

# IP Version 4 Addressing

# Objectives

- Explain the different classes of IP addresses
- Configure IP addresses
- Subdivide an IP network

# Objectives (continued)

- Discuss advanced routing concepts such as CIDR, summarization, and VLSM
- Convert between decimal, binary, and hexadecimal numbering systems
- Explain the differences between IPv4 and IPv6

# IP Addressing

- An IP address has 32 bits divided into four octets
- To make the address easier to read, people use decimal numbers to represent the binary digits
  - Example: 192.168.1.1
- Dotted decimal notation
  - When binary IP addresses are written in decimal format



# IP Addressing (continued)

	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
1	0	0	0	0	0	0	0	1
255	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0

**Table 4-1** Binary to decimal conversion

# MAC to IP Address Comparison

- MAC address
  - Identifies a specific NIC in a computer on a network
  - Each MAC address is unique
  - TCP/IP networks can use MAC addresses in communication
- Network devices cannot efficiently route traffic using MAC addresses because they:
  - Are not grouped logically
  - Cannot be modified
  - Do not give information about physical or logical network configuration

# MAC to IP Address Comparison (continued)

- **IP addressing**
  - Devised for use on large networks
- IP addresses have a hierarchical structure and do provide logical groupings
  - IP address identifies both a network and a host

# IP Classes

- **Internet Assigned Numbers Authority (IANA)**
  - Devised the hierarchical IP addressing structure
- **American Registry of Internet Numbers (ARIN)**
  - Manages IP addresses in the United States
- **Internet Corporation for Assigned Names and Numbers (ICANN)**
  - A global, government-independent entity with overall responsibility for the Internet
  - ICANN has effectively replaced IANA

# IP Classes (continued)

- Class A
  - Reserved for governments and large corporations throughout the world
  - Each Class A address supports 16,777,214 hosts
- Class B
  - Addresses are assigned to large- and medium-sized companies
  - Each Class B address supports 65,534 hosts

# IP Classes (continued)

Binary Place Values								Decimal Equivalent	Description
128	64	32	16	8	4	2	1		
0	0	0	0	0	0	0	0	= 0	Subnet identifier
0	0	0	0	0	0	0	1	= 1	Bottom of Class A range
0	1	1	1	1	1	1	0	= 126	Top of Class A range
0	1	1	1	1	1	1	1	= 127	Loopback address

**Figure 4-1** Class A addresses begin with a number between 1 and 126

Binary Place Values								Decimal Equivalent	Description
128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	= 128	First Class B address
1	0	1	1	1	1	1	1	= 191	Last Class B address

**Figure 4-2** Class B addresses begin with a number between 128 and 191

# IP Classes (continued)

- Class C
  - Addresses are assigned to groups that do not meet the qualifications to obtain Class A or B addresses
  - Each Class C address supports 254 hosts
- Class D
  - Addresses (also known as multicast addresses) are reserved for multicasting
  - **Multicasting** is the sending of a stream of data (usually audio and video) to multiple computers simultaneously

# IP Classes (continued)

Binary Place Values								Decimal Equivalent	Description
128	64	32	16	8	4	2	1		
1	1	0	0	0	0	0	0	= 192	First Class C address
1	1	0	1	1	1	1	1	= 223	Last Class C address

**Figure 4-3** Class C addresses begin with numbers between 192 and 223

Binary Place Values								Decimal Equivalent	Description
128	64	32	16	8	4	2	1		
1	1	1	0	0	0	0	0	= 224	First Class D address
1	1	1	0	1	1	1	1	= 239	Last Class D address

**Figure 4-4** Class D addresses begin with a number between 224 and 239



# IP Classes (continued)

- Class E
  - Addresses are reserved for research, testing, and experimentation
  - The Class E range starts where Class D leaves off
- Private IP ranges
  - Many companies use private IP addresses for their internal networks
    - Will not be routable on the Internet
  - Gateway devices have network interface connections to the internal network and the Internet
    - Route packets between them

# IP Classes (continued)

Binary Place Values								Decimal Equivalent	Description
128	64	32	16	8	4	2	1		
1	1	1	1	0	0	0	0	= 240	First Class E address
1	1	1	1	1	1	1	1	= 255	Last Class E address

**Figure 4-5** Class E addresses begin with a number between 240 and 255

Class	Private Address Range
A	10.x.x.x
B	172.16.x.x – 172.31.x.x
C	192.168.x.x

**Table 4-2** The private IP ranges

# Network Addressing

- IP addresses identify both the network and the host
  - The division between the two is not specific to a certain number of octets
- **Subnet mask**
  - Indicates how much of the IP address represents the network or subnet
- Standard (default) subnet masks:
  - Class A subnet mask is 255.0.0.0
  - Class B subnet mask is 255.255.0.0
  - Class C subnet mask is 255.255.255.0

# Subnetting in IP Version 4

## **Classful Subnetting**

# Network Addressing

- IP addresses identify both the network and the host
  - The division between the two is not specific to a certain number of octets
- **Subnet mask**
  - Indicates how much of the IP address represents the network or subnet
- Standard (default) subnet masks:
  - Class A subnet mask is 255.0.0.0
  - Class B subnet mask is 255.255.0.0
  - Class C subnet mask is 255.255.255.0

# Network Addressing (continued)

- TCP/IP hosts use the combination of the IP address and the subnet mask
  - To determine if other addresses are local or remote
  - The binary AND operation is used to perform the calculation
- **Subnetting**
  - Manipulation of the subnet mask to get more network numbers

```
Source IP:      64.168.1.1      01000000.10101000.00000001.00000001
Subnet mask:    255.255.255.0    11111111.11111111.11111111.00000000
ANDing result:  64.168.1.0      01000000.10101000.00000001.00000000
```

```
Destination IP: 64.168.5.7      01000000.10101000.00000101.00000111
Subnet mask      255.255.255.0  11111111.11111111.11111111.00000000
ANDing result:   64.168.5.0      01000000.10101000.00000101.00000000
```

When the mask 255.255.255.0 is used the hosts are remote.

```
Source IP:      64.168.1.1      01000000.10101000.00000001.00000001
Subnet mask:    255.255.0.0      11111111.11111111.00000000.00000000
ANDing result:  64.168.1.0      01000000.10101000.00000000.00000000
```

```
Destination IP: 64.168.5.7      01000000.10101000.00000101.00000111
Subnet mask      255.255.0.0      11111111.11111111.00000000.00000000
ANDing result:   64.168.5.0      01000000.10101000.00000000.00000000
```

When the mask 255.255.0.0 is used the hosts are local.

**Figure 4-6** ANDing operations

# Network Addressing (continued)

- Subnet address
  - Network is identified by the first, or first few, octets
  - A TCP/IP host must have a nonzero host identifier
- Broadcast address
  - When the entire host portion of an IP address is all binary ones
  - Examples: 190.55.255.255 and 199.192.65.63



# Network Addressing (continued)

Subnet ID:	199.192.65.0	11000111.11000000.01000001.00000000
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
Broadcast Address:	199.192.65.255	11000111.11000000.01000001.11111111

**Figure 4-7** Broadcast addresses

Subnet ID:	199.192.65.32	11000111.11000000.01000001.00100000
Subnet mask:	255.255.255.224	11111111.11111111.11111111.11100000
Broadcast Address:	199.192.65.63	11000111.11000000.01000001.00111111

**Figure 4-8** Broadcasts on partially masked octets

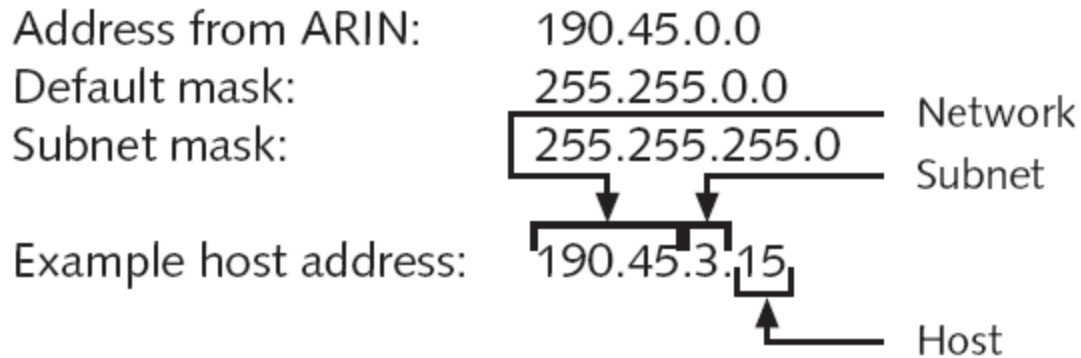
# Broadcast Types

- **Flooded broadcasts**
  - Broadcasts for any subnet
  - Use the IP address 255.255.255.255
  - A router does not propagate flooded broadcasts because they are considered local
- **Directed broadcasts** are for a specific subnet
  - Routers can forward directed broadcasts
  - For example, a packet sent to the Class B address 129.30.255.255 would be a broadcast for network 129.30.0.0

# Subdividing IP Classes

- Reasons for subnetting
  - To match the physical layout of the organization
  - To match the administrative structure of the organization
  - To plan for future growth
  - To reduce network traffic

# Subdividing IP Classes (continued)



**Figure 4-9** Dividing a Class B network

# Subnet Masking

- When network administrators create subnets
  - They borrow bits from the original host field to make a set of subnetworks
  - The number of borrowed bits determines how many subnetworks and hosts will be available
- Class C addresses also can be subdivided
  - Not as many options or available masks exist because only the last octet can be manipulated with this class

Subnet Mask	Subnets on Network	Hosts per Subnet
255.255.128.0	2	32,766
255.255.192.0	4	16,382
255.255.224.0	8	8,190
255.255.240.0	16	4,094
255.255.248.0	32	2,046
255.255.252.0	64	1,022
255.255.254.0	128	510
255.255.255.0	256	254
255.255.255.128	512	126
255.255.255.192	1,024	62
255.255.255.224	2,048	30
255.255.255.240	4,096	14
255.255.255.248	8,192	6
255.255.255.252	16,384	2

**Table 4-3** Class B subnet masks

# Subnet Masking (continued)

Subnet Mask	Subnets on Network	Hosts per Subnet
255.255.255.128	2	126
255.255.255.192	4	62
255.255.255.224	8	30
255.255.255.240	16	14
255.255.255.248	32	6
255.255.255.252	64	2

**Table 4-4** Class C subnet masks

# Subnet Masking (continued)

Binary Place Values	128	64	32	16	8	4	2	1	Decimal Equivalents
	1	0	0	0	0	0	0	0	=128
	1	1	0	0	0	0	0	0	=192
	1	1	1	0	0	0	0	0	=224
Binary Digits	1	1	1	1	0	0	0	0	=240
	1	1	1	1	1	0	0	0	=248
	1	1	1	1	1	1	0	0	=252
	1	1	1	1	1	1	1	0	=254
	1	1	1	1	1	1	1	1	=255

**Figure 4-10** Subnet mask values



# Learning to Subnet

- Suppose you had a network with:
  - Five different segments
  - Somewhere between 15 and 20 TCP/IP hosts on each network segment
- You just received your Class C address from ARIN (199.1.10.0)
- Only one subnet mask can handle your network configuration: 255.255.255.224
  - This subnet mask will allow you to create eight subnetworks and to place up to 30 hosts per network

# Learning to Subnet (continued)

- Determine the subnet identifiers (IP addresses)
  - Write the last masking octet as a binary number
  - Determine the binary place of the last masking digit
- Calculate the subnets
  - Begin with the major network number (subnet zero) and increment by 32
  - Stop counting when you reach the value of the mask
- Determine the valid ranges for your hosts on each subnet
  - Take the ranges between each subnet identifier
  - Remove the broadcast address for each subnet

# Learning to Subnet (continued)

Class C Address: 199.1.10.0  
Standard Mask: 255.255.255.0  
Selected Mask: 255.255.255.224

	128	64	32	16	8	4	2	1
224	1	1	1	0	0	0	0	0

**Figure 4-11** Subnet masking example

# Learning to Subnet (continued)

Subnet Identifier	Valid Host Range	Broadcast Address for Subnet
199.1.10.0	199.1.10.1 – 199.1.10.30	199.1.10.31
199.1.10.32	199.1.10.33 – 199.1.10.62	199.1.10.63
199.1.10.64	199.1.10.65 – 199.1.10.94	199.1.10.95
199.1.10.96	199.1.10.97 – 199.1.10.126	199.1.10.127
199.1.10.128	199.1.10.129 – 199.1.10.158	199.1.10.159
199.1.10.160	199.1.10.161 – 199.1.10.190	199.1.10.191
199.1.10.192	199.1.10.193 – 199.1.10.222	199.1.10.223
199.1.10.224	199.1.10.225 – 199.1.10.254	199.1.10.255

**Table 4-5** Class C address 199.1.10.0 masking 255.255.255.224

# Learning to Subnet (continued)

Binary			Binary		
Decimal	0	00000000	Decimal	32	00100000
Mask	224	11100000	Mask	224	11100000
Decimal	64	01000000	Decimal	96	01100000
Mask	224	11100000	Mask	224	11100000
Decimal	128	10000000	Decimal	160	10100000
Mask	224	11100000	Mask	224	11100000
Decimal	192	11000000	Decimal	224	11100000
Mask	224	11100000	Mask	224	11100000

**Figure 4-12** A binary look at the mask

# Subnetting Formulas

- Consider memorizing the following two formulas:
  - $2^y = \#$  of usable subnets (where  $y$  is the number of bits borrowed)
  - $2^x - 2 = \#$  of usable hosts per subnet (where  $x$  is the number of bits remaining in the host field after borrowing)

# Subnetting Formulas (continued)

C Address	199.4.10.0	11000111.11000000.01000001.00000000
Standard mask	255.255.255.0	11111111.11111111.11111111.00000000
Mask	255.255.255.240	11111111.11111111.11111111.11110000

y = 4 (borrowed bits)

x = 4 (bits left in host field after borrowing)

Formulas:

$2^y =$  # of usable subnets

$2^x - 2 =$  # of usable hosts per subnet

$2^4 =$  16 usable subnets

$2^4 - 2 =$  14 usable hosts per subnet

**Figure 4-13** Sample calculation using formulas

# Subnetting Formulas (continued)

	128	64	32	16	8	4	2	1
240	1	1	1	1	0	0	0	0

Below is a list of the last octets for the 16 subnets created from network number 199.4.10.0 with the subnet mask 255.255.255.240

0	128
16	144
32	160
48	176
64	192
80	208
96	224
112	240

↑  
Subnetwork numbers will increment by 16, as it is the decimal equivalent of the right-most significant digit in the mask

**Figure 4-14** 255.255.255.240 subnet mask



## *EXAMPLE 1*

*Given the address 23.56.7.91, find the beginning address (network address).*

### **Solution**

**The default mask is 255.0.0.0, which means that only the first byte is preserved and the other 3 bytes are set to 0s. The network address is **23.0.0.0**.**

## *EXAMPLE 2*

*Given the address 132.6.17.85, find the beginning address (network address).*

### **Solution**

***The default mask is 255.255.0.0, which means that the first 2 bytes are preserved and the other 2 bytes are set to 0s. The network address is 132.6.0.0.***

### *EXAMPLE 3*

*Given the address 201.180.56.5, find the beginning address (network address).*

### **Solution**

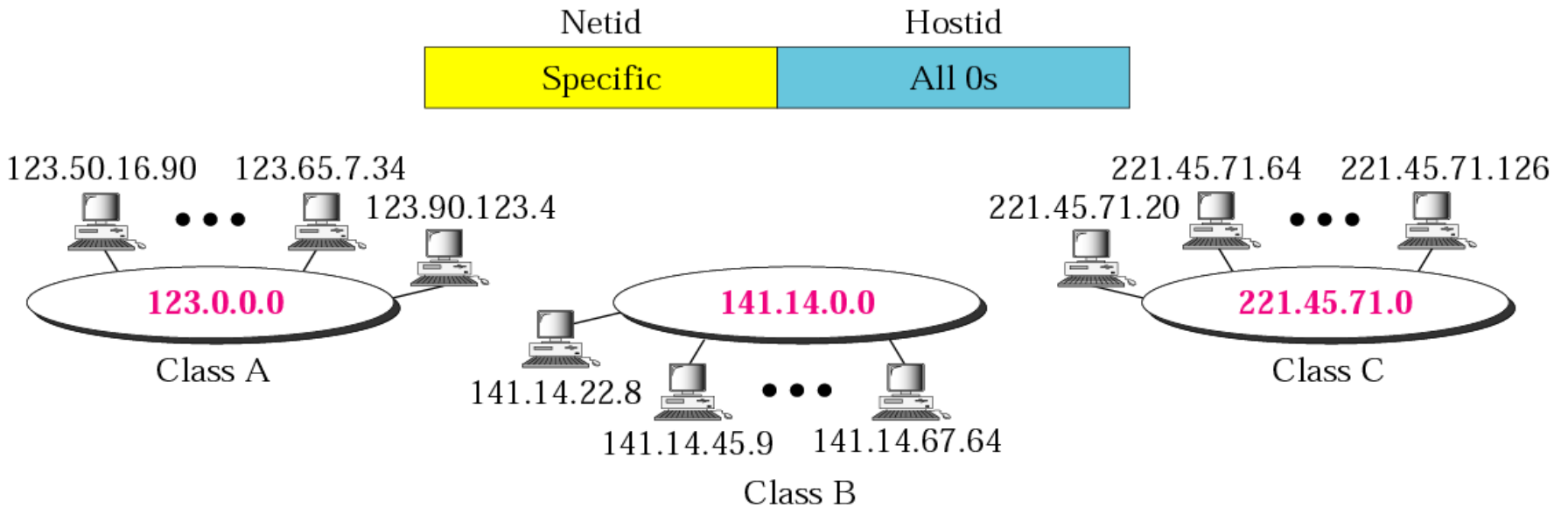
**The default mask is 255.255.255.0, which means that the first 3 bytes are preserved and the last byte is set to 0. The network address is 201.180.56.0.**

# Special Addressing

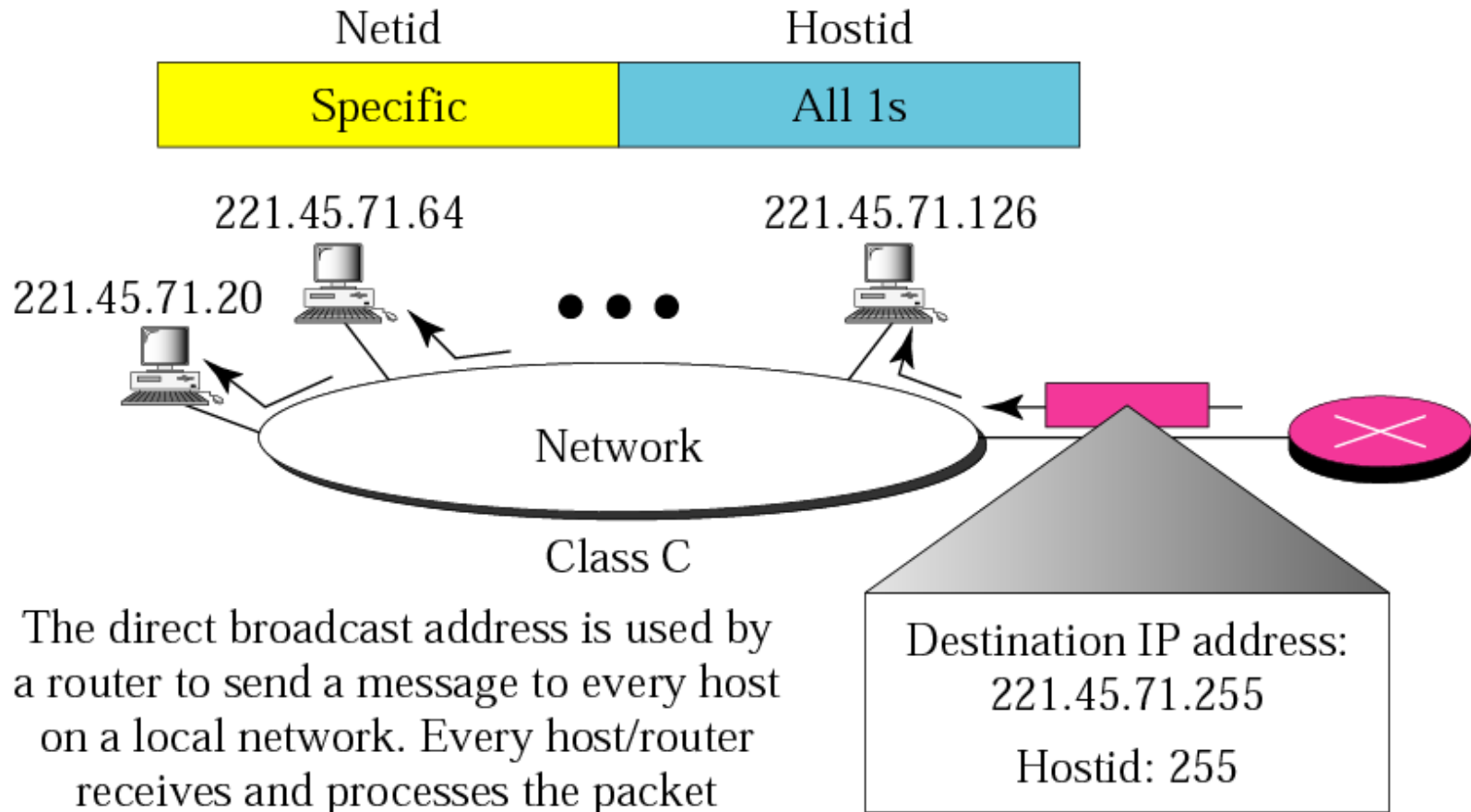
# Special Address :

<i>Special Address</i>	<i>Netid</i>	<i>Hostid</i>	<i>Source or Destination</i>
Network address	Specific	All 0s	None
Direct broadcast address	Specific	All 1s	Destination
<b>Limited broadcast address</b>	All 1s	All 1s	Destination
<b>This host on this network</b>	All 0s	All 0s	Source
<b>Specific host on this network</b>	All 0s	Specific	Destination
Loopback address	127	Any	Destination

# Network address :

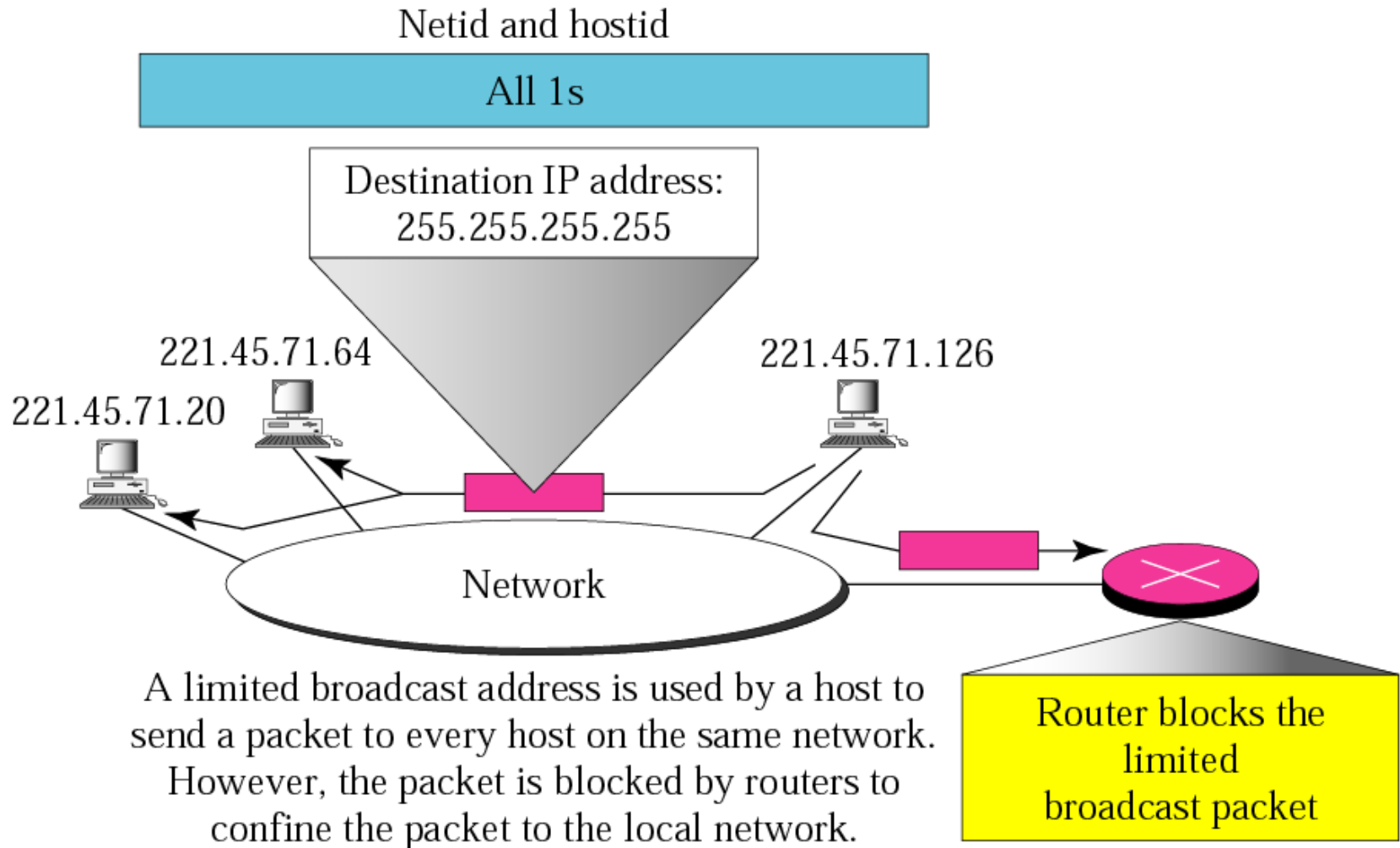


# Direct Broadcast:



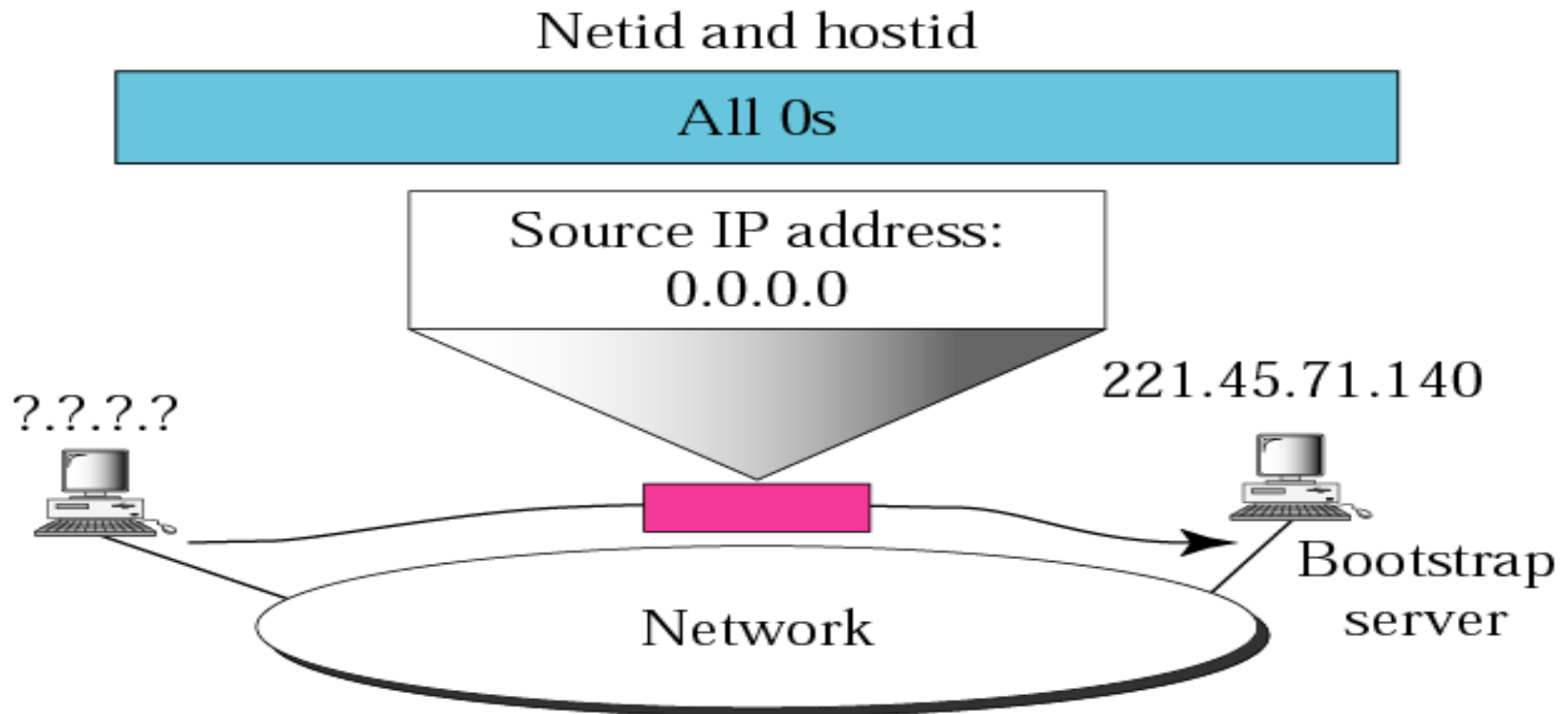
The direct broadcast address is used by a router to send a message to every host on a local network. Every host/router receives and processes the packet with a direct broadcast address.

# Limited Broadcast address:



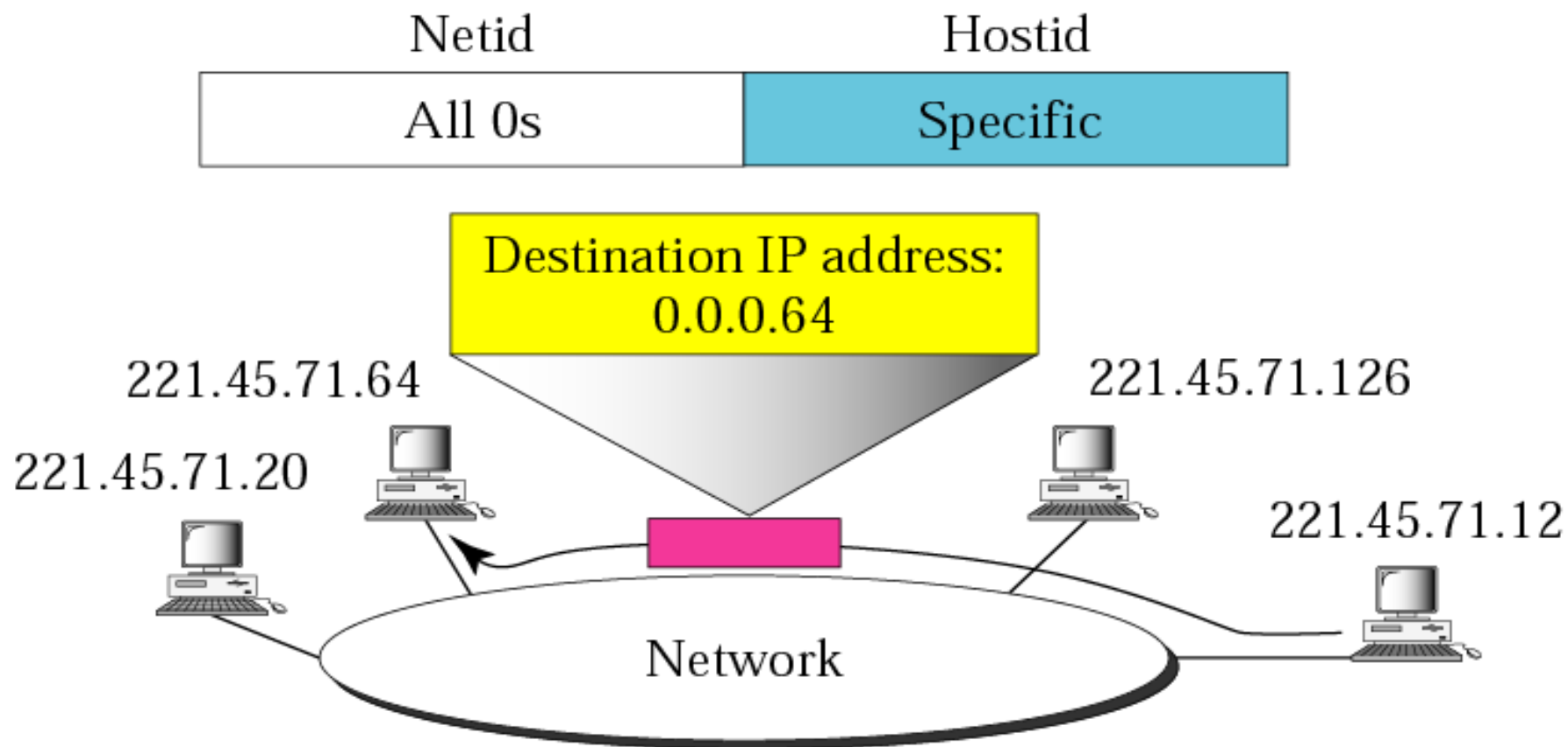


# This Host in this Network:



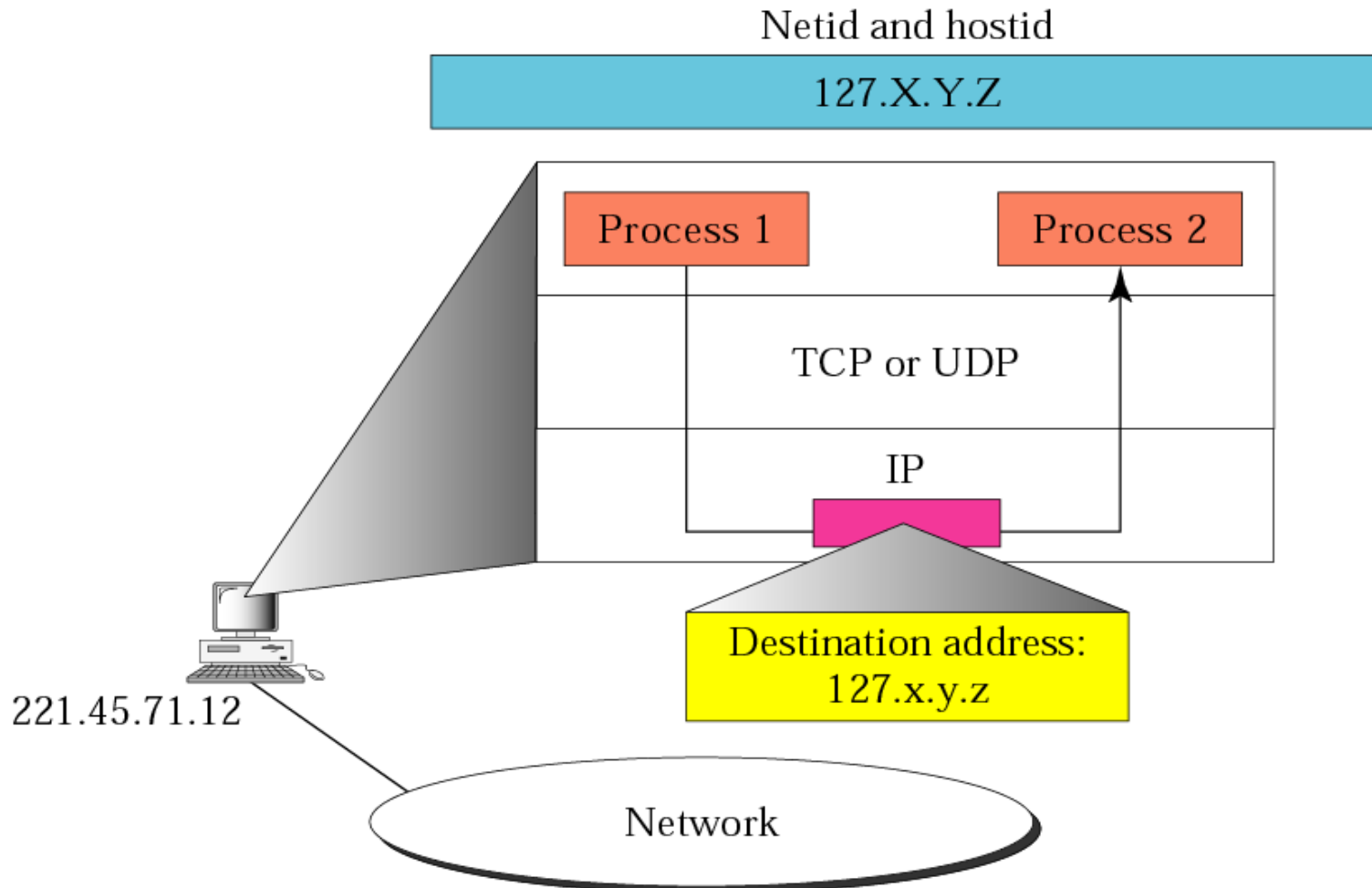
A host that does not know its IP address uses the IP address 0.0.0.0 as the source address and 255.255.255.255 as the destination address to send a message to a bootstrap server.

