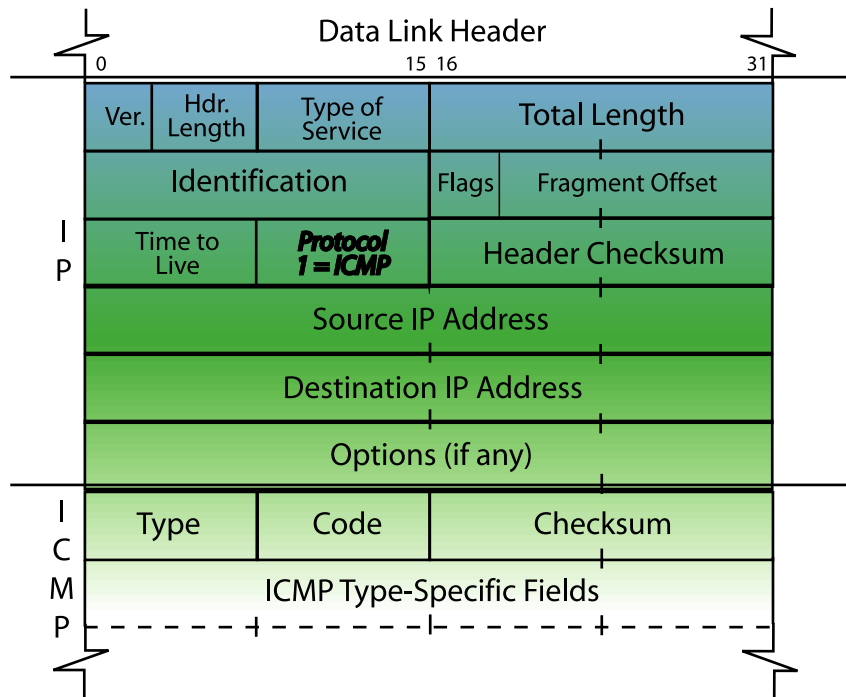


# ICMP Core Packet Structure



An IP header Protocol field value of 1 indicates that ICMP fields follow the IP header. ICMP does not use UDP; ICMP does not use TCP. ICMP packets only contain three required fields after the IP header: type, code and checksum. In some ICMP packets, however, there are added fields to provide information or details on the message. For example, an ICMP redirect packet needs to include the address of the gateway that a packet is being redirected to. Upon receipt of this packet, a host should add a dynamic route entry to their routing tables and begin using the new routing information immediately.

# ICMP Type/Code List

Type	Name and Reference (if available)	Type	Name and Reference (if available)
0	Echo Reply [RFC 792]	8	Echo [RFC 792]
1	Unassigned	9	Router Advertisement [RFC 1256]
2	Unassigned	10	Router Solicitation [RFC 1256]
3	Destination Unreachable [RFC 792]	11	Time Exceeded [RFC 792]
	Code Definition		Code Definition
0	Net Unreachable	0	Time to Live exceeded in Transit
1	Host Unreachable	1	Fragment Reassembly Time Exceeded
2	Protocol Unreachable	12	Parameter Problem [RFC 792]
3	Port Unreachable		Code Definition
4	Fragmentation Needed and Don't Fragment was Set	0	Pointer indicates the error
5	Source Route Failed	1	Missing a Required Option
6	Destination Network Unknown	2	Bad Length
7	Destination Host Unknown	13	Timestamp [RFC 792]
8	Source Host Isolated	14	Timestamp Reply [RFC 792]
9	Communication with Destination Network is Administratively Prohibited	15	Information Request [RFC 792]
10	Communication with Destination Host is Administratively Prohibited	16	Information Reply [RFC 792]
11	Destination Network Unreachable for Type of Service	17	Address Mask Request [RFC 950]
12	Destination Host Unreachable for Type of Service	18	Address Mask Reply [RFC 950]
13	Communication Administratively Prohibited	19	Reserved (for Security) [Solo]
14	Host Precedence Violation	20-29	Reserved (for Robustness Experiment) [ZSu]
15	Precedence cutoff in effect	30	Traceroute [RFC 1393]
4	Source Quench [RFC 792]	31	Datagram Conversion Error [RFC 1475]
5	Redirect [RFC 792]	32	Mobile Host Redirect [David Johnson]
	Code Definition	33	IPv6 Where-Are-You [Bill Simpson]
0	Redirect Datagram for the Network (or subnet)	34	IPv6 I-Am-Here [Bill Simpson]
1	Redirect Datagram for the Host	35	Mobile Registration Request [Bill Simpson]
2	Redirect Datagram for the Type of Service and Network	36	Mobile Registration Reply [Bill Simpson]
3	Redirect Datagram for the Type of Service and Host	37	Domain Name Request [Bill Simpson]
6	Alternate Host Address [JBP]	38	Domain Name Reply [Bill Simpson]
7	Unassigned	39	SKP [Markson]

