Computer Network

Lecture 6

Network Layer Part.1

2019. 03. 01

Sungwon Lee

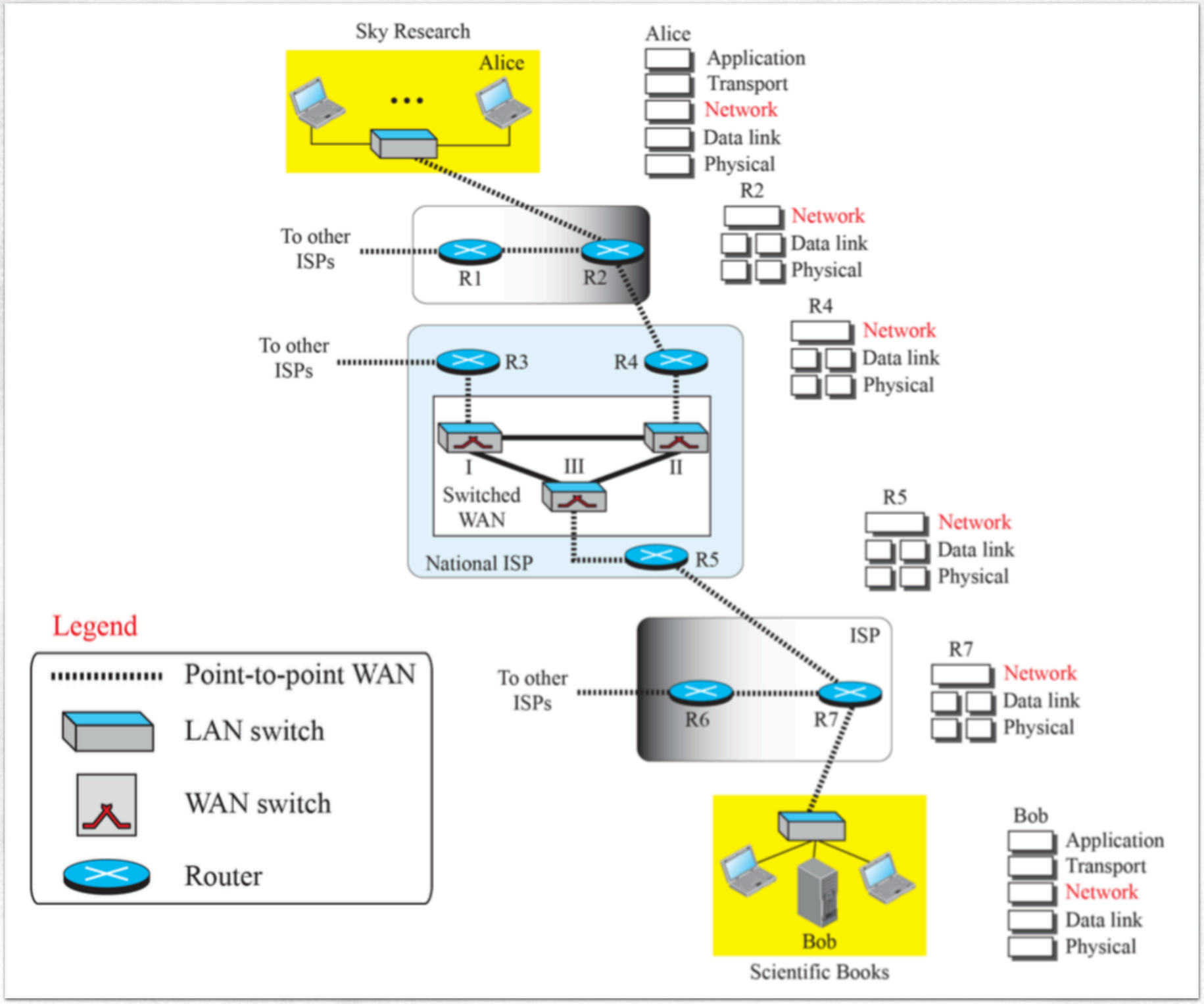
Department of Software Convergence

경희대학교
KYUNG HEE UNIVERSITY

Contents

- **Concept**
- Datagram and Virtual Circuit
- Network Performance
- Addressing
- More Issues
- IP Protocol

Host-to-Host communication concept



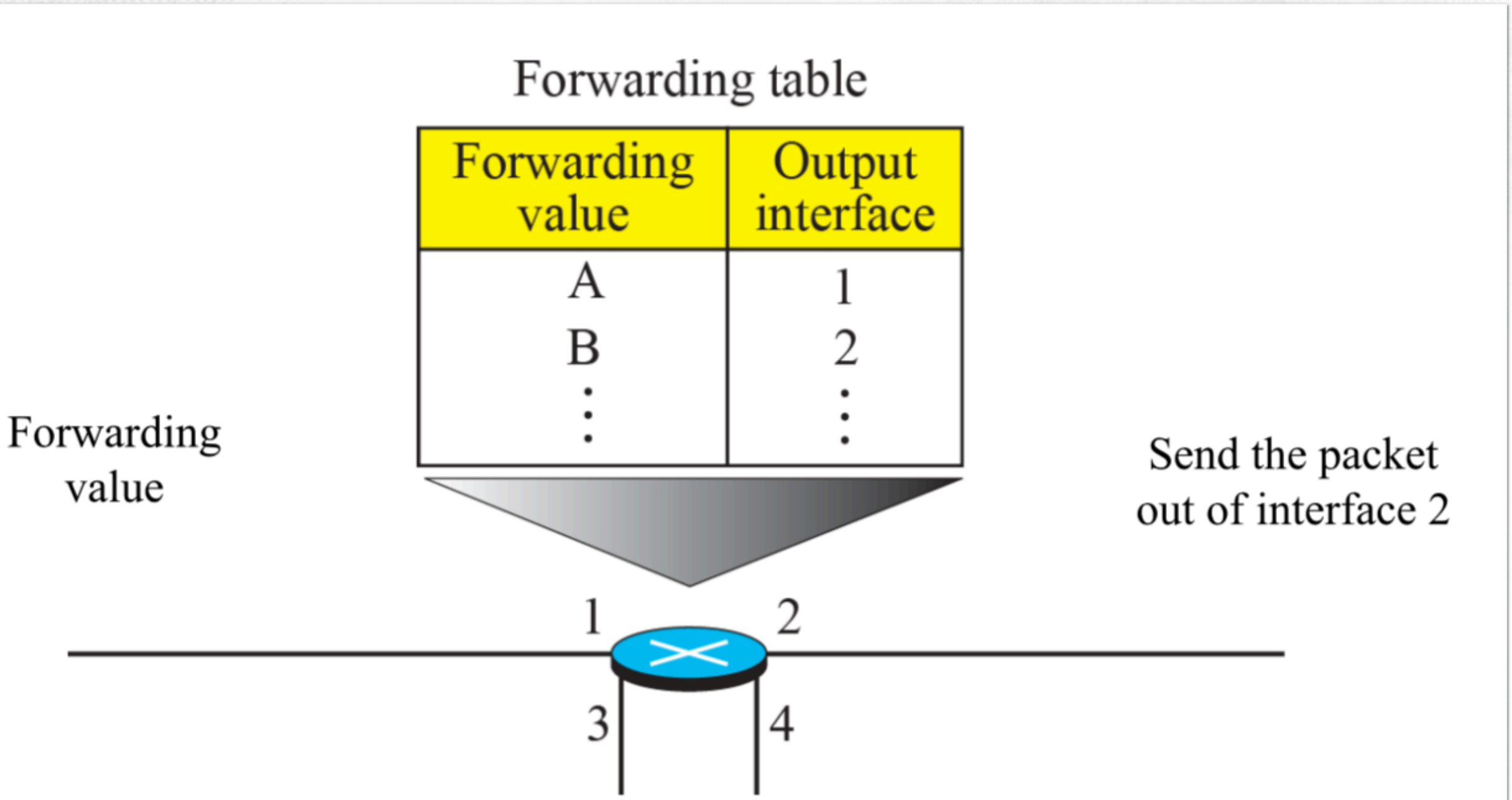
Packetizing

- The first duty of the network layer is definitely packetizing: encapsulating the payload in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination. In other words, one duty of the network layer is to carry a payload from the source to the destination without changing it or using it.
- The network layer is doing the service of a carrier such as the postal office, which is responsible for delivery of packages from a sender to a receiver without changing or using the contents.

Routing and Forwarding

- Other duties of the network layer, which are as important as the first, are routing and forwarding, which are directly related to each other.

Forwarding process



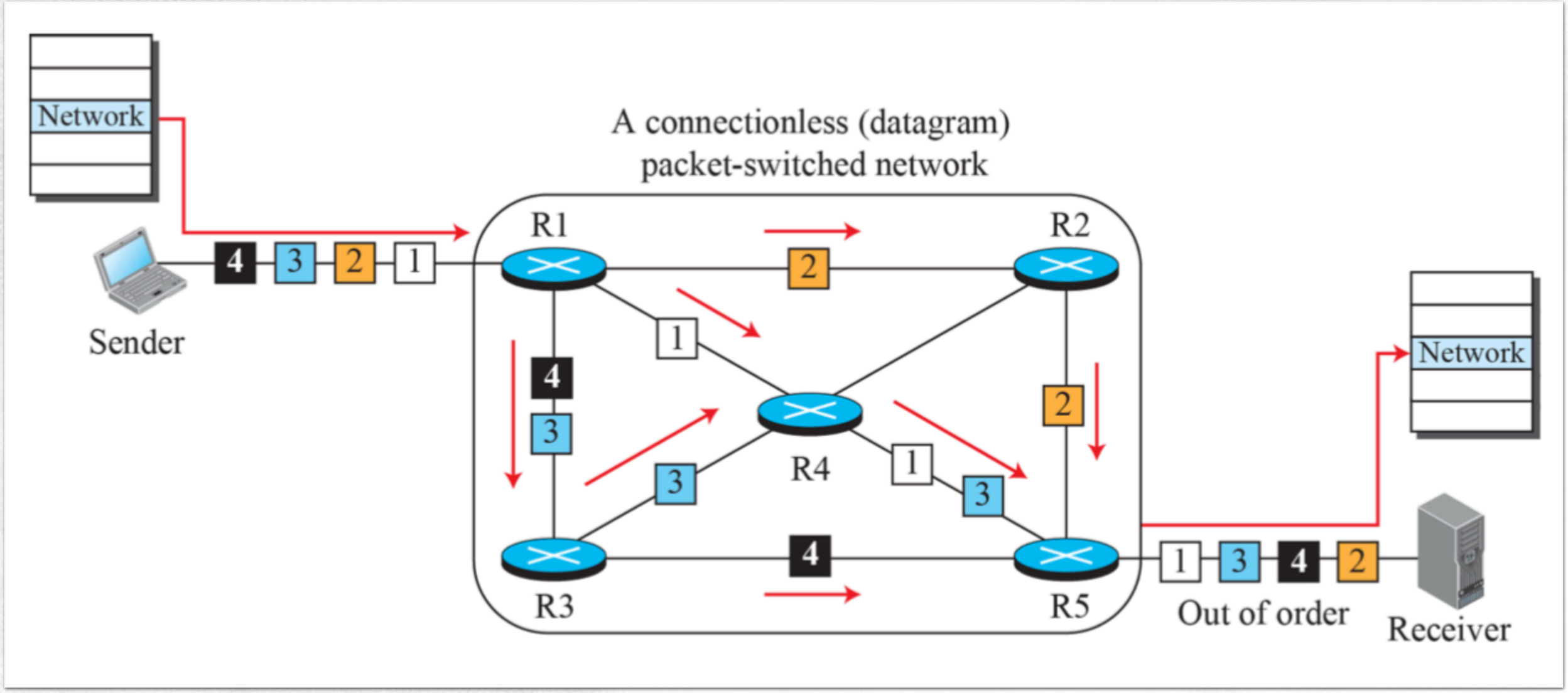
Contents

- Concept
- **Datagram and Virtual Circuit**
- Network Performance
- Addressing
- More Issues
- IP Protocol

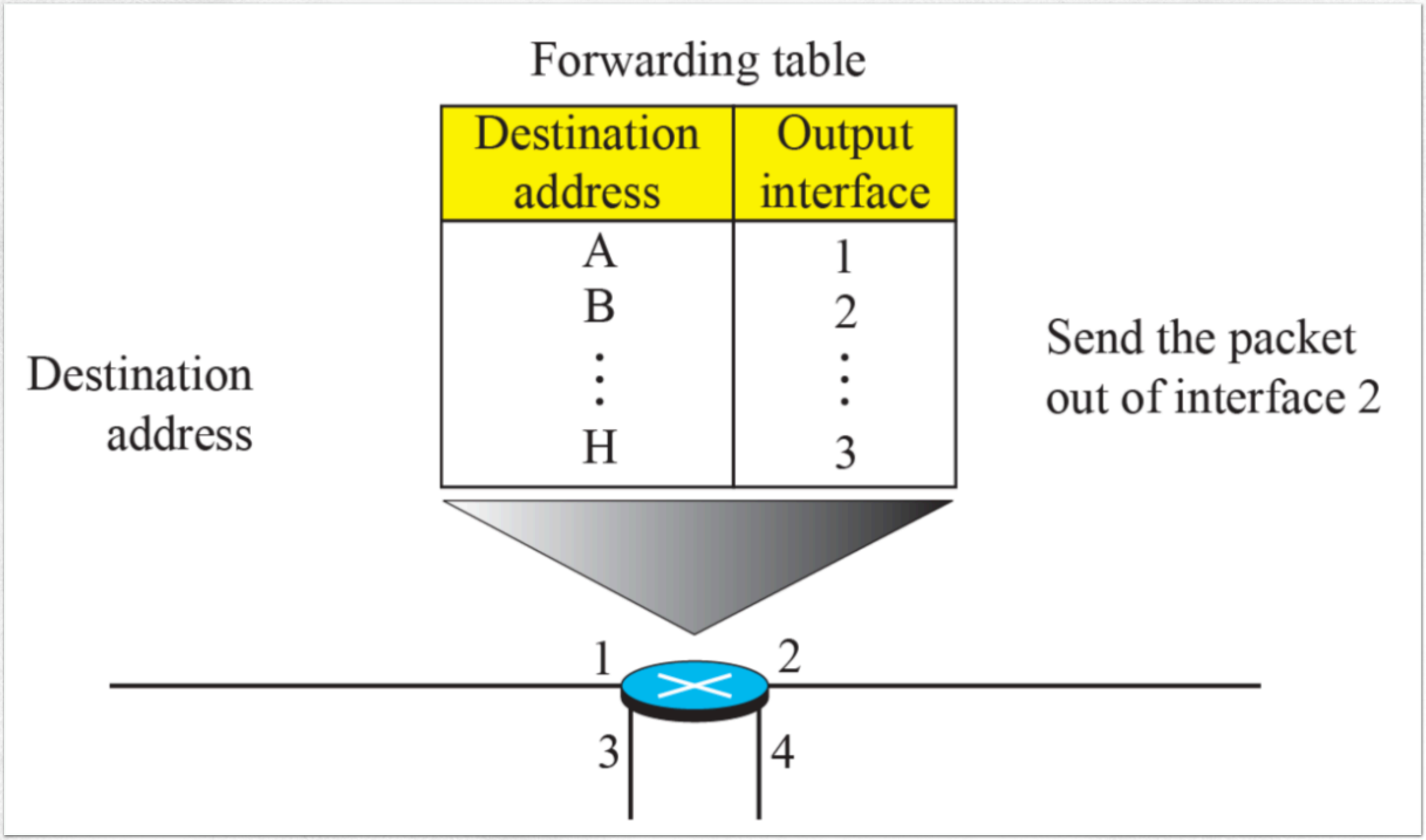
Concept

- When the Internet started, to make it simple, the network layer was designed to provide a connectionless service in which the network-layer protocol treats each packet independently, with each packet having no relationship to any other packet. The idea was that the network layer is only responsible for delivery of packets from the source to the destination. In this approach, the packets in a message may or may not travel the same path to their destination.

