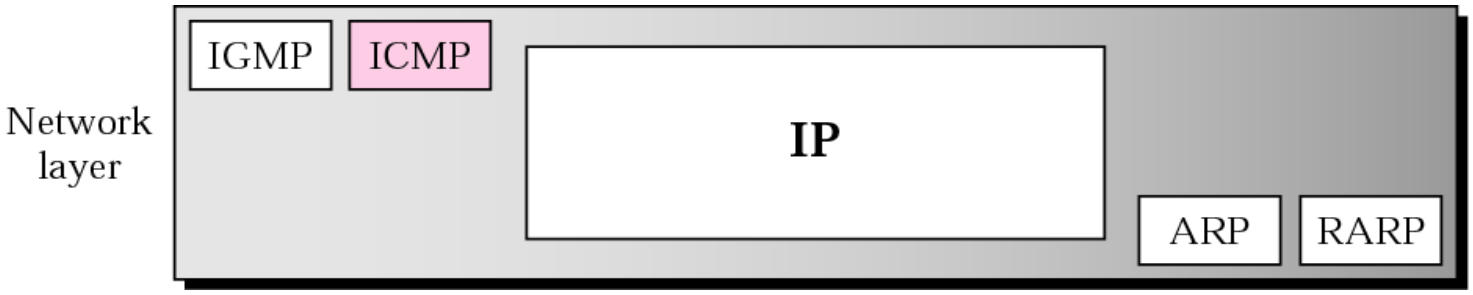
ICMPv4

- IP protocol has no error-reporting or error-correcting mechanism
  - When errors occur, no built-in mechanism to notify the original host.
- IP protocol also lacks a mechanism for host and management queries
  - A host sometimes needs to determine if a router or another host is alive
  - Network manager needs information from another host and router

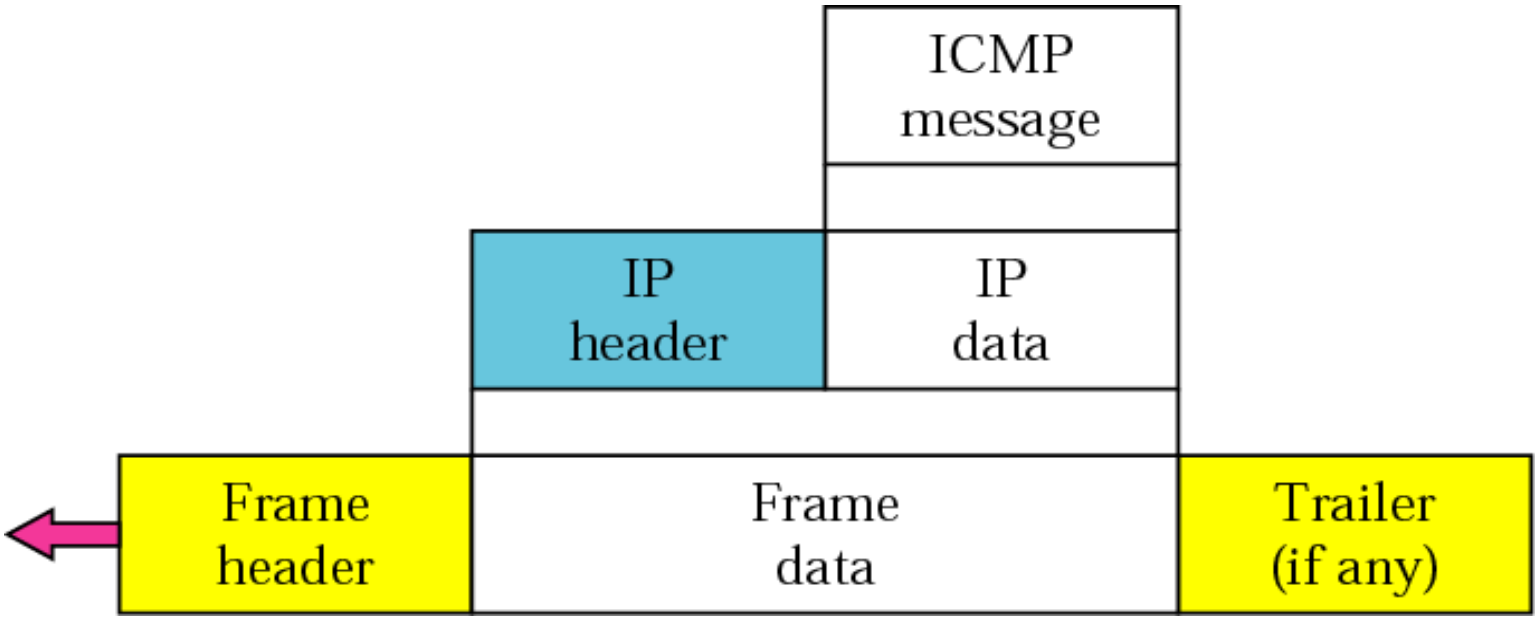
ICMPv4

- Position of ICMP in the network layer
  - ICMP messages are encapsulated inside IP datagrams



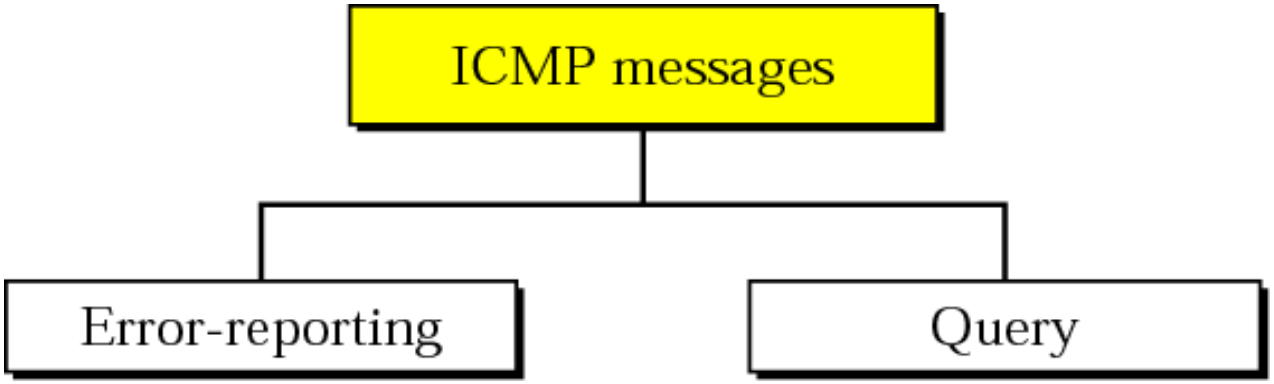
ICMPv4

- ICMP encapsulation
  - The value of the protocol field in the IP datagram : 1



Message

- Category of ICMP messages
  - Error-reporting : 장애 보고
  - Query : 라우터나 호스트의 정보수집



Message

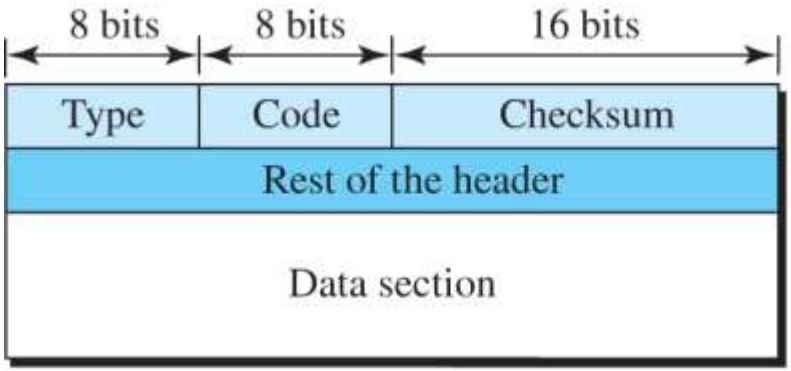
- ICMP messages

Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

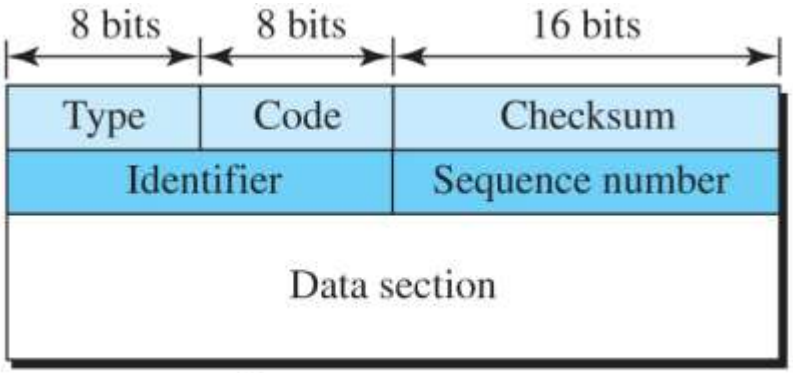
Message

- Having 8 byte header and variable-size data section
  - ICMP type : defining the type of the message
  - Code field : specifying the reason for the particular message type
  - Checksum field
  - Data section
    - In error message, carrying information for finding the original packet which caused the error
    - In query message, carrying extra information based on the type of the query

Figure 7.19 General format of ICMP messages



Error-reporting messages



Query messages

Type and code values

Error-reporting messages

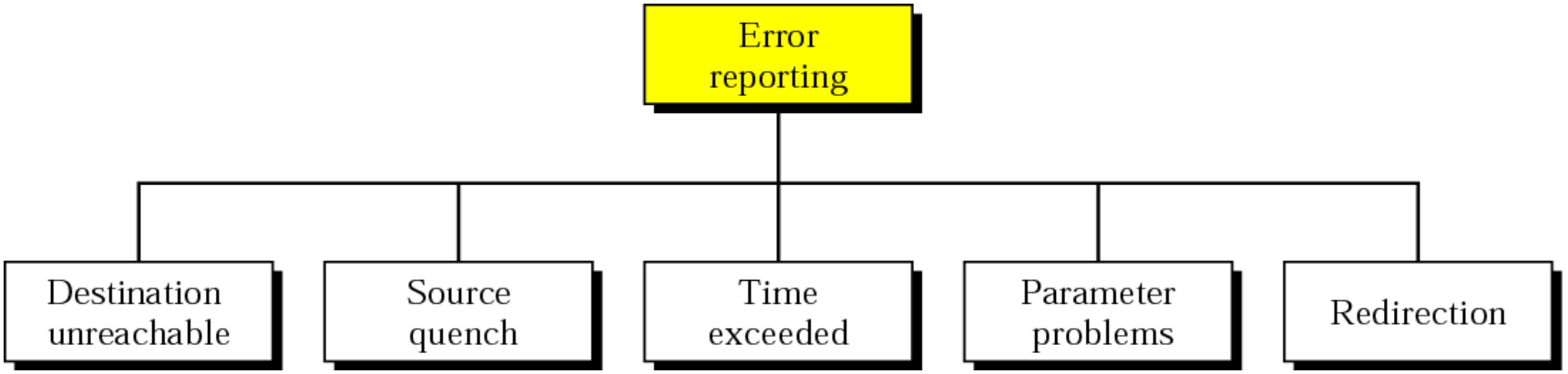
03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages

08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Error Reporting

- Error checking and control
- Not correcting errors : it is left to the higher level protocols
- Always reporting error messages to the original source



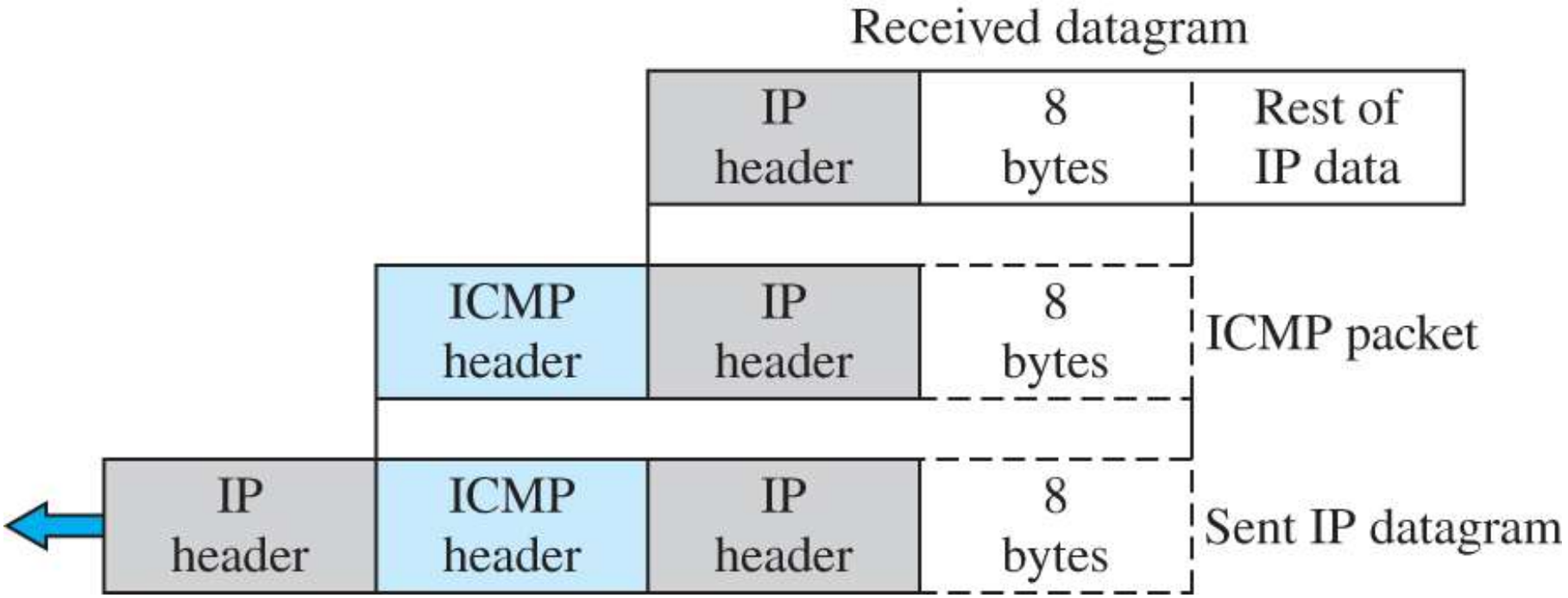
Error Reporting

- Important points about ICMP error messages
  - No ICMP error message will be generated in response to a datagram carrying an ICMP error message
  - No ICMP error message will be generated for a fragmented datagram that is not the first fragment
  - No ICMP error message will be generated for a datagram having a multicast address
  - No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0

Error Reporting

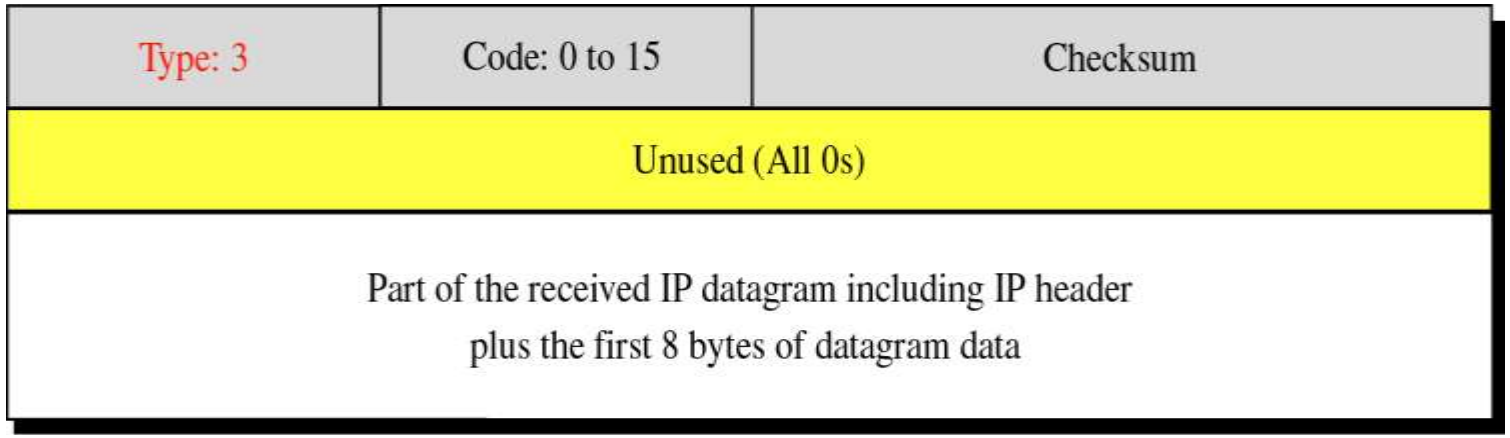
- All error messages
  - Containing a data section that includes the IP header of the original datagram + the first 8 bytes of data of that IP datagram
    - 8 bytes of data : port # (UDP and TCP) and sequence # (TCP)
    - Used for informing to the protocols (TCP or UDP) about the error situation

Figure 7.20 Contents of data field for error messages



Error Reporting

- Destination Unreachable
  - When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded.
  - Then, the router or the host sends a destination unreachable message back to the source that initiated the datagram.



