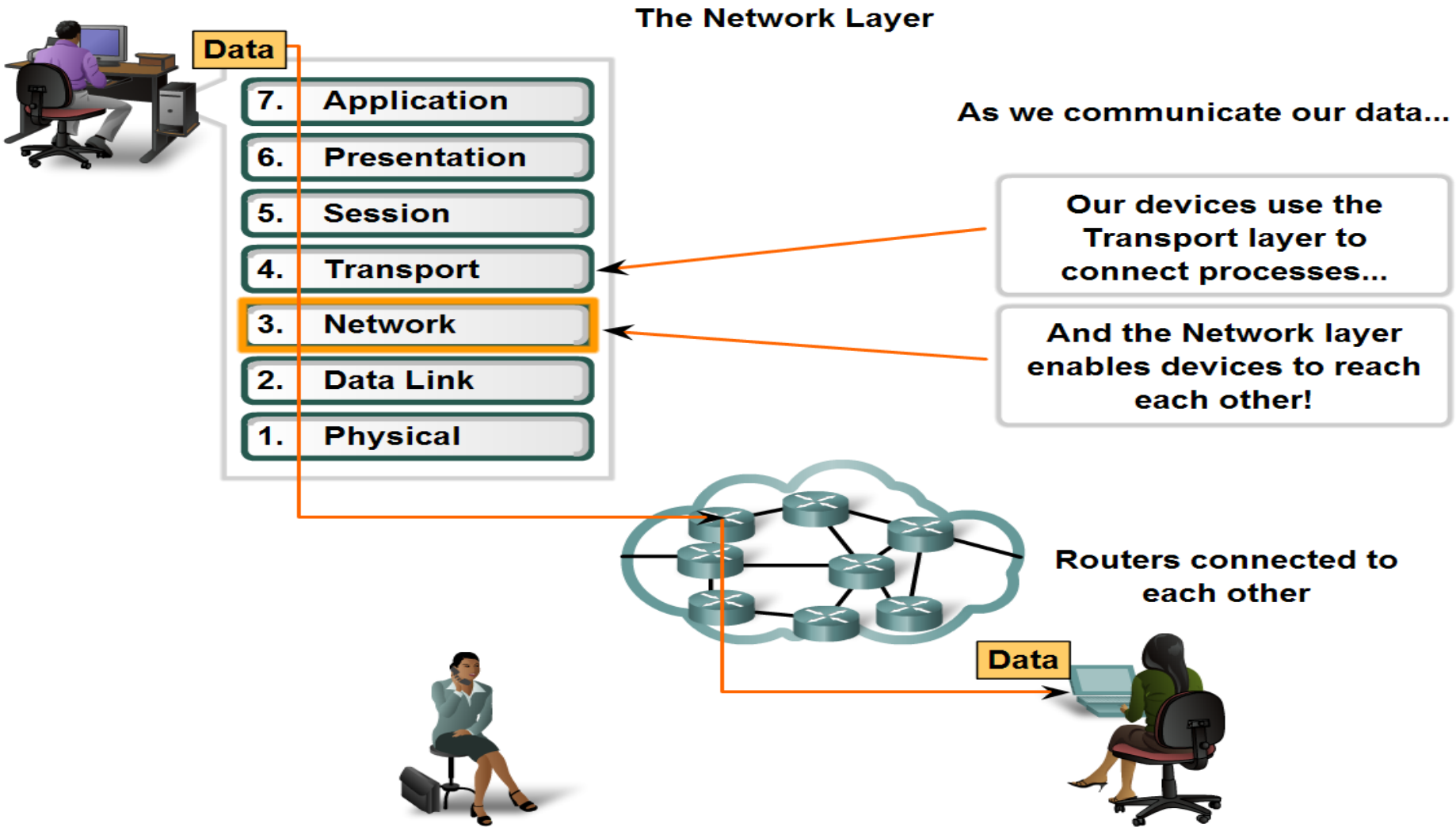
OSI Network Layer

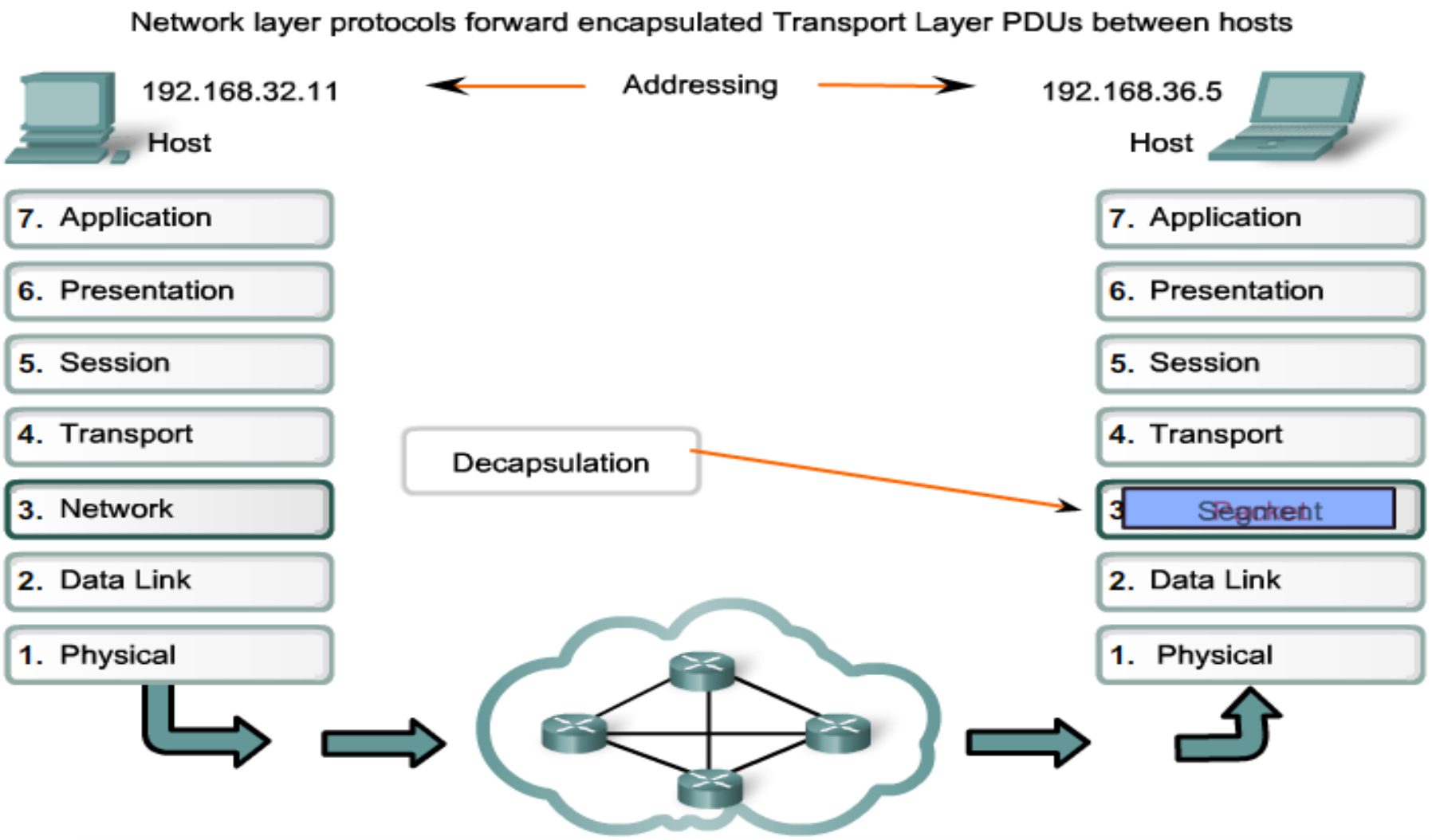
Objectives

- Identify the role of the Network Layer, as it describes communication from one end device to another end device
- Examine the most common Network Layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service
- Understand the principles used to guide the division or grouping of devices into networks
- Understand the hierarchical addressing of devices and how this allows communication between networks
- Understand the fundamentals of routes, next hop addresses and packet forwarding to a destination network

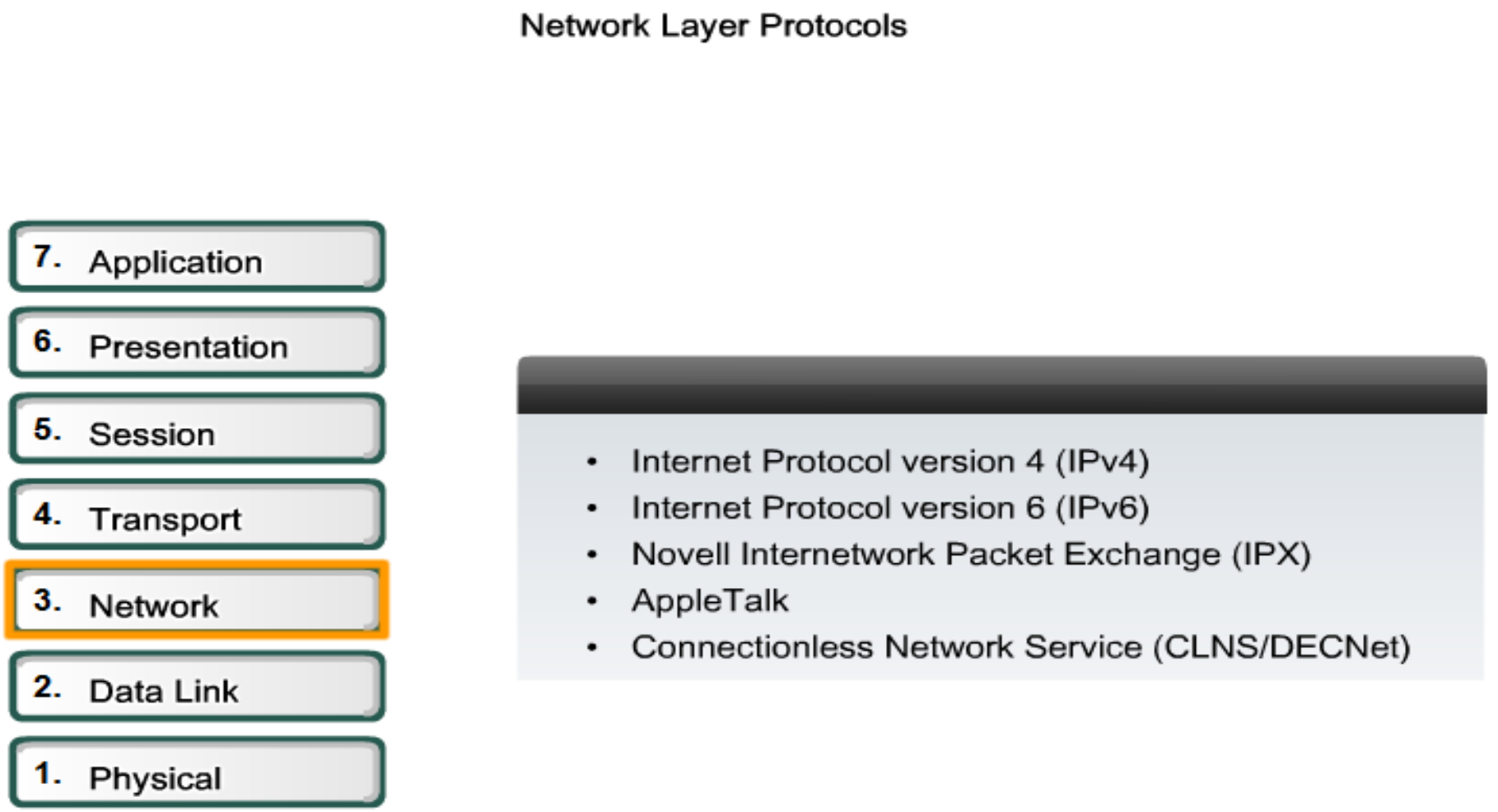
Network Layer Protocols



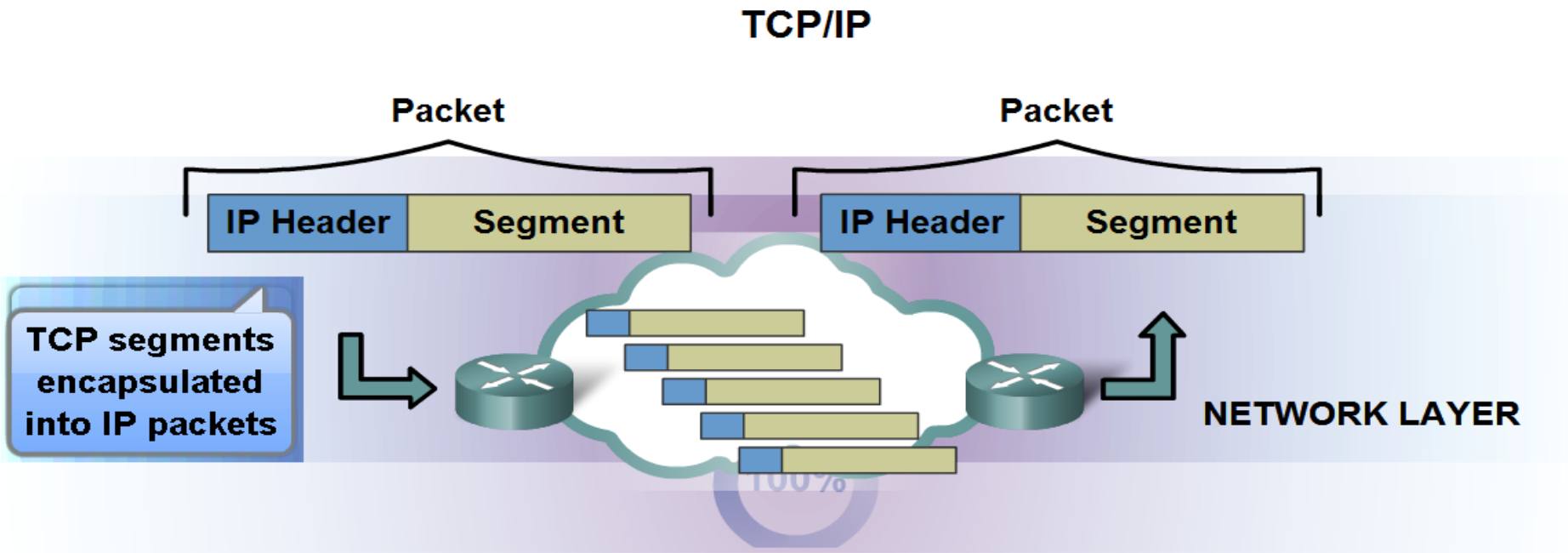
Network Layer Protocols



Network Layer Protocols



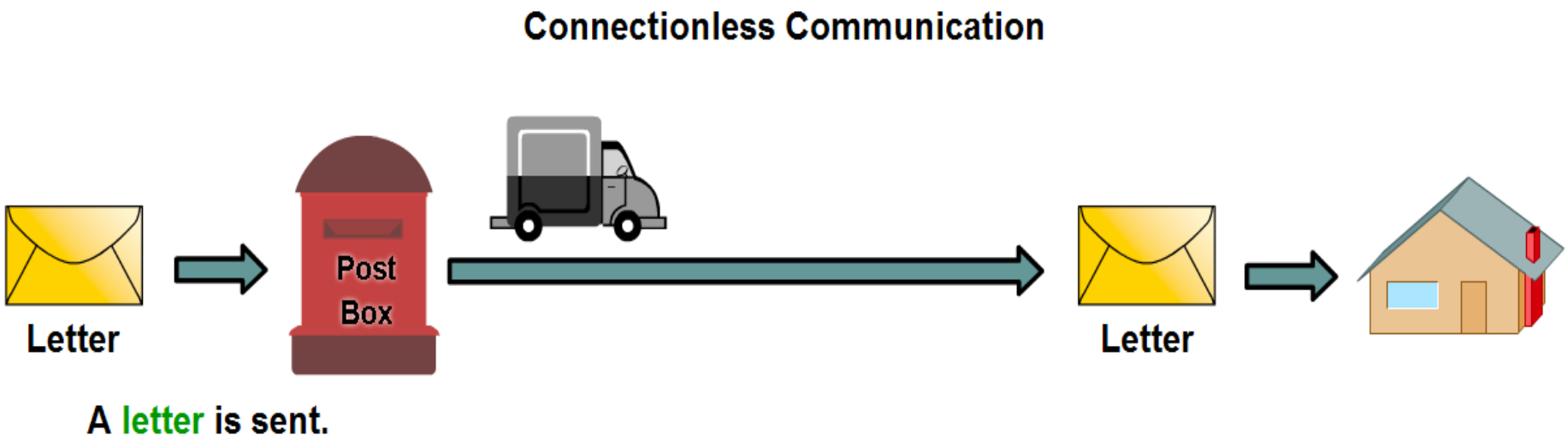
Network Layer Protocols and Internet Protocol (IP)



IP Packets flow through the internetwork.

- Connectionless - No connection is established before sending data packets.
- Best Effort (unreliable) - No overhead is used to guarantee packet delivery.
- Media Independent - Operates independently of the medium carrying the data.