A connectionless packet-switched network



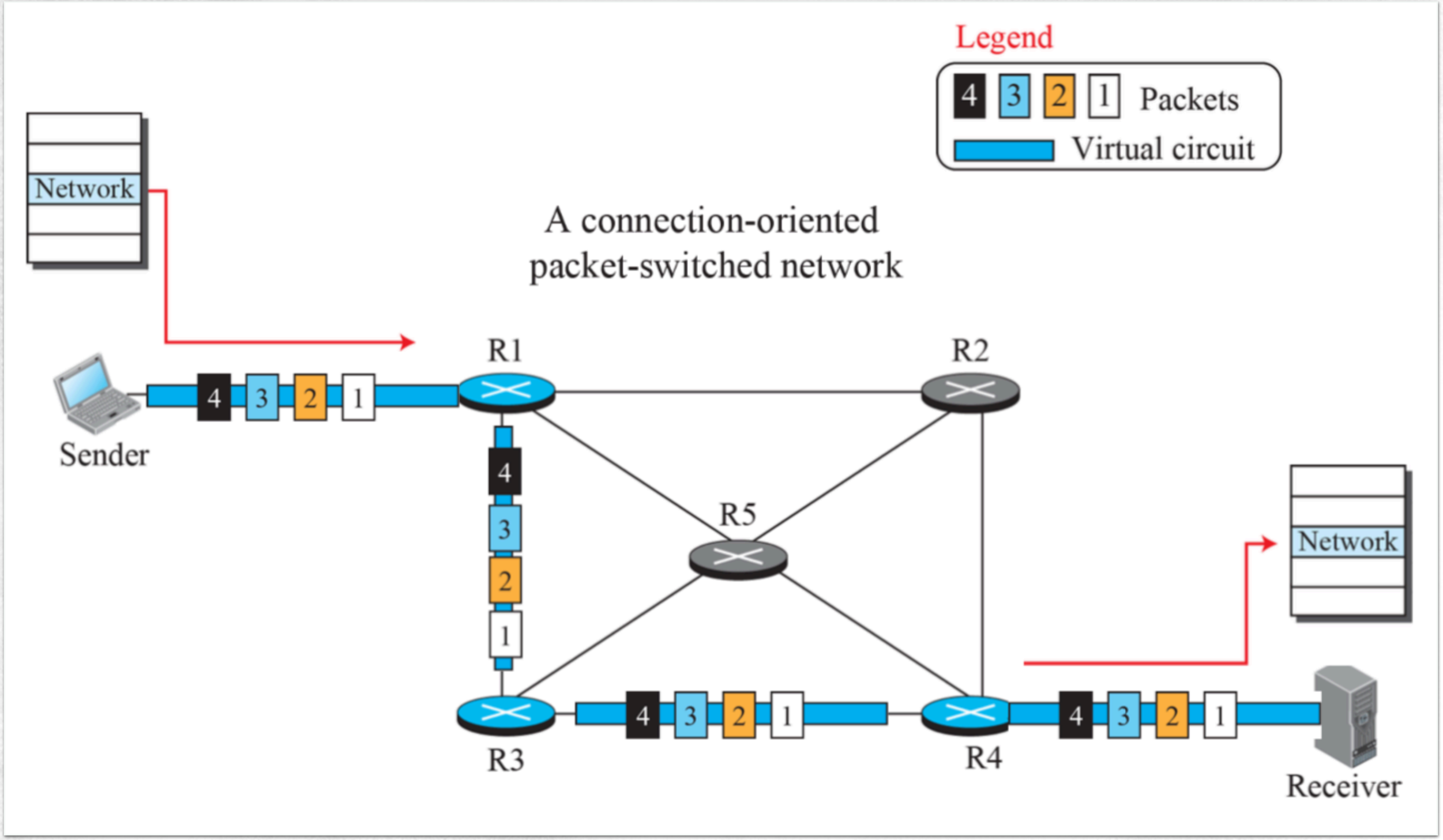
Forwarding process in a router



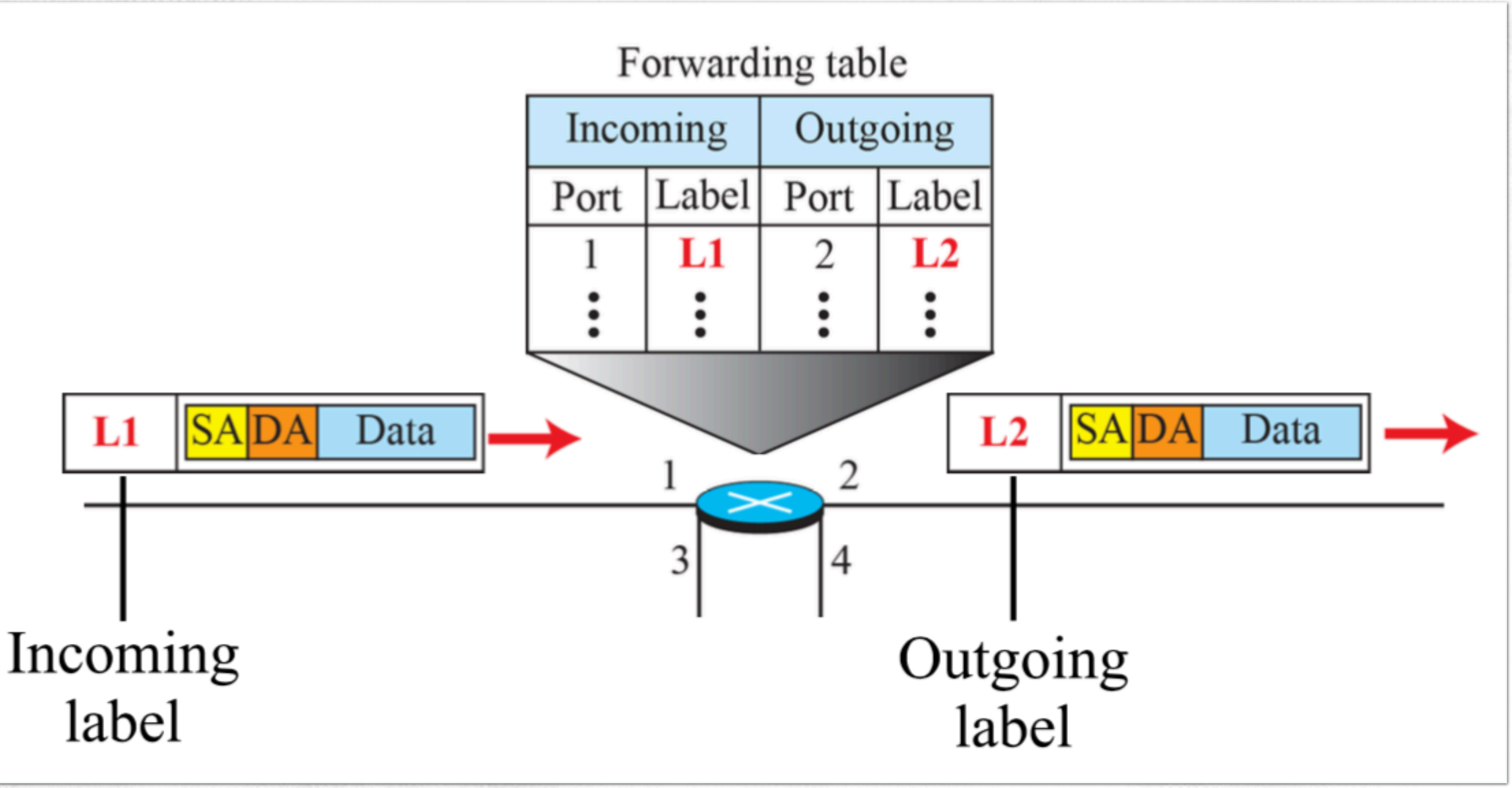
Concept

- In a connection-oriented service (also called virtual-circuit approach), there is a relationship between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams. After connection setup, the datagrams can all follow the same path. In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow.

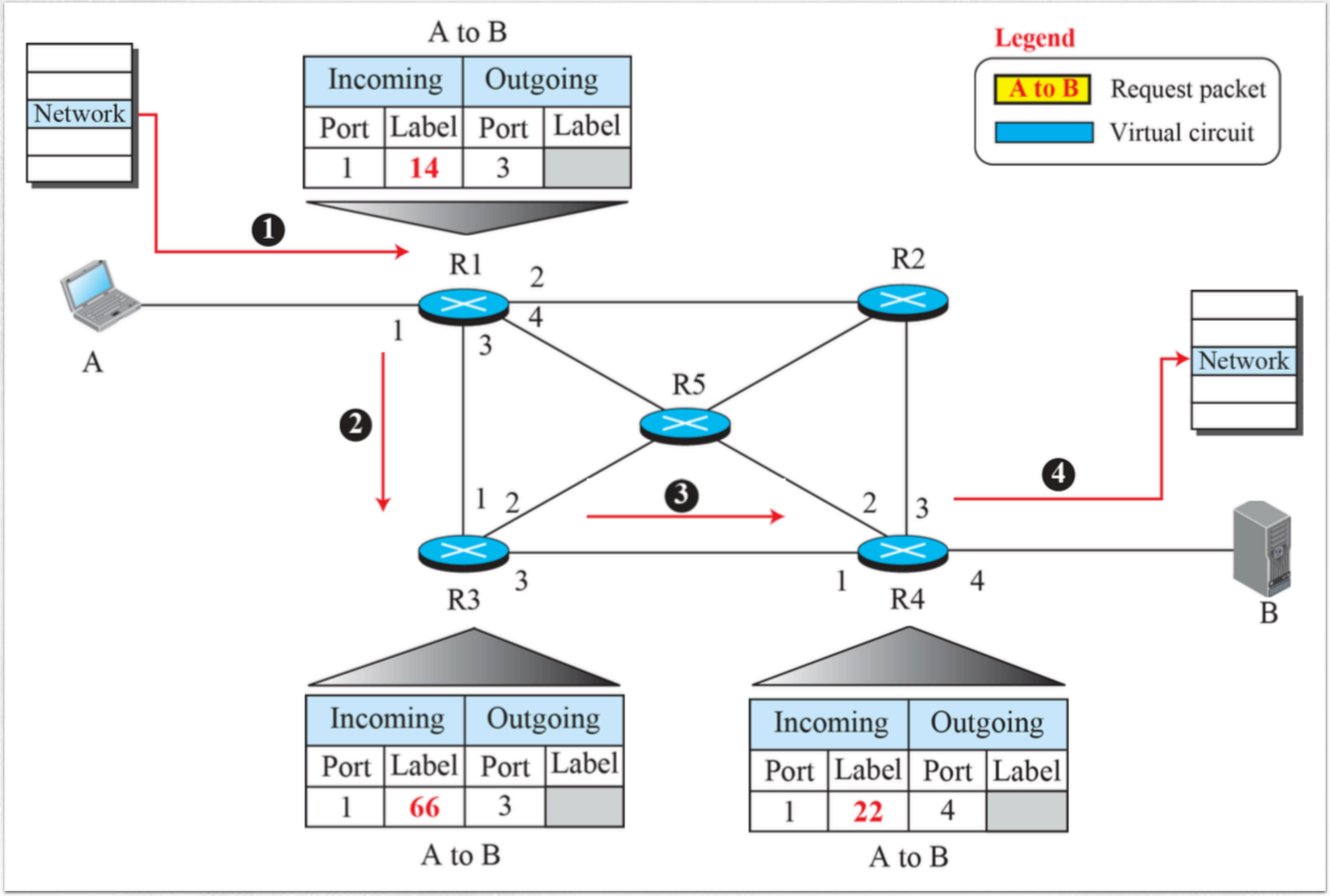
A virtual-circuit packet-switched network



Forwarding process in a VC Switch

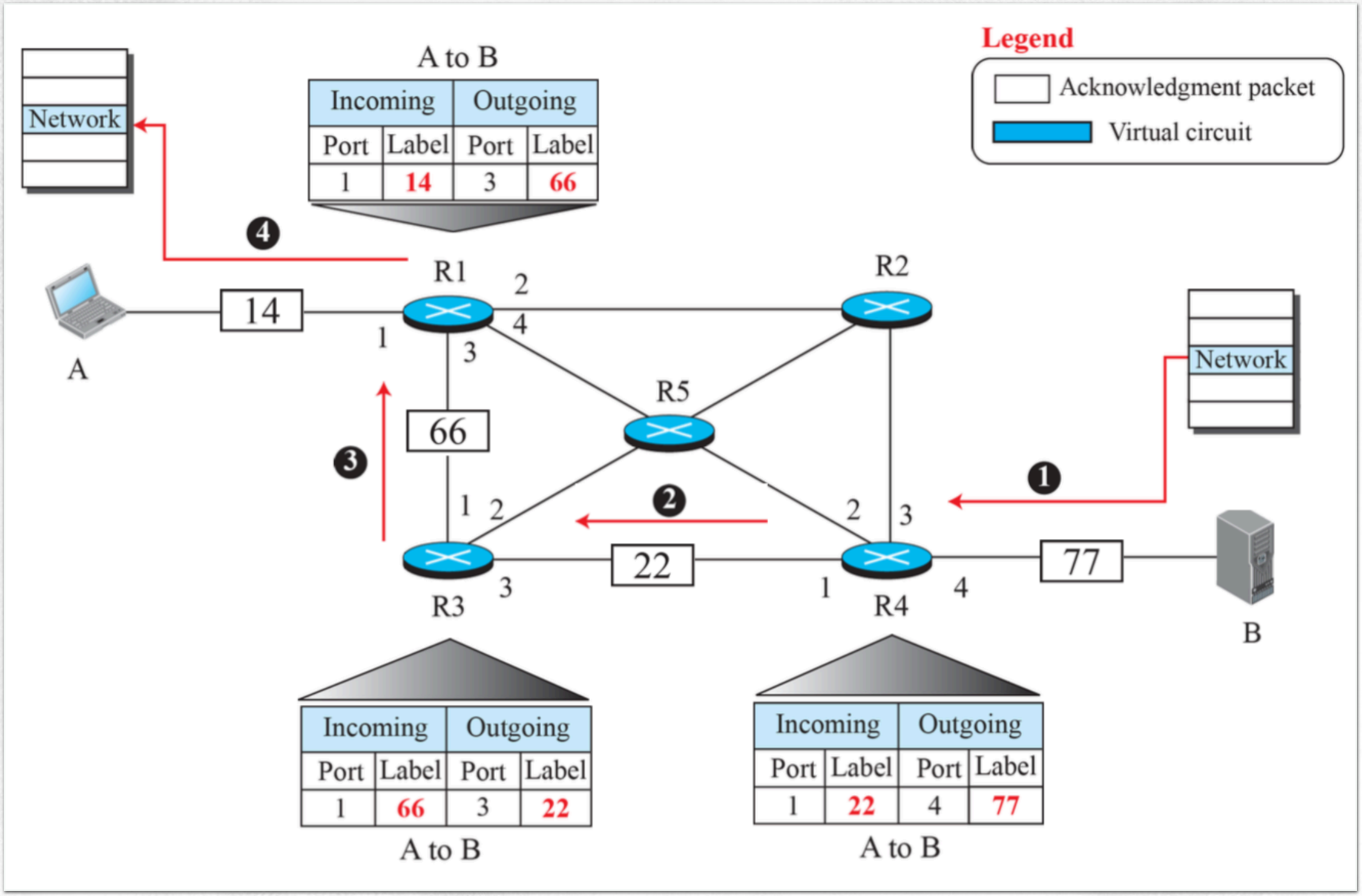


Sending request packet in a virtual-circuit network

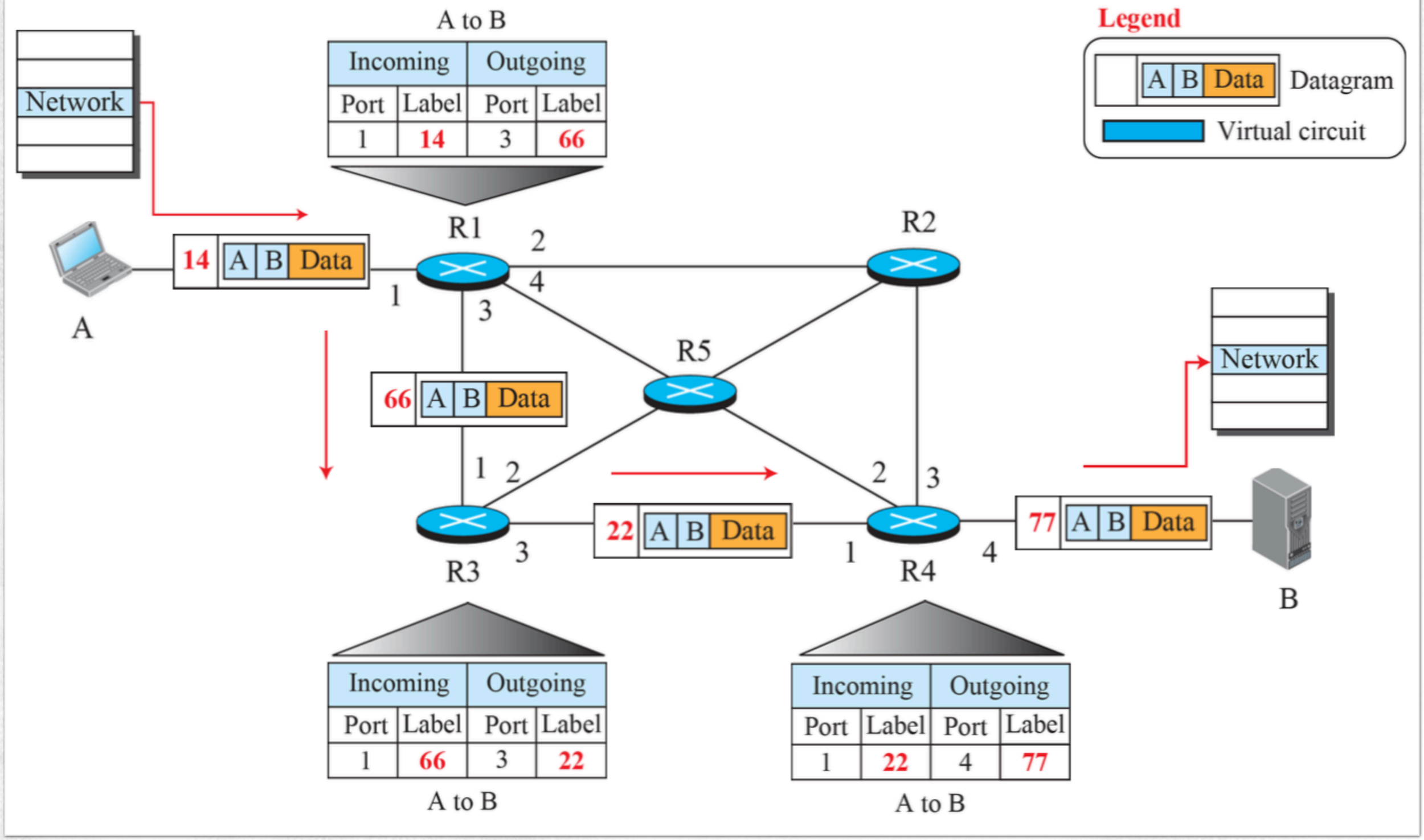


Virtual-Circuit Approach

Sending acknowledgments in a virtual-circuit network



Flow of one packet in an established virtual circuit



Contents

- Concept
- Datagram and Virtual Circuit
- **Network Performance**
- Addressing
- More Issues
- IP Protocol

Concept

- The upper-layer protocols that use the service of the network layer expect to receive an ideal service, but the network layer is not perfect. The performance of a network can be measured in terms of delay, throughput, and packet loss. Congestion control is an issue that can improve the performance.

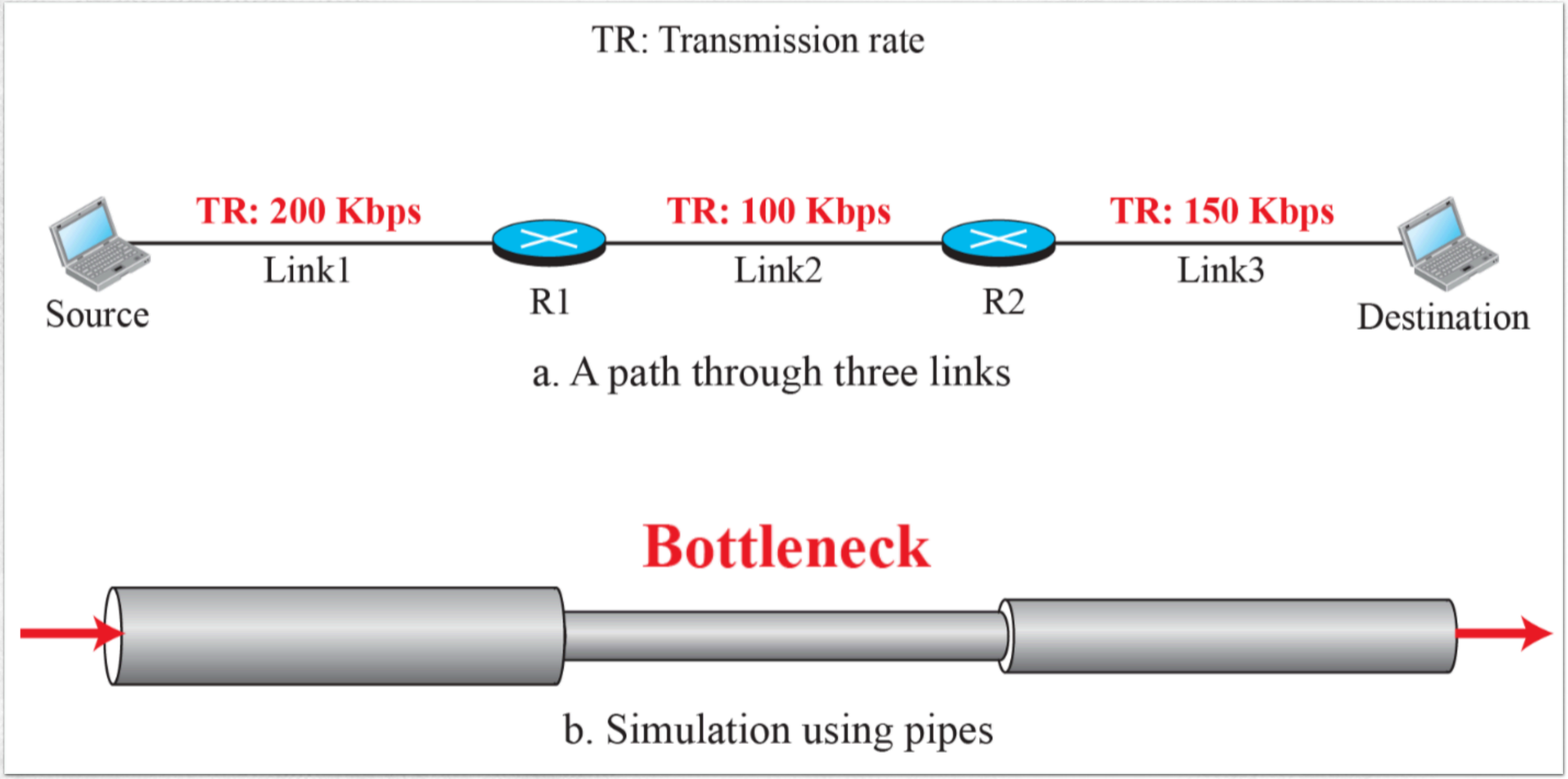
Delay

- All of us expect instantaneous response from a network, but a packet, from its source to its destination, encounters delays. The delays in a network can be divided into four types: transmission delay, propagation delay, processing delay, and queuing delay. Let us first discuss each of these delay types and then show how to calculate a packet delay from the source to the destination.