# Specific Host on this Network:



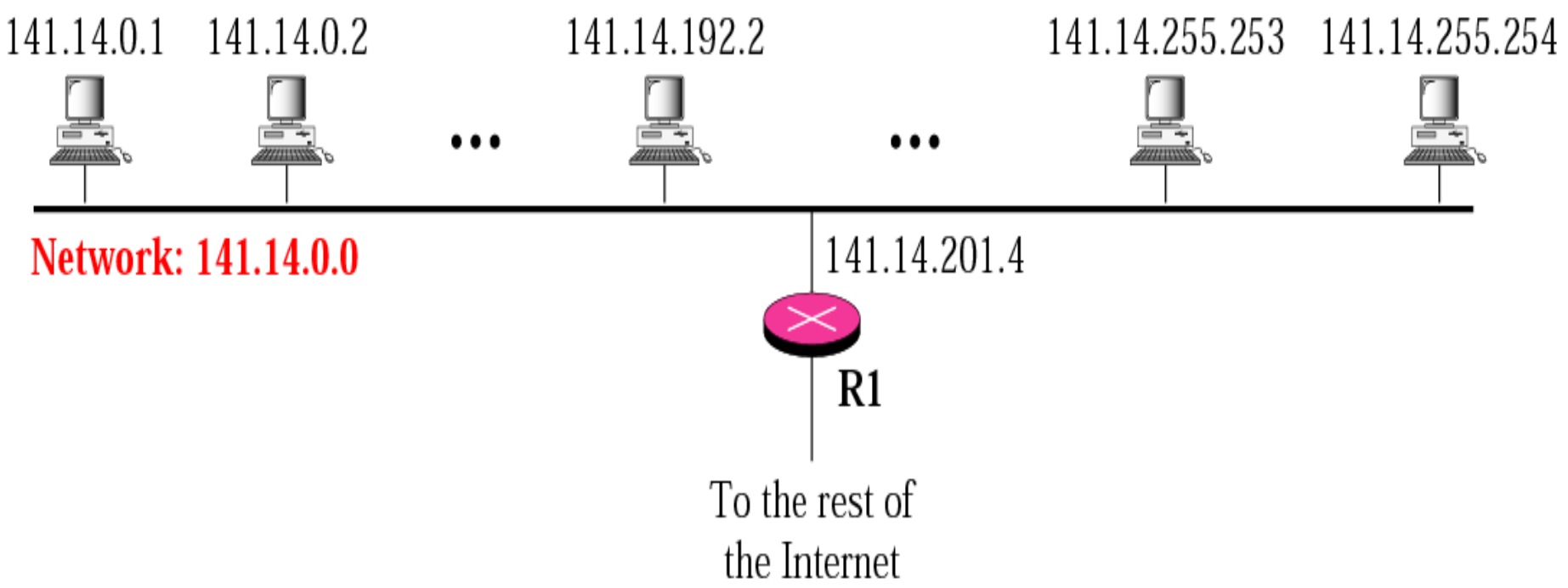
This address is used by a router or host to send a message to a specific host on the same network.

# Loopback Address:

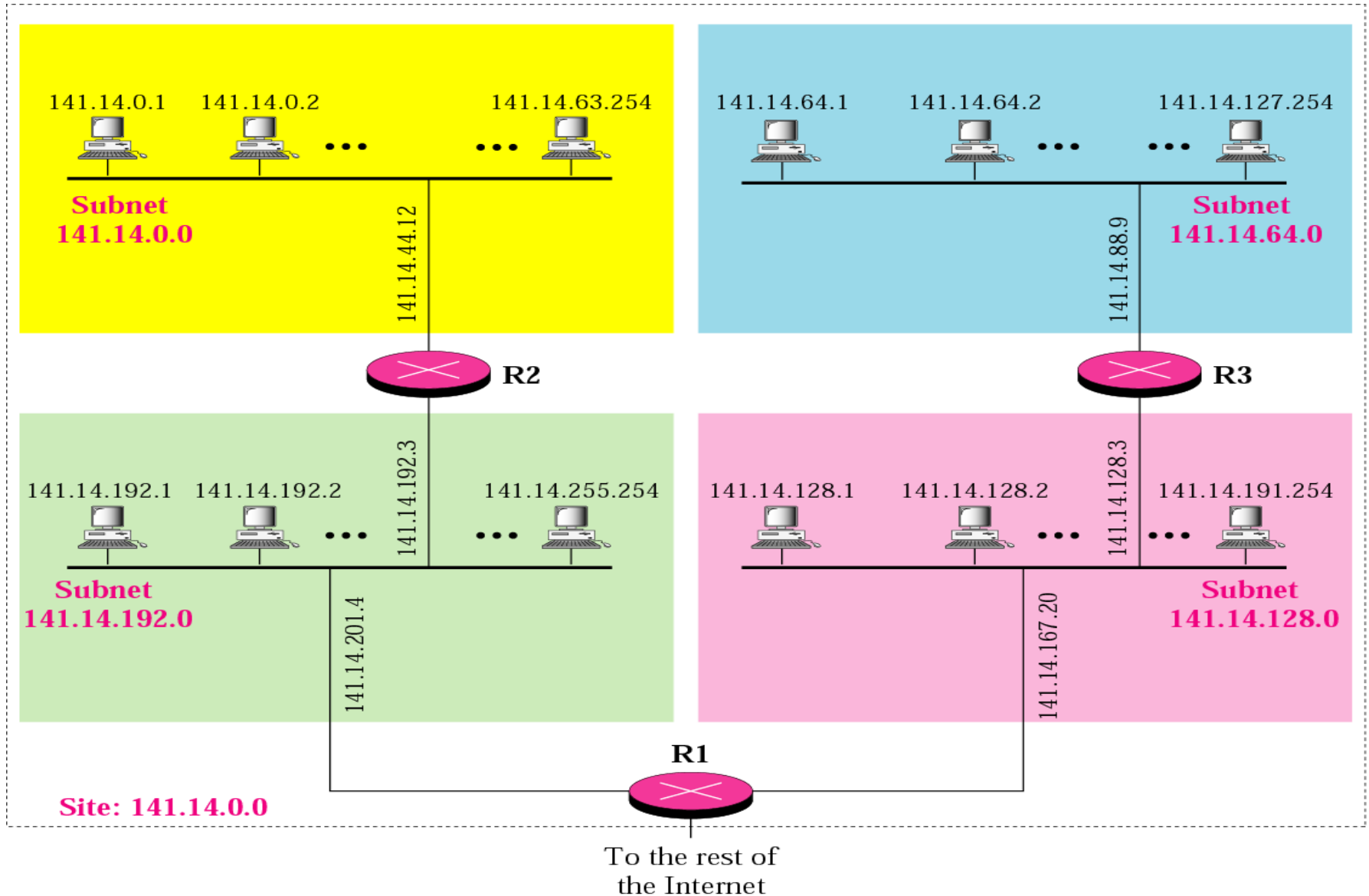


A packet with a loopback address will not reach the network.

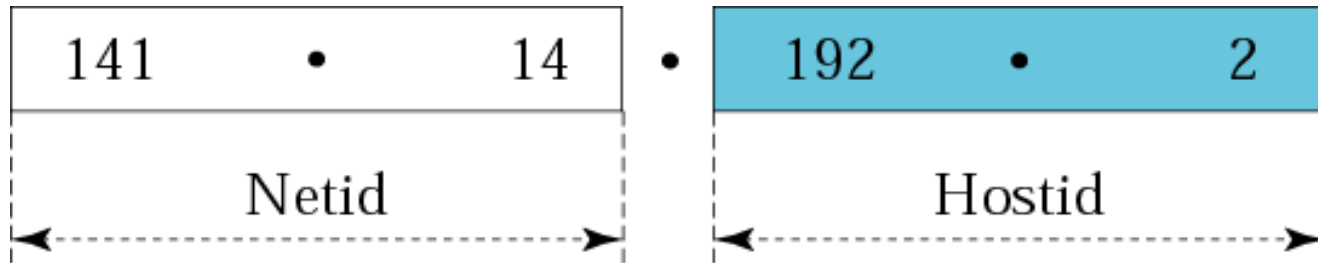
# A network with two levels of hierarchy (not subnetted):



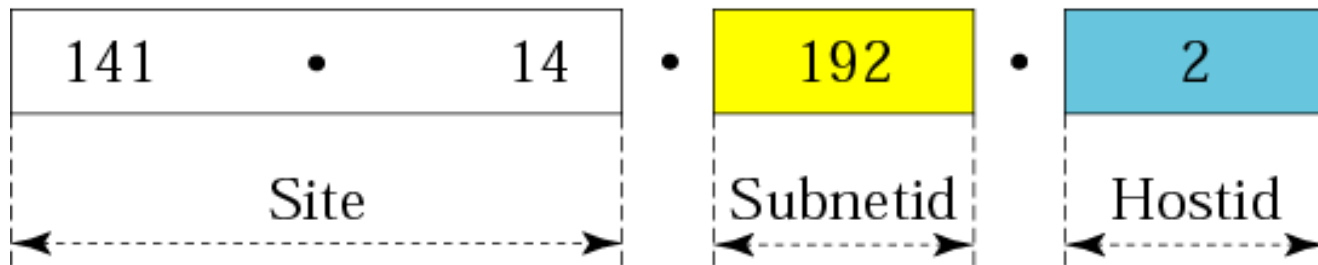
# A network with three levels of hierarchy (subnetted):



# Addresses in a network with and without subnetting :

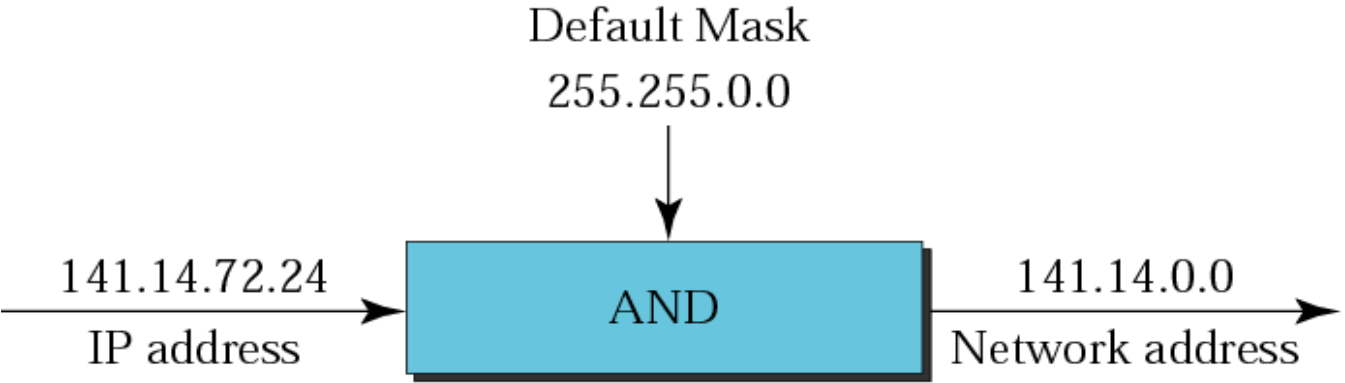


a. Without subnetting

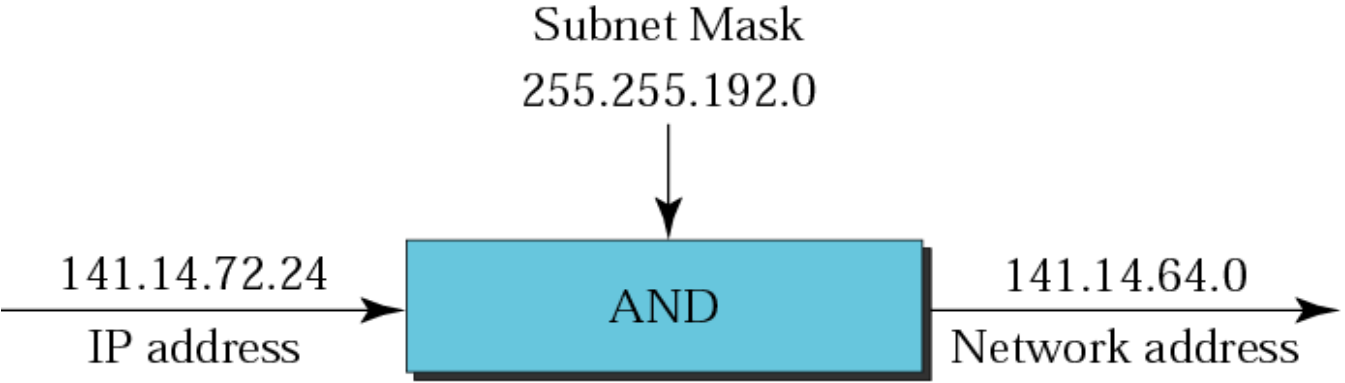


b. With subnetting

# Default and Subnet Mask :



a. Without subnetting



b. With subnetting

*What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?*

### **Solution**

**We apply the AND operation on the address and the subnet mask.**

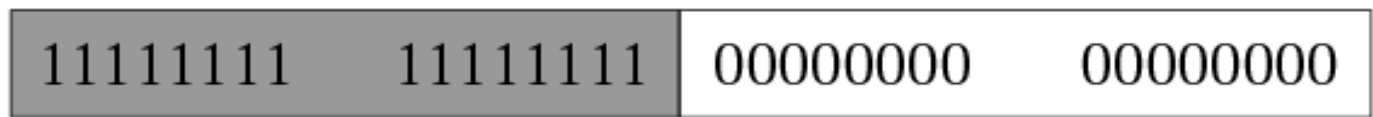
Address	→ 11001000 00101101 00100010 00111000
Subnet Mask	→ 11111111 11111111 11110000 00000000
Subnetwork Address	→ 11001000 00101101 00100000 00000000.



# Comparison Default mask and Subnet mask:

255.255.0.0

Default Mask



16

255.255.224.0

Subnet Mask



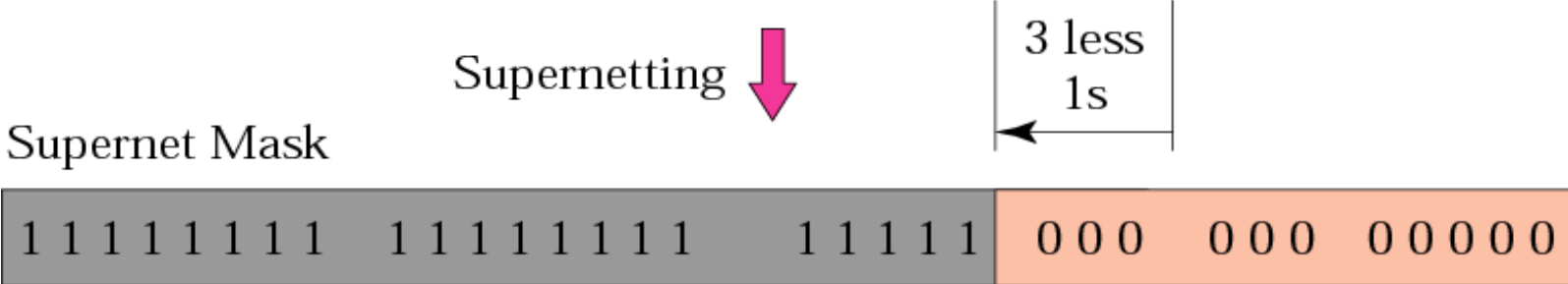
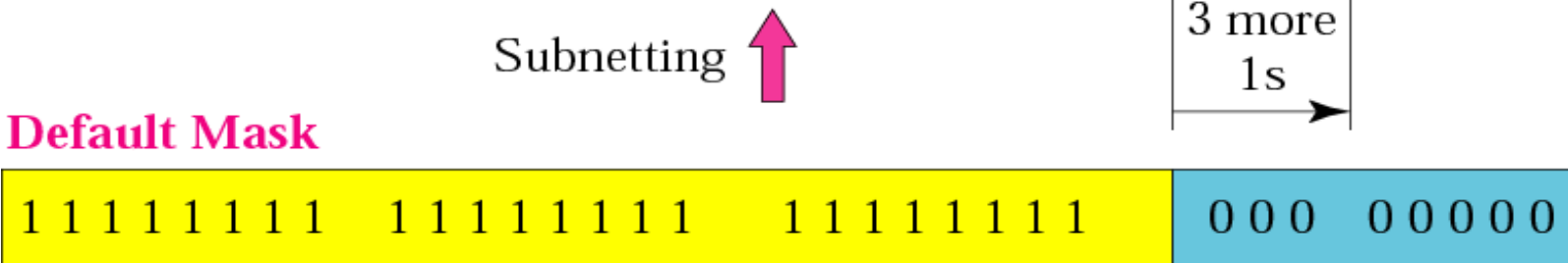
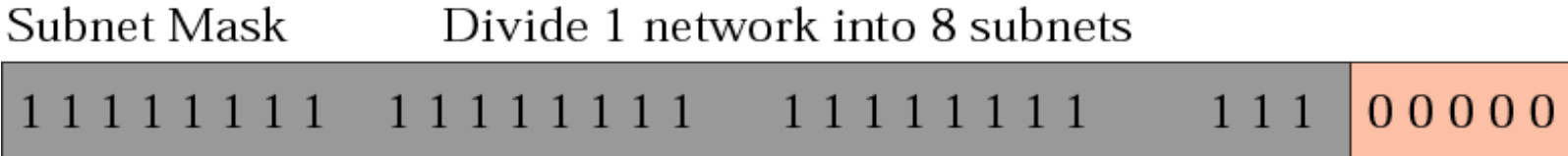
3

13

*In subnetting, we need the first address of the subnet and the subnet mask to define the range of addresses.*

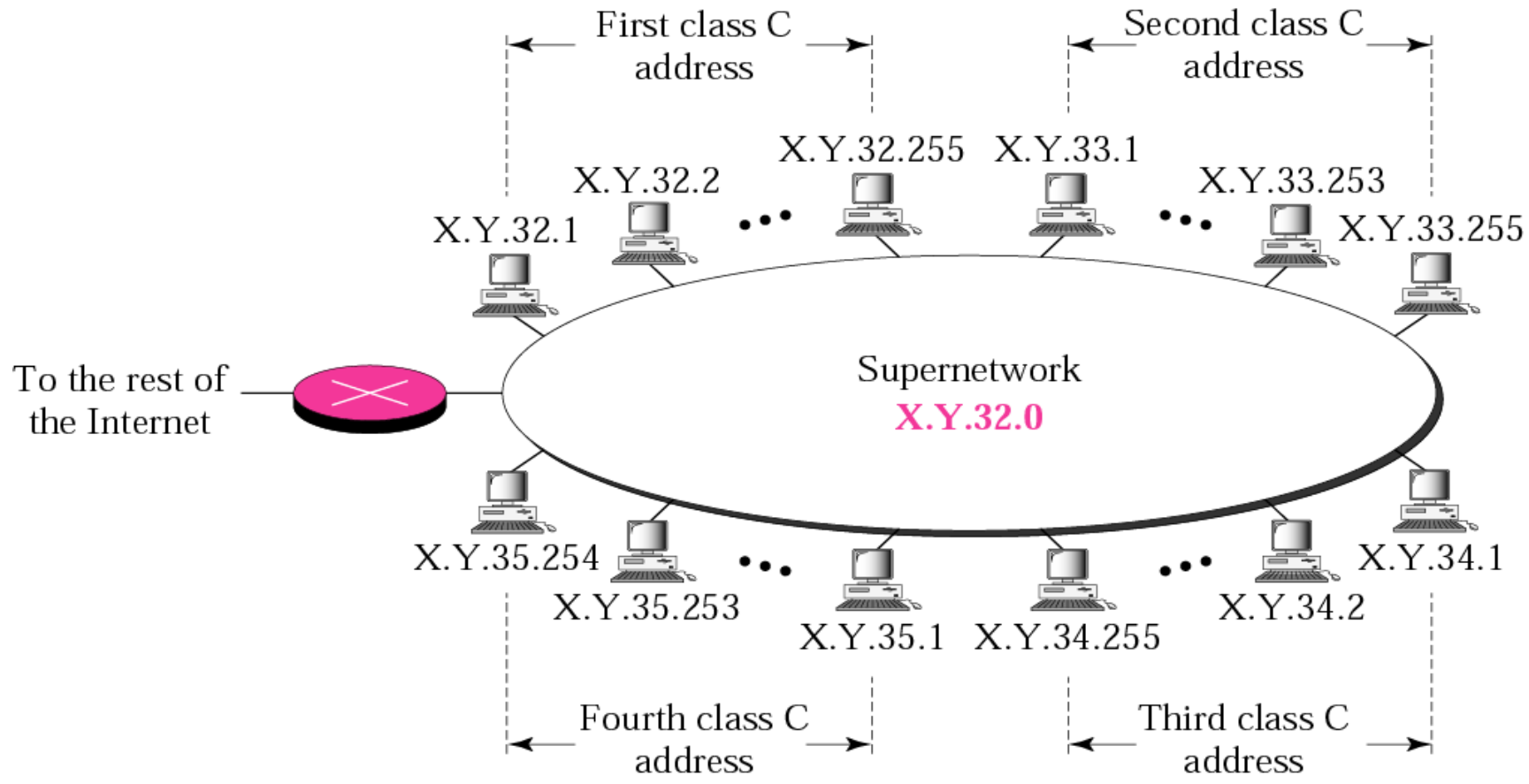
*In supernetting, we need the first address of the supernet and the supernet mask to define the range of addresses.*

# Comparison of subnet, default, and supernet masks :



Combine 8 networks into 1 supernet

# Supernetting :



*IP Addresses:  
Classless Addressing*

# Objectives

- *Understand the concept of classless addressing*
- *Be able to find the first and last address given an IP address*
- *Be able to find the network address given a classless IP address*

# CIDR

- **Classless Inter-Domain Routing (CIDR)**
  - Developed to slow the exhaustion of IP addresses
  - Based on assigning IP addresses on criteria other than octet boundaries
- CIDR addressing method allows the use of a **prefix** to designate the number of network bits in the mask
  - Example: 200.16.1.48 /25 (CIDR notation)
  - The first 25 bits in the mask are network bits (1s)
- The prefix can be longer than the default subnet mask (subnetting) or it can be shorter than the default mask (**supernetting**)

*Format of classless addressing address*

**x.y.z.t/n**



# *Prefix lengths*

<i>/n</i>	<i>Mask</i>	<i>/n</i>	<i>Mask</i>	<i>/n</i>	<i>Mask</i>	<i>/n</i>	<i>Mask</i>
/1	128.0.0.0	/9	255.128.0.0	/17	255.255.128.0	/25	255.255.255.128
/2	192.0.0.0	/10	255.192.0.0	/18	255.255.192.0	/26	255.255.255.192
/3	224.0.0.0	/11	255.224.0.0	/19	255.255.224.0	/27	255.255.255.224
/4	240.0.0.0	/12	255.240.0.0	/20	255.255.240.0	/28	255.255.255.240
/5	248.0.0.0	/13	255.248.0.0	/21	255.255.248.0	/29	255.255.255.248
/6	252.0.0.0	/14	255.252.0.0	/22	255.255.252.0	/30	255.255.255.252
/7	254.0.0.0	/15	255.254.0.0	/23	255.255.254.0	/31	255.255.255.254
/8	255.0.0.0	/16	255.255.0.0	/24	255.255.255.0	/32	255.255.255.255

*Example 1 :*

*What is the first address in the block if one of the addresses is **167.199.170.82/27**?*

### *Solution*

*The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s. The following shows the process:*

*Address in binary:      10100111 11000111 10101010 01010010*

*Keep the left 27 bits: **10100111 11000111 10101010 010**00000*

*Result in CIDR notation: 167.199.170.64/27*

*Example2 :*

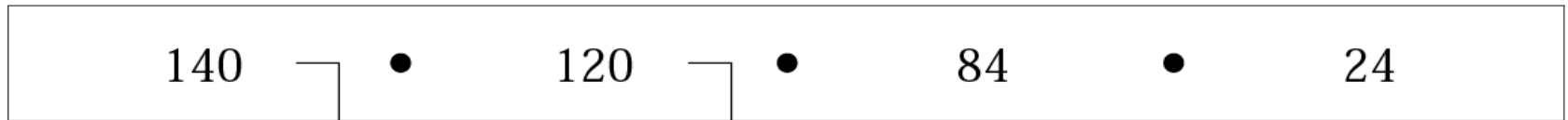
*What is the first address in the block if one of the addresses is **140.120.84.24/20**?*

### *Solution*

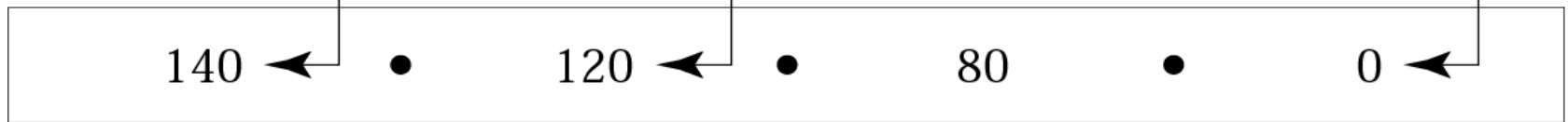
*Figure 5.3 shows the solution. The first, second, and fourth bytes are easy; for the third byte we keep the bits corresponding to the number of 1s in that group. The first address is **140.120.80.0/20**.*

**See Next Slide**

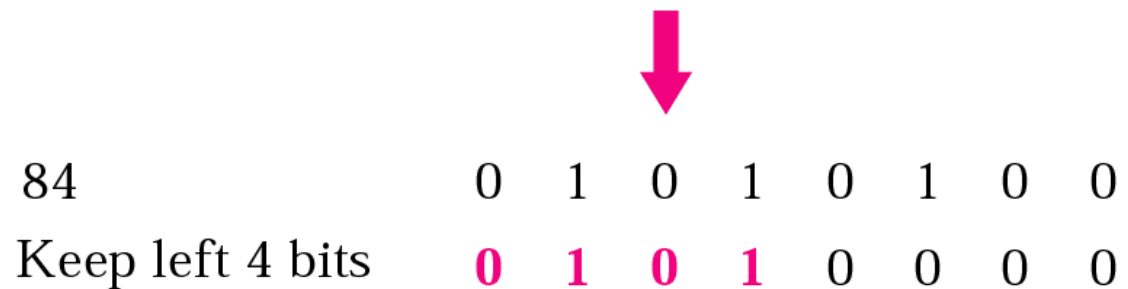
IP Address



/n



First Address



Result in decimal: 80

### *Example: 3*

*Find the first address in the block if one of the addresses is **140.120.84.24/20**.*

### *Solution*

*The first, second, and fourth bytes are as defined in the previous example. To find the third byte, we write 84 as the sum of powers of 2 and select only the leftmost 4 ( $m$  is 4) as shown in Figure 5.4. The first address is **140.120.80.0/20**.*

**See Next Slide**

Write 84 as sum of:

128	64	32	16	8	4	2	1
0	64	0	16	0	4	0	0

Select only leftmost 4:

0	64	0	16
---	----	---	----

Add to find the result: 80

# Summarization

- **Summarization**
  - Also known as route aggregation or supernetting
  - Allows many IP subnets to be advertised as one
    - Reduces the number of entries in the router's routing table
- Summarize a group of subnets
  - Count the number of bits that are common to all of the networks you want to advertise
  - Then use the prefix that identifies the number of common bits

# Summarization (continued)

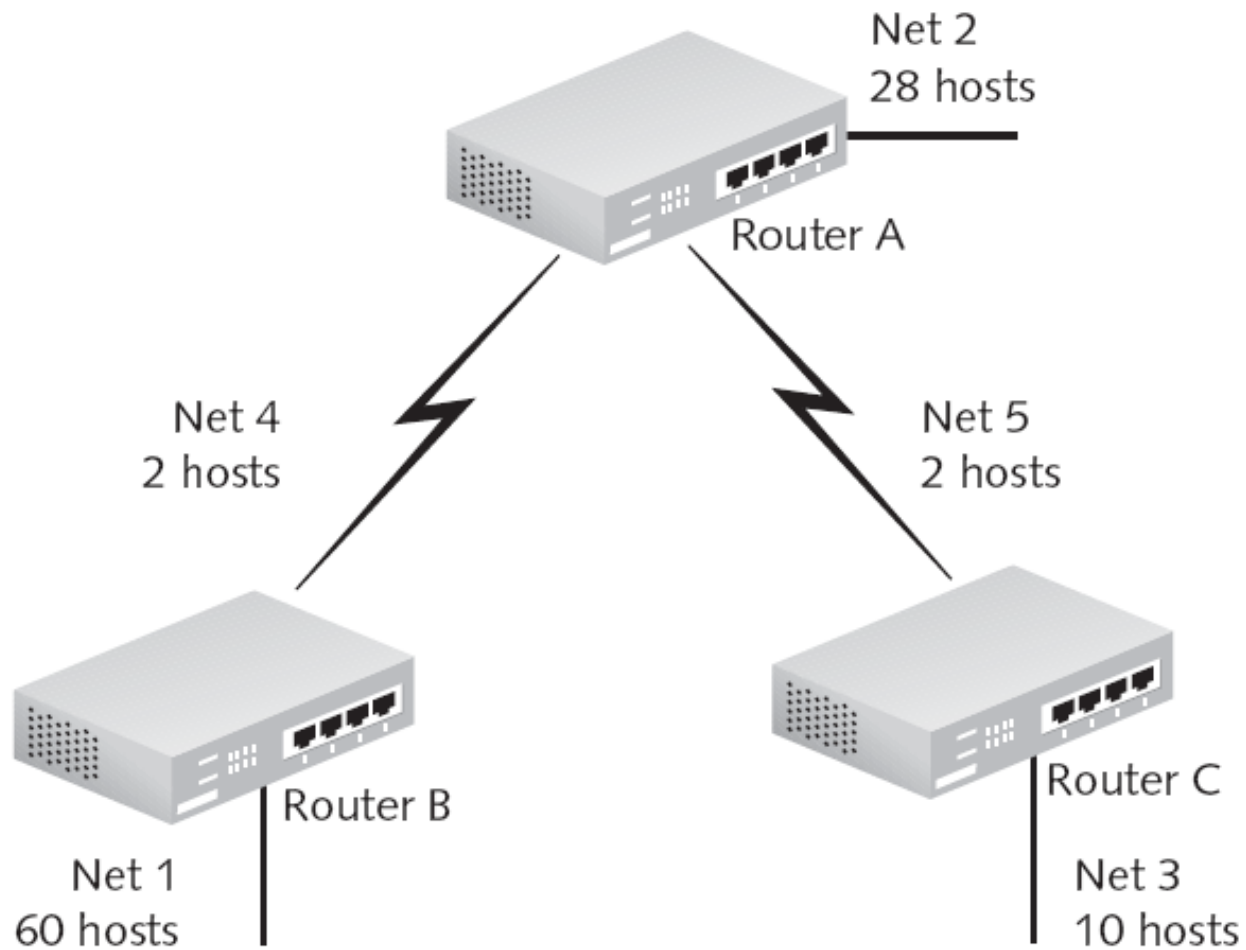
Decimal	Binary Equivalent
213.64.132.0 /24	11010101.01000000.10000100.00000000
213.64.133.0 /24	11010101.01000000.10000101.00000000
213.64.134.0 /24	11010101.01000000.10000110.00000000
213.64.135.0 /24	11010101.01000000.10000111.00000000

**Table 4-6** Example summarization



# Variable Length Subnet Masks

- **Variable length subnet masking (VLSM)**
  - Allows different masks on the subnets
  - Essentially done by subnetting the subnets
- Basic routing protocols such as RIP version 1 and IGRP
  - Do not support VLSM because they do not carry subnet mask information in their routing table updates
  - Are classful routing protocols
- RIP version 2, OSPF, or EIGRP are classless protocols



**Figure 4-15** Example internetwork for VLSM

# Variable Length Subnet Masks (continued)

192.168.59.128 /30	192.168.59.160 /30
192.168.59.132 /30	192.168.59.164 /30
192.168.59.136 /30	192.168.59.168 /30
192.168.59.140 /30	192.168.59.172 /30
192.168.59.144 /30	192.168.59.176 /30
192.168.59.148 /30	192.168.59.180 /30
192.168.59.152 /30	192.168.59.184 /30
192.168.59.156 /30	192.168.59.188 /30

**Table 4-7** VLSM subnets created from 192.168.59.128 /26

# Variable Length Subnet Masks (continued)

Major Network	Original Subnets	Subnetted Subnets Using VLSM	Subnet Assignments
192.168.59.0 /24	192.168.59.0 /26		Net 1
	192.168.59.64 /26	192.168.59.64 /27	Net 2
		192.168.59.96 /27	Net 3
	192.168.59.128 /26	192.168.59.128 /30	Net 4
		192.168.59.132 /30	Net 5
		192.168.59.136 through 192.168.59.188	Reserved
	192.168.59.192 /26		Reserved

**Table 4-8** VLSM IP scheme for 192.168.59.0

*IP Addresses:  
Classless Addressing2*

# Working with Hexadecimal Numbers

- **Hexadecimal** numbering system is base 16
  - 16 numerals are used to express any given number
  - Numerals include 0 through 9 as well as A through F
  - For example, the decimal number 192 is C0 in hexadecimal
- Often you will come across hexadecimal numbers when working with computers and networking
  - The MAC address is a 12-digit hexadecimal number
- Computers typically process information in 8-bit chunks (bytes)
  - Easier to express bytes with two hex digits

