Fragmentation

- The format and size of a frame depend on the protocol used by the physical network through which the frame has just traveled.
  - We must divide the datagram to make it possible to pass through these networks. This is called fragmentation.
- Each data link layer protocol has its own frame format in most protocols.

- When a datagram is encapsulated in a frame, the total size of the datagram must be less than the maximum size.
  - Maximum transfer(transmission) unit (MTU)

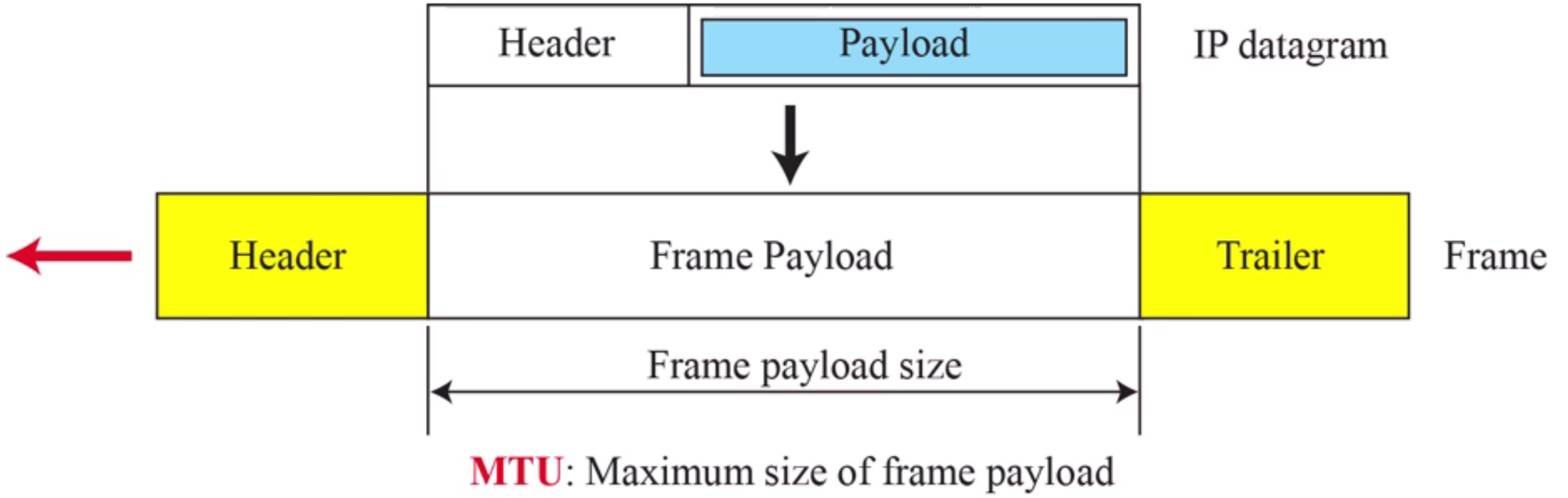
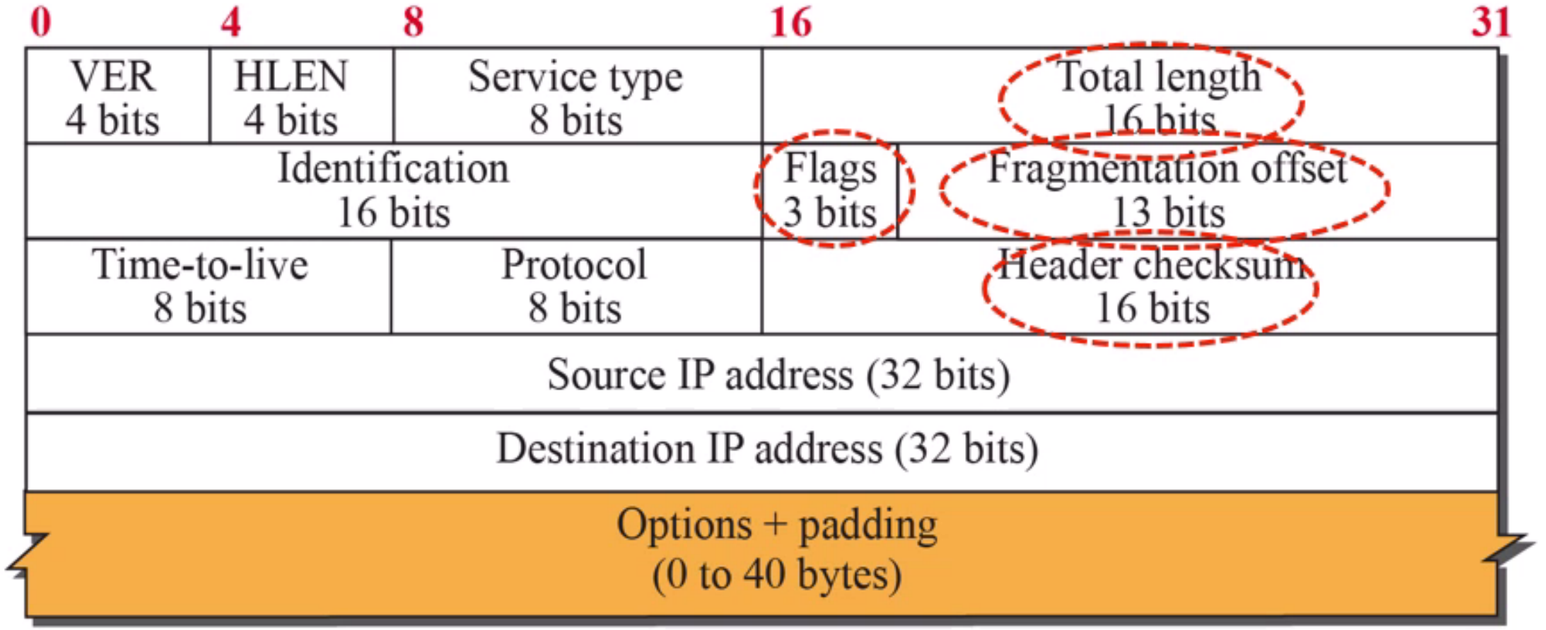