Error Reporting

- Code 0 : Network is unreachable, can only be generated by a router
  - 예를 들면 하드웨어 고장 등의 이유로 네트워크에 도달 불 가능
- Code 1 : Host is unreachable, can only be generated by a router
- Code 2 : Protocol is unreachable, protocol such as UDP, TCP or OSPF is not running at the moment.
  - generated only by the destination
- Code 3 : The port is unreachable, the application program that the datagram is destined for is not running at the moment
- Code 4 : Fragmentation is required, but the DF field has been set
- Code 5 : Source routing cannot be accomplished
- Code 6 : The destination network is unknown.
  - A router has no information about the destination network

Error Reporting

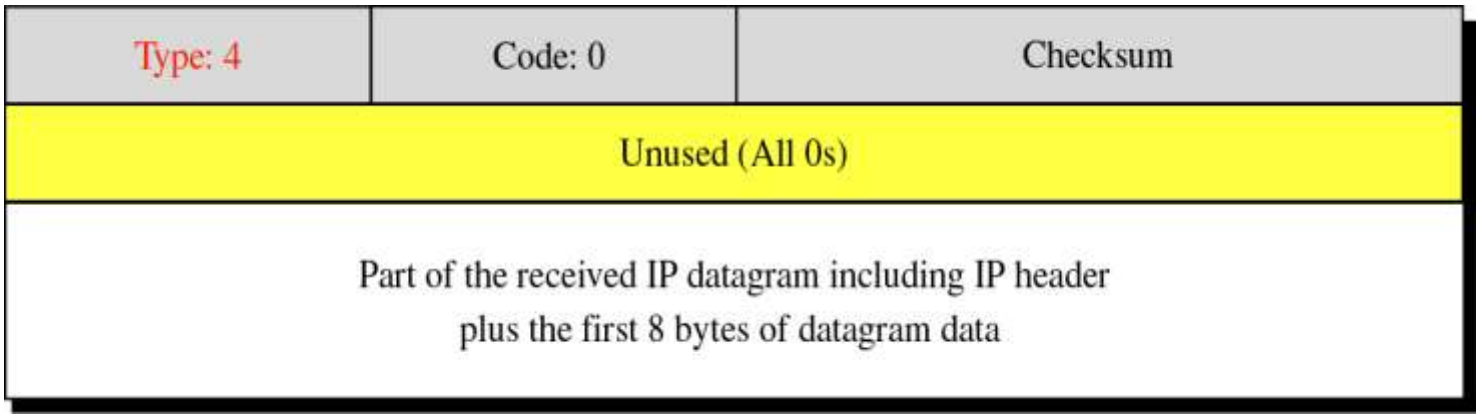
- Code 7 : The destination host is unknown.
  - the router is unaware of the existence of the destination
- Code 8 : The source host is isolated
- Code 9 : Communication with the destination network is administratively prohibited
- Code 10 : Communication with the destination host is administratively prohibited
- Code 11 : The network is unreachable for the specified type of service
- Code 12 : The host is unreachable for the specified type of service
- Code 13 : The host is unreachable because the administration has put a filter on it
- Code 14 : The host is unreachable because the host precedence is violated.
- Code 15 : The host is unreachable because its precedence was cut off.

Error Reporting

- Destination-unreachable messages with codes 2 or 3 can be created only by the destination host. Other destination-unreachable message can be created only by routers
- A router can not detect all problems that prevent the delivery of a packet

Error Reporting

- Source Quench
  - Designed to add a kind of flow control to the IP
    - IP does not have a flow-control mechanism embedded in the protocol
  - When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram
    - making slow down the sending process



Error Reporting

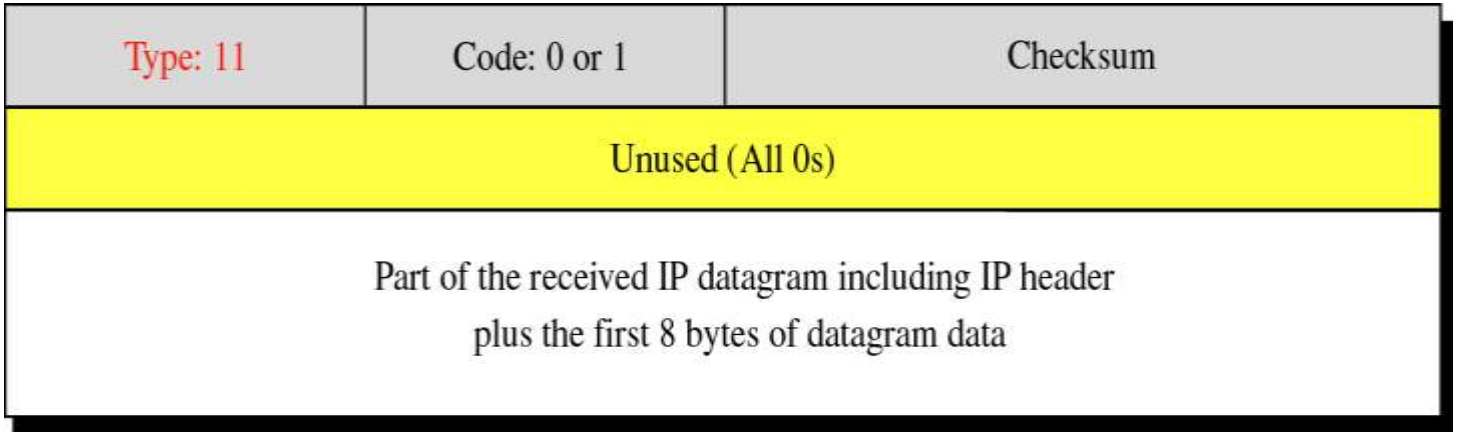
- 혼잡을 겪고 있는 라우터나 목적지 호스트는 폐기되는 데이터그램 하나 당 Source Quench 메시지 하나를 발신지 호스트에 보내야 함
- 혼잡이 해소되었고 발신지가 데이터그램의 송신 속도를 예전의 속도로 회복할 수 있다는 것을 알리는 mechanism이 없음
  - 발신자는 더 이상의 Source Quench 메시지가 수신되지 않을 때까지 송신 속도를 낮춤
- May-to-one case에서 어느 호스트가 혼잡의 책임이 있는지를 알 수 없고 따라서 유용하지 않을 수 있음

Error Reporting

- Time exceeded
  - Whenever a router receives a datagram whose time-to-live field has the value of zero, it discards the datagram and sends a time-exceeded message to the original source
  - When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source

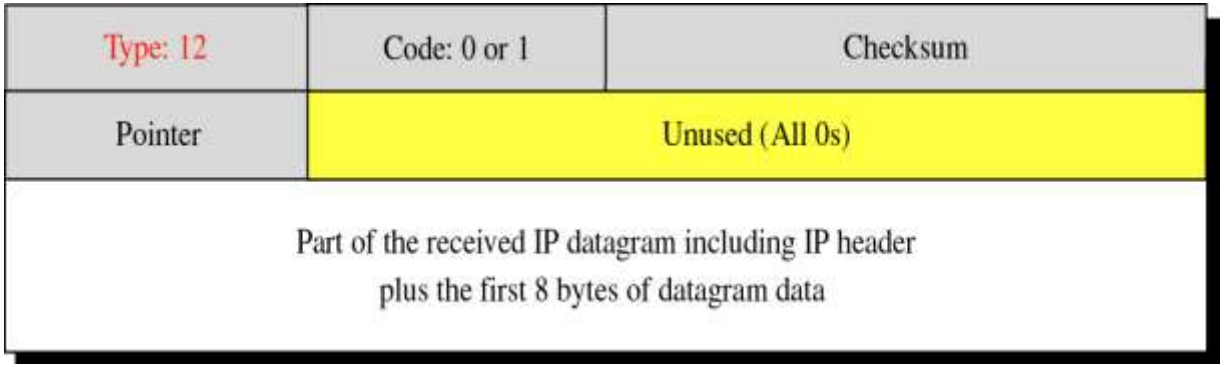
Error Reporting

- Code 0 : The value of the TTL is zero.
- Code 1 : Not all of the fragments have arrived within a set time
- Time-exceeded message format



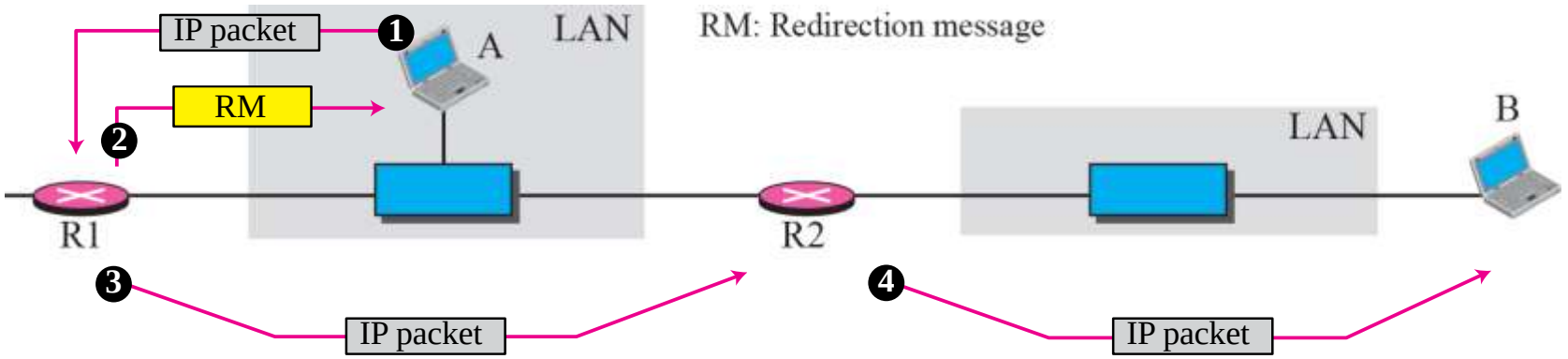
Error Reporting

- Parameter-problem
  - A parameter-problem message caused by ambiguity in the header part can created by a router or the destination host
  - Code 0 : error or ambiguity in one of the header fields
    - Pointer field points to the byte with the problem
  - Code 1 : the required part of an option is missing. In this case, pointer is not used



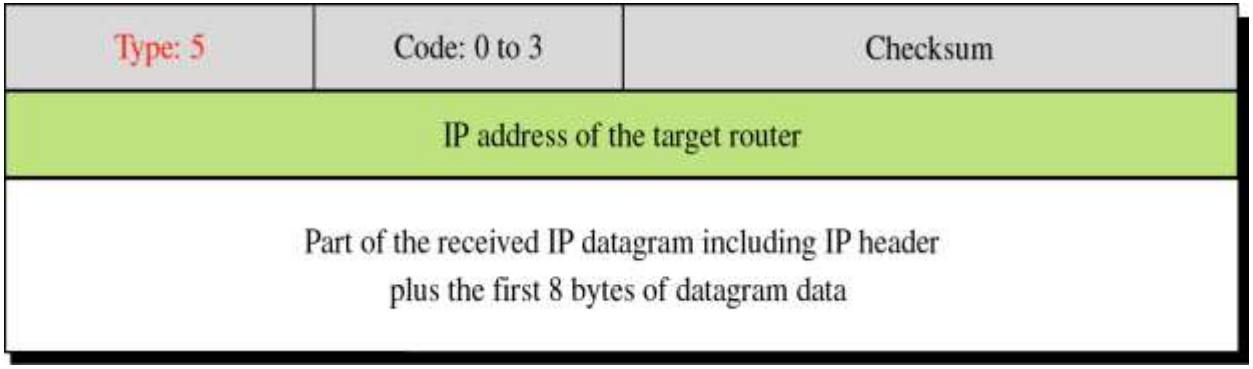
Error Reporting

- Redirection
  - 잘못된 곳으로 packet을 전송하는 호스트에게 정확한 route 를 알려주는 역할.
  - A redirection message is sent from a router to a host on the same local network.



Error Reporting

- Redirection message format



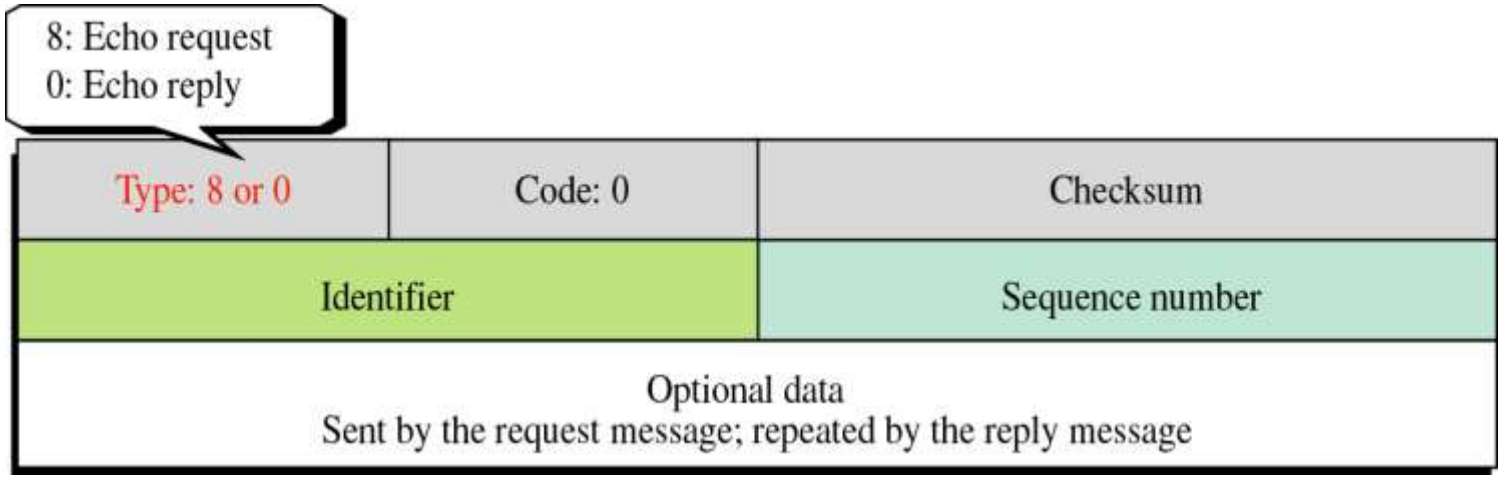
  - Code 0 : redirection for the network-specific route
  - Code 1 : redirection for the host-specific route
  - Code 2 : redirection for network-specific route based on specific type of service
  - Code 3 : redirection for the host-specific route based on the specified type of service

Query Message

- Echo Request and Reply messages
  - designed for diagnostic purpose
  - Echo-request and echo-reply message can be used by network managers to check the operation of the IP protocol
  - Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command(사용자 level)

Query Message

- The identifier field
  - ex) process ID
- The sequence number field
  - keeps track of the particular echo request messages sent