Binary	Hexadecimal	Decimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

**Table 4-9** Binary to hex to decimal conversion

# IPv4 versus IPv6

- IP version 4 (**IPv4**)
  - The version of IP currently deployed on most systems today
- IP version 6 (**IPv6**)
  - Originally designed to address the eventual depletion of IPv4 addresses
- CIDR has slowed the exhaustion of IPv4 address space and made the move to IPv6 less urgent
  - However, CIDR is destined to become obsolete because it is based on IPv4



# IPv4 versus IPv6 (continued)

- Network address translation (**NAT**)
  - Another technique developed in part to slow the depletion of IPv4 addresses
  - Allows a single IP address to provide connectivity for many hosts
- NAT is CPU intensive and expensive
  - Some protocols do not work well with NAT, such as the IP Security Protocol (**IPSec**)
- IPv4 does not provide security in itself
  - Has led to security issues with DNS and ARP

# IPv4 versus IPv6 (continued)

- Security concerns were factored into the design of IPv6
- IPv4 networks rely on broadcasting
  - Inefficient because many hosts unnecessarily see and partially process traffic not ultimately destined for them
- IPv6 does away completely with broadcasting and replaces it with multicasting
- IPv6 addresses are 128 bits compared with IPv4's 32-bit structure

# IPv4 versus IPv6 (continued)

- IPv6 addresses are expressed as hexadecimal numbers
  - Example:  
3FFE:0501:0008:0000:0260:97FF:FE40:EFAB
- IPv6 can be subnetted
  - CIDR notation is also used with IPv6
    - Example: 2001:702:21:: /48
- Organizations requesting an IPv6 address may be assigned a /64 prefix
  - Minimum subnet with space for over a billion hosts

# Transitioning to IPv6

- **Dual stack**

- Involves enabling IPv6 on all routers, switches, and end nodes but not disabling IPv4
- Both version 4 and version 6 stacks run at the same time

- **Tunneling**

- Encapsulates IPv6 traffic inside IPv4 packets
- Done when portions of a network are running IPv6 and other network areas have not been upgraded yet
- Greatest concern: security



# *Delivery, Forwarding, and Routing of IP Packets*

---

## **Objectives**

*Upon completion you will be able to:*

- *Understand the different types of delivery and the connection*
- *Understand forwarding techniques in classful addressing*
- *Understand forwarding techniques in classless addressing*
- *Understand how a routing table works*
- *Understand the structure of a router*

# 6.1 DELIVERY

*The network layer supervises delivery, the handling of the packets by the underlying physical networks. Two important concepts are the type of connection and direct versus indirect delivery.*

*The topics discussed in this section include:*

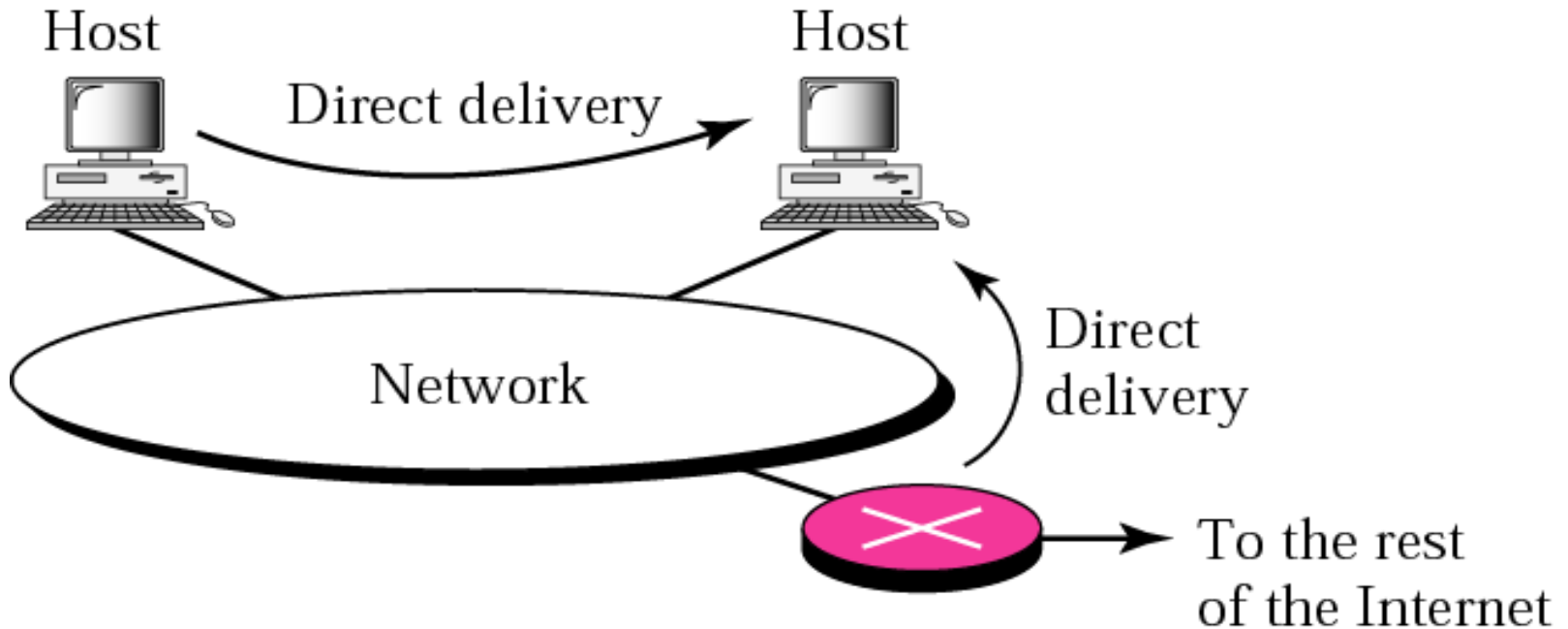
*Connection Types*

*Direct Versus Indirect Delivery*



*IP is a connectionless protocol.*

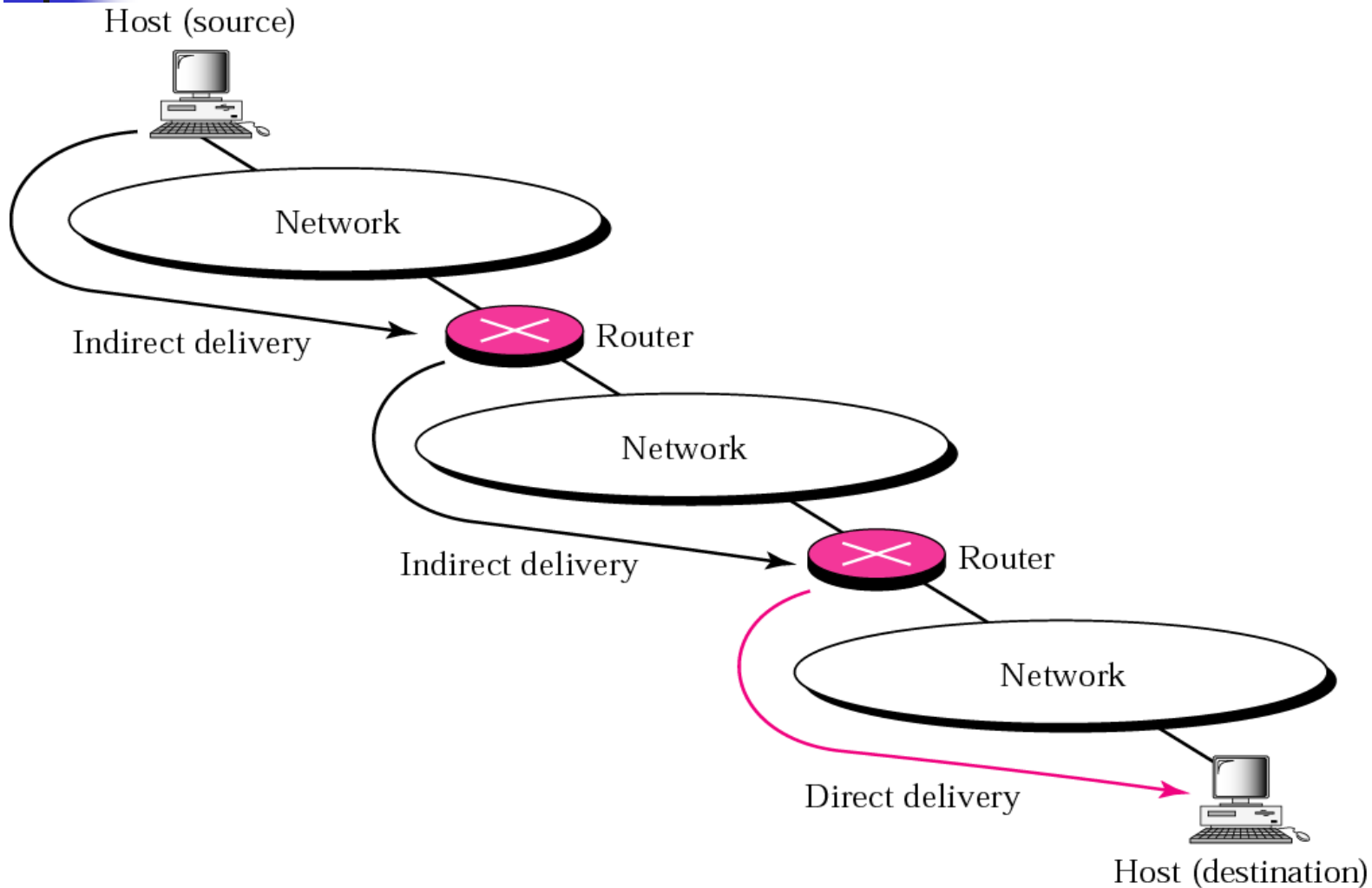
**Figure 6.1** *Direct delivery*



**Mapping the IP address to the physical address (Address Resolution Protocol)**



**Figure 6.2** *Indirect delivery*



**Address mapping between the IP address of the next router and physical address of the next router.**

## 6.2 FORWARDING

*Forwarding means to place the packet in its route to its destination.  
Forwarding requires a host or a router to have a routing table. .*

*The topics discussed in this section include:*

*Forwarding Techniques*

*Forwarding with Classful Addressing*

*Forwarding with Classless Addressing*

*Combination*

*Several techniques make the size of routing table manageable :*

# 1- Next-hop method

Routing table for host A

Destination	Route
Host B	R1, R2, Host B

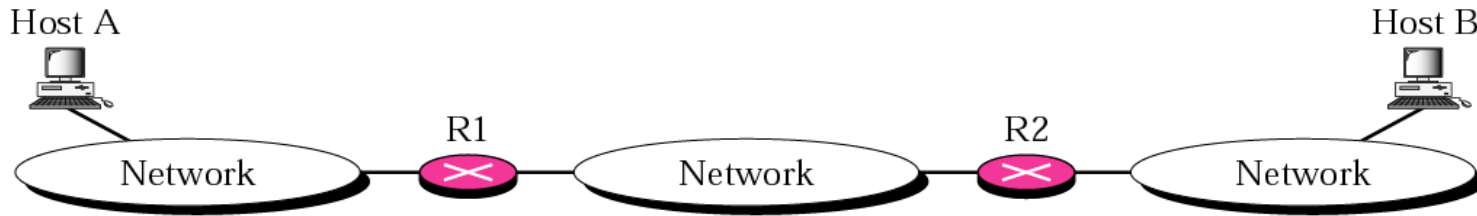
Routing table for R1

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

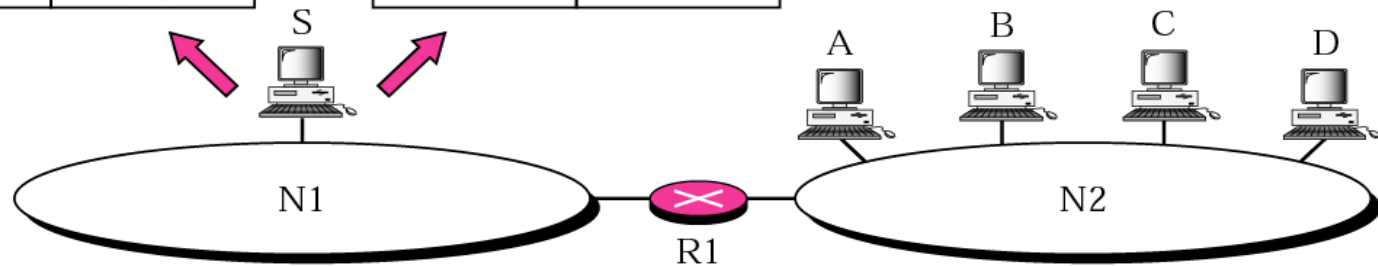
## 2- Network-specific method

Routing table for host S based on host-specific method

Destination	Next Hop
A	R1
B	R1
C	R1
D	R1

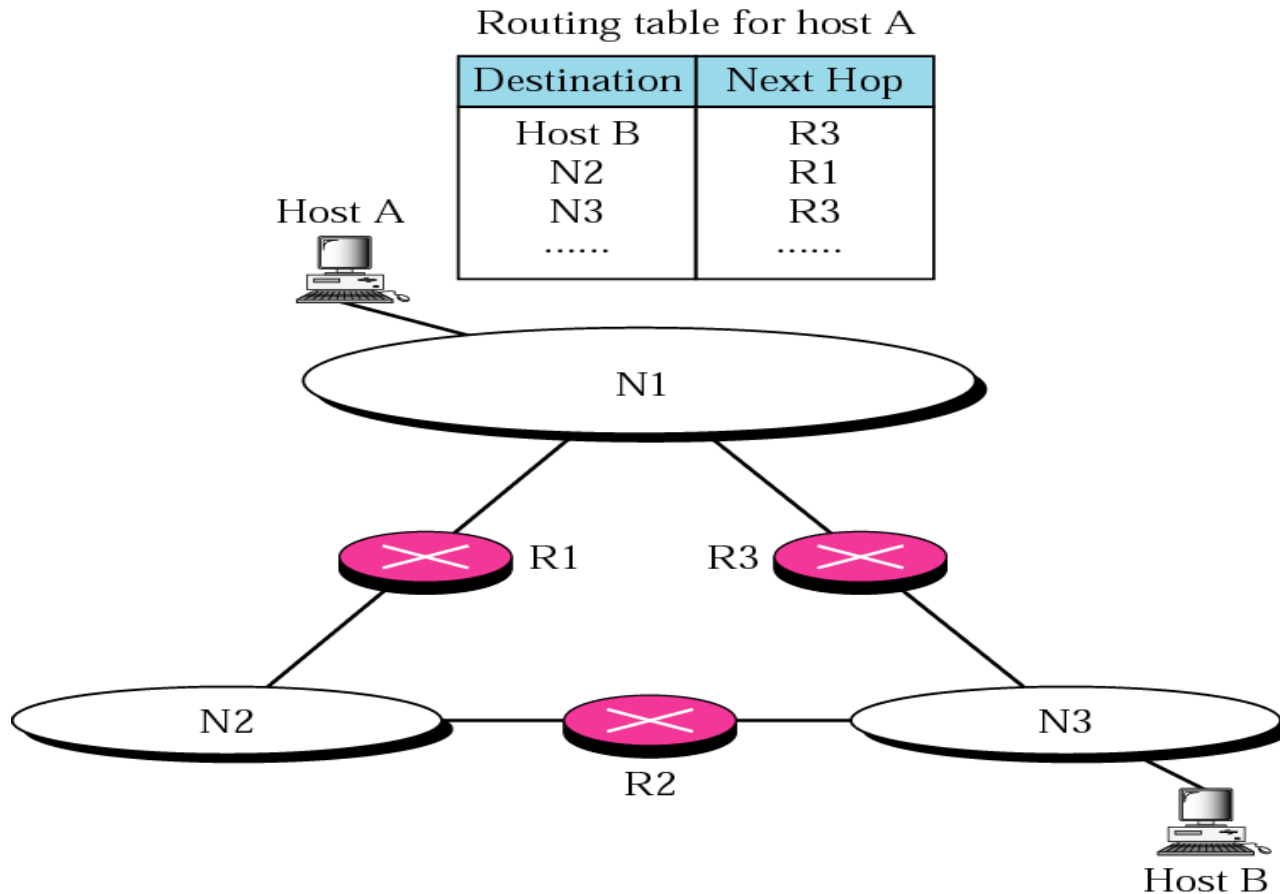
Routing table for host S based on network-specific method

Destination	Next Hop
N2	R1



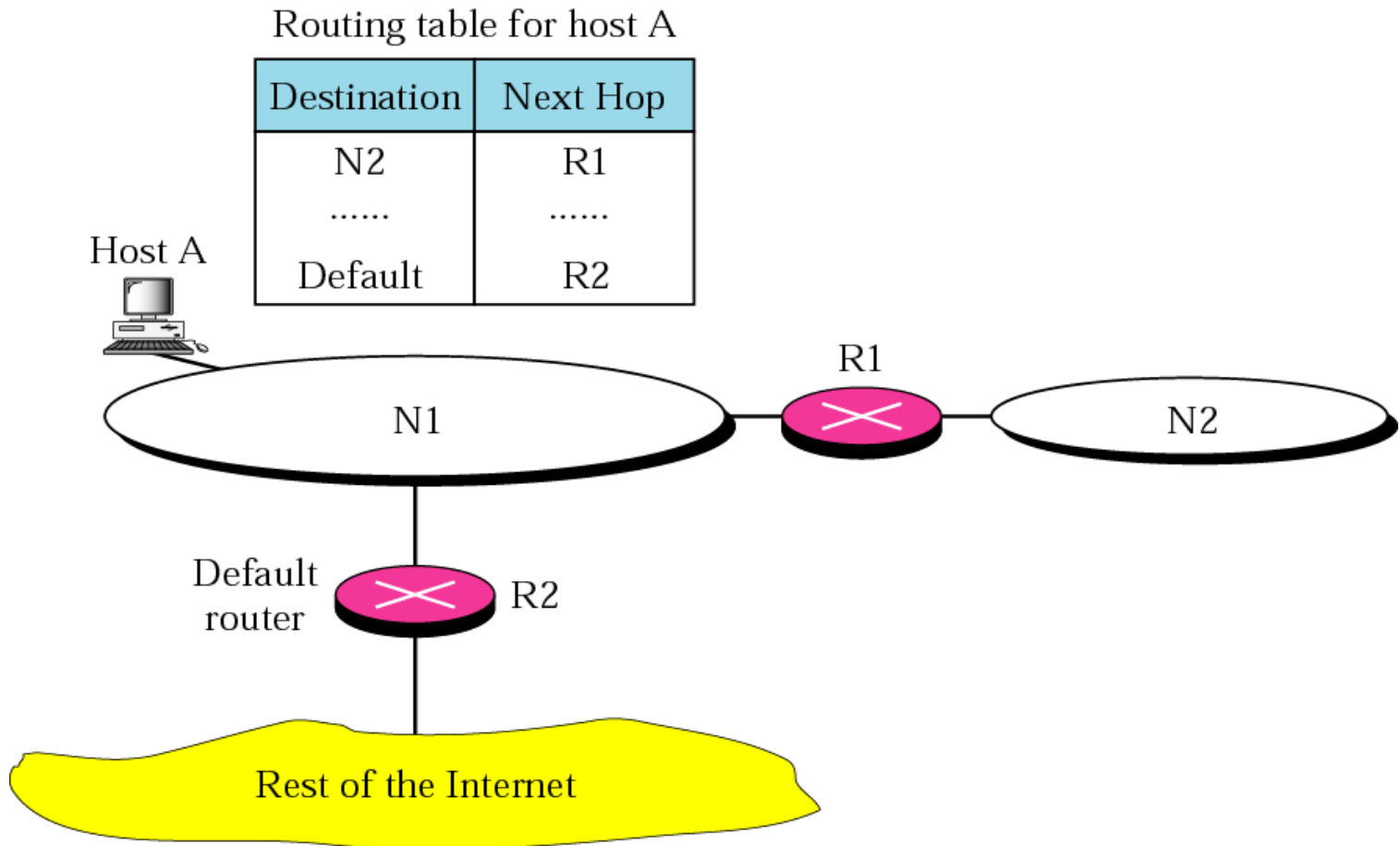
**Figure 6.5** *Host-specific routing*

**Host-specific routing is used for purposes such as checking the route or providing security measures (The inverse of the network-specific method).**



**Figure 6.6** *Default routing*

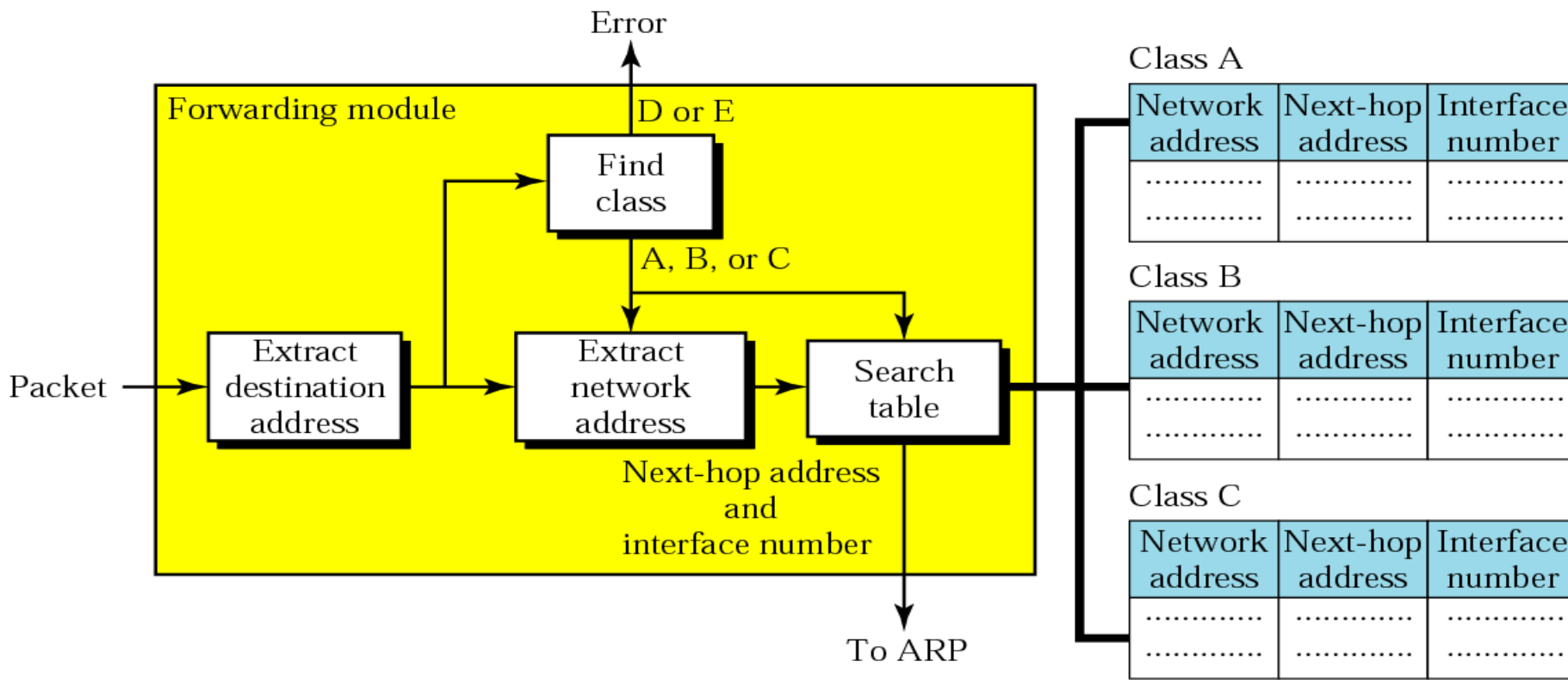
instead of listing all networks in the entire Internet, host A can just have one entry called the *default* (normally defined as network address *0.0.0.0*).



**Figure 6.7** Simplified forwarding module in classful address without subnetting

In classful addressing, most of the routers in the global Internet are not involved in subnetting. Subnetting happens inside the organization. A typical forwarding module in this case can be designed using three tables, one for each unicast class (A, B, C). If the router supports multicasting, another table can be added to handle class D addresses. Having three different tables makes searching more efficient.

1. The network address of the destination network tells us where the destination host is located(network-specific).
2. The next-hop address tells us to which router the packet must be delivered for an indirect delivery.
3. The interface number defines the outgoing port from which the packet is sent out.



**Figure 6.7** *Simplified forwarding module in classful address without subnetting*

In its simplest form, the forwarding module follows these steps:

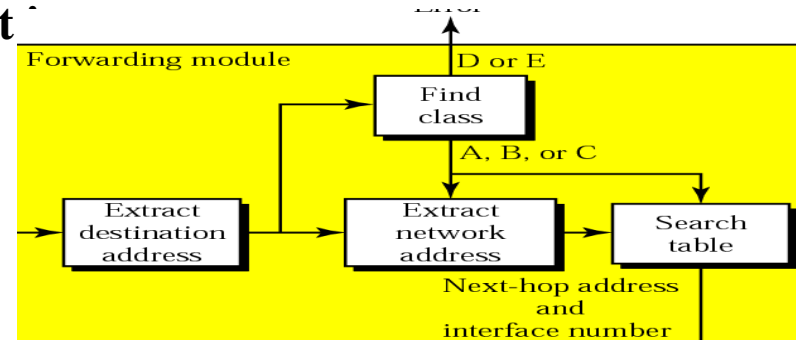
❑ The destination address of the packet is extracted.  
❑ A copy of the destination address is used to find the class of the address. This is done by shifting the copy of the address 28 bits to the right. The result is a 4-bit number between 0 and 15. If the result

- 0 to 7, the class is A.
- 8 to 11, the class is B.
- 12 or 13, the class is C
- 14, the class is D.
- 15, the class is E.

❑ The result of Step 2 for class A, B, or C and the destination address are used to extract the network address. This is done by masking off (changing to 0s) the rightmost 8, 16, or 24 bits based on the class.

❑ The class of the address and the network address are used to find next-hop information. The module searches this table for the network address. If a match is found, the next-hop address and the interface number of the output port are extracted from the table. If no match is found, the default is used.

❑ The ARP module uses the next-hop address and the interface number to find the physical address of the next router. It then asks the data link layer to deliver the packet to the next hop.





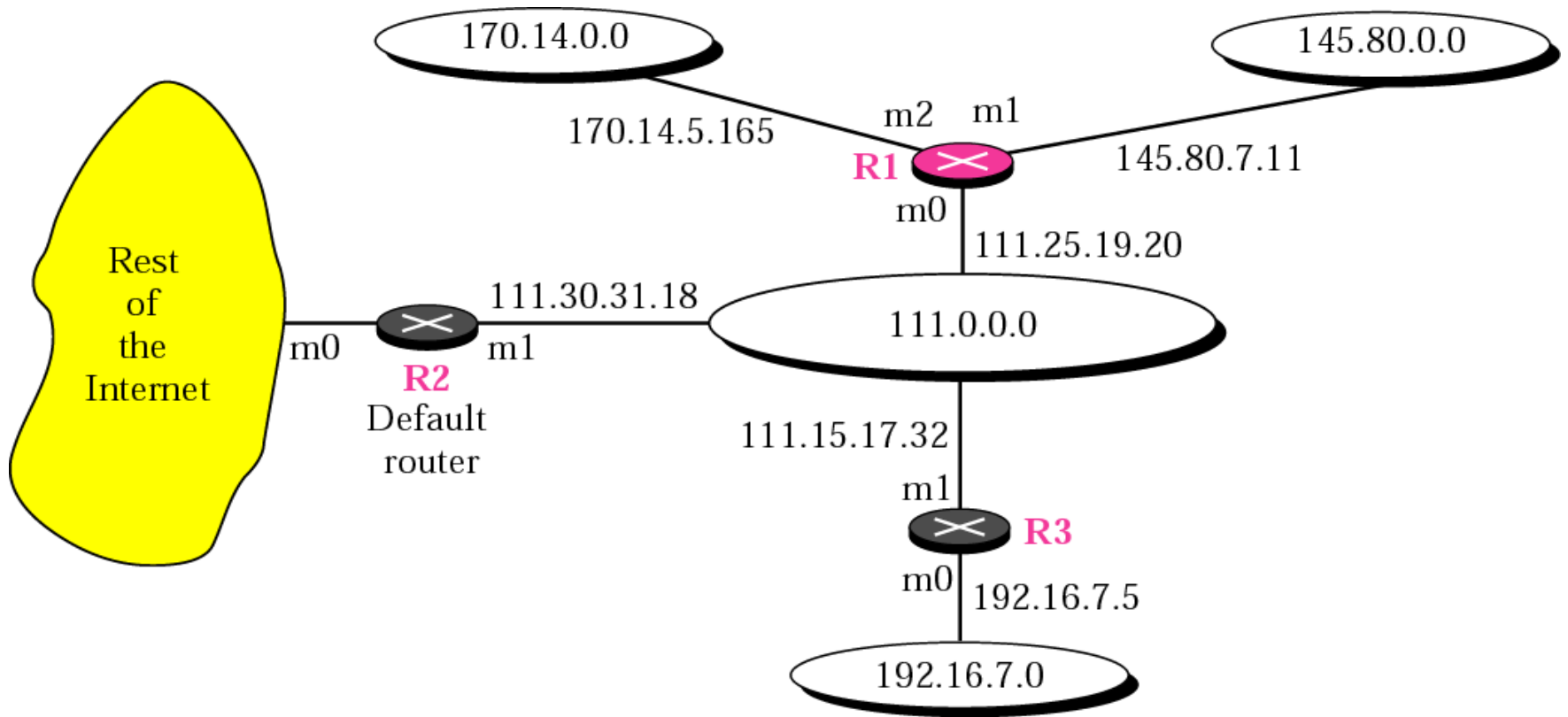


## ***EXAMPLE 1***

*Figure 6.8 shows an imaginary part of the Internet.  
Show the routing tables for router R1.*

**See Next Slide**

**Figure 6.8** Configuration for routing, Example 1





## ***EXAMPLE 1 (CONTINUED)***

### ***Solution***

*Figure 6.9 shows the three tables used by router R1. Note that some entries in the next-hop address column are empty because in these cases, the destination is in the same network to which the router is connected (direct delivery). In these cases, the next-hop address used by ARP is simply the destination address of the packet as we will see in Chapter 7.*

**See Next Slide**

**Figure 6.9** *Tables for Example 1*

Class A

Network address	Next-hop address	Interface
111.0.0.0	-----	m0

Class B

Network address	Next-hop address	Interface
145.80.0.0	-----	m1
170.14.0.0	-----	m2

Class C

Network address	Next-hop address	Interface
192.16.7.0	111.15.17.32	m0

Default: 111.30.31.18, m0



## ***EXAMPLE 2***

*Router R1 in Figure 6.8 receives a packet with destination address 192.16.7.14. Show how the packet is forwarded.*

### ***Solution***

*The destination address in binary is 11000000 00010000 00000111 00001110. A copy of the address is shifted 28 bits to the right. The result is 00000000 00000000 00000000 00001100 or **12**. The destination network is class C. The network address is extracted by masking off the leftmost 24 bits of the destination address; the result is **192.16.7.0**. The table for Class C is searched. The network address is found in the first row. The next-hop address **111.15.17.32**, and the interface *m0* are passed to ARP.*



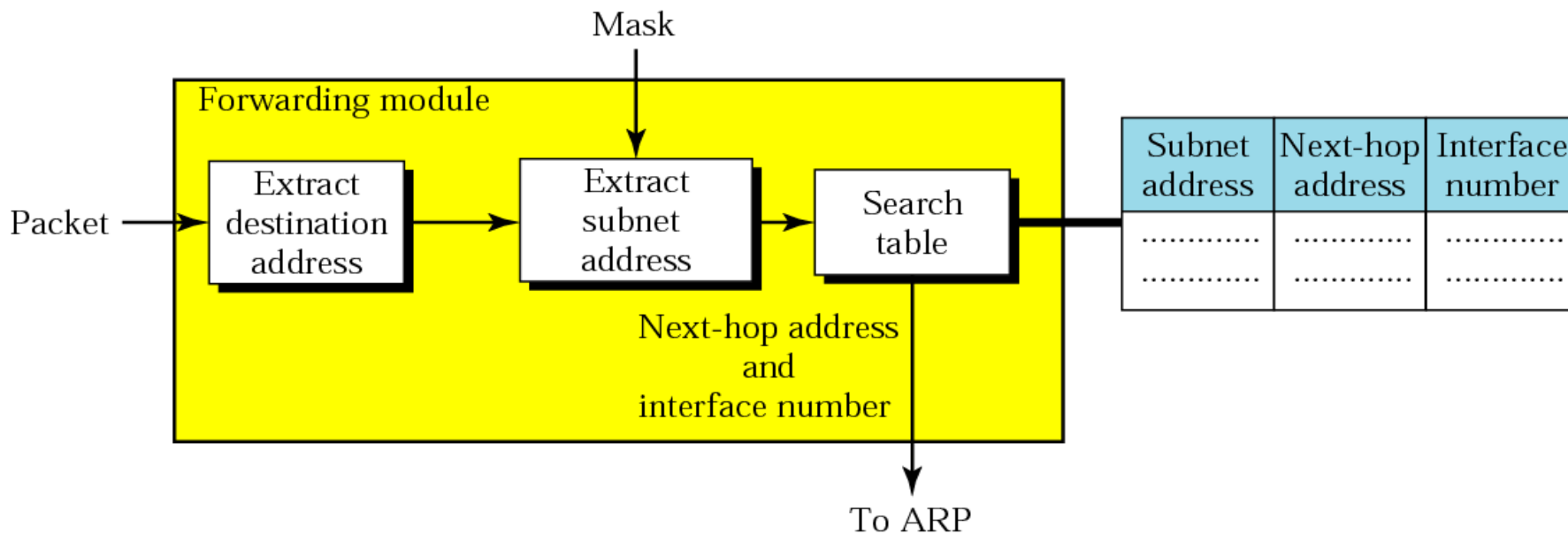
### **EXAMPLE 3**

*Router R1 in Figure 6.8 receives a packet with destination address **167.24.160.5**. Show how the packet is forwarded.*

#### **Solution**

*The destination address in binary is 10100111 00011000 10100000 00000101. A copy of the address is shifted 28 bits to the right. The result is **00000000 00000000 00000000 00001010** or 10. The class is B. The network address can be found by masking off 16 bits of the destination address, the result is 167.24.0.0. The table for Class B is searched. No matching network address is found. The packet needs to be forwarded to the default router (the network is somewhere else in the Internet). The next-hop address 111.30.31.18 and the interface number m0 are passed to ARP.*