Figure 7.16 Maximum transfer unit (MTU)

Media for IP transport	Maximum transmission unit (bytes)	Notes
Internet IPv4 path MTU	At least 68,[5] max of 64 KiB[6]	Systems may use Path MTU Discovery[7] to find the actual path MTU. Routing from larger MTU to smaller MTU causes IP fragmentation.
Internet IPv6 path MTU	At least 1280,[8] max of 64 KiB, but up to 4 GiB with optional jumbogram[9]	Systems must use Path MTU Discovery[10] to find the actual path MTU.
X.25	Minimal 576 (sending) or 1600 (receiving)[11]	
Ethernet v2	1500[12]	Nearly all IP over Ethernet implementations use the Ethernet II frame format.
Ethernet with LLC and SNAP	1492[13]	
Ethernet jumbo frames	1501 – 9202[14] or more[15]	The limit varies by vendor. For correct interoperation, frames should be no larger than the maximum frame size supported by any device on the network segment.[16] Jumbo frames are usually only seen in special-purpose networks.
PPPoE v2	1492[17]	Ethernet II MTU (1500) less PPPoE header (8)
DS-Lite over PPPoE	1452	Ethernet II MTU (1500) less PPPoE header (8) and IPv6 header (40)
PPPoE jumbo frames	1493 – 9190 or more[18]	Ethernet Jumbo Frame MTU (1501 - 9198) less PPPoE header (8)
IEEE 802.11 Wi-Fi (WLAN)	2304[19]	The maximum MSDU size is 2304 before encryption. WEP will add 8 bytes, WPA-TKIP 20 bytes, and WPA2-CCMP 16 bytes.
Token Ring (802.5)	4464	
FDDI	4352[7]	

- When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but some changed.
- A datagram can be fragmented *by the source host* or *any router in the path*.
  - A datagram can be fragmented several times before it reaches the final destination.
  - **Flags, fragmentation offset, total length, and checksum field** must be changed.
- The reassembly of the datagram, however, is done *only by the destination host*.

Datagram



b. Header format

Fields related to fragmentation

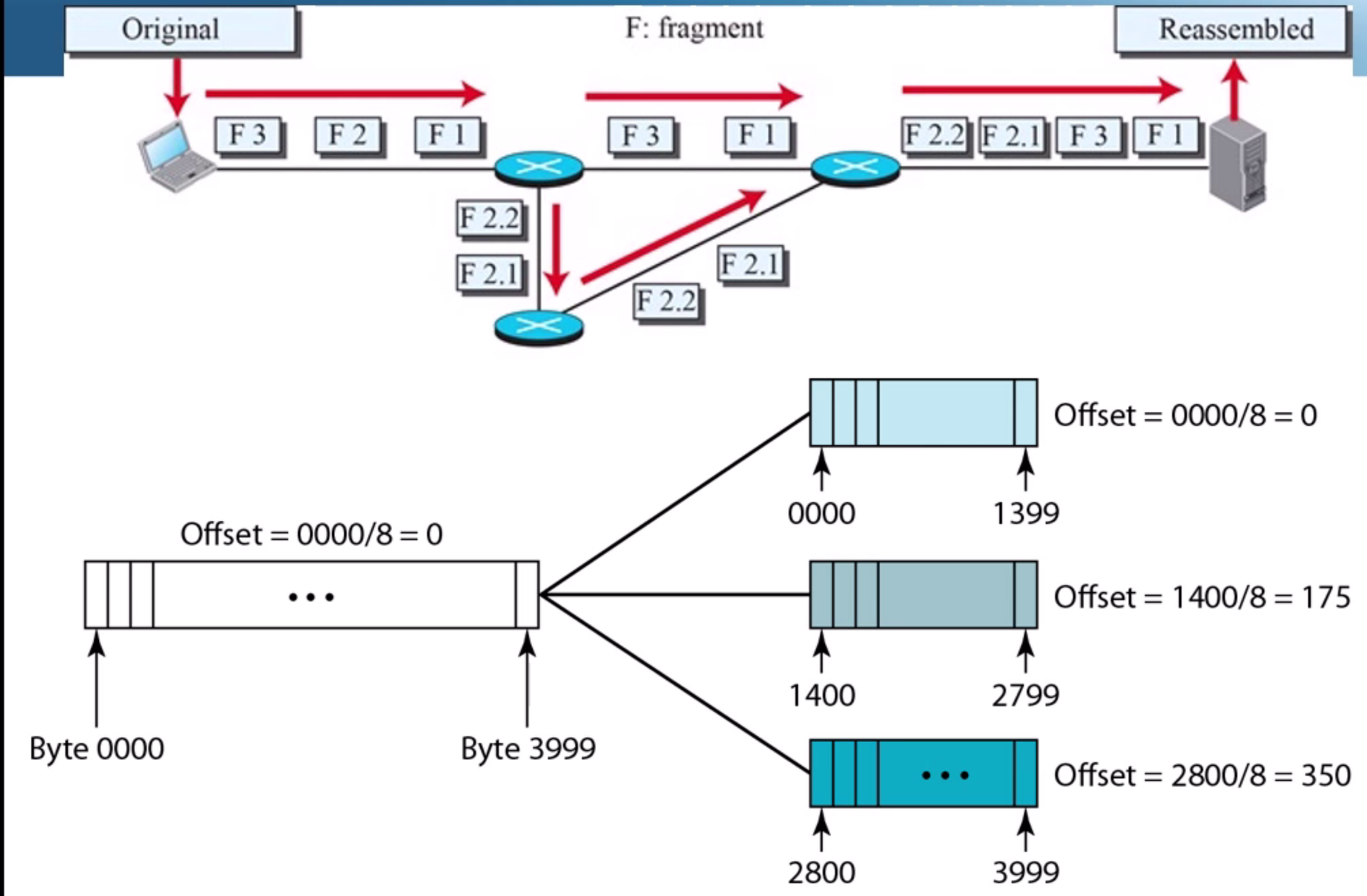
- Identification
  - This identifies a datagram originating from the source.
  - When a datagram is fragmented, the value in the identification field is copied into all fragments.
  - It knows that all fragments having the same identification value must be assembled into one datagram.