Network Layer Protocols and Internet Protocol (IP)



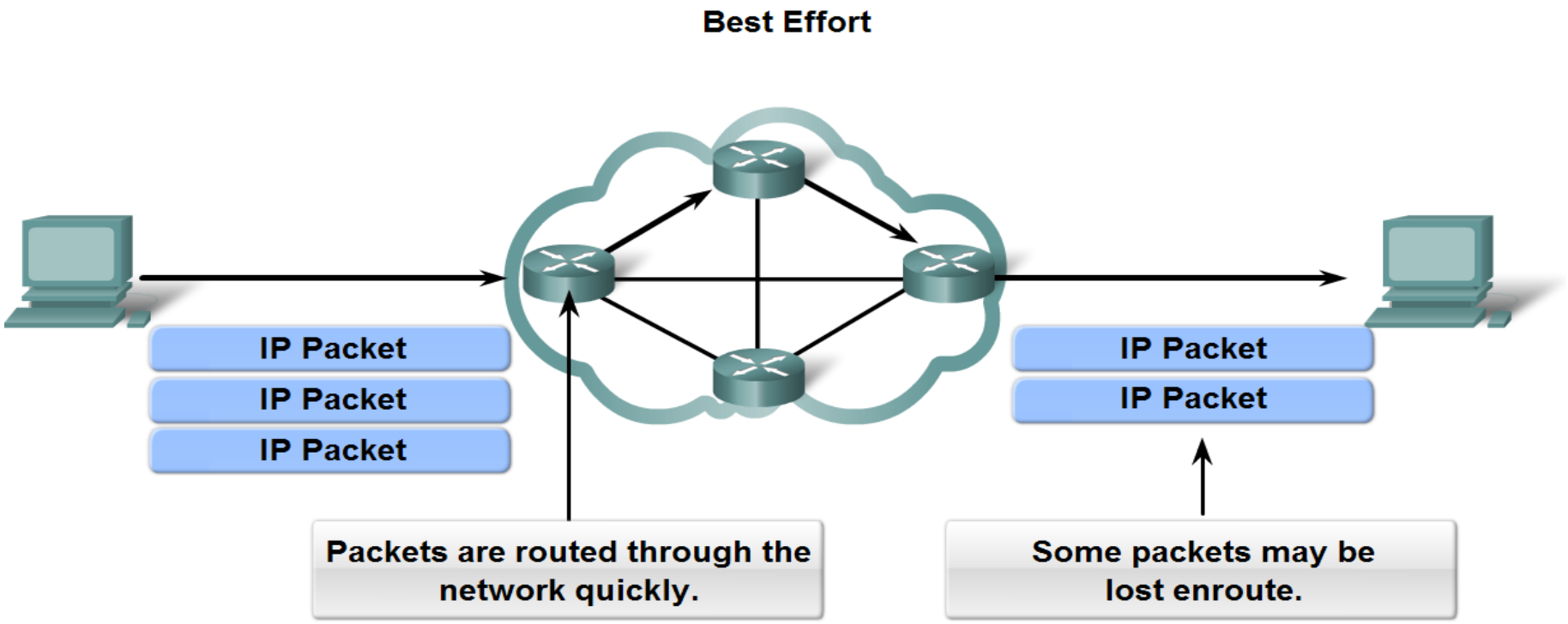
The sender doesn't know:

- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

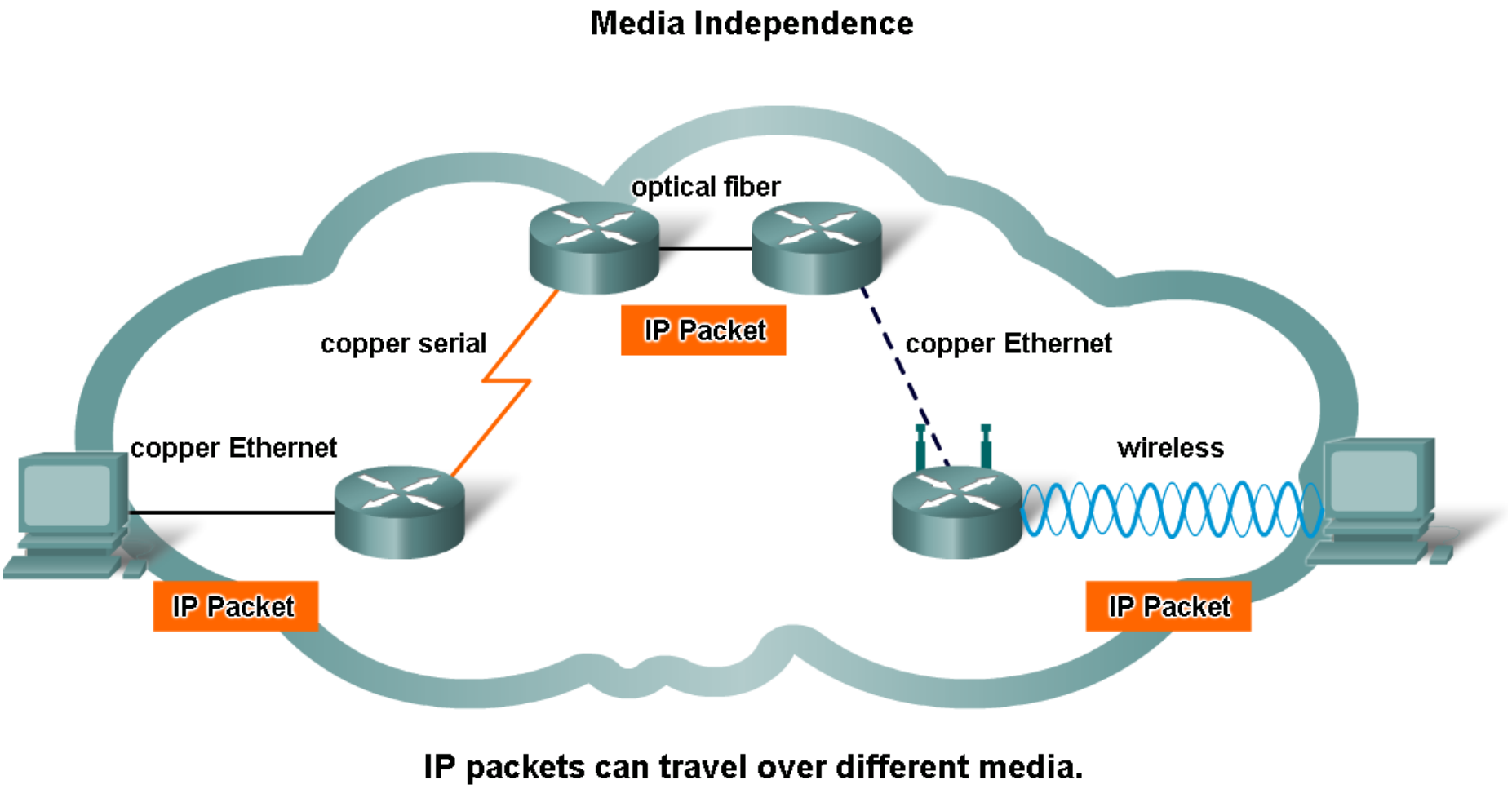
Network Layer Protocols and Internet Protocol (IP)



As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

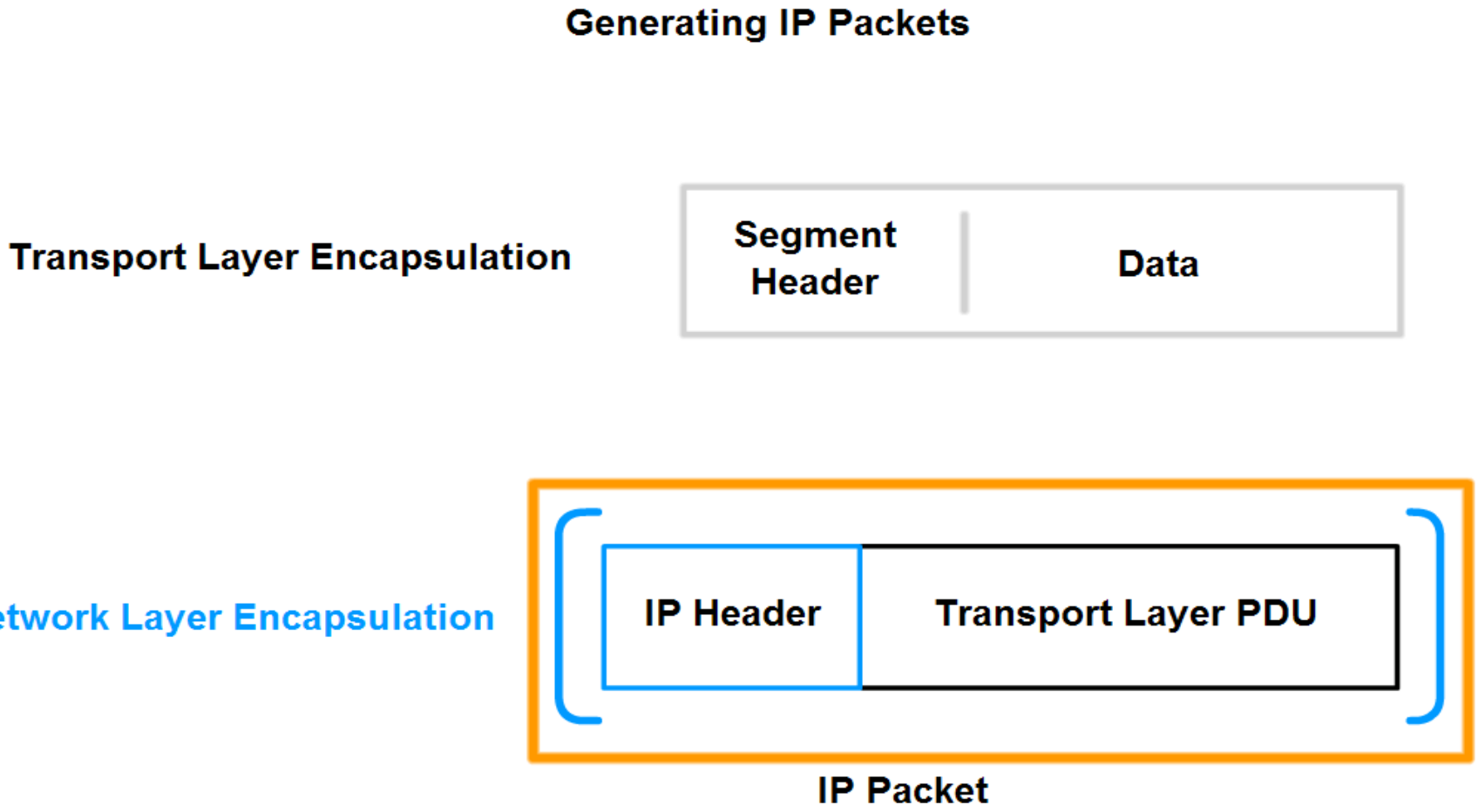
Other protocols manage the process of tracking packets and ensuring their delivery.

Network Layer Protocols and Internet Protocol (IP)



IP packets can travel over different media.

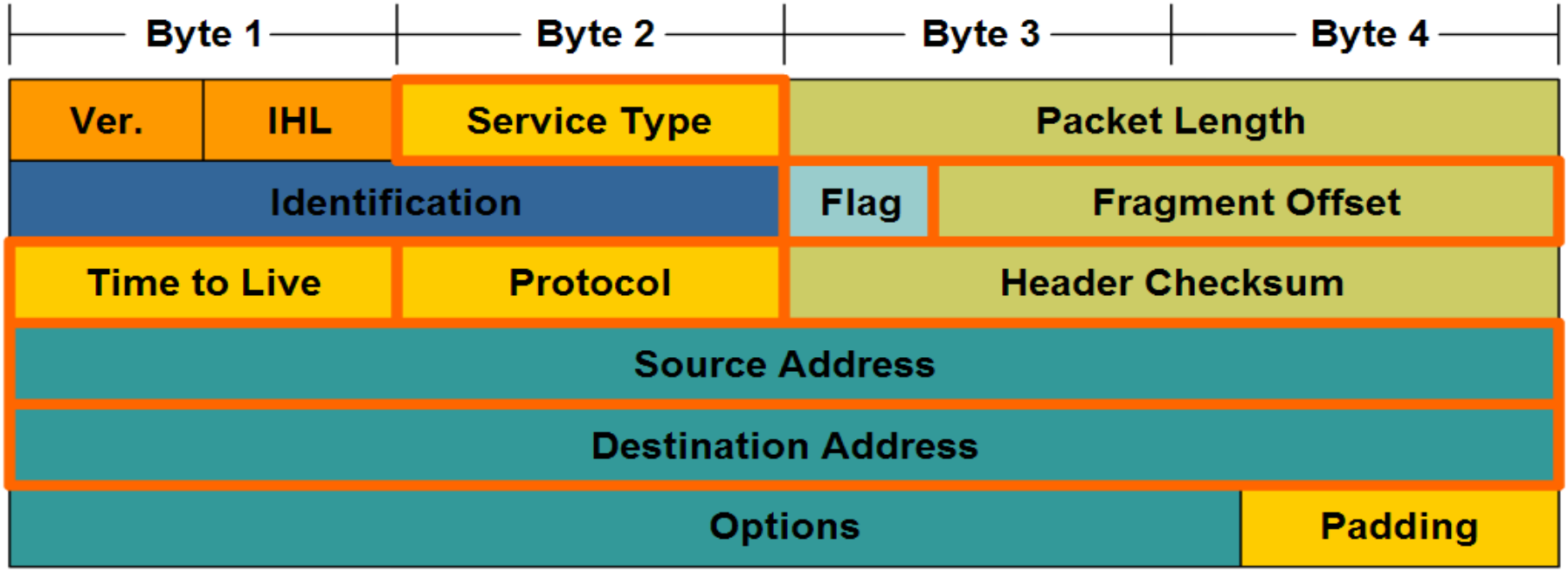
Network Layer Protocols and Internet Protocol (IP)



In TCP/IP based networks, the Network layer PDU is the IP packet.

Network Layer Protocols and Internet Protocol (IP)

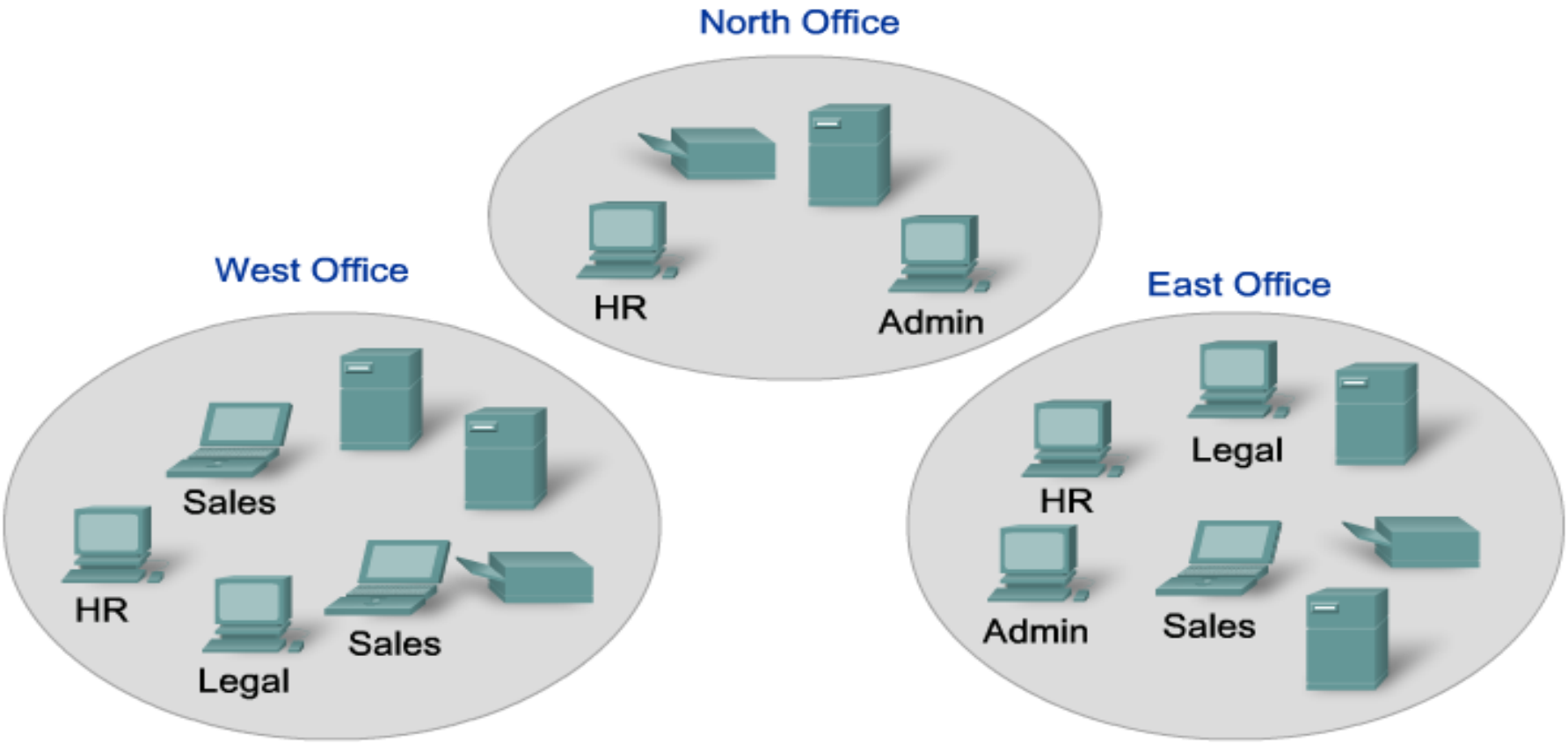
IPv4 Packet Header Fields



Traffic Types

- Unicast Vs Multicast Vs Broadcast
  - Unicast:- One source , One destination
  - Multicast:- One source , Many destination
  - Broadcast:-One source , All destinations
- Routers never forward the Broadcast traffic

Grouping Devices into Networks and Hierarchical Addressing

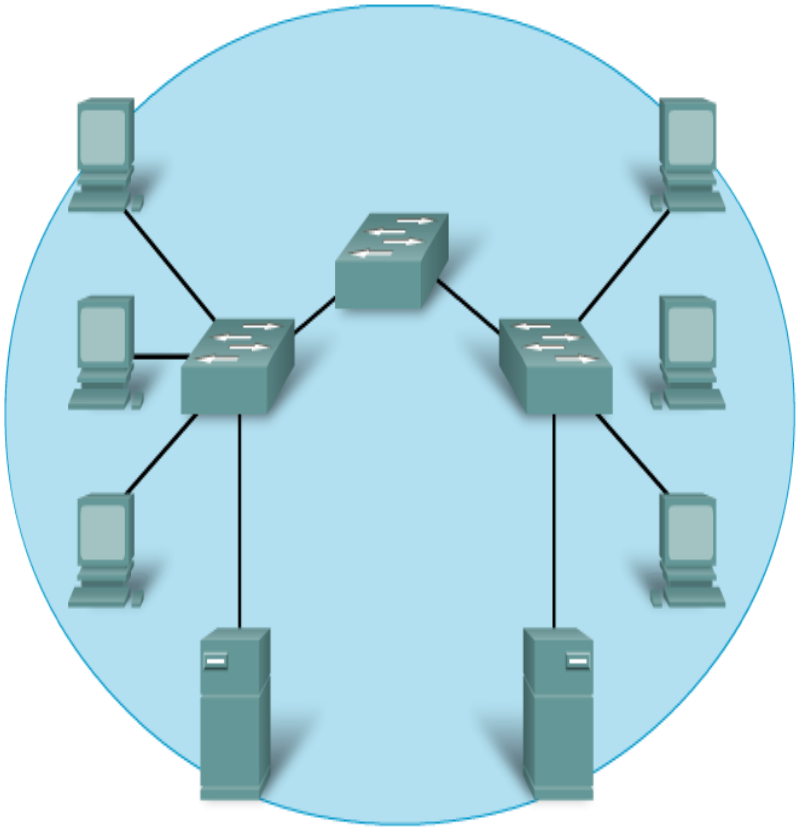


The simple fact of wiring together the physical network can make geographic location a logical place to start when segmenting a network.