**Figure 6.10** *Simplified forwarding module in classful address with subnetting*





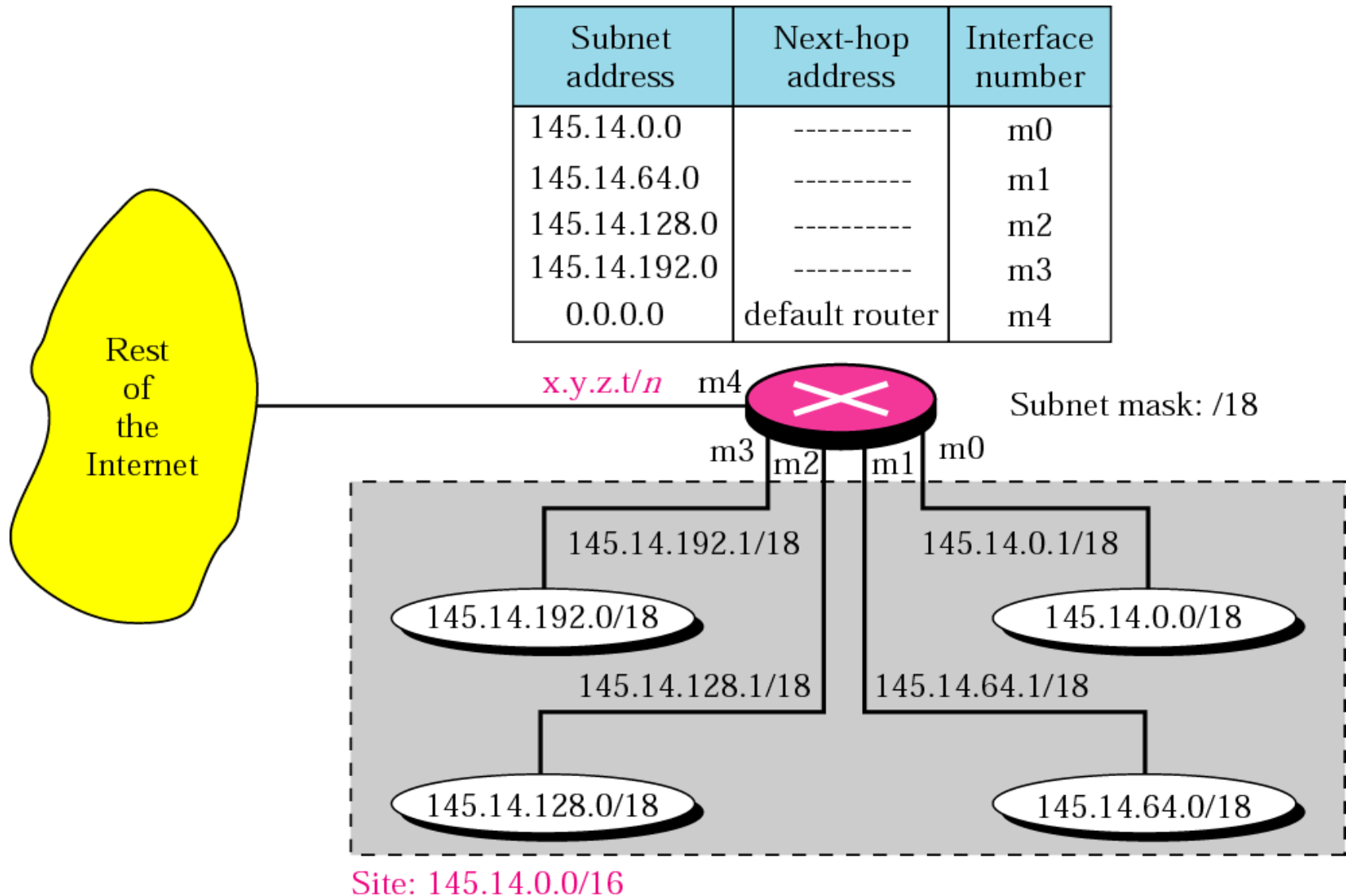
## ***EXAMPLE 4***

*Figure 6.11 shows a router connected to four subnets.*

**See Next Slide**



**Figure 6.11** Configuration for Example 4





## ***EXAMPLE 4 (CONTINUED)***

*Note several points. First, the site address is **145.14.0.0/16** (a class B address). Every packet with destination address in the range 145.14.0.0 to 145.14.255.255 is delivered to the interface m4 and distributed to the final destination subnet by the router. Second, we have used the address **x.y.z.t/n** for the interface m4 because we do not know to which network this router is connected. Third, the table has a default entry for packets that are to be sent out of the site. The router is configured to apply the mask /18 to any destination address.*



## ***EXAMPLE 5***

*The router in Figure 6.11 receives a packet with destination address **145.14.32.78**. Show how the packet is forwarded.*

### ***Solution***

*The mask is **/18**. After applying the mask, the subnet address is **145.14.0.0**. The packet is delivered to ARP with the next-hop address **145.14.32.78** and the outgoing interface **m0**.*



## ***EXAMPLE 6***

*A host in network 145.14.0.0 in Figure 6.11 has a packet to send to the host with address **7.22.67.91**. Show how the packet is routed.*

### ***Solution***

*The router receives the packet and applies the mask (/18). The network address is **7.22.64.0**. The table is searched and the address is not found. The router uses the address of the default router (not shown in figure) and sends the packet to that router.*



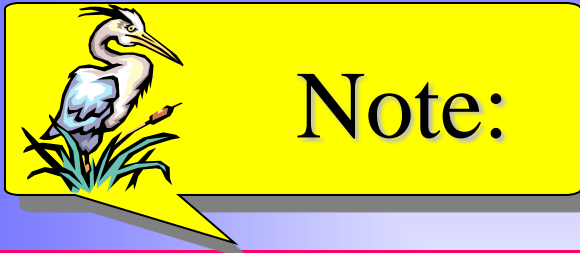
# *Delivery, Forwarding, and Routing of IP Packets*

---

## **Objectives**

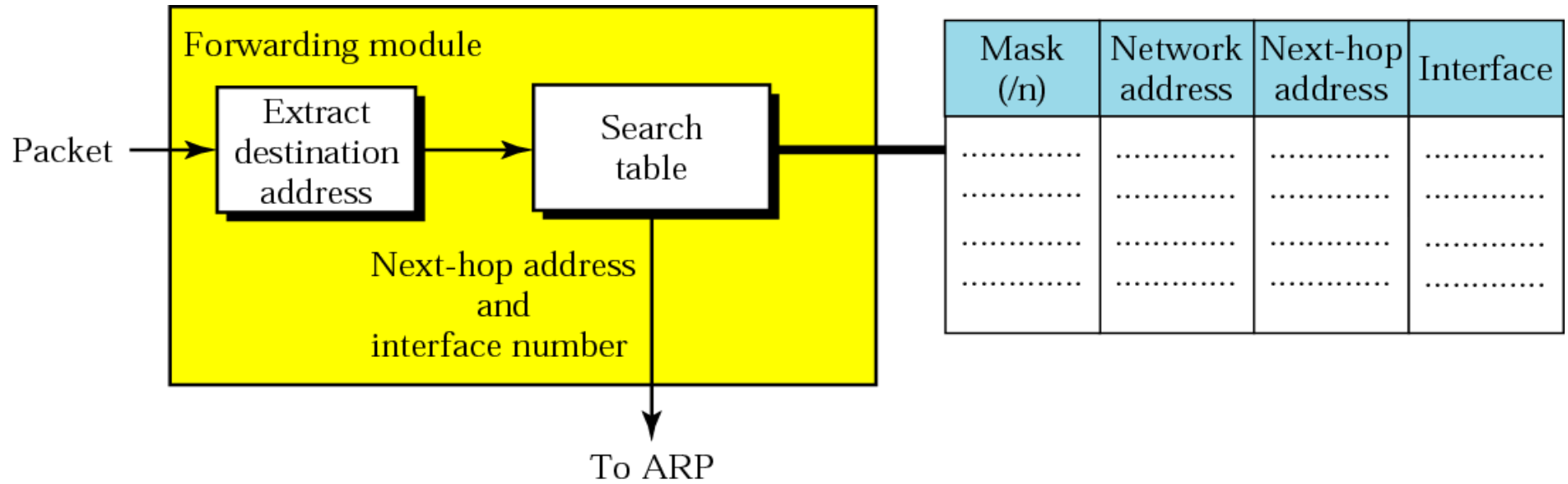
*Upon completion you will be able to:*

- *Understand the different types of delivery and the connection*
- *Understand forwarding techniques in classful addressing*
- *Understand forwarding techniques in classless addressing*
- *Understand how a routing table works*
- *Understand the structure of a router*



*In classful addressing we can have a routing table with three columns; in classless addressing, we need at least four columns.*

**Figure 6.12** *Simplified forwarding module in classless address*



- In classless addressing, the whole address space is one entity; there are no classes.
- This means that forwarding requires one row of information for each block involved.
- The table needs to be searched based on the network address (first address in the block).
- The destination address in the packet gives no clue about the network address (as it does in classful addressing).
- To solve the problem, we need to include the mask (/n) in the table; we need to have an extra column that includes the mask for the corresponding block.



## ***EXAMPLE 7***

*Make a routing table for router R1 using the configuration in Figure 6.13.*

**See Next Slide**

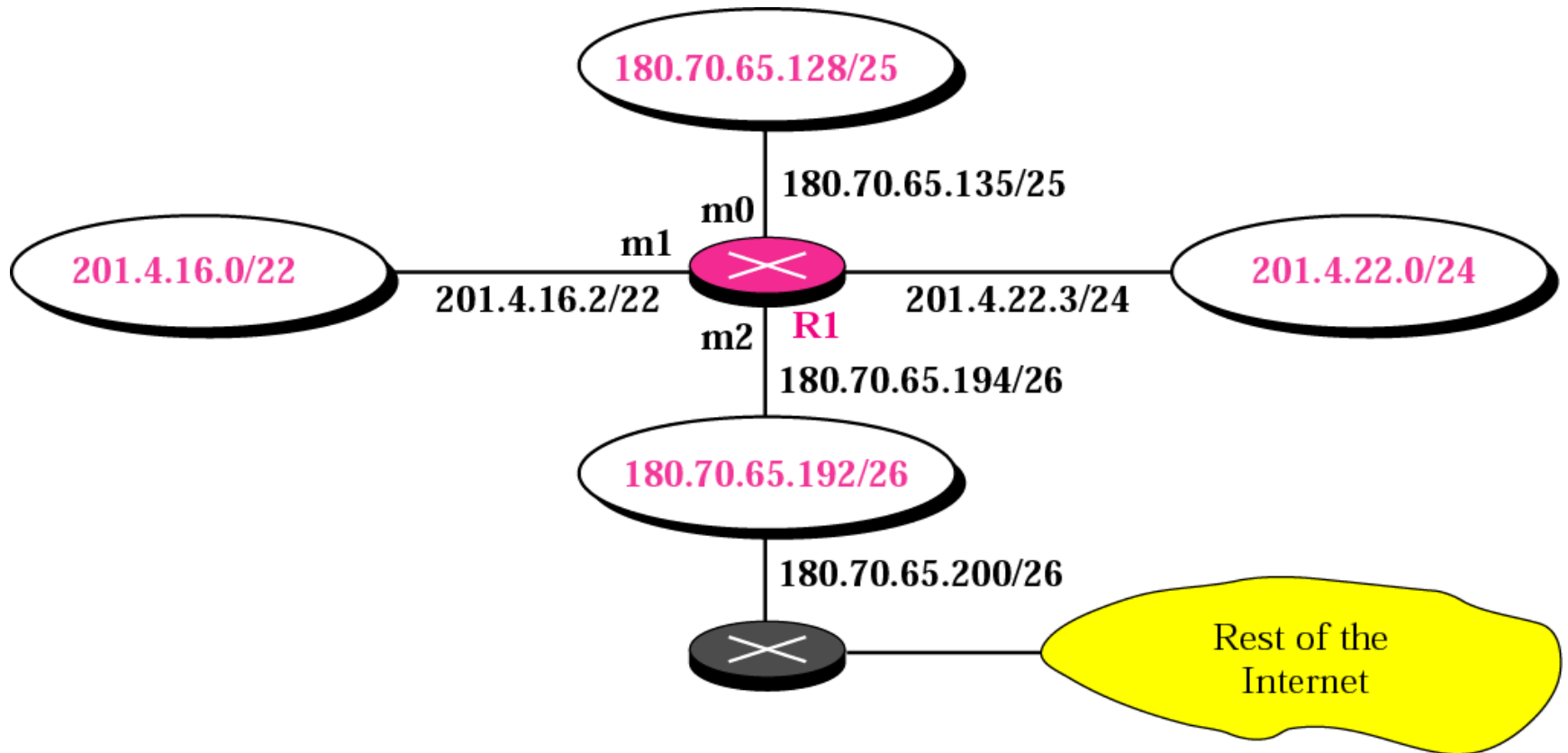
### ***Solution***

*Table 6.1 shows the corresponding table.*

**See the table after the figure.**



**Figure 6.13** *Configuration for Example 7*



***Table 6.1 Routing table for router R1 in Figure 6.13***

<i>Mask</i>	<i>Network Address</i>	<i>Next Hop</i>	<i>Interface</i>
<i>/26</i>	180.70.65.192	-	m2
<i>/25</i>	180.70.65.128	-	m0
<i>/24</i>	201.4.22.0	-	m3
<i>/22</i>	201.4.16.0	....	m1
Default	Default	180.70.65.200	m2



## ***EXAMPLE 8***

*Show the forwarding process if a packet arrives at R1 in Figure 6.13 with the destination address **180.70.65.140**.*

### ***Solution***

*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.*

**See Next Slide**



## ***EXAMPLE 8 (CONTINUED)***

***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 (the destination address of the packet in this case) and the interface number m0 are passed to ARP for further processing.***



## ***EXAMPLE 9***

*Show the forwarding process if a packet arrives at R1 in Figure 6.13 with the destination address **201.4.22.35**.*

### ***Solution***

*The router performs the following steps:*

**See Next Slide**



## ***EXAMPLE 9 (CONTINUED)***

- 1. The first mask (/26) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 1).*
- 2. The second mask (/25) is applied to the destination address. The result is 201.4.22.0, which does not match the corresponding network address (row 2).*
- 3. The third mask (/24) is applied to the destination address. The result is 201.4.22.0, which matches the corresponding network address. The destination address of the package and the interface number m3 are passed to ARP.*



## ***EXAMPLE 10***

*Show the forwarding process if a packet arrives at R1 in Figure 6.13 with the destination address **18.24.32.78**.*

### ***Solution***

*This time all masks are applied to the destination address, but no matching network address is found. When it reaches the end of the table, the module gives the next-hop address 180.70.65.200 and interface number m2 to ARP. This is probably an outgoing package that needs to be sent, via the default router, to some place else in the Internet.*



## ***EXAMPLE 11***

*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 6.2. Can we draw its topology?*

**See Next Slide**



***Table 6.2 Routing table for Example 11***

<i>Mask</i>	<i>Network Address</i>	<i>Next-Hop Address</i>	<i>Interface Number</i>
/26	140.6.12.64	180.14.2.5	m2
/24	130.4.8.0	190.17.6.2.0	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



## ***EXAMPLE 11*** (CONTINUED)

### ***Solution***

*We know some facts but we don't have all for a definite topology. We know that router R1 has three interfaces: m0, m1, and m2. We know that there are three networks directly connected to router R1. We know that there are two networks indirectly connected to R1. There must be at least three other routers involved (see next-hop column). We know to which networks these routers are connected by looking at their IP addresses. So we can put them at their appropriate place.*

**See Next Slide**

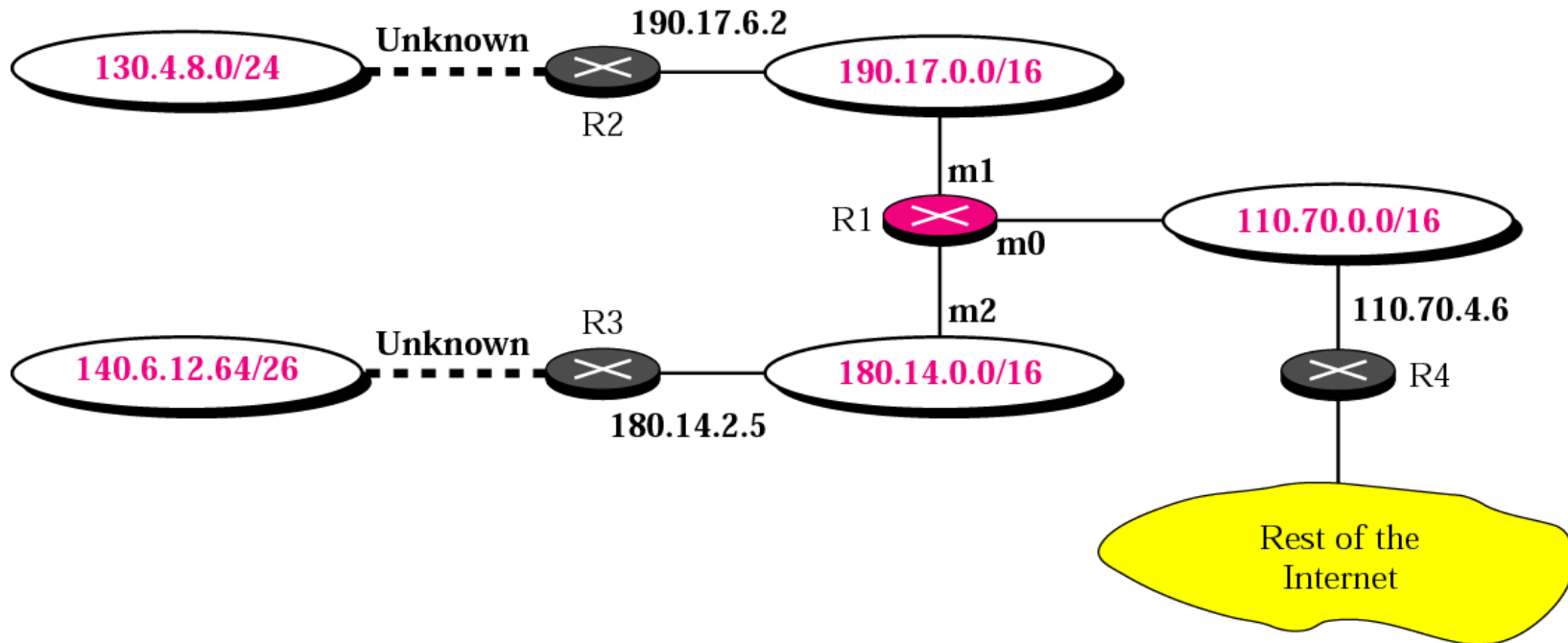


## ***EXAMPLE 11 (CONTINUED)***

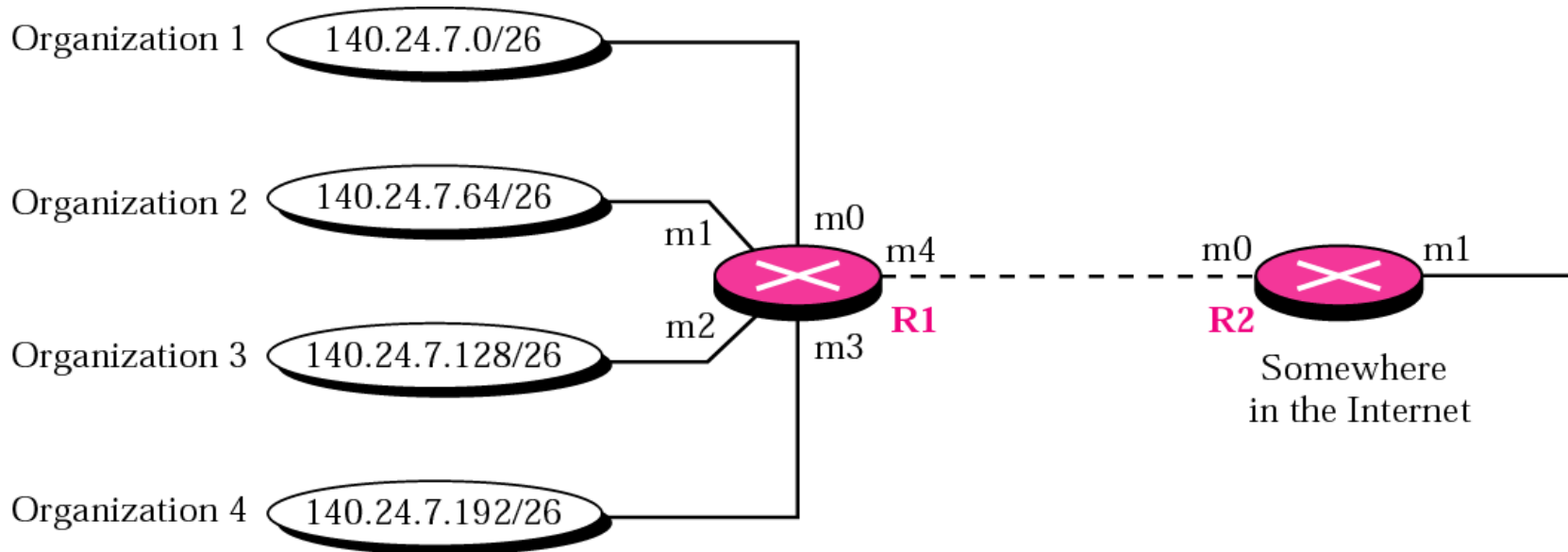
*We know that one router, the default router, is connected to the rest of the Internet. But there is some missing information. We do not know if network 130.4.8.0 is directly connected to router R2 or through a point-to-point network (WAN) and another router. We do not know if network 140.6.12.64 is connected to router R3 directly or through a point-to-point network (WAN) and another router. Point-to-point networks normally do not have an entry in the routing table because no hosts are connected to them. Figure 6.14 shows our guessed topology.*

**See Next Slide**

**Figure 6.14** *Guessed topology for Example 6*



**Figure 6.15** *Address aggregation*



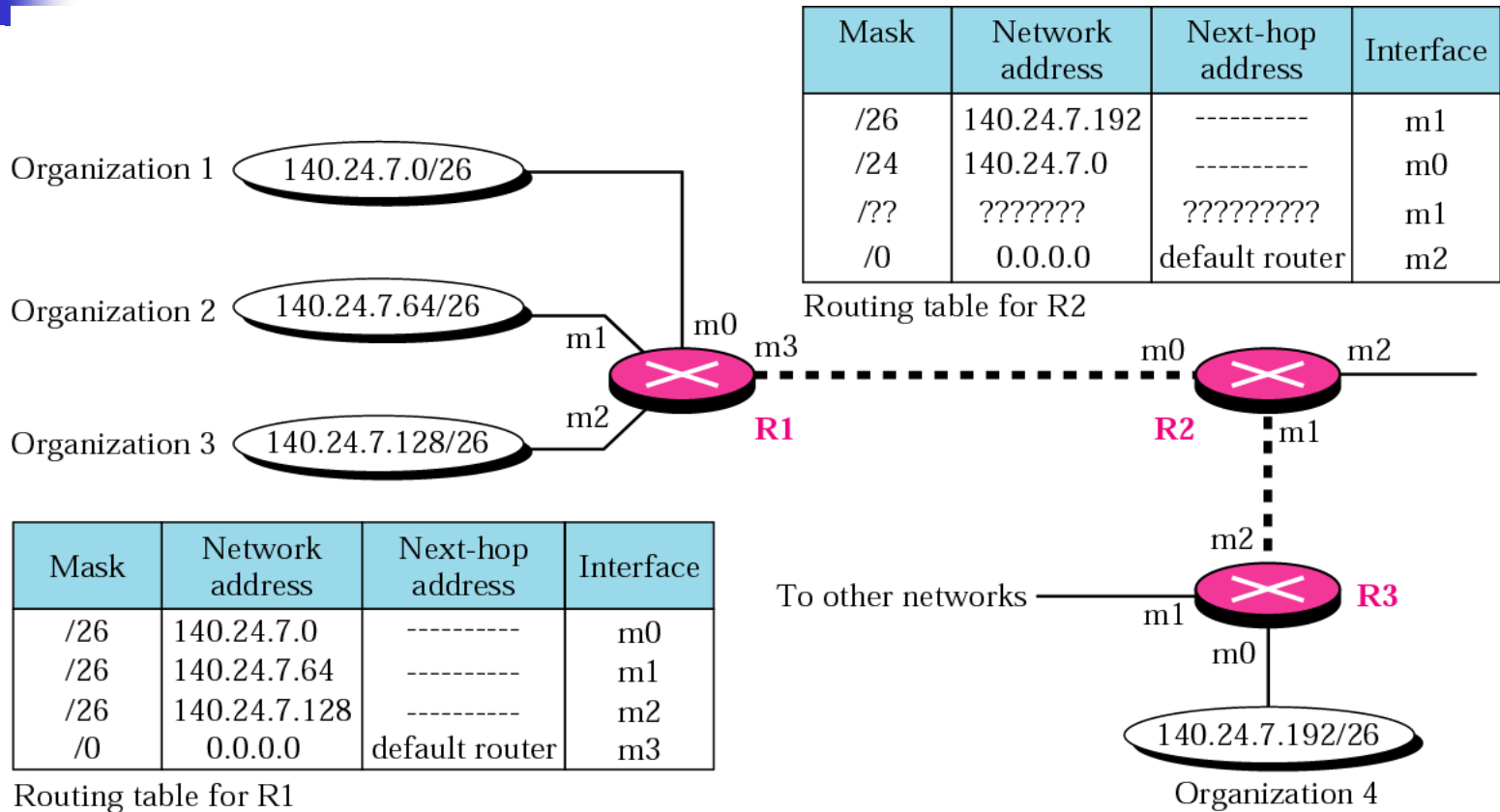
Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	-----	m0
/26	140.24.7.64	-----	m1
/26	140.24.7.128	-----	m2
/26	140.24.7.192	-----	m3
/0	0.0.0.0	default router	m4

Routing table for R1

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

Routing table for R2

**Figure 6.16** Longest mask matching



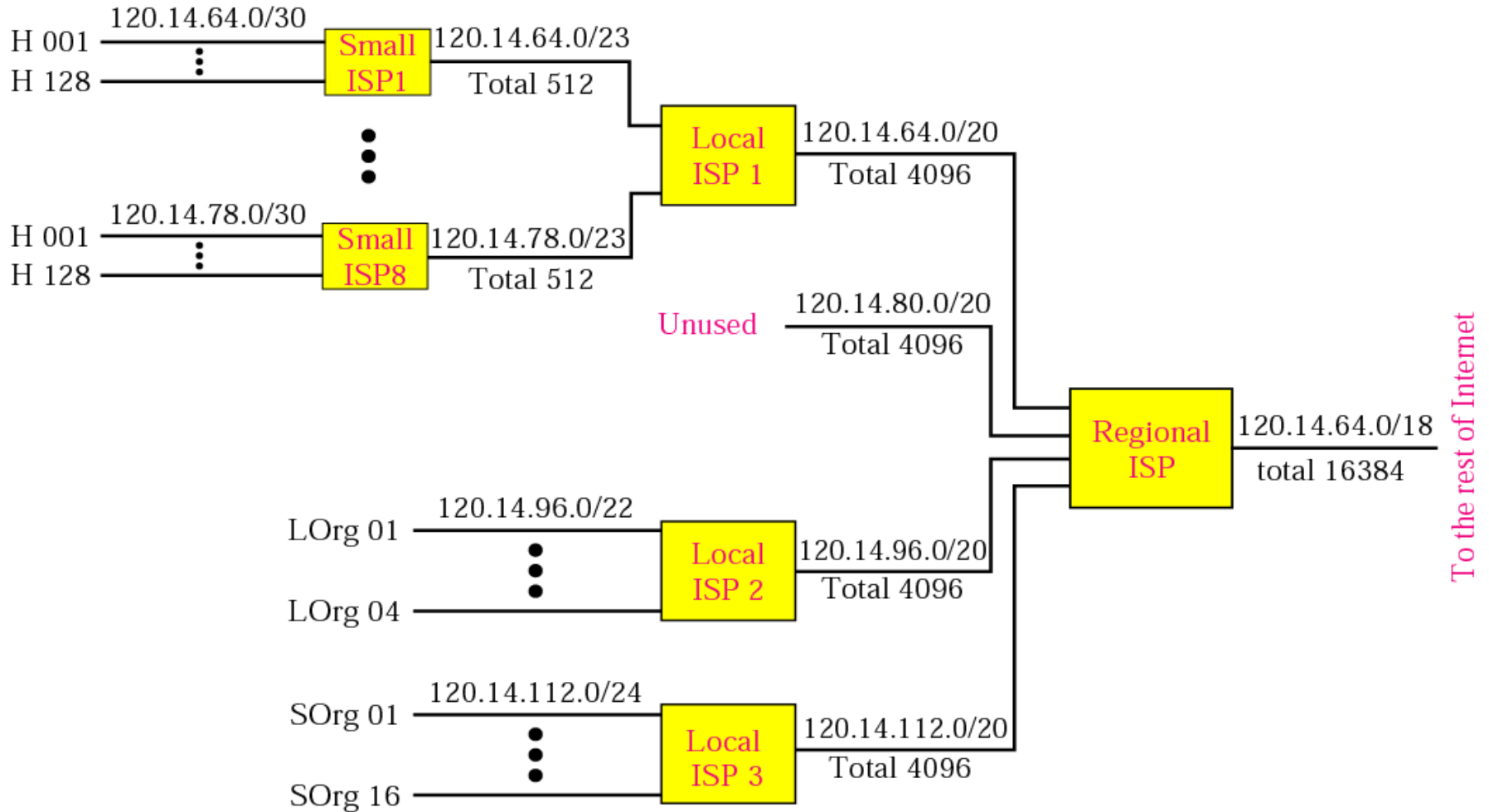


## ***EXAMPLE 12***

*As an example of hierarchical routing, let us consider Figure 6.17. A regional ISP is granted 16384 addresses starting from 120.14.64.0. The regional ISP has decided to divide this block into four 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.*

**See Next Slide**

**Figure 6.17** *Hierarchical routing with ISPs*







## ***EXAMPLE 12 (CONTINUED)***

*The first local ISP has divided its assigned subblock into 8 smaller blocks and assigned each to a small ISP. Each small ISP provides services to 128 households (H001 to H128), each using four addresses. Note that the mask for each small ISP is now /23 because the block is further divided into 8 blocks. Each household has a mask of /30, because a household has only 4 addresses ( $2^{32-30}$  is 4).*

*The second local ISP has divided its block into 4 blocks and has assigned the addresses to 4 large organizations (LOrg01 to LOrg04). Note that each large organization has 1024 addresses and the mask is /22.*

**See Next Slide**



## ***EXAMPLE 12 (CONTINUED)***

*The third local ISP has divided its block into 16 blocks and assigned each block to a small organization (SOrg01 to SOrg15). Each small organization has 256 addresses and the mask is /24.*

*There is a sense of hierarchy in this configuration. All routers in the Internet send a packet with destination address 120.14.64.0 to 120.14.127.255 to the regional ISP. The regional ISP sends every packet with destination address 120.14.64.0 to 120.14.79.255 to Local ISP1. Local ISP1 sends every packet with destination address 120.14.64.0 to 120.14.64.3 to H001.*

# Forwarding Based on Label

- *In 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 connectionless network (datagram approach), a router forwards a packet based on the destination address in the header of packet. On the other hand, in a connection-oriented network (virtual-circuit approach), a switch forwards a packet based on the label attached to a 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.*
- *Later IETF approved a standard that is called Multi-Protocol Label Switching. In this standard, some conventional routers in the Internet can be replaced by MPLS routers that can behave like a router and a switch. 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.*

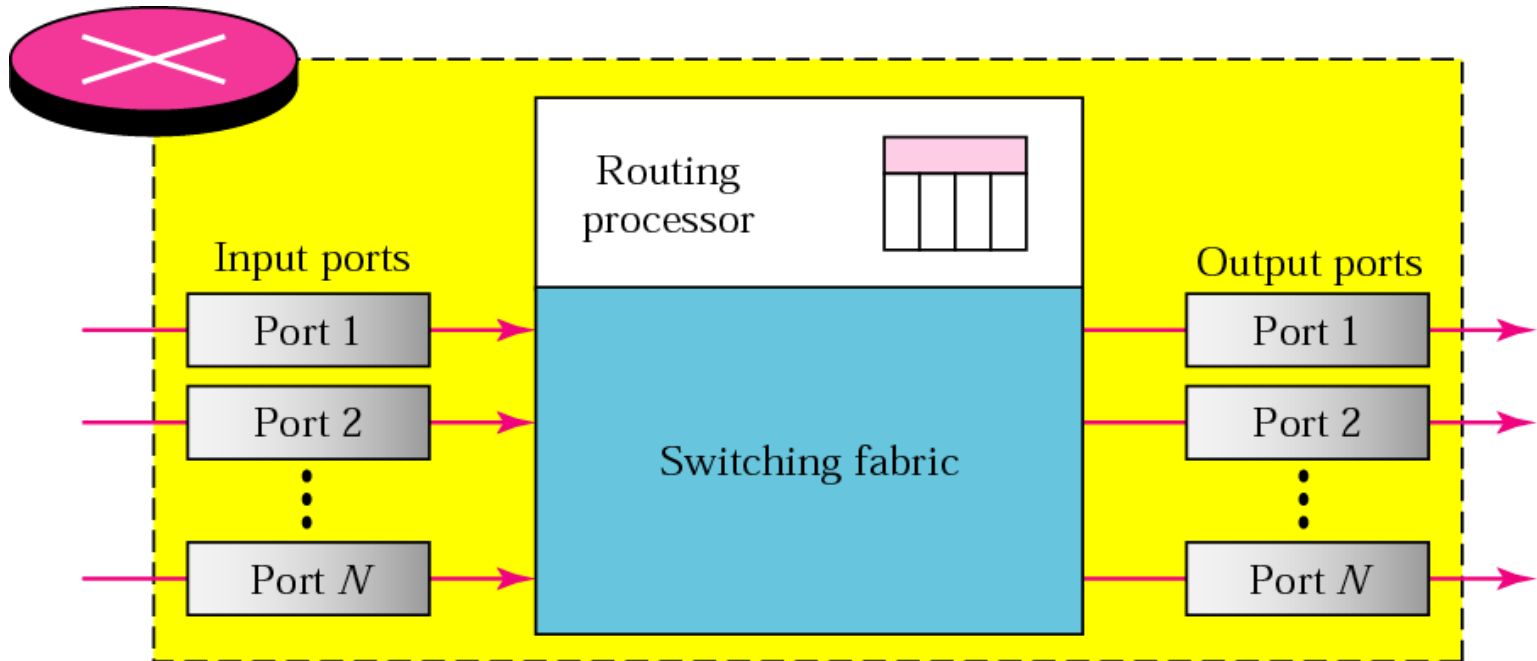
## 6.4 STRUCTURE OF A ROUTER

*We represent a router as a black box that accepts incoming packets from one of the input ports (interfaces), uses a routing table to find the departing output port, and sends the packet from this output port.*

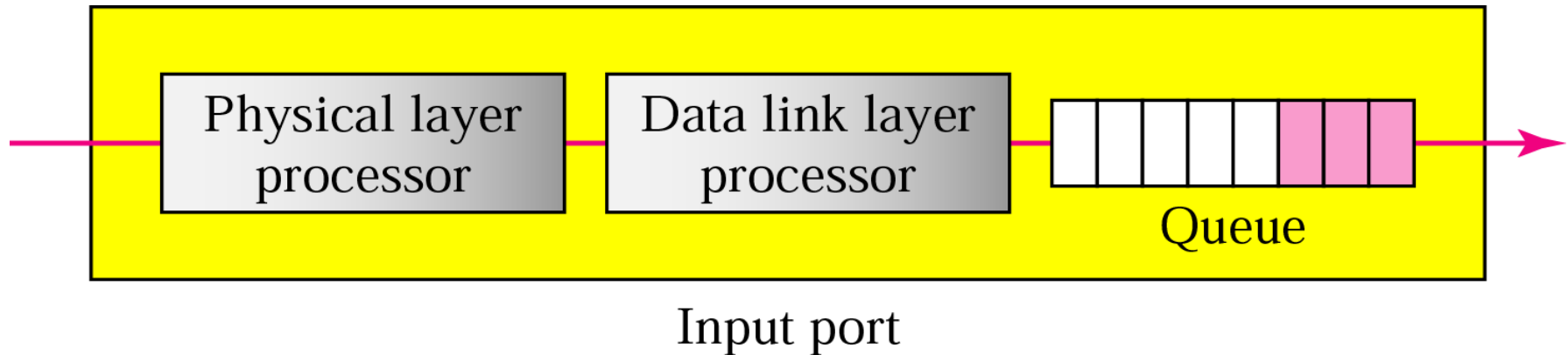
*The topics discussed in this section include:*

*Components*

**Figure 6.20** *Router components*

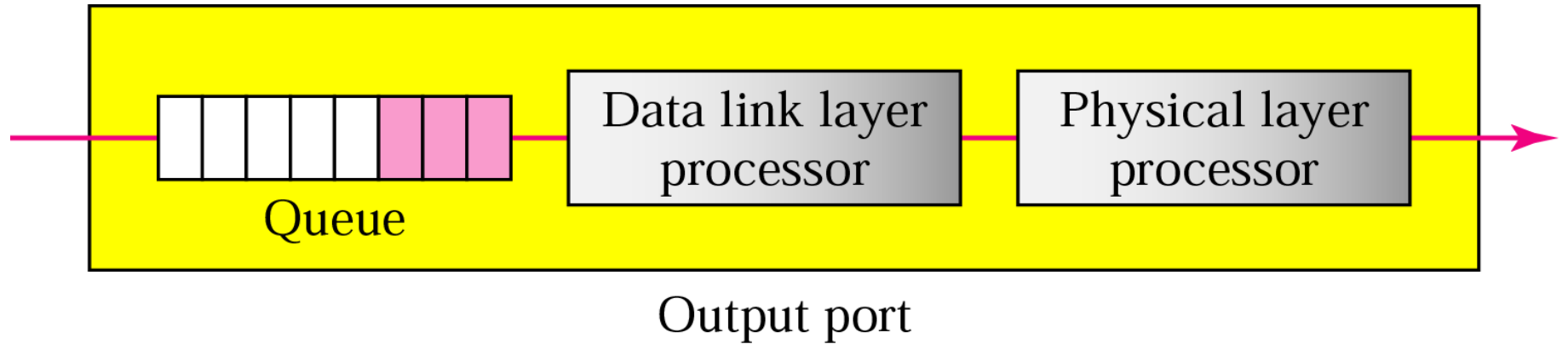


**Figure 6.21** *Input port*



*An input port performs the physical and data link layer functions of the router. The bits are constructed from the received signal. The packet is decapsulated from the frame. Errors are detected and corrected. The packet is ready to be forwarded by the network layer. In addition to a physical layer processor and a data link processor, the input port has buffers (queues) to hold the packets before they are directed to the switching fabric.*

**Figure 6.22** *Output port*



*An output port performs the same functions as the input port, but in the reverse order. First the outgoing packets are queued, then the packet is encapsulated in a frame, and finally the physical layer functions are applied to the frame to create the signal to be sent on the line.*

### *Routing Processor*

*The routing processor performs the functions of the network layer. The destination address is used to find the address of the next hop and, at the same time, the output port number from which the packet is sent out.*

### *Switching Fabrics*

*The most difficult task in a router is to move the packet from the input queue to the output queue. The speed with which this is done affects the size of the input/output queue and the overall delay in packet delivery.*



# Network Address Translation

## NAT



# The IPv4 Shortage

2

- ❑ Problem: consumer ISPs typically only give one IP address per-household
  - ❑ Additional IPs cost extra
  - ❑ More IPs may not be available
- ❑ Today's households have more networked devices than ever
  - ❑ Laptops and desktops
  - ❑ TV, bluray players, game consoles
  - ❑ Tablets, smartphones, eReaders
- ❑ How to get all these devices online?

