ICMPv6 Packet Types and Codes

Document ID: 22974

Contents

Introduction

This document list all the possible types and codes for the Internet Control Message Protocol version 6 (ICMPv6) packet.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Types of Messages

Error Messages

Error Message	Type Field Value	Code Field Value/Description	Description
	1		

Destination Unreachable Message		0 − No route to destination 1 − Communication with the destination is administratively prohibited, such as a firewall filter 2 − Not assigned 3 − Address unreachable 4 − Port unreachable	A Destination Unreachable message (Type 1) is generated in response to a packet that can not be delivered to its destination address for reasons other than congestion. The reasons for the non−delivery of a packet is described by code field value. For details of all codes, refer to RFC 2463 Section 3.1.
Packet Too Big Message	2	0	A Packet Too Big message is sent in response to a packet that it cannot forward because the packet is larger than the Maximum Transmission Unit (MTU) of the outgoing link.
Time Exceeded Message	3	0 − Hop limit exceeded in transit 1 − Fragment reassembly time exceeded	If a router receives a packet with a hop limit of zero, or a router decrements a packet's hop limit to zero, it *must* discard the packet and send an ICMPv6 Time Exceeded message with Code 0 to the source of the packet. This indicates either a routing loop or an initial hop limit value that is too small. For

			more details refer to RFC 2463 section 3.3.
Parameter Problem Message	4	0 − Erroneous header field encountered 1 − Unrecognized next header type encountered 2 − Unrecognized IPv6 option encountered	A Parameter Problem message is generated in response to an IPv6 packet with problem in its IPv6 header, or extension headers, such the node cannot process the packet and must discard it. For more details refer to RFC 2463 section 3.4.

Informational Messages

ICMPv6 Information message	Type Field value	Code Field value	Description
Echo Request Message	128	0	Used to check and troubleshoot connectivity using the IPv6 **ping** command.
Echo Reply Message	129	0	This message is generated in response to an echo request message.

Refer to RFC 2463 section 4 for more information on ICMPv6 informational message types and codes.

Neighbor Discovery ICMPv6 Messages

ICMPv6 Neighbor Discovery Message	Type Field Value	Code Field Value	Description
Router Solicitation Message	133	0	Hosts send router solicitations messages in order to prompt routers to generate router advertisements messages quickly.
Router Advertisement	134	0	Routers send out router advertisement message

Message			periodically, or in response to a router solicitation.
Neighbor Solicitation Message	135	0	Nodes send neighbor solicitations to request the link−layer address of a target node while also providing their own link−layer address to the target.
Neighbor Advertisement Message	136	0	A node sends neighbor advertisements in response to neighbor solicitations and sends unsolicited neighbor advertisements in order to propagate new information quickly (which is unreliable).
Redirect Message	137	0	Routers send redirect packets to inform a host of a better first−hop node on the path to a destination. Hosts can be redirected to a better first−hop router but can also be informed by a redirect that the destination is in fact a neighbor. The latter is accomplished by setting the ICMP target address equal to the ICMP destination address.

Refer to RFC 2461 for more information on Neighbor Discovery for ICMPv6.

Type−Length−Value (TLVs) Options for Neighbor Discovery ICMP Messages

Option Name	Type	Description
Source Link−Layer Address	1	The Source Link−Layer Address option contains the link−layer address of the sender of the packet. It is used in the neighbor solicitation, router solicitation, and router advertisement packets.
Target Link−Layer Address	2	The Target Link−Layer Address option contains the link−layer address of the target. It is used in neighbor advertisement and redirect packets.
Prefix Information	3	The Prefix Information option provide hosts with on−link prefixes and prefixes for address autoconfiguration.

Redirect Header	4	The Redirected Header option is used in redirect messages and contains all or part of the packet that is being redirected.
MTU	5	The MTU option is used in router advertisement messages to insure that all nodes on a link use the same MTU value in those cases where the link MTU is not well known.

Refer to RFC 2461 for more information on Neighbor Discovery for ICMPv6.

Related Information

- **IP Routed Protocols Support Page**
- **IP Routing Support Page**
- **Technical Support − Cisco Systems**

Updated: Aug 10, 2005 Document ID: 22974