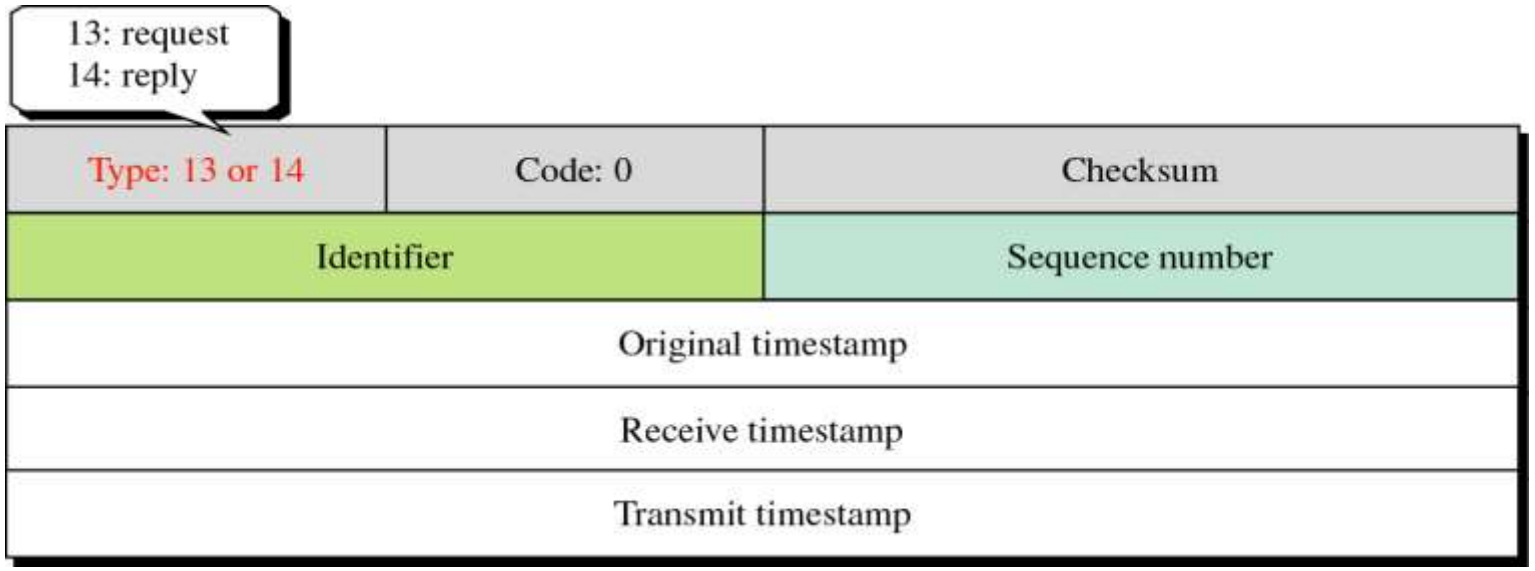


Query Message

- Timestamp Request and Reply message
  - 2 machines (routers or hosts) can use the timestamp-request and timestamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them
  - can be used to synchronize the clocks in two machines
  - Three timestamp field are each 32 bits long
    - holding a number representing time measured in milliseconds from midnight in Universal Time
      - Cannot exceed 86,400,000 = 24 x 60 x 60 x 1,000

Query Message

- Timestamp-request and reply message format



- original timestamp field : clock at departure time
- receive timestamp field : at the time the request was received
- transmit timestamp field : at the time the reply message departs

Query Message

- Round-trip time 계산
  - 양쪽 clock 이 동기가 맞지 않아도 계산가능
  - Sending time = value of receive timestamp – value of original time stamp
  - Receiving time = time the packet returned – value of transmit timestamp
  - Round-trip time = sending time + receiving time
- Example
  - Value of original timestamp : 46
  - Value of receive timestamp : 59
  - Value of transmit timestamp : 60
  - Time the packet arrived : 67

Sending time = 13 ms
Receive time = 7 ms
Round-trip time = 20 ms

Query Message

- Synchronizing clocks between two machines
  - Time difference = receive timestamp – (original timestamp field + oneway time duration)
  - Oneway time duration은 roundtrip time 의 반으로 계산 가능
  - In previous example,
    - Time difference = 59 – (46 + 10) = 3

Debugging Tools

- Ping : find if a host is alive and responding
  - Sends ICMP echo request message
  - If the destination is alive, responds with ICMP echo reply message
  - Can calculate the round trip time
    - Inserts the sending time in the data section of the message
    - Packet arrival: RTT 계산

Example 7.17

- The following shows how we send a ping message to the auniversity.edu site.

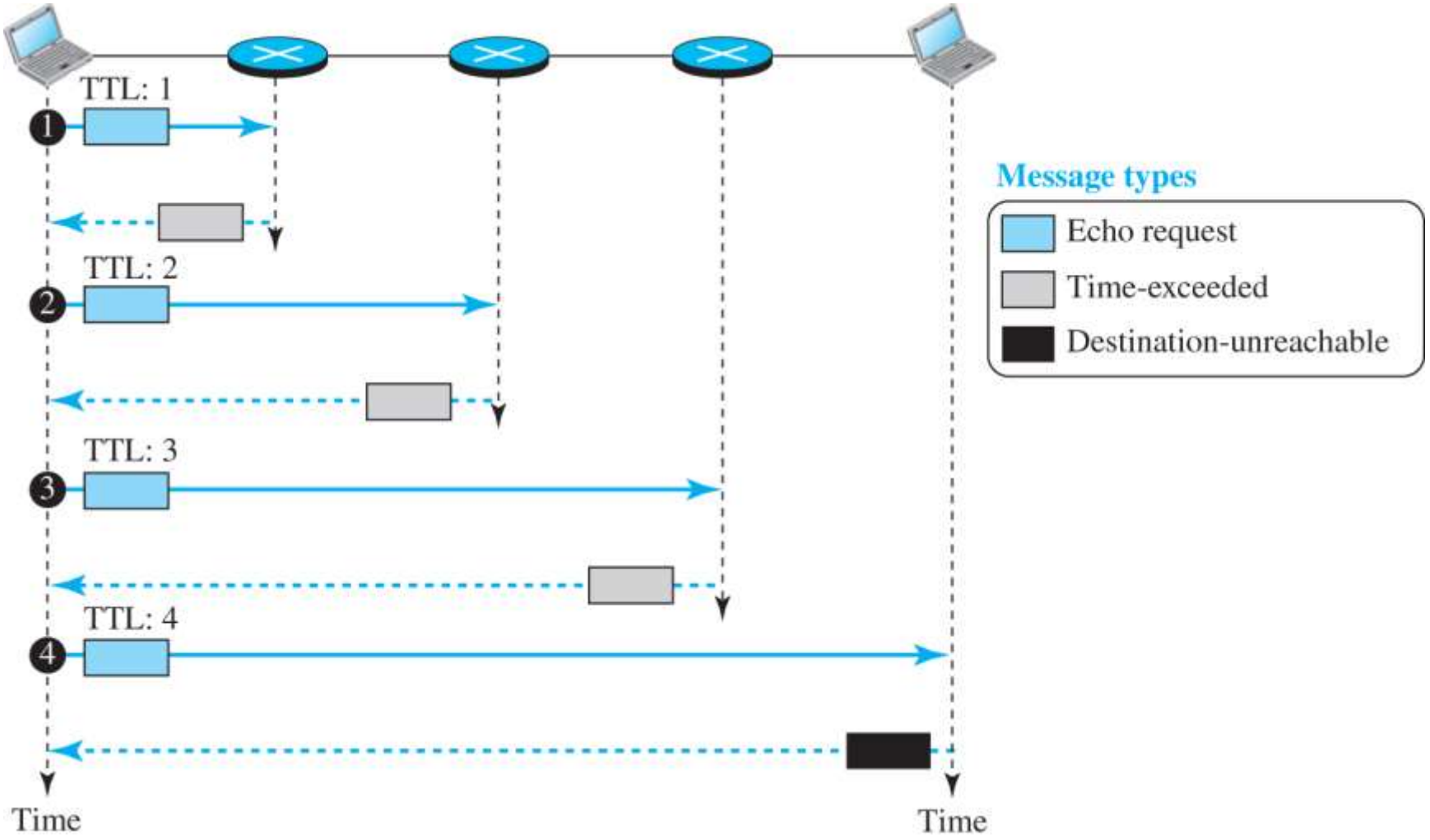
```
$ ping auniversity.edu
PING auniversity.edu (152.181.8.3) 56 (84)  bytes of data.      ttl=62    time=1.91 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=0        ttl=62    time=2.04 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=1        ttl=62    time=1.90 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=2        ttl=62    time=1.90 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=3        ttl=62    time=1.97 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=4        ttl=62    time=1.93 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=5        ttl=62    time=2.00 ms
--- auniversity.edu statistics ---
6 packets transmitted, 6 received, 0% packet loss
rtt min/avg/max = 1.90/1.95/2.04 ms
```

traceroute

- Traceroute(in UNIX) or tracert(in Windows)
  - Used to trace the route of a packet from the source to the destination
  - Uses two ICMP messages
    - Time exceeded and destination unreachable ICMP messages

```
$ traceroute fhda.edu
traceroute to fhda.edu     (153.18.8.1), 30 hops max, 38 byte packets
1 Dcore.fhda.edu           (153.18.31.25)     0.995 ms     0.899 ms     0.878 ms
2 Dbackup.fhda.edu         (153.18.251.4)     1.039 ms     1.064 ms     1.083 ms
3  tiptoe.fhda.edu         (153.18.8.1)       1.797 ms     1.642 ms     1.757 ms
```

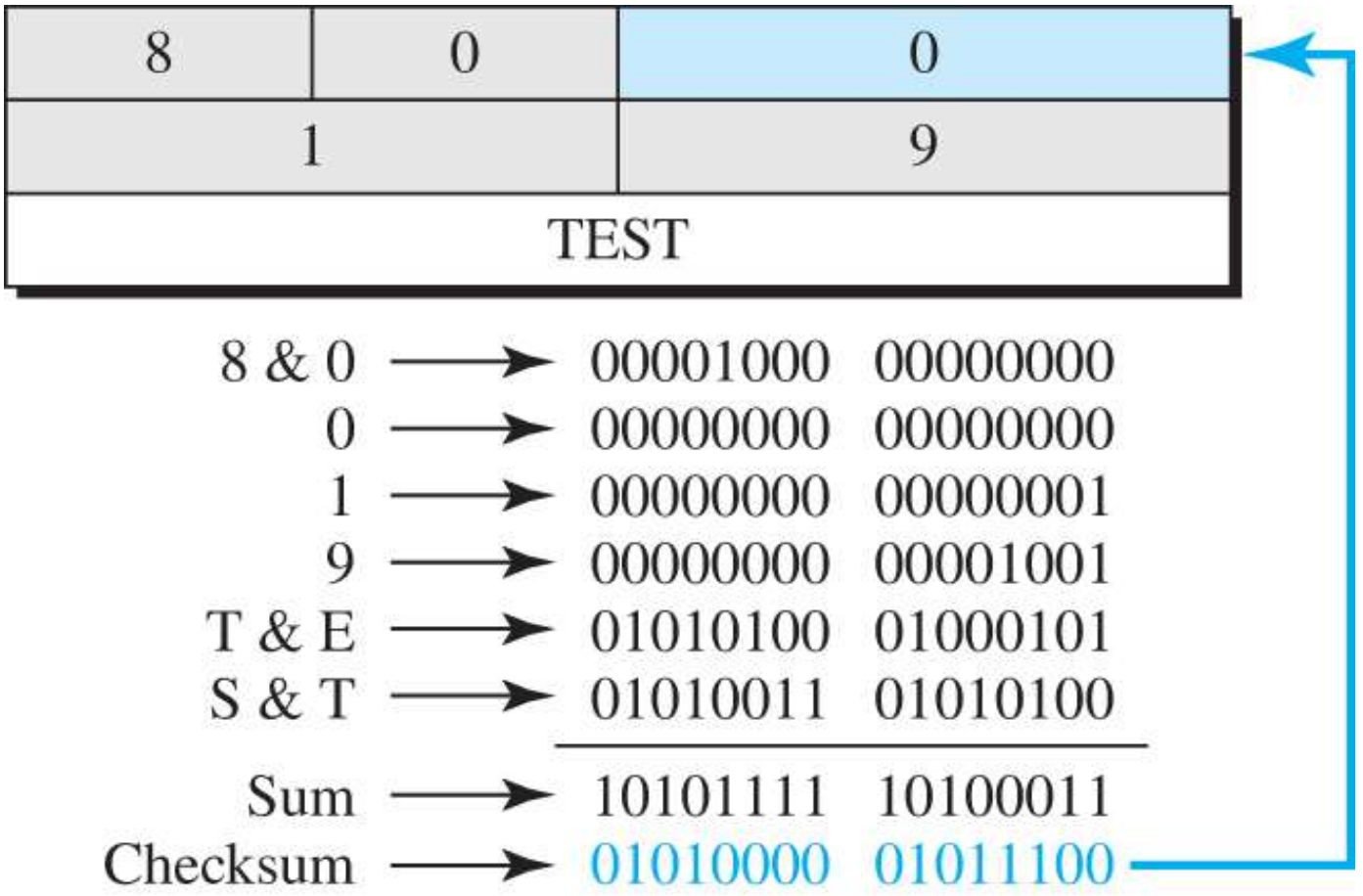
Figure 7.21 Example of traceroute program



Example 7.18

- Figure 7.22 shows an example of checksum calculation for a simple echo-request message. We randomly chose the identifier to be 1 and the sequence number to be 9. The message is divided into 16-bit (2-byte) words. The words are added and the sum is complemented. Now the sender can put this value in the checksum field.

Figure 7.22 Example of checksum calculation

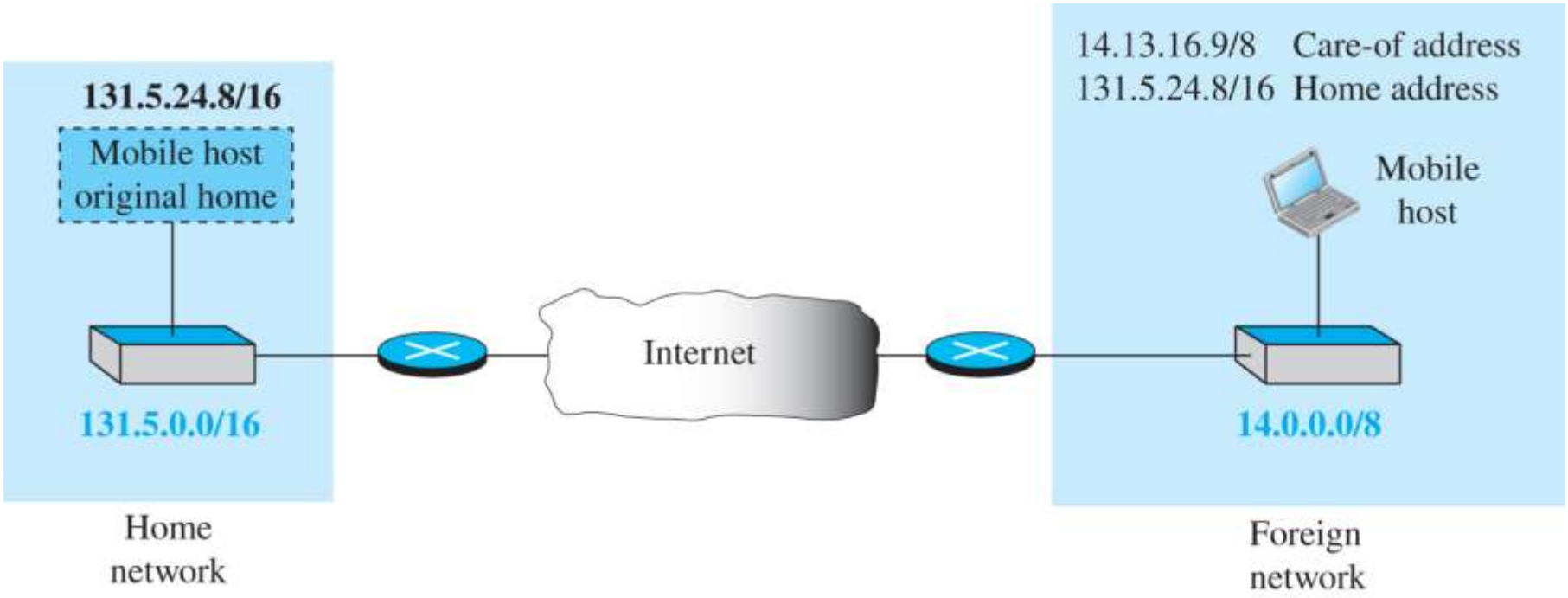


Mobile IP

- IP 주소의 구성
  - Locator + Identifier(LOC-ID colocation 구조)
  - 이동성이 없음
- Previous IP routing method
  - 기존의 IPv4는 network address-based longest prefix match방식의 routing algorithm 사용
  - Routing aggregation으로 인해 가입자의 network prefix에 근거한 routing → host-based routing의 경우 scalability 문제
  - 가입자 노드가 이동하는 경우?