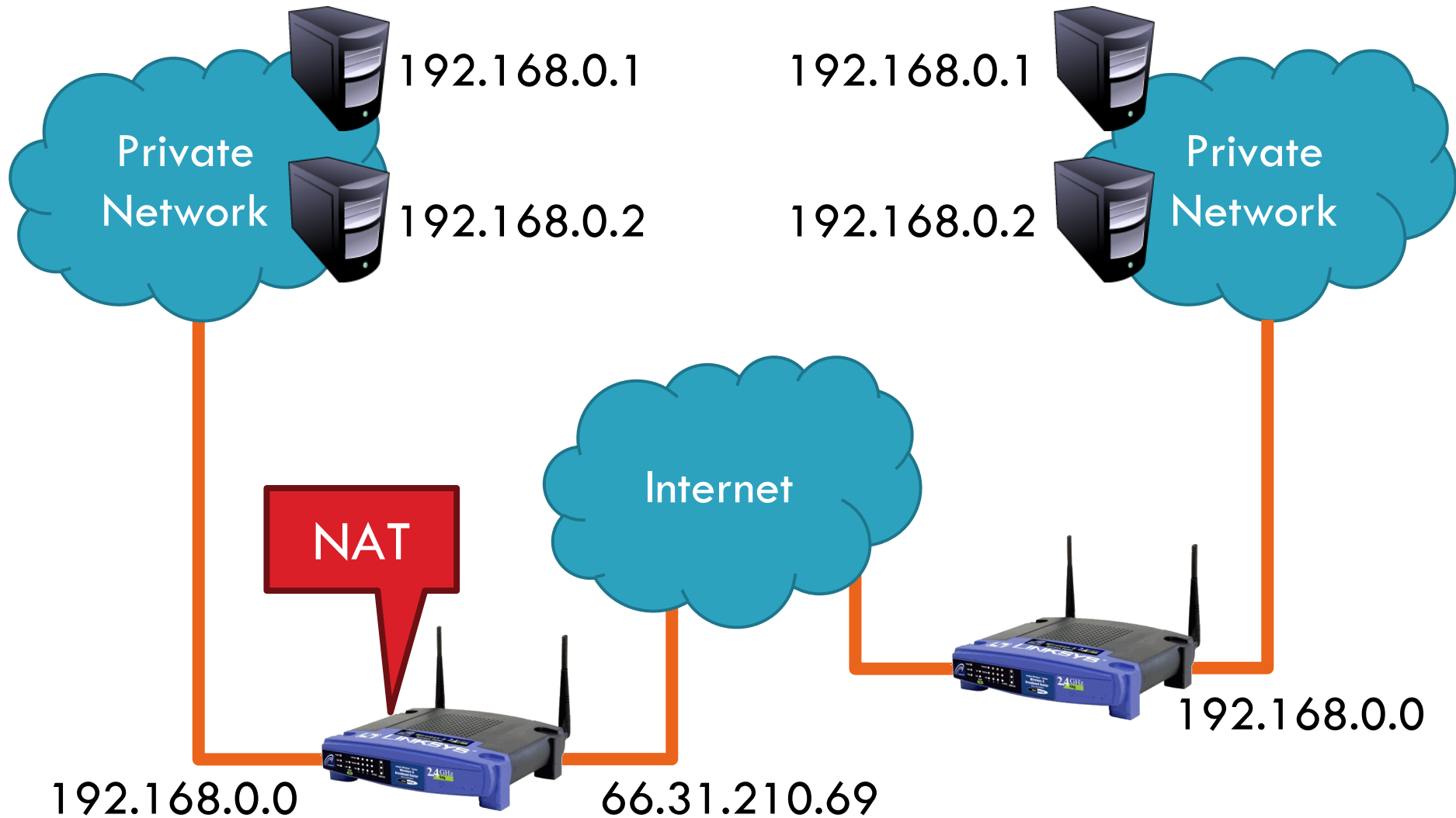
# Private IP Networks

3

- ❑ Idea: create a range of private IPs that are separate from the rest of the network
  - ❑ Use the private IPs for internal routing
  - ❑ Use a special router to bridge the LAN and the WAN
- ❑ Properties of private IPs
  - ❑ Not globally unique
  - ❑ Usually taken from non-routable IP ranges (why?)
- ❑ Typical private IP ranges
  - ❑ 10.0.0.0 – 10.255.255.255
  - ❑ 172.16.0.0 – 172.31.255.255
  - ❑ 192.168.0.0 – 192.168.255.255

# Private Networks

4



# Network Address Translation (NAT)

5

- NAT allows hosts on a private network to communicate with the Internet
  - ▣ Warning: connectivity is not seamless
- Special router at the boundary of a private network
  - ▣ Replaces internal IPs with external IP
    - This is “Network Address Translation”
  - ▣ May also replace TCP/UDP port numbers
- Maintains a table of active flows
  - ▣ Outgoing packets initialize a table entry
  - ▣ Incoming packets are rewritten based on the table

# Basic NAT Operation

6

## Private Network

## Internet

Source: 192.168.0.1  
Dest: 74.125.228.67

Source: 66.31.210.69  
Dest: 74.125.228.67

### Private Address

192.168.0.1:2345

### Public Address

74.125.228.67:80



192.168.0.1



66.31.210.69



74.125.228.67

Source: 74.125.228.67  
Dest: 192.168.0.1

Source: 74.125.228.67  
Dest: 66.31.210.69

# Advantages of NATs

7

- Allow multiple hosts to share a single public IP
- Allow migration between ISPs
  - ▣ Even if the public IP address changes, you don't need to reconfigure the machines on the LAN
- Load balancing
  - ▣ Forward traffic from a single public IP to multiple private hosts



# Natural Firewall

8

**Private Network**

**Internet**

**Private Address**

**Public Address**



192.168.0.1



66.31.210.69



74.125.228.67

Source: 74.125.228.67  
Dest: 66.31.210.69





# Port Forwarding

9

## Private Network

## Internet

Private Address

Public Address

192.168.0.1:7000

\*.\*.\*.\*.\*



192.168.0.1



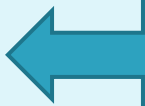
66.31.210.69



74.125.228.67

Source: 74.125.228.67:8679  
Dest: 192.168.0.1:7000

Source: 74.125.228.67:8679  
Dest: 66.31.210.69:7000



# Concerns About NAT

10

- ❑ Performance/scalability issues
  - ❑ Per flow state!
  - ❑ Modifying IP and Port numbers means NAT must recompute IP and TCP checksums
- ❑ Breaks the layered network abstraction
- ❑ Breaks end-to-end Internet connectivity
  - ❑ 192.168.\*.\* addresses are private
  - ❑ Cannot be routed to on the Internet
  - ❑ Problem is worse when **both** hosts are behind NATs
- ❑ What about IPs embedded in data payloads?

# Concerns about NAT

## □ **Performance:**

- Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
- Modifying port number requires that NAT boxes recalculate TCP checksum

## □ **Fragmentation**

- Care must be taken that a datagram that is fragmented before it reaches the NAT device, is not assigned a different IP address or different port numbers for each of the fragments.

# Concerns about NAT

## □ **End-to-end connectivity:**

- NAT destroys universal end-to-end reachability of hosts on the Internet.
- A host in the public Internet often cannot initiate communication to a host in a private network.
- The problem is worse, when two hosts that are in a private network need to communicate with each other.



# *Unicast Routing Protocols: RIP, OSPF, and BGP*

---

## **Objectives**

*Upon completion you will be able to:*

- *Distinguish between intra and interdomain routing*
- *Understand distance vector routing and RIP*
- *Understand link state routing and OSPF*
- *Understand path vector routing and BGP*

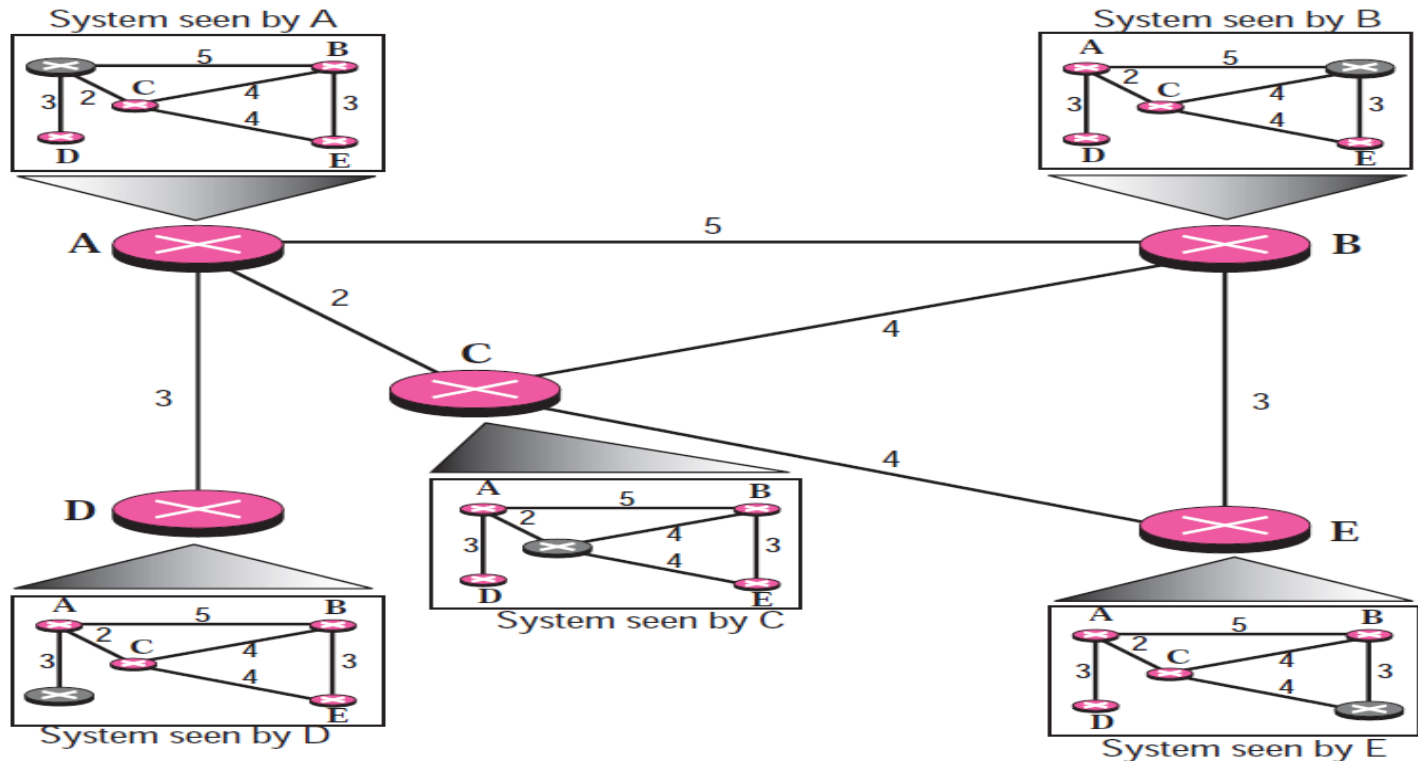
# LINK STATE ROUTING

*In link state routing, if each node in the domain has the entire topology of the domain, the node can use Dijkstra's algorithm to build a routing table.*

*The topics discussed in this section include:*

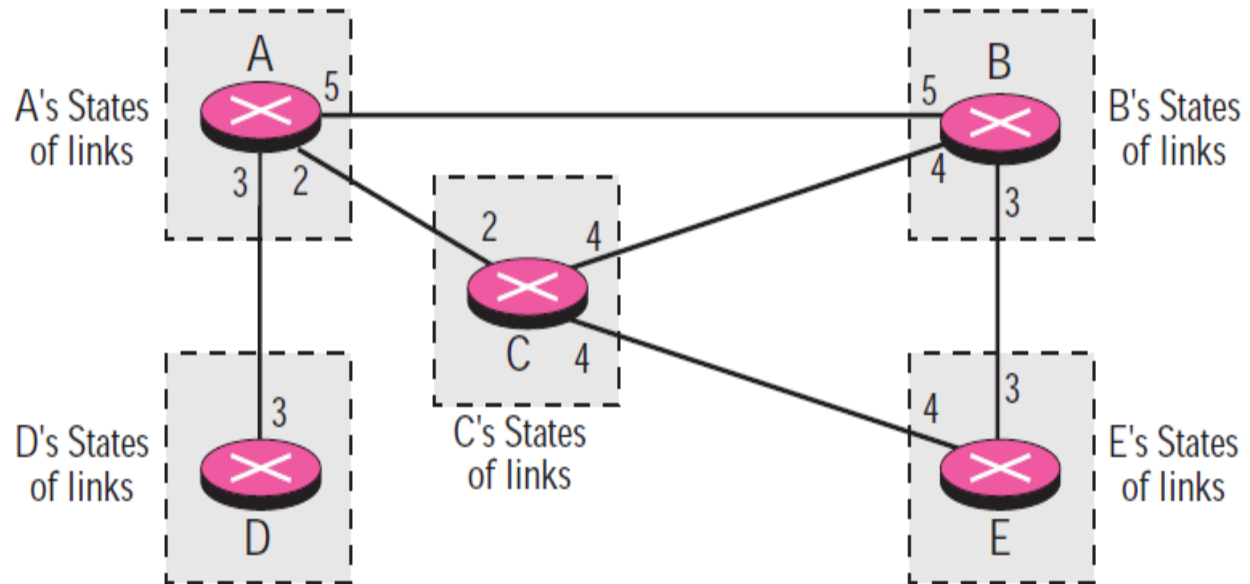
*Building Routing Tables*

## Concept of link state routing



The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. This is analogous to a city map. Two persons in two different cities may have the same map, but each needs to take a different route to reach his destination.

## Link state knowledge



Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3. Node C knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4. Node D knows that it is connected only to node A with metric 3. And so on. Although there is an overlap in the knowledge, the overlap guarantees the creation of a common topology: a picture of the whole domain for each node.



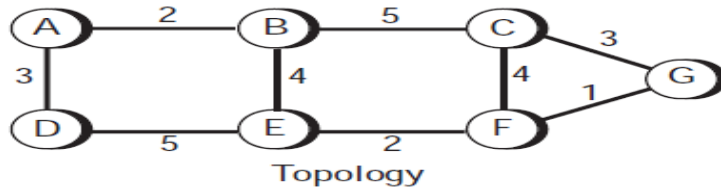
## 1. Building Routing Table

1. Creation of the states of the links by each node, called the link state packet or LSP
2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way
3. Formation of a shortest path tree for each node
4. Calculation of a routing table based on the shortest path tree

## 2. Creation of LSP

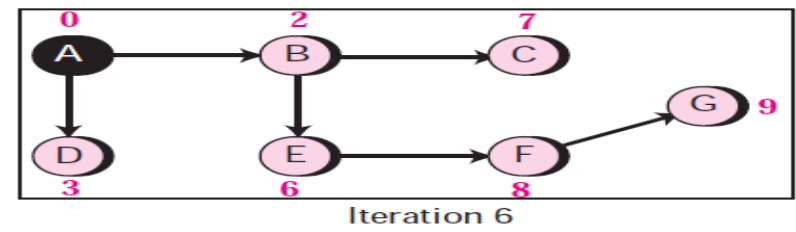
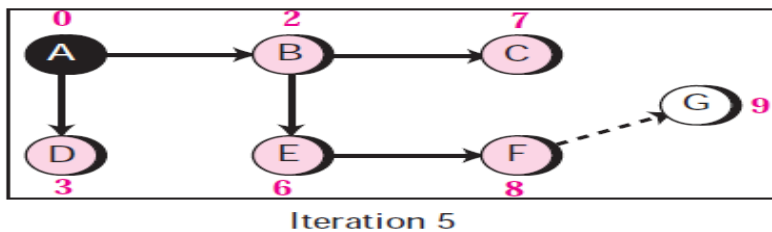
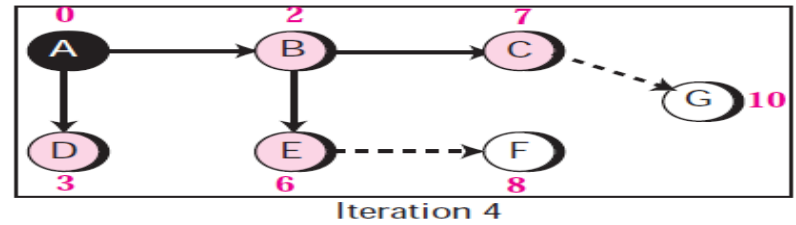
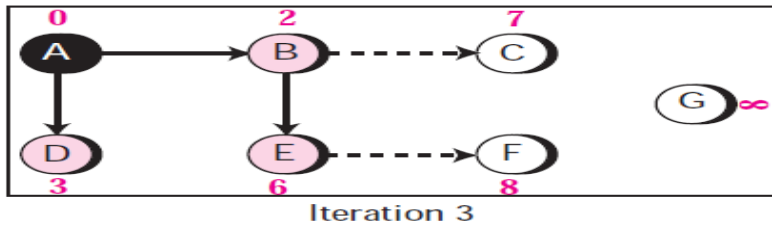
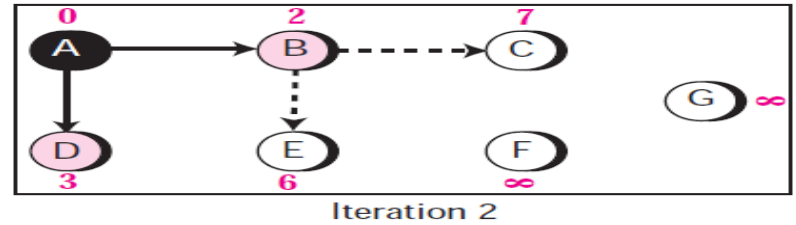
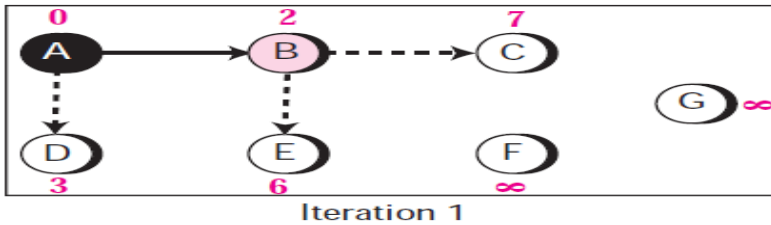
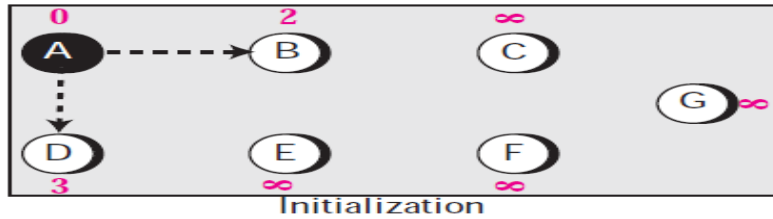
- When there is a change in the topology of the domain
- On a periodic basis
  - 60 minutes or 2 hours

# Example of formation of shortest path tree



**Legend**

- Root node
- Node in the path
- Node not in the path
- Path



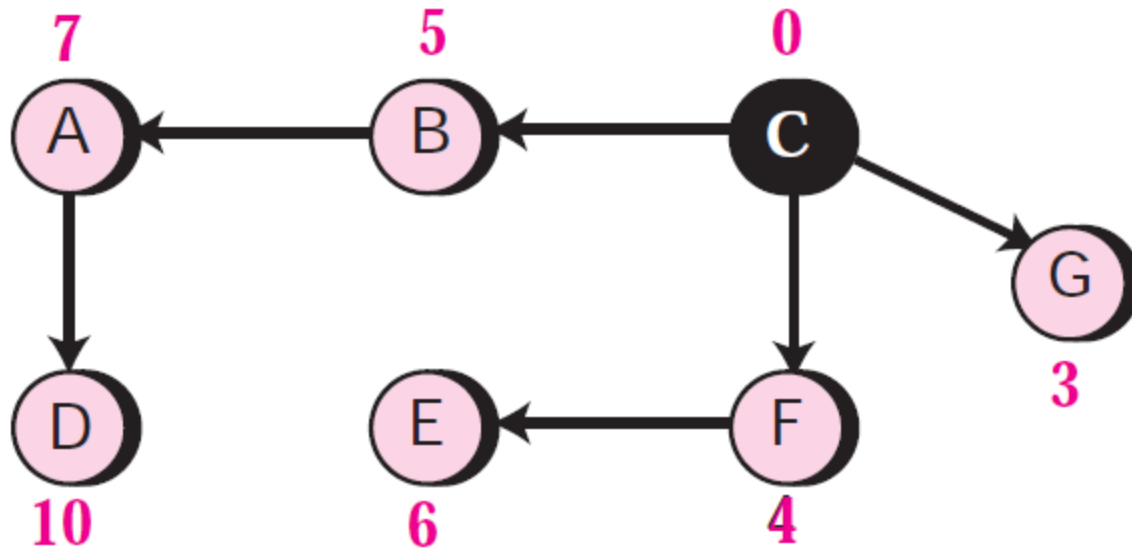
## *Example of formation of shortest path tree*

- In each iteration, the next node with minimum distance is selected and added to the path. Then all shortest distances are updated with respect to the last node selected. For example, in the first iteration, node B is selected and added to the path and the shortest distances are updated with respect to node B (The shortest distances for C and E are changed, but for the others remain the same). After six iterations, the shortest path tree is found for node A. Note that in iteration 4, the shortest path to G is found via C, but in iteration 5, a new shortest route is discovered (via G); the previous path is erased and the new one is added.

## *Routing table for node A*

<i>Destination</i>	<i>Cost</i>	<i>Next Router</i>
A	0	—
B	2	—
C	7	B
D	3	—
E	6	B
F	8	B
G	9	B

# Example for solving



- To show that the shortest path tree for each node is different, we found the shortest path tree as seen by node C. We leave the detail as an exercise.

# Open shortest Path First (OSPF)

*The Open Shortest Path First (OSPF) protocol is an intradomain routing protocol based on link state routing. Its domain is also an autonomous system.*

*The topics discussed in this section include:*

*Areas*

*Metric*

*Types of Links*

*Graphical Representation*

*OSPF Packets*

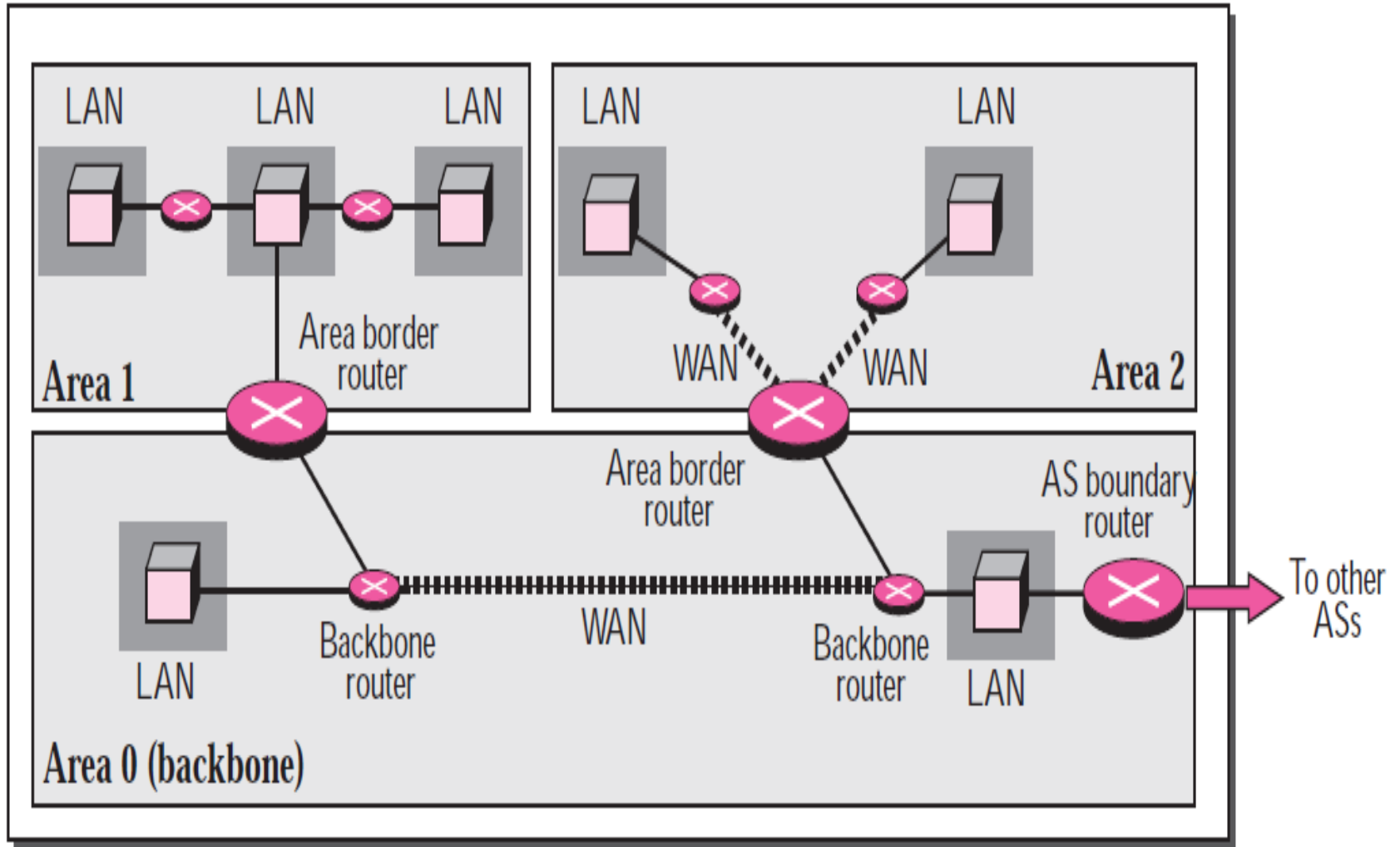
*Link State Update Packet*

*Other Packets*

*Encapsulation*

# Areas in an autonomous system

## Autonomous System (AS)



## ■ **Areas**

- Is a collection of networks, hosts, and routers in AS
- AS can be divided into many different areas.
- All networks inside an area must be connected.
- Routers inside an area flood the area with routing information.

## ■ **Area Border Router**

- Summarizes the information about the area and sends it to other areas

## ■ **Backbone**

- All of the areas inside an AS must be connected to the backbone
- Serving as a primary area
- Consisting of backbone routers
- Backbone routers can be an area border router



## ■ Metric

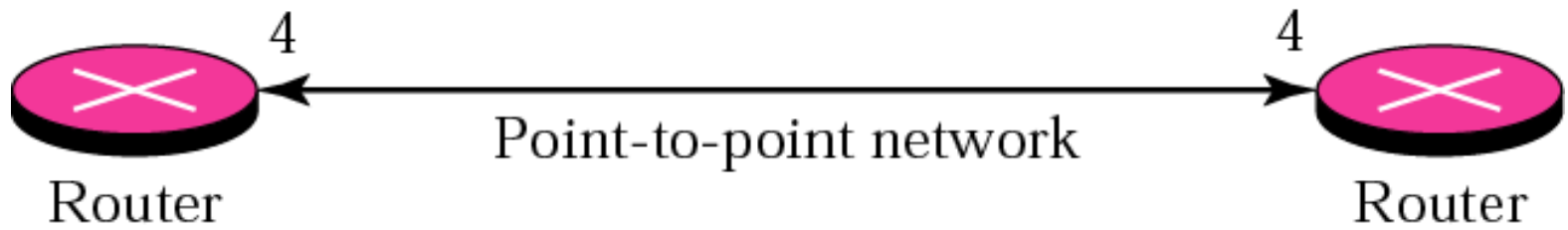
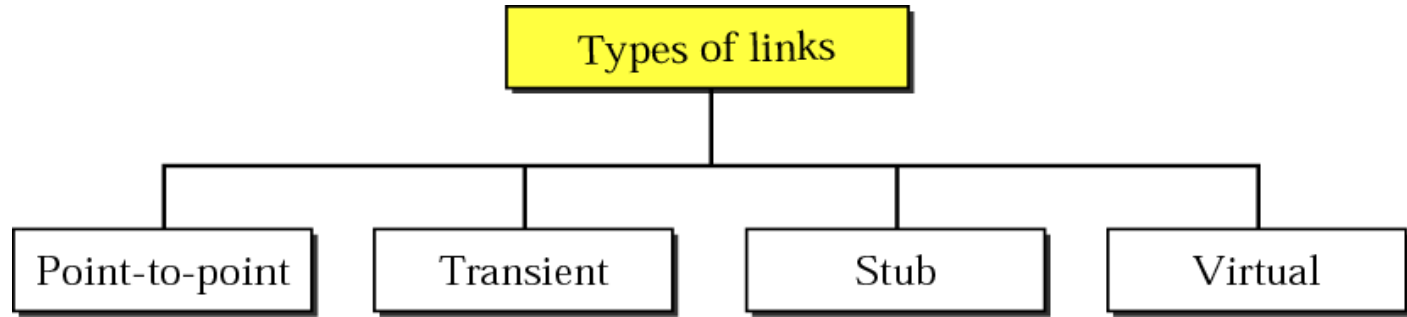
- OSPF protocol allows the administrator to assign a cost, called the *metric*, to each route
- Based on a type of service (minimum delay, maximum throughput, and so on)
- A router can have multiple routing tables, each based on a different type of service.

## ■ Link State Routing

- OSPF uses Link State Routing to update the routing tables in an area
- Each router shares its knowledge about its neighborhood with every router in the area.

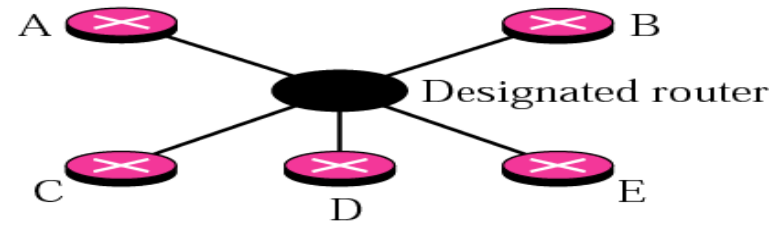
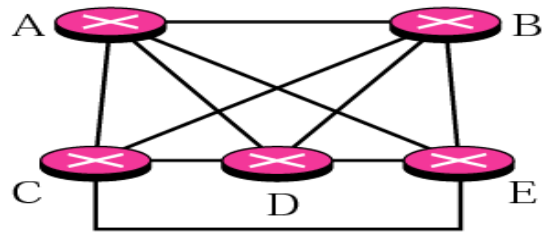
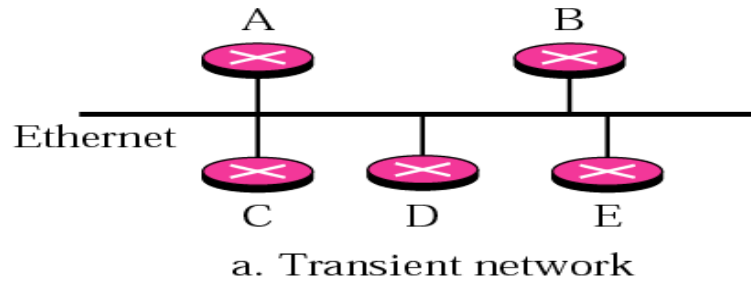
1. Sharing knowledge about the neighborhood
2. Sharing with every other router by *flooding*
3. Sharing when there is a change
  - cf. Distance Vector Routing : sending the information at regular intervals regardless of change
  - So, every router can calculate the shortest path between itself and each network

# Types of links



- 1. Point to point link:** connects two routers without any other host or router in between. In other words, the purpose of the link (network) is just to connect the two routers.