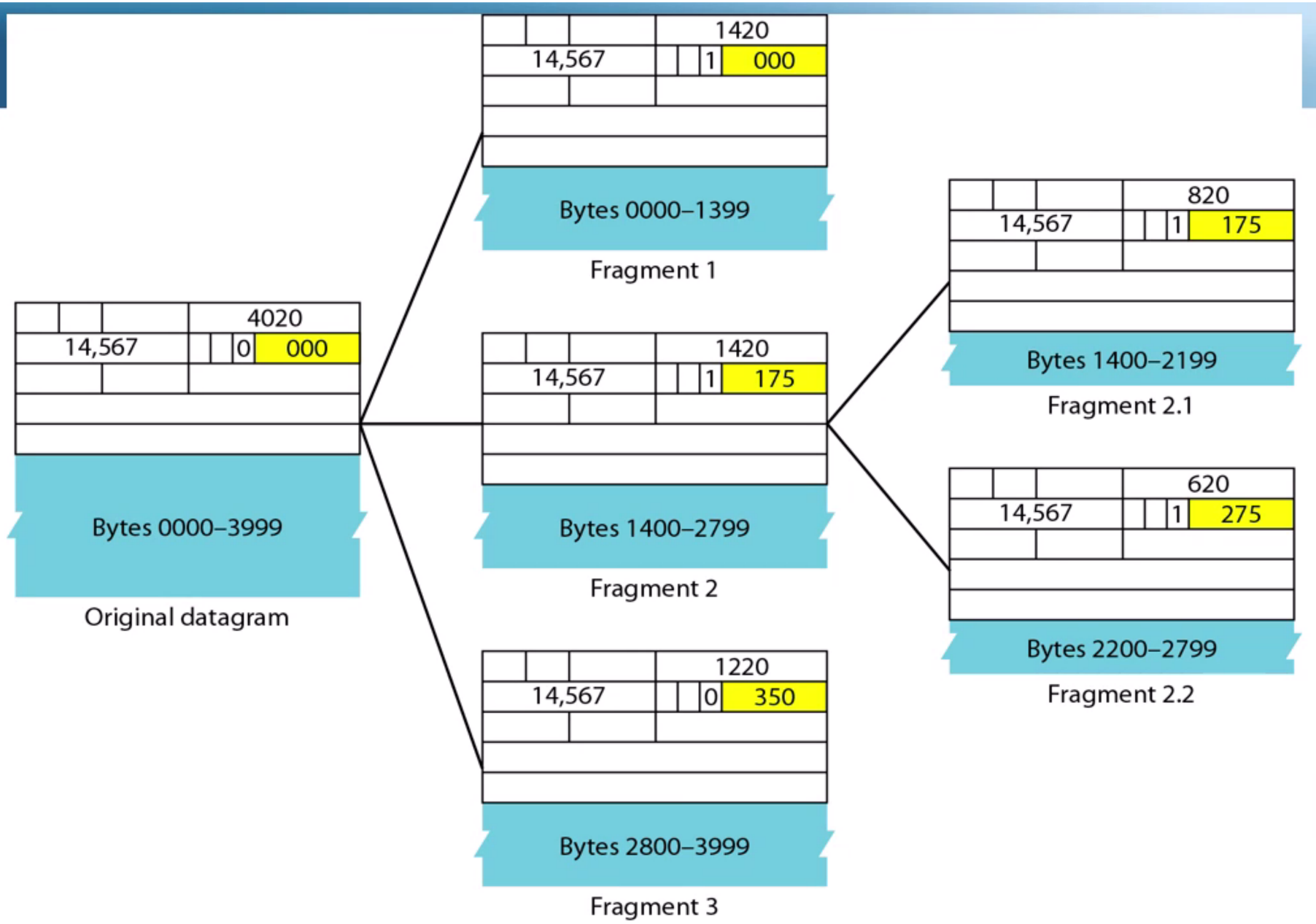
- Flags
  - This is a 3-bit field.
  - The first bit is reserved.

