ICMPv6

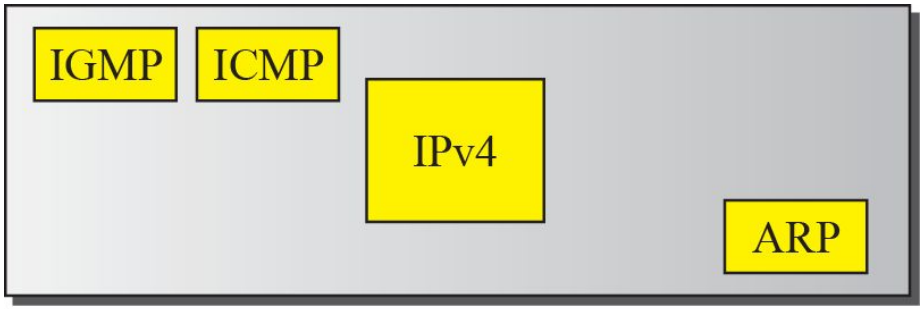
Dr. Kunwar Pal
CSED
NITJ

1 INTRODUCTION

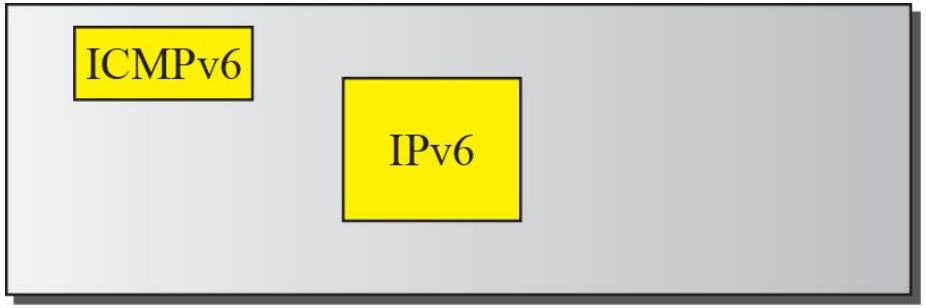
Another protocol that has been modified in version 6 of the TCP/IP protocol suite is ICMP. This new version, Internet Control Message Protocol version 6 (ICMPv6), follows the same strategy and purposes of version 4.

ICMPv6, however, is more complicated than ICMPv4: some protocols that were independent in version 4 are now part of ICMPv6 and some new messages have been added to make it more useful.

Figure 1 *Comparison of network layers in version 4 and version 6*

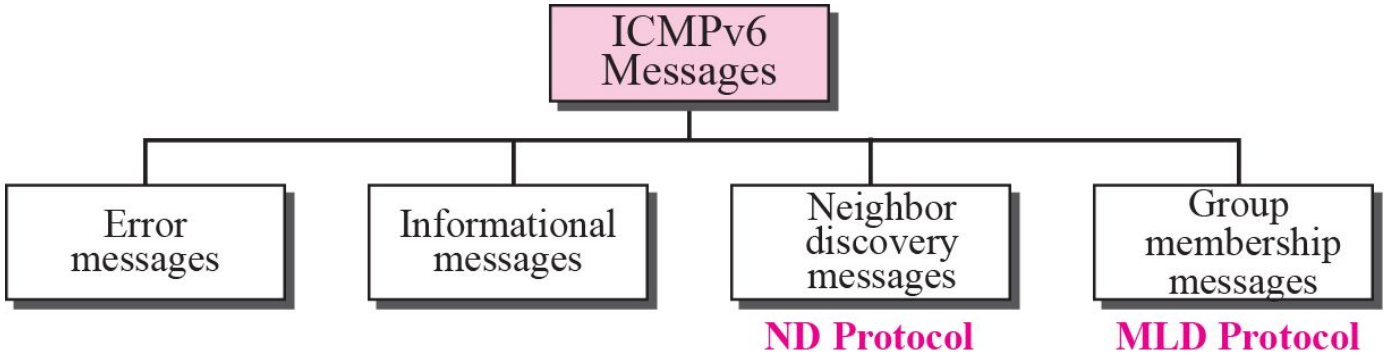


Network layer in version 4



Network layer in version 6

Figure 2 *Taxonomy of ICMPv6 messages*



2 ERROR MESSAGES

One of the main responsibilities of ICMP is to report errors. Four types of errors are handled: destination unreachable, packet too big, time exceeded, and parameter problems (see Figure 3).