# Transient link



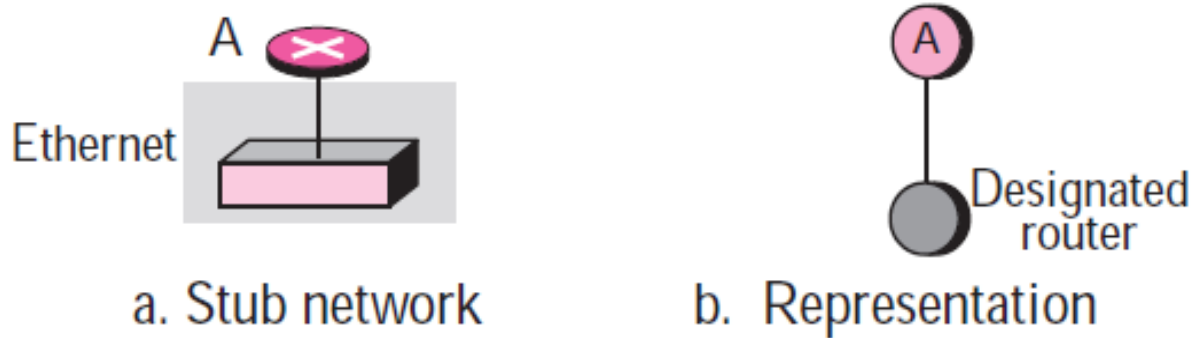
**A-Transient Link:** A transient link is a network with several routers attached to it. The data can enter through any of the routers and leave through any router. All LANs and some WANs with two or more routers are of this type.

**B-** It is not realistic, because there is no single network (link) between each pair of routers; there is only one network that serves as a crossroad between all five routers.

**C-** To show that each router is connected to every other router through one single network, One of the routers in the network takes this responsibility.

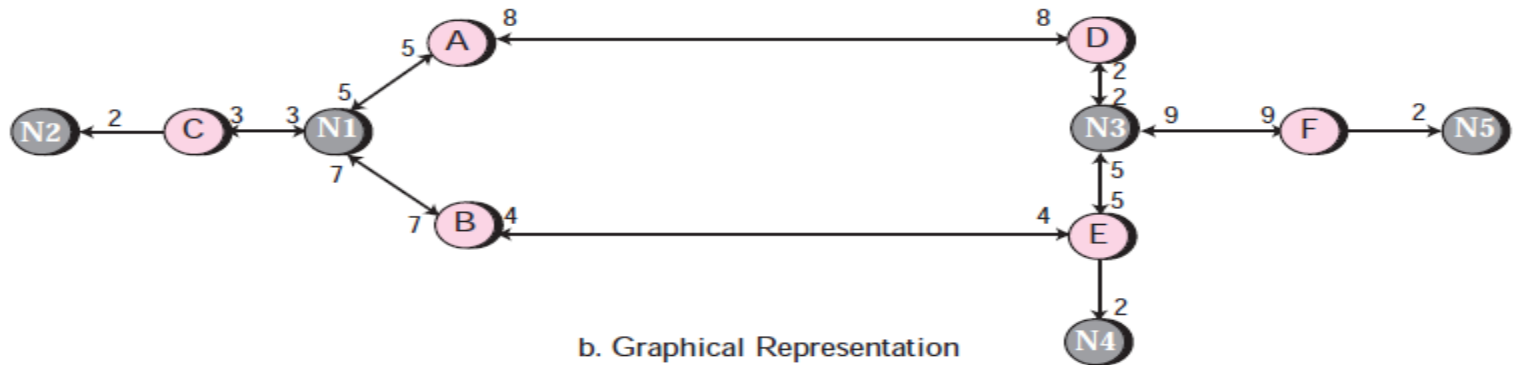
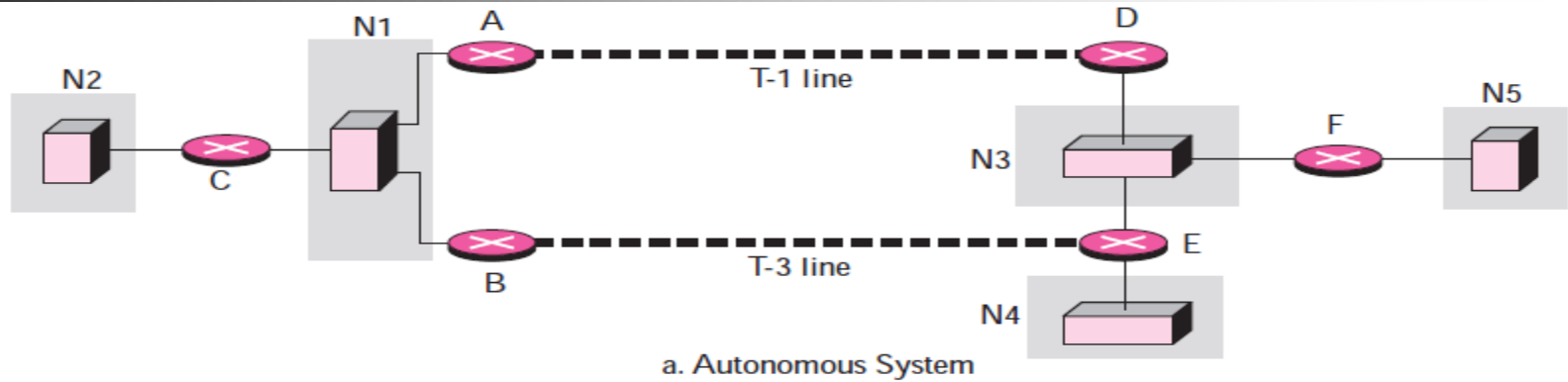
It is assigned a dual purpose; it is a true router and a designated router. We can use the topology shown in c to show the connections of a transient network.

## *stub and virtual link*



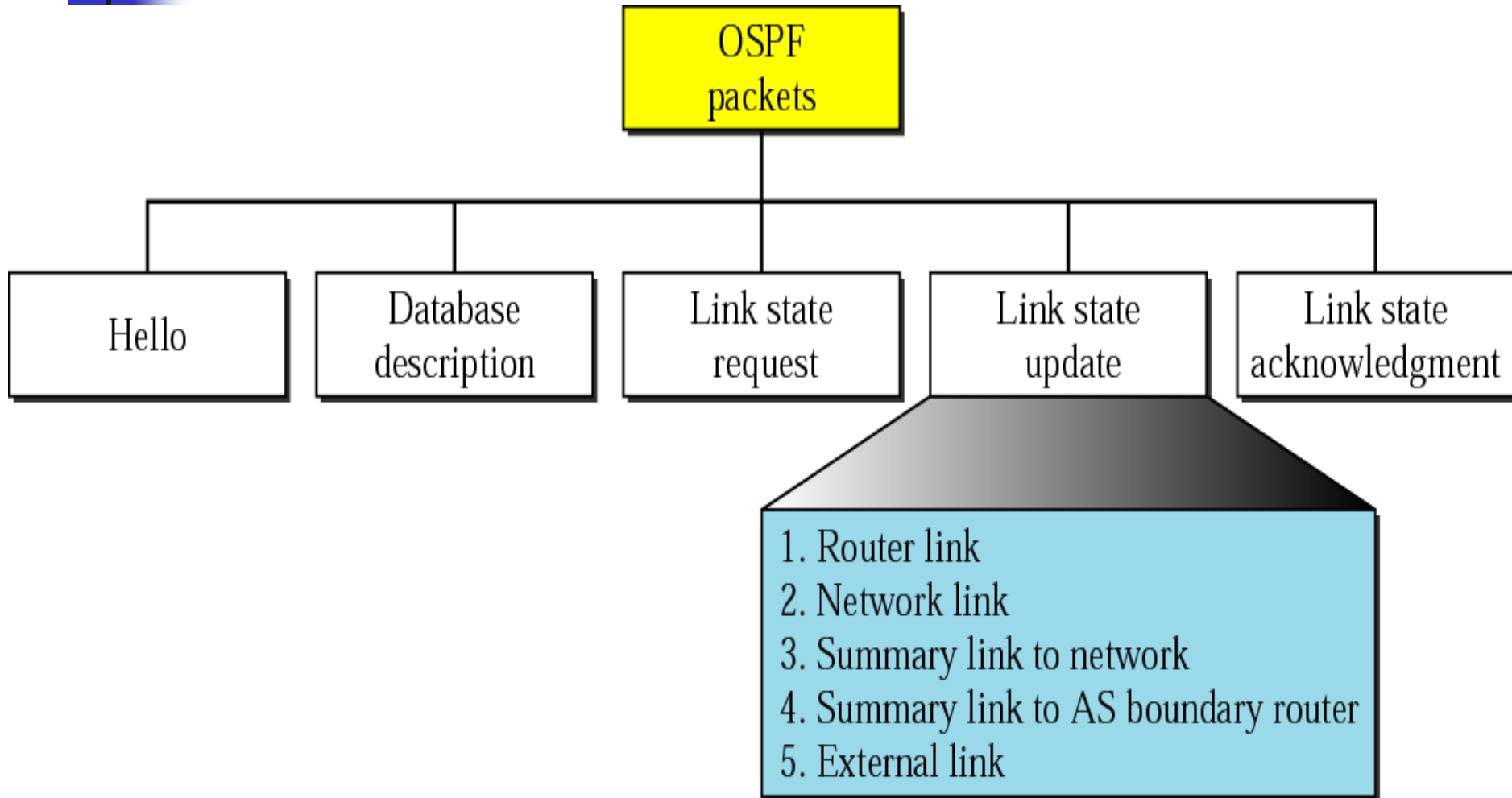
- 3. A stub link** is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same router. This is a special case of the transient network. We can show this situation using the router as a node and using the designated router for the network. However, the link is only one directional, from the router to the network.
- 4. Virtual Link** When the link between two routers is broken, the administration may create a virtual link between them using a longer path that probably goes through several routers.

## Example of an AS and its graphical representation in OSPF

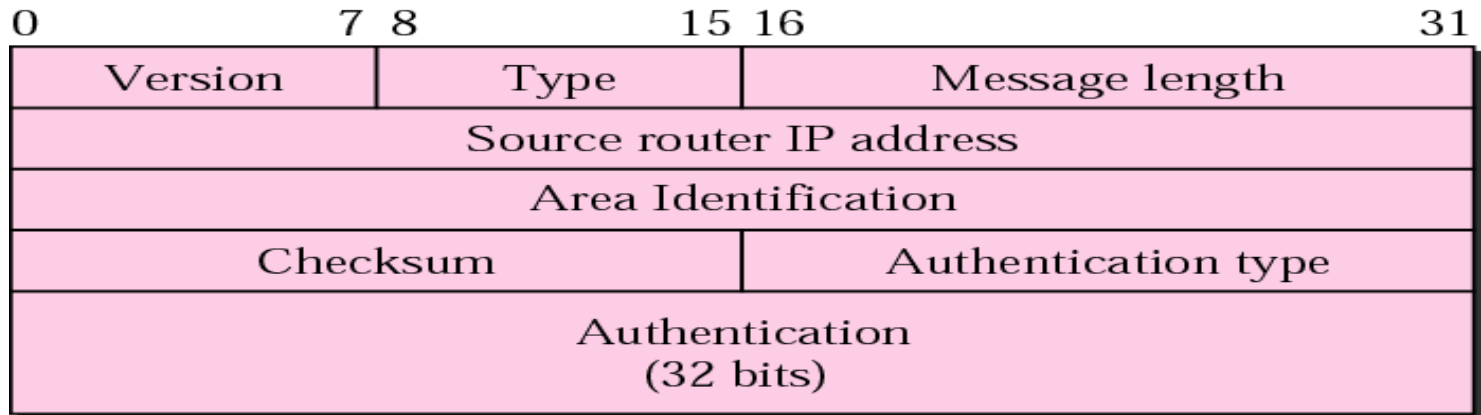


Let us now examine how an AS can be represented graphically. Figure above shows a small AS with seven networks and six routers. Two of the networks are point-to-point networks. We use symbols such as N1 and N2 for transient and stub networks. There is no need to assign an identity to a point-to-point network. The figure also shows the graphical representation of the AS as seen by OSPF. We have used colour nodes for the routers and shaded nodes for the networks (represented by designated routers). However, OSPF sees both as nodes. Note that we have three stub networks.

# Types of OSPF packets



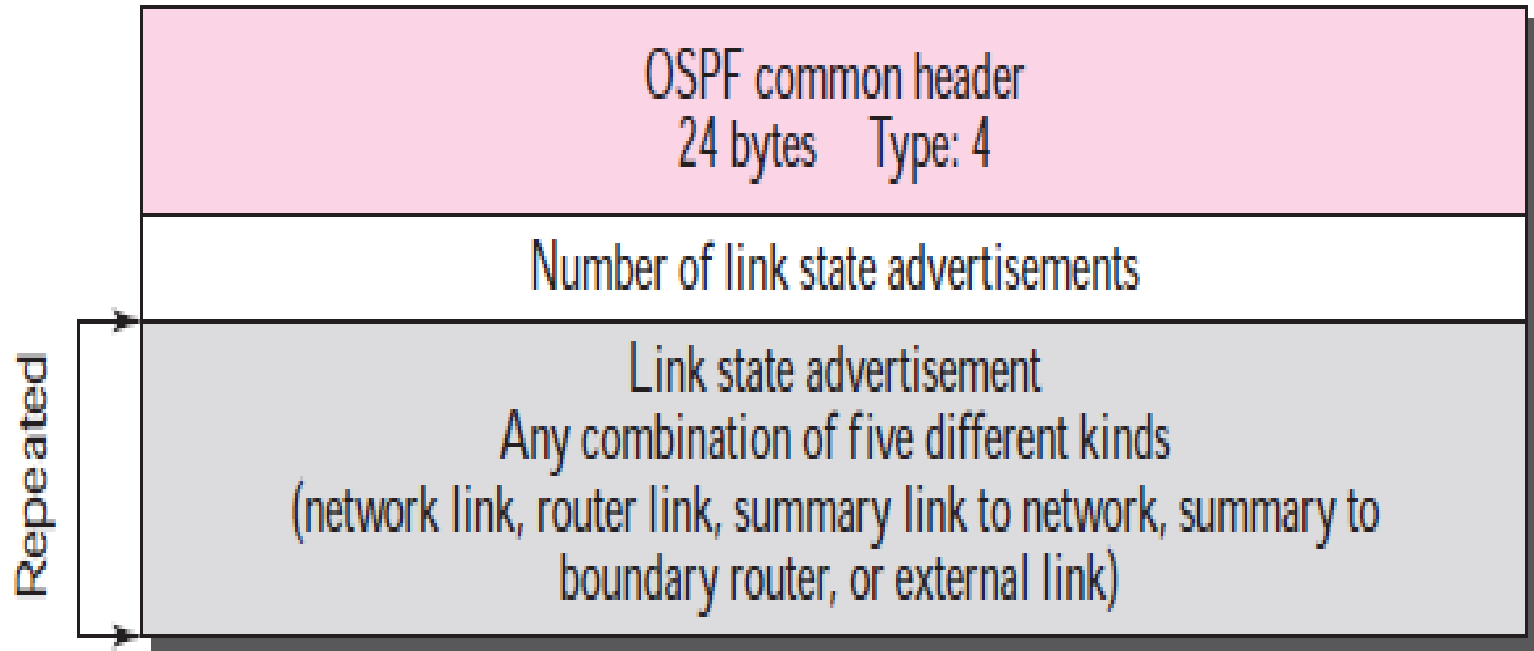
## *SPF common header (\*\*)*



- ❑ **Version.** This 8-bit field defines the version of the OSPF protocol. It is currently version 2.
- ❑ **Type.** This 8-bit field defines the type of the packet. We have five types, with values 1 to 5 defining the types.
- ❑ **The Message length.** This 16-bit field defines the length of the total message including the header.
- ❑ **Source router IP address.** This 32-bit field defines the IP address of the router that sends the packet.
- ❑ **Area identification.** This 32-bit field defines the area within which the routing takes place.
- ❑ **Checksum.** This field is used for error detection on the entire packet excluding the authentication type and authentication data field.
- ❑ **Authentication type.** This 16-bit field defines the authentication protocol used in this area
- ❑ **Authentication.** This 64-bit field is the actual value of the authentication data.



# Link state update packet (\*\*)



## *LSA general header (\*\*)*

Link state age	Reserved	E	T	Link state type
Link state ID				
Advertising router				
Link state sequence number				
Link state checksum	Length			

- Link state age.** This field indicates the number of seconds elapsed since this message was first generated.
- E flag.** If this 1-bit flag is set to 1, it means that the area is a stub area. A stub area is an area that is connected to the backbone area by only one path.
- T flag.** If this 1-bit flag is set to 1, it means that the router can handle multiple types of service.
- Link state type.** This field defines the LSA type
- Link state ID.** The value of this field depends on the type of link.
- Advertising router.** This is the IP address of the router advertising this message.
- Link state sequence number.** This is a sequence number assigned to each link state update message.
- Link state checksum**
- Length.** This defines the length of the whole packet in bytes.



# *Unicast Routing Protocols: RIP, OSPF, and BGP2*

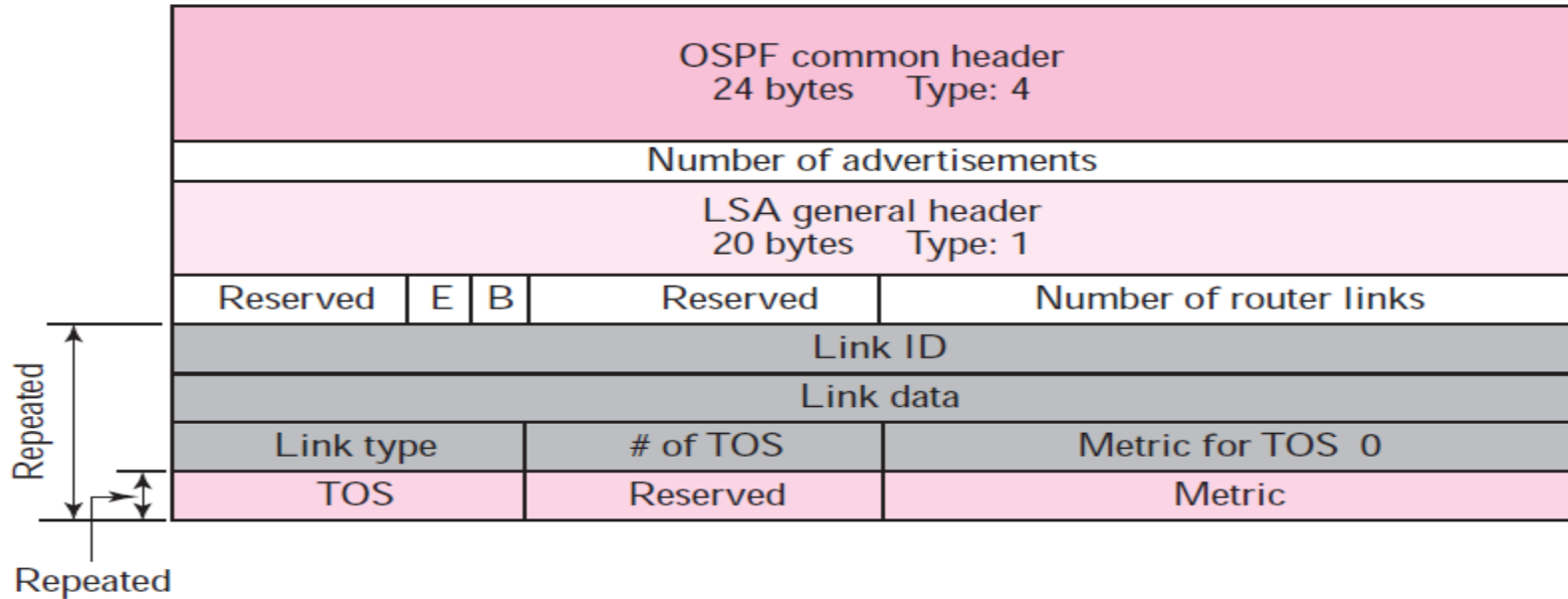
---

## **Objectives**

*Upon completion you will be able to:*

- *Distinguish between intra and interdomain routing*
- *Understand distance vector routing and RIP*
- *Understand link state routing and OSPF*
- *Understand path vector routing and BGP*

# The format of the router link packet (\*\*)



The fields of the router link LSA are as follows:

- ❑ **Link ID.** The value of this field depends on the type of link.
- ❑ **Link data.** This field gives additional information about the link.
- ❑ **Link type.** Four different types of links are defined based on the type of network to which the router is connected.
- ❑ **Number of types of service (TOS).** This field defines the number of types of services announced for each link.
- ❑ **Metric for TOS 0.** This field defines the metric for the default type of service (TOS 0).
- ❑ **TOS.** This field defines the type of service.
- ❑ **Metric.** This field defines the metric for the corresponding TOS.

## *Link types, link identification, and link data*

<i>Link Type</i>	<i>Link Identification</i>	<i>Link Data</i>
Type 1: Point-to-point	Address of neighbor router	Interface number
Type 2: Transient	Address of designated router	Router address
Type 3: Stub	Network address	Network mask
Type 4: Virtual	Address of neighbor router	Router address



## *EXAMPLE*

*Give the router link LSA sent by router 10.24.7.9 .*

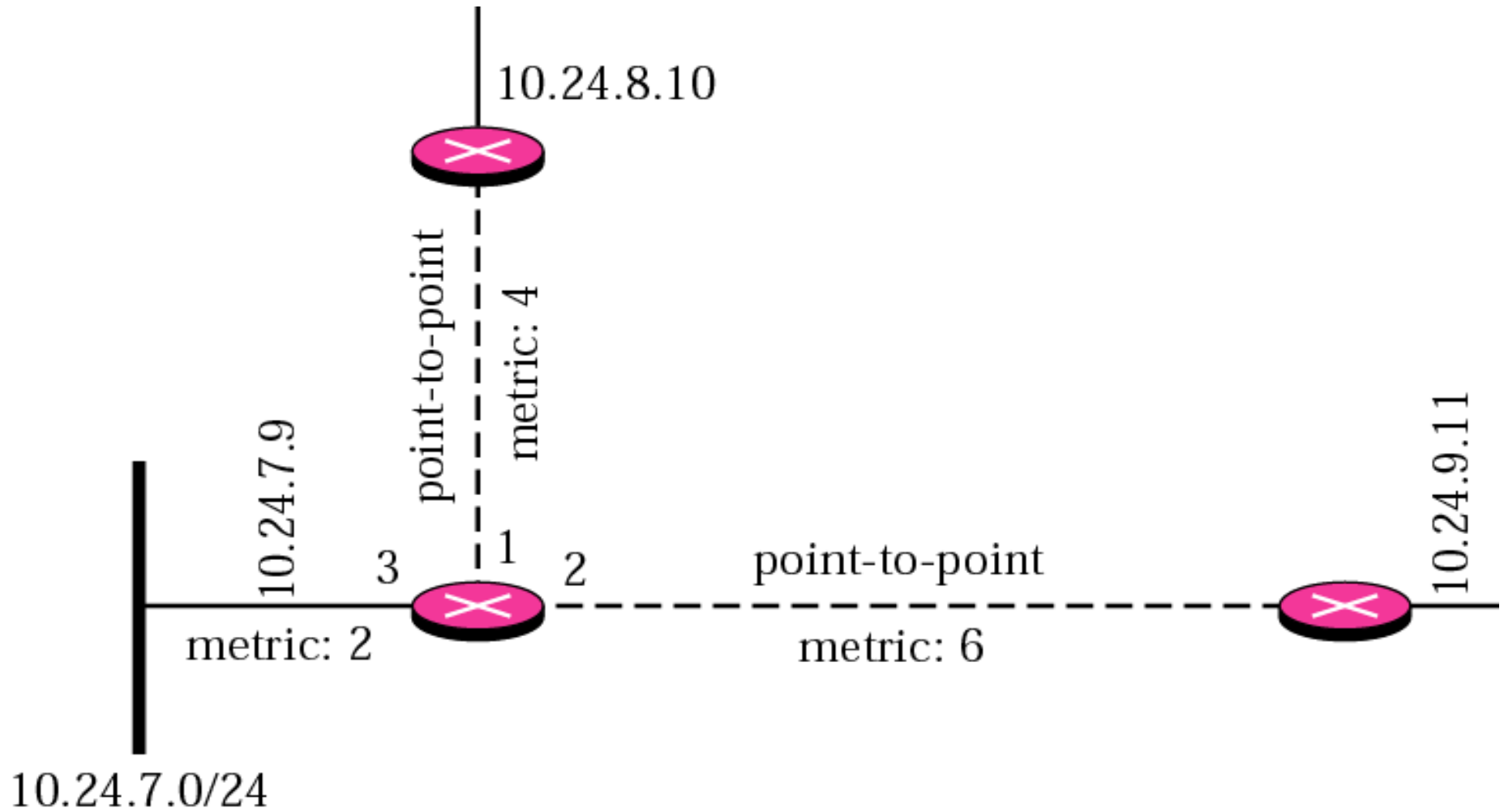
**See Next Slide**

## *Solution*

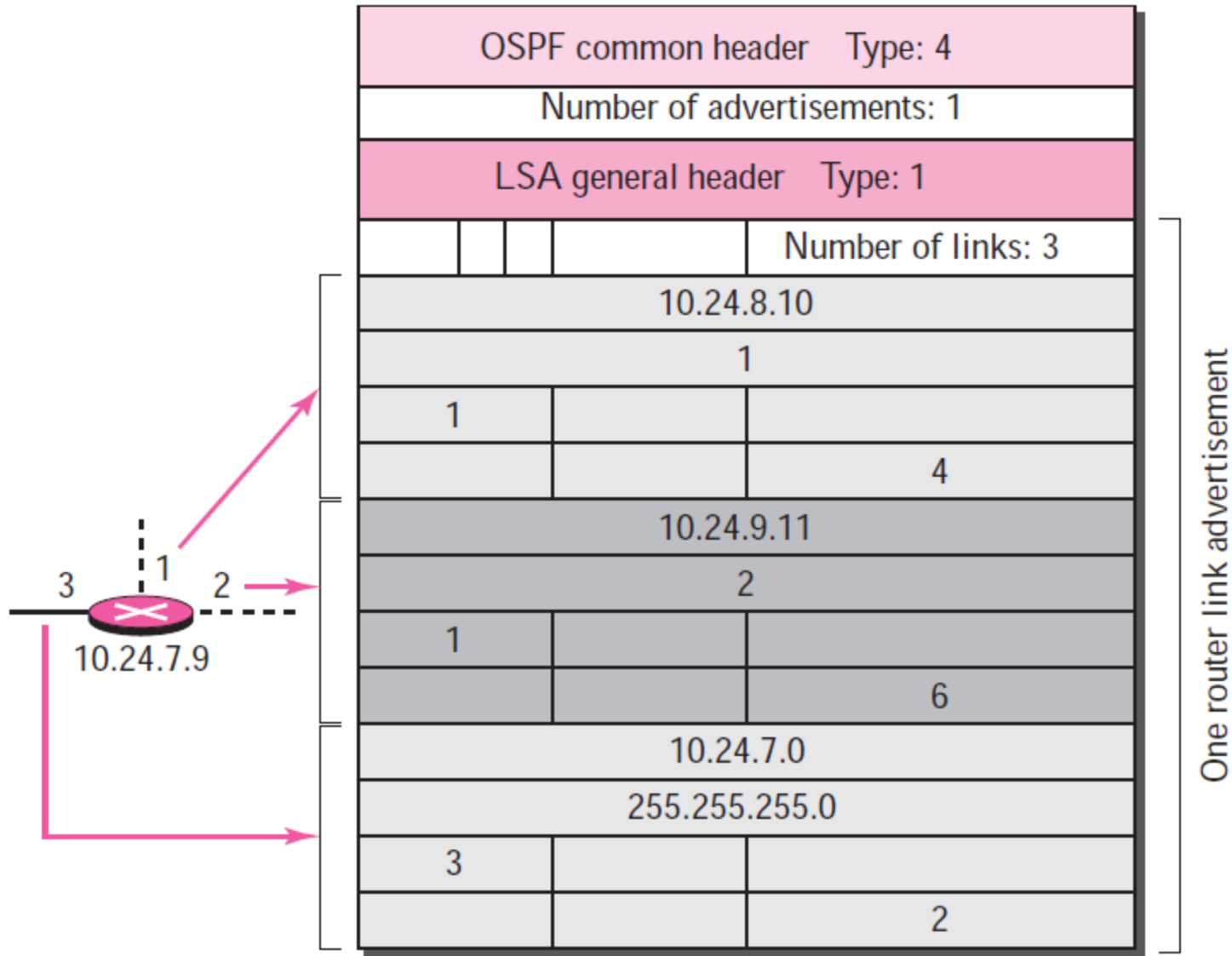
*This router has three links: two of type 1 (point-to-point) and one of type 3 (stub network).*

**See Next Slide**

# Example 3



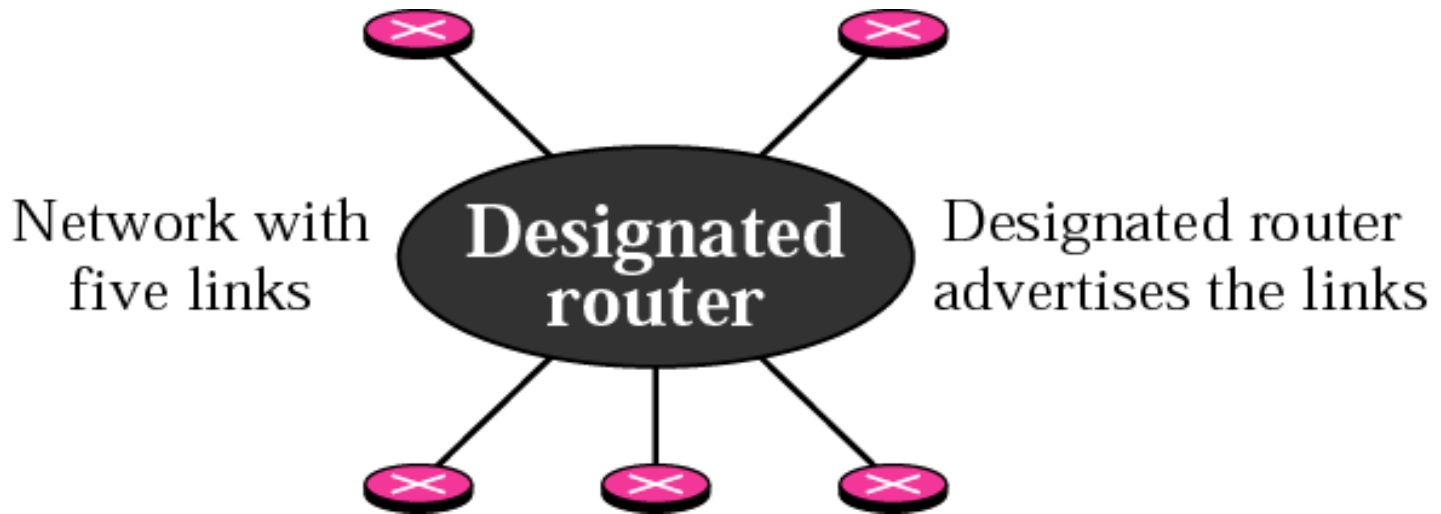
# Solution to Example 3





## *Network link*

**A network link defines the links of a network. A designated router, on behalf of the transient network, distributes this type of LSP packet. The packet announces the existence of all of the routers connected to the network**

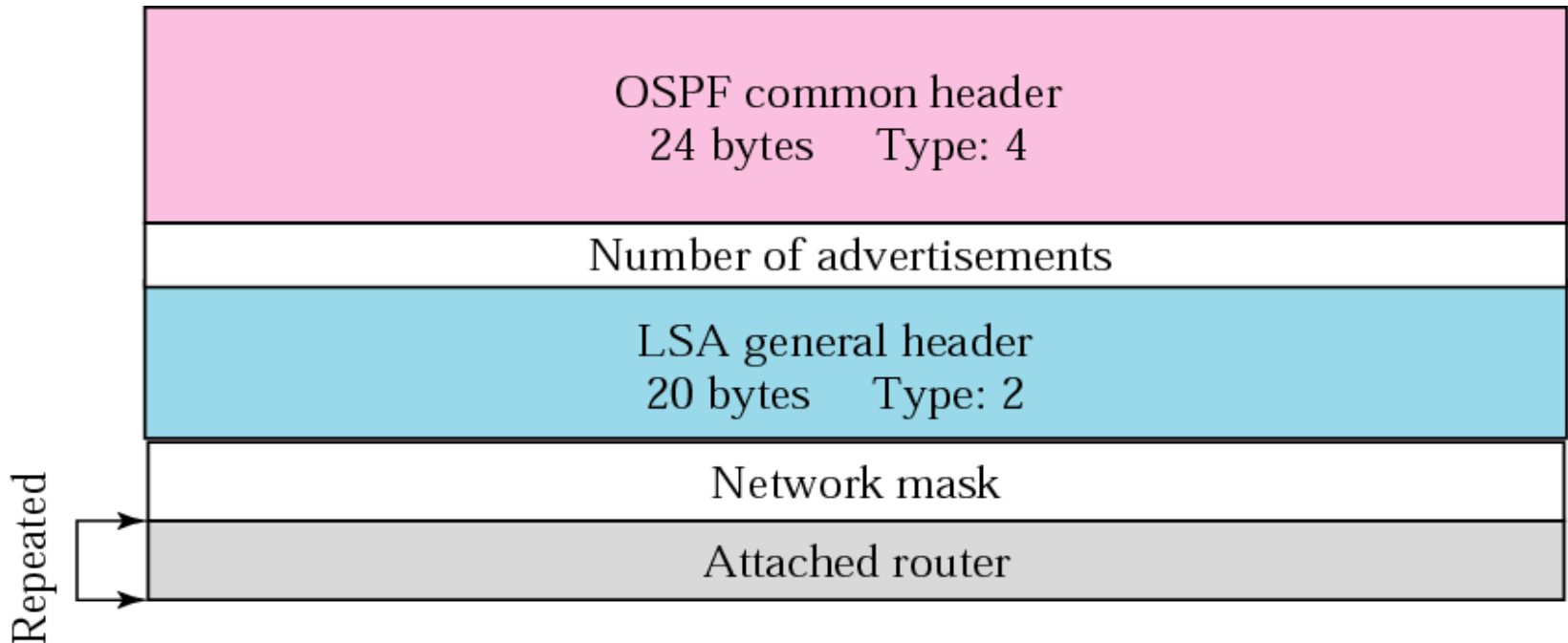


## *Network link advertisement format (\*\*)*

The format of the network link advertisement is shown in Figure below.