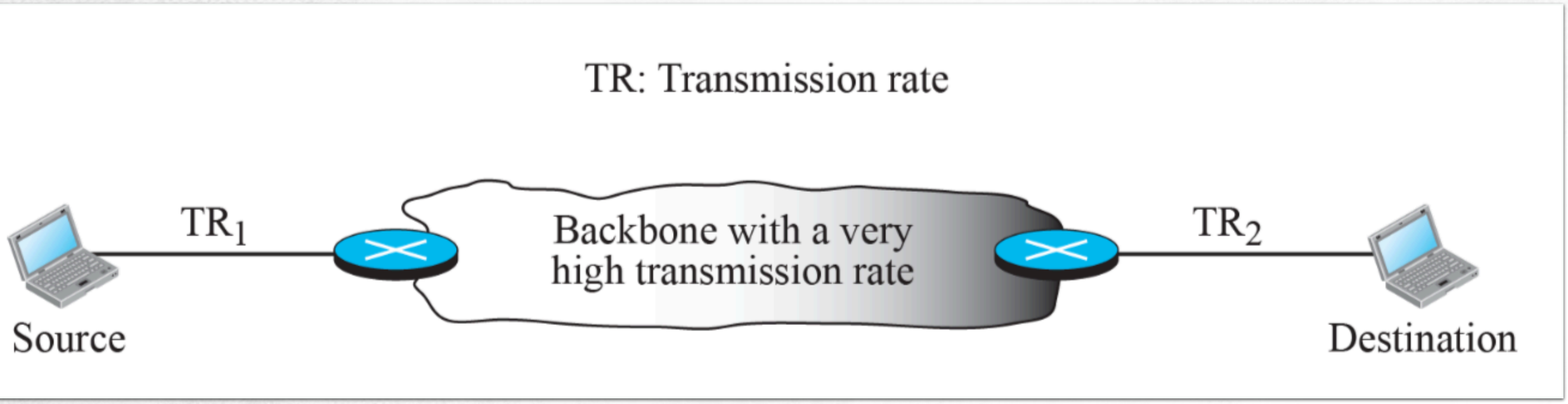
Throughput

- Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point. In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate. How, then, can we determine the throughput of the whole path? To see the situation, assume that we have three links, each with a different transmission rate.

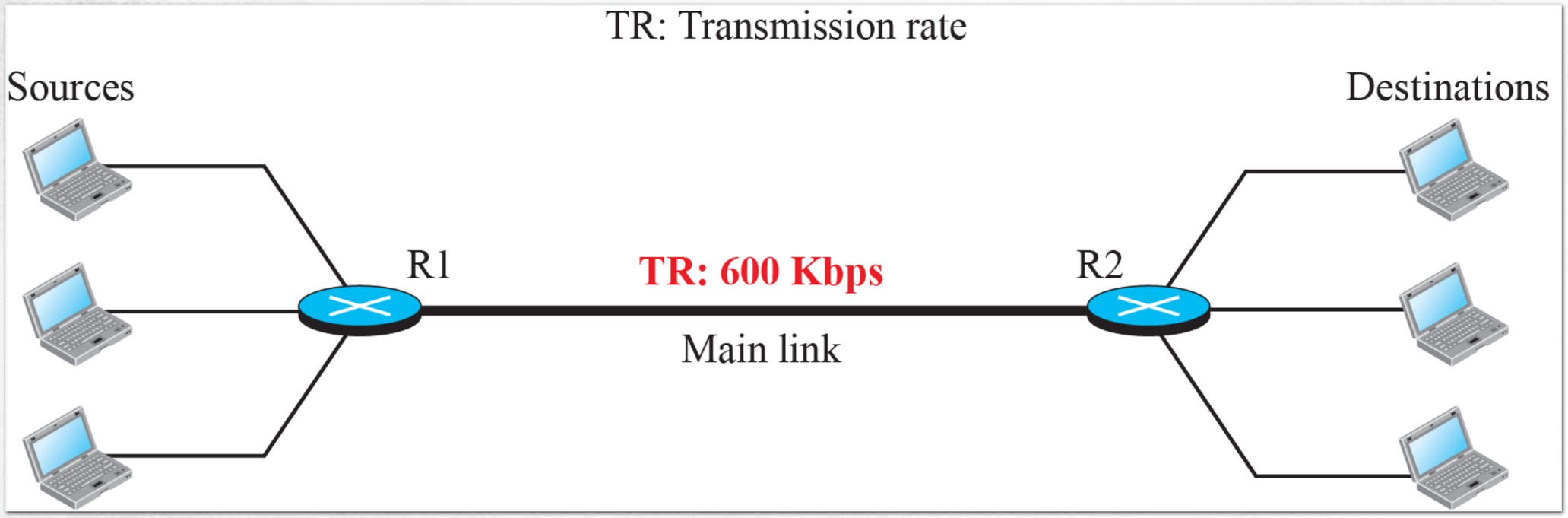
Throughput in a path with three links in a series



A path through the Internet backbone



Effect of throughput in shared links



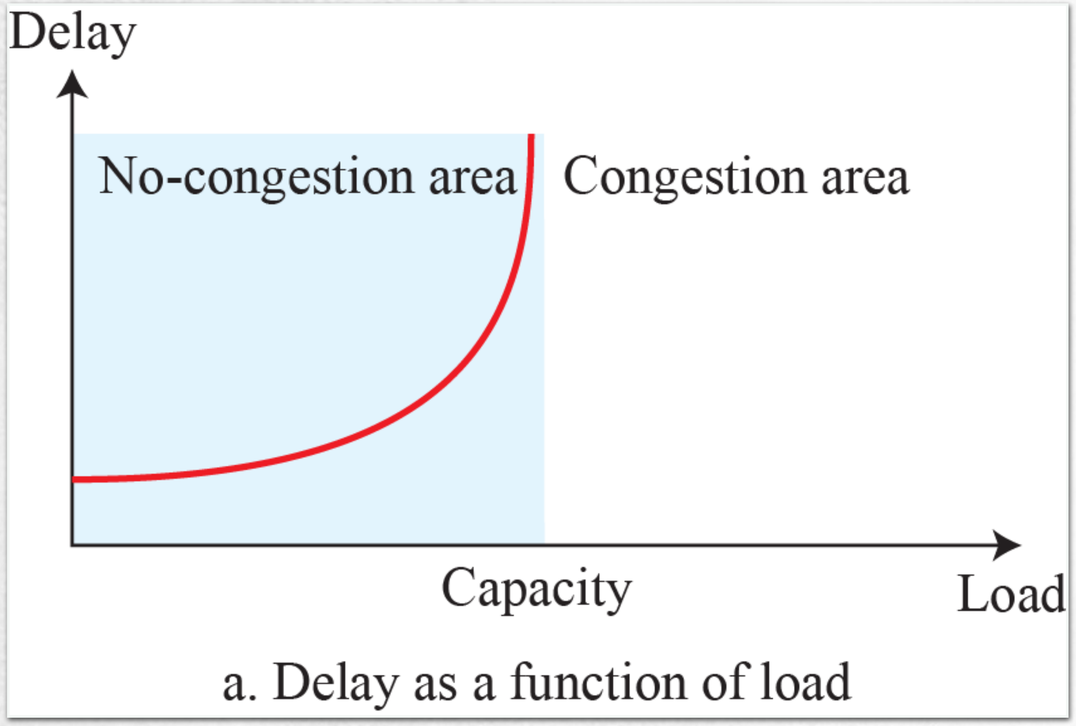
Packet Loss

- Another issue that severely affects the performance of communication is the number of packets lost during transmission. When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn. A router, however, has an input buffer with a limited size. A time may come when the buffer is full and the next packet needs to be dropped. The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.

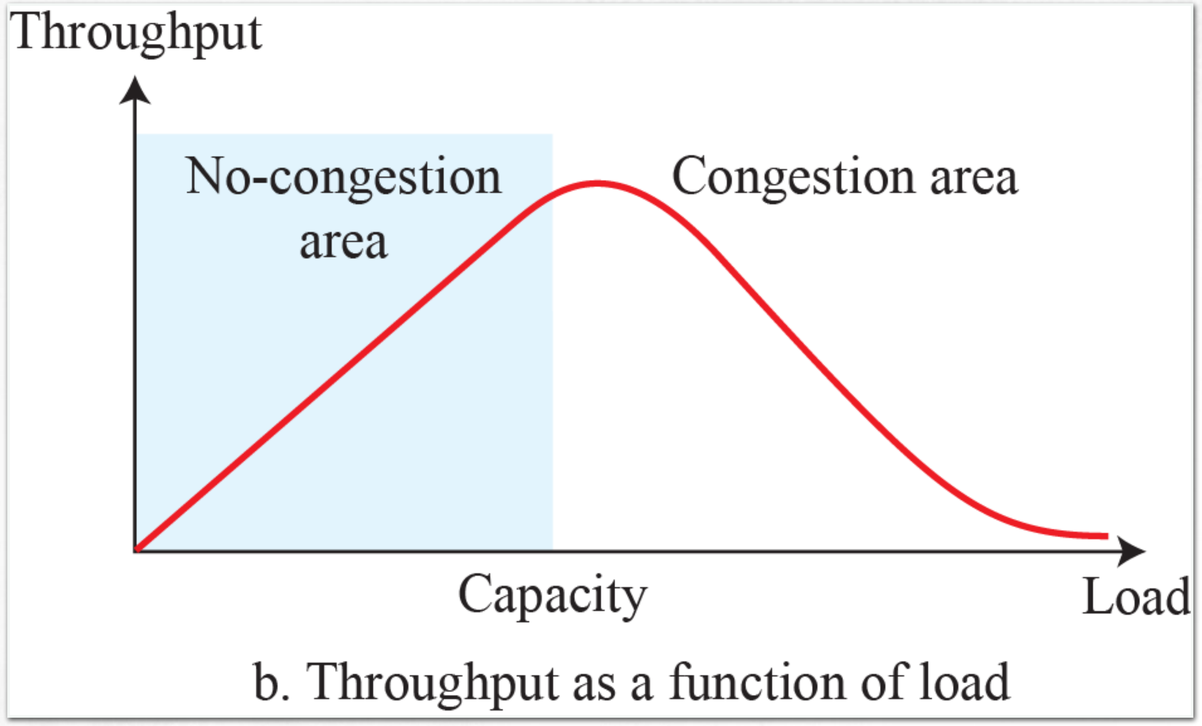
Congestion Control

- Congestion control is a mechanism for improving performance. Although congestion at the network layer is not explicitly addressed in the Internet model, the study of congestion at this layer may help us to better understand the cause of congestion at the transport layer and find possible remedies to be used at the network layer. Congestion at the network layer is related to two issues, throughput and delay, which we discussed in the previous section.

Packet delay and throughput as functions of load



a. Delay as a function of load



b. Throughput as a function of load

Contents

- Concept
- Datagram and Virtual Circuit
- Network Performance
- **Addressing**
- More Issues
- IP Protocol

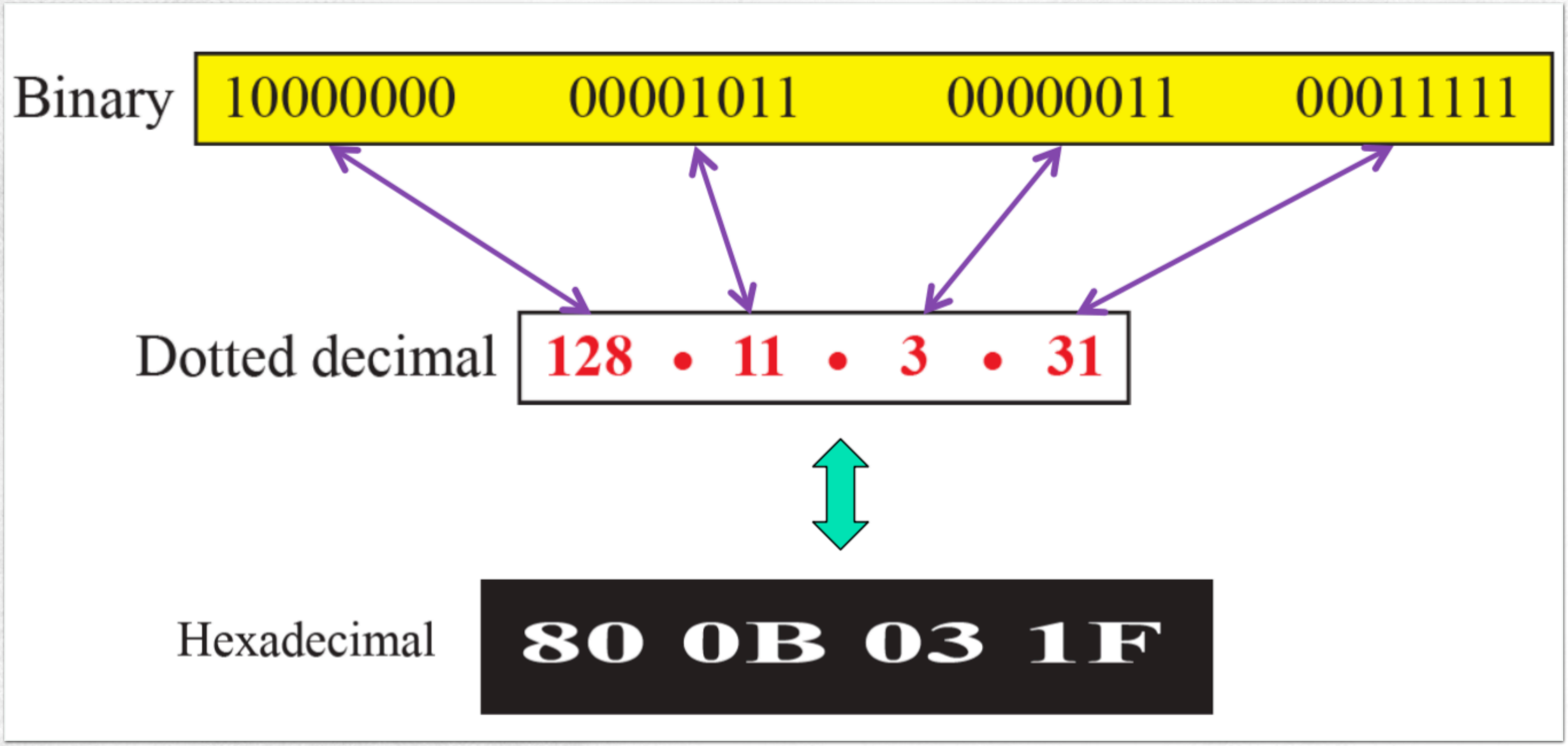
IPv4 Address

- The identifier used in the IP layer of the TCP/ IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address. An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet. The IP address is the address of the connection, not the host or the router.

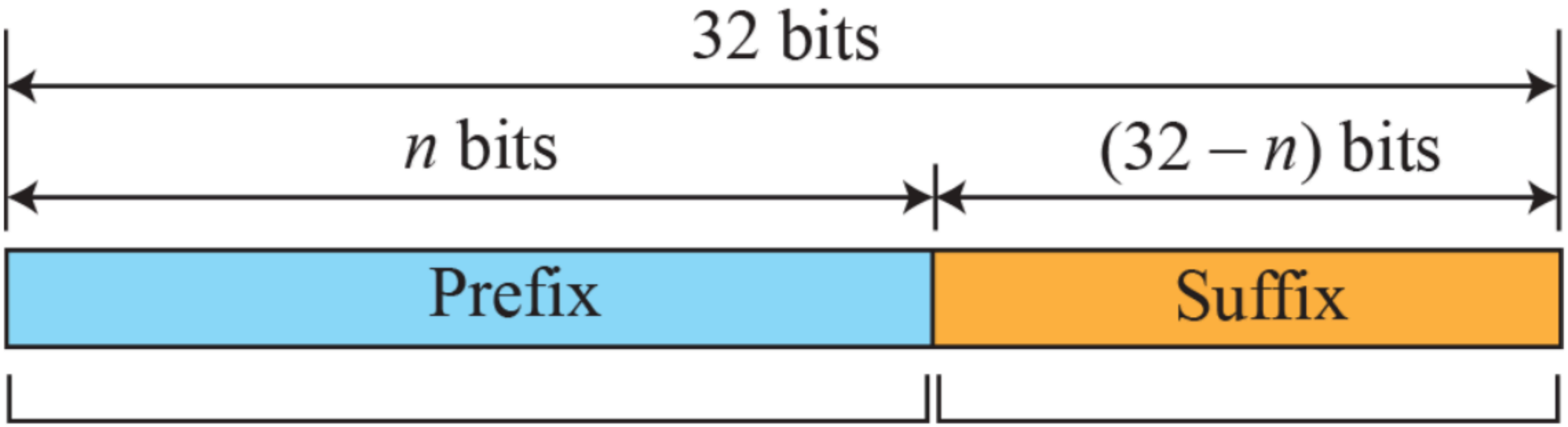
IPv4 Address Space

- A protocol like IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses b bits to define an address, the address space is 2b because each bit can have two different values (0 or 1). IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion). If there were no restrictions, more than 4 billion devices could be connected to the Internet.