D: Do not fragment
M: More fragments

  - The second bit is called the *do not fragment* bit.
    - If its value is 1, the machine must not fragment the datagram.
    - If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.
  - The third bit is called the *more fragment* bit.
    - If its value is 1, it means the datagram is not the last fragment.
    - If its value is 0, it means this is the last or only fragment.

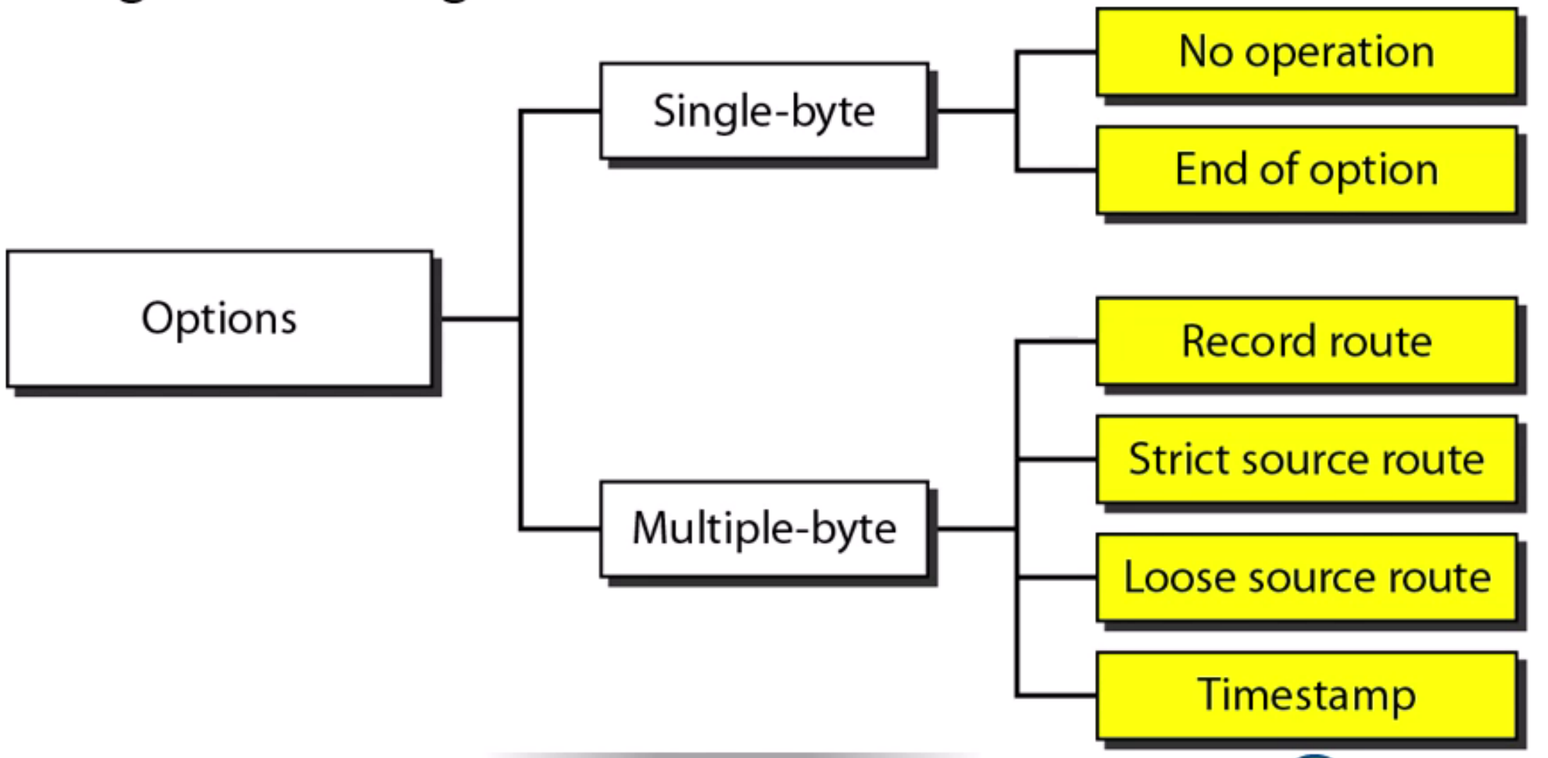
- Fragmentation offset
  - This 13-bit field shows the relative position of this fragment with respect to the whole datagram.
  - It is the offset of the data in the original datagram *measured in units of 8 bytes*.





Options

- Options can be a maximum of 40 bytes.
  - Options can be used for network testing and debugging.
  - The existence of options in a header creates some burden on the datagram handling.



- A no-operation option is a 1-byte option used as a filler between options.
- An end-of-option option is a 1-byte option used for padding at the end of the option field.
- A record route option is used to record the Internet routers.
  - It can list up to nine router addresses.
- A strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet.

Security of IPv4 Datagrams

- No security was provided for the IPv4 protocol.
- There are three security issues that are particularly applicable to the IP protocol: packet sniffing, packet modification, and IP spoofing.
- Packet sniffing
  - It is a passive attack, in which the attacker does not change the contents of the packet.
  - *Encryption* of the packet can make the attacker's effort useless.