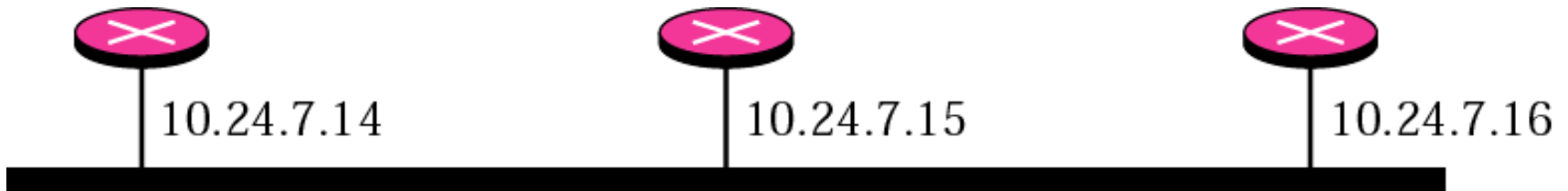
The fields of the network link LSA are as follows:

- ❑ **Network mask.** This field defines the network mask.
- ❑ **Attached router.** This repeated field defines the IP addresses of all attached routers.



## ***EXAMPLE***

*Give the network link LSA in Figure below*

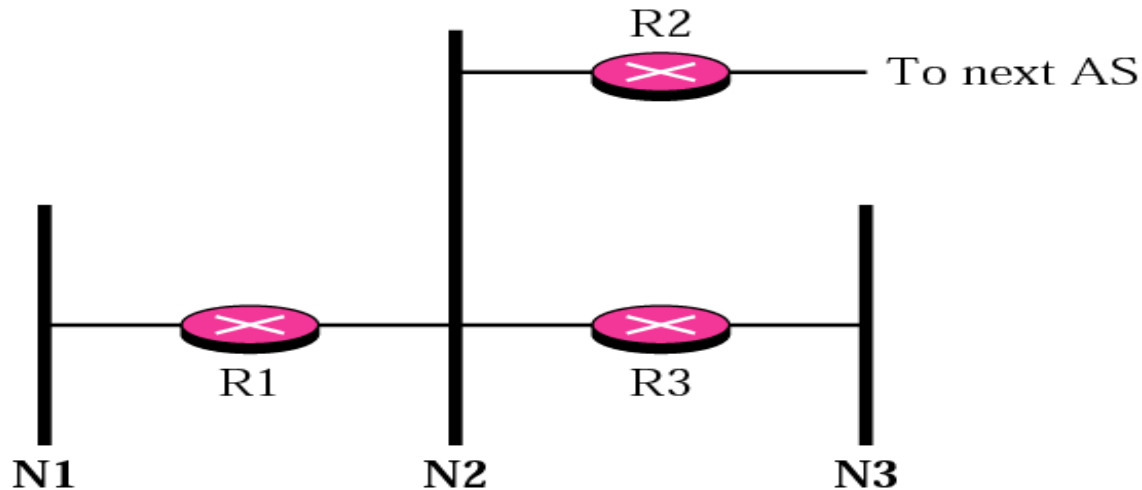


***Solution.***

OSPF common header	Type: 4
Number of advertisements: 1	
LSA general header	Type: 2
255.255.255.0	
10.24.7.14	
10.24.7.15	
10.24.7.16	

## ***EXAMPLE***

*In Figure below, which router(s) sends out router link LSAs?*



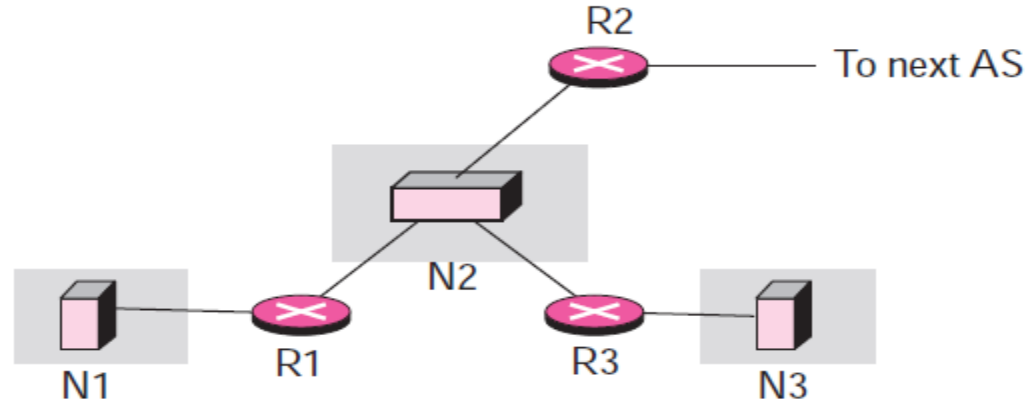
## ***Solution***

*All routers advertise router link LSAs.*

- a. R1 has two links, N1 and N2.*
- b. R2 has one link, N1.*
- c. R3 has two links, N2 and N3.*

## **EXAMPLE**

*In Figure below, which router(s) sends out the network link LSAs?*



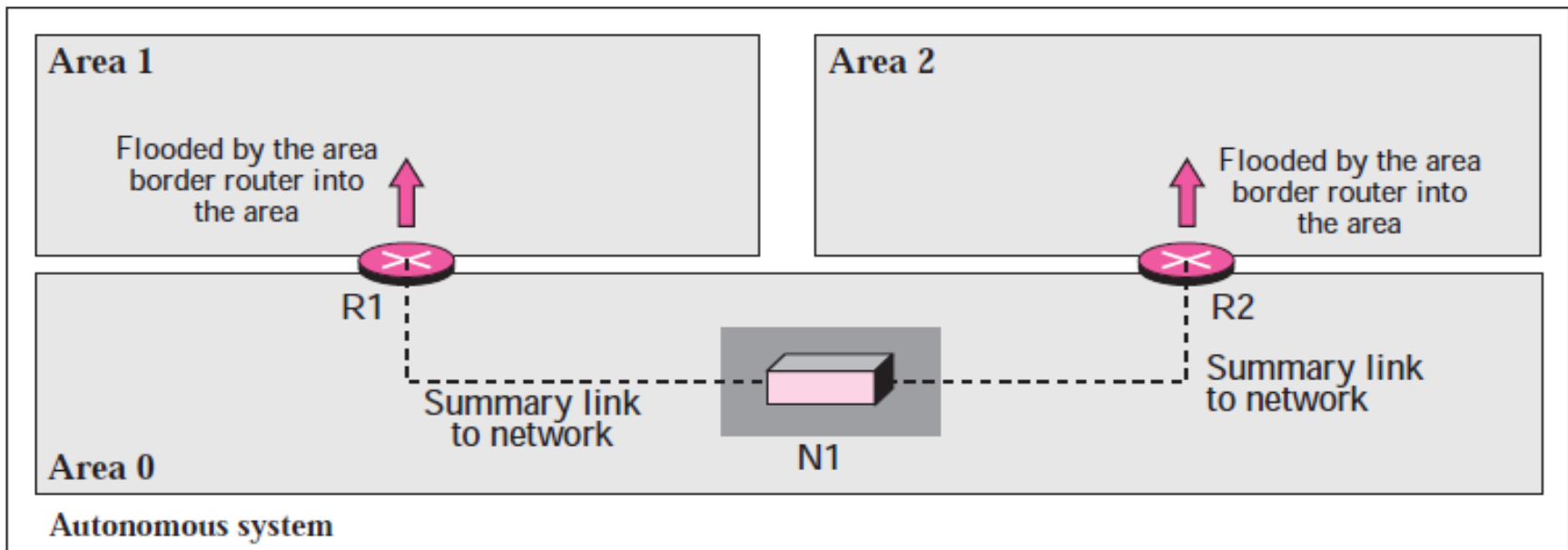
## **Solution**

*All three network must advertise network links:*

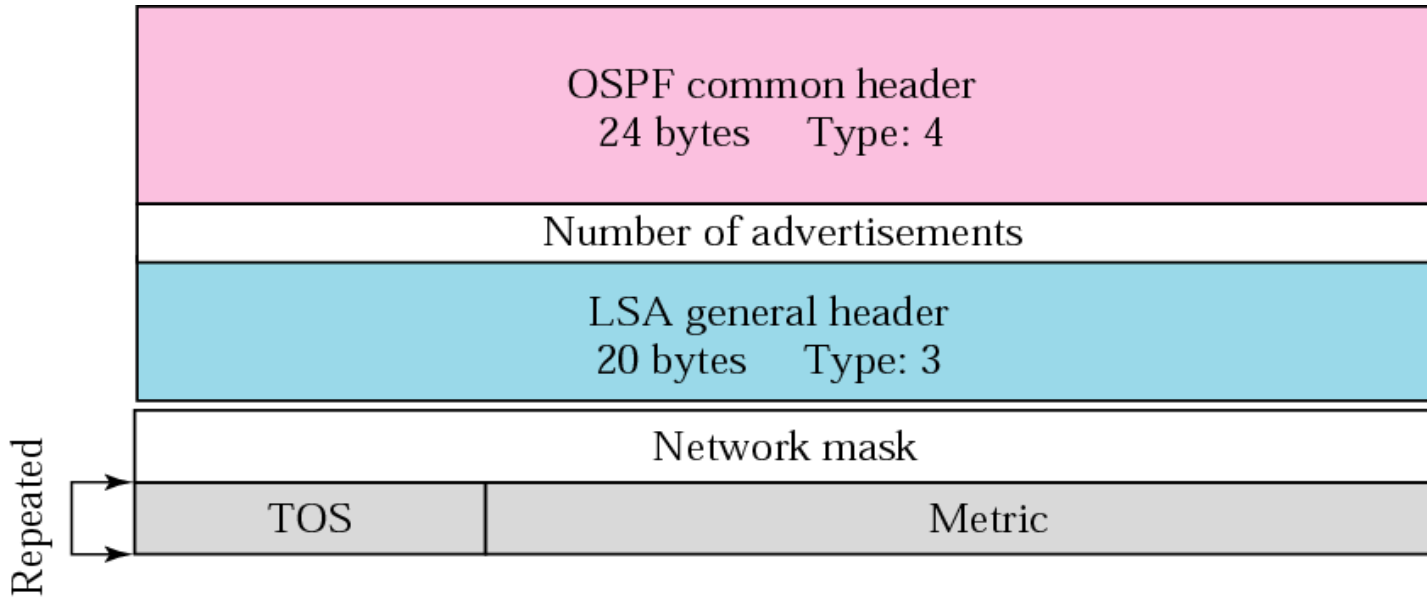
- a. Advertisement for N1 is done by R1 because it is the only attached router and therefore the designated router.*
- b. Advertisement for N2 can be done by either R1, R2, or R3, depending on which one is chosen as the designated router.*
- c. Advertisement for N3 is done by R3 because it is the only attached router and therefore the designated router.*

## Summary link to network

- ❑ **Router link** and **network link** advertisements flood the area with information about the router links and network links **inside an area**.
- ❑ But a router must also know about the networks outside its area; **the area border routers can provide this information**.
- ❑ An area border router is active in more than one area. It receives router link and network link advertisements, and **creates a routing table for each area**.
- ❑ Router R1 is an area border router. It has two routing tables, one for area 1 and one for area 0. R1 floods area 1 with information about how to reach a network located in area 0 and vice versa.

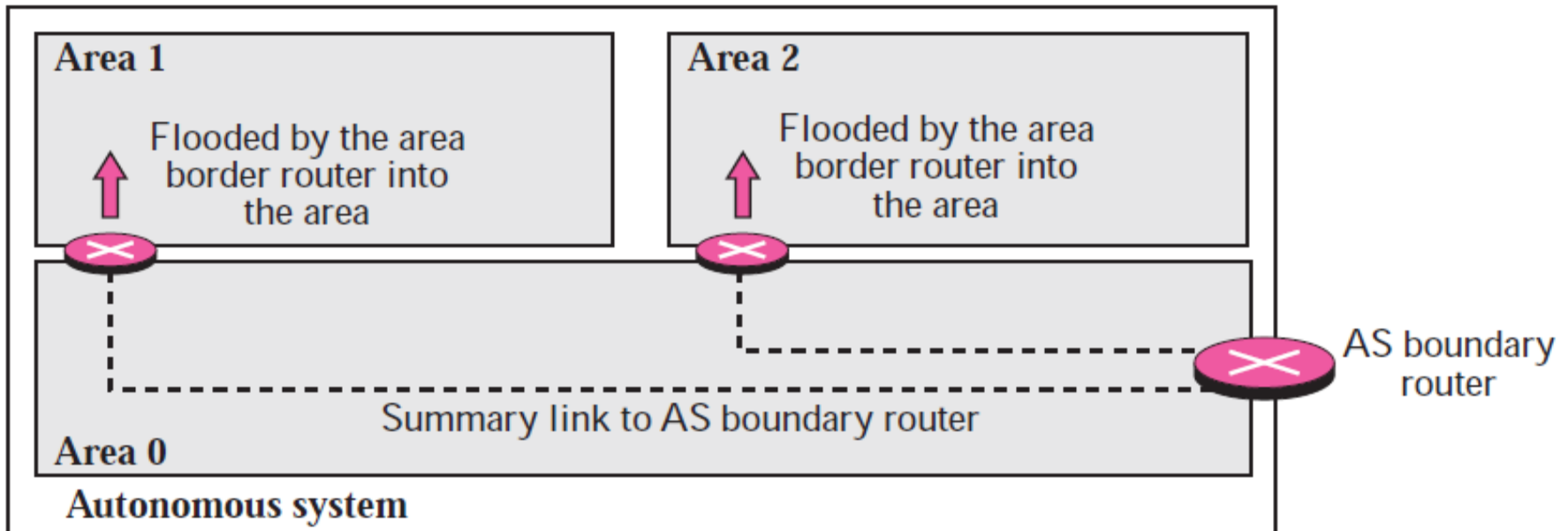


# Summary link to network LSA (\*\*)



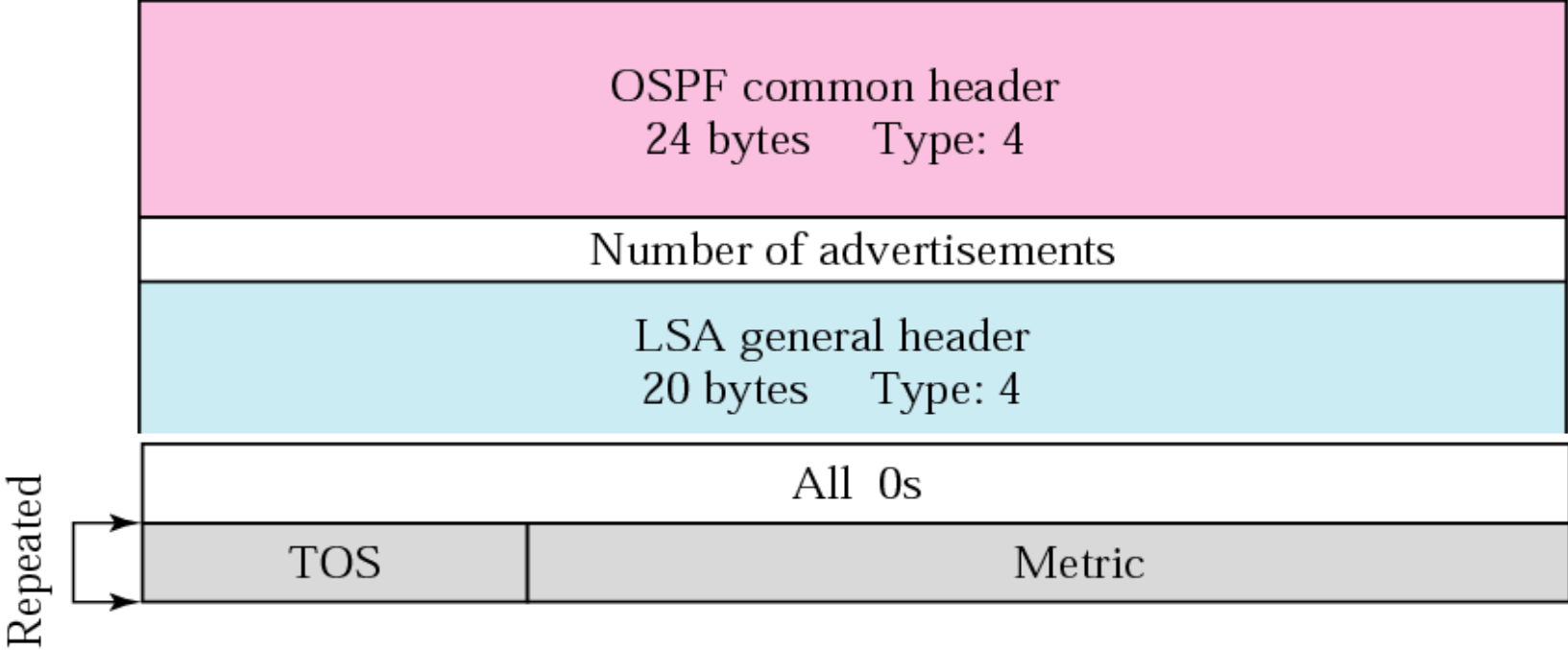
## Summary link to AS boundary router

- ❑ what about a network outside the autonomous system?
- ❑ If a router inside an area wants to send a packet outside the autonomous system, it should first know the route to an autonomous boundary router; the summary link to AS boundary router provides this information.
- ❑ The area border routers flood their areas with this information.



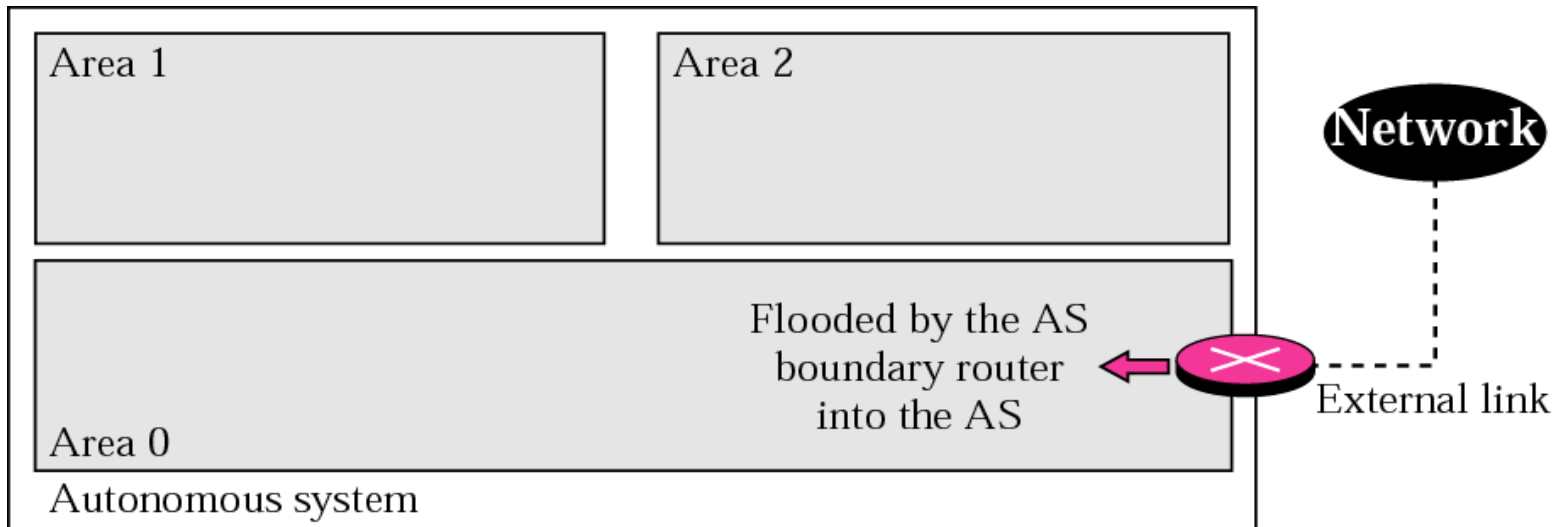


# Summary link to AS boundary router LSA (\*\*)

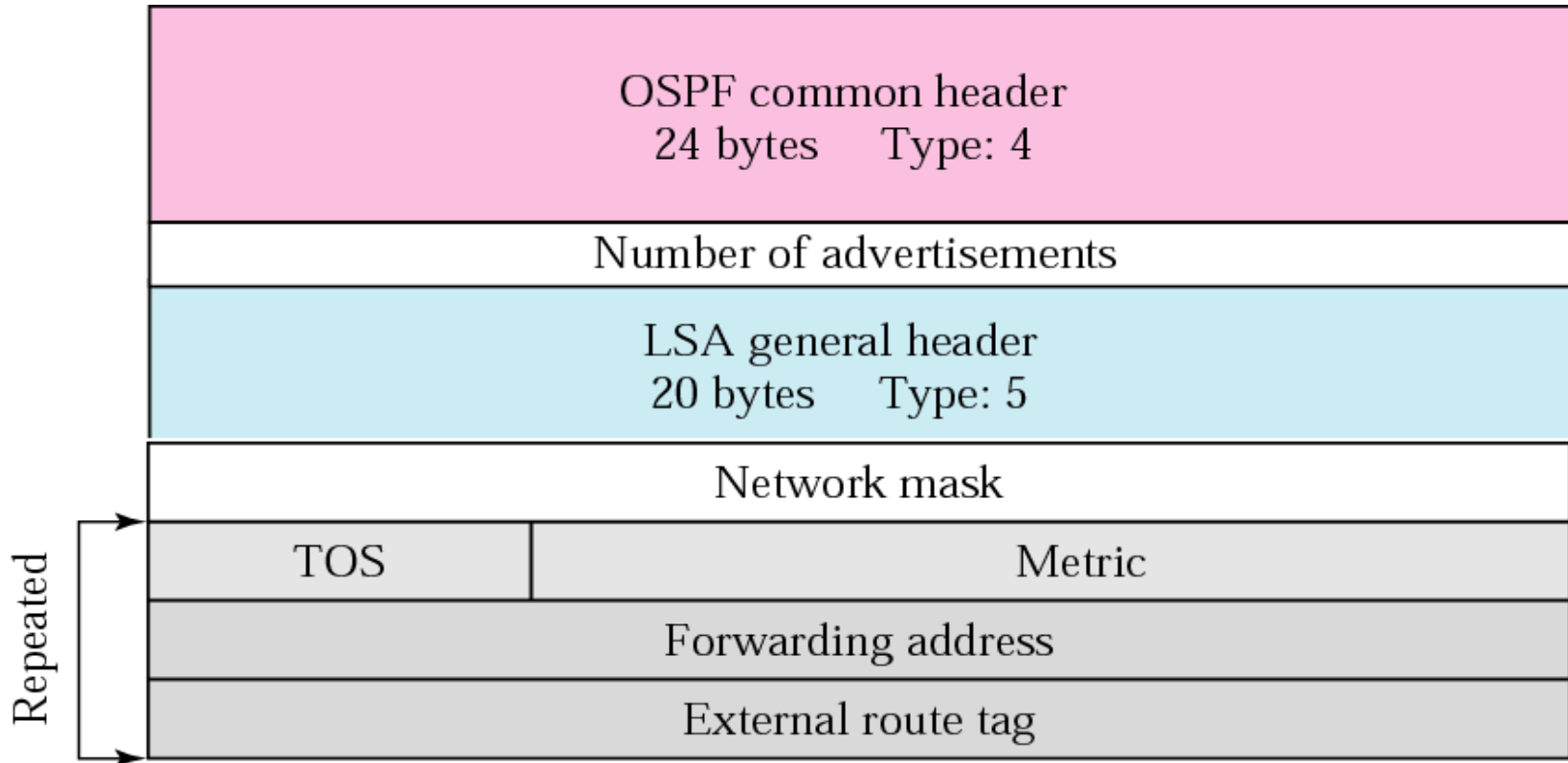


## *External link*

- ❑ Although the previous advertisement lets each router know the route to an **AS boundary router**, this information is not enough. A router inside an autonomous system wants to know which networks are available outside the autonomous system;
- ❑ the **external link advertisement** provides this information.
- ❑ The AS boundary router floods the autonomous system with the cost of each network outside the autonomous system using a routing table created by an interdomain routing protocol.

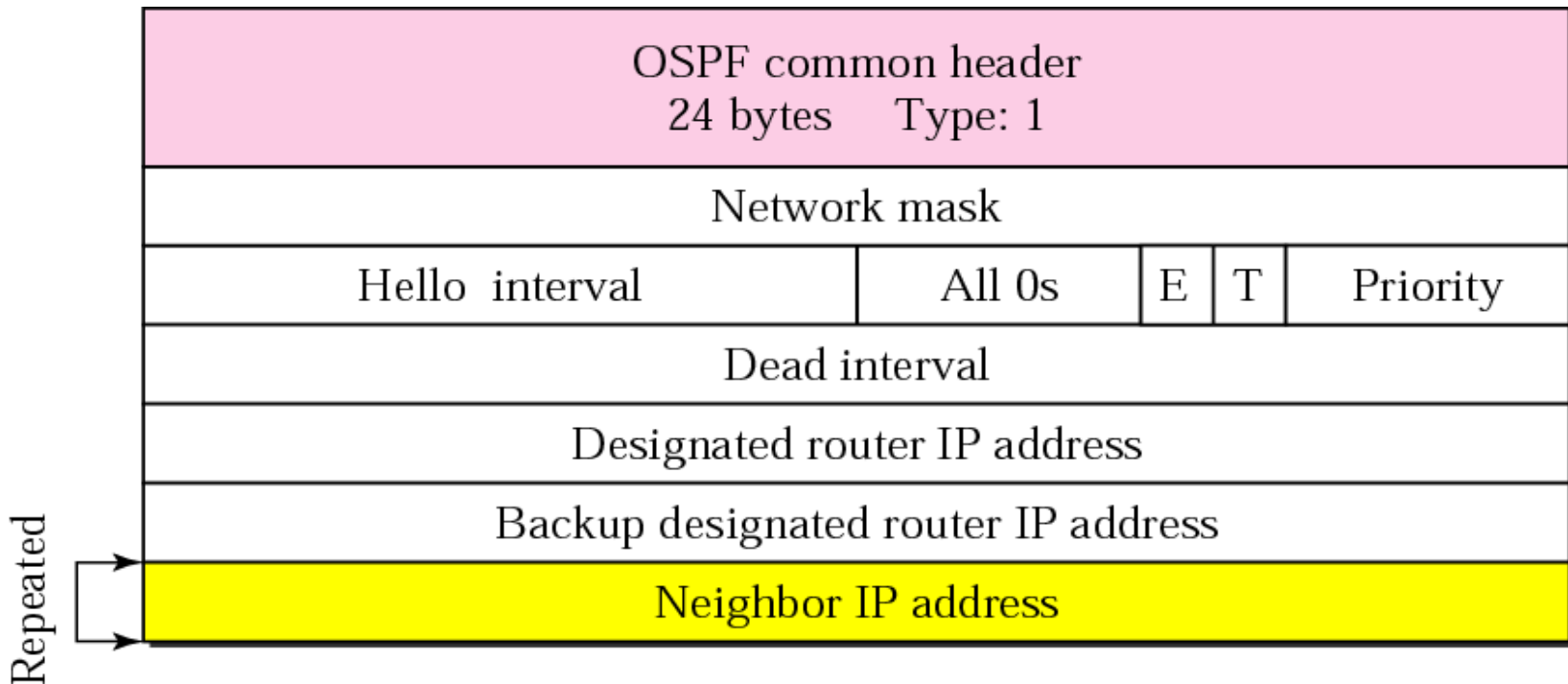


# External link LSA(\*\*)



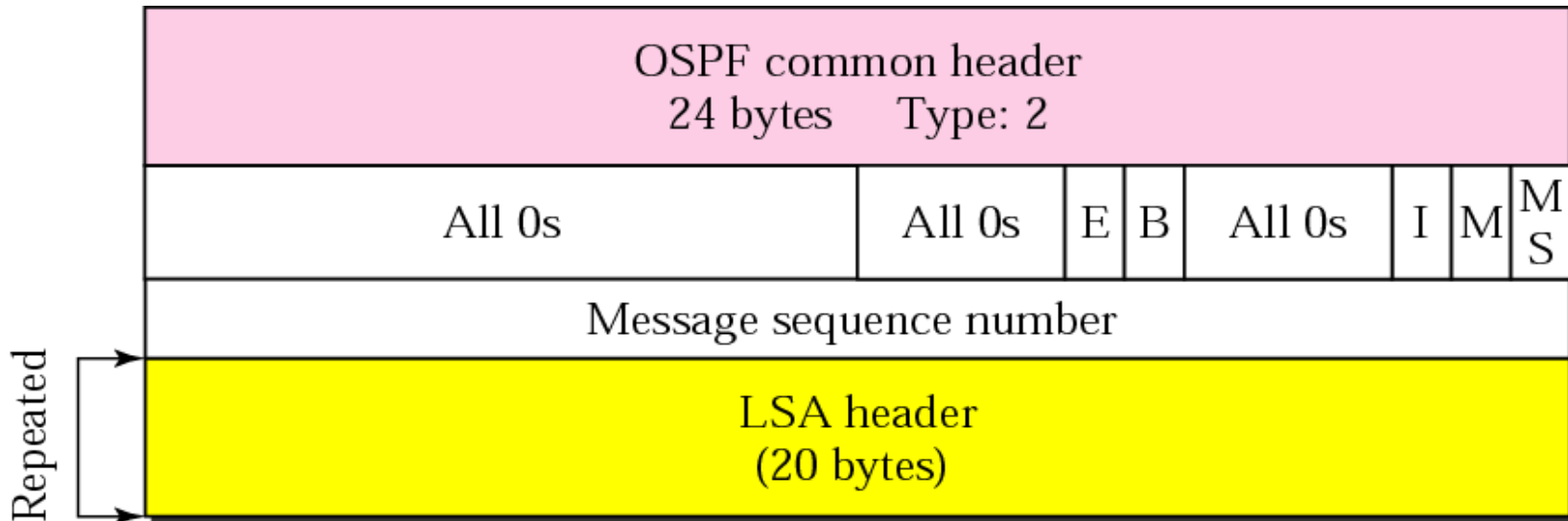
# *Hello packet*

**OSPF uses the hello message to create neighbourhood relationships and to test the reachability of neighbours. This is the first step in link state routing. Before a router can flood all of the other routers with information about its neighbours**



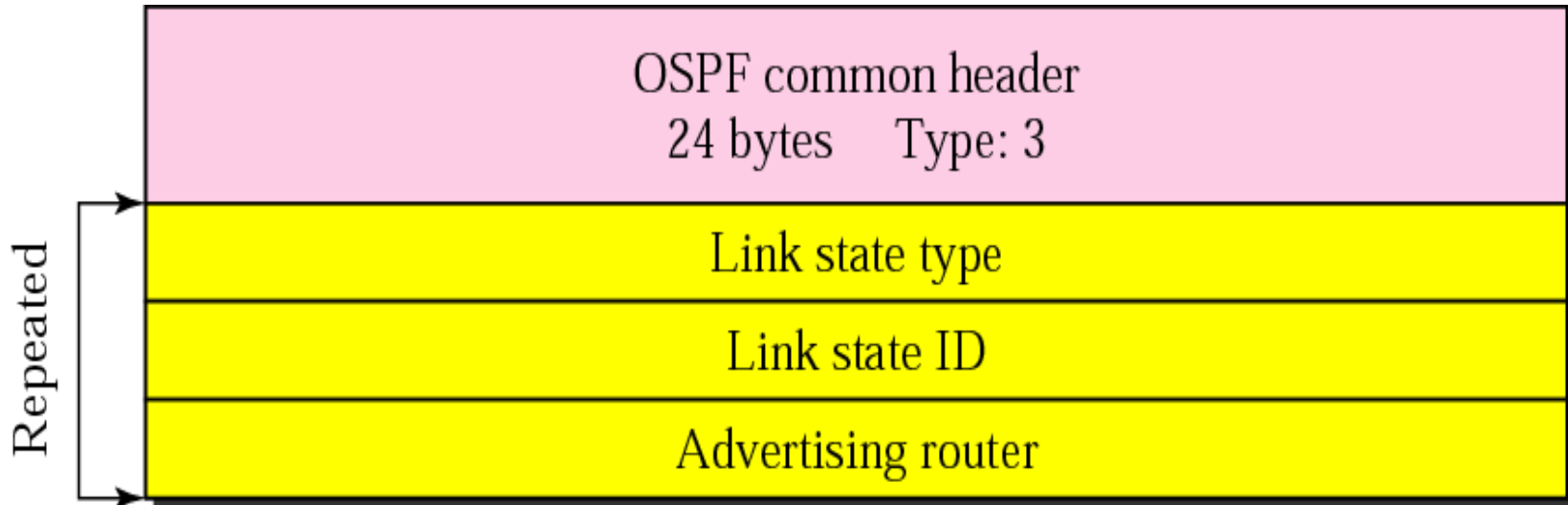
## Database description packet

When a router is connected to the system for the **first time** or after a **failure**, it needs the complete link state database immediately. It cannot wait for all link state update packets to come from every other router before making its own database and calculating its routing table.



