitted for the combination of source/destination host or network, upper layer protocol, and source/destination port.	RFC1812
		15	precedence cutoff in effect	-	yes	no	The datagram's requested precedence is below the administratively set required level for this operation.	RFC1812
11	Time Exceeded	0	time to live exceeded in transit	-	yes	no	Datagram has time to live field set to 0 (zero)	RFC792
		1	fragment reassembly time exceeded	-	no	yes	A fragmented datagram cannot be reassembled with the host's time limit.	RFC792
12	Parameter Problem	0	pointer indicates the error	-	yes	yes	A problem exists with the datagram's header parameters.	RFC792
		1	required option is missing	-	yes	yes	Datagram has no Basic Security Option option and this was required for receival on a given network port.	RFC1108
		2	bad length	-	yes	yes	bad length	IANA
4	Source Quench	0	pointer indicates the error	-	yes	yes	Datagram arrival is too fast for processing.	RFC792
5	Redirect	0	redirect datagrams for the network	-	yes	no	Gateway advises the source host to send datagram instead to alternate gateway.	RFC792
		1	redirect datagrams for the host	-	yes	no		RFC792
		2	redirect datagrams for the Type of Service and Network	-	yes	no		RFC792
		3	redirect datagrams for the Type of Service and Host	-	yes	no		RFC792
8	Echo or Echo Reply	0	echo	yes	-	-	echo	RFC792
0		0	echo reply	-	yes	yes	echo reply	RFC792
13	Timestamp or Timestamp Reply	0	timestamp	-	-	-	timestamp	RFC792
14		0	timestamp reply	-	yes	yes	timestamp reply	RFC792
15	Information Request or Information Reply	0	information request	yes	-	-	information request (Obsolete)	RFC792
16		0	information reply	-	no	yes	information reply (Obsolete)	RFC792
17	Address Mask	0	address mask request	yes	yes	-	Request for net mask information.	RFC950
18		0	address mask reply	-	yes	yes	Reply containing net mask information.	RFC950
9	Router Discovery	0	router advertisement	-	yes	no	Announcement of IP address(es) of a given interface.	RFC1256
		16	does not route common traffic	-	yes	no	Mobility agent does not route common traffic.	RFC2002
10		0	router solicitation	yes	no	no	Solicitation for a router advertisement.	RFC1256
30	Traceroute	0	outbound packet successfully forwarded	-	yes	no	Request has been forwarded.	RFC1393
		1	no route for outbound packet; packet discarded	-	yes	no	Request cannot be forwarded.	RFC1393
31	Conversion Failed (Historic)	0	unknown/unspecified error	-	yes	yes	These ICMP Messages are in support of RFC1475's "TP/IX: The Next Internet" specification. This RFC, published in June 1993, proposed "IP version 7."	RFC1475
		1	don't convert option present	-	yes	yes		RFC1475
		2	unknown mandatory option present	-	yes	yes		RFC1475
		3	known unsupported option present	-	yes	yes		RFC1475
		4	unsupported transport protocol	-	yes	yes		RFC1475
		5	overall length exceeded	-	yes	yes		RFC1475

Table 1: ICMP Message Types with IPv4 (Organized by group - usually the Type label)

Message				Origin			Description	Reference
Type		Code		src host	gateway	dest host		
#	Label	#	Label					
		6	IP header length exceeded	-	yes	yes		RFC1475
		7	transport protocol > 255	-	yes	yes		RFC1475
		8	port conversion out of range	-	yes	yes		RFC1475
		9	transport header length exceeded	-	yes	yes		RFC1475
		10	32 bit rollover missing and ACK set	-	yes	yes		RFC1475
		11	unknown mandatory transport option present	-	yes	yes		RFC1475
37	Domain Name (Historic)	0	domain name request	yes	-	-	Domain Name request	RFC1788
38		0	domain name reply	-	yes	yes	Domain Name reply	RFC1788
40	Security Failures (Historic)	0	bad SPI	-	yes	yes		RFC2521
		1	authentication failed	-	yes	yes		RFC2521
		2	decompression failed	-	yes	yes		RFC2521
		3	decryption failed	-	yes	yes		RFC2521
		4	need authentication	-	yes	yes		RFC2521
		5	need authorization	-	yes	yes		RFC2521