    ICMP Host unreachable error message back to the source

Figure 7.23 Home address and care-of address



Mobile IP

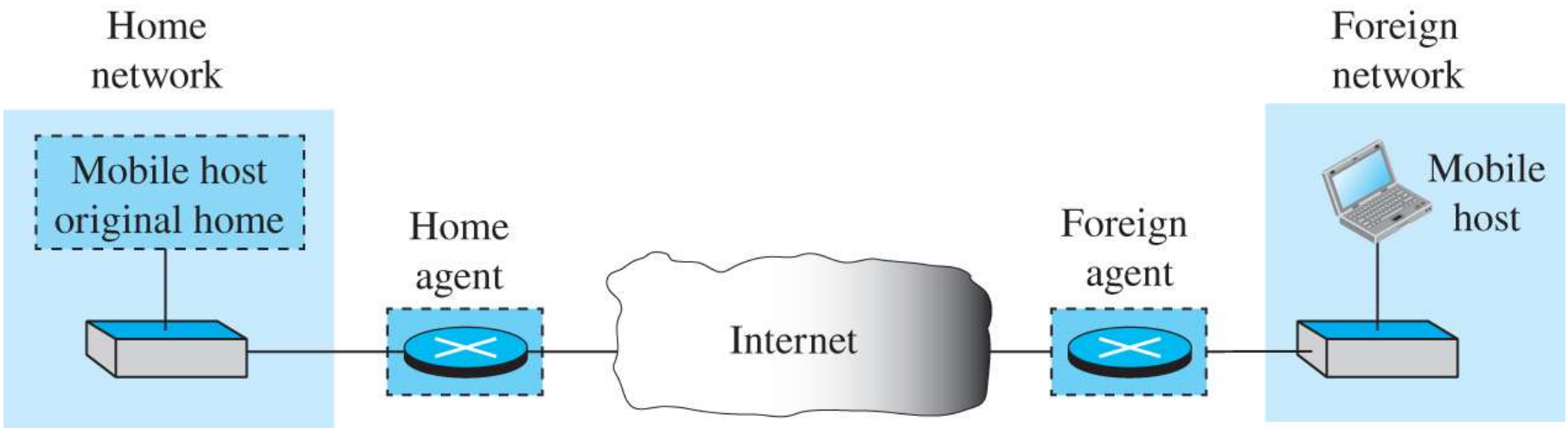
❖의탁주소(COA; Care-of address)란?

- 이동한 MN로 전송할 패킷의 도착 주소로 HA에 의해 tunneling 되는 패킷의 목적지
- Foreign Agent COA

  Agent advertisement message에 의해 FA의 주소를 획득
  MN의 COA는 FA주소와 동일
  Encapsulated datagram의 de-tunneling : FA
  MN의 현재 위치와 one-hop이내 router가 됨
- Co-located COA

  외부 네트웍에 속하는 임시적인 IP주소가 할당됨
  DHCP혹은 PPP로 할당 가능
  Encapsulated datagram의 de-tunneling : MN

Figure 7.24 Home agent and foreign agent



Mobile IP

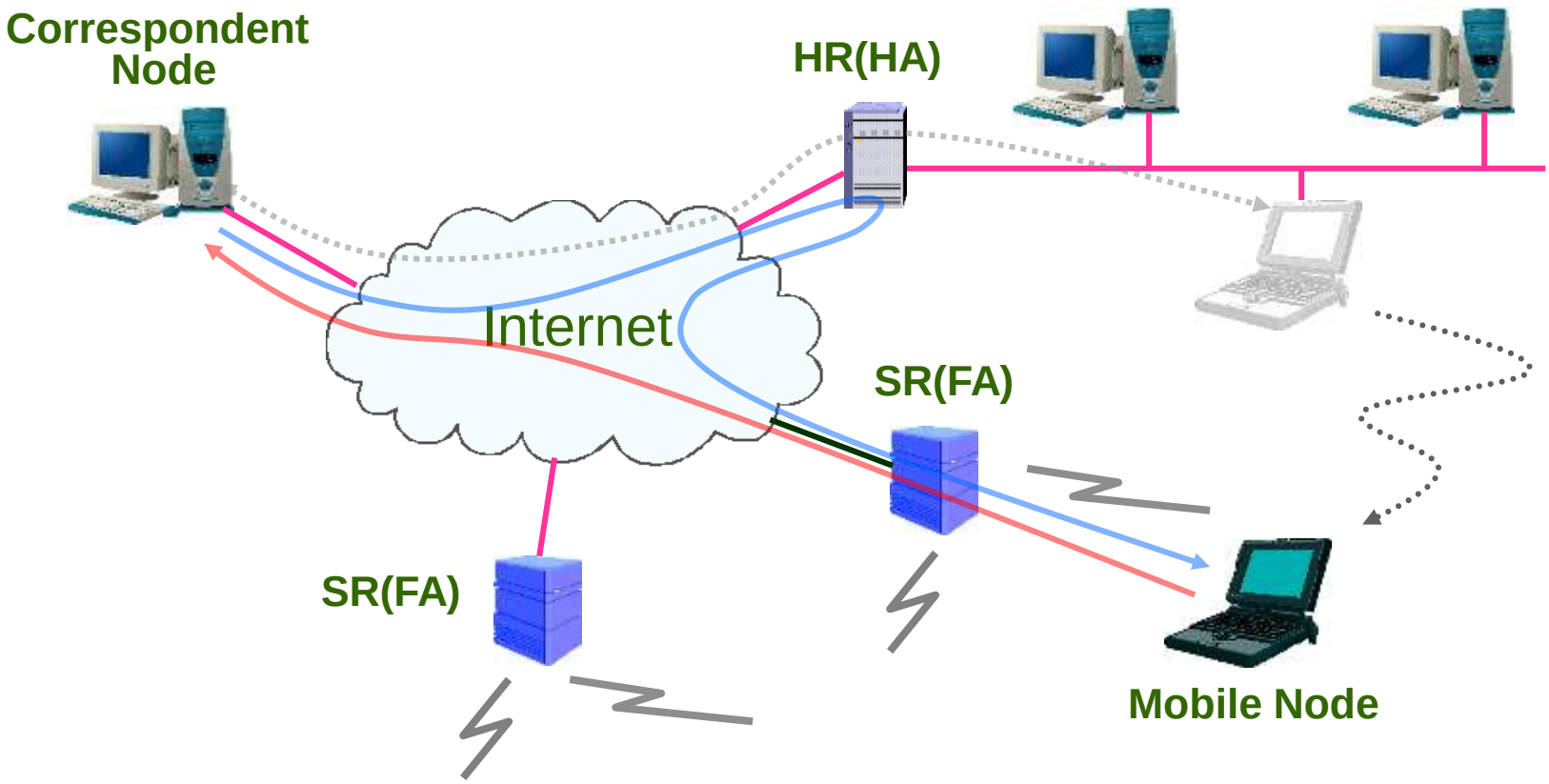
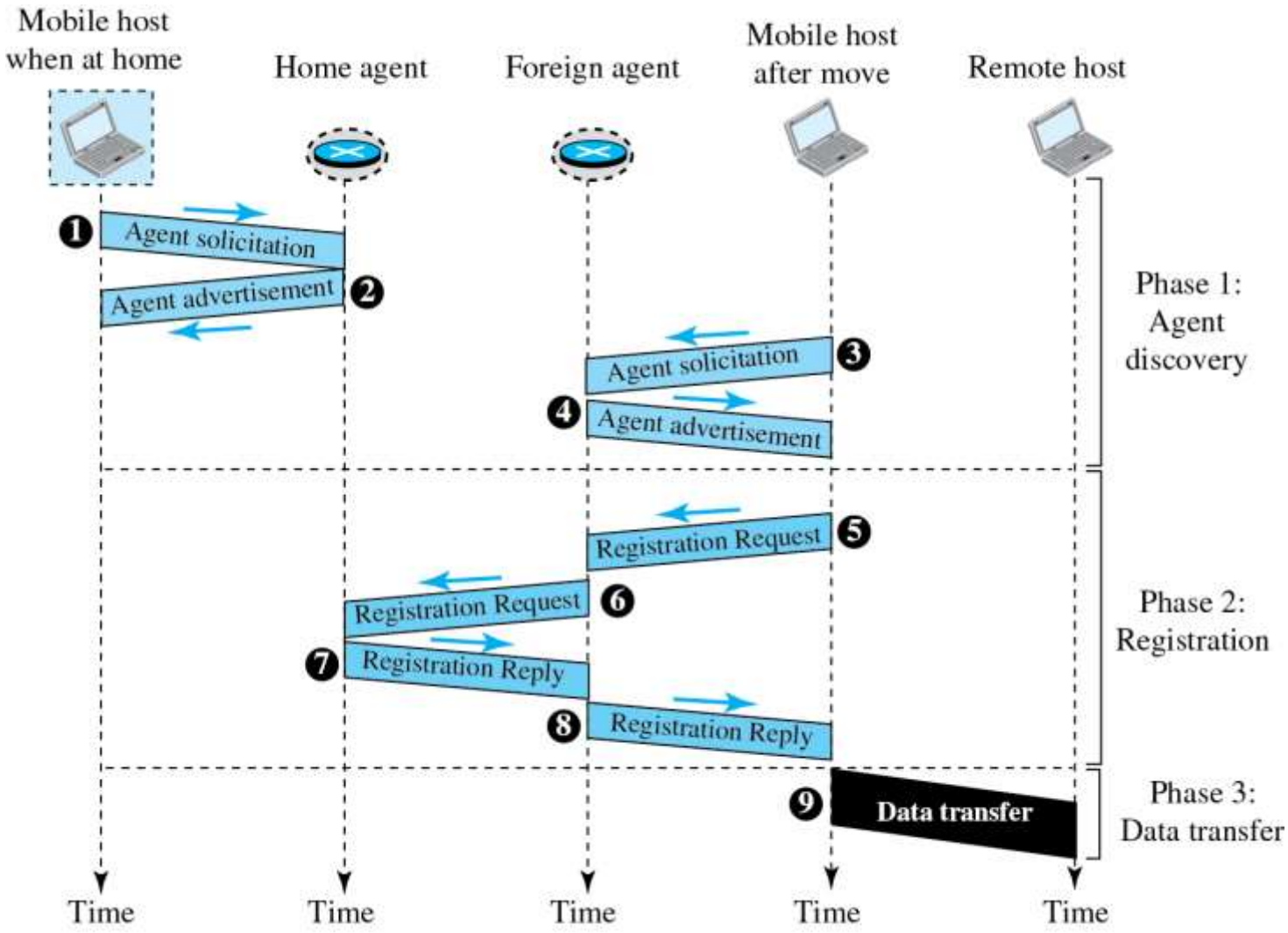


Figure 7.25 Remote host and mobile host communication



Agent Discovery

- Agent Advertisement : Agent가 MN에 자신의 capabilities를 선언
  - Periodically transmit : multicast or broadcast
  - 그 link에 연결된 노드들은 Agent의 id(IP address)와 그 capability를 결정
- Agent solicitation : MN가 Advertisement의 전송을 기다리지 않고 응답을 요청하는 경우 사용
  - Advertisement 간 주기가 너무 긴 경우 사용
- 이상의 메시지들은 key management가 어려우므로 인증되지 않고 그냥 사용되며 ICMP Router Discovery message format을 확장하여 사용

Figure 7.26 Agent advertisement

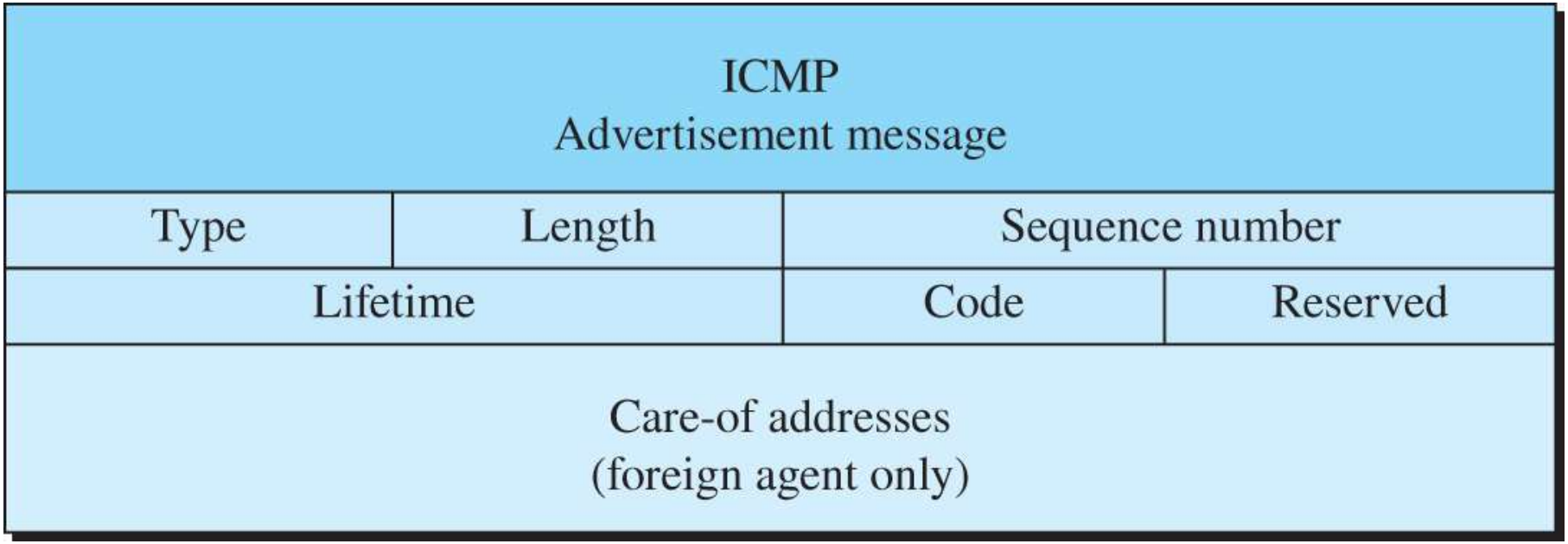


Table 7.1 Code Bits

Bit	*Meaning*
0	Registration required. No collocated care-of address.
1	Agent is busy and does not accept registration at this mo ment.
2	Agent acts as a home agent.
3	Agent acts as a foreign agent.
4	Agent uses minimal encapsulation.
5	Agent uses generic routing encapsulation (GRE).
6	Agent uses generic routing encapsulation (GRE).
7	Unused (0).

Registration

- The second phase in mobile communication is registration. After a mobile host has moved to a foreign network and discovered the foreign agent, it must register. There are four aspects of registration:

1. The mobile host must register itself with the foreign agent.
2. The mobile host must register itself with its home agent.
3. The mobile host must renew registration if it has expired.
4. The mobile host must cancel its registration when it returns.

Registration

❖등록을 하면 HA와 FA에는 어떤 영향?

- HA의 경우 이동성 바인딩 리스트(mobility binding list) 생성 및 갱신

  Binding : MN의 home address와 현재 COA를 mapping하는 table
  →등록이란 이 table의 binding entry를 생성, 변경, 삭제하는 것
  Binding entry는 제한된 시간 동안만 유지(등록 lifetime) → 재 등록 필요
- FA에 이동 단말에 대한 visiting MN list 갱신

❖언제 registration을 수행?