# Decoding ICMP Packets



There are numerous ICMP trace files online at [www.packet-level.com](http://www.packet-level.com). The image above is an ICMP echo request packet. ICMP echo requests use Type 8 and Code 0. The ICMP echo replies use Type 0 and Code 0. By default, Windows devices pad this packet with an alphabetical pattern. This ICMP packet was generated by the ping utility.

- Trace file ping.pkt: <http://www.packet-level.com/traces.htm>
- Ping: <http://www.packet-level.com/resources/syntax.pdf>

The image above is an ICMP Destination Unreachable packet. As you can see on the right-hand side of this foldout, there are numerous causes for a Destination Unreachable packet. This packet uses Type 3 and Code 3 (Port Unreachable). Further in the packet, there is an indication of the port that was unreachable – NetBIOS, in this case – probably a good thing.

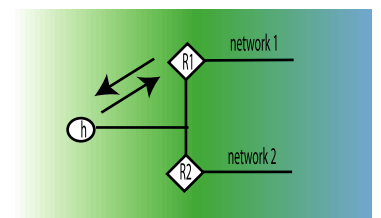
- Trace file icmp-port.pkt: <http://www.packet-level.com/traces.htm>
- See <http://www.isi.edu/in-notes/iana/assignments/icmp-parameters>

# Watch for...

## ICMP Redirections

ICMP Redirections are generated by routers when a packet arrives for forwarding, but the receiving router knows there is another local router that offers an optimal route. A high number of these indicates a possible problem with the clients' default gateway setting.

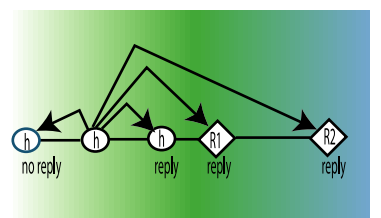
\*In the figure to the right, the host (h) sends a packet to R1 that is actually destined for network 2. R1 sends a redirection to the host. The redirection includes the address of the optimal router, R2.



## ICMP Echo Requests/Replies

An excessive number of ICMP Echo requests may indicate a reconnaissance probe is underway on the network. By sending these packets to various IP addresses, an attacker can learn which systems are running on the network. Consider blocking ICMP packets from coming in through your Internet router.

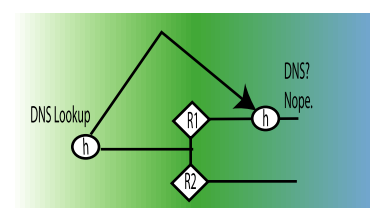
\*In the figure to the right, the host (h) sends an ICMP echo request to numerous devices on a network. Replies provide an indication of active systems.



## ICMP Destination Unreachable

A high number of ICMP Destination Unreachable packets indicates possible configuration problems or possibly a reconnaissance probe – someone trying to find out what services are loaded on a system or network. Check above.

\*In the figure to the right, a host sends a DNS query to a device that does not support DNS services (port 53).



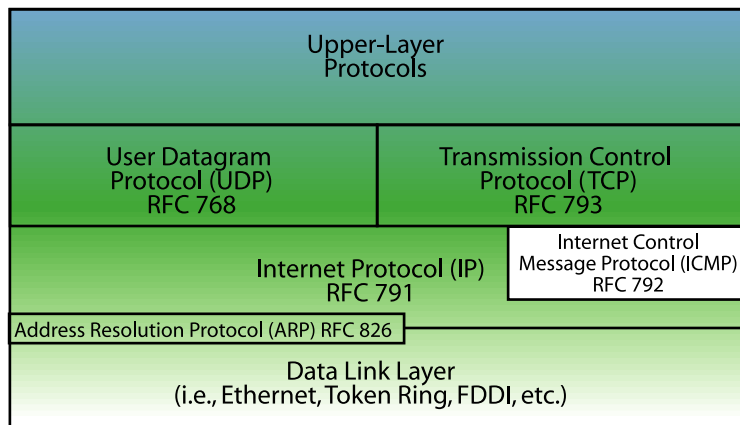
# ICMP

## Internet Control Message Protocol

ICMP is a protocol used for error notification and information distribution on an internetwork. ICMP is connectionless, residing directly over the IP header (without UDP or TCP). ICMP offers the following features:

- ICMP can redirect a client's traffic and route information to flow through more optimal router.
- ICMP can send an echo request to a device to test connectivity or define a network route.
- ICMP can provide clients with the IP address of their local router.
- ICMP can indicate network loops and fragmentation problems.
- ICMP can indicate unreachable devices and applications.

ICMP is covered in detail in RFC 792. Many ICMP trace files are available online at [www.packet-level.com](http://www.packet-level.com).

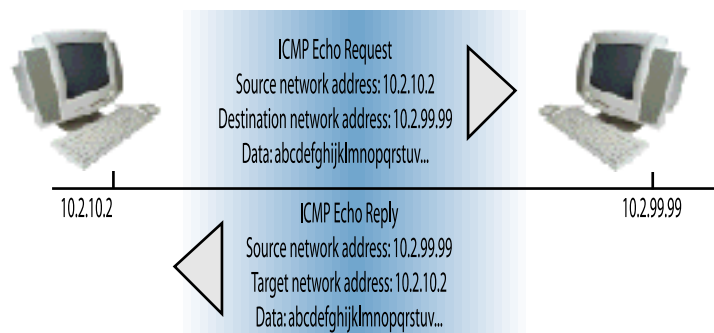


## ICMP References and Resources

- RFC 792: Internet Control Message Protocol
- RFC 1256: ICMP Router Discovery Messages
- RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 1122: Requirements for Internet Hosts -- Communication Layers
- Trace files online at Laura Chappell's [www.packet-level.com](http://www.packet-level.com).

## Sample ICMP Ping Process

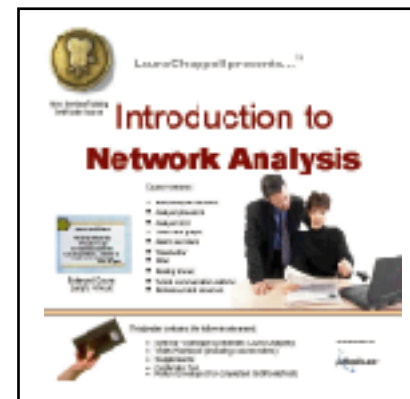
Ping (Packet Internet Groper) is used to test connectivity to another device. The Ping process uses ICMP Echo Requests (Type 8) and ICMP Echo Replies (Type 0).



Sponsored by:

**protocol  
analysis  
institute**

**podbooks.com™**



Laura Chappell's Protocol Analysis Institute focuses on network analysis, troubleshooting and optimization. The mission of PAI is to educate and inform -- through onsite analysis visits, specialized training sessions and our partnership with podbooks.com.

Visit Protocol Analysis Institute at [www.packet-level.com](http://www.packet-level.com).

Join the Protocol Analysis Institute mailing list for the latest information on analysis and troubleshooting.

Podbooks.com offers electronic and hardcopy books and video-based training courses developed from the research performed by the Protocol Analysis Institute and the PAI partners. Currently, podbooks.com carries the following titles:

Book: *Introduction to Network Analysis*

Book: *Advanced Network Analysis Techniques*

Book: *TCP/IP Analysis and Troubleshooting*

Book: *Hands-On Cisco: Basic TCP/IP LAN Configurations*

Course: *Introduction to Network Analysis*

Course: *Packet-Level IPv4*

Course: *Introduction to Cyber Crime*

Course: *Packet-Level DHCP*

Course: *Network Designs and Data Paths*

Course: *Packet-Level ICMP*

Less talk; more rock.  
Hands-On Technology Labs  
for real hands-on training.

**HOT  
Labs**

Click here for more information:

[www.nuihotlabs.org/register](http://www.nuihotlabs.org/register)