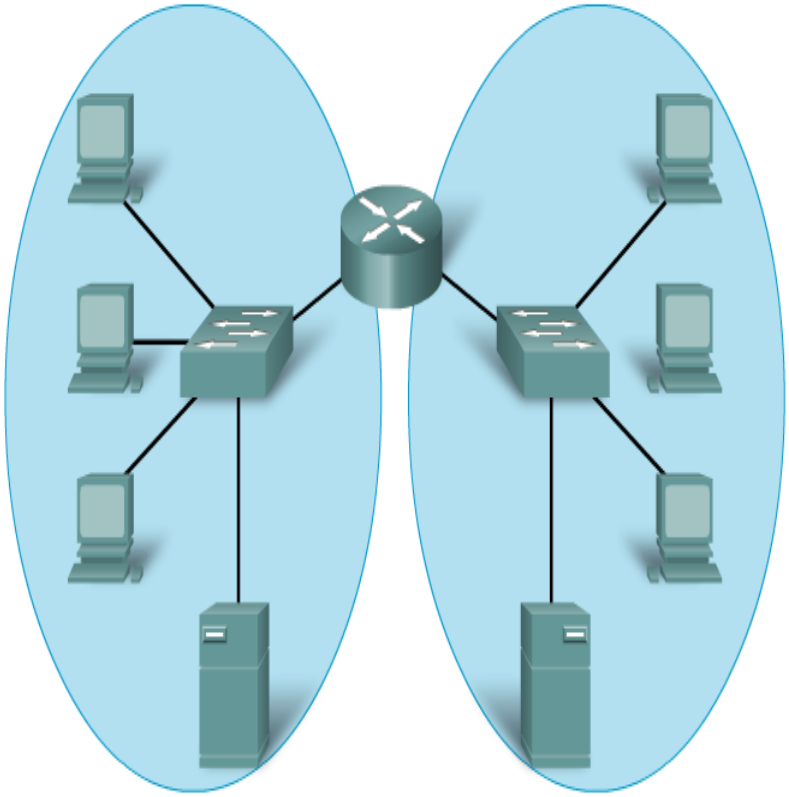
Segmentation of networks

- Purpose of network segmentation are:-
  - Increase Network performance
  - Increase Network Security
  - Increase Network Management

Increase Network performance

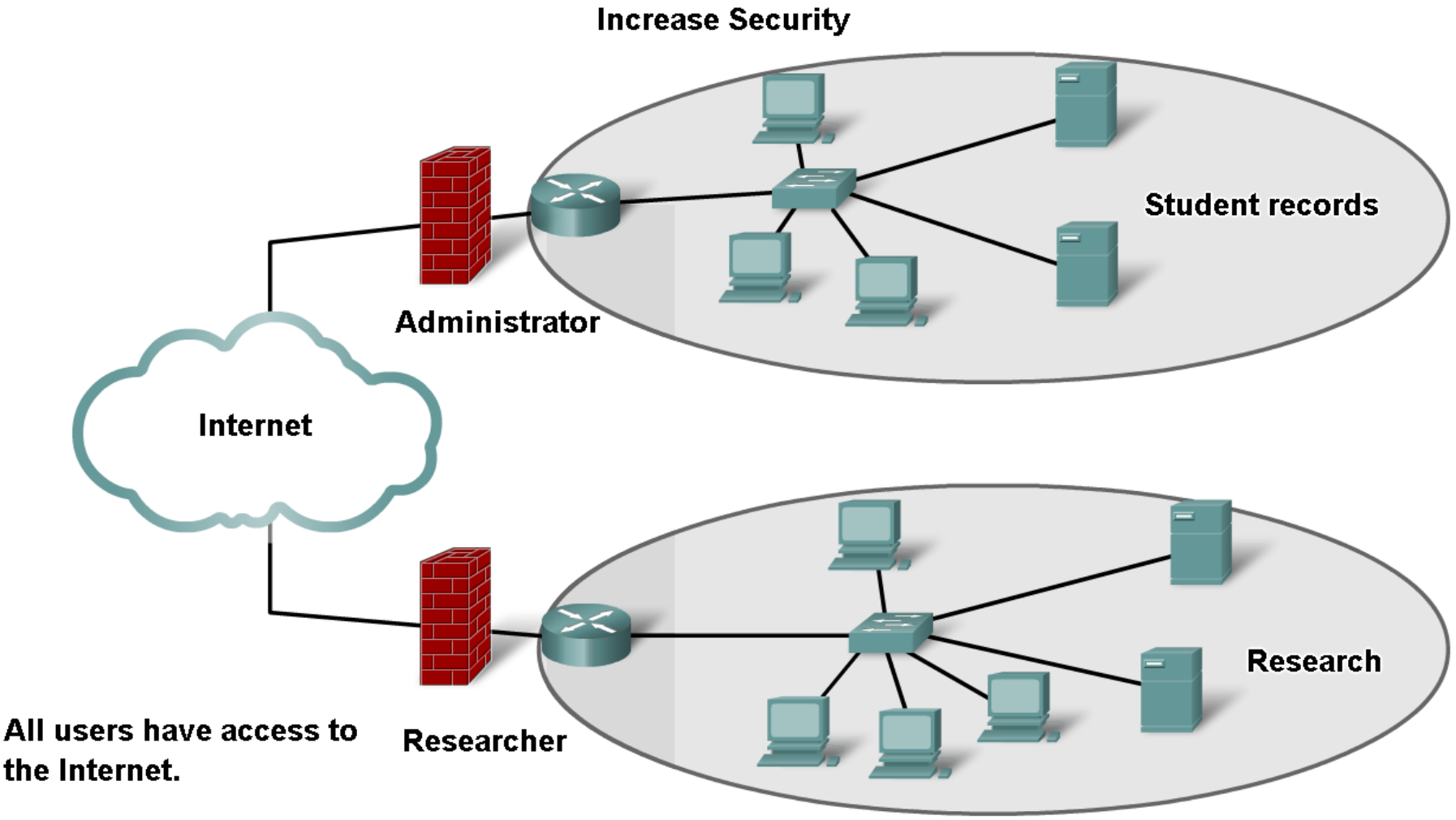


All devices in this network are connected in one broadcast domain when the switch is set to the factory default settings. Since switches forward broadcasts by default, broadcasts are processed by all devices in this network.