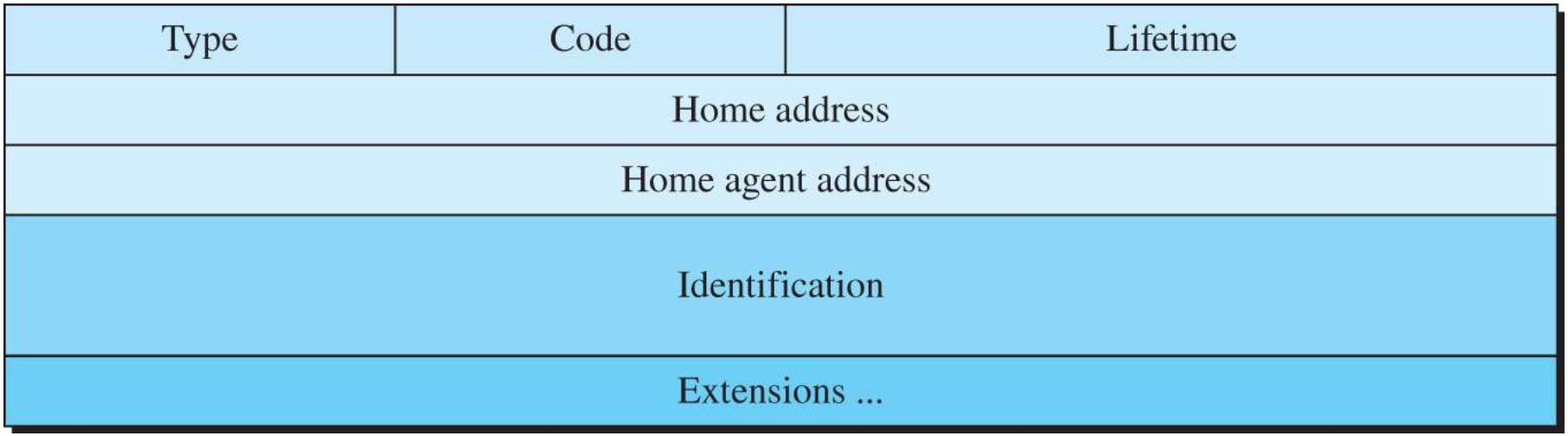
- Link 를 이동했다고 단말이 판단하는 경우
- FA가 reboot 되었다고 판단하는 경우
- 현재 binding이 expire되려고 하는 경우

Figure 7.27 Registration request format

Table 7.2 Registration request flag field bits

Bit	*Meaning*
0	Mobile host requests that home agent retain its prior care-of address.
1	Mobile host requests that home agent tunnel any broadcast message.
2	Mobile host is using collocated care-of address.
3	Mobile host requests that home agent use minimal encapsulation.
4	Mobile host requests generic routing encapsulation (GRE).
5	Mobile host requests header compression.
6 –7	Reserved bits.

Figure 7.28 Registration reply format



Data Transfer

❖HA에서의 packet intercept 과정

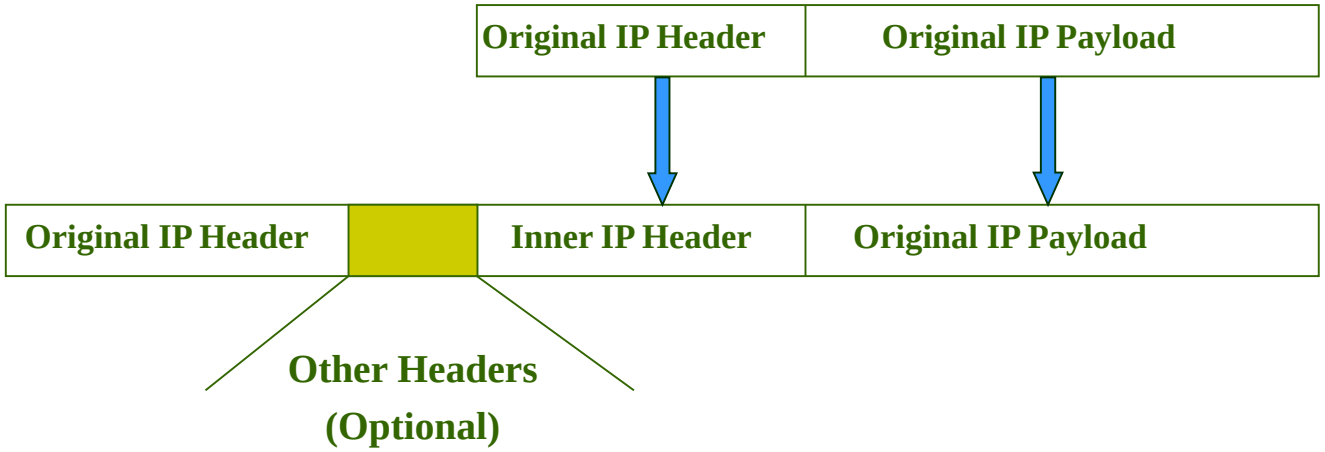
- MN의 home address로의 reachability를 advertise

  Gratuitous and proxy ARPs
- Home link의 사용자가 address resolution을 위해 ARP request 전송하며 HA가 ARP Reply를 답장

  HA의 link-layer address를 MN의 IP 주소에 해당하는 값으로 설정
- ARP cache에 있는 기존 내용을 update하기 위해 gratuitous ARP 전송
- 이동 단말이 home에 오면 ARP cache update → gratuitous ARP 및 proxy ARP 기능 중지

Mobile IP

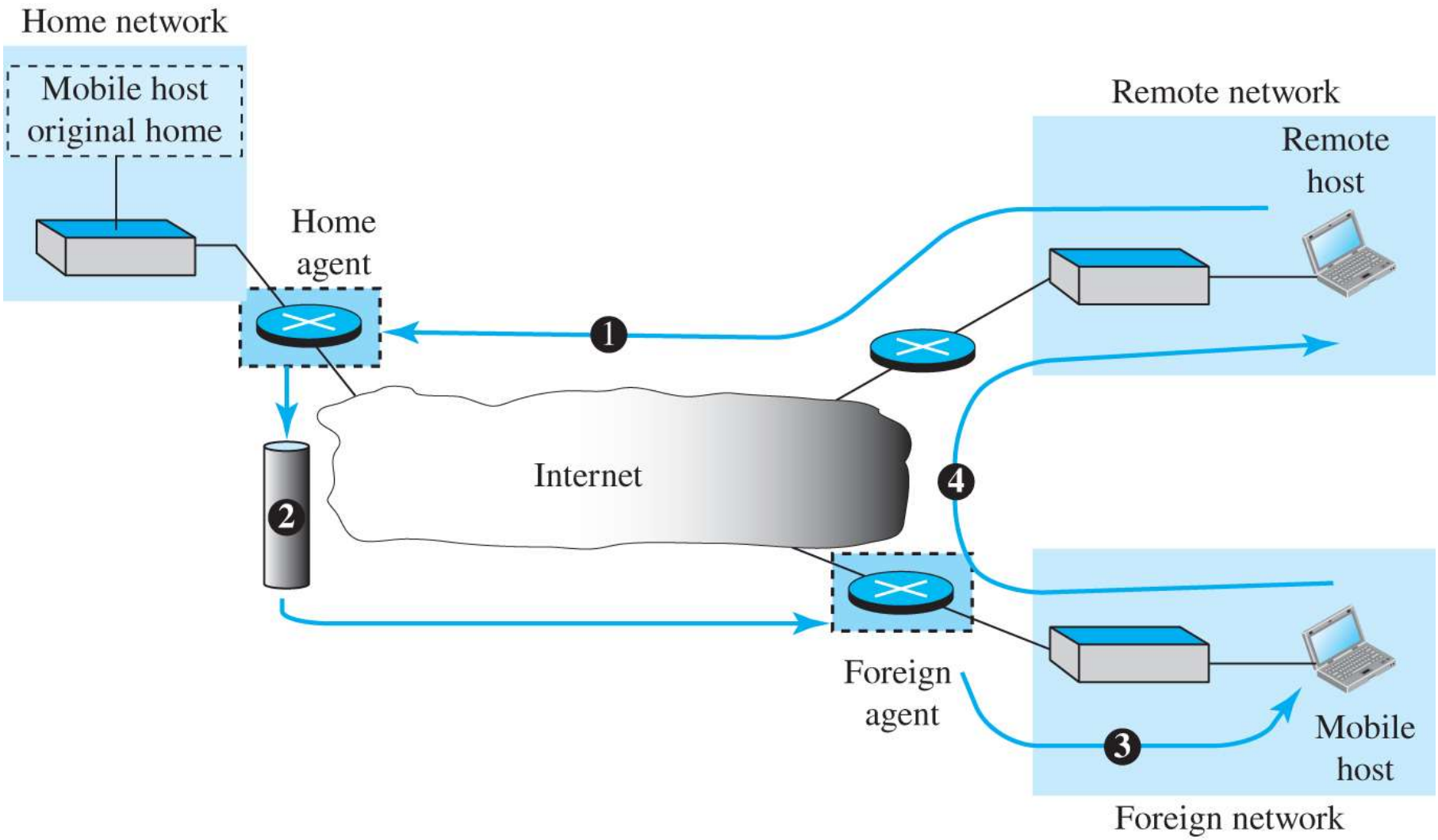
❖IP in IP encapsulation(Tunneling): 기본적인 캡슐화 방법



- 20바이트의 외부 헤더 추가
- 외부 IP헤더의 근원지 주소와 목적지 주소

  터널의 종단점(FA-COA or CCOA)

Figure 7.29 Data transfer



Reverse Tunneling

- Mobile IP assumed that IP is routed based on the destination address, not by source address
- Because of security concerns, routers that break this assumption are increasingly more common
- In the presence of such routers, the source and destination IP address in a packet must be topologically correct

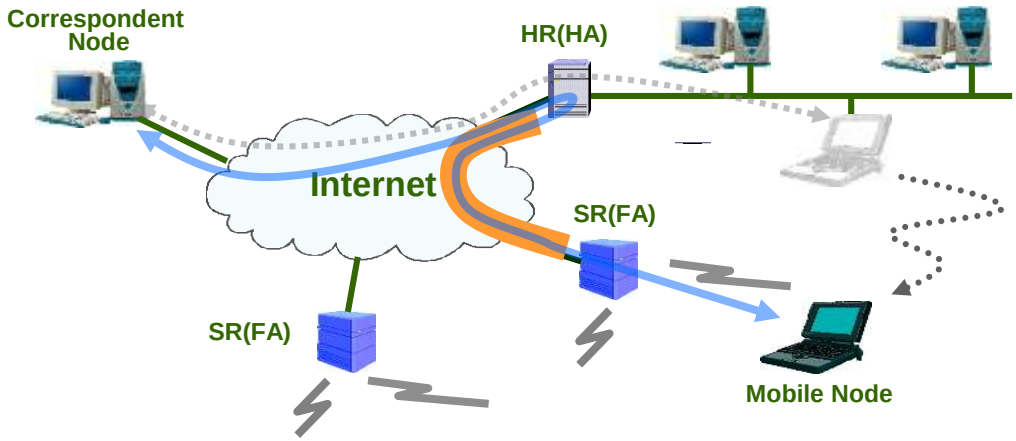


Figure 7.30 Double crossing

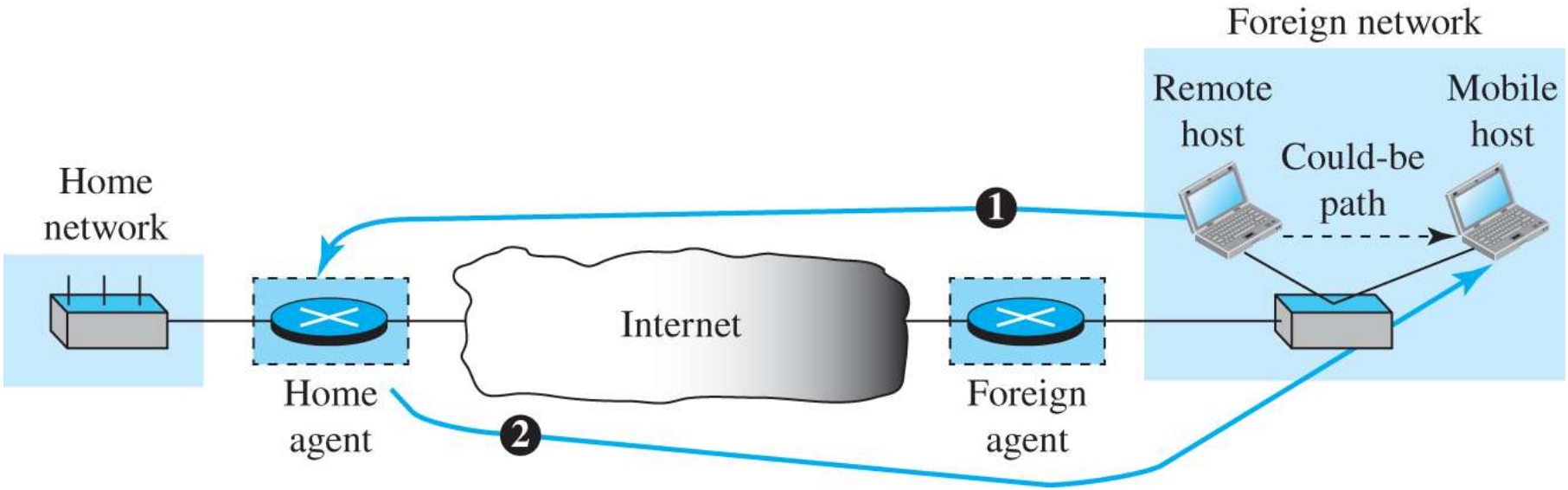
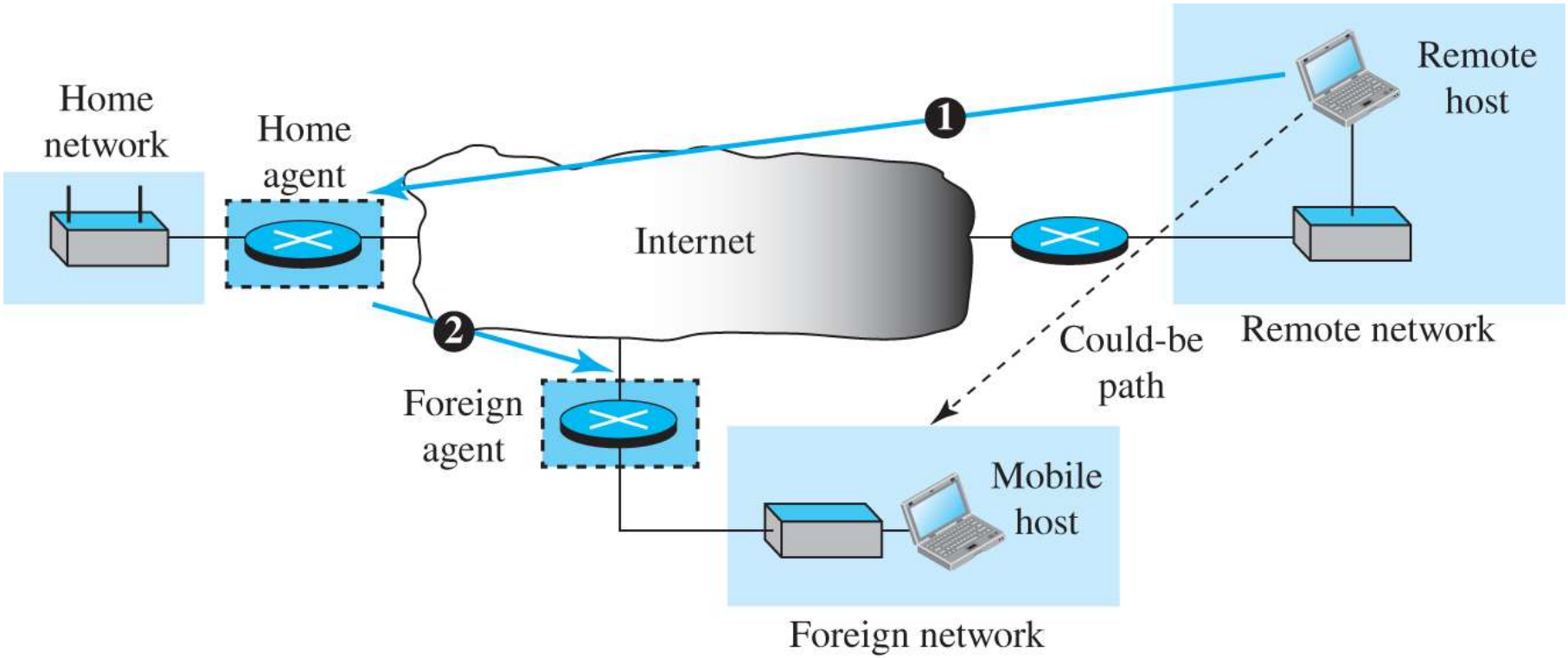