Figure 3 *Error-reporting messages*

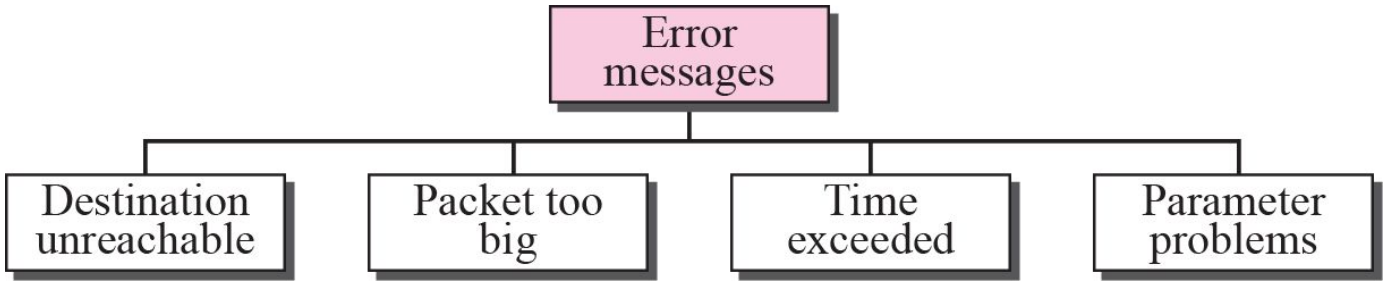
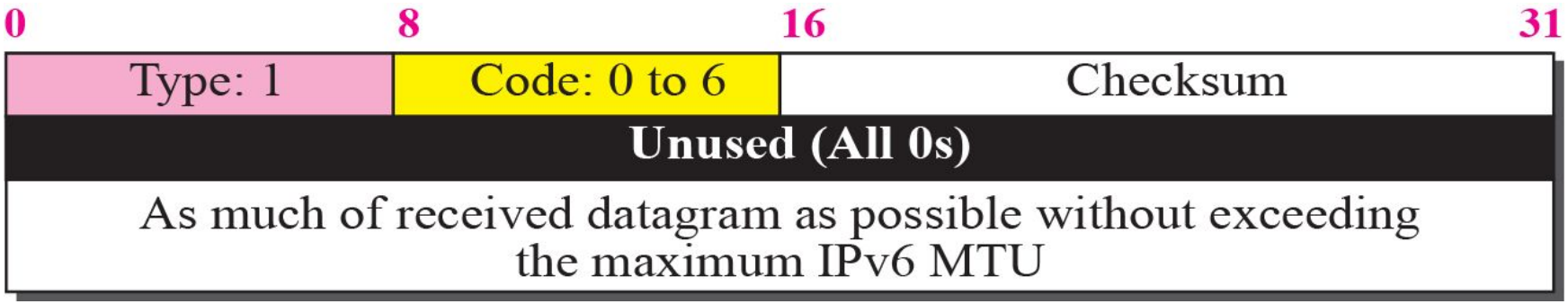


Figure 4 *Destination unreachable message*



- The code field for this type specifies the reason for discarding the datagram and explains exactly what has failed:

- **Code 0.** No path to destination.
- **Code 1.** Communication with the destination is administratively prohibited.
- **Code 2.** Beyond the scope of source address.
  - **Code 3.** Destination address is unreachable.
  - **Code 4.** Port unreachable.
  - **Code 5.** Source address failed (filtering policy).
  - **Code 6.** Reject route to destination