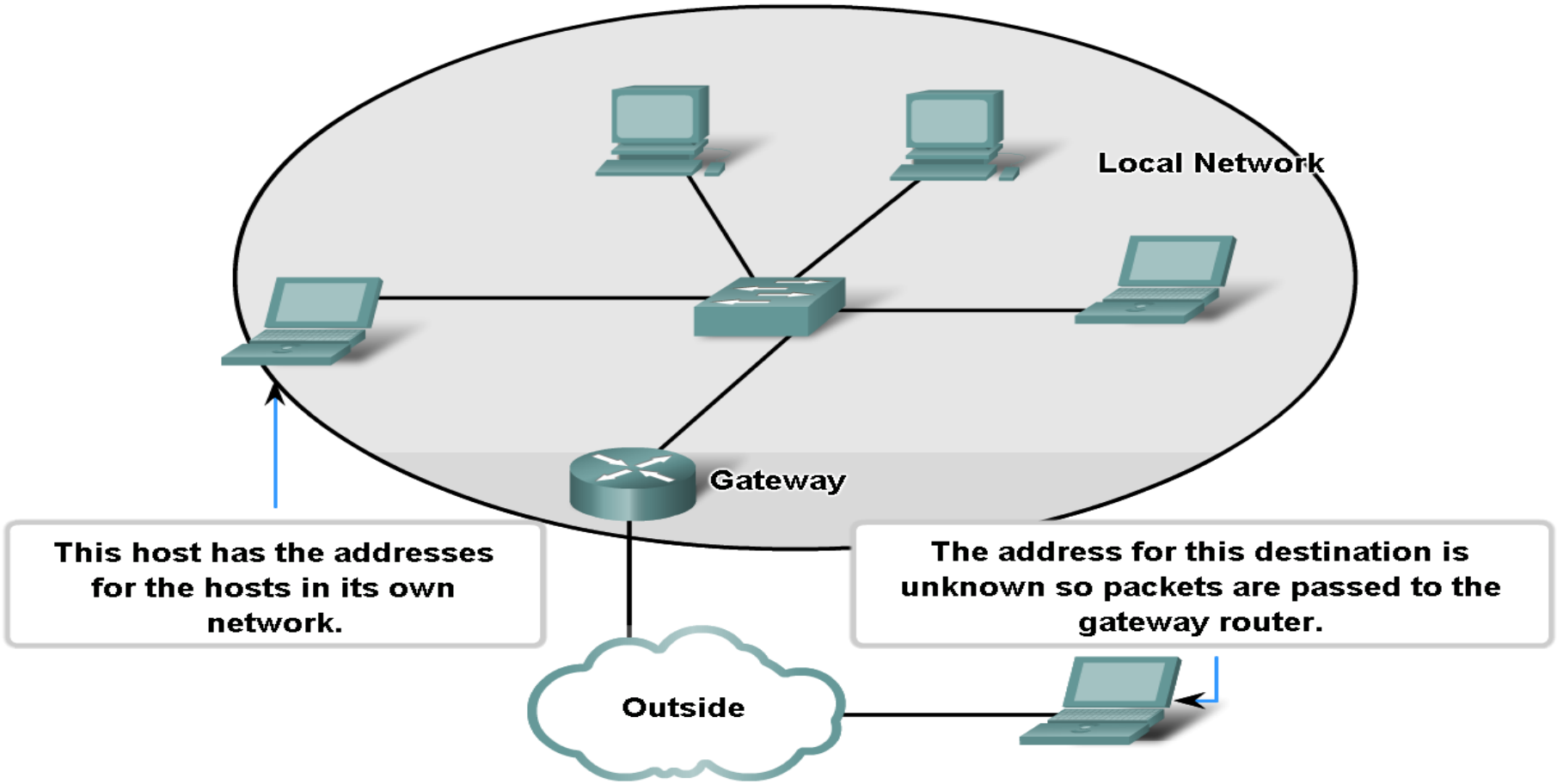


Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

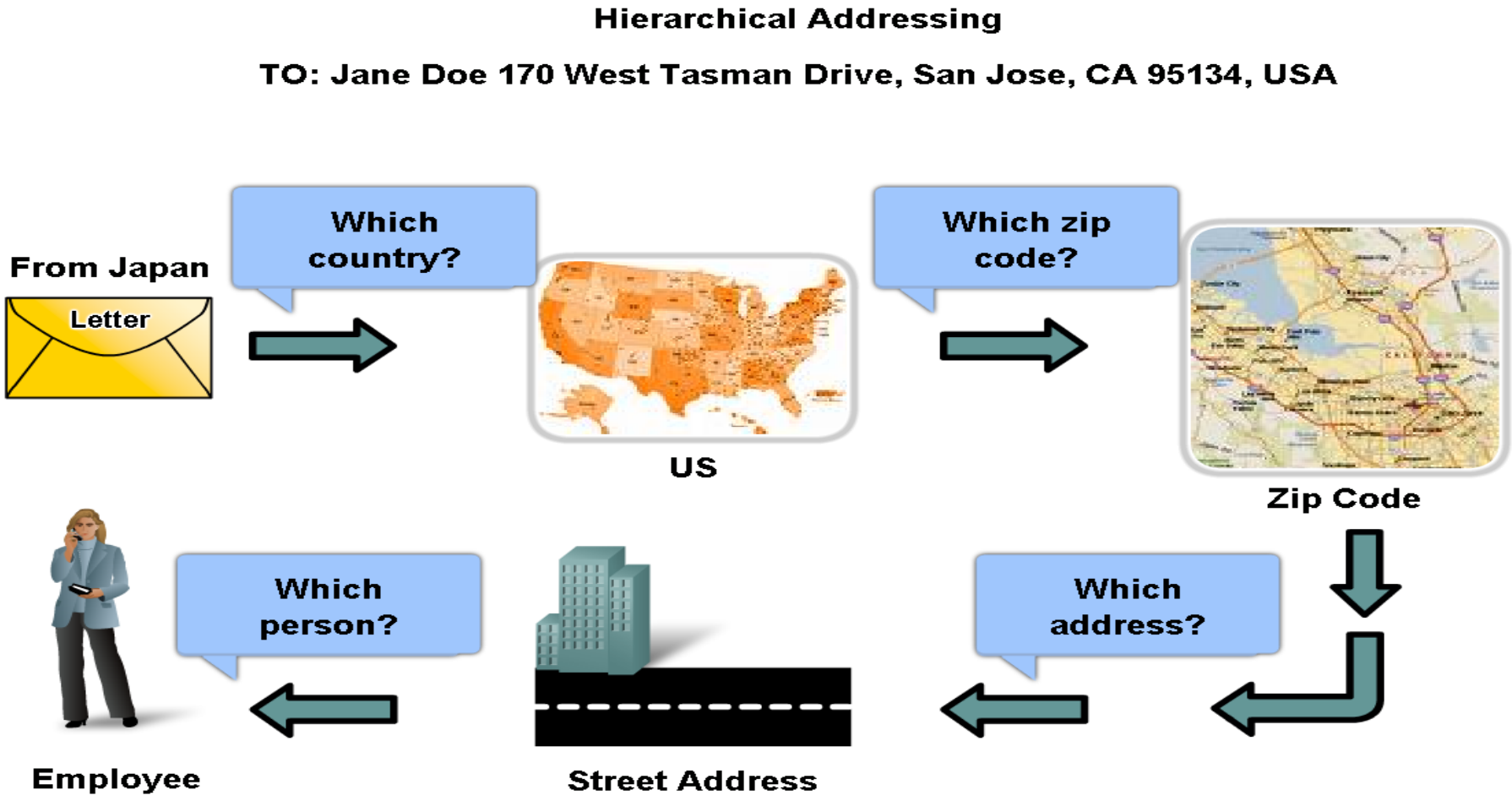
Increase Network Security



Increase Network manageability

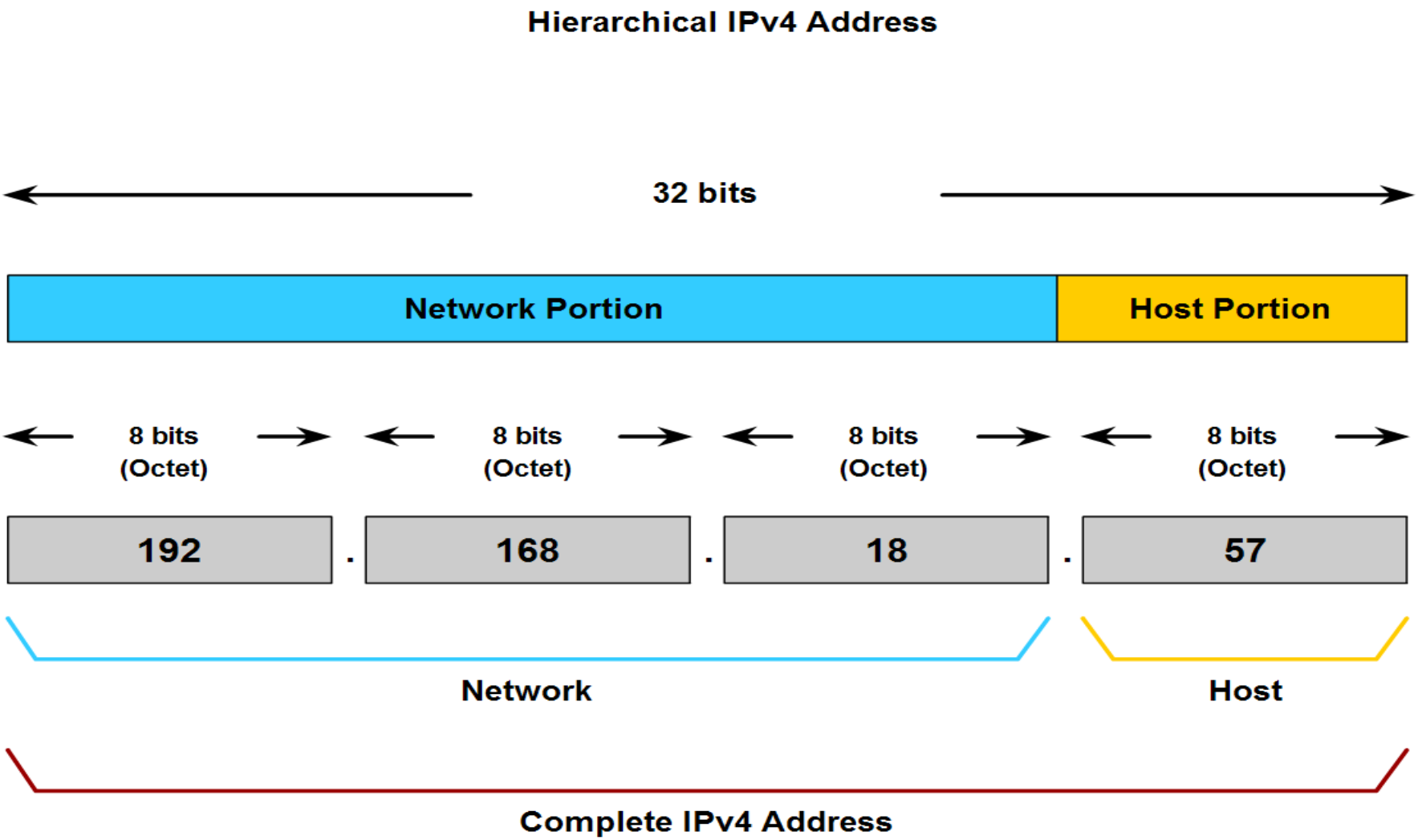


Grouping Devices into Networks and Hierarchical Addressing

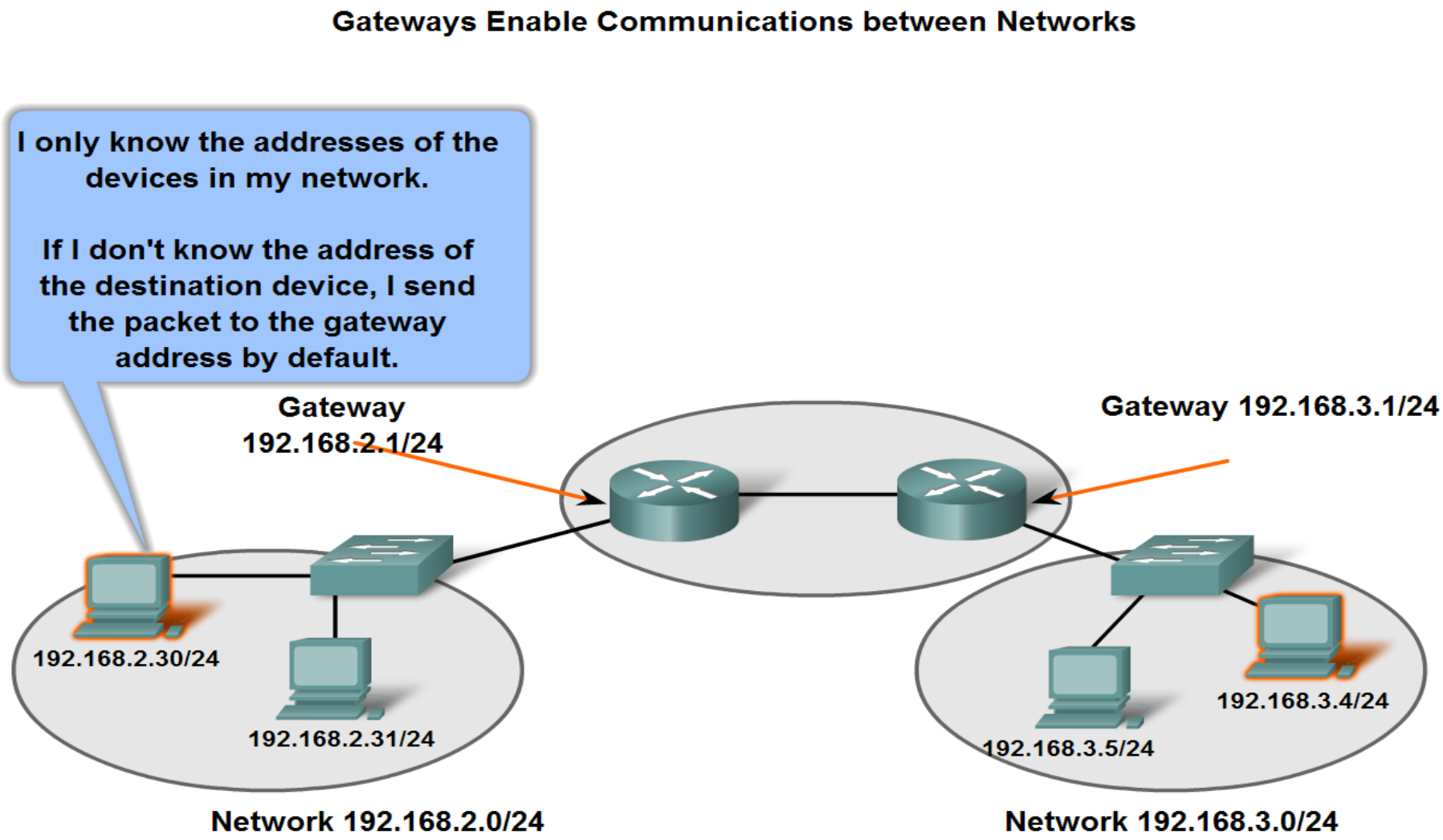


At each step of delivery, the post office need only examine the next hierarchical level.

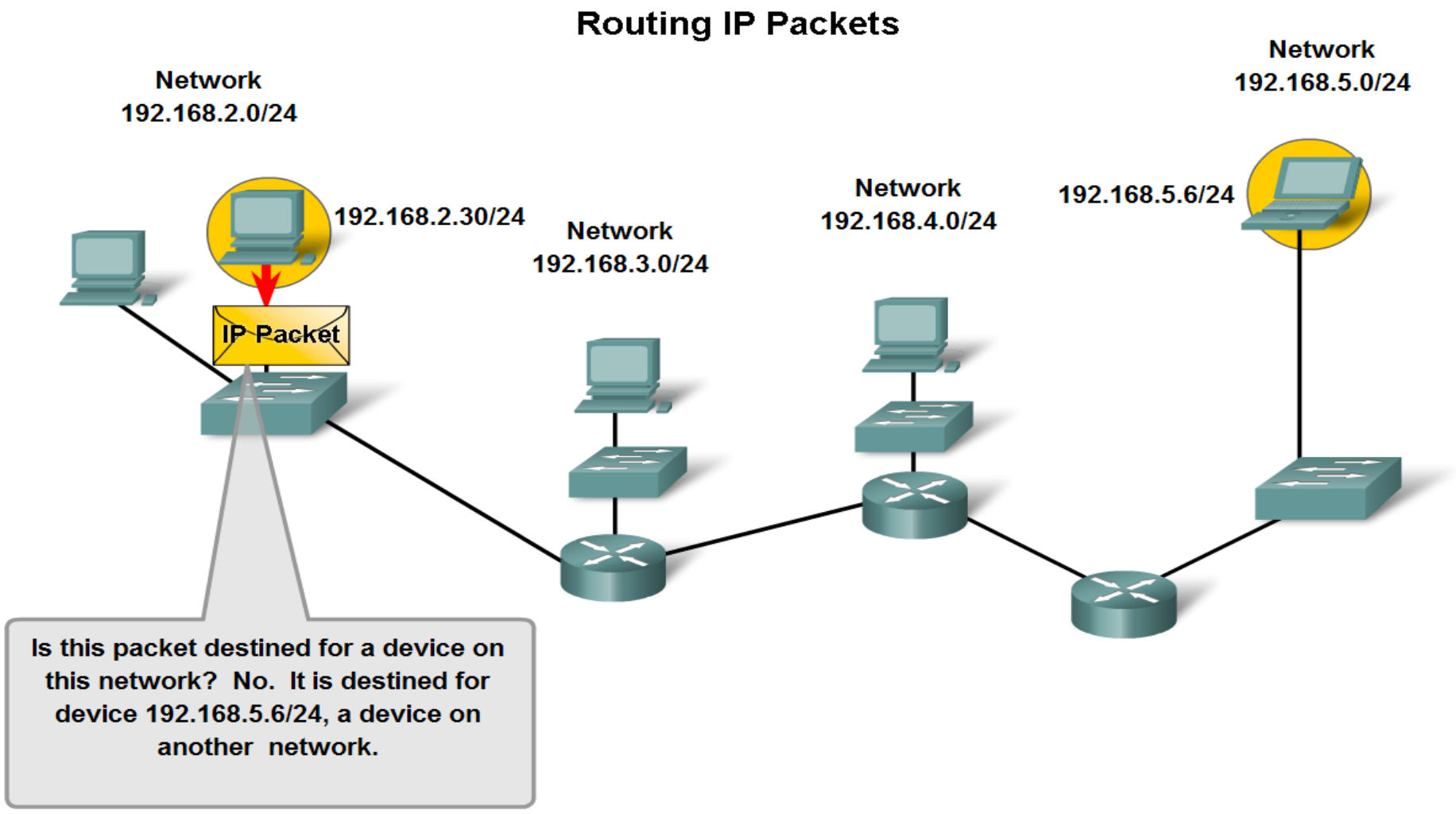
Grouping Devices into Networks and Hierarchical Addressing



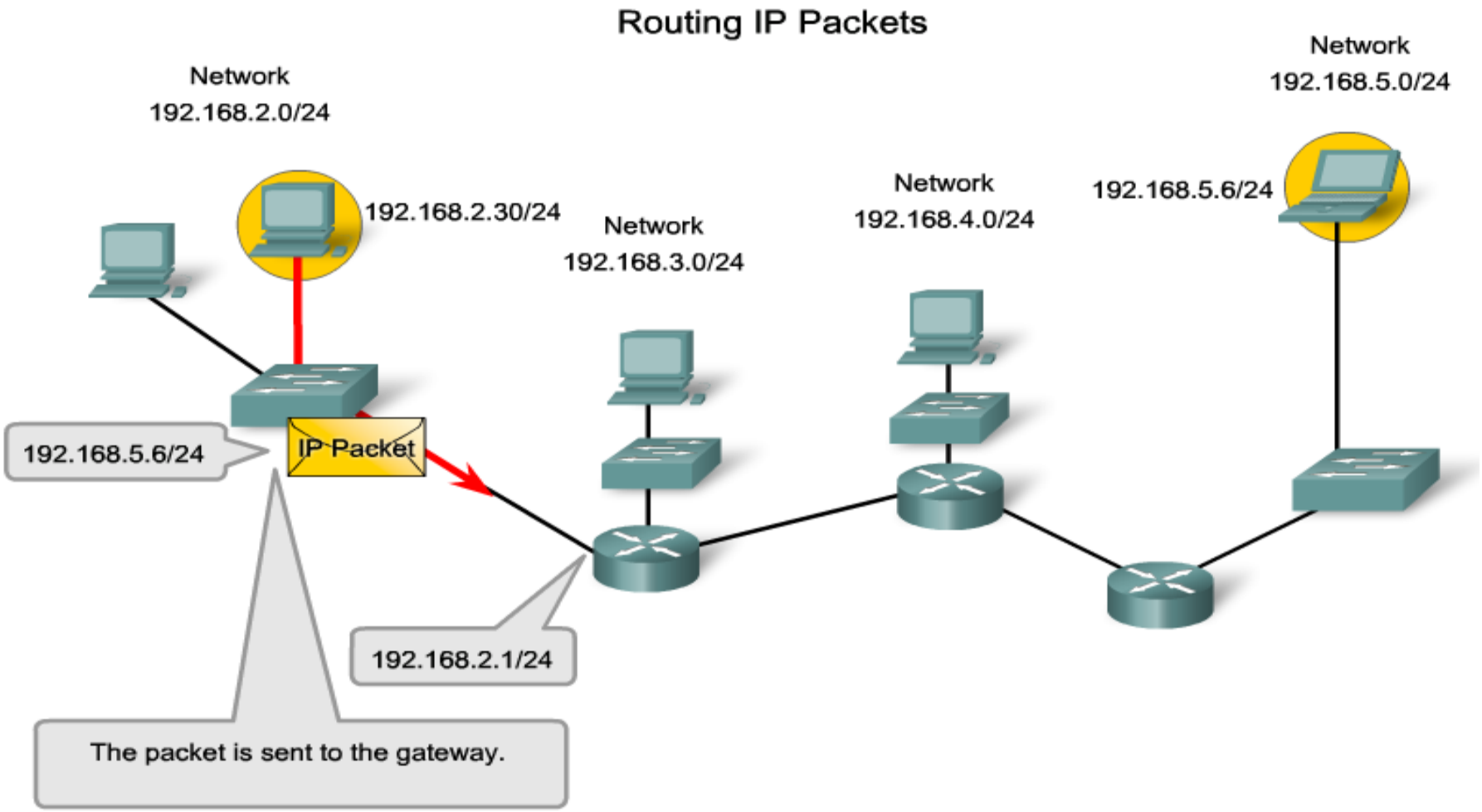
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



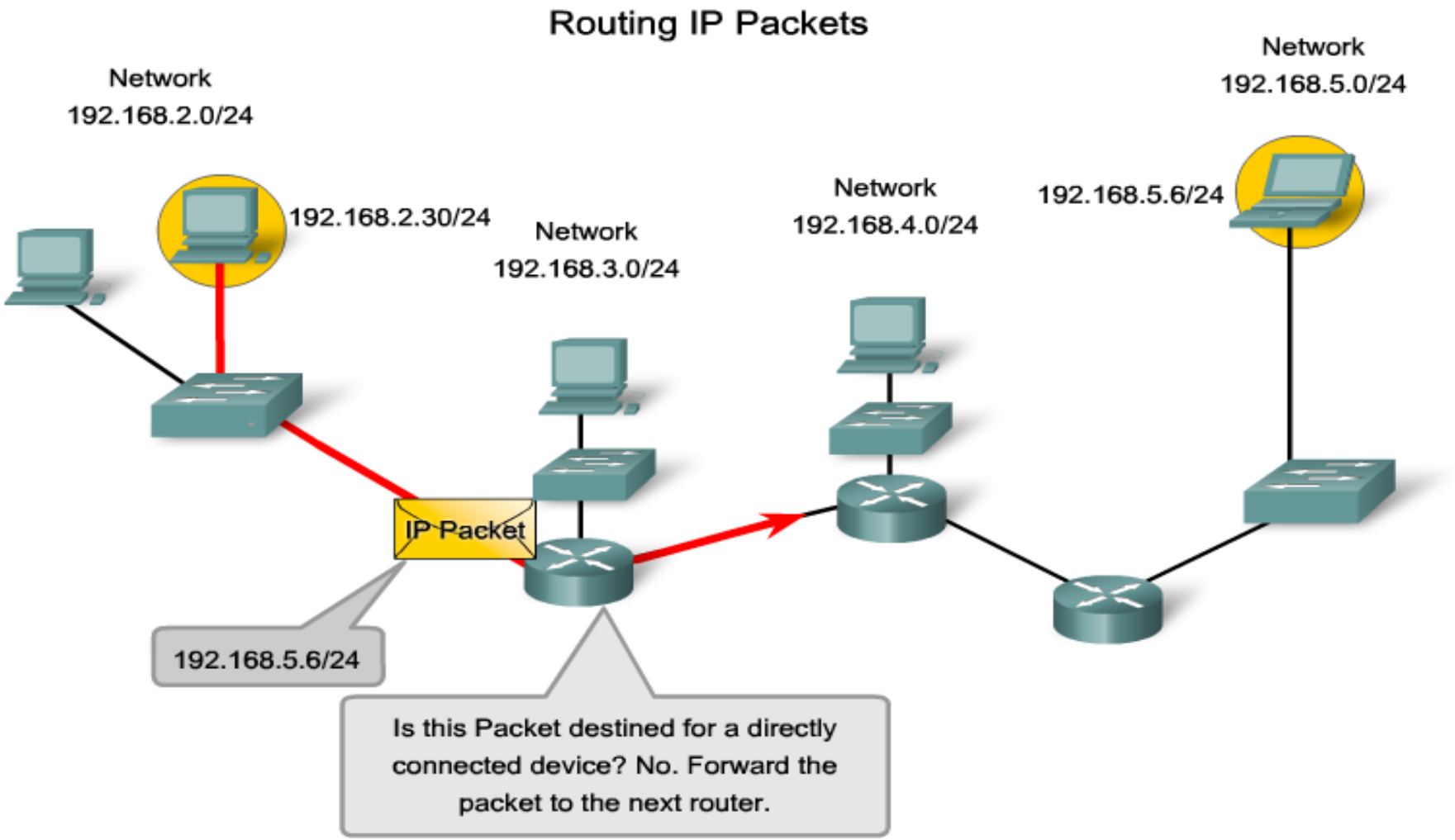
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