- Packet modification
  - The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.
  - This type of attack can be detected using *a data integrity* mechanism.
- IP spoofing
  - An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.
  - This type of attack can be prevented using *an origin authentication mechanism.*

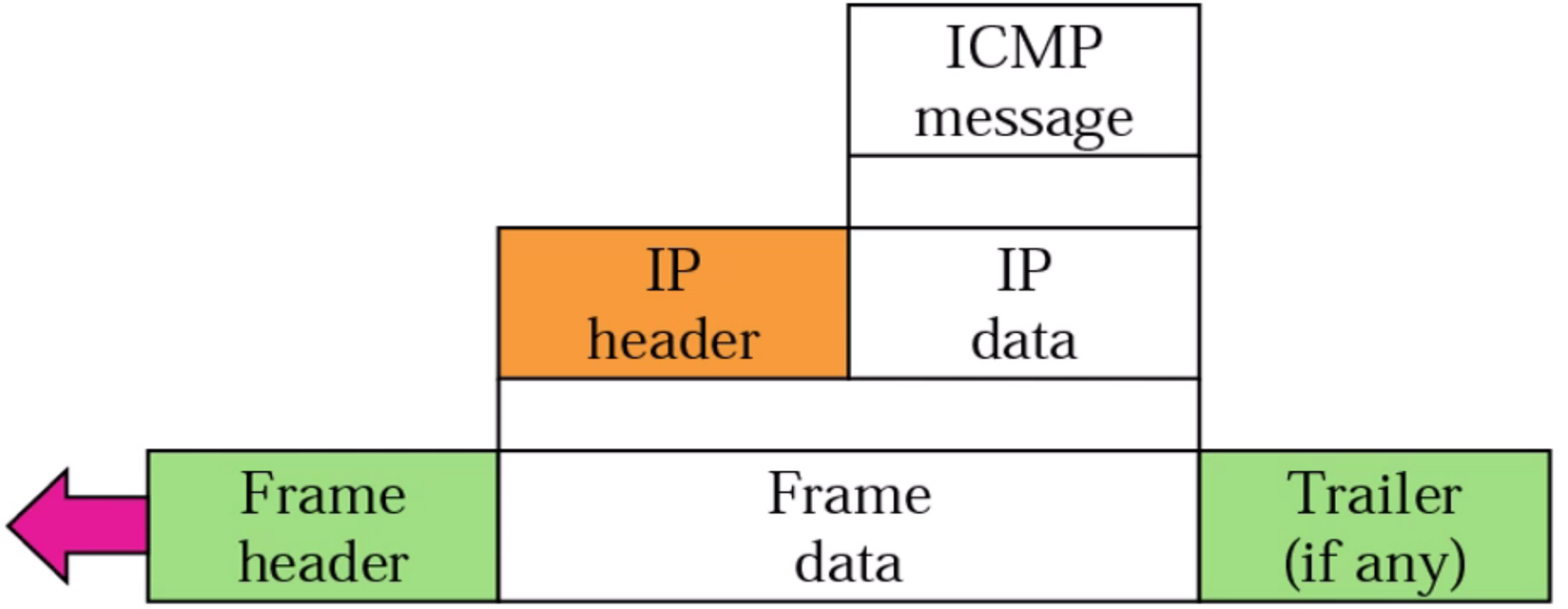
IPSec

- This protocol, which is used in conjunction with the IP protocol, creates a connection-oriented service between two entities in which they can exchange IP packets without worrying about the three attacks discussed above.
- IPSec provides the following four services:
  - Defining algorithms and keys
  - Packet encryption
  - Data integrity
  - Origin authentication