Figure 5 ***Packet-too-bit message***

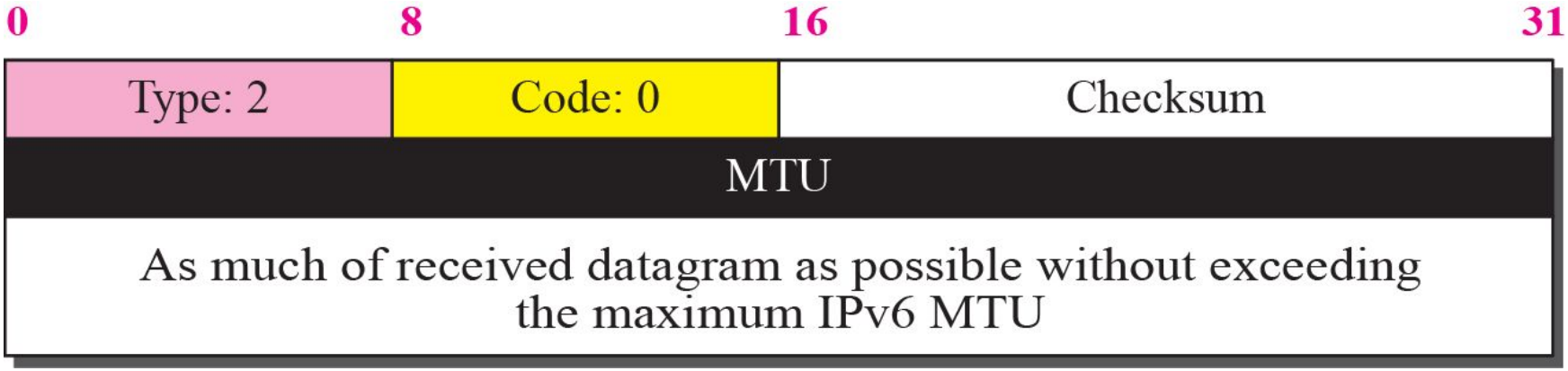


Figure 6 *Time-exceeded message*

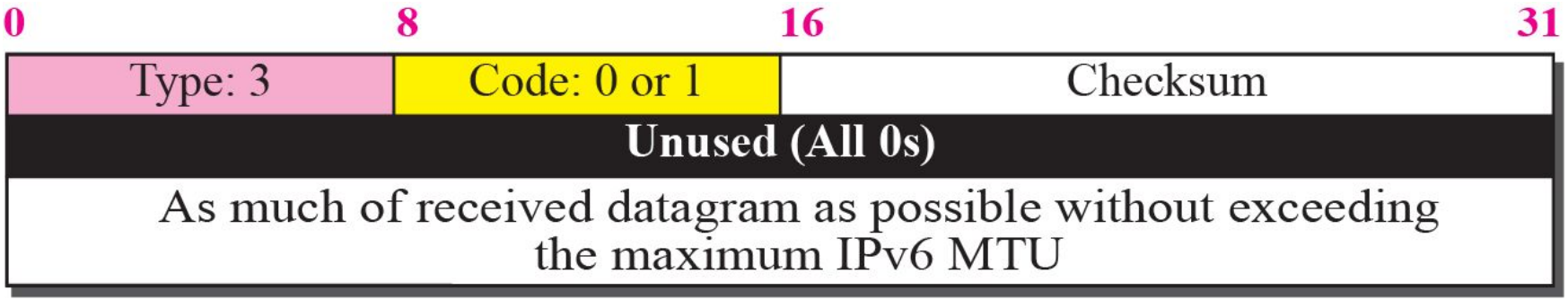
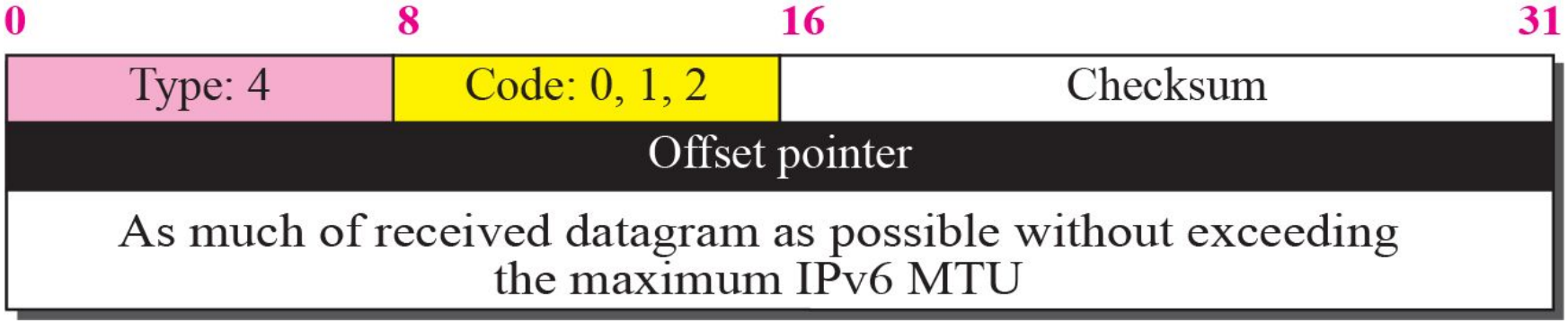


Figure 7 ***Parameter-problem message***



3 INFORMATIONAL MESSAGES

Two of the ICMPv6 messages can be categorized as informational messages: echo request and echo reply messages. The echo request and echo response messages are designed to check if two devices in the Internet can communicate with each other. A host or router can send an echo request message to another host; the receiving computer or router can reply using the echo response message.