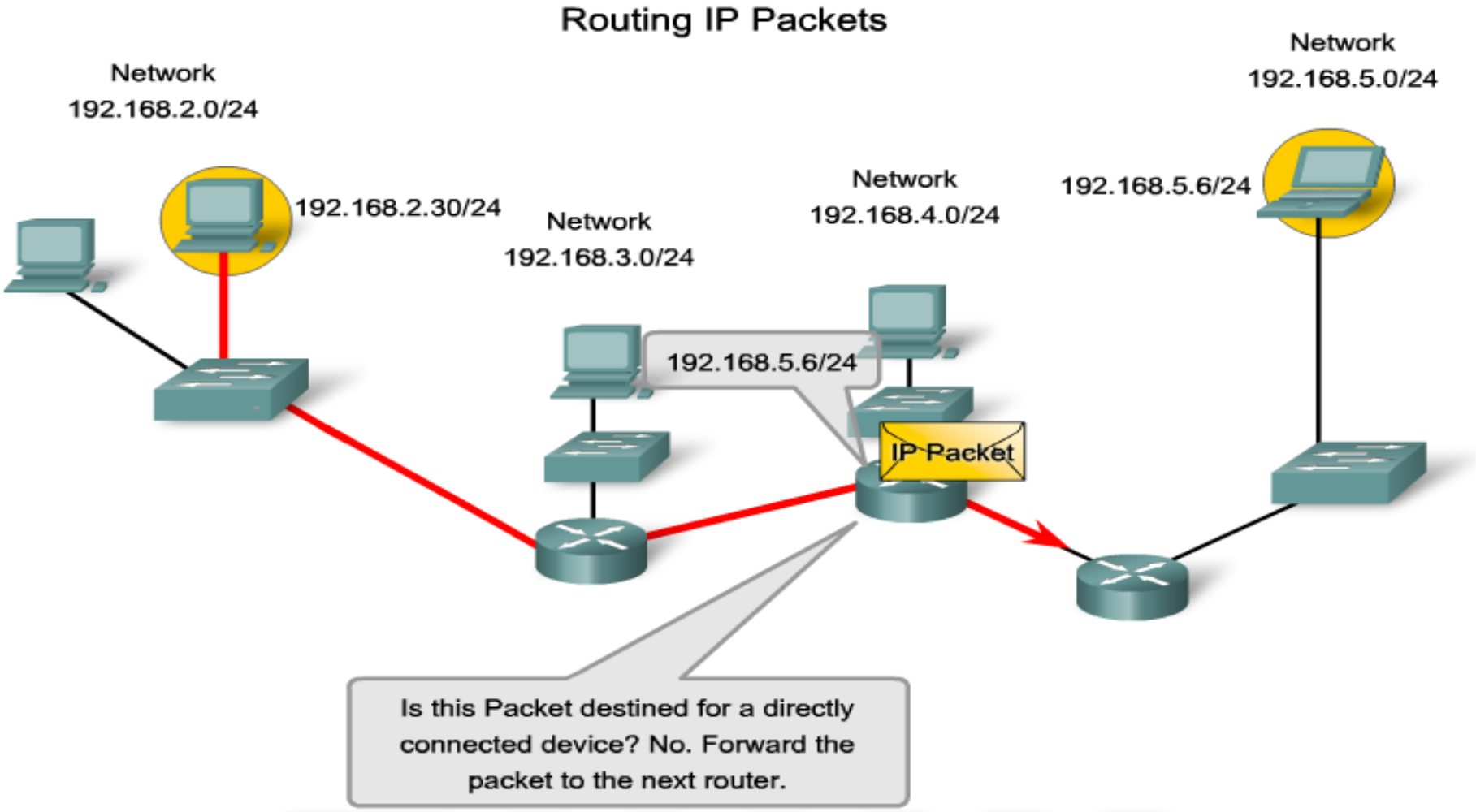
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



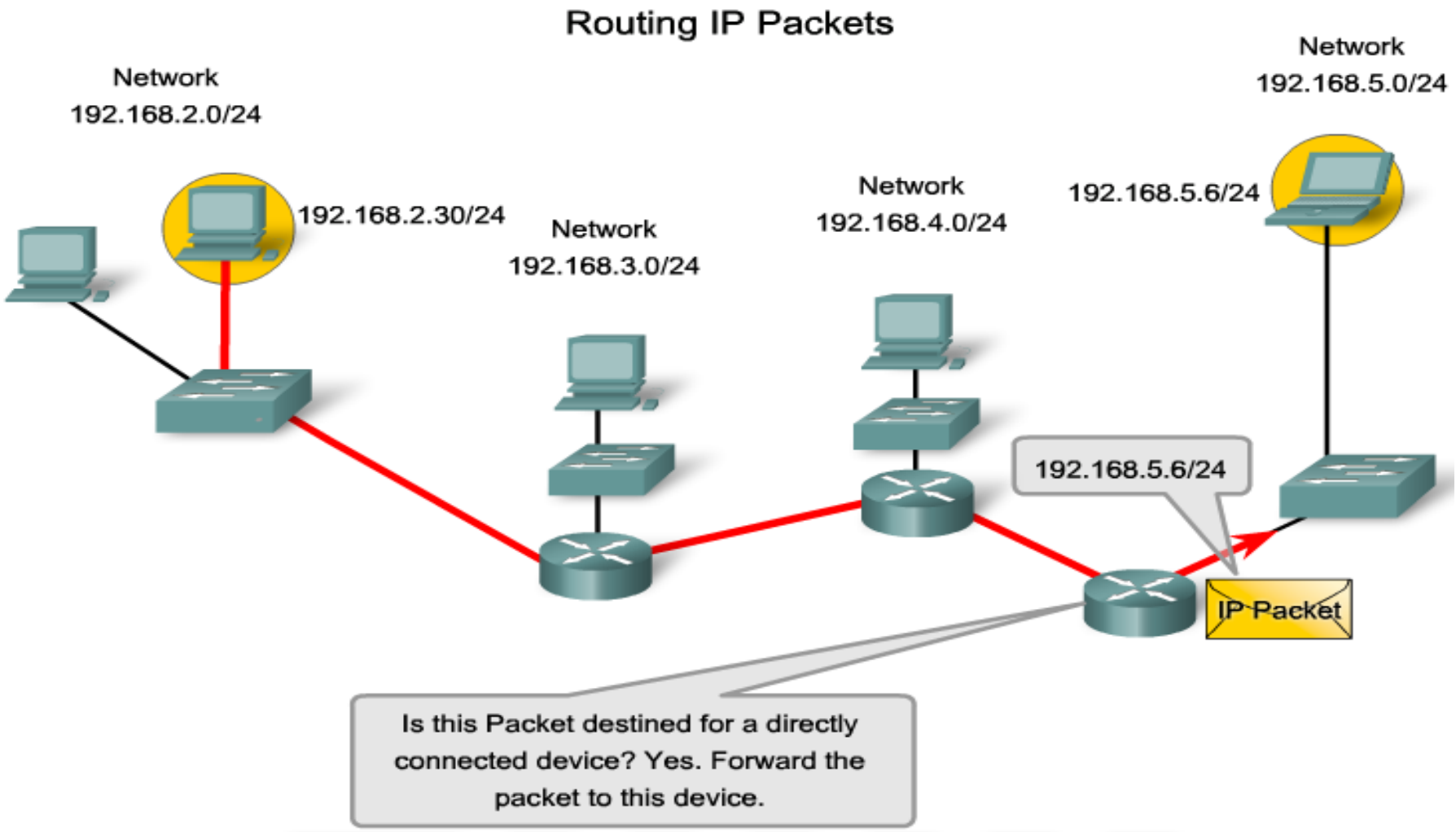
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



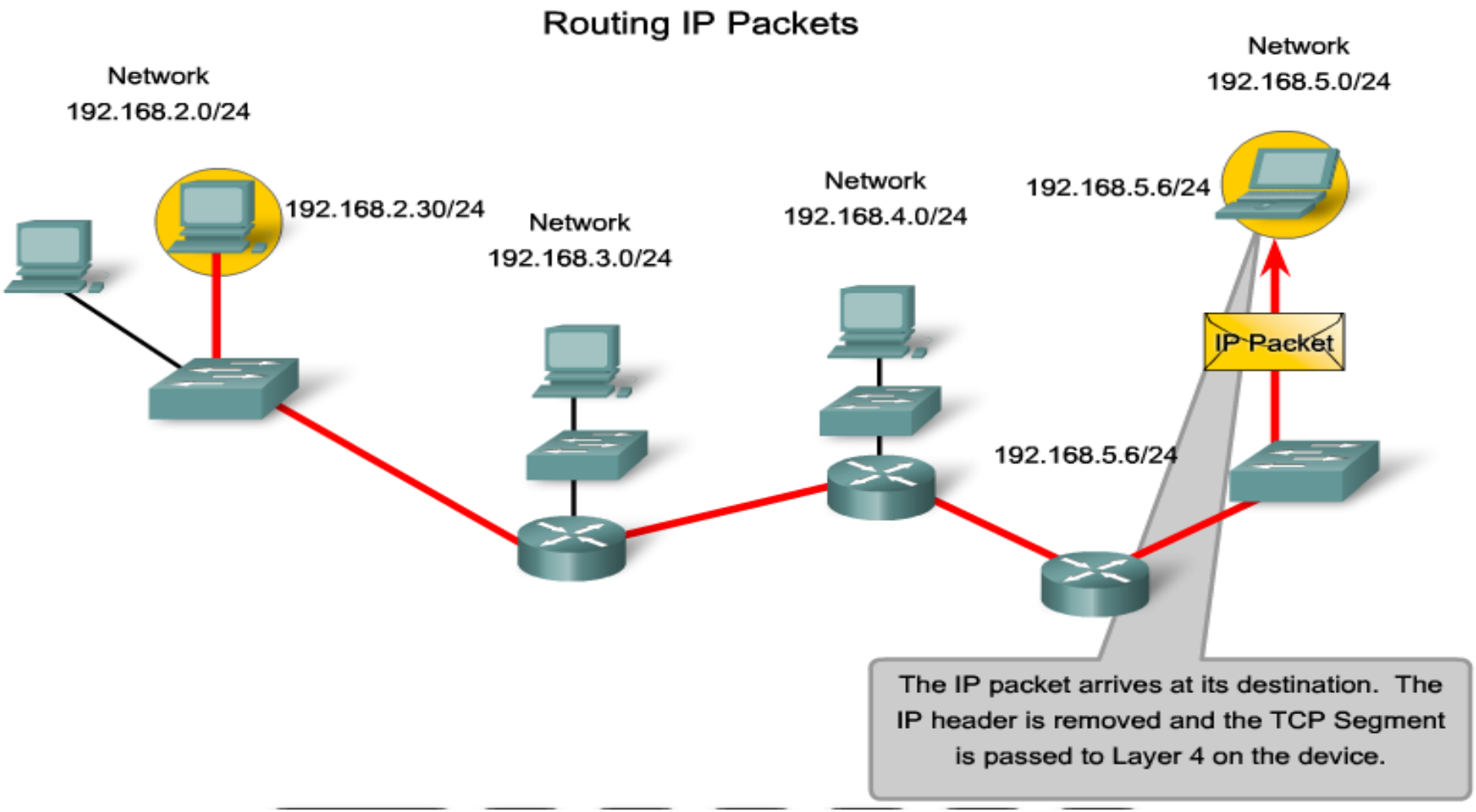
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



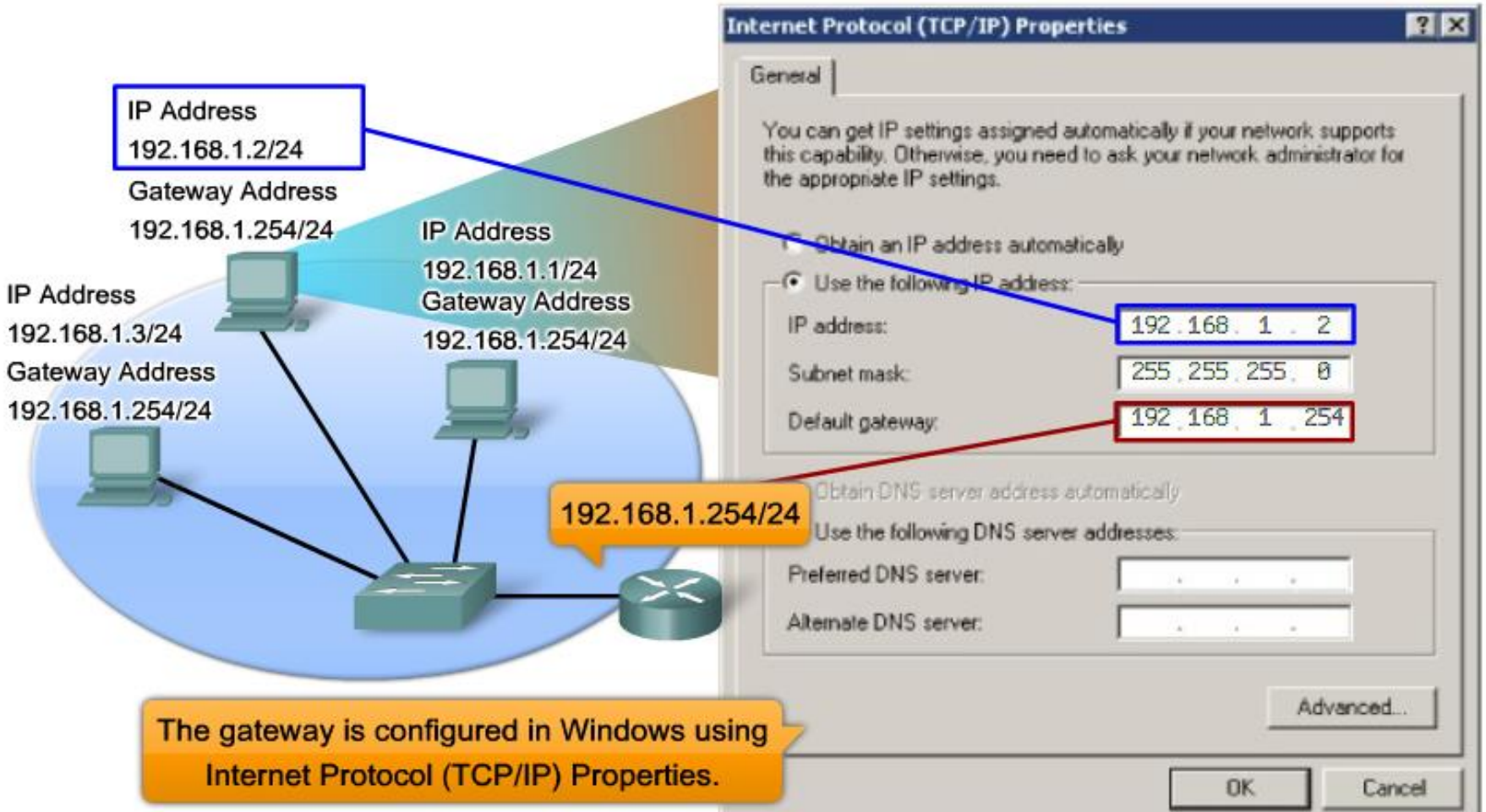
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