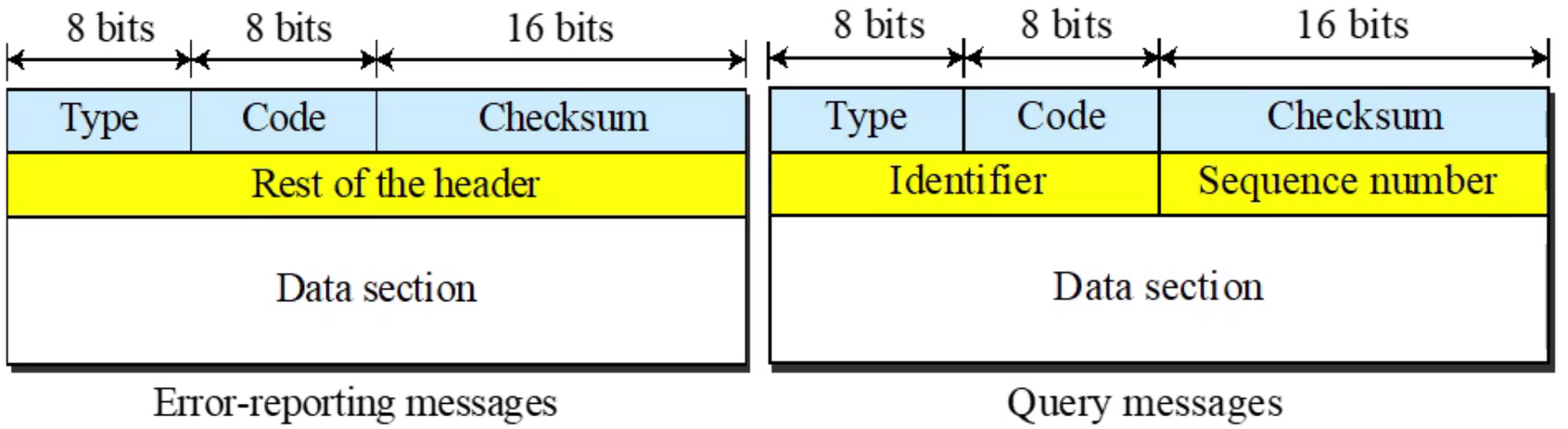
ICMPv4

- IP has two deficiencies: lack of error control and lack of assistance mechanisms.
  - No error-reporting or error-correcting mechanism
  - Lack of a mechanism for host and management queries.
- The Internet Control Message Protocol (ICMP) has been designed to compensate for the deficiencies.
- ICMP messages are divided into two broad categories.
  - Error-reporting messages
  - Query messages

- The value of the protocol field in the IP datagram is 1 to indicate that the IP data are an ICMP message.



Message format



Type and code values

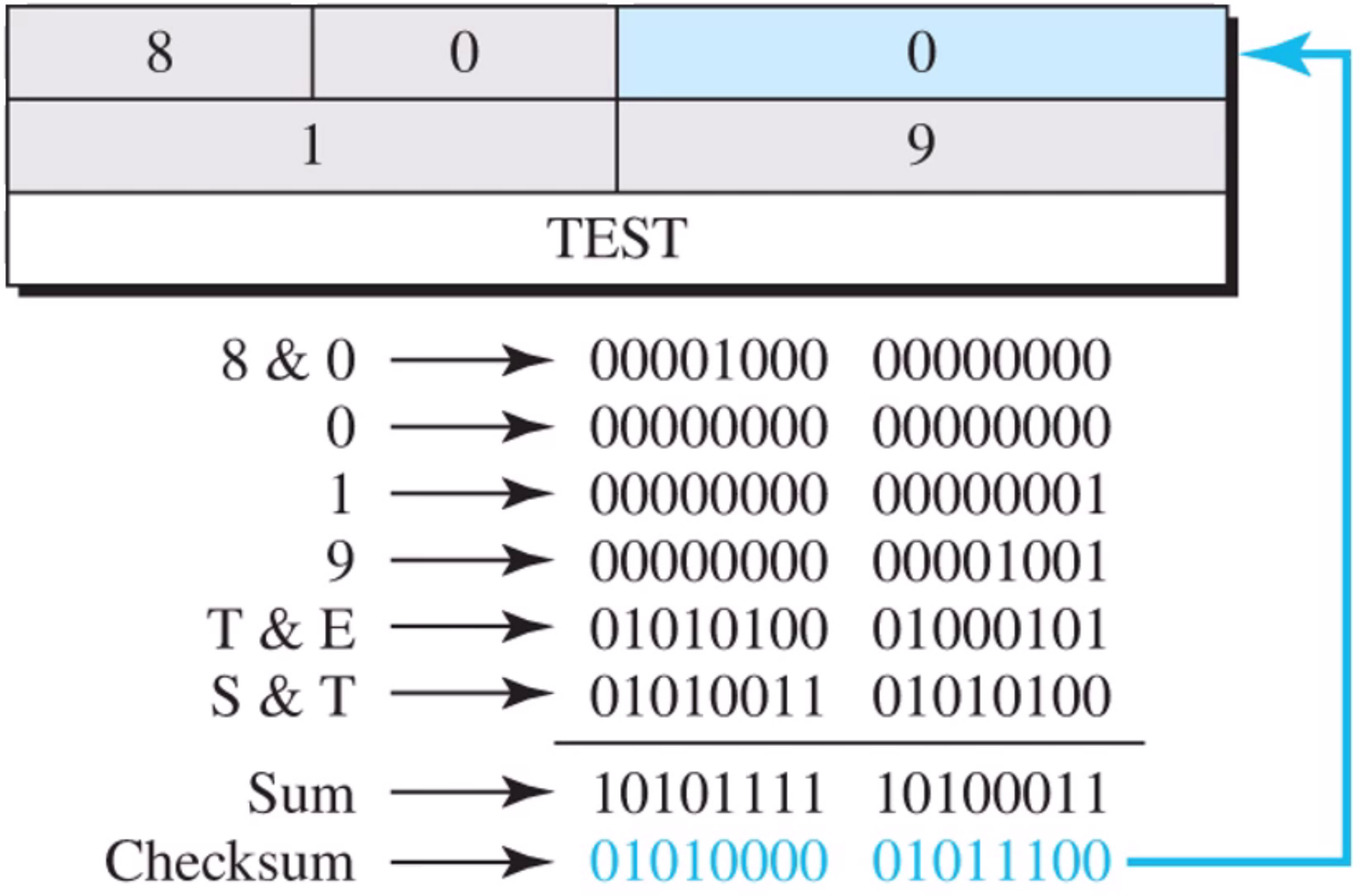
Error-reporting messages	Query messages
03: Destination unreachable (codes 0 to 15)	08 and 00: Echo request and reply (only code 0)
04: Source quench (only code 0)	13 and 14: Timestamp request and reply (only code 0)
05: Redirection (codes 0 to 3)	
11: Time exceeded (codes 0 and 1)	
12: Parameter problem (codes 0 and 1)	

Note: See the book website for more explanation about the code values.