Figure 8 *Echo-request message*

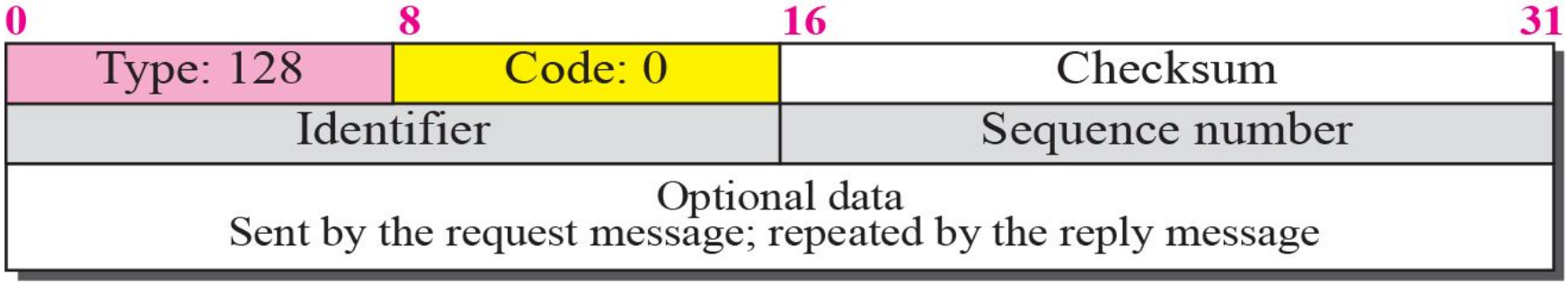
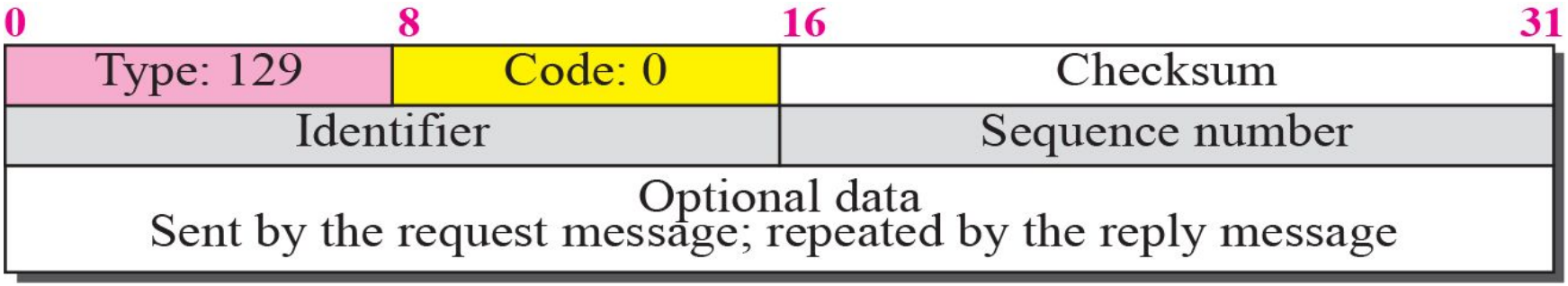


Figure 9 *Echo-reply message*



4 NEIGHBOR-DISCOVERY MESSAGES

Several messages in the ICMPv4 have been redefined in ICMPv6 to handle the issue of neighbor discovery. Some new messages have also been added to provide extension. The most important issue is the definition of two new protocols that clearly define the functionality of these group messages: the Neighbor-Discovery (ND) protocol and the Inverse-Neighbor-Discovery (IND) protocol. These two protocols are used by nodes (hosts or routers) on the same link (network).