Three different notations in IPv4 addressing

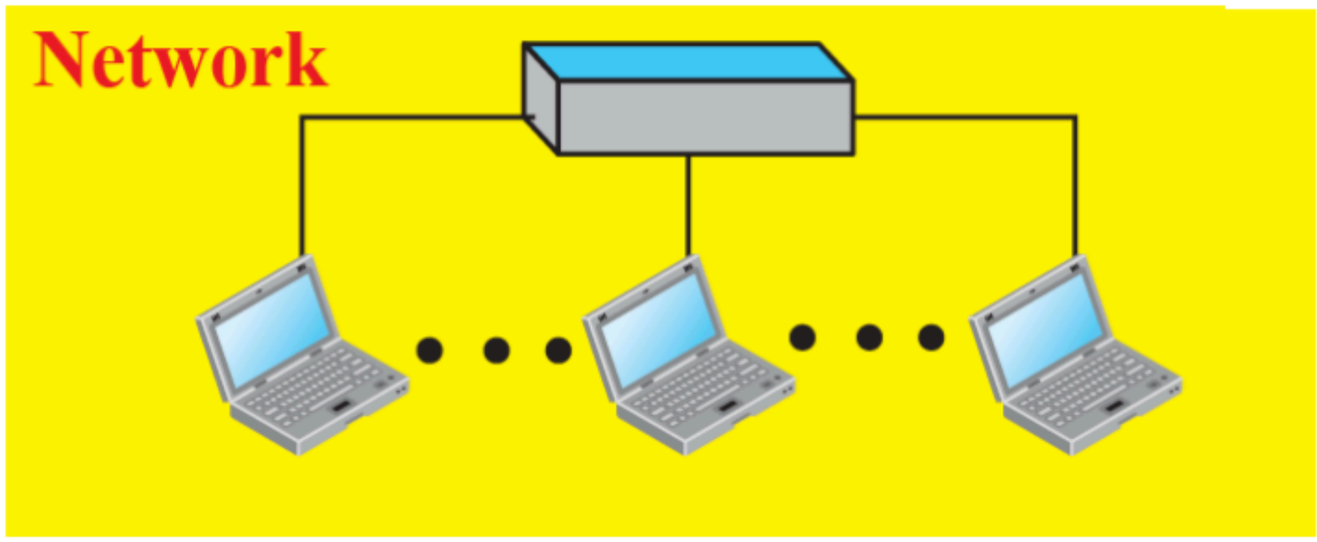


Hierarchy in addressing



Defines network

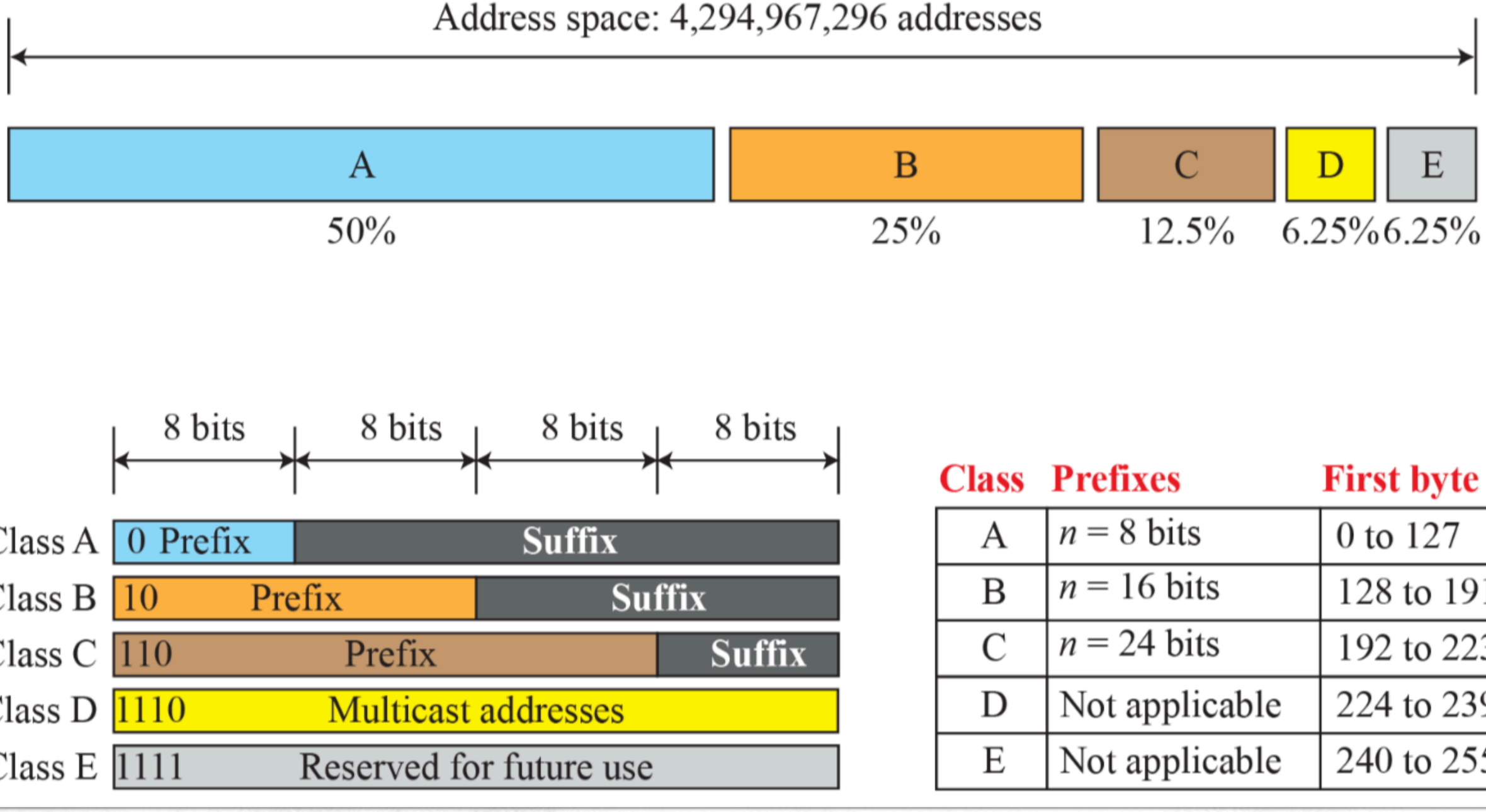
Defines connection to the node



Classful Addressing

- When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24). The whole address space was divided into five classes (class A, B, C, D, and E). This scheme is referred to as classful addressing. Although classful addressing belongs to the past, it helps us to understand classless addressing, discussed later.

Occupation of the address space in classful addressing

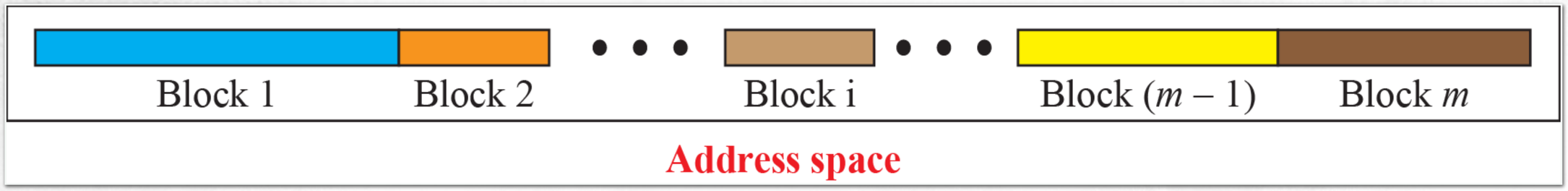


Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

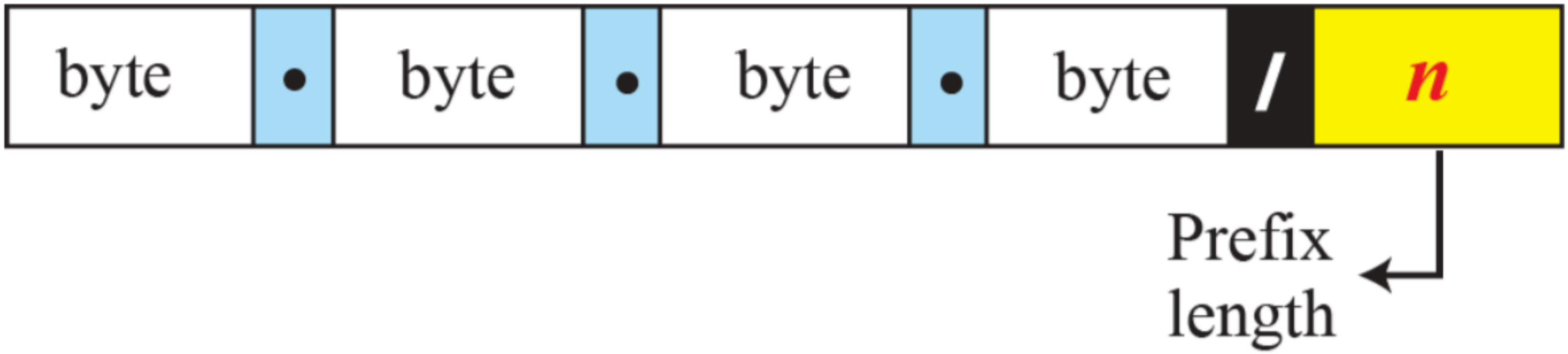
Classless Addressing

- With the growth of the Internet, it was clear that a larger address space was needed as a long-term solution. The larger address space, however, requires that the length of IP addresses also be increased, which means the format of the IP packets needs to be changed. Although the long-range solution has already been devised and is called IPv6, a short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization. The short-term solution still uses IPv4 addresses, but it is called classless addressing.

Variable-length blocks in classless addressing



Slash notation (CIDR)



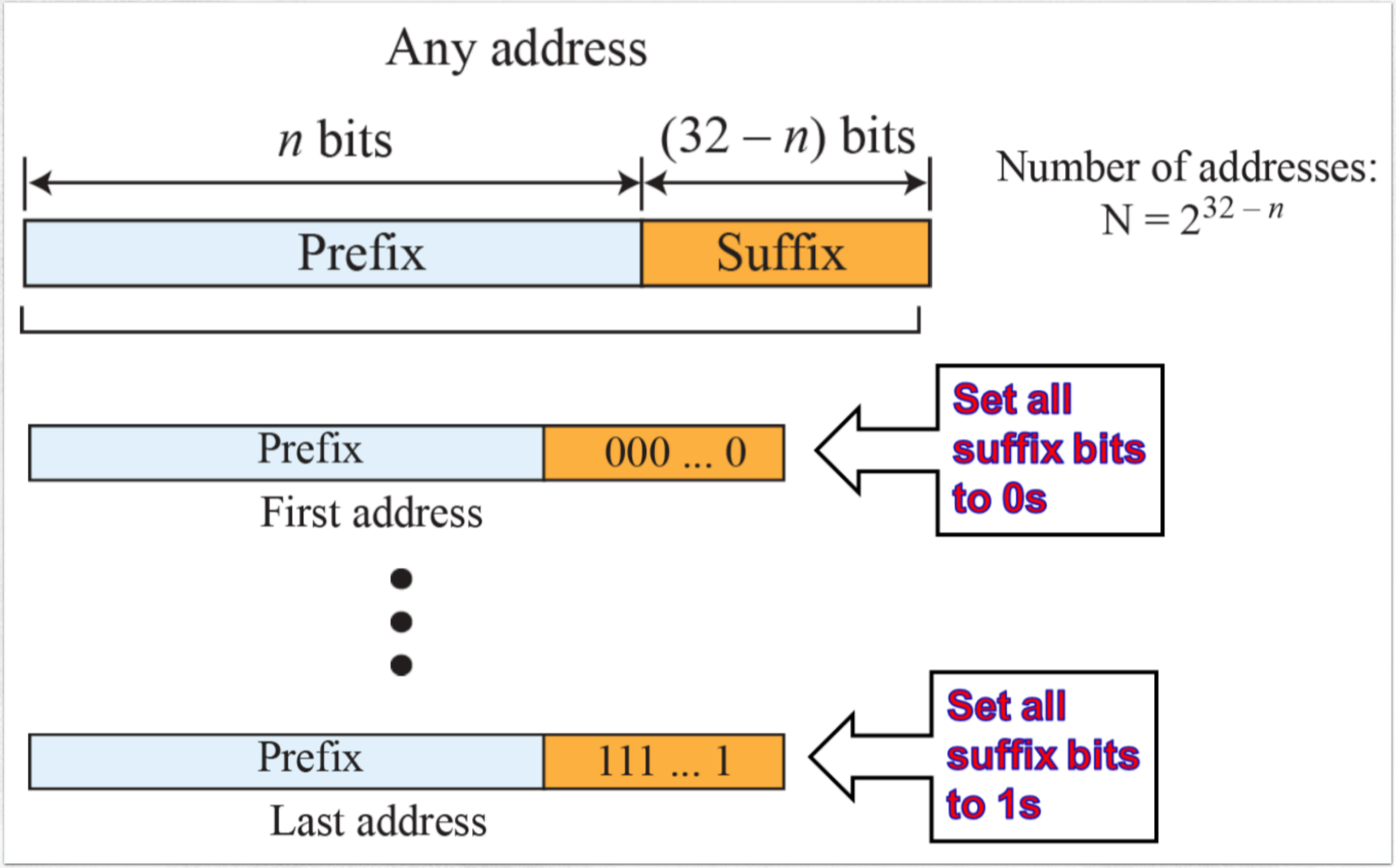
Examples:

12.24.76.8/**8**

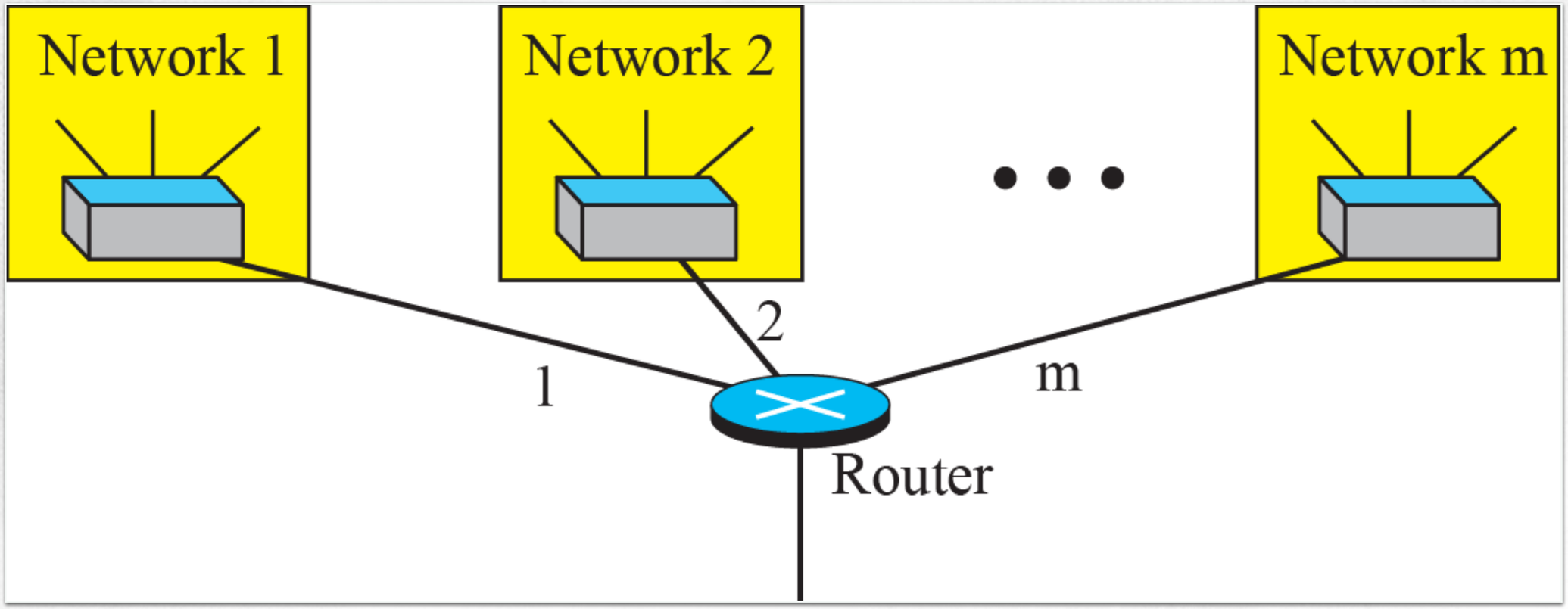
23.14.67.92/**12**

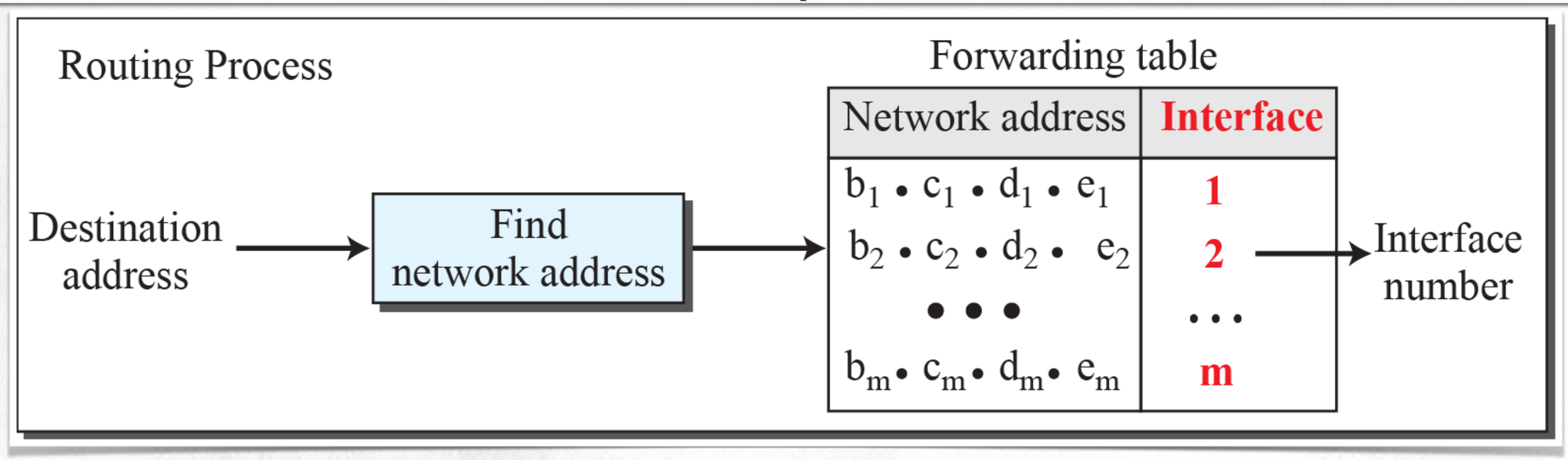
220.8.24.255/**25**

Information extraction in classless addressing

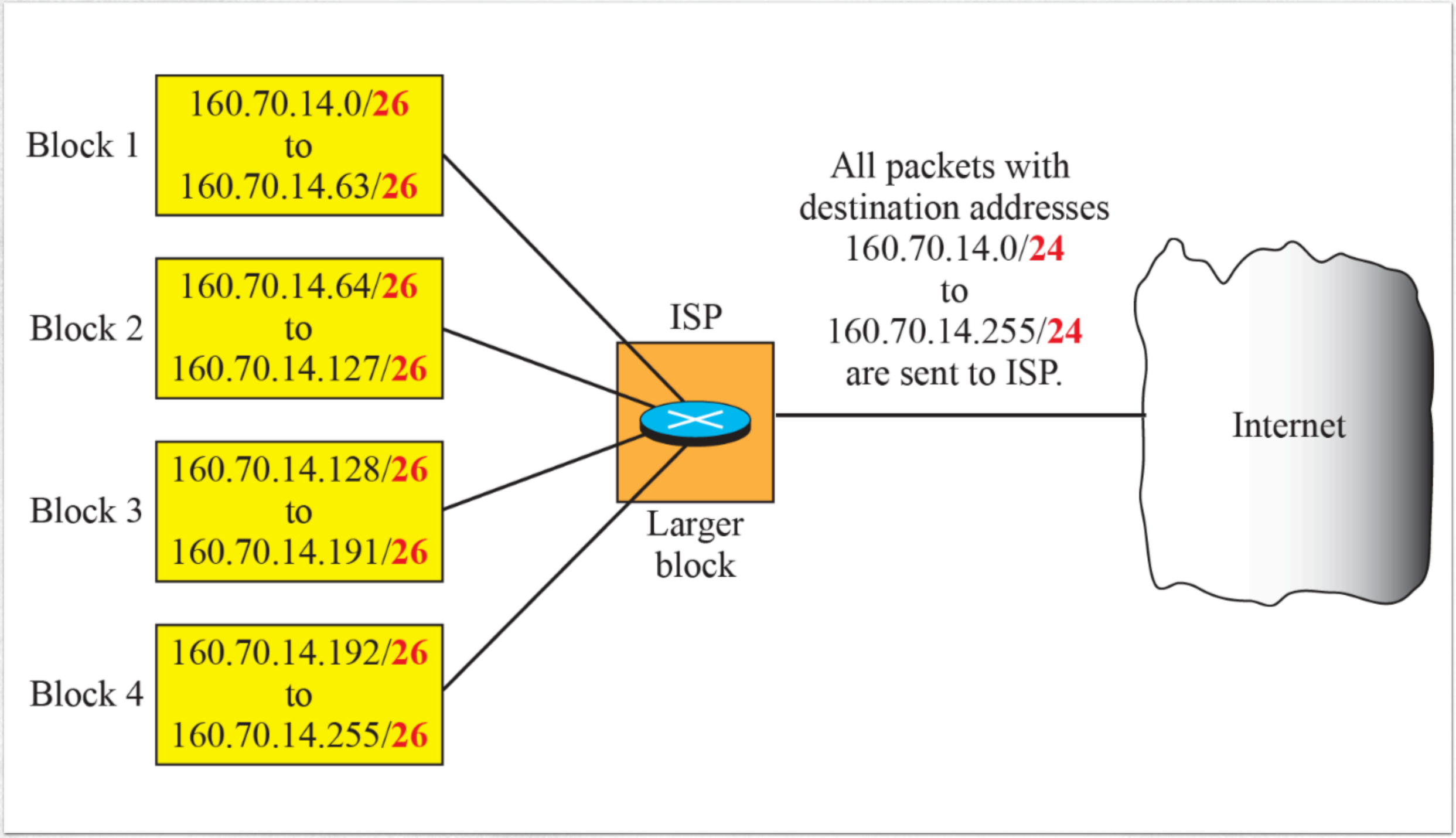


Network address routing example





Example of address aggregation



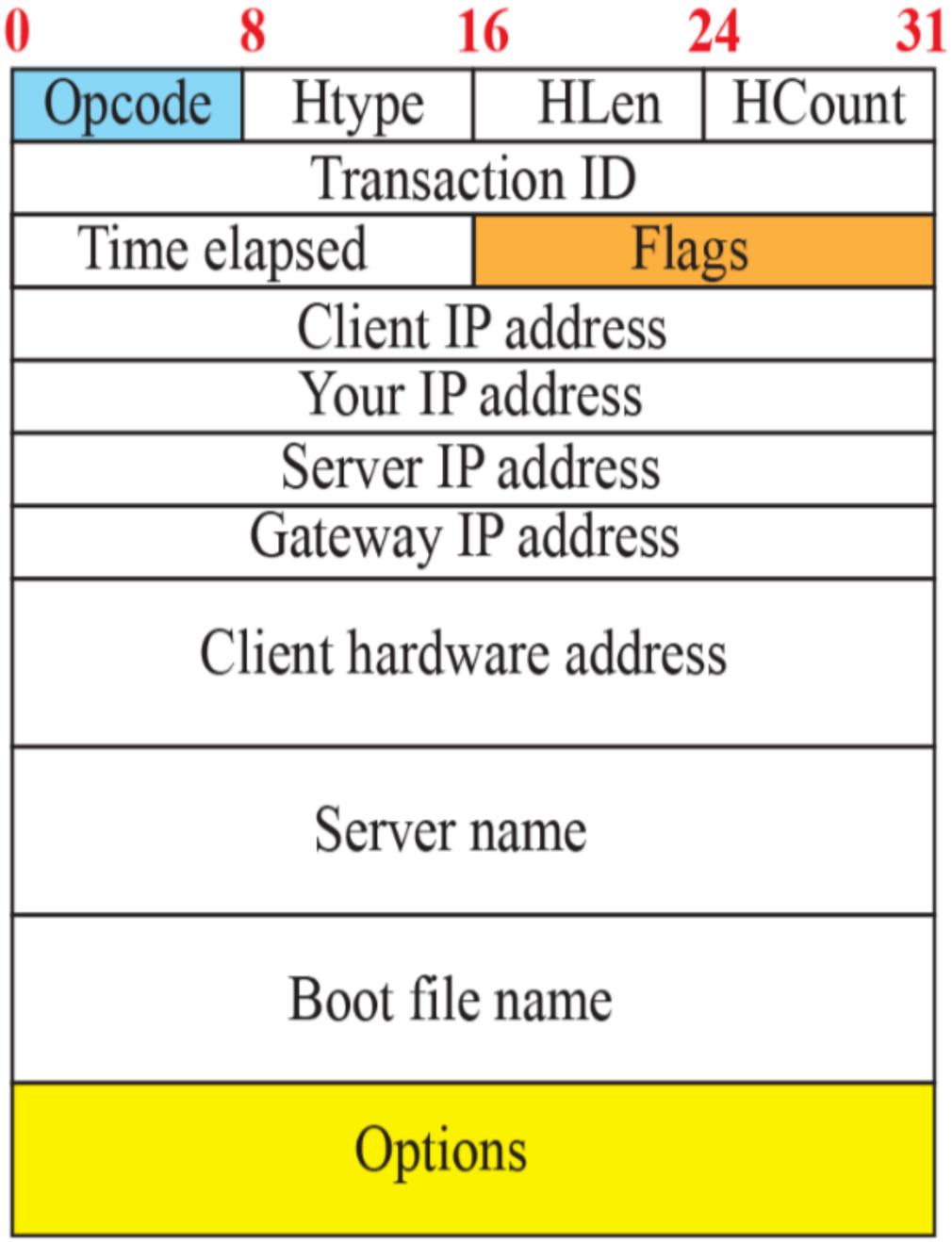
Contents

- Concept
- Datagram and Virtual Circuit
- Network Performance
- Addressing
- **More Issues**
- IP Protocol

Concept

- After a block of addresses are assigned to an organization, the network administration can manually assign addresses to the individual hosts or routers. However, address assignment in an organization can be done automatically using the Dynamic Host Configuration Protocol (DHCP). DHCP is an application-layer program, using the client-server paradigm, that actually helps TCP/IP at the network layer.

Message Format



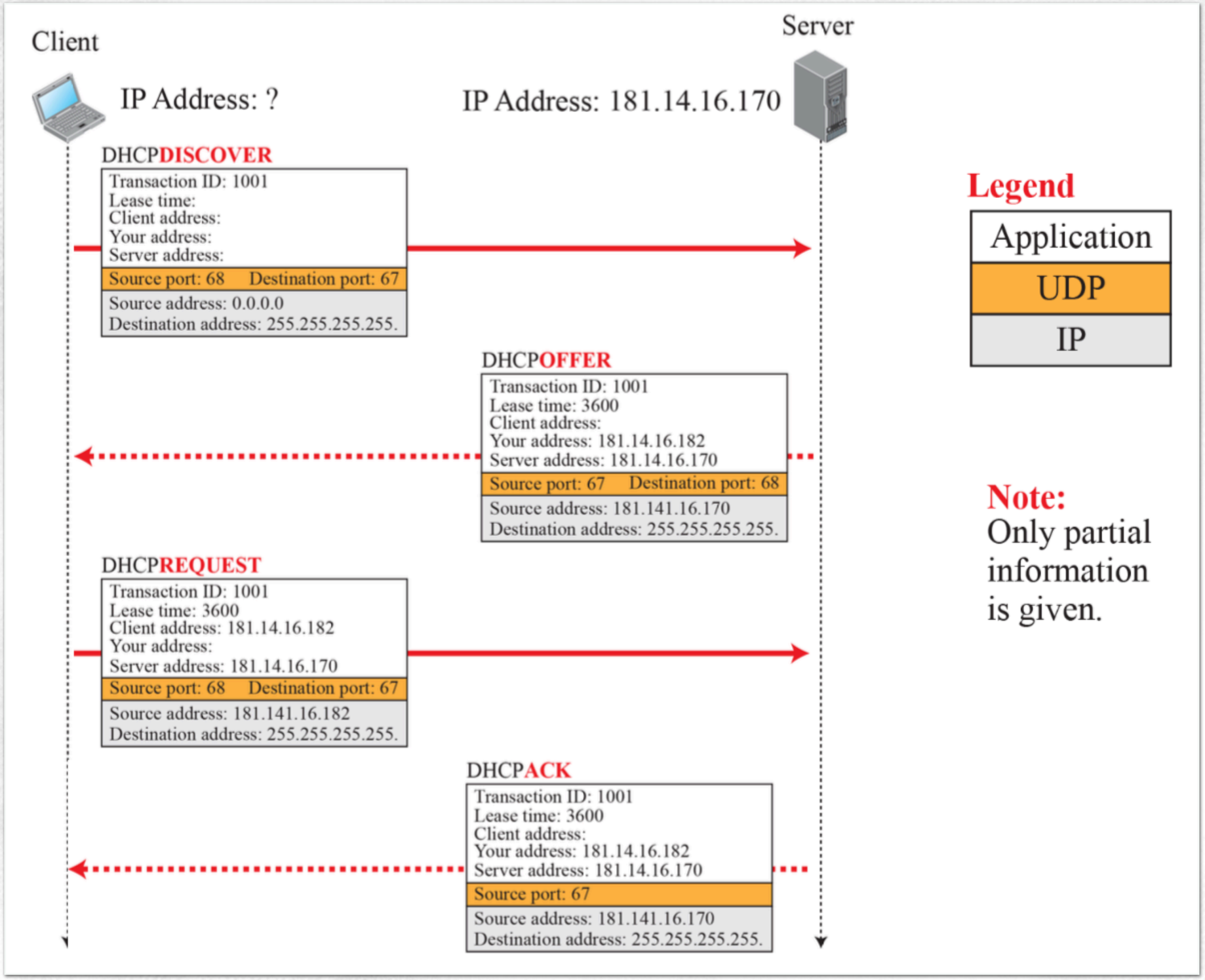
Fields:

Opcode: Operation code, request (1) or reply (2)
Htype: Hardware type (Ethernet, ...)
HLen: Lengh of hardware address
HCount: Maximum number of hops the packet can travel
Transaction ID: An integer set by client and repeated by the server
Time elapsed: The number of seconds since the client started to boot
Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used
Client IP address: Set to 0 if the client does not know it
Your IP address: The client IP address sent by the server
Server IP address: A broadcast IP address if client does not know it
Gateway IP address: The address of default router
Server name: A 64-byte domain name of the server
Boot file name: A 128-byte file name holding extra information
Options: A 64-byte field with dual purpose described in text

Message Option format

1 **DHCP**DISCOVER
2 **DHCP**OFFER
3 **DHCP**REQUEST
4 **DHCP**DECLINE
5 **DHCP**ACK
6 **DHCP**NACK
7 **DHCP**RELEASE
8 **DHCP**INFORM

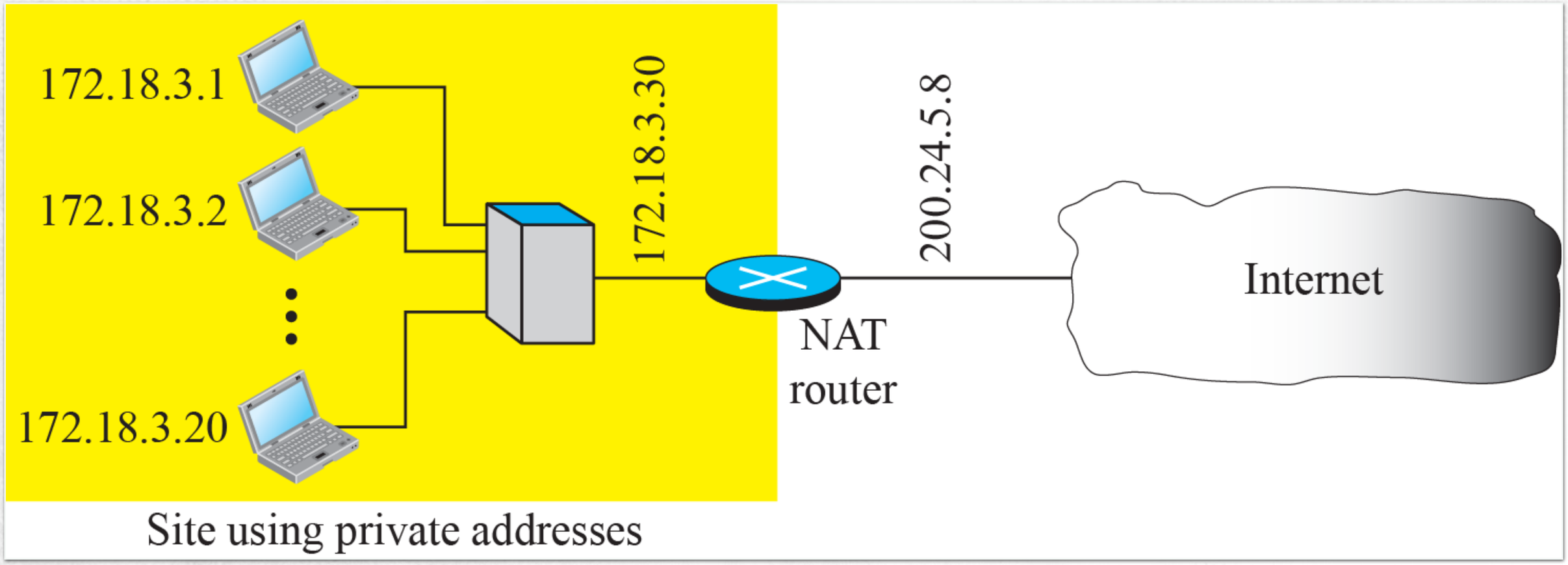
Operation


Client
Server
IP Address: ?
IP Address: 181.14.16.170
DHCPDISCOVER
Transaction ID: 1001
Lease time:
Client address:
Your address:
Server address:
Source port: 68 Destination port: 67
Source address: 0.0.0.0
Destination address: 255.255.255.255.
DHCPOFFER
Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.141.16.170
Destination address: 255.255.255.255.
DHCPREQUEST
Transaction ID: 1001
Lease time: 3600
Client address: 181.14.16.182
Your address:
Server address: 181.14.16.170
Source port: 68 Destination port: 67
Source address: 181.141.16.182
Destination address: 255.255.255.255.
DHCPACK
Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67
Source address: 181.141.16.170
Destination address: 255.255.255.255.
Legend
Application
UDP
IP
Note:
Only partial information is given.

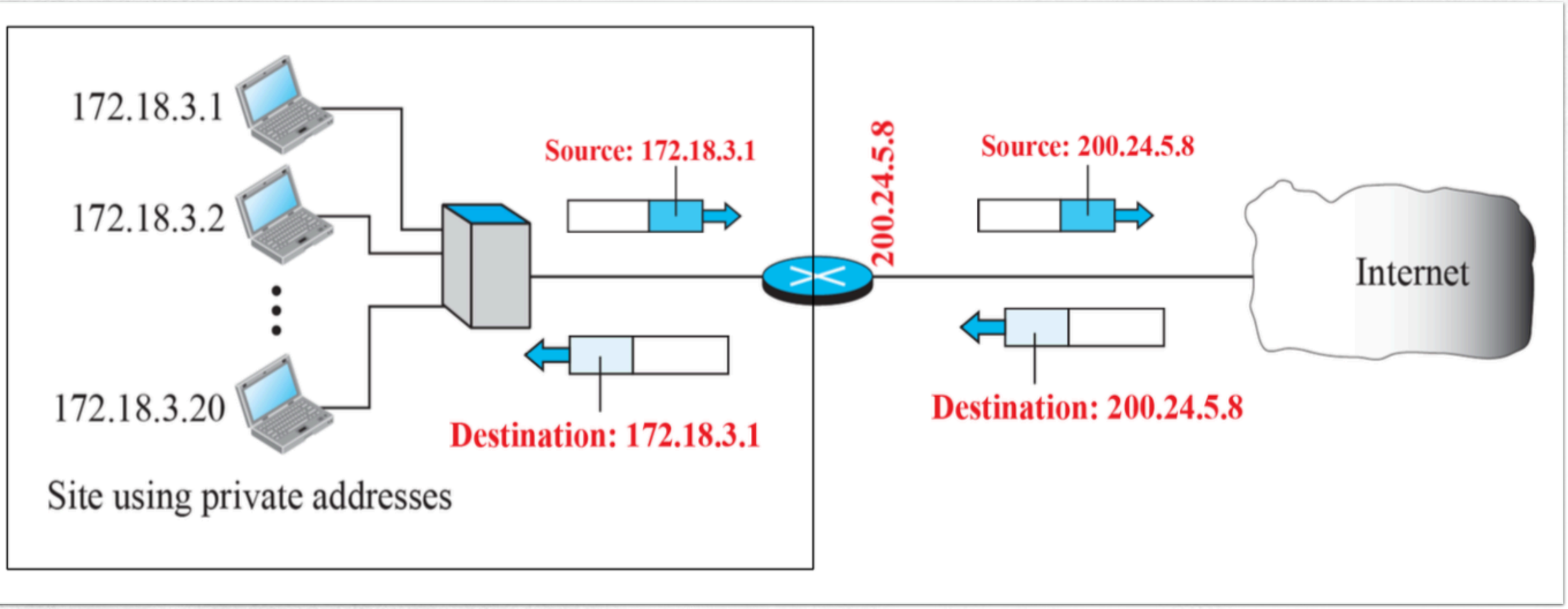
Concept

- In most situations, only a portion of computers in a small network need access to the Internet simultaneously. A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks, is Network Address Translation (NAT). The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world.

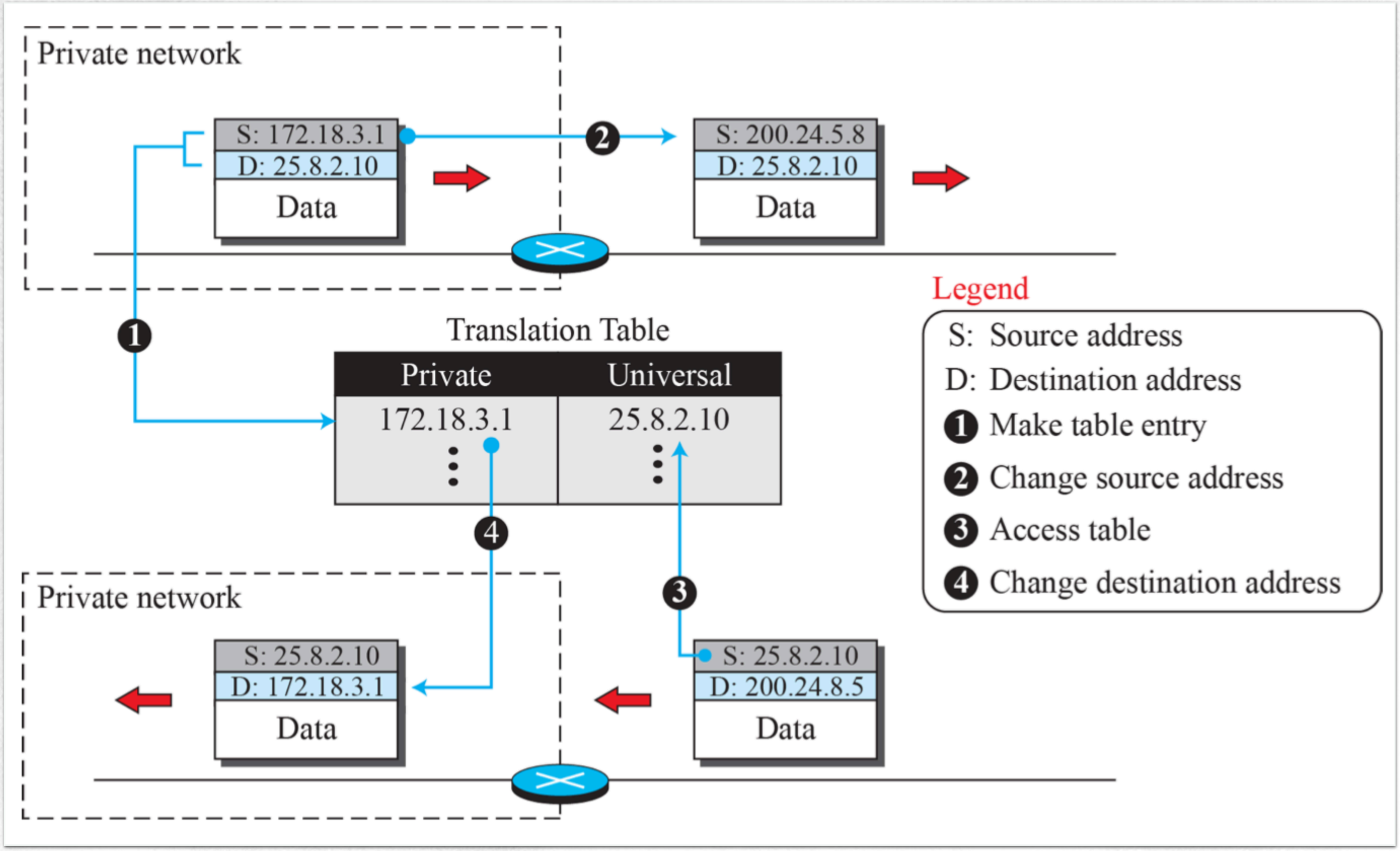
Concept


172.18.3.1
172.18.3.2
172.18.3.20
172.18.3.30
200.24.5.8
NAT
router
Internet
Site using private addresses