Figure 7.19 General format of ICMP messages

- Type defines the type of message.
- The code field specifies the reason for the particular message type.
- The checksum is calculated over the entire message (header and data).
  - Figure 7.22 shows an example of checksum calculation for a simple echo-request message.
  - The identifier and the sequence number are randomly chosen by 1 and 9 respectively.

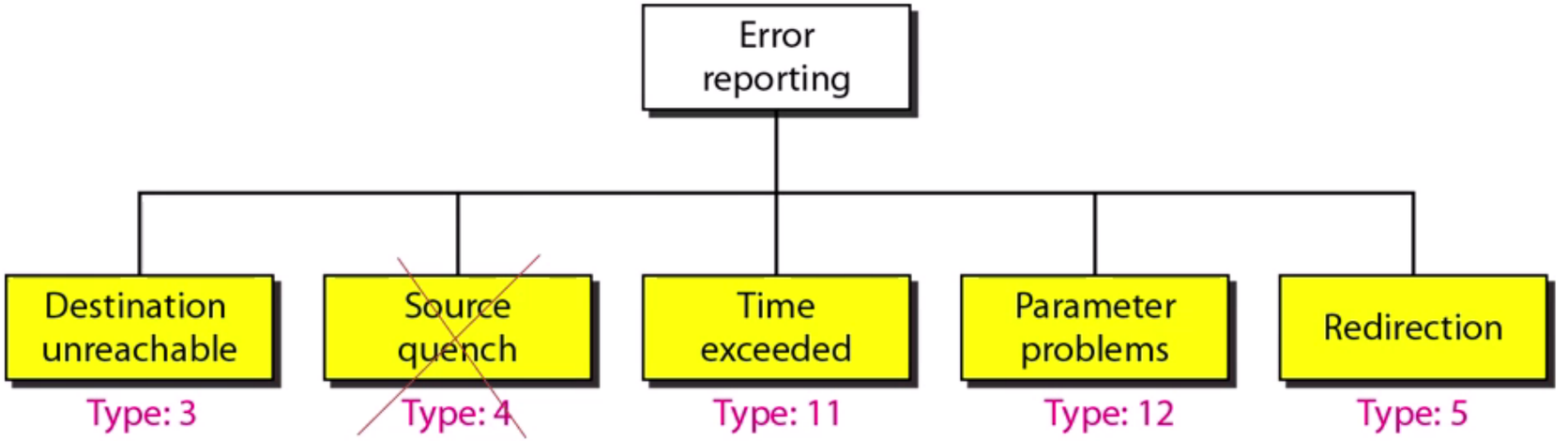
Figure 7.22 Example of checksum calculation



- The rest of the header is specific for each message.
- The data section in error messages carries information for finding the original packet that had the error.
- In query messages, the data section carries extra information based on the type of the query.

Error reporting

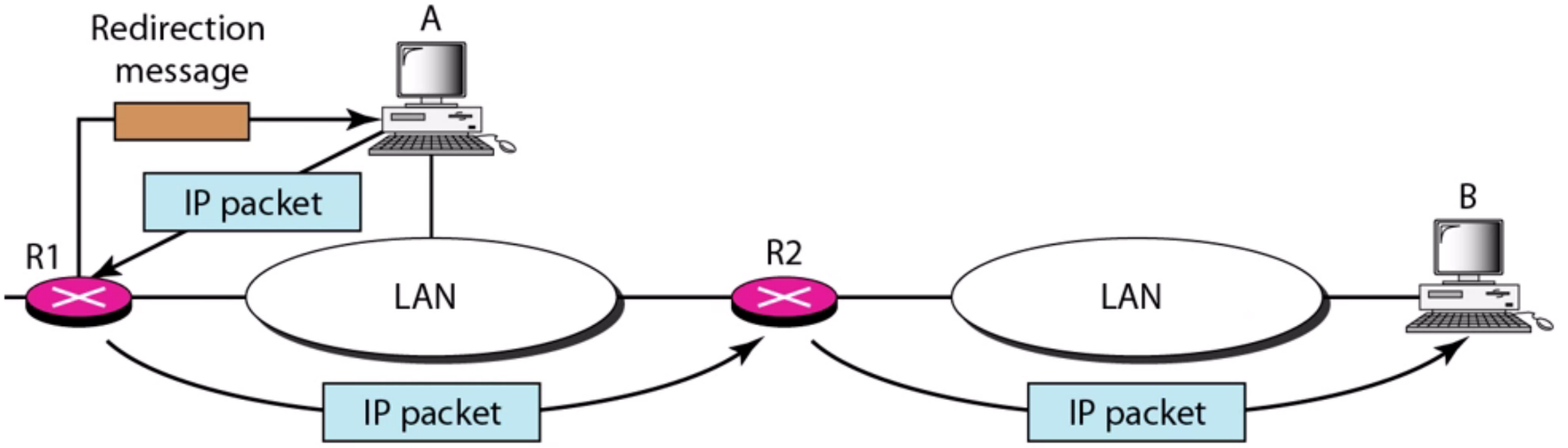
- ICMP does not correct errors: it simply reports them.