- These two protocols are used by nodes (hosts or routers) on the same link (network) for three main purposes:
  1. Hosts use the ND protocol to find routers in the neighborhood that will forward packets for them.
  2. Nodes use the ND protocol to find the link layer addresses of neighbors (nodes attached to the same network).
  3. Nodes use the IND protocol to find the IPv6 addresses of the neighbor

Figure 10 *Router-solicitation message*

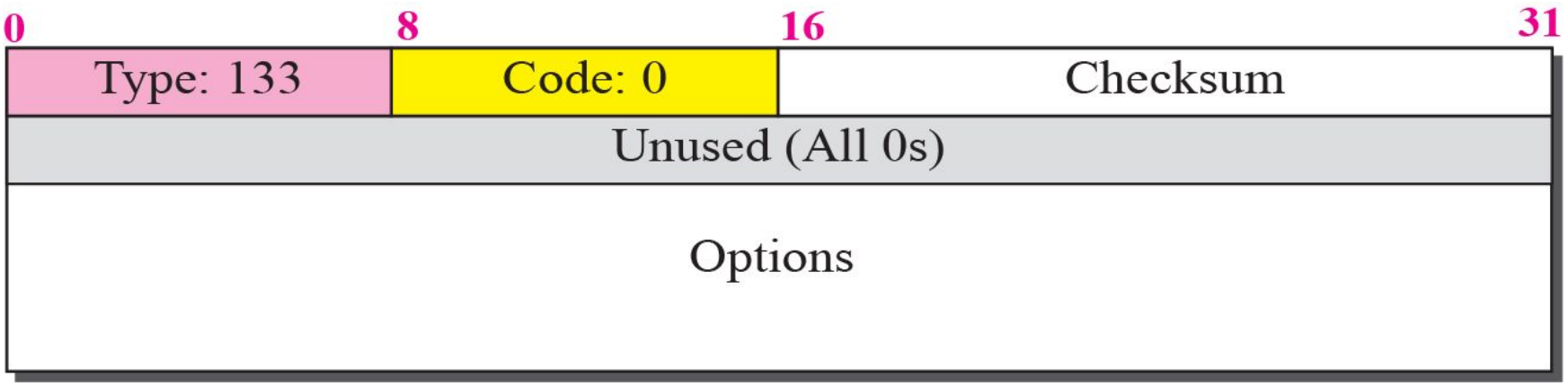
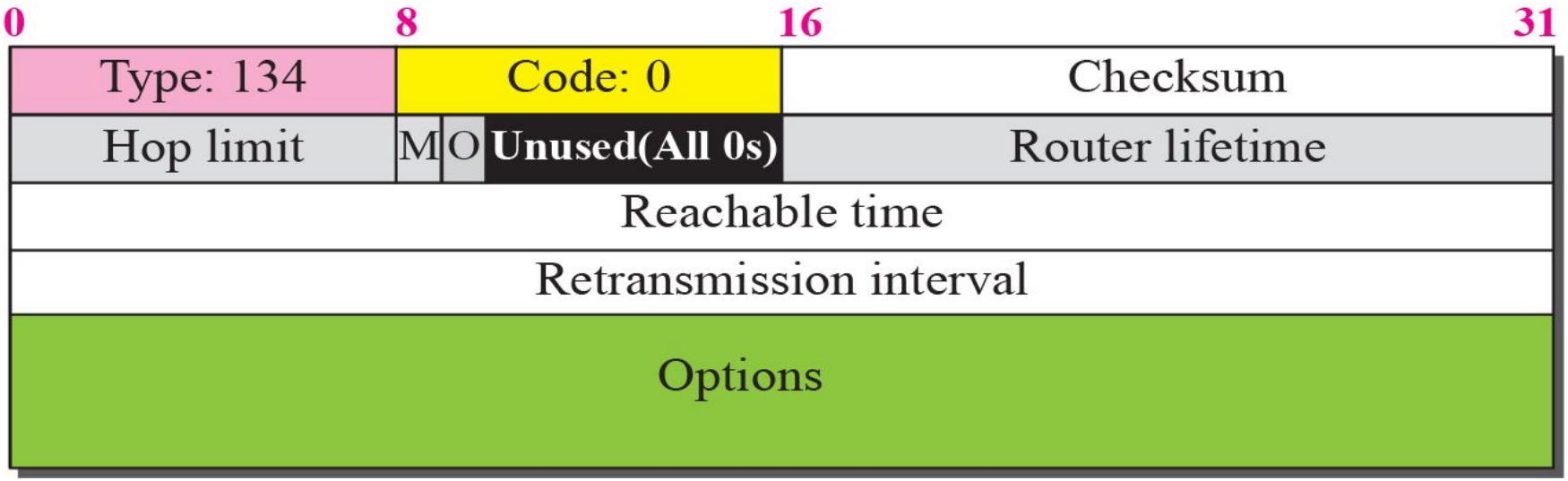