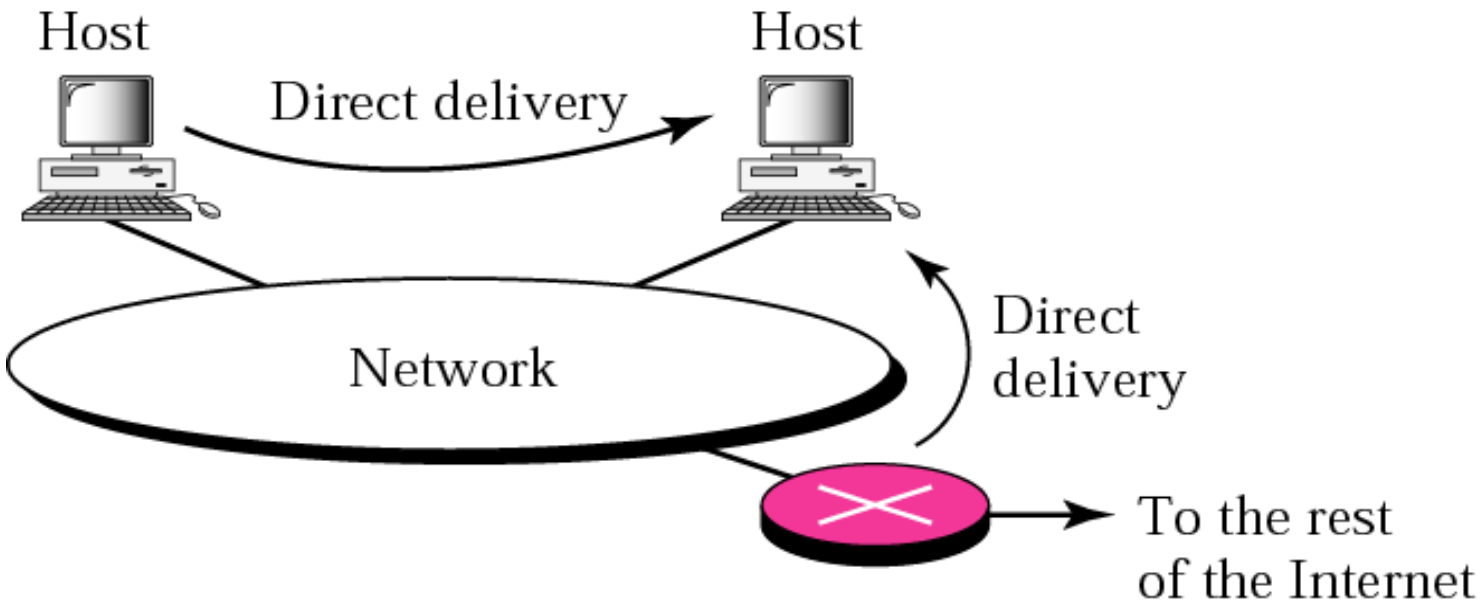
Figure 7.31 Triangle routing



Delivery

- Two methods delivering a packet to its final destination
  - Direct delivery
  - Indirect delivery
  - Decision making whether delivery is direct or not
    - Extracting the network address of the destination packet (setting the hostid part to all 0s)
    - Then, comparing the addresses of the network to which it is connected
- Direct delivery
  - The final destination of the packet is a host to the same physical network as the deliverer
  - or the delivery is between the last router and the destination host
  - 목적지 주소로부터 물리주소(physical address) 결정

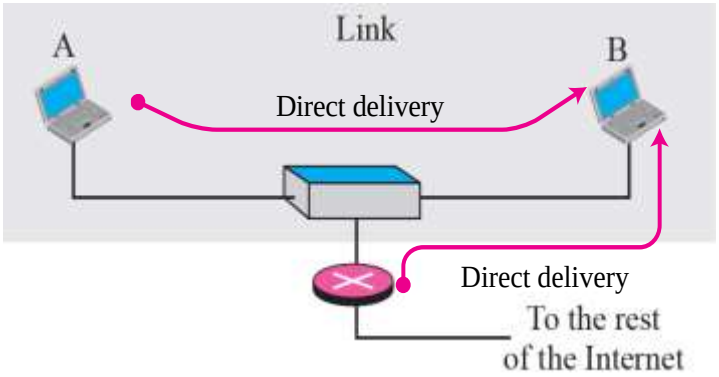
Direct Delivery

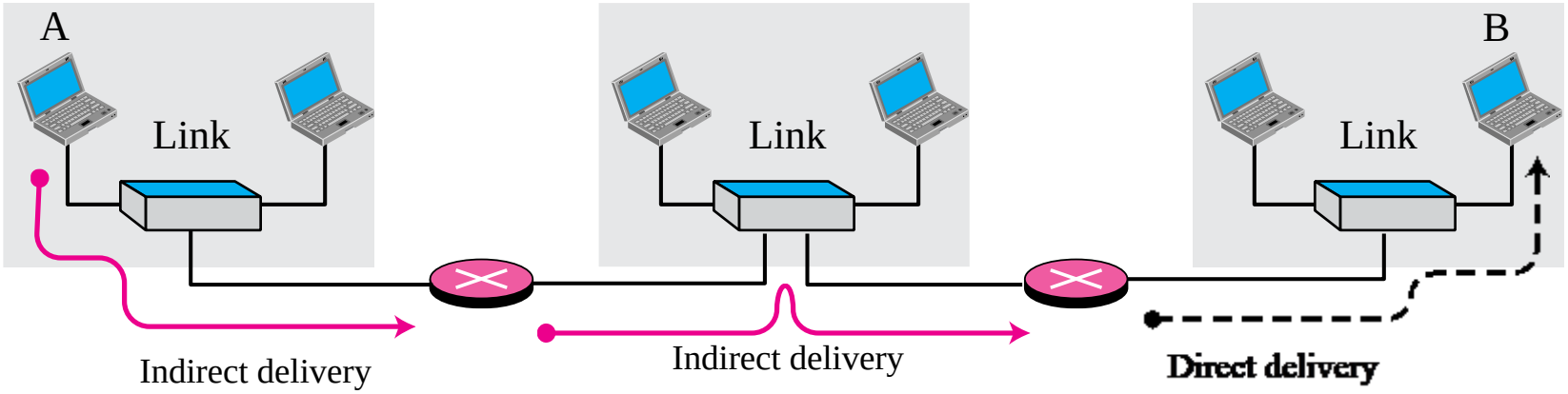


Indirect Delivery

- Indirect delivery
  - The destination host is not on the same network as the deliverer
  - The packet goes from router to router until finding the final destination
  - Using ARP to find the next physical address
    - Mapping between the IP address of next router and the physical address of the next router

Indirect Delivery





Forwarding of IP Packets

- Next-Hop Method
  - Can reduce the contents of a routing table
  - Holds only the address of the next hop instead of information about the complete route

Routing table for host A

Destination	Route
Host B	R1, R2, Host B

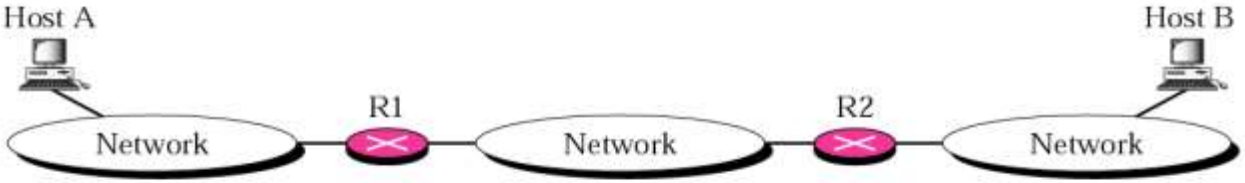
Routing table for R1

Destination	Route
Host B	R2, Host B

Routing table for R2

Destination	Route
Host B	Host B

a. Routing tables based on route



Routing table for host A

Destination	Next Hop
Host B	R1

Routing table for R1

Destination	Next Hop
Host B	R2

Routing table for R2

Destination	Next Hop
Host B	Ñ

b. Routing tables based on next hop

Forwarding of IP Packets

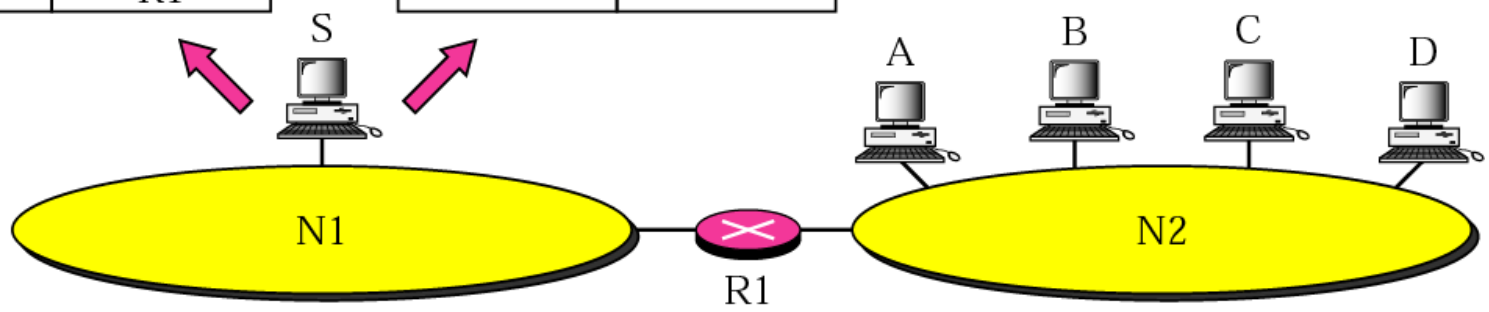
- Network-Specific Routing
  - Having only one entry to define the address of network itself

Routing table for host S based on host-specific routing

Destination	Next Hop
A	R1
B	R1
C	R1
D	R1

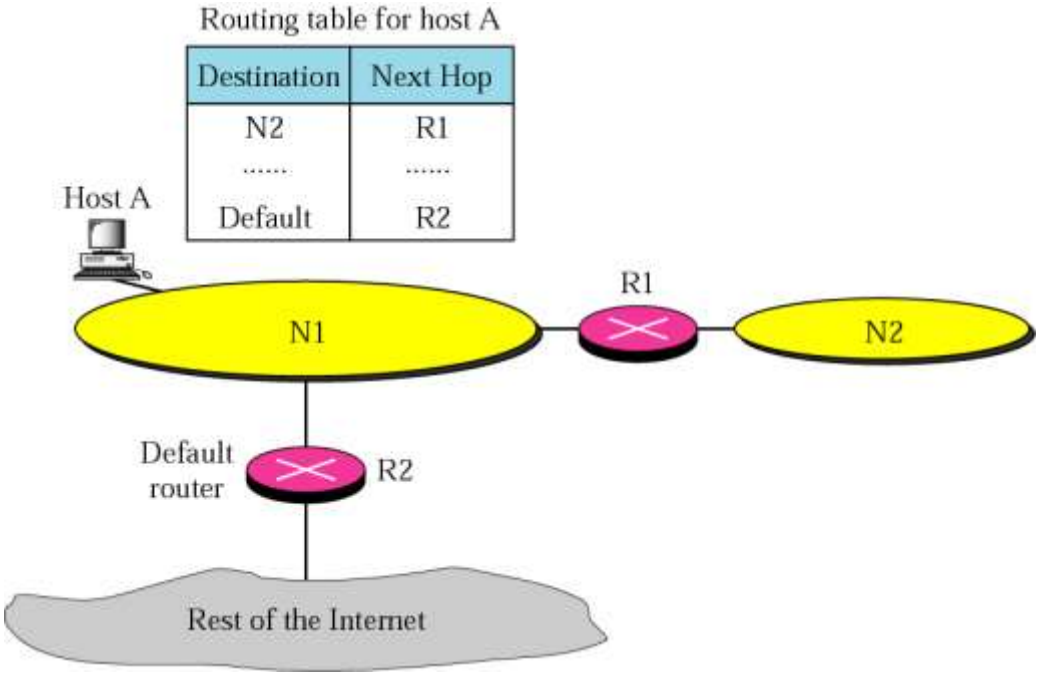
Routing table for host S based on network-specific routing

Destination	Next Hop
N2	R1



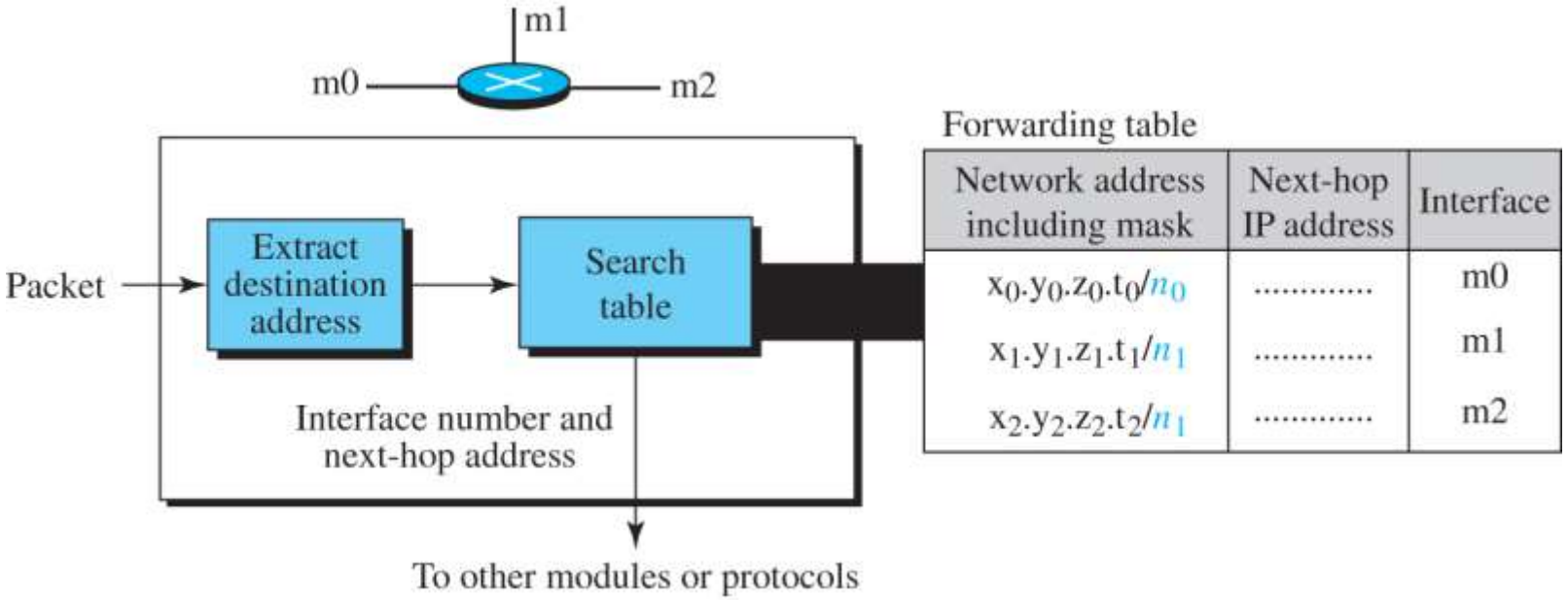
Forwarding of IP Packets

- Default routing
  - Instead of listing all networks in the entire Internet, a host just one entry called the default (network address & mask 0.0.0.0)



Forwarding with Classless Addressing

- Whole address spacing is one entity: there are no classes
- Destination address in the packet gives no clue about the network address
  - Need to include the mask(/n) in the table



Example 7.19

- Make a forwarding table for router R1 using the configuration in Figure 7.33.

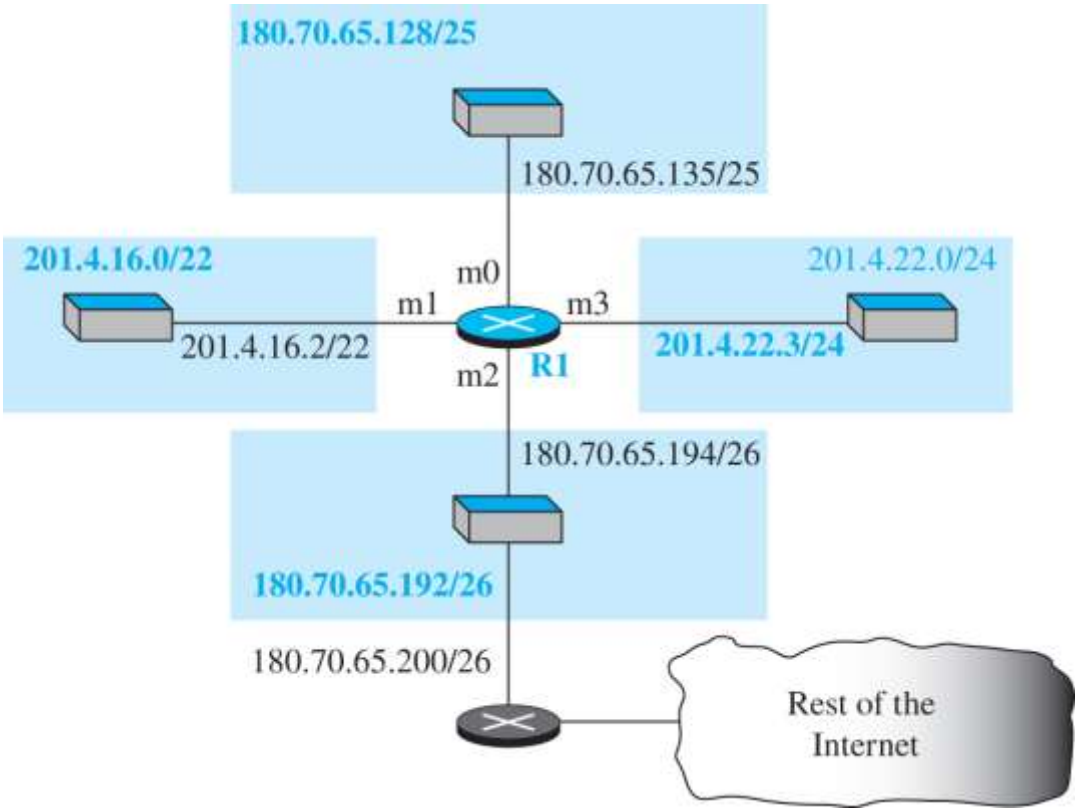


Table 7.3 Forwarding table for router R1

Network address/mask	Next hop	Interface
180.70.65.192/**26**	—	m2
180.70.65.128/**25**	—	m0
201.4.22.0/**24**	—	m3
201.4.16.0/**22**	—	m1
Default	180.70.65.200	m2

Example 7.20

- Instead of Table 7.3, we can use Table 7.4, in which the network address/mask is given in bits.