Address translation



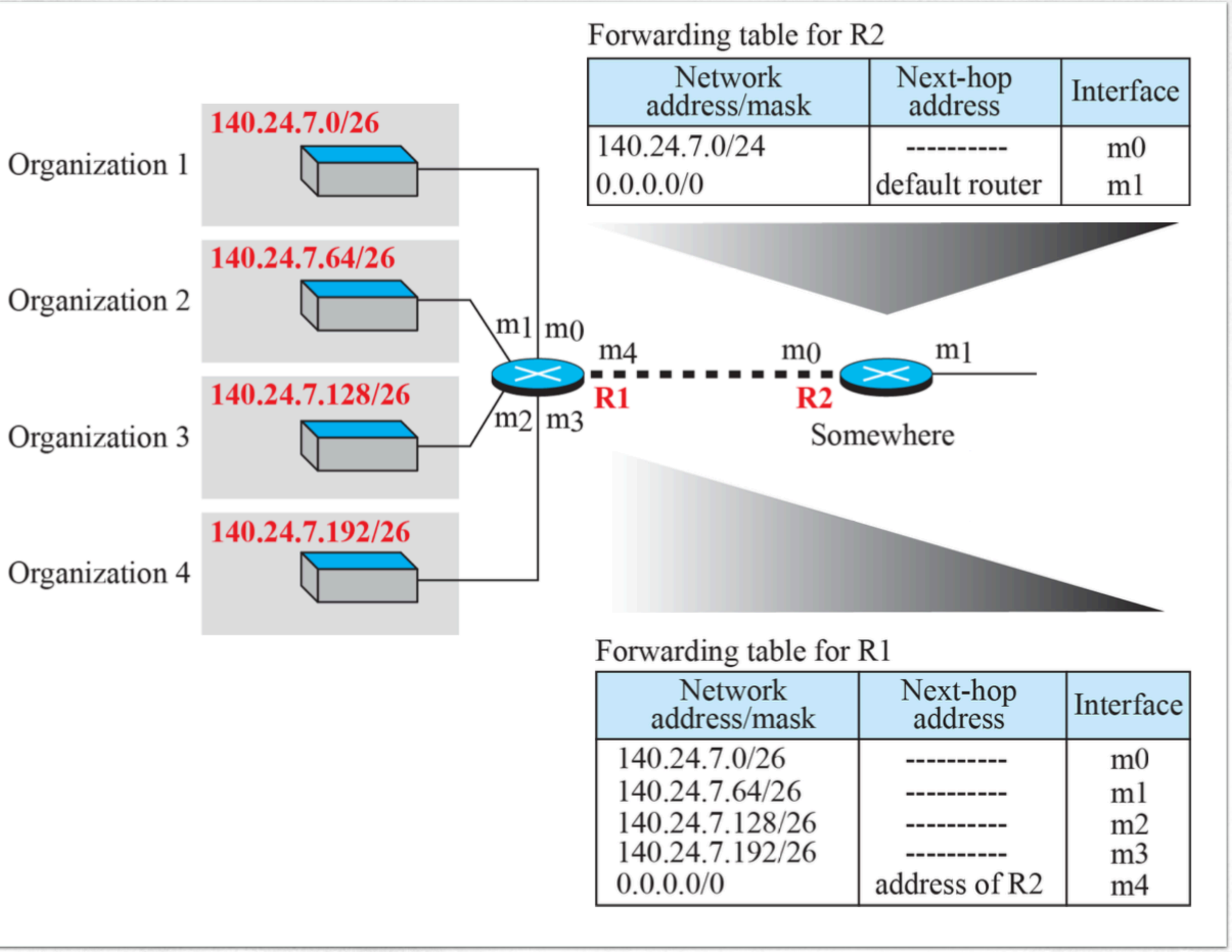
Address translation



Five-column translation table

Private address	*Private port*	*External address*	*External port*	*Transport protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮

Address aggregation



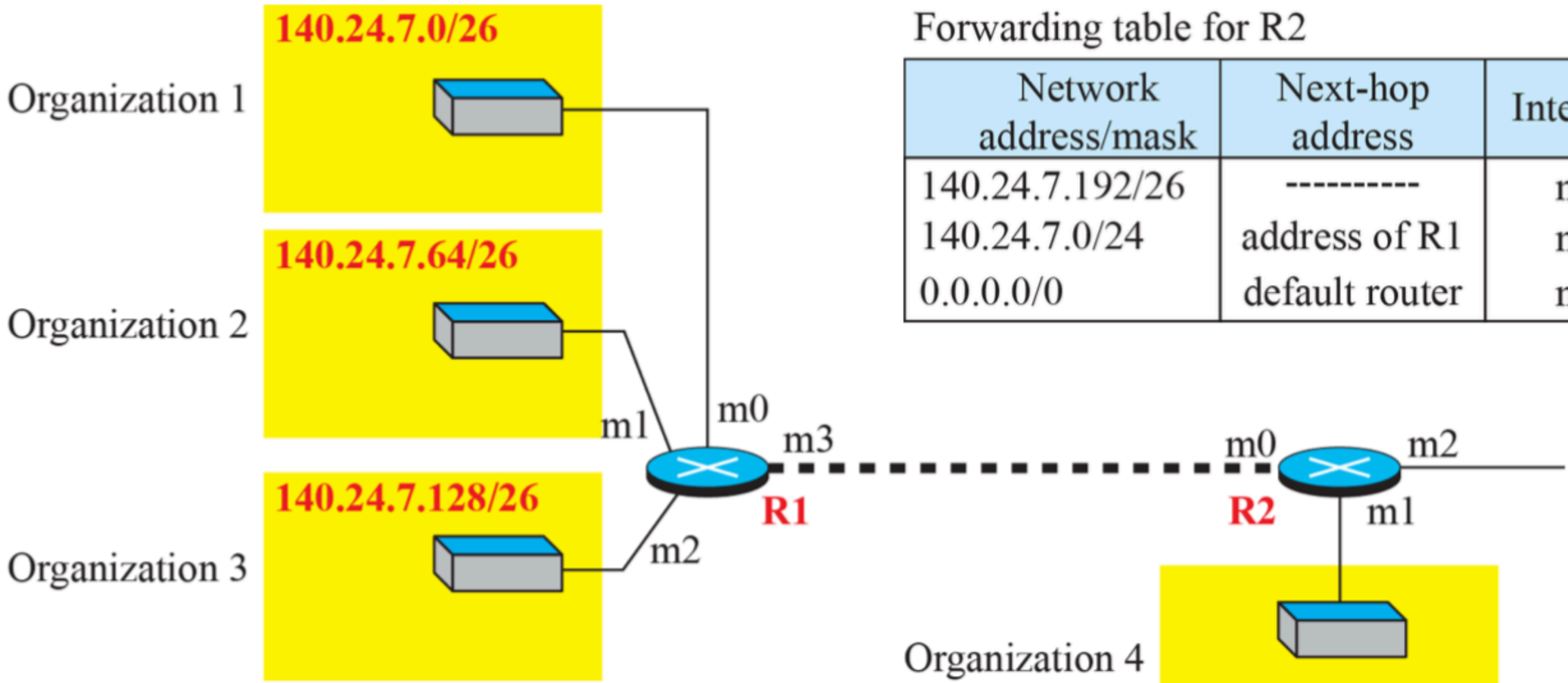
Forwarding table for R2

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

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

Longest mask matching



Forwarding table for R2

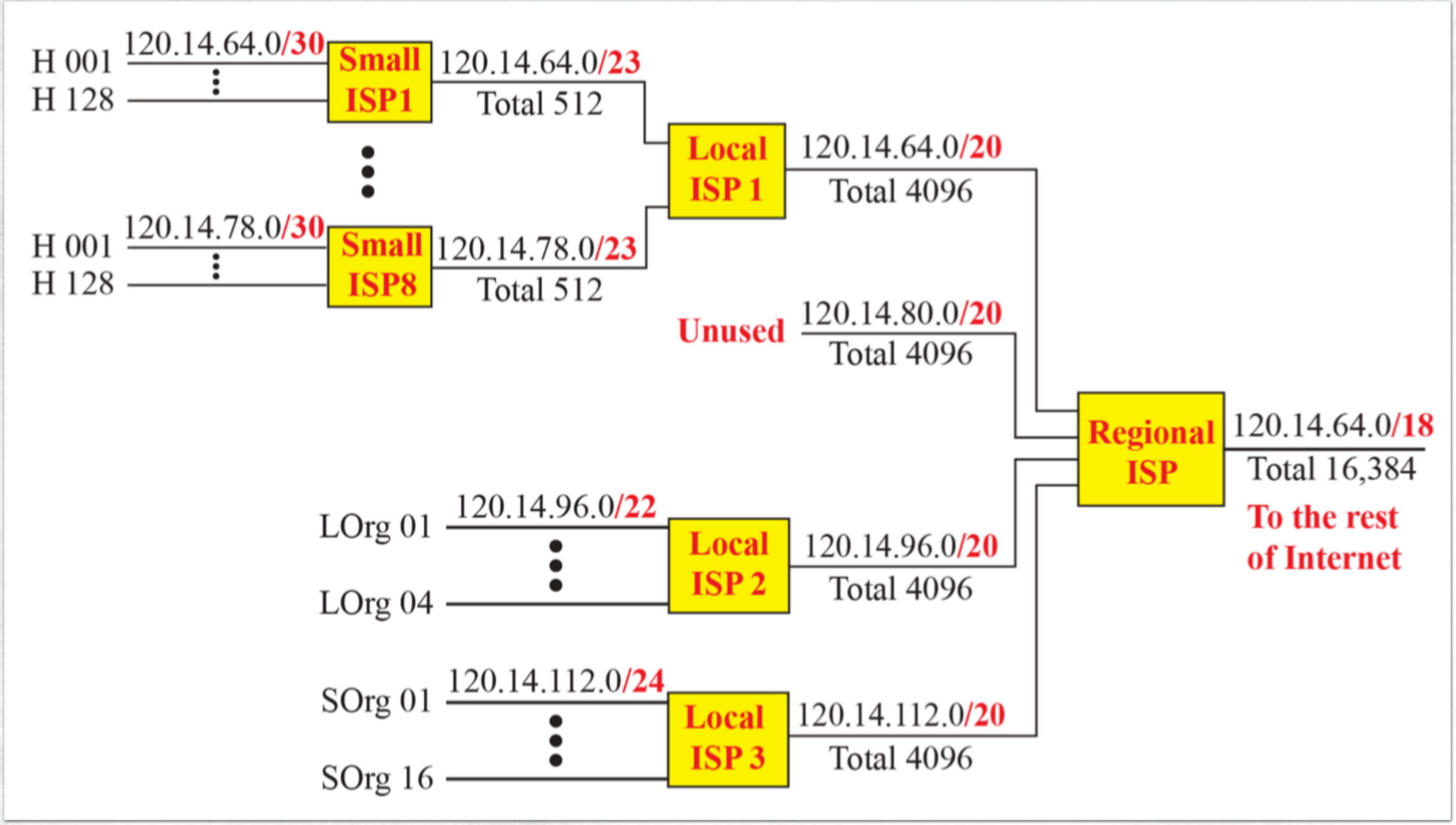
Network address/mask	Next-hop address	Interface
140.24.7.192/26	----------	m1
140.24.7.0/24	address of R1	m0
0.0.0.0/0	default router	m2

Forwarding table for R1

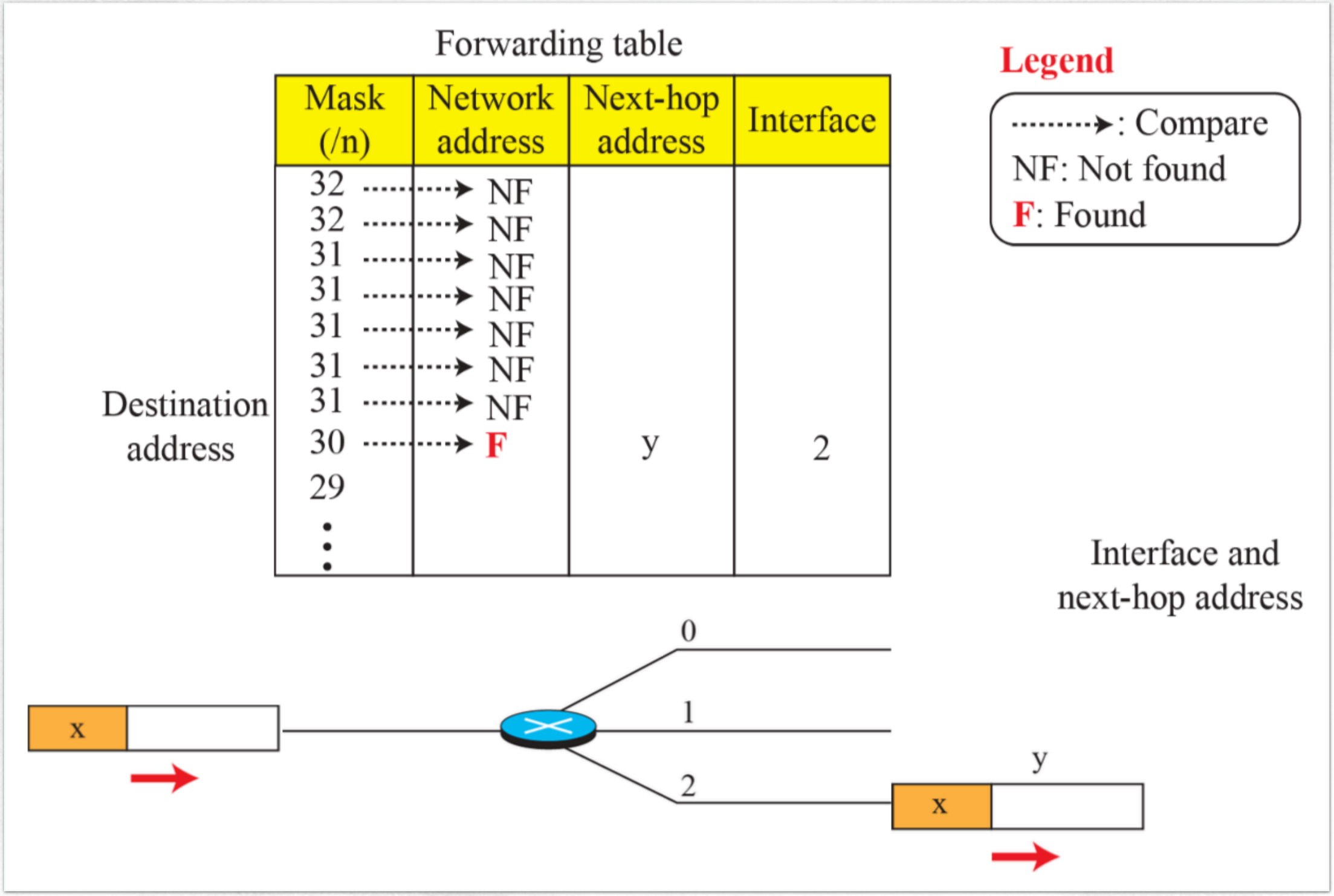
Network address/mask	Next-hop address	Interface
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
0.0.0.0/0	default router	m3

Addressing again

Hierarchical routing with ISPs



Forwarding based on destination address



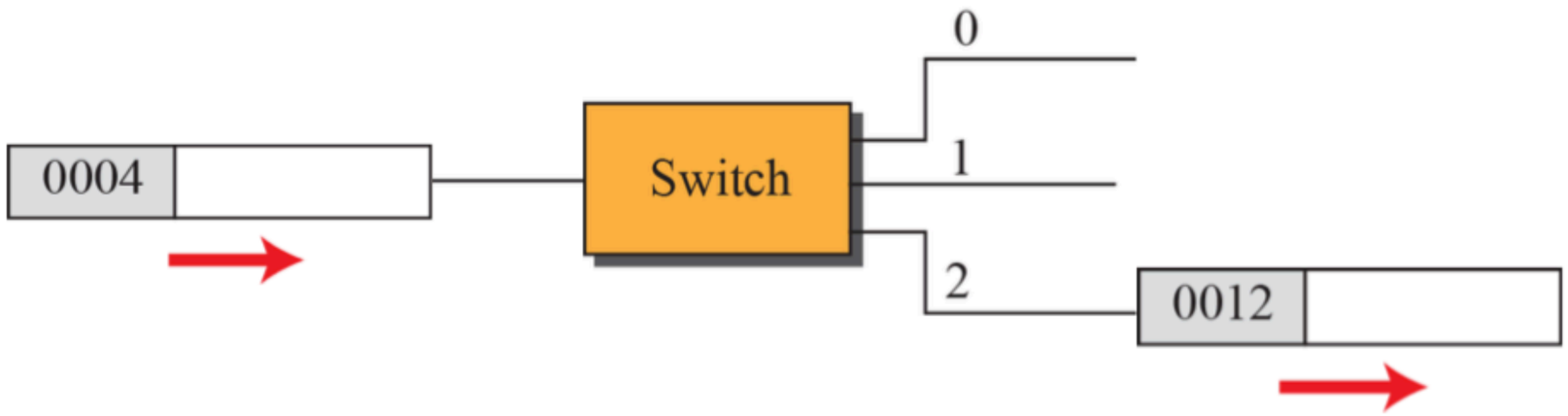
Forwarding based on label

Switching Table

Label used as index	Interface	Next label
0000		
0001		
0002		
0003		
0004	2	0012
0005		
0006		
⋮	⋮	⋮
1000		

