Troubleshooting IP using ICMP

The Internet Control Message Protocol (ICMP) is used for a multitude of informational and error messaging purposes.
The two most common troubleshooting tools that utilize ICMP are:

- **Packet Internet Groper (ping)**
- **Traceroute**

Packet Internet Groper (ping)

Ping command is a very common troubleshooting tool, which utilizes the Echo Request and Echo Reply ICMP messages to determine if an IP address is reachable and responding. Ping will additionally provide the round-trip time between the source and destination, usually measured in milliseconds. Ping can also tell us whether there is any packet loss

The ping command first sends an echo request packet to an address, then waits for a reply. The ping is successful only if:

- The echo request gets to the destination
- The destination is able to get an echo reply back to the source within a predetermined time called a timeout. The default value of this timeout is two seconds on Cisco routers.

Example :
Router#Ping 192.168.10.1

The Extended ping Command

When a normal ping command is sent from a router, the source address of the ping is the IP address of the interface that the packet uses to exit the router. If an extended ping command is used, the source IP address can be changed to any IP address on the router. The extended ping is used to perform a more advanced check of host reachability and network connectivity. The extended ping command works only at the privileged EXEC command line. The normal ping works both in the user EXEC mode and the privileged EXEC mode.

Example

Router A>enable
Router A#ping
Protocol [ip]:
Target IP address: 192.168.40.1
!--- The address to ping.
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Extended commands [n]: y
Source address or interface: 172.16.23.2
!---Ping packets are sourced from this address.
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 162.108.21.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms
!--- Ping is successful.

Traceroute command
The traceroute command is used to discover the routes that packets actually take when traveling to their destination. Traceroute will not only identify each router the packet has been forwarded through, but will also measure the delay experienced at each router hop.
Example
Router#traceroute 34.0.0.4

The Extended traceroute Command
The extended traceroute command is a variation of the traceroute command. An extended traceroute command can be used to see what path packets take in order to get to a destination. The command can also be used to check routing at the same time. This is helpful for when you troubleshoot routing loops, or for when you determine where packets are getting lost (if a route is missing, or if packets are being blocked by an Access Control List (ACL) or firewall). You can use the extended ping command in order to determine the type of connectivity problem, and then use the extended traceroute command in order to narrow down where the problem occurs.

Example
Router A>enable
Router A#traceroute
Protocol [ip]:
Target IP address: 192.168.40.2
!--- The address to which the path is traced.
Source address: 172.16.23.2
Numeric display [n]:
Timeout in seconds [3]:

Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.40.2
1 172.31.20.2 16 msec 16 msec 16 msec
2 172.20.10.2 28 msec 28 msec 32 msec
*3 192.168.40.2 32 msec 28 msec **
!--- The traceroute is successful.