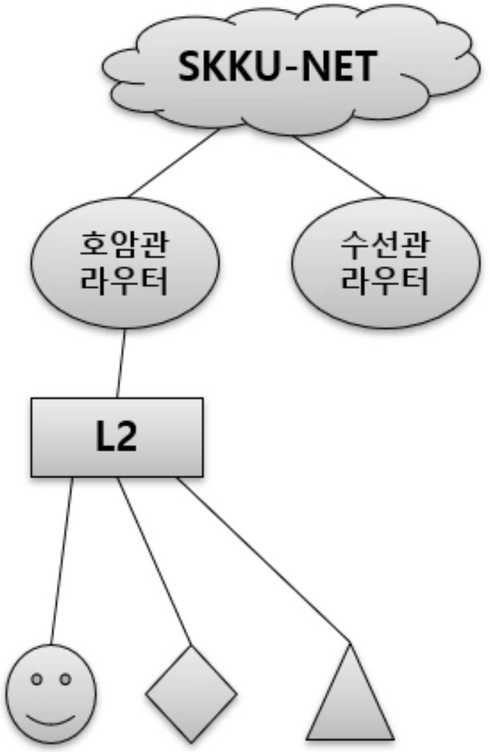


- Destination unreachable
  - When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination unreachable message back to the source host.
- Source quench
  - There is no flow control or congestion control mechanism in IP.
  - When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram.

- Time exceeded
  - The router that receives a datagram with a value of 0 in the TTL field discards the datagram.
  - A time-exceeded message is also generated when all fragments that make up a message do not arrive at the destination host within a certain time limit.
- Parameter problem
  - If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends this type of message.

- Redirection
  - A host usually use static routing. The host may send a datagram, which is destined for another network, to the wrong router.
  - To update the routing table of a host, it sends a redirection message back to the host.





인터넷 프로토콜 버전 4(TCP/IPv4) 속성

일반

네트워크가 IP 자동 설정 기능을 지원하면 IP 설정이 자동으로 할당되도록 할 수 있습니다. 지원하지 않으면, 네트워크 관리자에게 적절한 IP 설정값을 문의해야 합니다.

○ 자동으로 IP 주소 받기(O)

● 다음 IP 주소 사용(S):

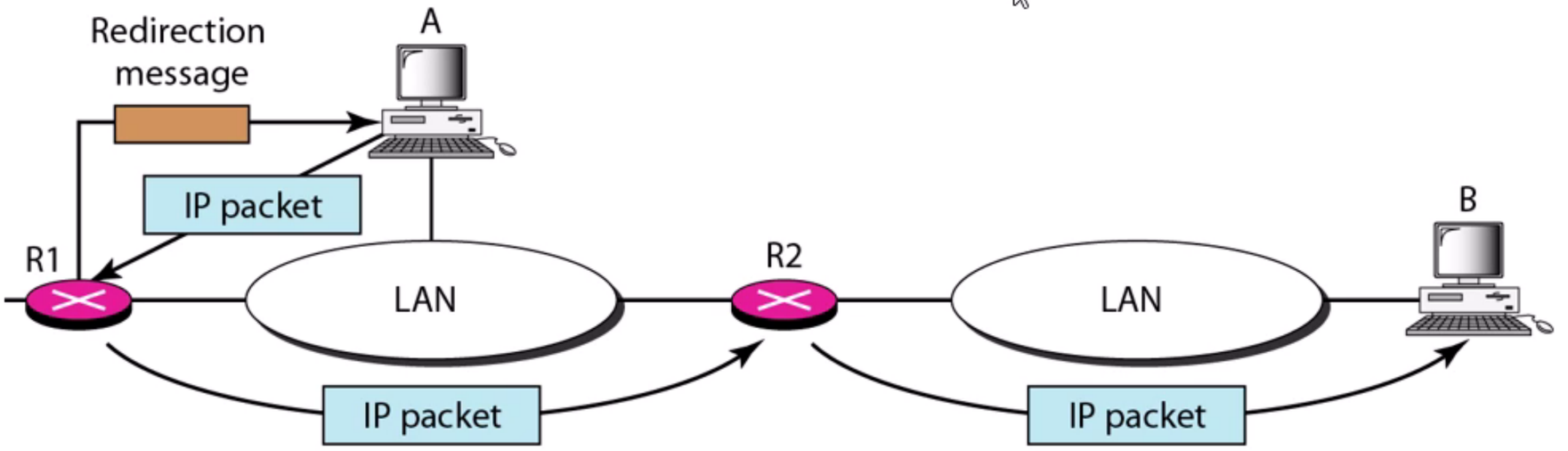
IP 주소(I):	115 . 145 . 34 .
서브넷 마스크(U):	255 . 255 . 255 . 0
기본 게이트웨이(D):	115 . 145 . 34 . 1

○ 자동으로 DNS 서버 주소 받기(B)

● 다음 DNS 서버 주소 사용(E):

기본 설정 DNS 서버(P):	115 . 145 . 0 . 11
보조 DNS 서버(A):	168 . 126 . 63 . 1

- Redirection
  - A host usually use static routing. The host may send a datagram, which is destined for another network, to the wrong router.
  - To update the routing table of a host, it sends a redirection message back to the host.



- Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram.
  - The original datagram header is added to give the original source, which receives the error message.
  - The first 8 bytes of data provide information about the port numbers (UDP and TCP) and sequence number (TCP).