Label

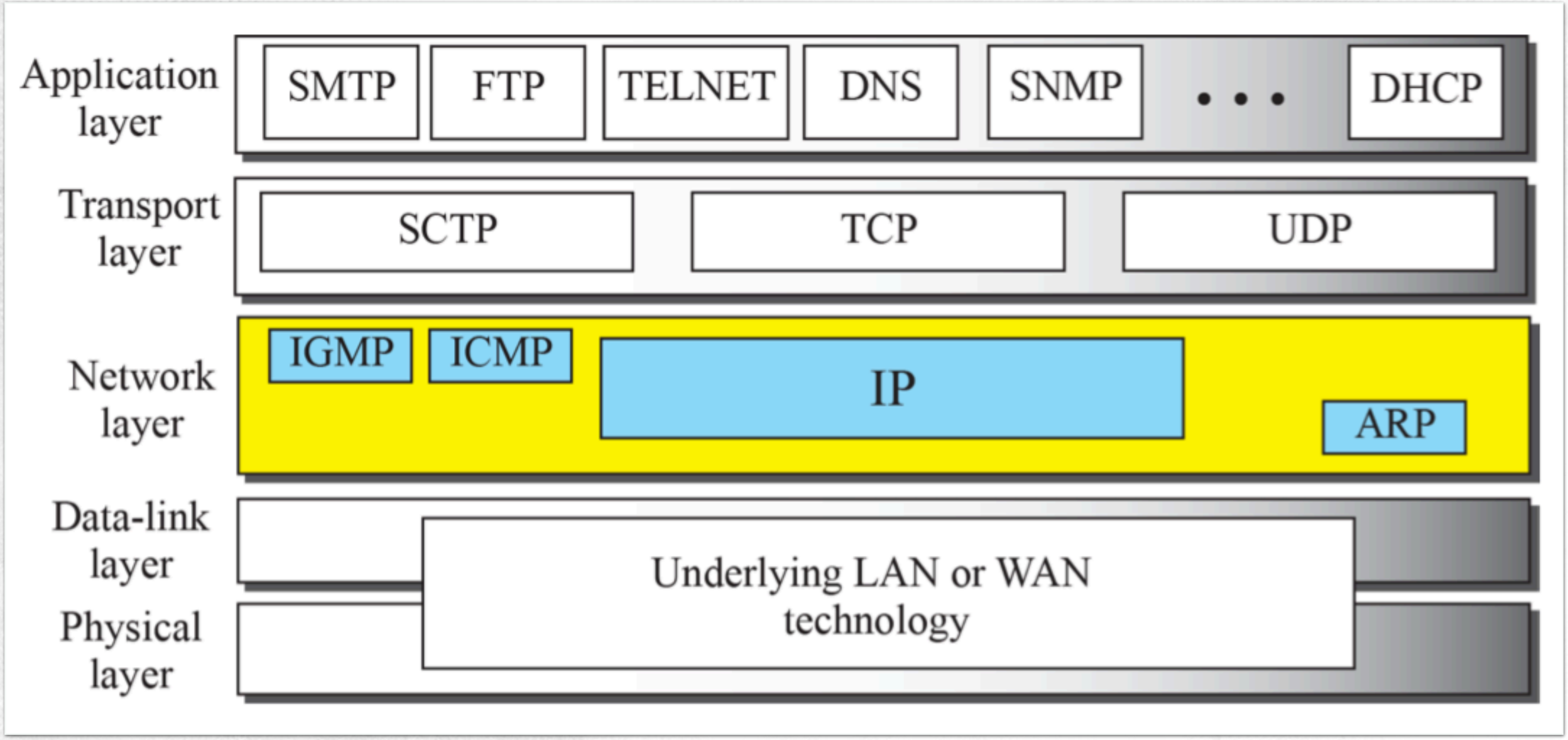
Interface and label address



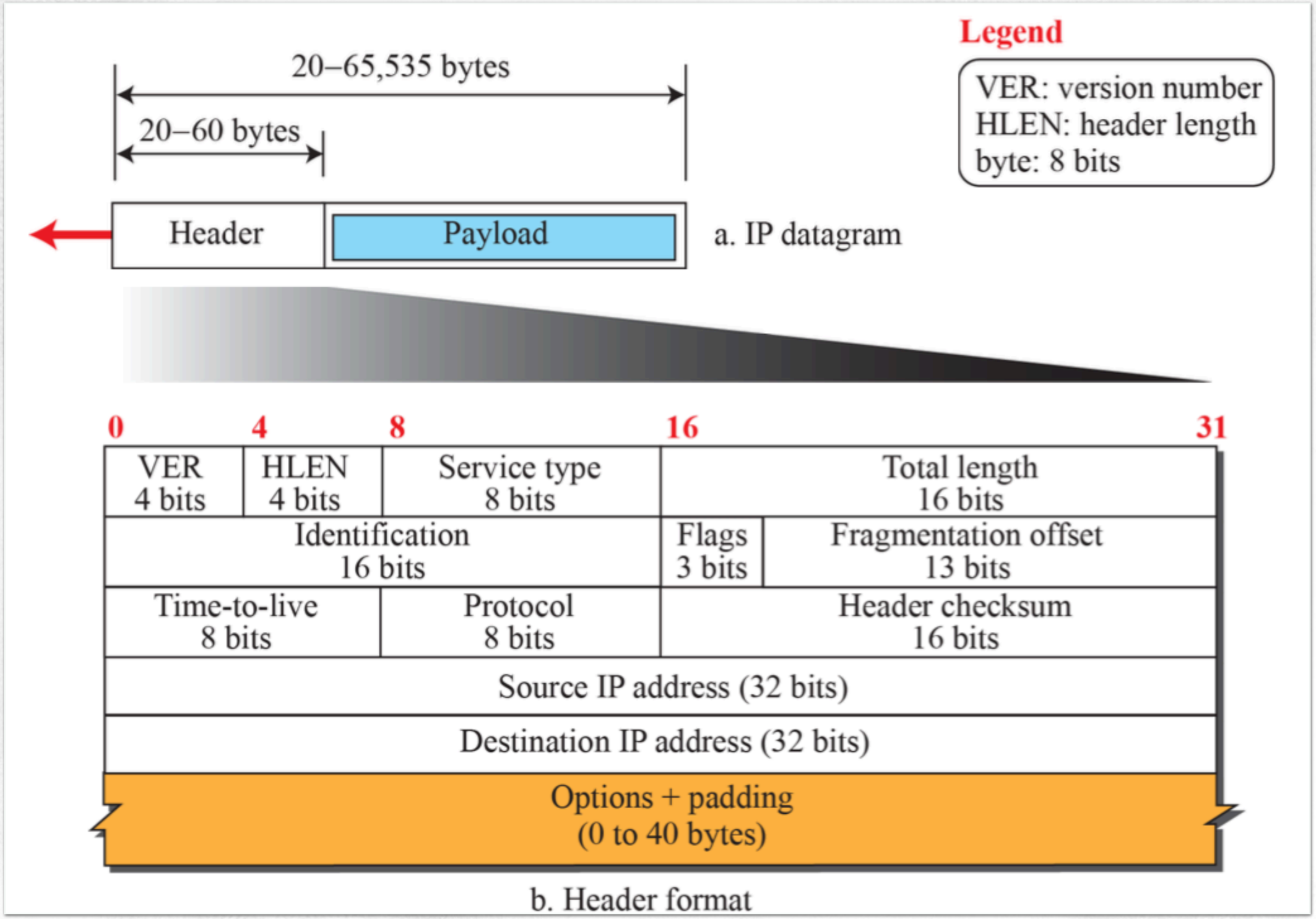
Contents

- Concept
- Datagram and Virtual Circuit
- Network Performance
- Addressing
- More Issues
- **IP Protocol**

Positioning of IP Protocol



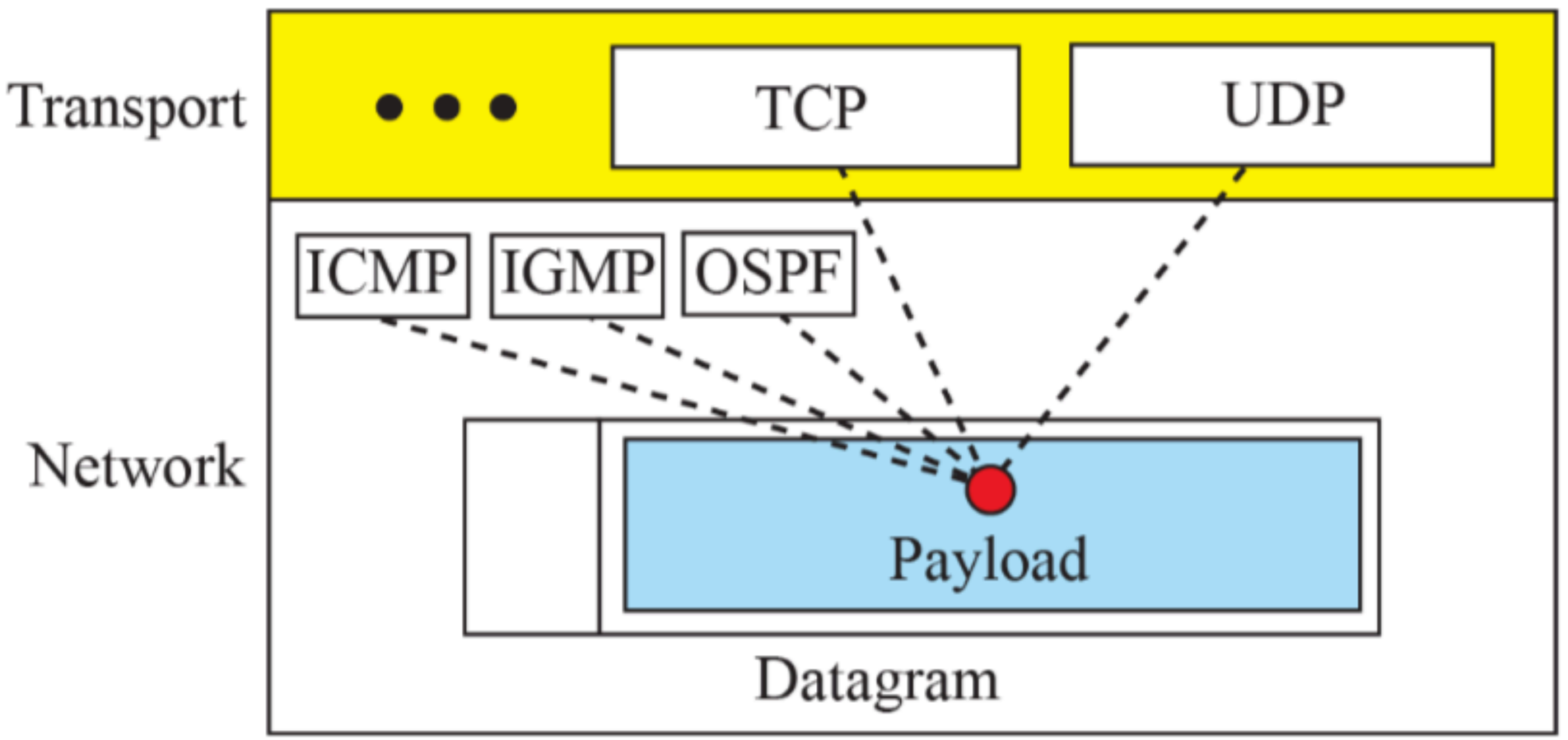
Datagram format



Multiplexing

ICMP: 01	UDP: 17
IGMP: 02	OSPF: 89
TCP: 06	

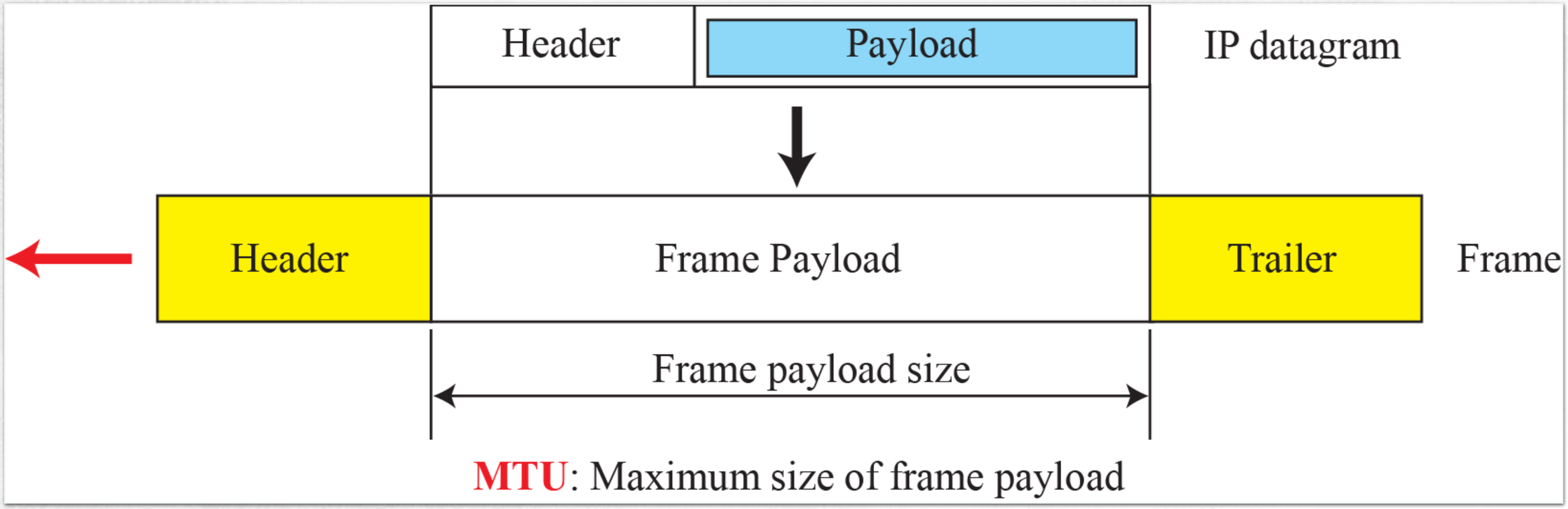
Some protocol values



Fragmentation

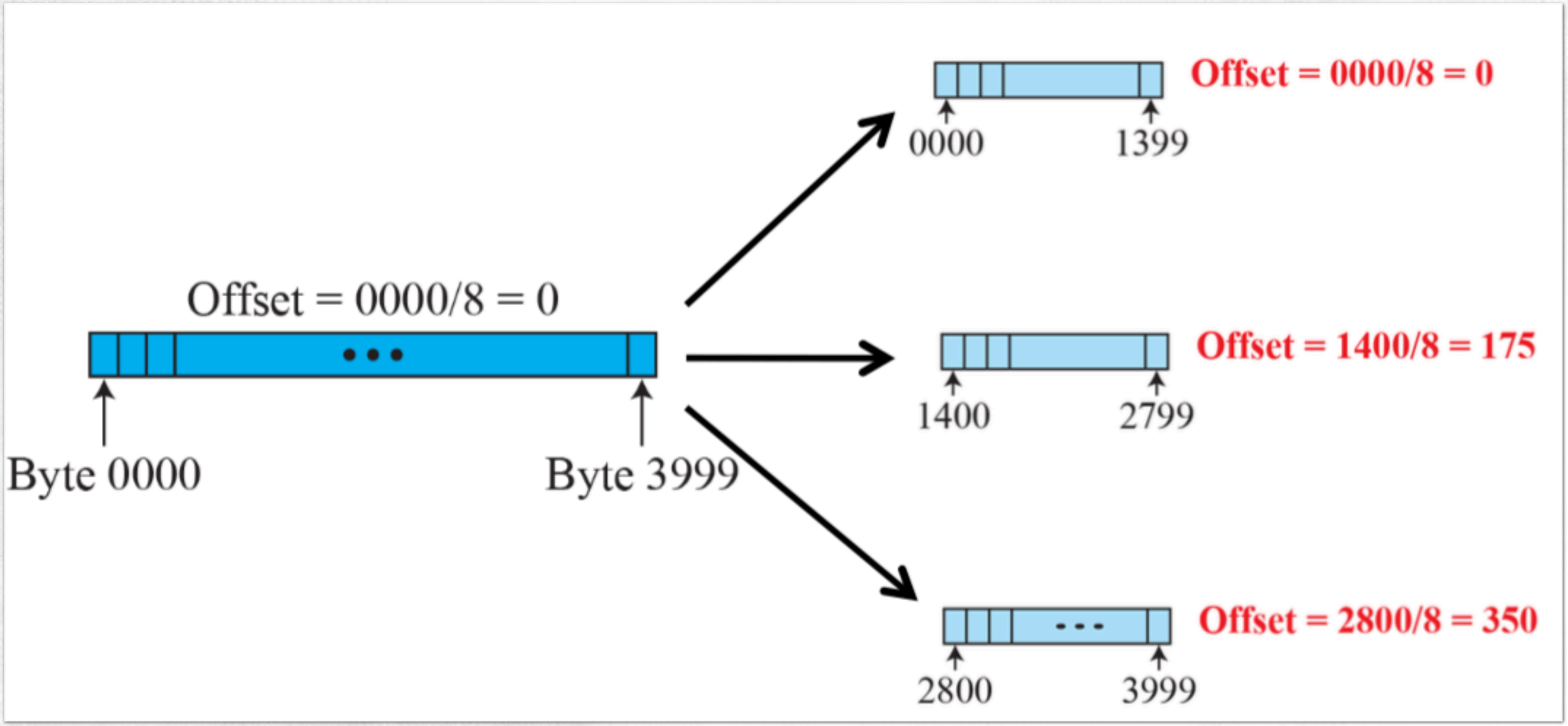
- A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel. For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

Maximum transfer unit (MTU)

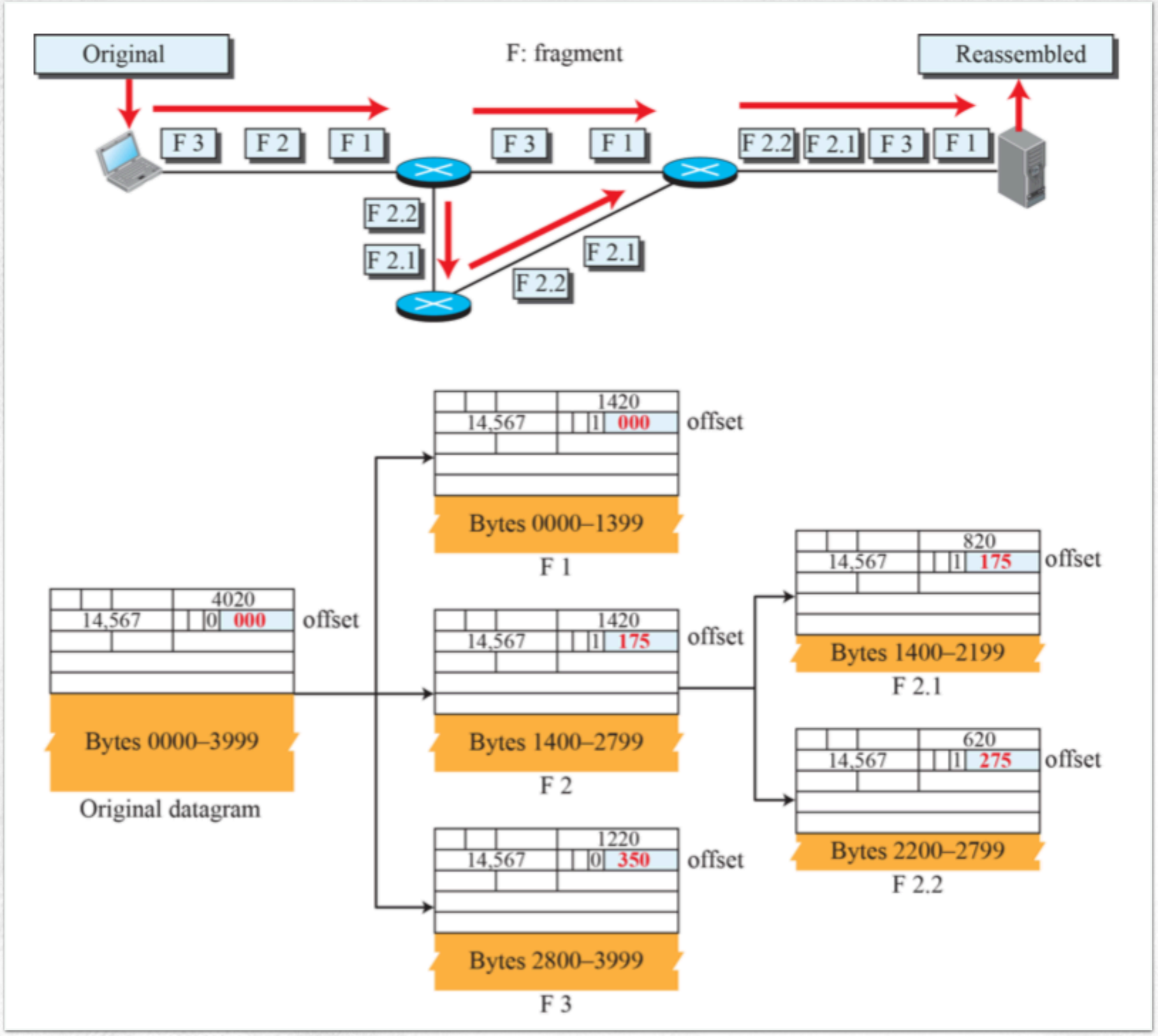


MTU: Maximum size of frame payload

Fragmentation example



Detailed fragmentation example



Security of IPv4 Datagrams

- The IPv4 protocol, as well as the whole Internet, was started when the Internet users trusted each other. No security was provided for the IPv4 protocol. Today, however, the situation is different; the Internet is not secure anymore. There are three security issues that are particularly applicable to the IP protocol: packet sniffing, packet modification, and IP spoofing.