Configuring the IP address & default gateway



Configuring the IP address & default gateway

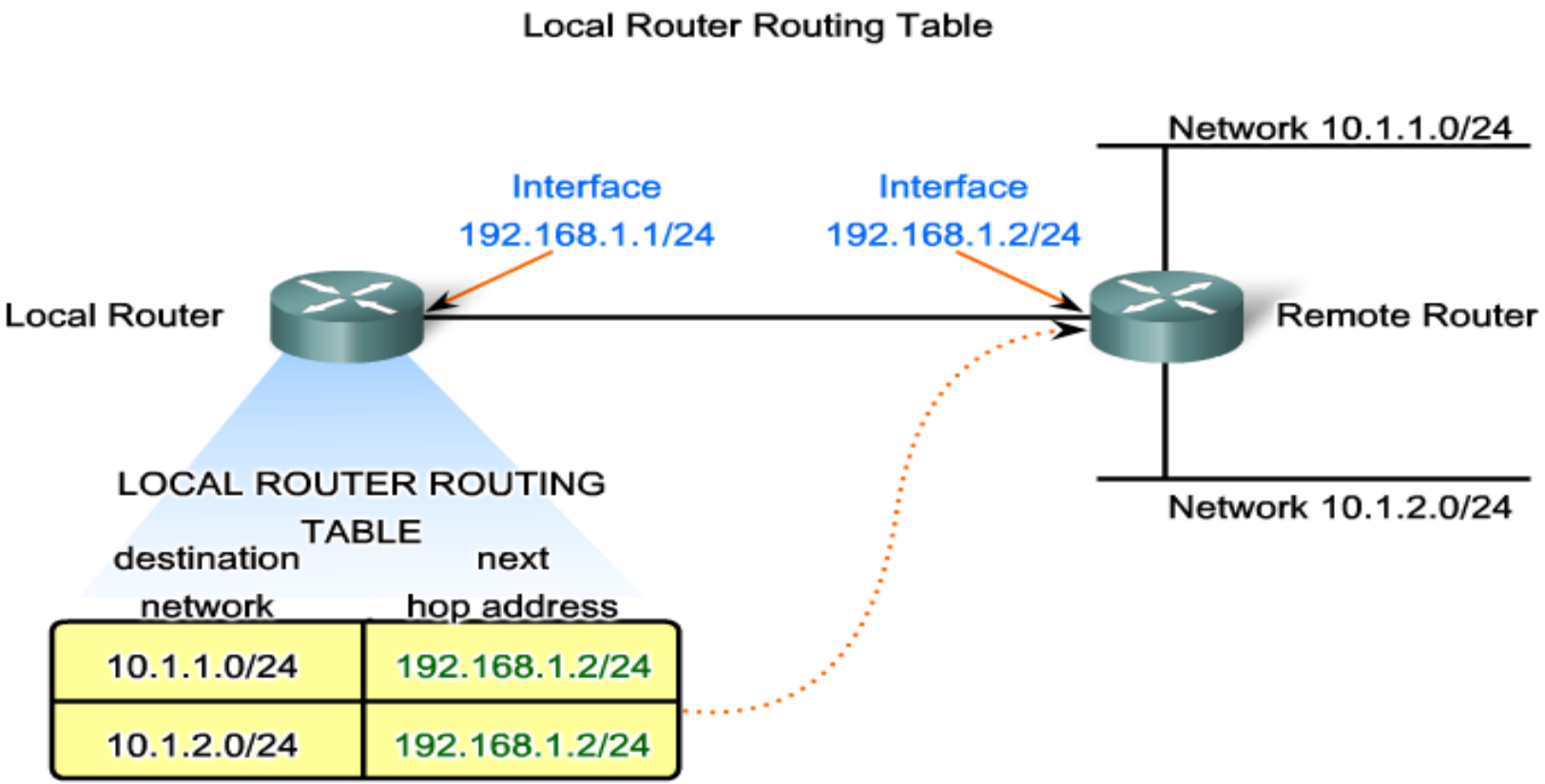
Confirming the Gateway Settings

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
     ① IP Address. . . . . . . . . . . . : 192.168.1.2
     ② Subnet Mask . . . . . . . . . . . : 255.255.255.0
     ③ Default Gateway . . . . . . . . . : 192.168.1.254
```

Default gateway address for this host computer

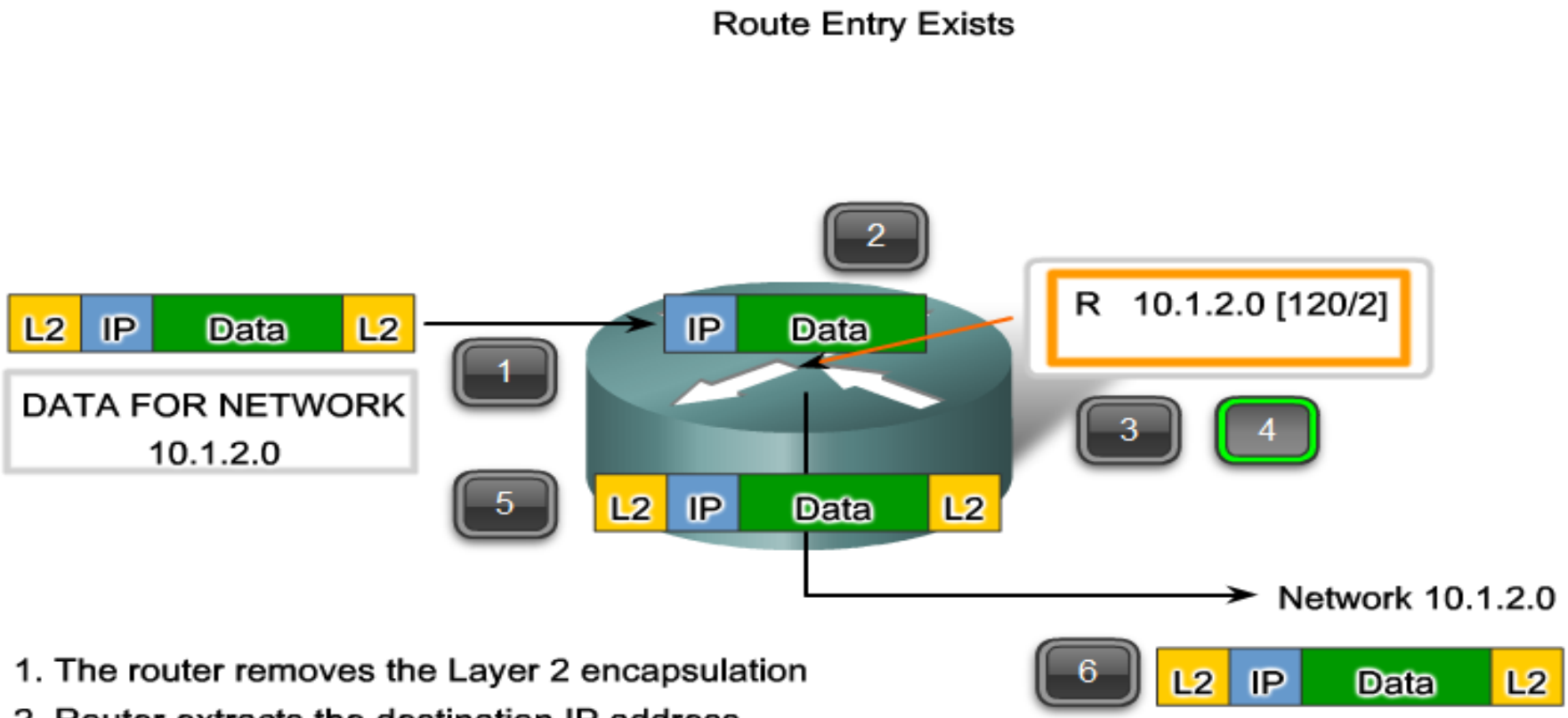
Sample ipconfig output showing default gateway address

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



The next hop for both networks 10.1.1.0/24 and 10.1.2.0/24 from Local Router is 192.168.1.2/24

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

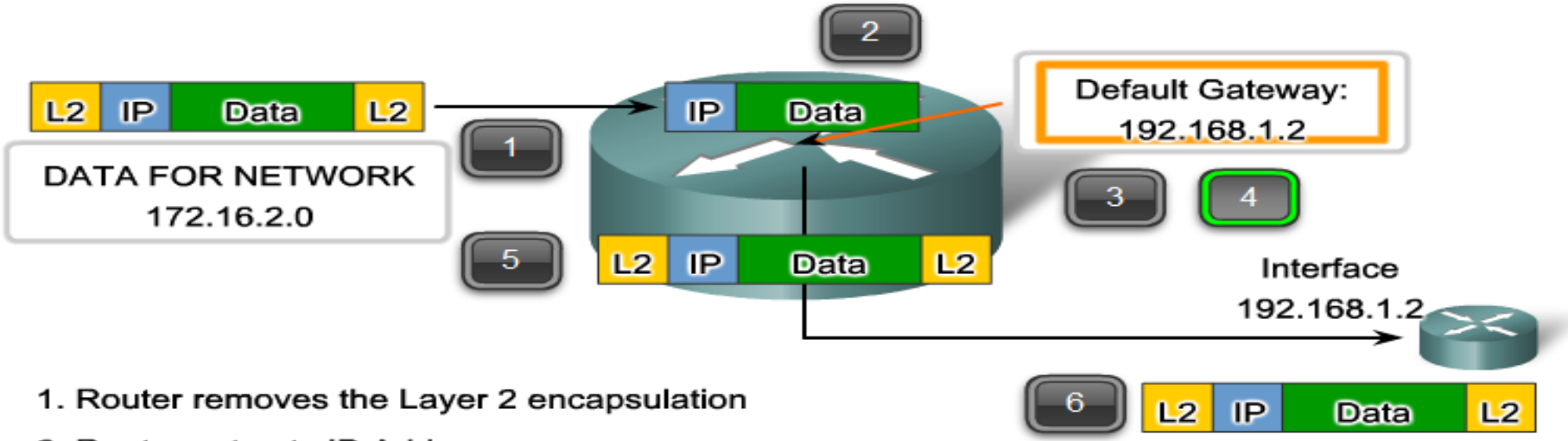


1. The router removes the Layer 2 encapsulation
2. Router extracts the destination IP address
3. Router checks the routing table for a match
4. Network 10.1.2.0 is found in the routing table
5. Router re-encapsulates the packet
6. Packet is sent to Network 10.1.2.0

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

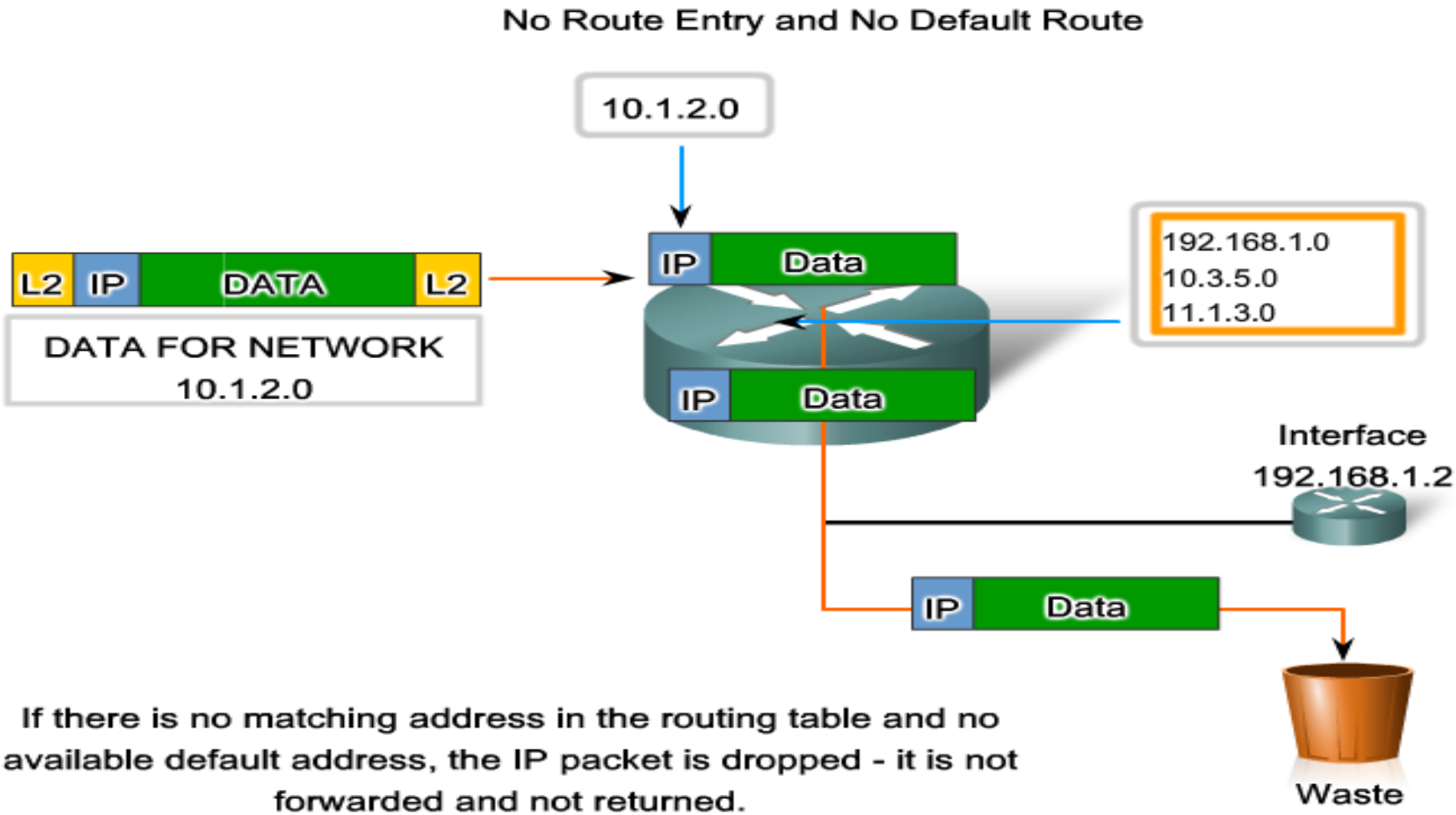
No Route Entry But Default Route Exists

Roll over to see the steps the router takes.

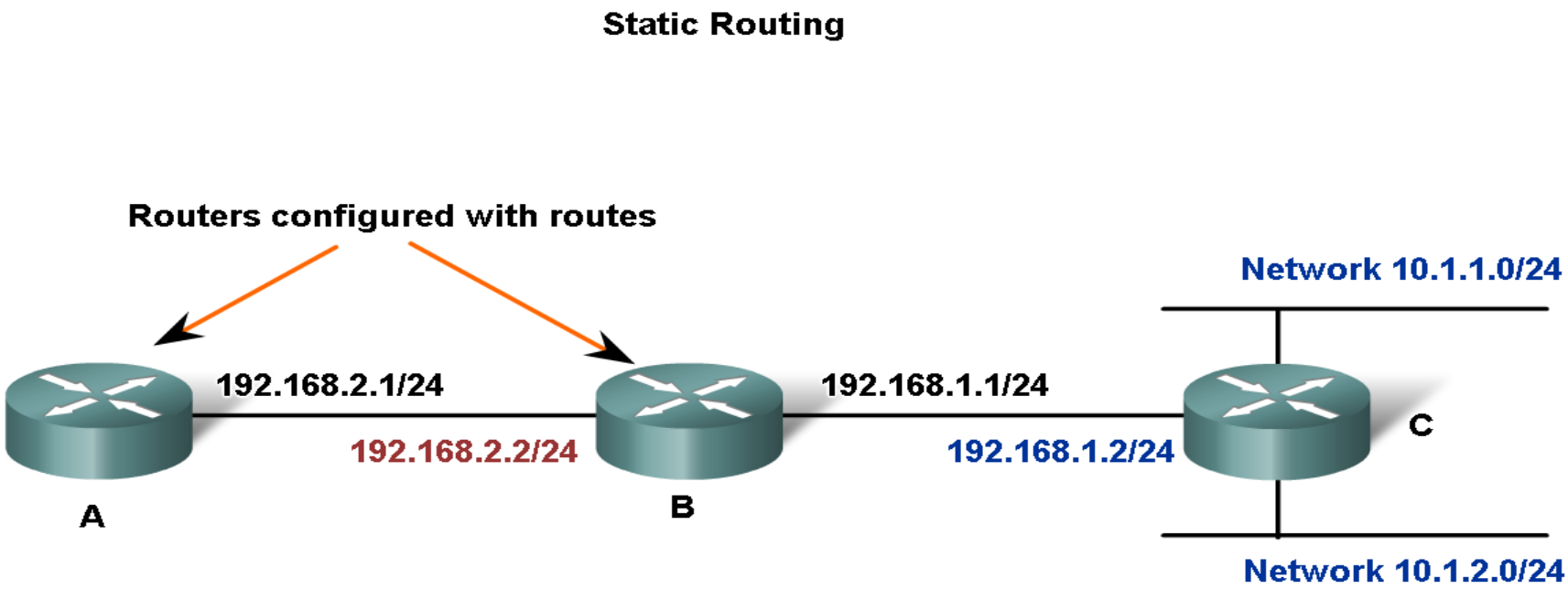


1. Router removes the Layer 2 encapsulation
2. Router extracts IP Address
3. Router checks the routing table for a match
4. Network 172.16.2.0 not in the routing table but default route to 192.168.1.2 exists
5. Router re-encapsulates the packet
6. Packet is sent to Interface 192.168.1.2