Leftmost bits in the destination address	*Next hop*	*Interface*
10110100 01000110 01000001 11	—	m2
10110100 01000110 01000001 1	—	m0
11001001 00000100 00011100	—	m3
11001001 00000100 000100	—	m1
Default	180.70.65.200	m2

Example 7.21

- Show the forwarding process if a packet arrives at R1 with the destination address 180.70.65.140.
- The router performs the following steps

1. The first mask (/26) is applied to the destination address. The result is 180.70.65.128, which does not match the corresponding network address.

2. The second mask (/25) is applied to the destination address. The result is 180.70.65.128, which matches the corresponding network address. The next-hop address and the interface number m0 are extracted for forwarding the packet.

Do it Yourself!!

- Show the forwarding process if a packet arrives at R1 with the destination address 201.4.22.35

- Show the forwarding process if a packet arrives at R1 with the destination address 18.24.32.78

Do it Yourself!!

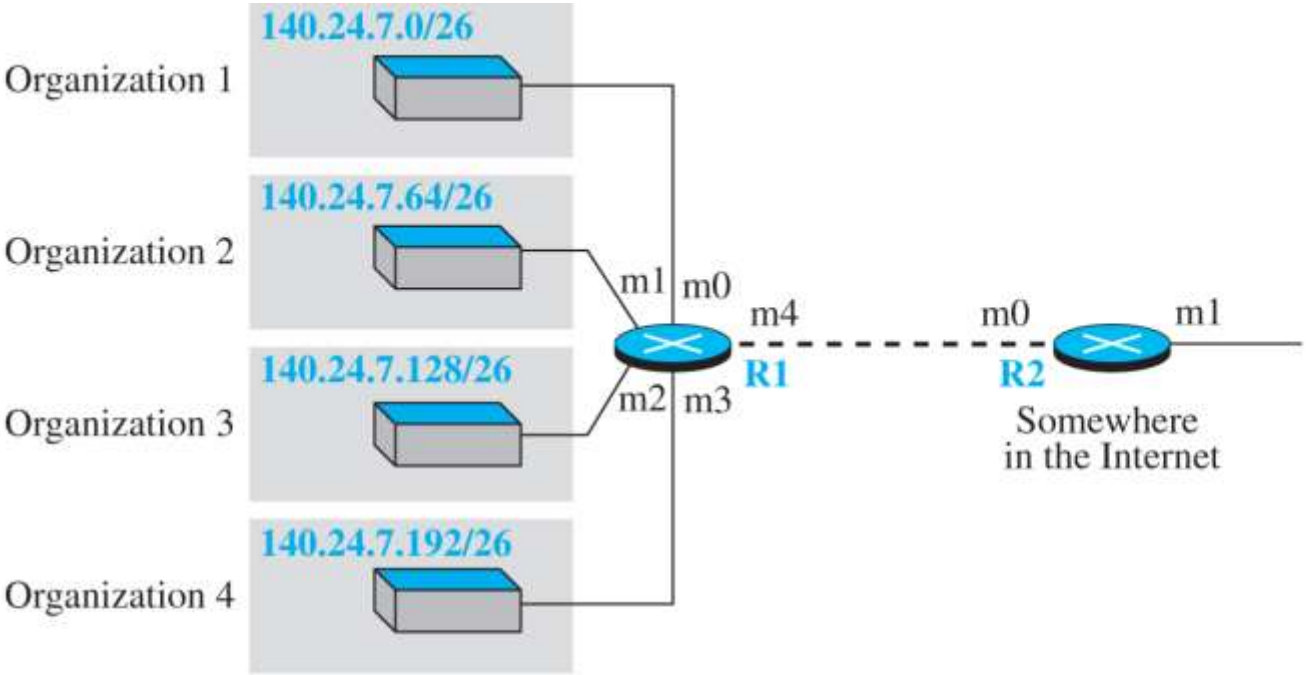
- Now let us give a different type of example. Can we find the configuration of a router if we know only its routing table? The routing table for router R1 is given in Table. Can we draw its topology?

Mask	*Network Address*	*Next-Hop Address*	*Interface Number*
/26	140.6.12.64	180.14.2.5	m2
/24	130.4.8.0	190.17.6.2	m1
/16	110.70.0.0	----------	m0
/16	180.14.0.0	----------	m2
/16	190.17.0.0	----------	m1
Default	Default	110.70.4.6	m0

Address Aggregation

- Classless addressing
  - Number of routing table entries will increase
  - The increased size of the table results in an increase in the amount of time needed to search the table
  - Address aggregation 개념 도입이 필요

Figure 7.34 Address aggregation



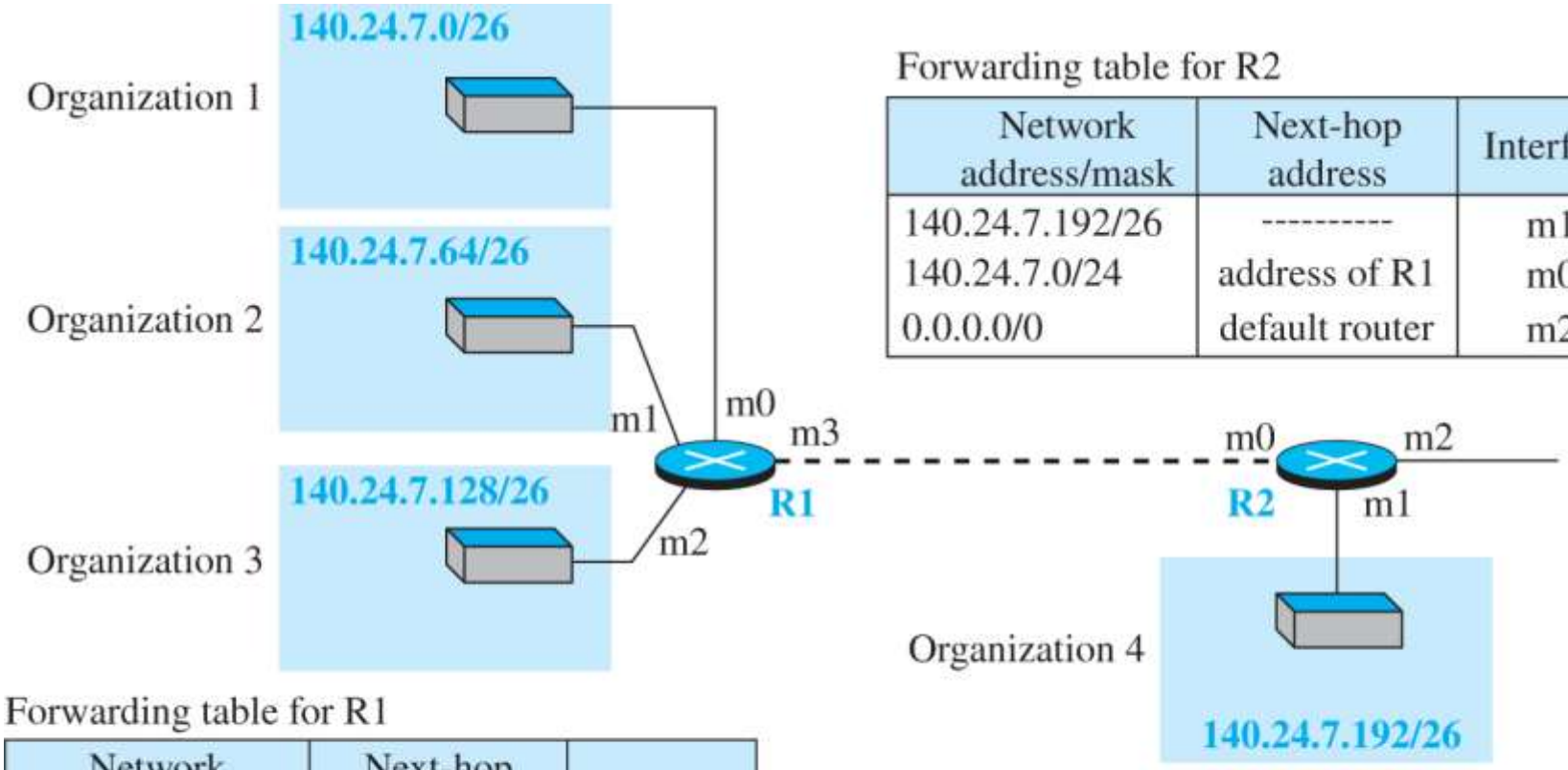
Forwarding table for R1

Network address/mask	Next-hop address	Interface
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
140.24.7.192/26	----------	m3
0.0.0.0/0	address of R2	m4

Forwarding table for R2

Network address/mask	Next-hop address	Interface
140.24.7.0/24	----------	m0
0.0.0.0/0	default router	m1

Figure 7.35 Longest mask addressing



Forwarding table for R2

Network address/mask	Next-hop address	Interface
140.24.7.192/26	----------	m1
140.24.7.0/24	address of R1	m0
0.0.0.0/0	default router	m2

Forwarding table for R1

Network address/mask	Next-hop address	Interface
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
0.0.0.0/0	default router	m3

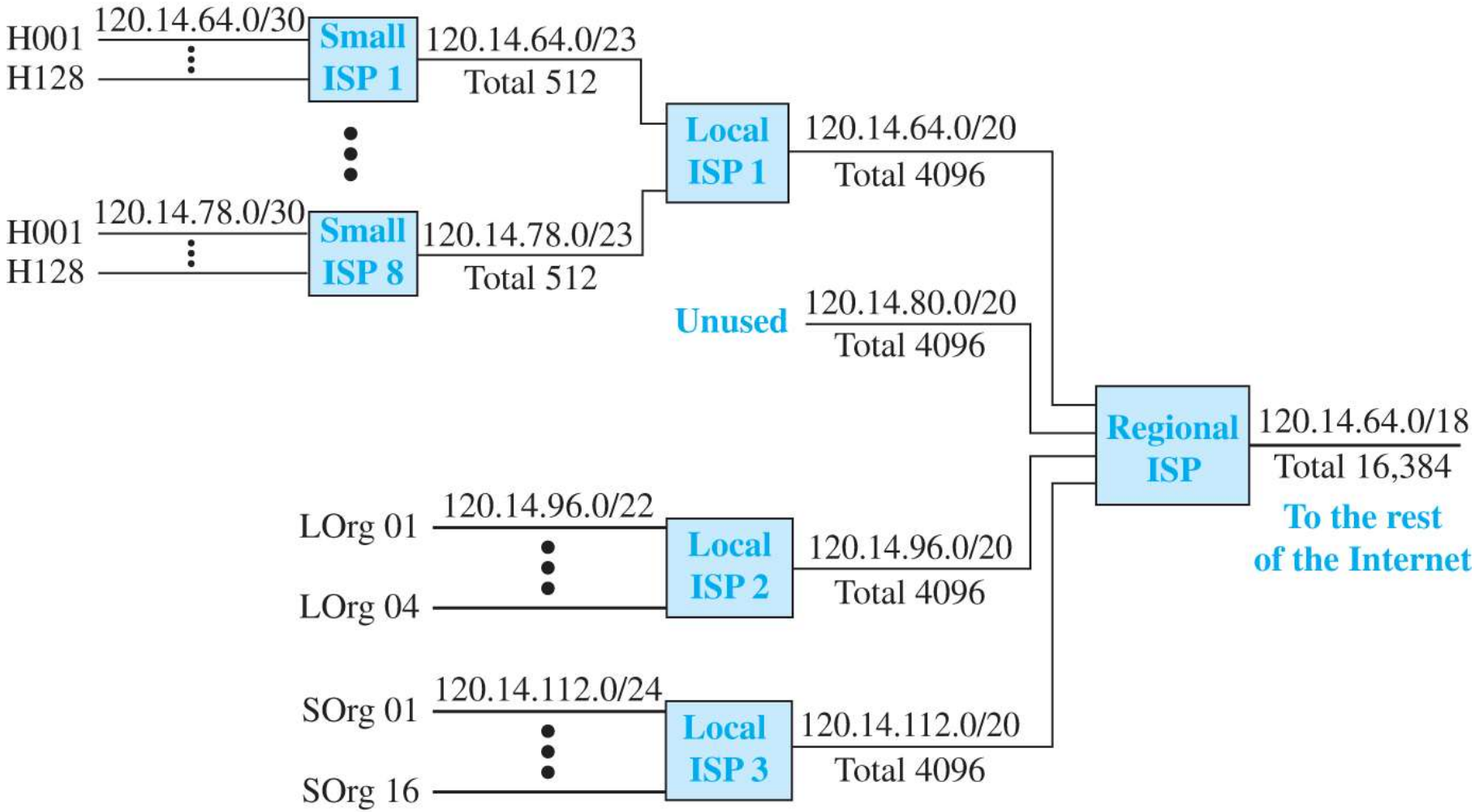
Hierarchical Routing

- To solve the problem of gigantic routing tables, we can create a sense of hierarchy in the routing table
- Today Internet 망 구조
  - International ISP, national ISP, regional ISP, …..
  - Routing table도 이와 같이 계층 구조를 가지면 routing table 크기를 줄일 수 있음
- Local ISP가 할당 받아 나눈 주소의 상세한 상황을 외부 망에서 알 필요 없이 모두 regional ISP로 전달하면 그 내부에서 상세 라우팅 수행

Example 7.22

- As an example of hierarchical routing, let us consider . A regional ISP is granted 16,384 addresses starting from 120.14.64.0
- The regional ISP has decided to divide this block into 4 subblocks, each with 4096 addresses
- Three of these subblocks are assigned to three local ISPs, the second subblock is reserved for future use
- Note that the mask for each block is /20 because the original block with mask /18 is divided into 4 blocks.