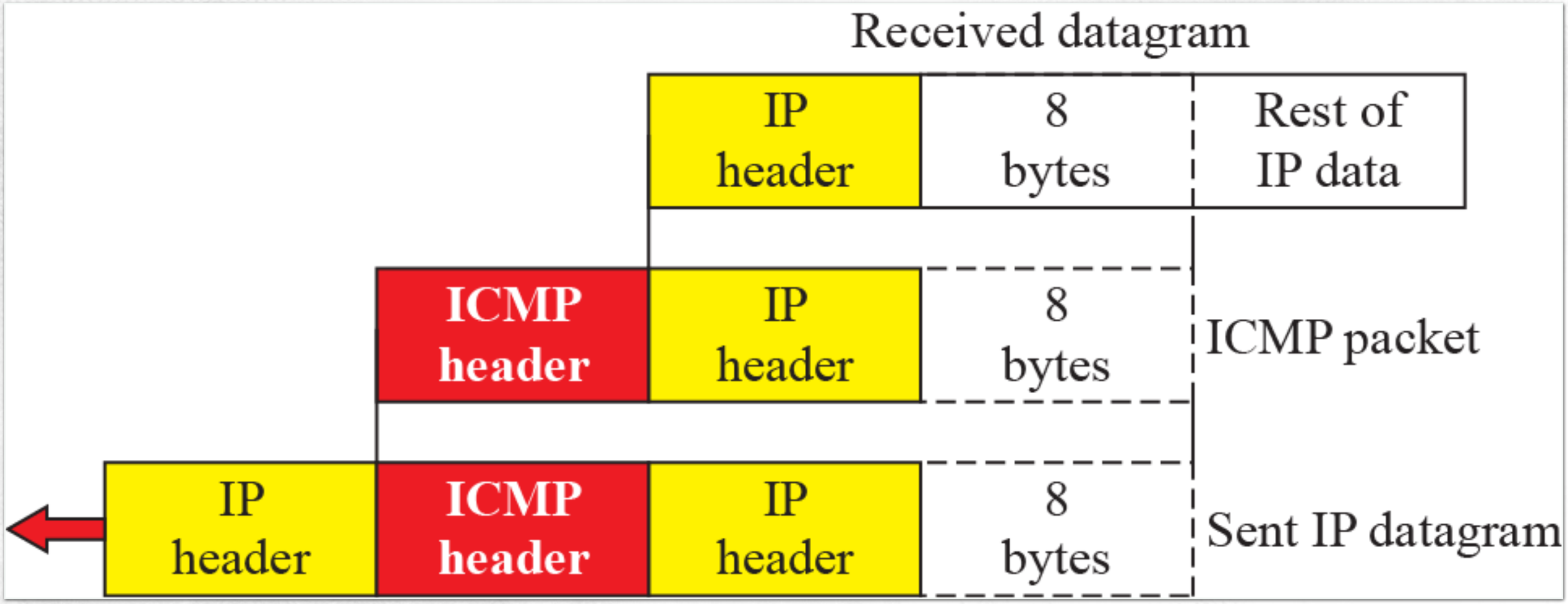
ICMPv4

- The IPv4 has no error-reporting or error- correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol version 4 (ICMPv4) has been designed to compensate for the above two deficiencies.

ICMPv4

- ICMP messages are divided into two broad categories: error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

Contents of data field for the error messages



Debugging using ICMP

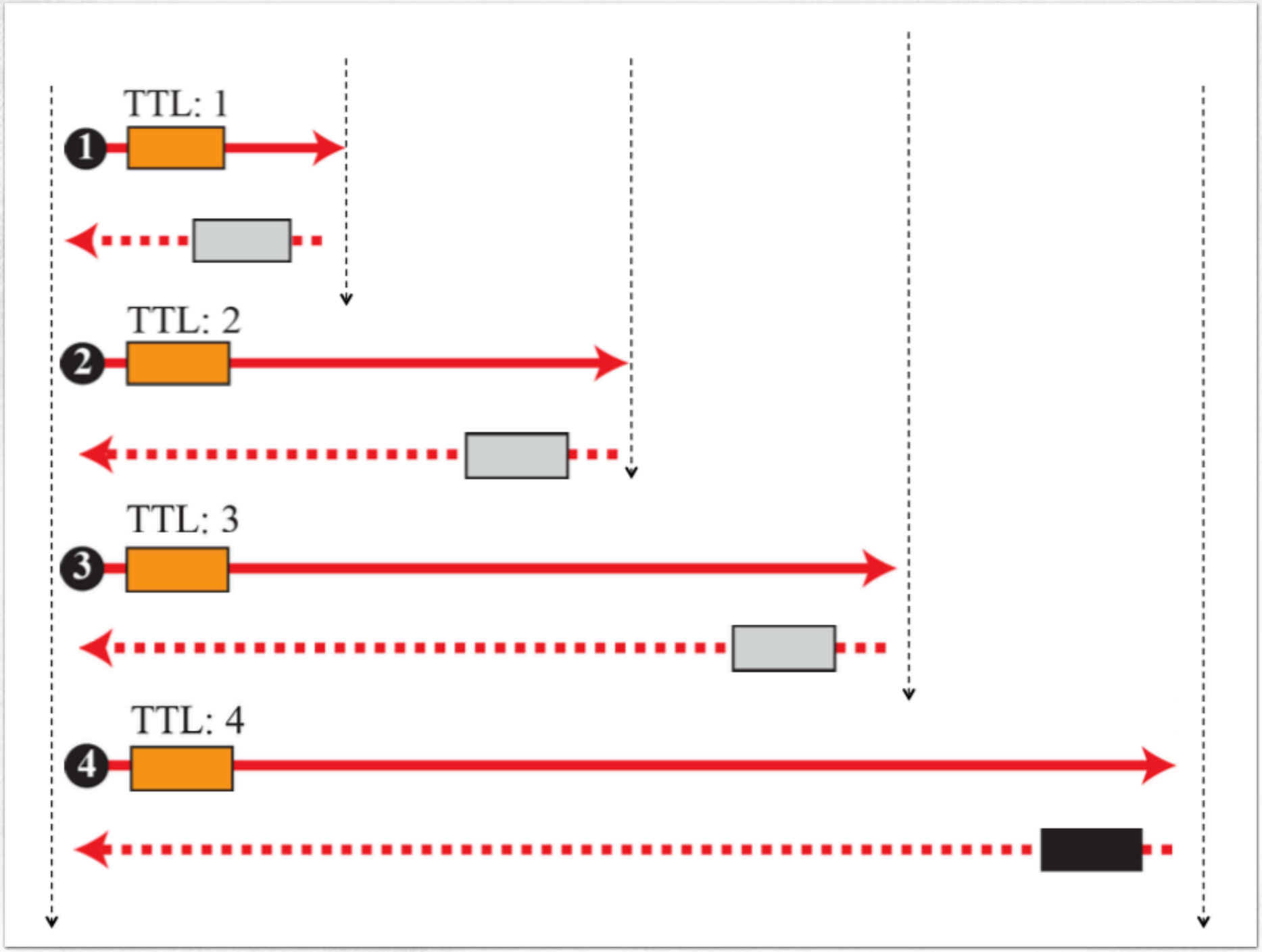
- There are several tools that can be used in the Internet for debugging. We can determine the viability of a host or router. We can trace the route of a packet. We introduce two tools that use ICMP for debugging: ping and traceroute.

Ping

```
$ ping auniversity.edu
PING auniversity.edu (152.181.8.3)   56 (84)  bytes of data.
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=0      ttl=62      time=1.91 ms
```

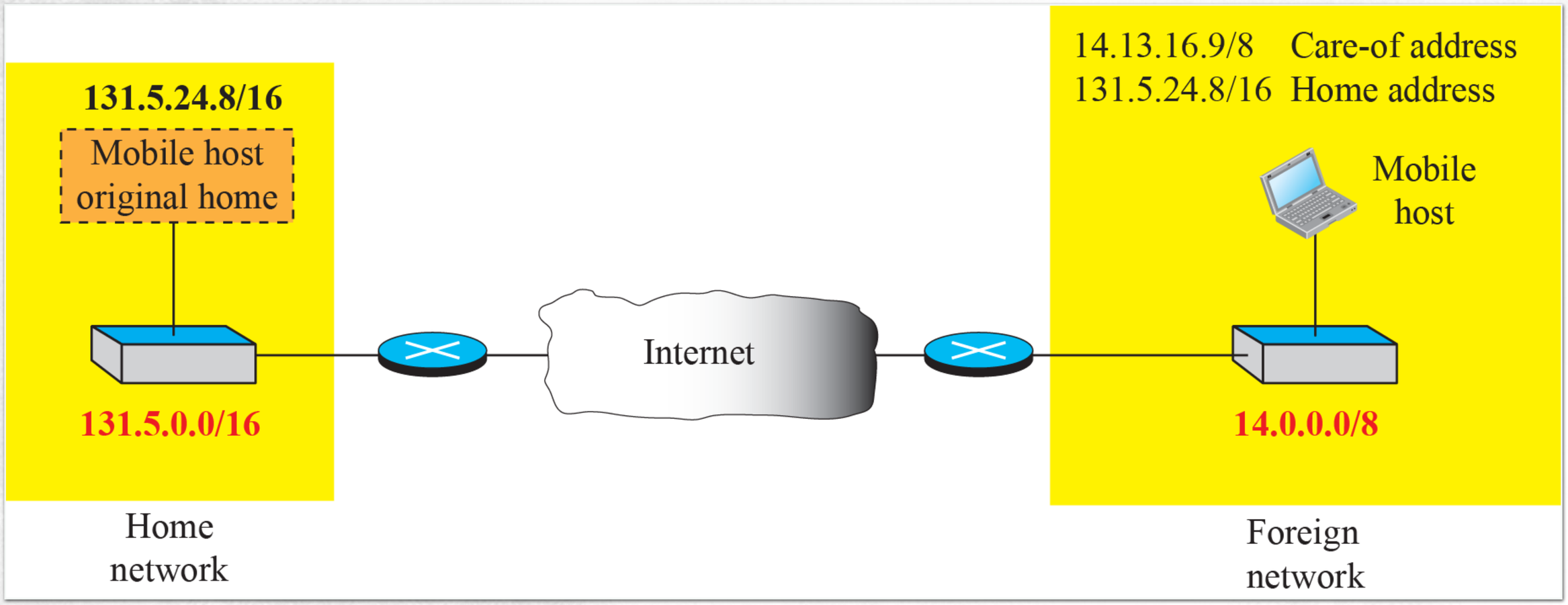
```
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=1      ttl=62      time=2.04 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=2      ttl=62      time=1.90 ms
64 bytes from auniversity.edu (152.181.8.3): icmp_seq=3      ttl=62      time=1.97 ms
64 bytes from auniversity.edu (152.181.8.3): 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



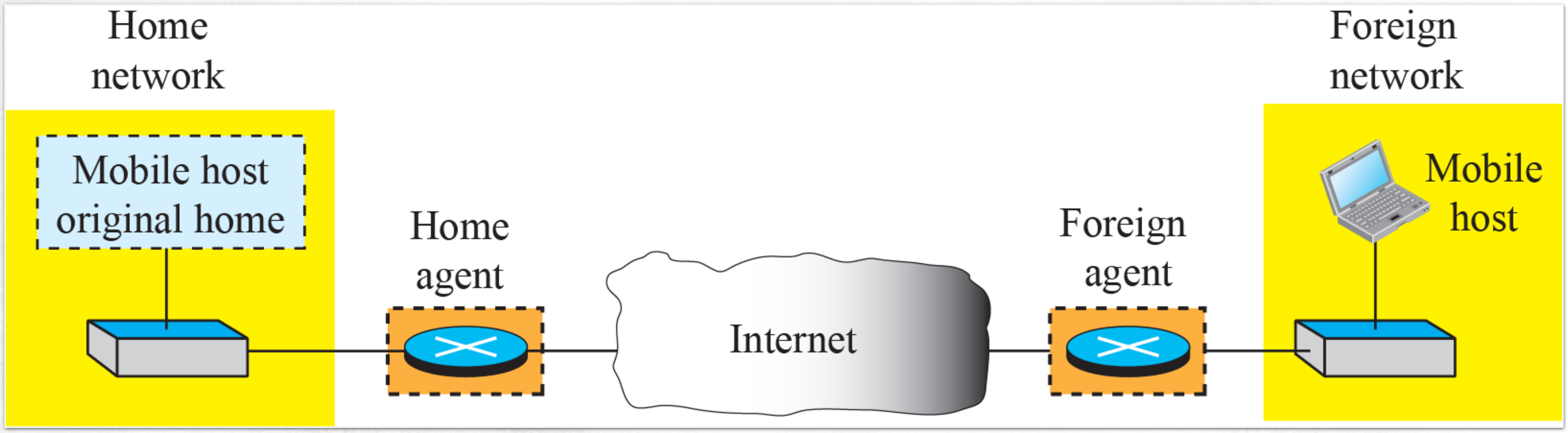
Concept

- The main problem that must be solved in providing mobile communication using the IP protocol is addressing.

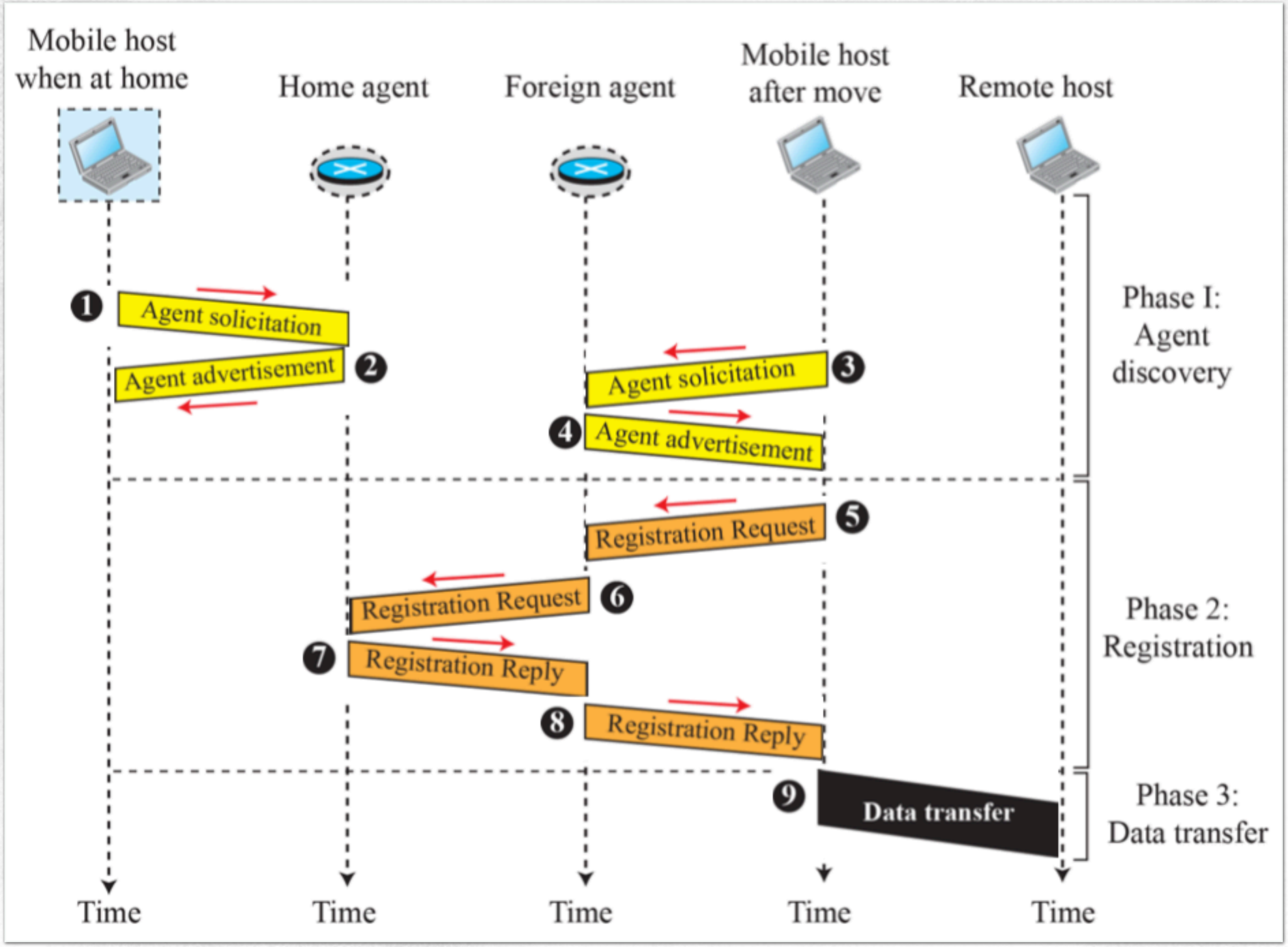


Agents

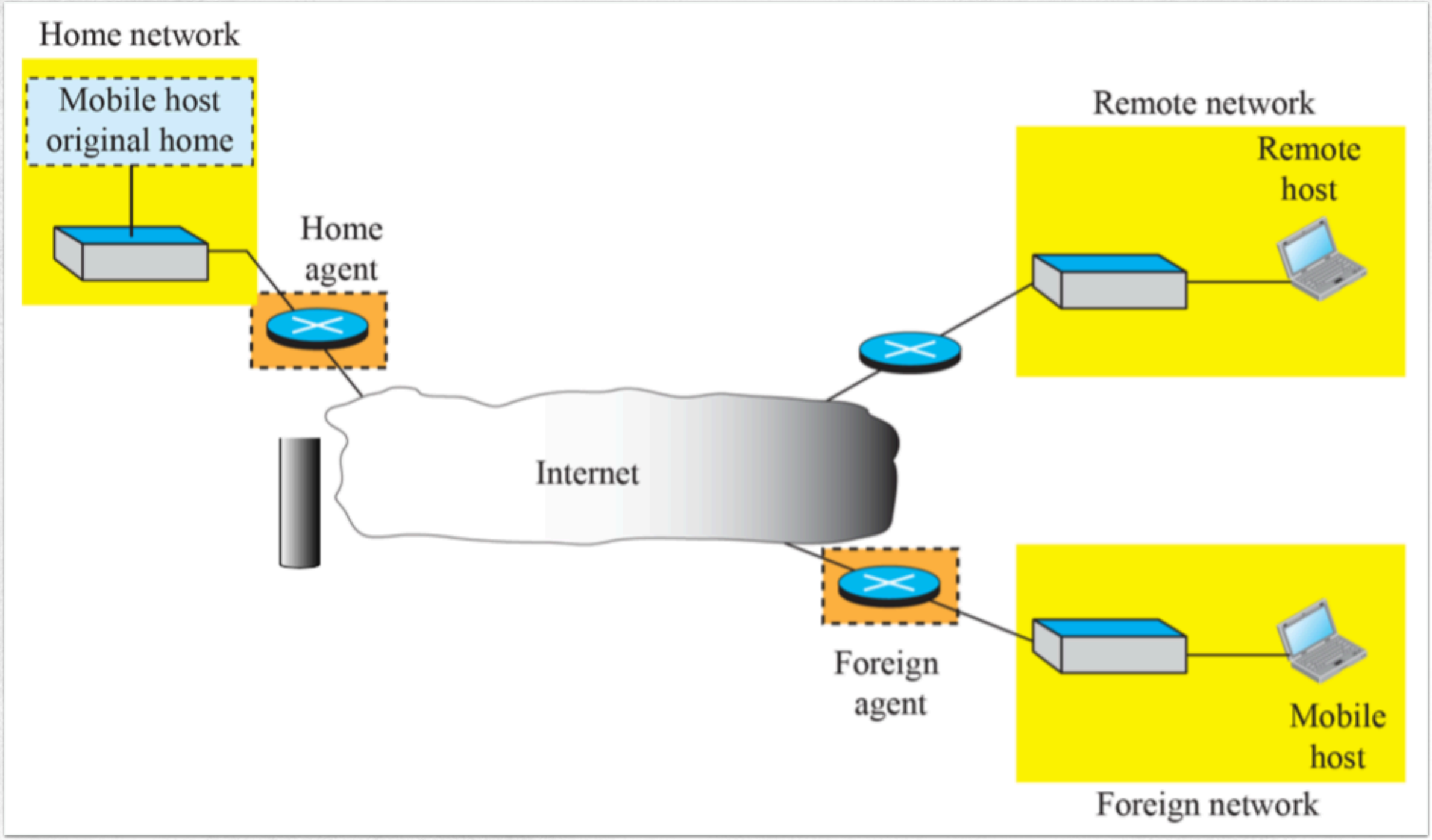
- To make the change of address transparent to the rest of the Internet requires a home agent and a foreign agent. Figure shows the position of a home agent relative to the home network and a foreign agent relative to the foreign network.



Remote host and mobile host communication



Data transfer



Thank you

경희대학교
KYUNG HEE UNIVERSITY