ICMP Data Fields

(from ICP, pg. 202-204)

Original Headers

In order for ICMP to determine which datagram failed, it must be given information about that datagram. For this reason, the original headers from the failing IP datagram are always included with the ICMP error message.

Size

20 to 60 bytes, depending on the length of the original datagram's IP header.

Notes

IP is a datagram-centric protocol, and not a circuit-centric protocol. As such, it cannot keep track of failed datagrams by referencing a sequence number or some other counter like TCP can. Instead, in order for IP to know when a datagram failed, the headers from the failing datagram must be returned to the sender, allowing it to parse through the information and locate the transport protocol that caused the problem.

This feature is especially important when a host sends many different datagrams to another specific destination. If the host sends hundreds of datagrams and then gets an ICMP error message, which datagram does the failure apply to? The only way to authoritatively answer this question is to examine the failing datagram explicitly.

Typically, this information is used in conjunction with the Original Data field, which allows a transport protocol to determine the application that generated the failing datagram.

Original Data

Just as ICMP needs to know which IP datagram failed in order to inform the appropriate transport protocol of the problem, the transport protocols also need to know which application sent the failing datagram before they can notify the application of the failure. For this reason, the first eight bytes of data from the failing IP datagram are always included with the ICMP error message, since these bytes contain the source and destination port number fields used by UDP and TCP (or the Message Type and Code fields from ICMP query messages).

Size

Sixty-four bits.

Notes

In order for the transport protocols to know which application generated the failing datagram, they have to be able to examine data that is outside of the original IP headers. All of the upper-layer protocols in use with IP—including TCP, UDP, and ICMP itself—place the source and destination application information in the first eight bytes of the datagram's data segment. As long as the transport protocols have access to that data, they can locate the offending application.

This information is used in conjunction with the Original Headers field, which allows ICMP to determine the higher-layer protocol that sent the failing datagram.