Figure 7.36 Hierarchical routing with ISPs



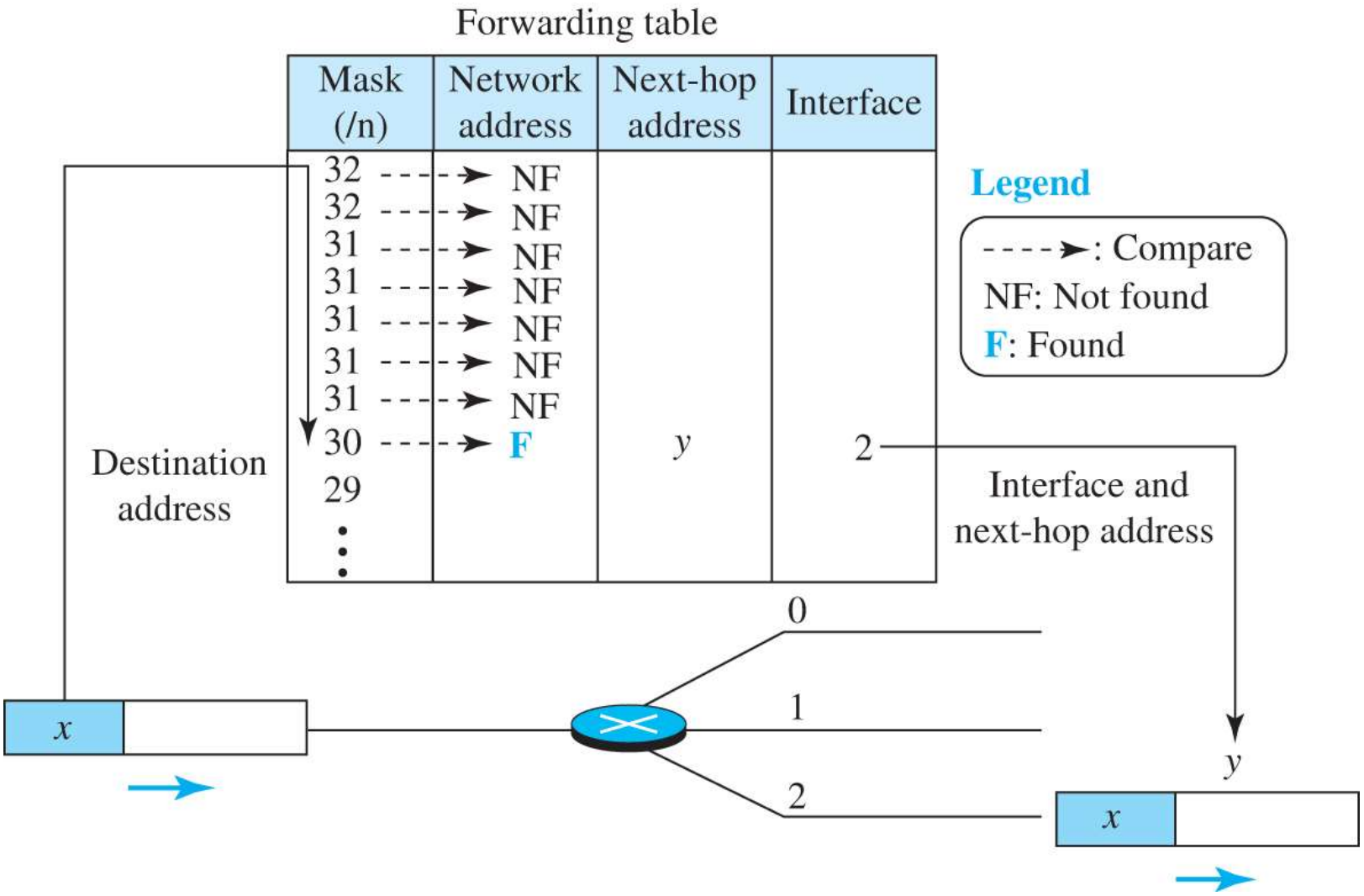
Forwarding Table Search Algorithm

- The simplest, but not the most efficient, search method is called the longest prefix match
- The forwarding table can be divided into buckets, one for each prefix
  - The router first tries the longest prefix. If the destination address is found in this bucket, the search is complete
  - If the address is not found, the next prefix is searched, and so on
- It is obvious that this type of search takes a long time.

Example 7.23

- Figure 7.37 shows a simple example of searching in a forwarding table using the longest mask algorithm. Although there are some more efficient algorithms today, the principle is the same.

Figure 7.37 Example 7.23



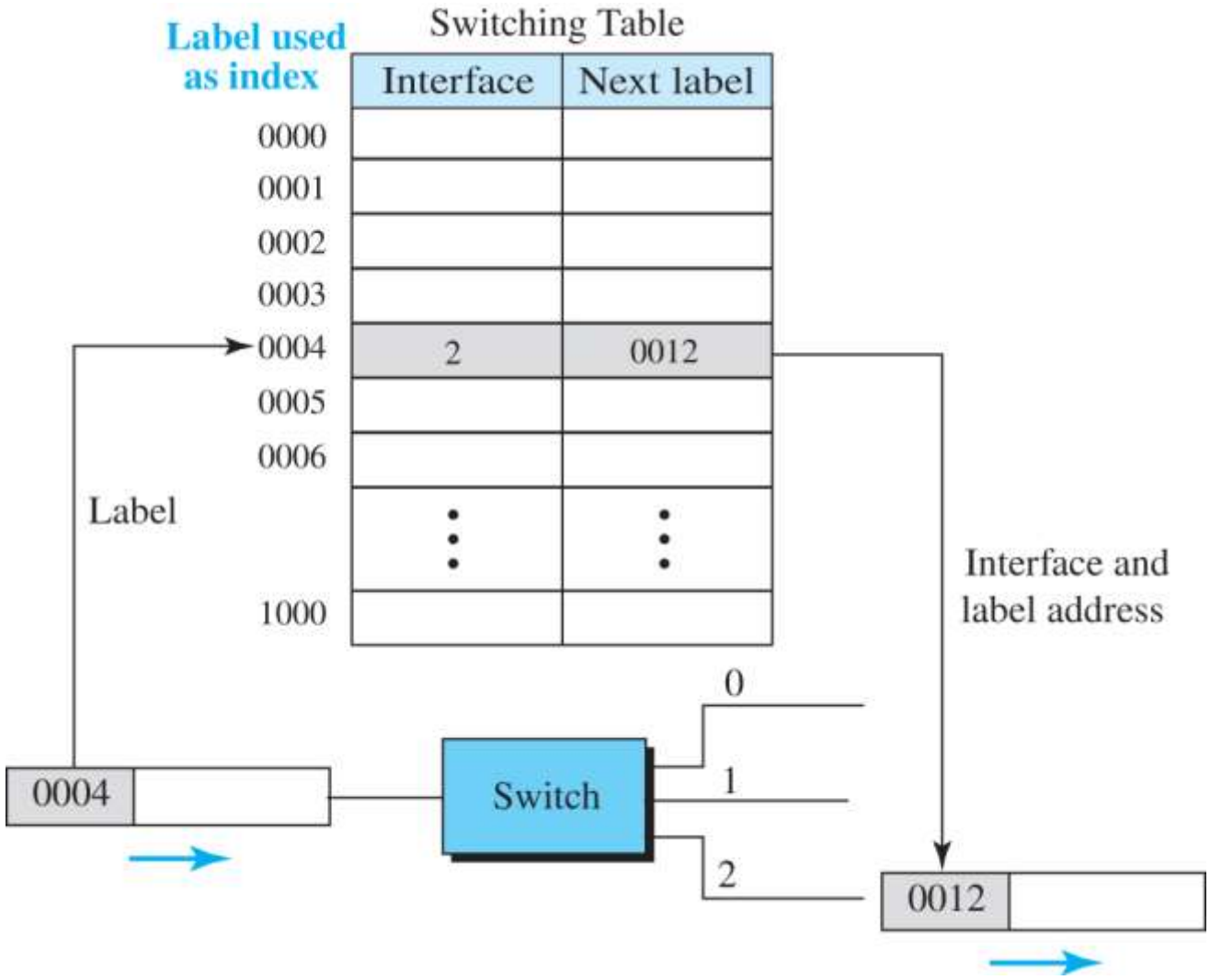
Forwarding Based on Label

- In the 1980s, an effort started to somehow change IP to behave like a connection-oriented protocol in which the routing is replaced by switching
- In a connection-oriented network (virtual-circuit approach), a switch forwards a packet based on the label attached to the packet
  - Routing is normally based on searching the contents of a table; switching can be done by accessing a table using an index
- **In other words, routing involves searching; switching involves accessing.**

Example 7.24

- Figure 7.38 shows a simple example of using a label to access a switching table. Since the labels are used as the index to the table, finding the information in the table is immediate.

Figure 7.38 Example 7.24

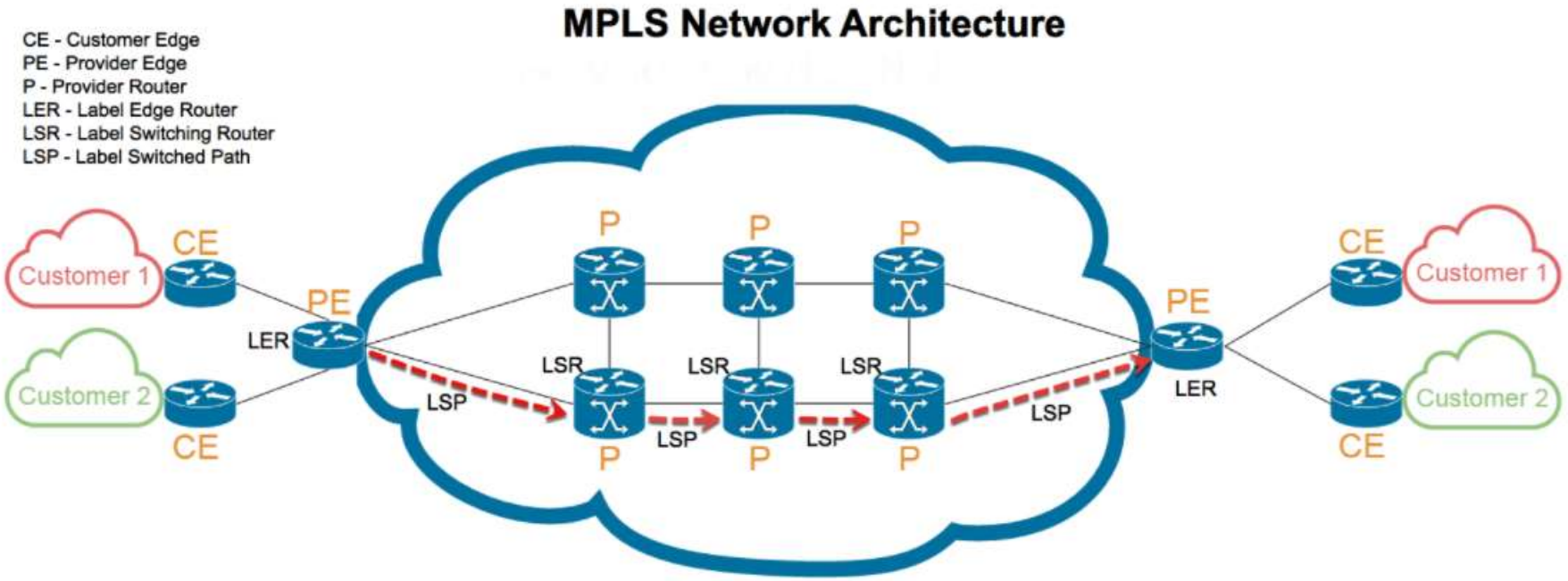


MPLS

- Multi-Protocol Label Switching
  - 고속의 라우팅 및 전송기능을 제공하기 위해 연구
  - 고속 전송기능 이외에 트래픽 엔지니어링, QoS제공, VPN기능 제공 등 기존 인터넷에서 구현하기 어려운 다양한 응용 분야를 제공
- When behaving like a router, MPLS can forward the packet based on the destination address; when behaving like a switch, it can forward a packet based on the label

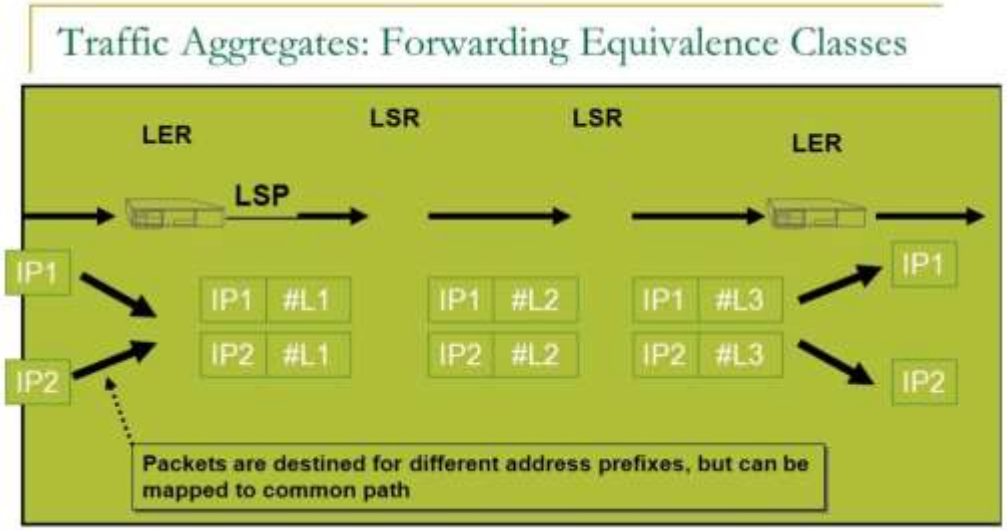
MPLS

- Architecture



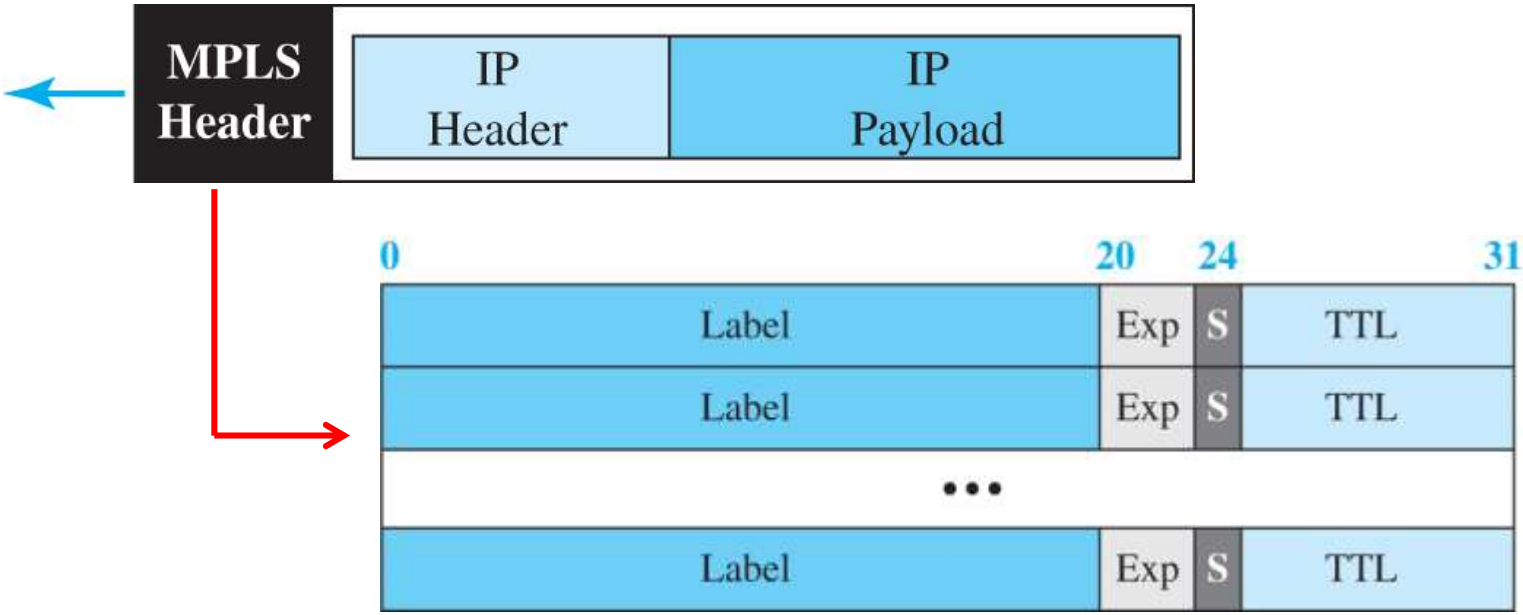
MPLS

- 미리 결정된 고효율 경로를 설정하는 방법으로 성능 문제를 해결하는데, 패킷이 처음 네트워크로 진입할 때 특정 FEC (Forwarding Equivalence Class)에 할당되며, 이는 패킷에 짧은 비트 시퀀스(레이블)로 표시
  - FEC: Group of packets forwarded over the same path with same forwarding treatment



A New Header

- The MPLS header is actually a stack of subheaders that is used for multilevel hierarchical switching
- Figure shows the format of an MPLS header in which each subheader is 32 bits (4 bytes) long



A New Header

- Label: define the label that is used to index the forwarding table in the router
- Exp: reserved for experimental purposes
- S: defines the situation of the sub-header in the stack
  - 1: means that header is the last one in the stack
- TTL: each visited router decrements the value of this field

Hierarchical Switching

- A stack of labels in MPLS allows hierarchical switching
- A packet with two labels can use the top label to forward the packet through switches outside an organization; the bottom label can be used to route the packet inside the organization to reach the destination subnet

Hierarchical Switching