Figure 11 *Router-advertisement message*



The fields are explained below:

- **Hop Limit.** This 8-bit field limits the number of hops that the requestor should use as the hop limit in its IPv6 datagram.
- **M.** This 1-bit field is the "manage address configuration" field. When this bit is set to 1, the host needs to use the administration configuration.
- **O.** This 1-bit field is the "other address configuration" field. When this bit is set to 1, the host needs to use the appropriate protocol for configuration.
- **Router Lifetime.** This 16-bit field defines the lifetime (in units of seconds) of the router as the default router. When the value of this field is 0, it means that the router is not a default router.
- **Reachable Time.** This 32-bit field defines the time (in units of seconds) that the router is reachable.
- **Retransmission Interval.** This 32-bit field defines the retransmission interval (in units of seconds).
- **Option.** Some possible options are the link layer address of the link from which the message is sent, the MTU of the link, and address prefix information.

Figure 12 *Neighbor-solicitation message*

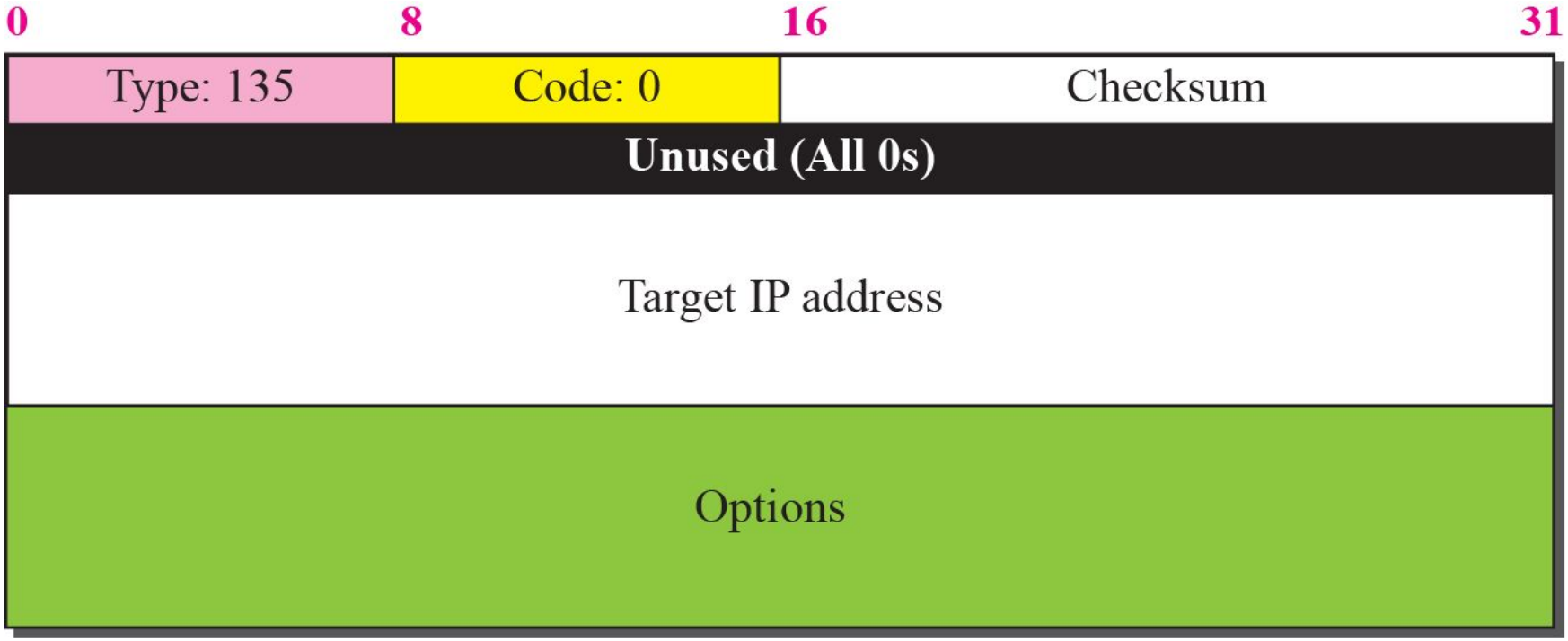
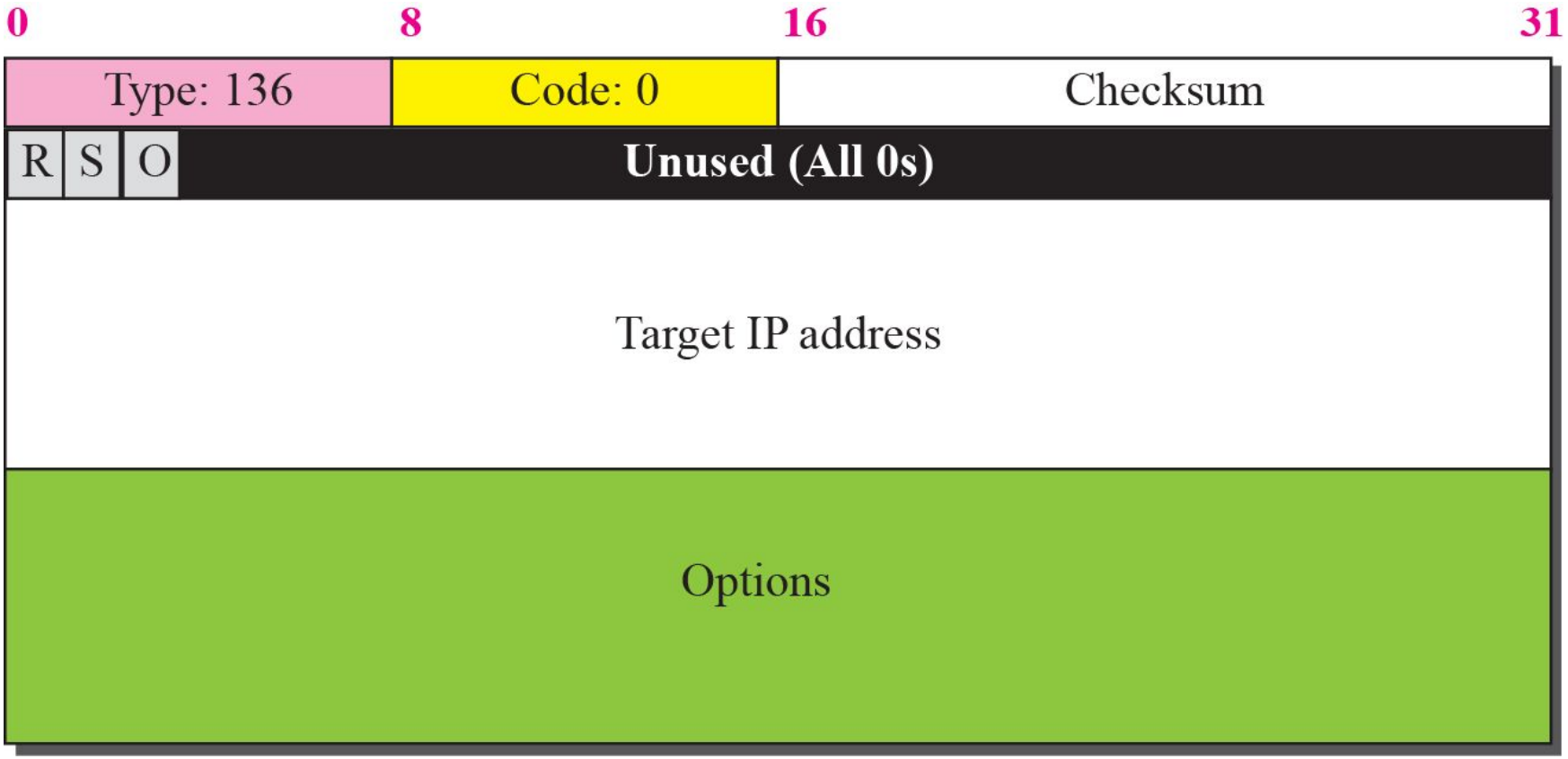