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



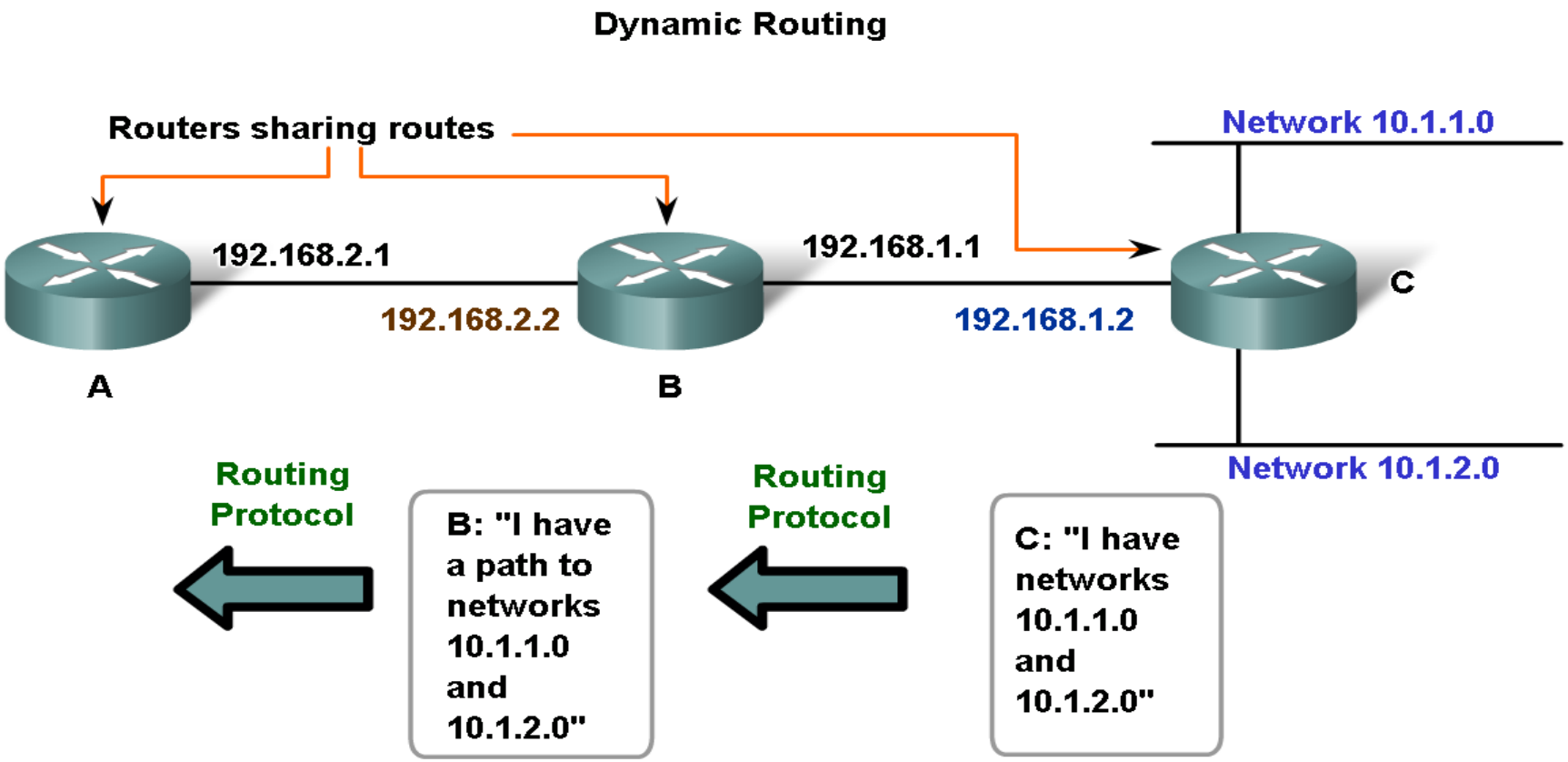
Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



Router A:
192.168.2.2/24
configured manually as next hop for networks 10.1.1.0/24 and 10.1.2.0/24

Router B:
192.168.1.2/24
configured manually as next hop for networks 10.1.1.0/24 and 10.1.2.0/24

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



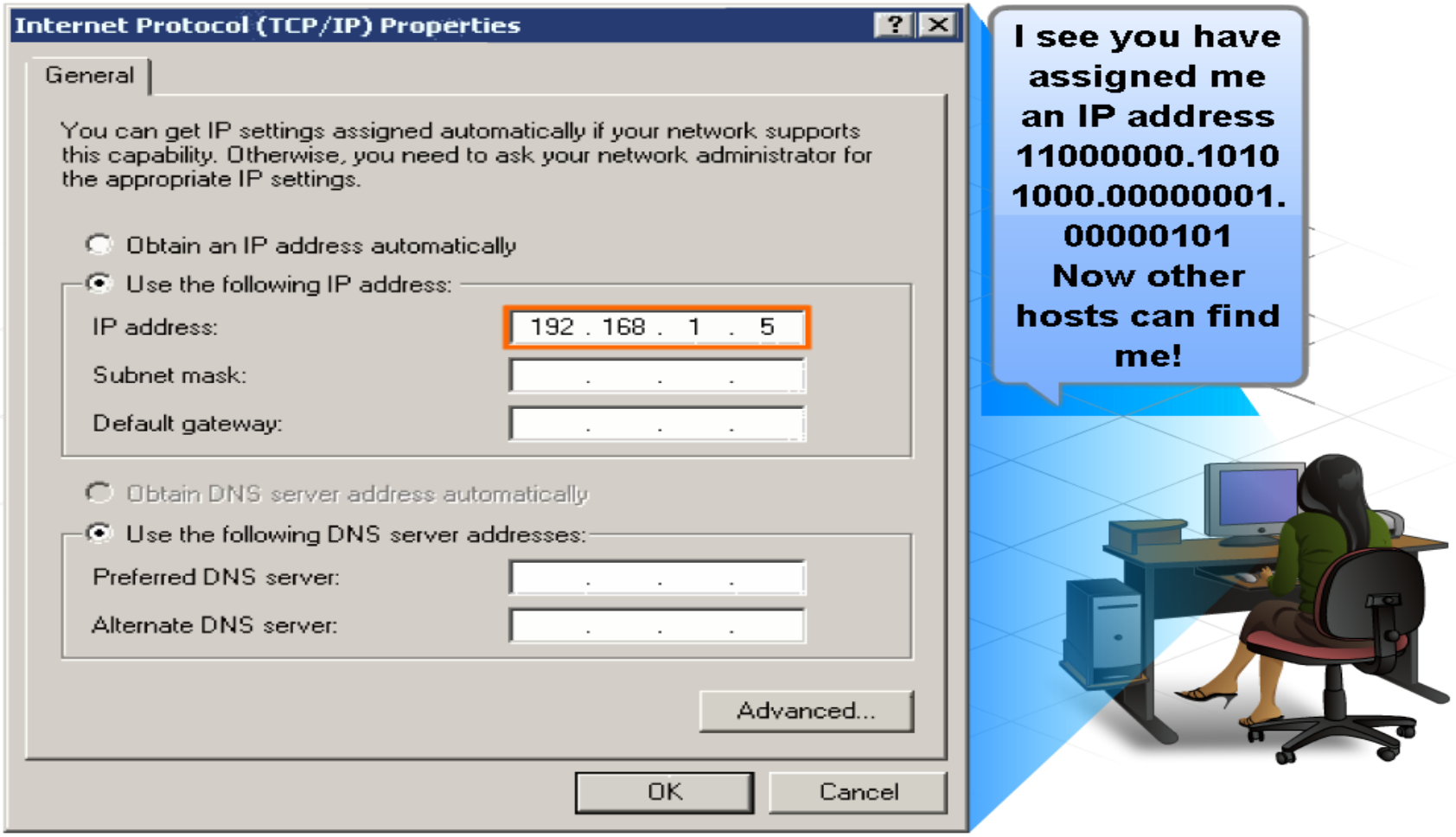
Router B learns about Router C's networks dynamically.
Router B's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.1.2 (Router C).
Router A learns about Router C's networks dynamically from Router B.
Router A's next hop to 10.1.1.0 and 10.1.2.0 is 192.168.2.2 (Router B).

Addressing the Network – IPv4

Objectives

- Explain the structure IP addressing and demonstrate the ability to convert between 8-bit binary and decimal numbers.
- Given an IPv4 address, classify by type and describe how it is used in the network
- Explain how addresses are assigned to networks by ISPs and within networks by administrators
- Determine the network portion of the host address and explain the role of the subnet mask in dividing networks.
- Given IPv4 addressing information and design criteria, calculate the appropriate addressing components.
- Use common testing utilities to verify and test network connectivity and operational status of the IP protocol stack on a host.

IP Addressing Structure



IP version 4 (IPv4) is the current form of addressing used on the Internet.

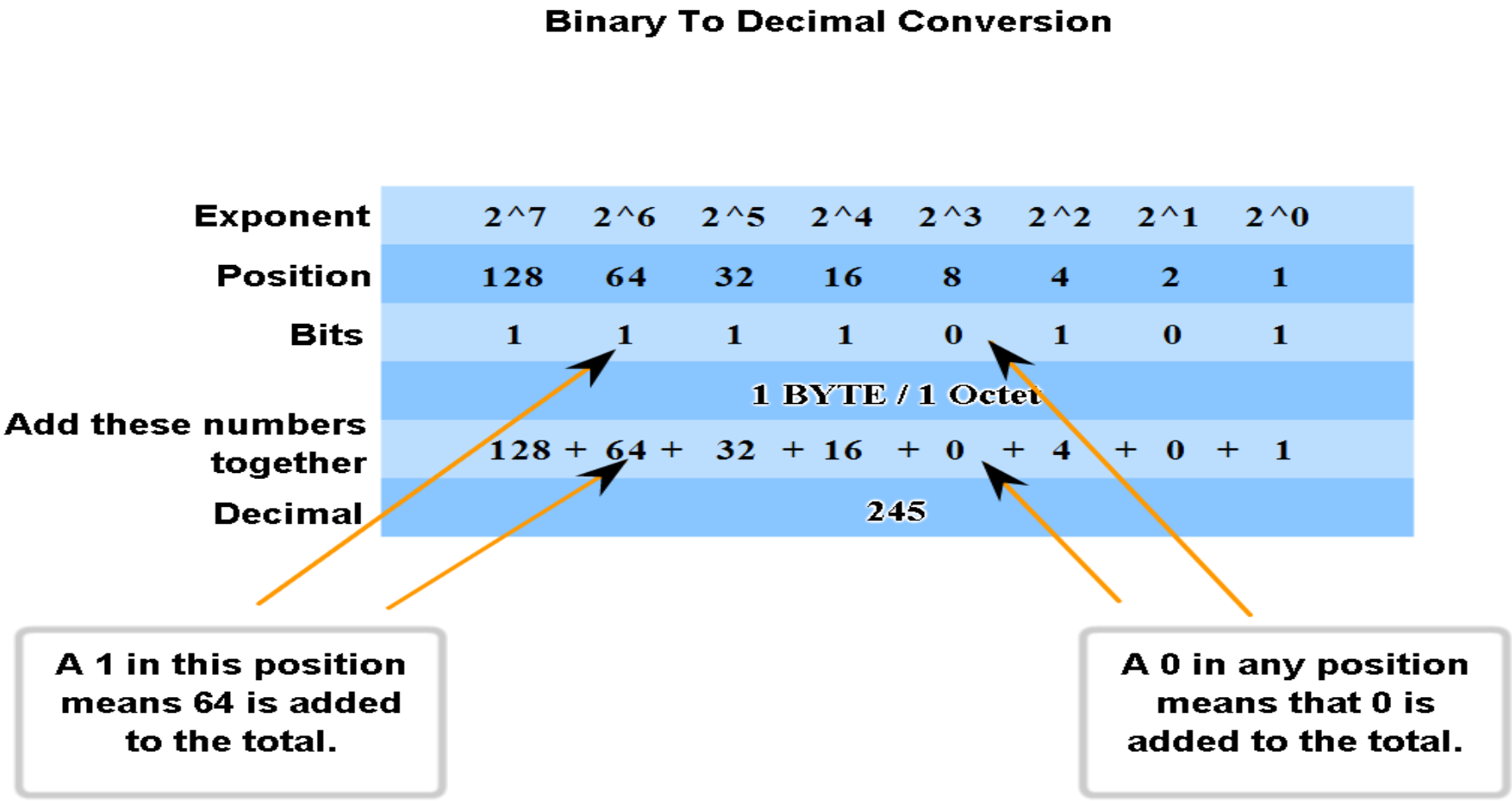
IP Addressing Structure

IPv4 Addresses