Although the above table reveals that there is a large set of defined ICMP messages, a management application's usage of ICMP and SNMP limits the range that the application needs to handle. The context of the traffic issued by the management application defines the range of potential ICMP replies. Table 2a and Table 2b demonstrate this. Each shows the potential range of ICMP replies based on the communication context: an issued ICMP or SNMP request message.

The fields marked "yes" are possible replies to the request message. For example, an ICMP Echo request [Refer to the Olive colored row in the following table] issued by an application can only be responded to by one of the indicated ICMP message types. An Echo Reply is the "normal" response; yet, messages from the groups Destination Unreachable, Time Exceeded, Parameter Problem, Source Quence and Redirect are also possible. A Timestamp query or reply would not occur as a response; the messages defined in this group do not fit the context of an Echo request. However zero, one or more Traceroute messages might also be received if the Echo request also contained the traceroute option in its IP header. This is a deliberate action on the part of the sending application. These traceroute messages would arrive *in addition to* one of the already listed replies.

Table 2a: Possible ICMP replies to ICMP request messages

ICMP Request Message	Possible ICMP Responses (by group name)											
	Destination Unreachable	Time Exceeded	Parameter Problem	Source Quench	Redirect	Echo Reply	Timestamp	Information	Address Mask	Router Discovery	Traceroute[1]	Domain Name
Notes: 1. **ICMP Traceroute** messages are sent only when an originator has requested such by setting an option in the outgoing message's IP header. The outgoing message any be any message type, not just ICMP or SNMP.												
Echo [8,0]	yes	yes	yes	yes	yes	yes	no	no	no	no	yes	no
Timestamp [8,0]	yes	yes	yes	yes	yes	no	yes	no	no	no	yes	no
Information Request [15,0]	yes	yes	yes	yes	yes	no	no	yes	no	no	yes	no
Address Mask Request [17,0]	yes	yes	yes	yes	yes	no	no	no	yes	no	yes	no
Router Solicitation [9,0]	yes	yes	yes	yes	yes	no	no	no	no	yes	yes	no
Domain Name Request [37,0]	yes	yes	yes	yes	yes	no	no	no	no	no	yes	yes

For SNMP messages, the range of possible ICMP replies maps into the same set of error reporting as seen for ICMP messages. The "normal" SNMP reply is the Response PDU. Report PDUs and the marked range of ICMP replies all indicate various forms of error responses.[ii]

Table 2b: Possible SNMP and ICMP replies to SNMP request messages

SNMP Request Message	Possible SNMP responses		Possible ICMP Responses (by group name)											
	Response[1]	Report[2]	Destination Unreachable	Time Exceeded	Parameter Problem	Source Quench	Redirect	Echo Reply	Timestamp	Information	Address Mask	Router Discovery	Traceroute[3]	Domain Name
Notes: 1. SNMPv1 Agents reply to requests using the **Get Response** PDU. SNMPv2 and SNMPv3 Agents use the **Response** PDU. 2. **Report** PDU messages can only encountered when using SNMPv3. Though the **Report** PDU is defined in the SNMPv2 RFCs, it is not used until SNMPv3. 3. **ICMP Traceroute** messages are sent only when an originator has requested such by setting an option in the outgoing message's IP header. The outgoing message any be any message type, not just ICMP or SNMP.														
SNMPv1 / SNMPv2c / SNMPv3														
Get	yes	yes	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no
GetNext	yes	yes	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no
Set	yes	yes	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no
SNMPv2c / SNMPv3 only														
GetBulk	yes	yes	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no
Inform	yes	yes	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no
SNMPv2-Trap	no	no	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no
SNMPv1 only														
Trap	no	no	yes	yes	yes	yes	yes	no	no	no	no	no	yes	no