Figure 13 *Neighbor advertisement message*



- **R.** This 1-bit field is the "router" flag. When it is set to 1, it means the sender of this message is a router.
- **S.** This 1-bit field is the "solicitation" flag. When it is set to 1, it means that the sender is sending this advertisement in response to a neighbor solicitation. An advertisement can be sent by a host or router without solicitation.
- **O.** This 1-bit field is the "override" flag. When it is set, it means that the advertisement should override existing information in the cache.
- **Option.** The only possible option is the link layer address of the advertiser.

Figure 14 ***Redirection message***

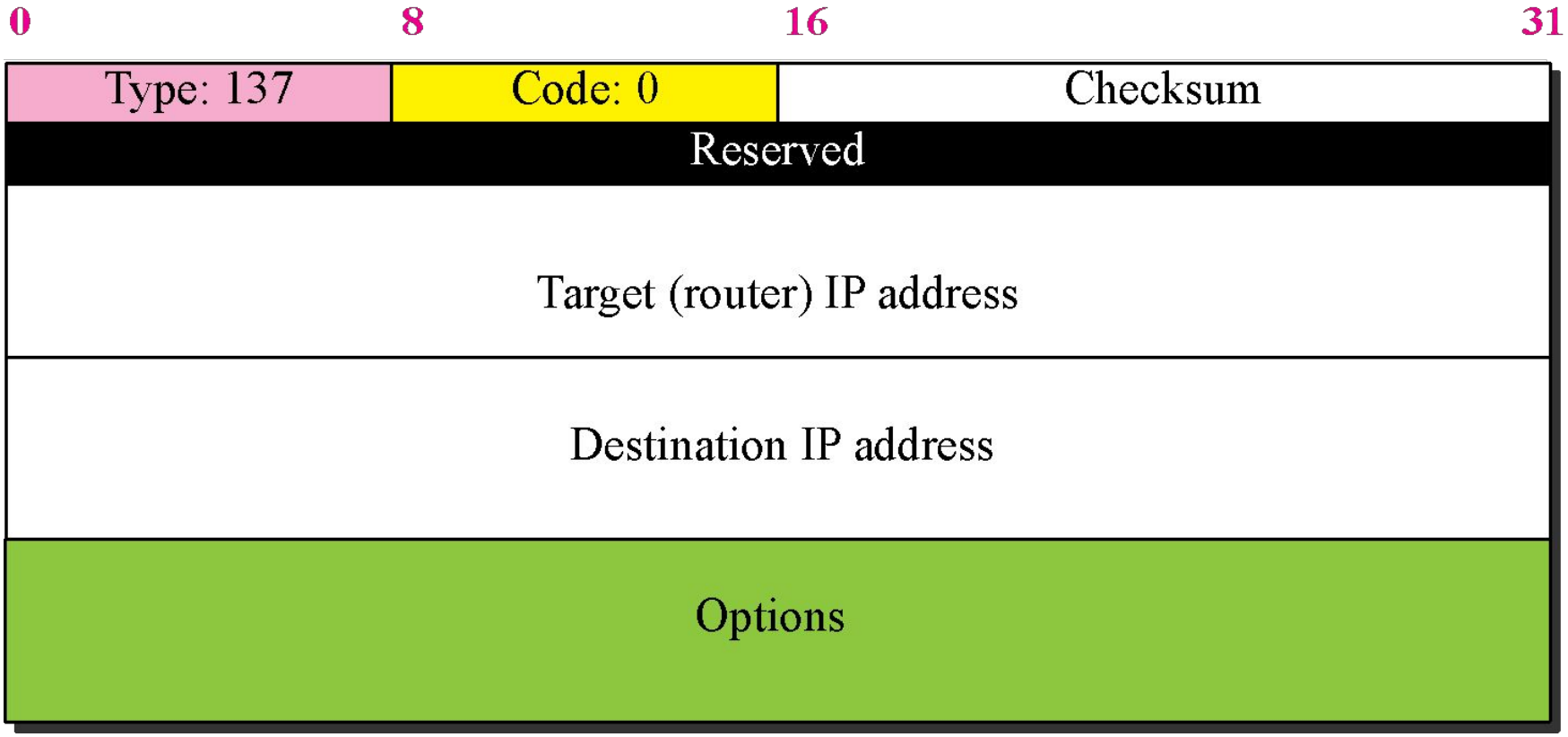


Figure 15 *Inverse-neighbor-solicitation message*

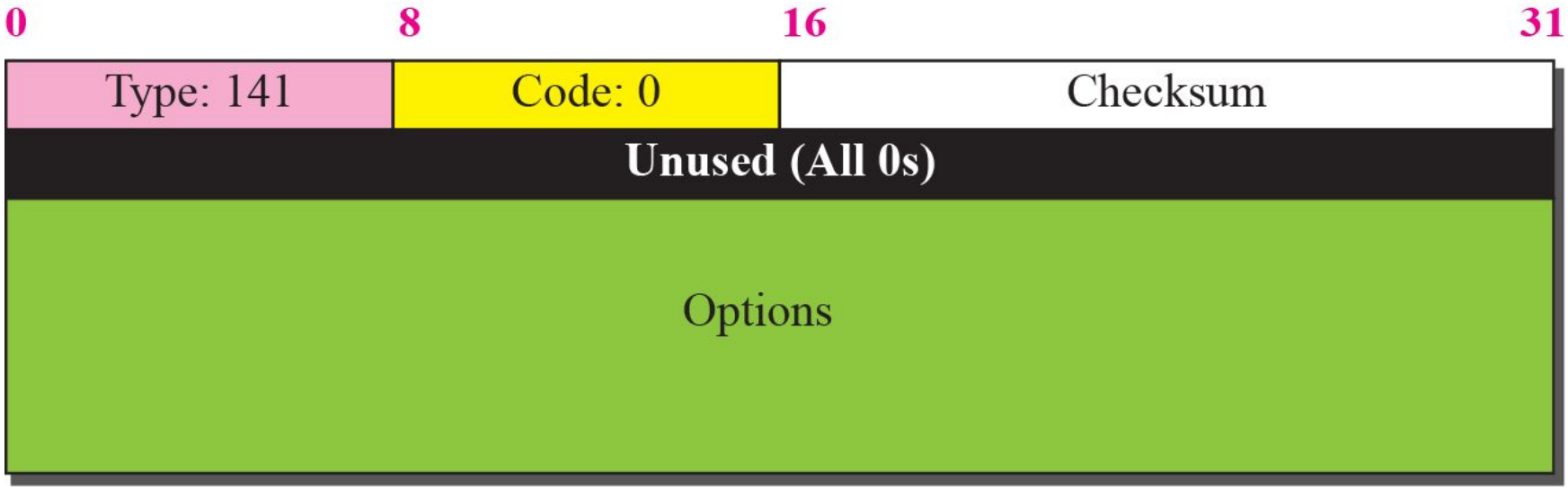
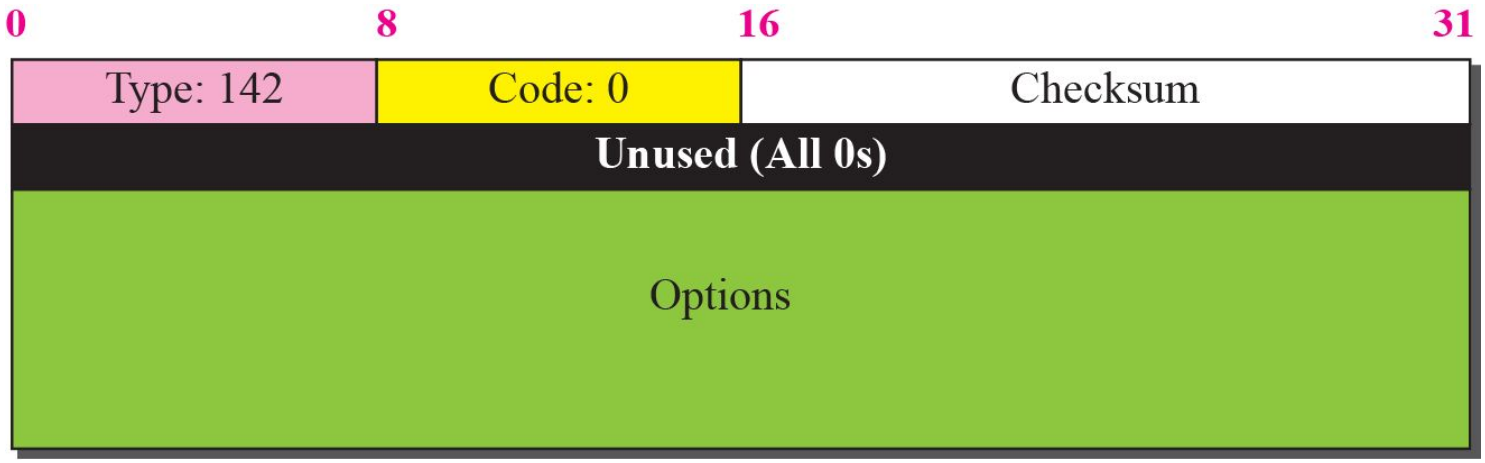