## *Link state request packet*

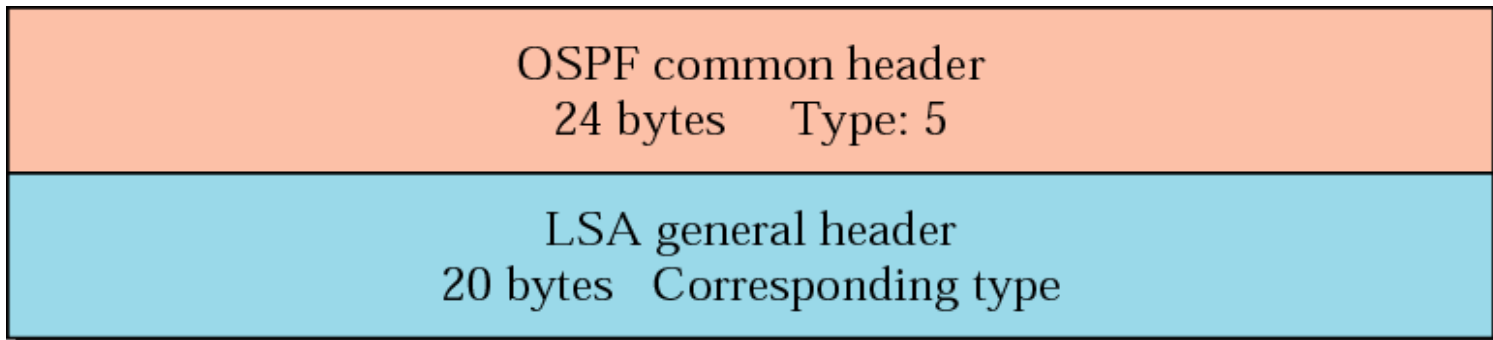
**This is a packet that is sent by a router that needs information about a specific route or routes. It is answered with a link state update packet. It can be used by a newly connected router to request more information about some routes after receiving the database description packet.**





## *Link state acknowledgment packet*

**OSPF makes routing more reliable by forcing every router to acknowledge the receipt of every link state update packet.**





*OSPF packets are encapsulated in IP datagrams.*





# *Unicast Routing Protocols: RIP, OSPF, and BGP*

---

## **Objectives**

*Upon completion you will be able to:*

- *Distinguish between intra and interdomain routing*
- *Understand distance vector routing and RIP*
- *Understand link state routing and OSPF*
- *Understand path vector routing and BGP*

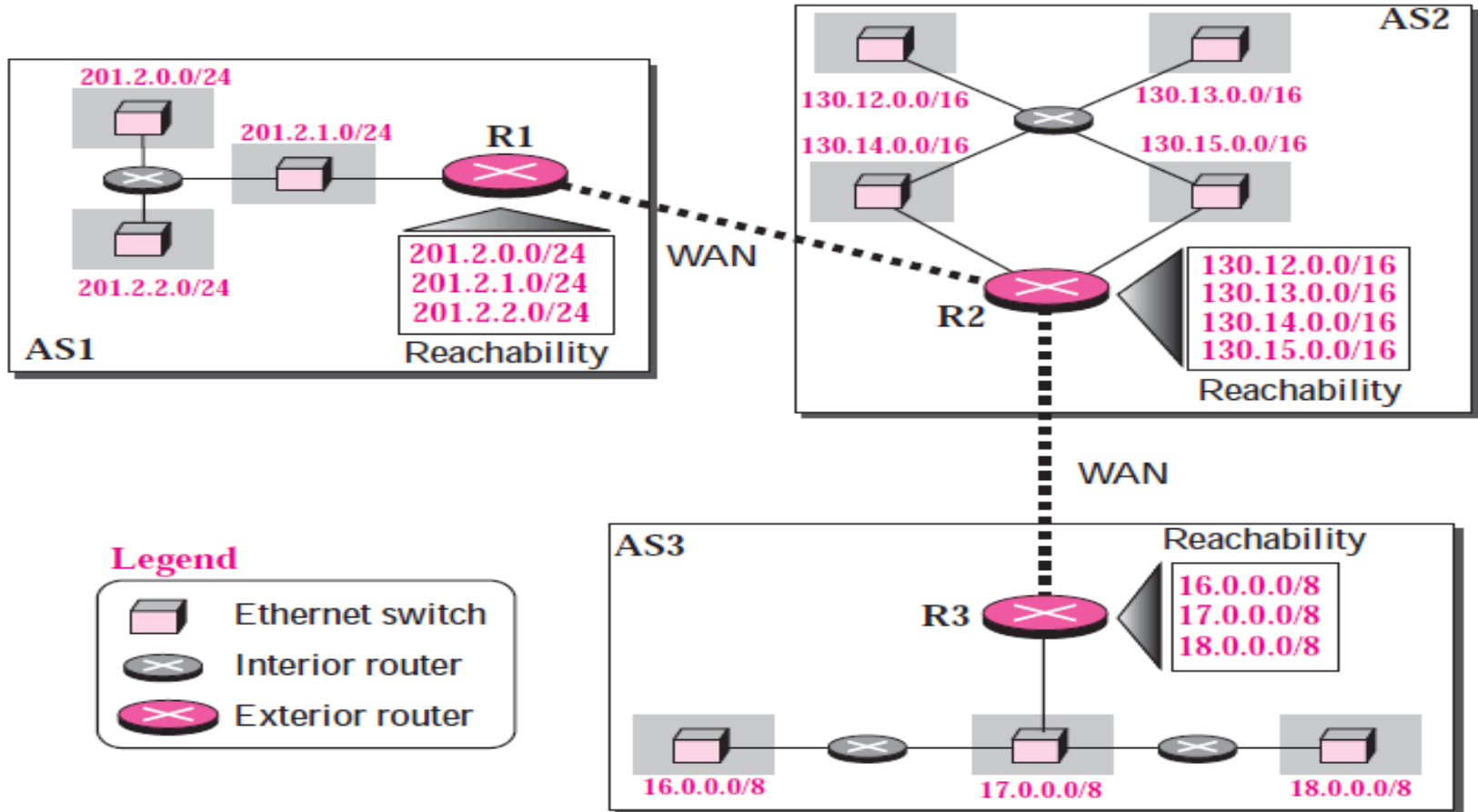
# Review

- Distance vector and link state routing are both *interior routing protocols*.
- Both of these routing protocols become intractable when the domain of operation becomes large.
- Distance vector routing is subject to instability if there is more than a few hops in the domain of operation.
- Link state routing needs a huge amount of resources to calculate routing tables.

# PATH VECTOR ROUTING

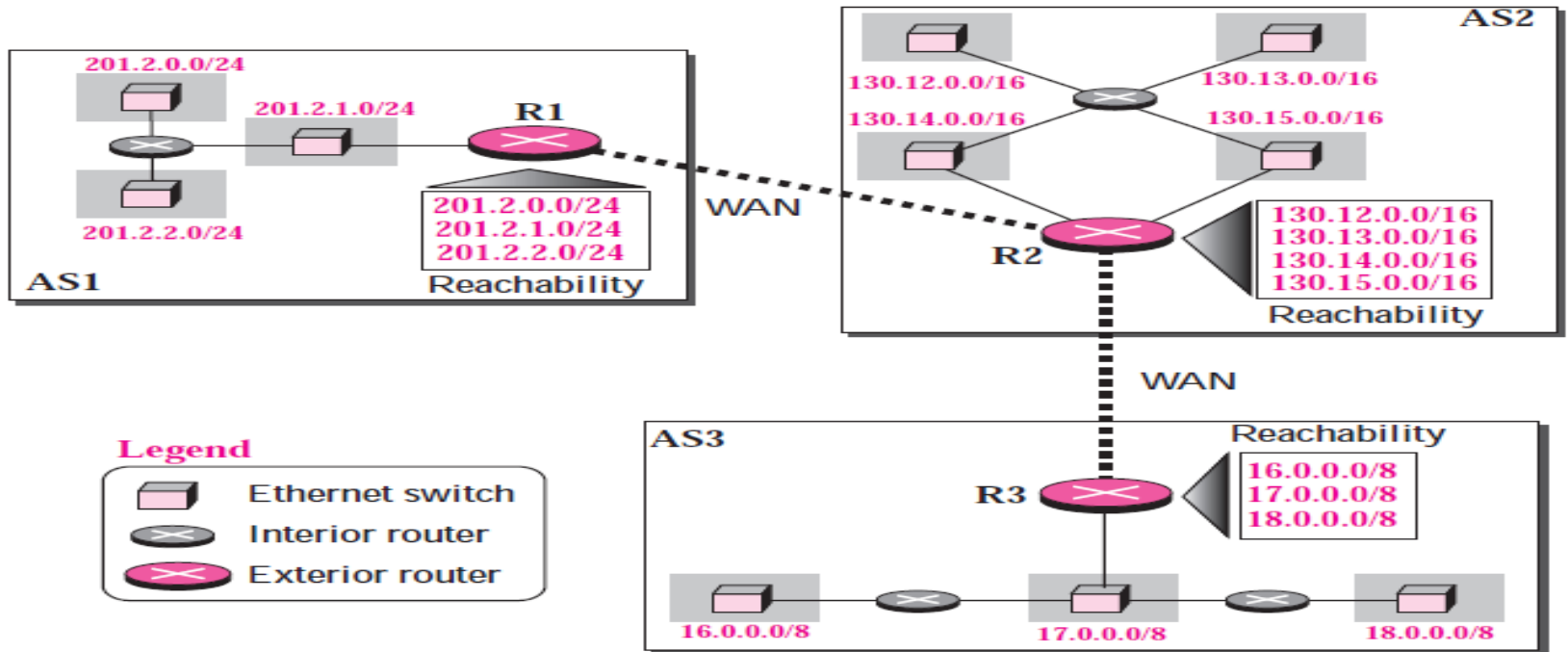
- **Path vector routing is exterior routing protocol proved to be useful for interdomain or inter-AS routing.**
- **in distance vector router has a list of networks that can be reached in the same AS.**
- **in path vector routing, a router has a list of networks that can be reached with the path (list of ASs to pass).**
- **the domain of operation of the distance vector routing is a single AS; the domain of operation of the path vector routing is the whole Internet.**
- **The distance vector routing tells us the distance to each network; the path vector routing tells us the path.**

# Reachability



To be able to provide information to other ASs, each AS must have at least one path vector routing that collects **reachability information** about each network in that AS. The information collected in this case only means which network, identified by its network address (CIDR prefix), exists (can be reached in this AS).

# Reachability



**R1**

Network	Path
201.2.0.0/24	AS1 (This AS)
201.2.1.0/24	AS1 (This AS)
201.2.2.0/24	AS1 (This AS)
130.12.0.0/16	AS1, AS2
130.13.0.0/16	AS1, AS2
130.14.0.0/16	AS1, AS2
130.15.0.0/16	AS1, AS2
16.0.0.0/8	AS1, AS2, AS3
17.0.0.0/8	AS1, AS2, AS3
18.0.0.0/8	AS1, AS2, AS3

Path-Vector Routing Table

**R2**

Network	Path
201.2.0.0/24	AS2, AS1
201.2.1.0/24	AS2, AS1
201.2.2.0/24	AS2, AS1
130.12.0.0/16	AS2 (This AS)
130.13.0.0/16	AS2 (This AS)
130.14.0.0/16	AS2 (This AS)
130.15.0.0/16	AS2 (This AS)
16.0.0.0/8	AS2, AS3
17.0.0.0/8	AS2, AS3
18.0.0.0/8	AS2, AS3

Path-Vector Routing Table

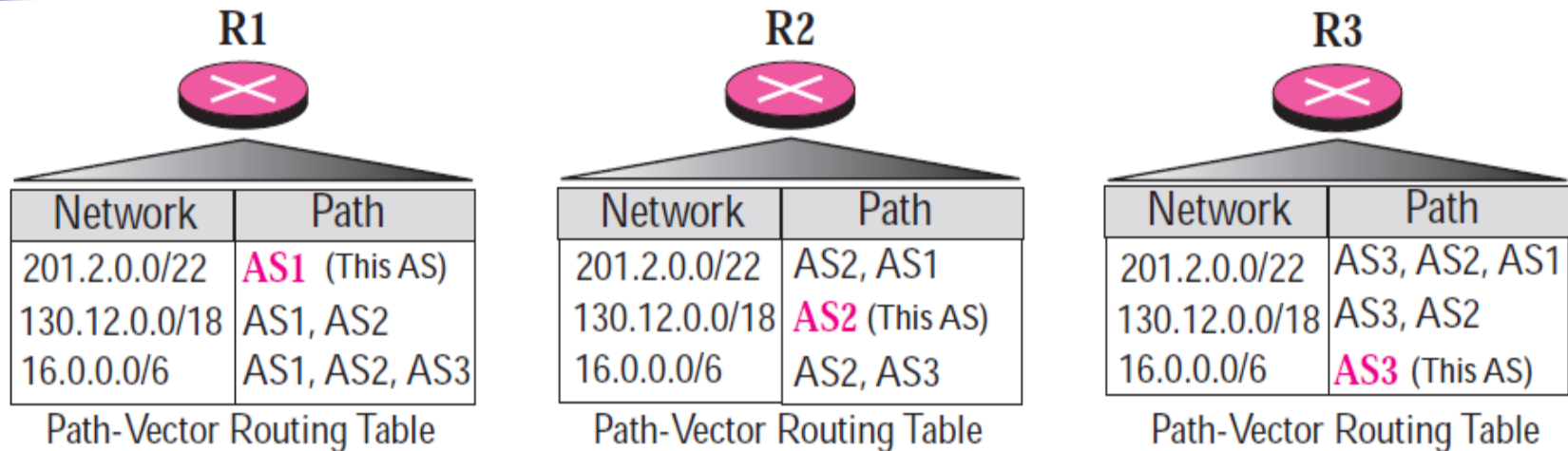
**R3**

Network	Path
201.2.0.0/24	AS3, AS2, AS1
201.2.1.0/24	AS3, AS2, AS1
201.2.2.0/24	AS3, AS2, AS1
130.12.0.0/16	AS3, AS2
130.13.0.0/16	AS3, AS2
130.14.0.0/16	AS3, AS2
130.15.0.0/16	AS3, AS2
16.0.0.0/8	AS3 (This AS)
17.0.0.0/8	AS3 (This AS)
18.0.0.0/8	AS3 (This AS)

Path-Vector Routing Table

The instability of distance vector routing and the creation of loops can be **avoided in path vector routing**. When a router receives a reachability information, it checks to see if its autonomous system is in the path list to any destination. If it is, looping is involved and that **network-path pair is discarded**.

# Aggregation



The path vector routing protocols normally support **CIDR notation** and the aggregation of addresses (if possible). This helps to make the path vector routing table **simpler** and **exchange** between **routers faster**. Note that a range may also include a block that may not be in the corresponding AS. For example, the range **201.2.0.0/22** also includes the range **201.2.0.3/24**, which is not the network address of any network in AS1. However, if this network exists in some other ASs, it eventually becomes part of the routing table.

# Border Gateway Protocol (BGP)

*Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.*

*The topics discussed in this section include:*

*Types of Autonomous Systems*

*Path Attributes*

*BGP Sessions*

*External and Internal BGP*

*Types of Packets*

*Packet Format*

*Encapsulation*





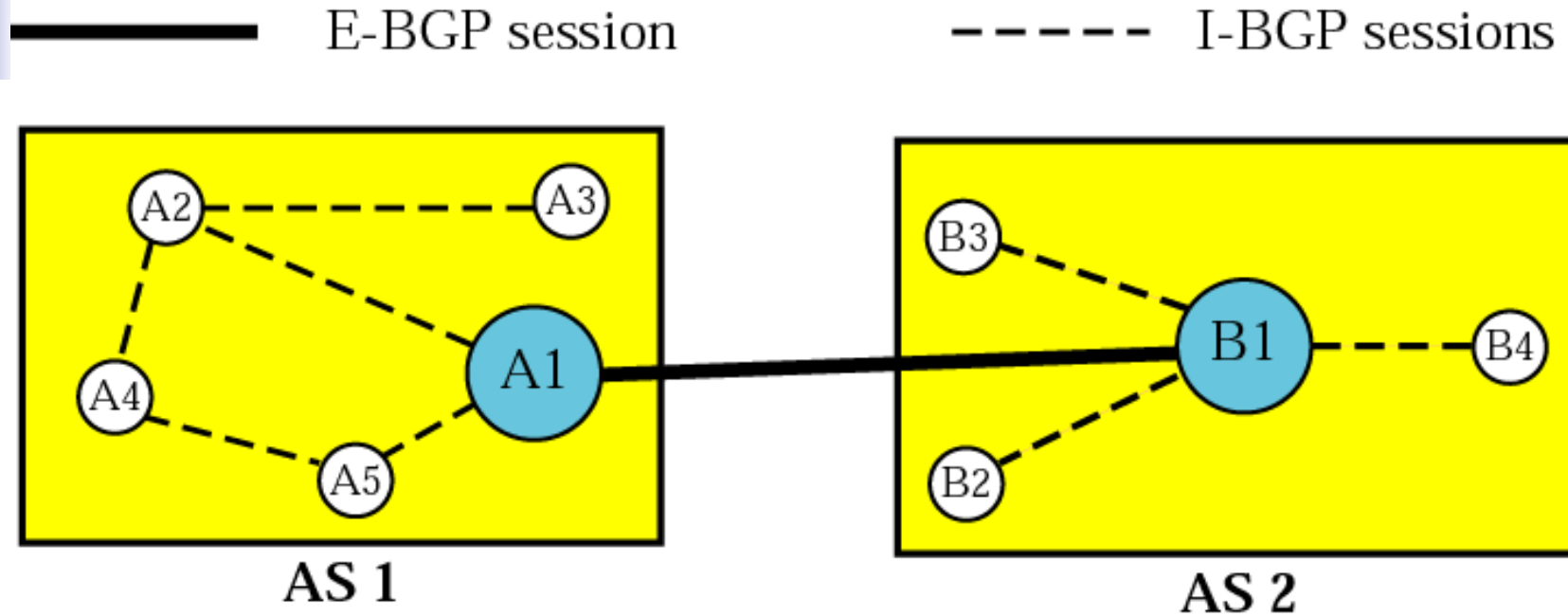
## *Types of Autonomous Systems*

---

**We can divide autonomous systems into three categories: stub, multihomed, and transit:**

- ***Stub AS*** : A stub AS has only one connection to another AS. The hosts in the AS can send and received data traffic to other ASs. Data traffic, however, cannot pass through a stub AS. A stub AS is either a source or a sink. A good example of a stub AS is a small corporation or a small local ISP.
- ***Multihomed AS*** : A multihomed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive and send data traffic from more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multihomed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.
- ***Transit AS***: A transit AS is a multihomed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).

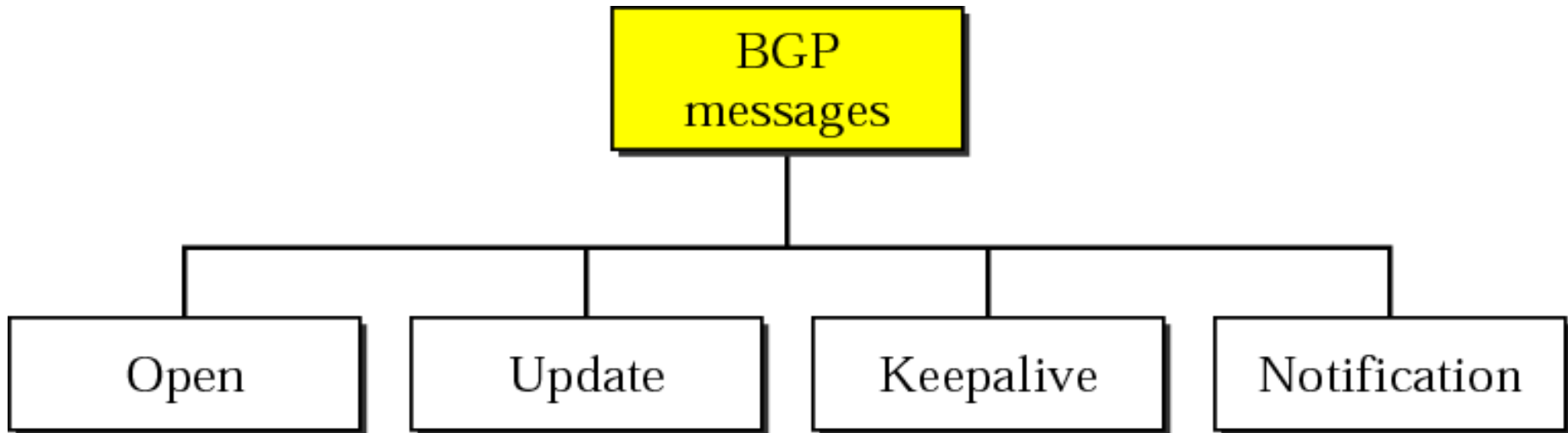
# Internal and external BGP sessions



The exchange of routing information between two routers using BGP takes place in a **session**. BGP can have two types of sessions: external BGP (E-BGP) and internal BGP (I-BGP) sessions. The E-BGP session is used to exchange information between two speaker nodes belonging to two different autonomous systems. The I-BGP session, on the other hand, is used to exchange routing information between two routers inside an autonomous system

# *Types of BGP messages*

**BGP uses four different types of messages: open, update, keepalive, and notification**

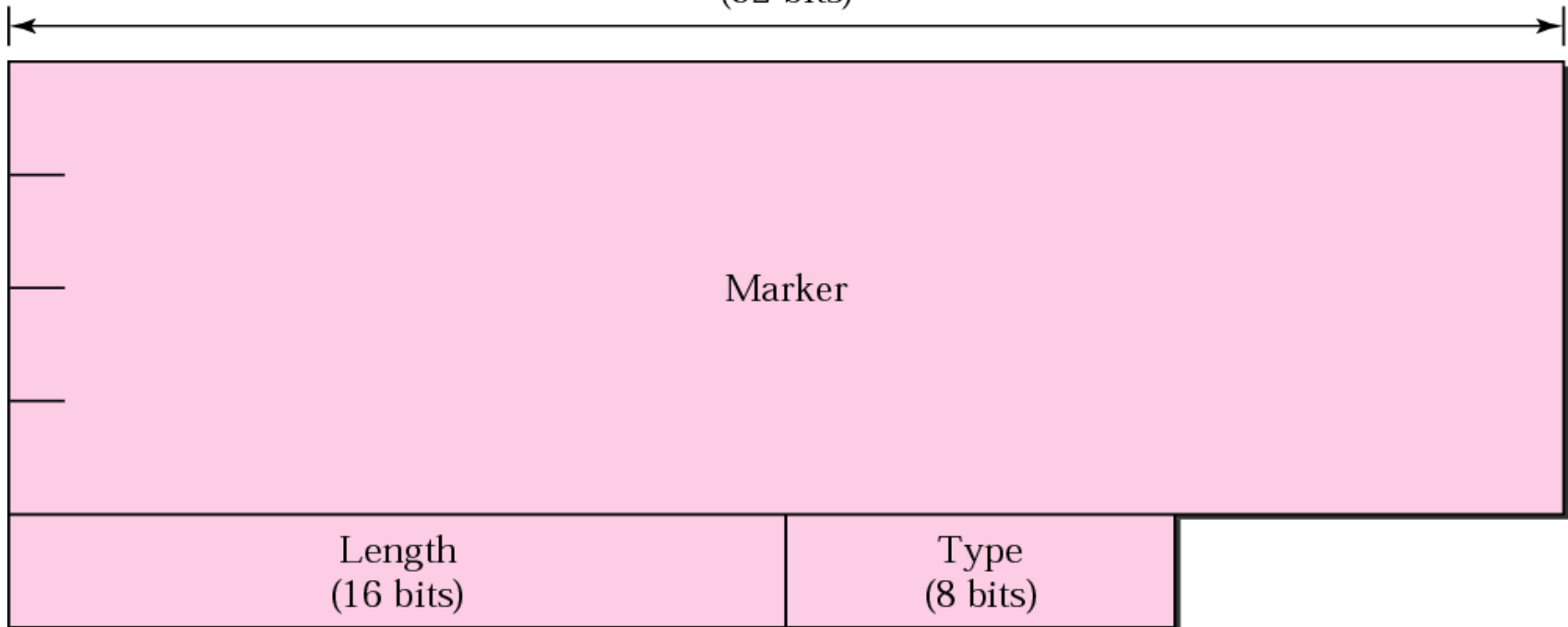


# *BGP packet header(\*\*)*

All BGP packets share the same common header. The fields of this header are as follows:

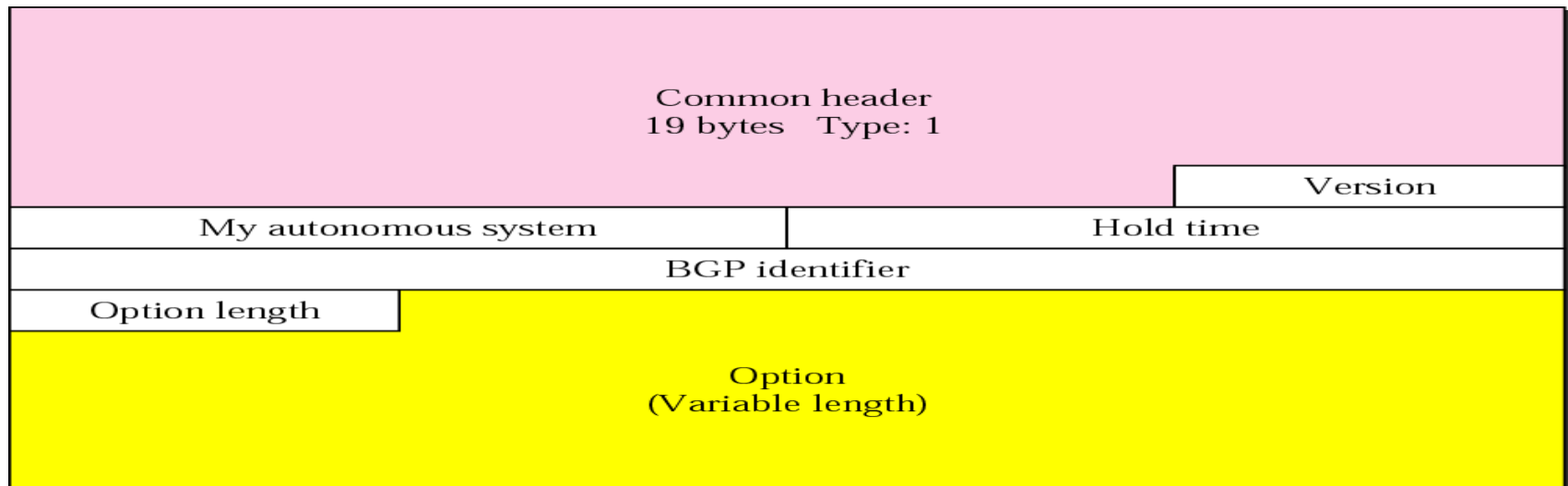
- ❑ **Marker.** The 16-byte marker field is reserved for authentication.
- ❑ **Length.** This 2-byte field defines the length of the total message including the header.
- ❑ **Type.** This 1-byte field defines the type of the packet. As we said before, we have four types, and the values 1 to 4 define those types.

(32 bits)



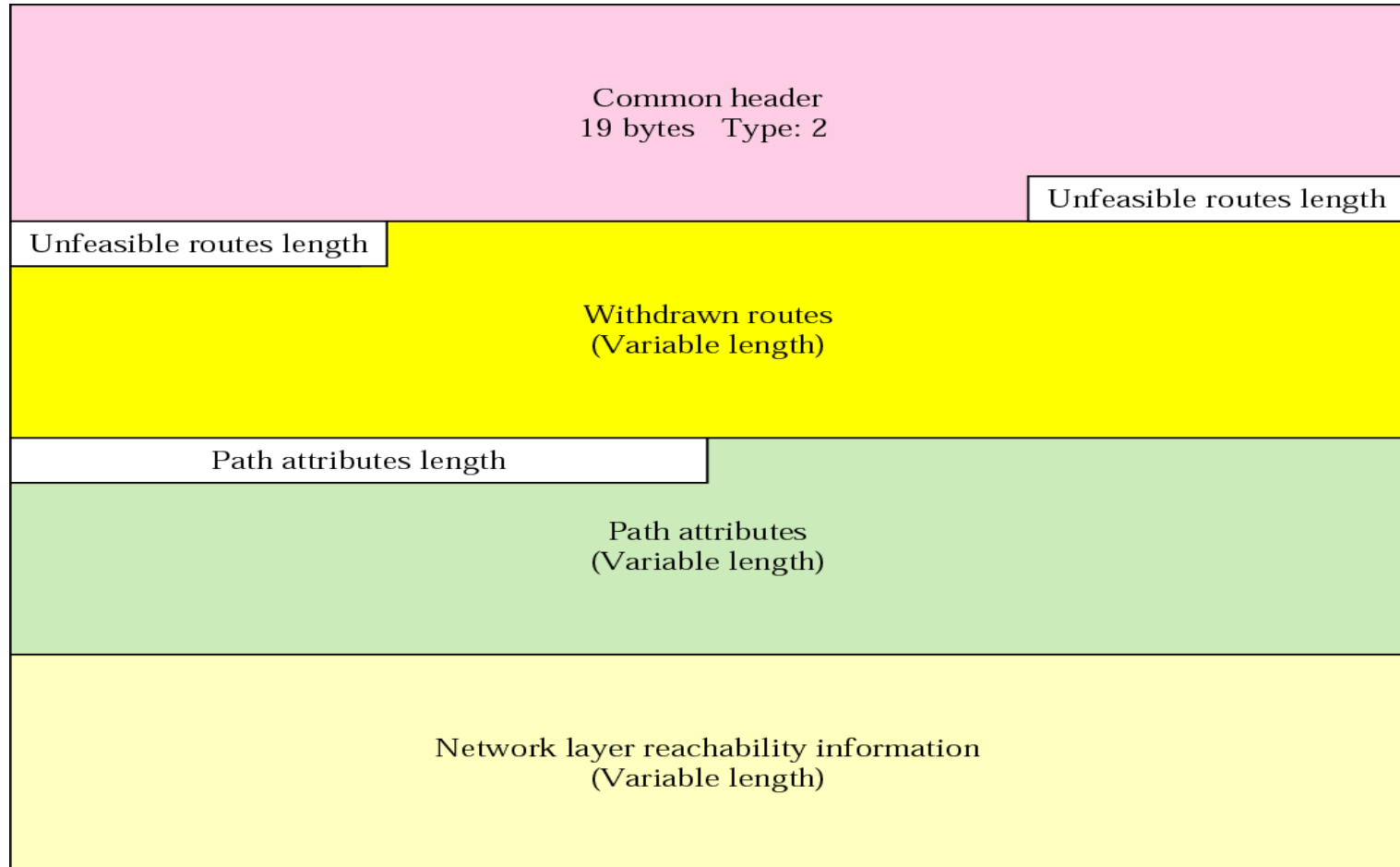
## Open message(\*\*)

To create a neighbourhood relationship, a router running BGP opens a TCP connection with a neighbour and sends an open message. If the neighbour accepts the neighbourhood relationship, it responds with a **keepalive message**, which means that a relationship has been established between the two routers



# Update message(\*\*)

The update message is the heart of the BGP protocol. It is used by a router to withdraw destinations that have been advertised previously, announce a route to a new destination, or both.



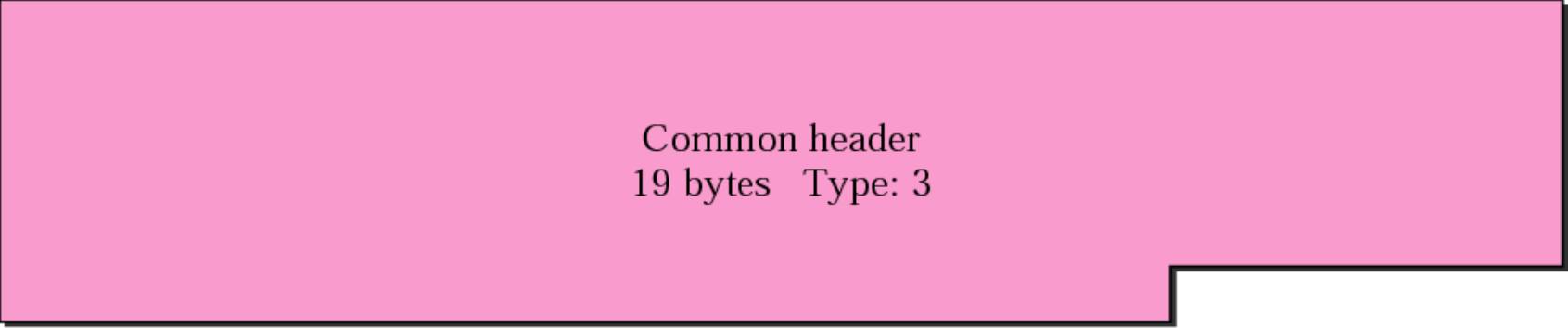


***BGP supports classless addressing and  
CIDR.***



## *Keepalive message(\*\*)*

***Keepalive Message*** The routers (called *peers in BGP parlance*) running the *BGP protocols* exchange keepalive messages regularly (before their hold time expires) to tell each other that they are alive.

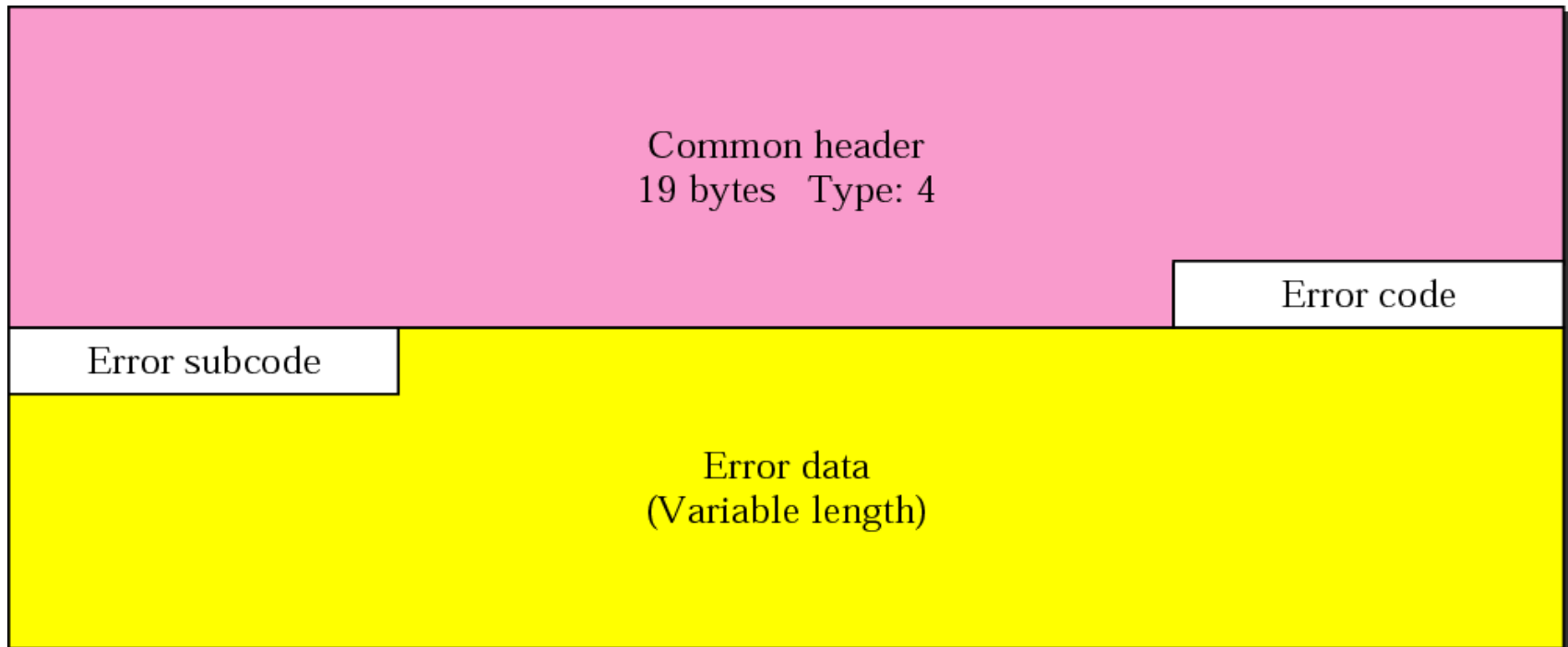


Common header  
19 bytes Type: 3



# *Notification message(\*\*)*

**A notification message is sent by a router whenever an error condition is detected or a router wants to close the connection.**



**Table 14.3 Error codes**

<i>Error Code</i>	<i>Error Code Description</i>	<i>Error Subcode Description</i>
1	Message header error	Three different subcodes are defined for this type of error: synchronization problem (1), bad message length (2), and bad message type (3).
2	Open message error	Six different subcodes are defined for this type of error: unsupported version number (1), bad peer AS (2), bad BGP identifier (3), unsupported optional parameter (4), authentication failure (5), and unacceptable hold time (6).
3	Update message error	Eleven different subcodes are defined for this type of error: malformed attribute list (1), unrecognized well-known attribute (2), missing well-known attribute (3), attribute flag error (4), attribute length error (5), invalid origin attribute (6), AS routing loop (7), invalid next hop attribute (8), optional attribute error (9), invalid network field (10), malformed AS_PATH (11).
4	Hold timer expired	No subcode defined.
5	Finite state machine error	This defines the procedural error. No subcode defined.
6	Cease	No subcode defined.



***BGP uses the services of TCP  
on port 179.***