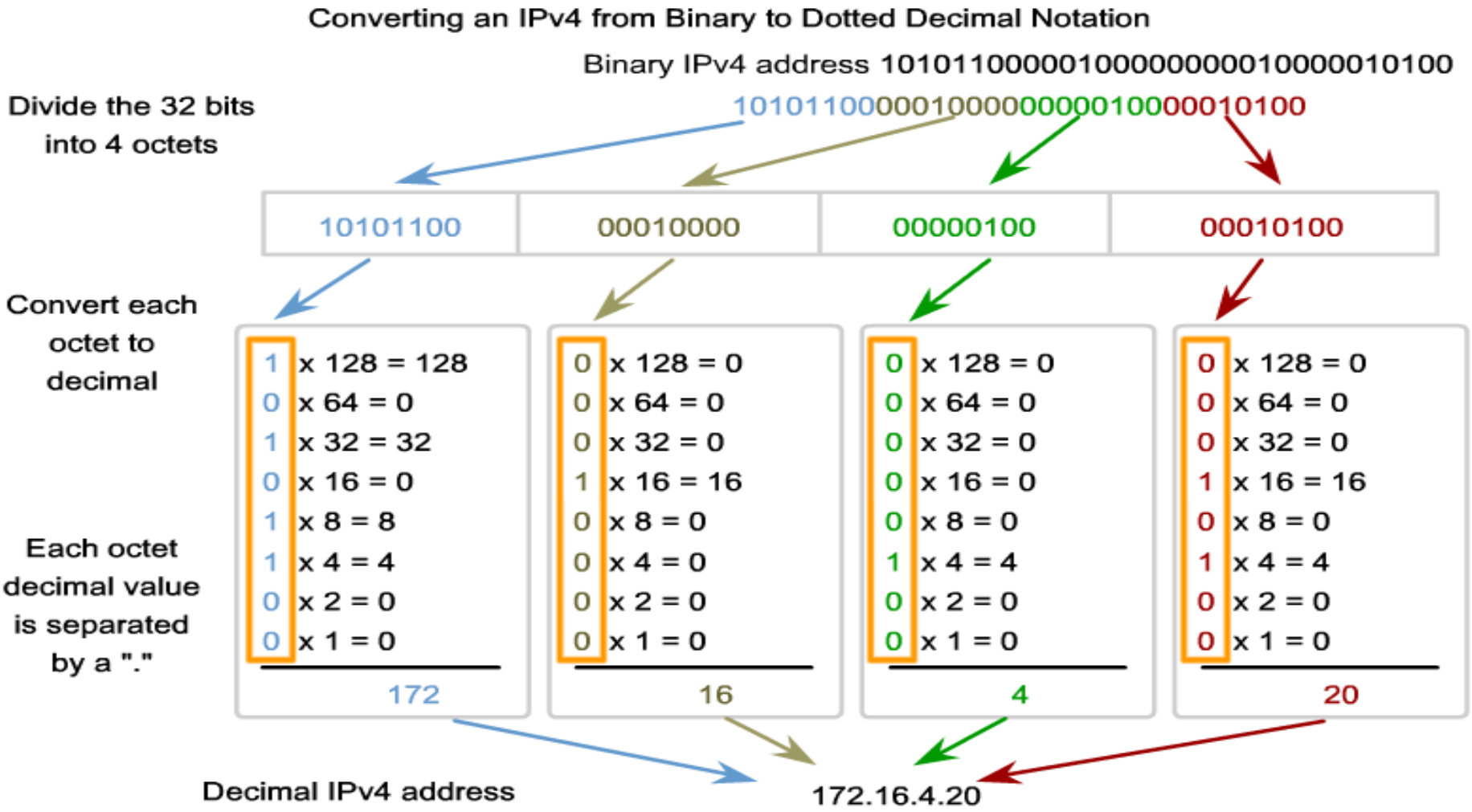
192	.	168	.	10	.	1	
11000000		11000000		11000000		11000000	

The computer using this IP address is on network 192.168.10.0.

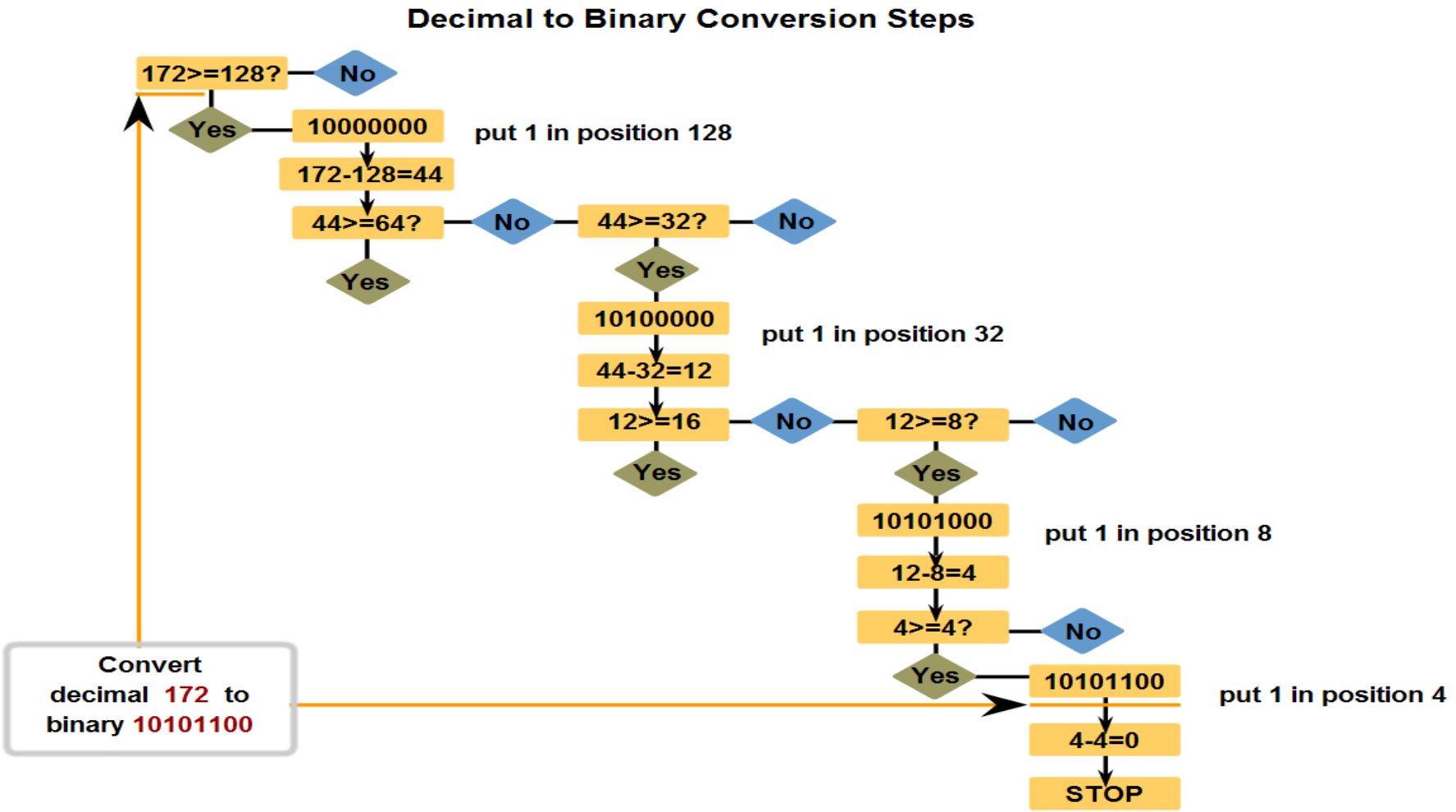
Binary & Decimal Numbering System



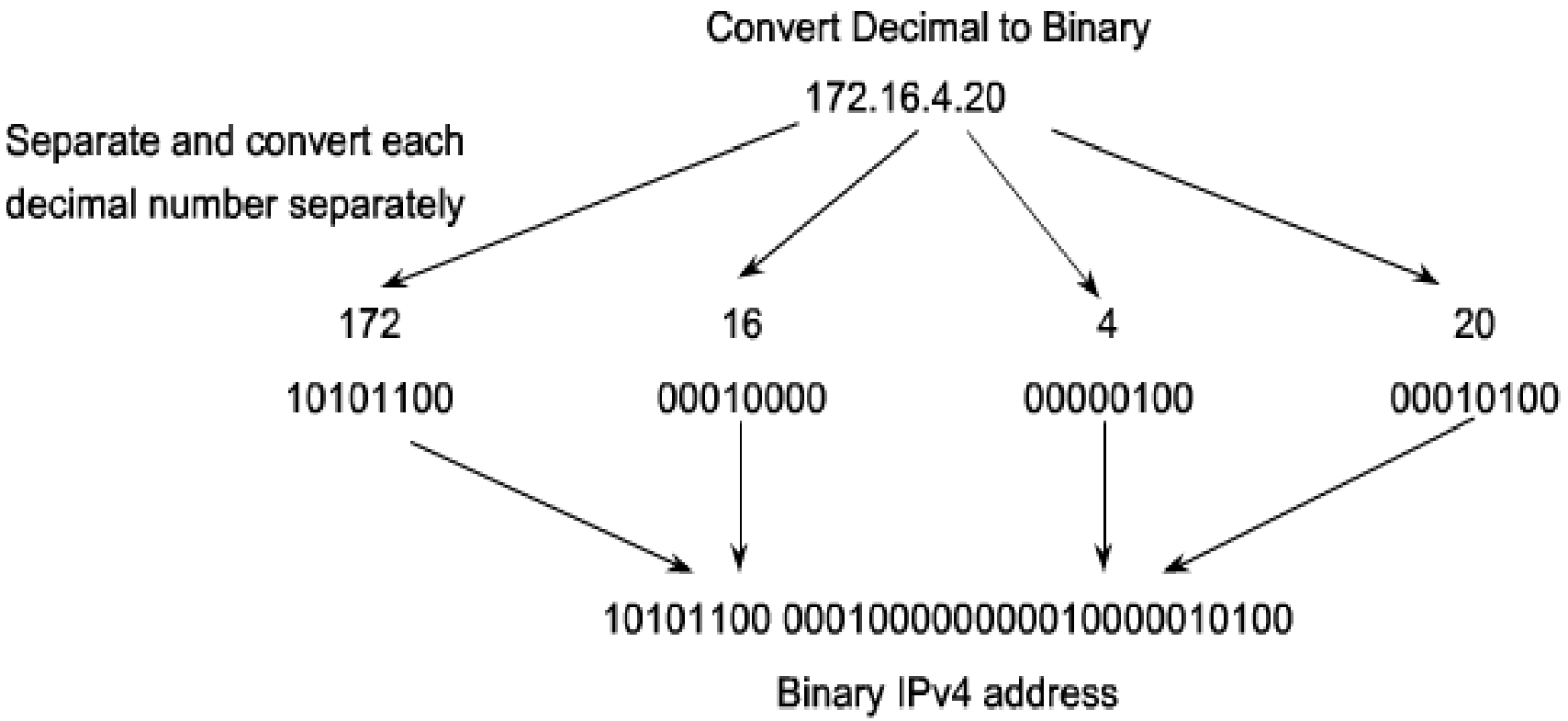
Binary & Decimal Numbering System



Binary & Decimal Numbering System



Binary & Decimal Numbering System



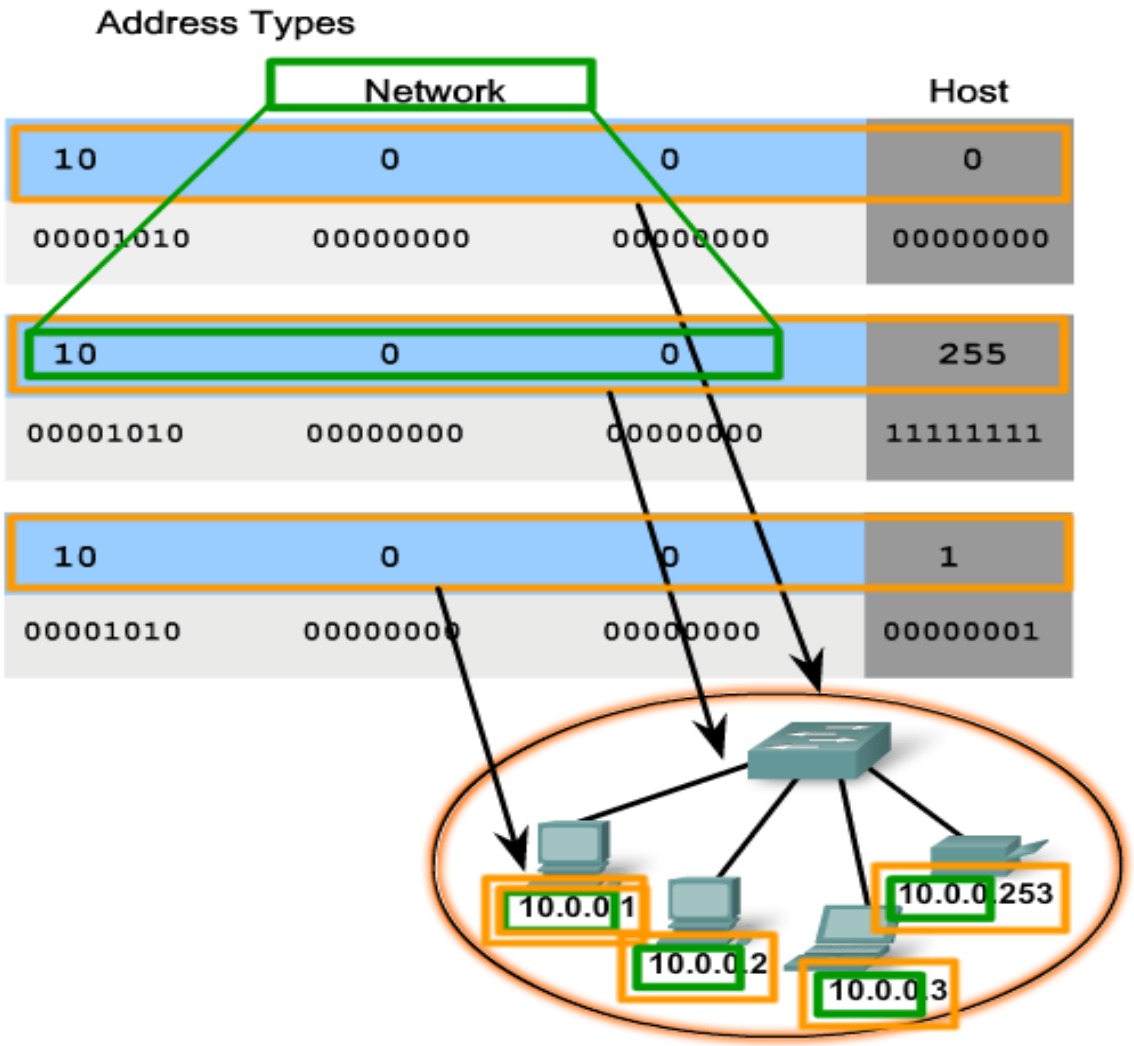
Classify and Define IPv4 Addresses

Network Address

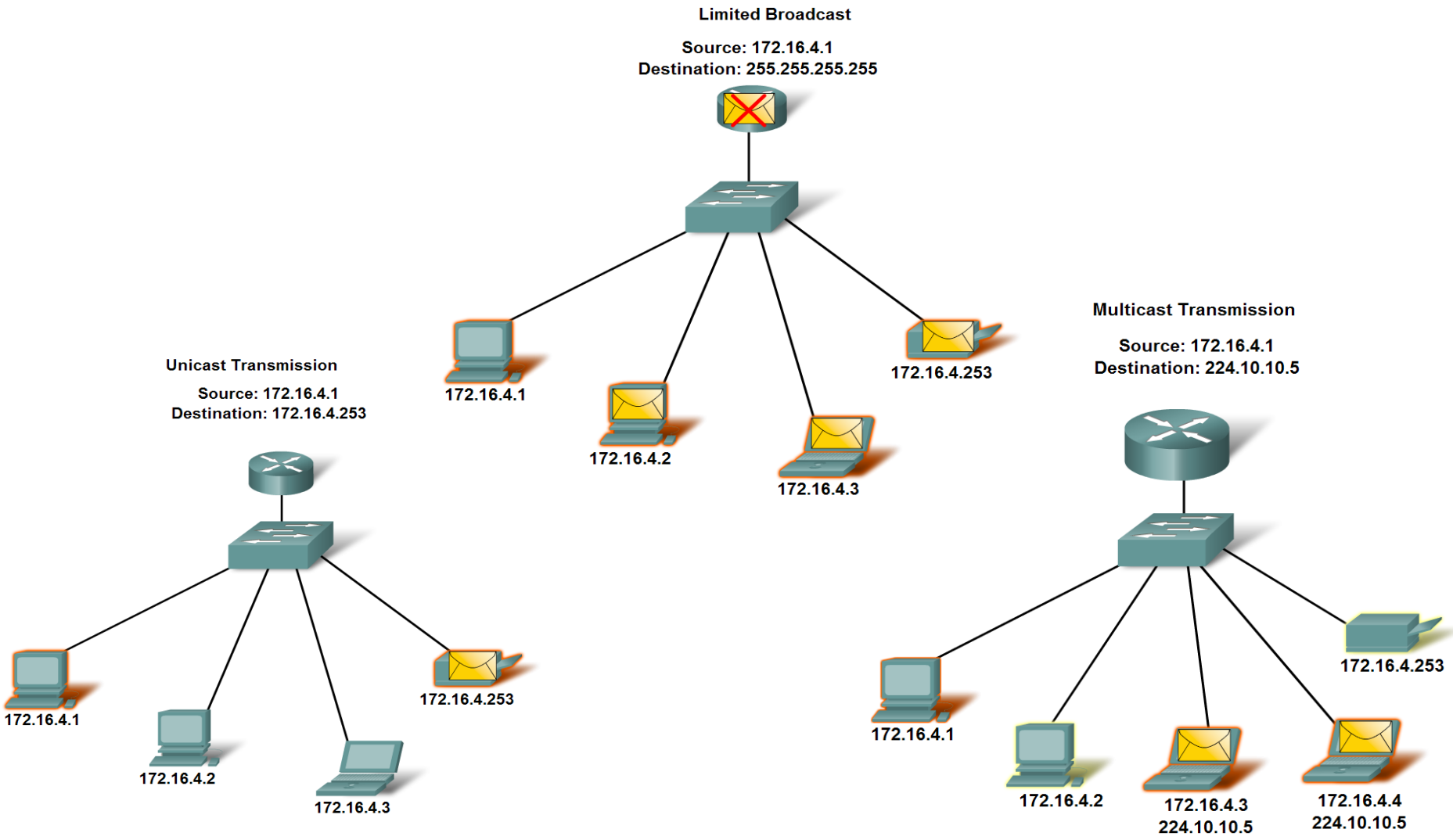
Broadcast Address

Host Address

Roll over to learn more.



Classify and Define IPv4 Addresses



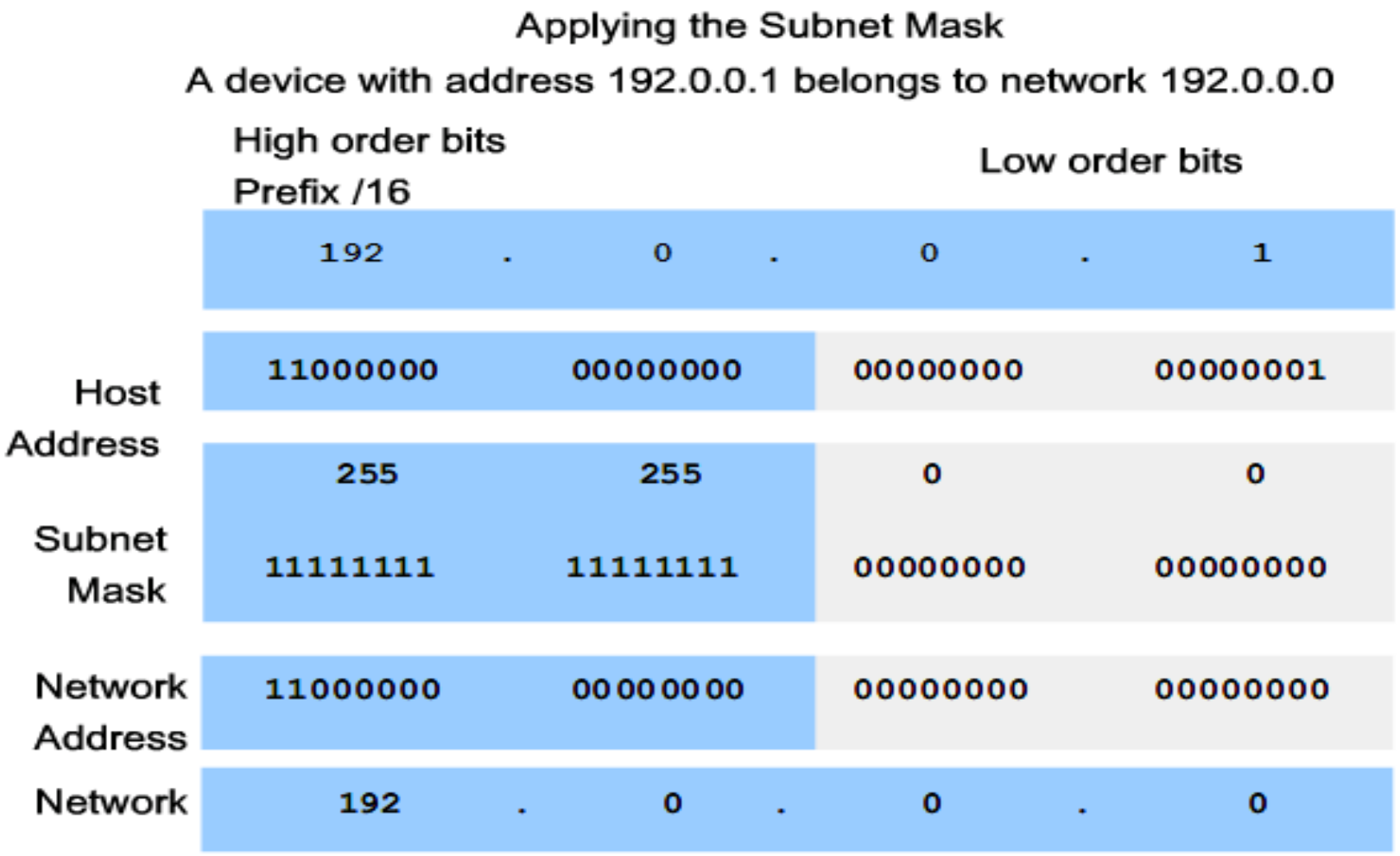
IP address Classes

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Subnet mask



Private Addresses

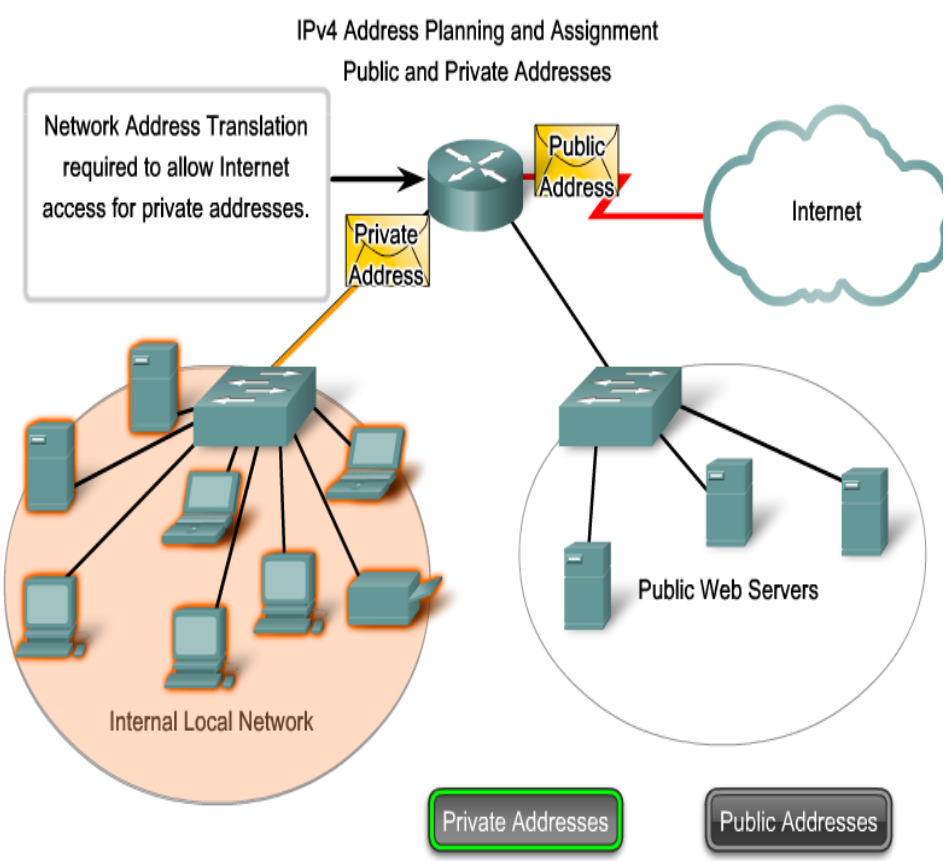
- These private IP addresses are for intra-network use only and can not be routed across the Internet.
- These private addresses are
  - Class A → 10.0.0.0/8 to 10.255.255.255/8
  - Class B → 172.16.0.0/16 to 172.31.255.255/16
  - Class C → 192.168.0.0/24 to 192.168.255.255/24

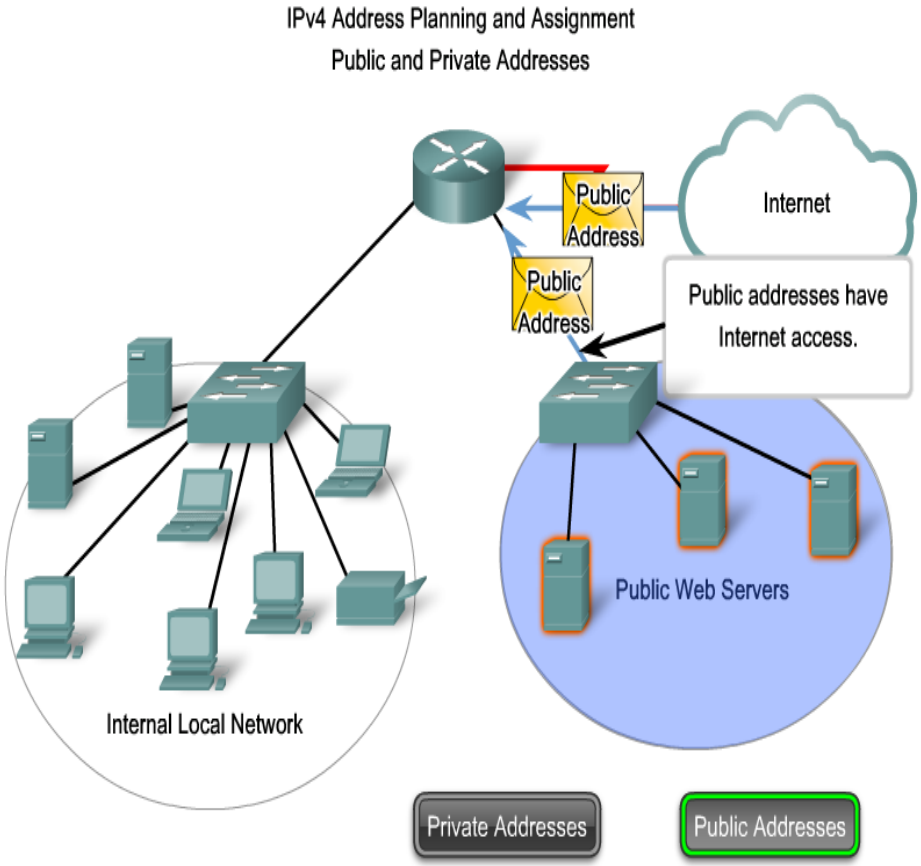
Private IP Addresses

Private IP addresses are another solution to the problem of the impending exhaustion of public IP addresses.As mentioned, public networks require hosts to have unique IP addresses.
However, private networks that are not connected to the Internet may use any host addresses, as long as each host within the private network is unique.

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Private IP Addresses





Classify and Define IPv4 Addresses