Figure 16 *Inverse-neighbor-advertisement message*



5 GROUP MEMBERSHIP MESSAGES

The management of multicast delivery handling in IPv4 is given to the IGMPv3 protocol. In IPv6, this responsibility is given to the Multicast Listener Delivery protocol. MLDv1 is the counterpart to IGMPv2; MLDv2 is the counterpart to IGMPv3. The material discussed in this section is taken from RFC 3810. The idea is the same as in IGMPv3, but the sizes and formats of the messages have been changed to fit the larger multicast address size in IPv6.

Figure 17 *Membership query message format*

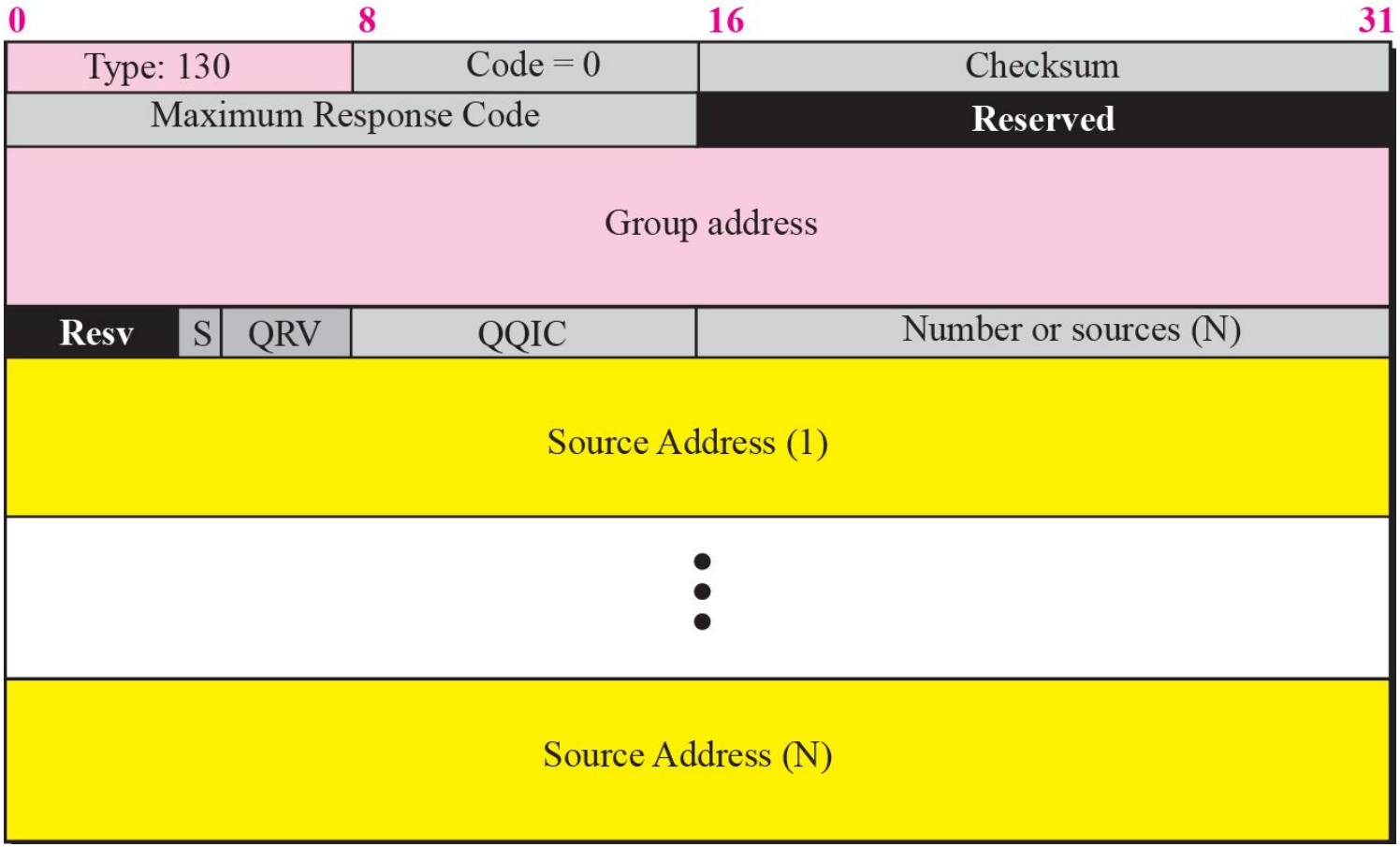


Figure 18 *Membership-report message format*