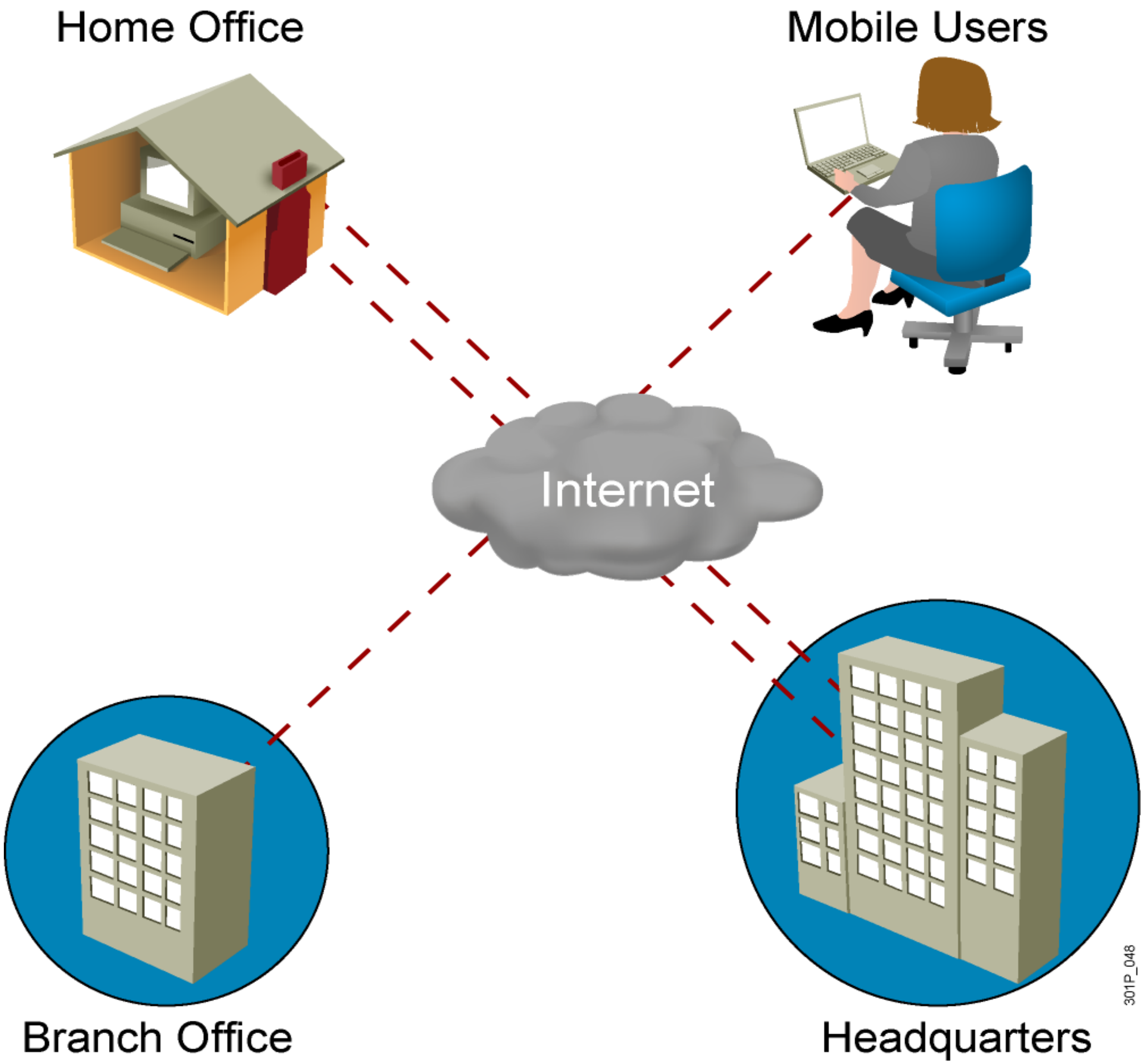
Chapter 1.

Networking fundamentals

Contents

1. What is a network?
2. Components of a network
3. Network topology
4. Types of networks
5. OSI & TCP/IP models
6. Data encapsulation & De-encapsulation
7. Packet delivery process

What is a network?



Some definitions

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through **cables, telephone lines, radio waves, satellites, or infrared light beams.**

https://fcit.usf.edu/network/chap1/chap1.htm

A computer network can be described as a system of interconnected devices that can communicate using some common standards (called **protocols**). These devices communicate to exchange resources (e.g. files and printers) and services.

https://study-ccna.com/what-is-a-network/

A **computer network**, or **data network**, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as WiFi.

https://en.wikipedia.org/wiki/Computer_network

Some definitions …

A network, in computing, is a group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections. The scale can range from a single PC sharing out basic peripherals to massive data centers located around the World, to the Internet itself. Regardless of scope, all networks allow computers and/or individuals to share information and resources.

Computer networks serve a number of purposes, some of which include:

- **Communications** such as email, instant messaging, chat rooms, etc.
- **Shared hardware** such as printers and input devices
- **Shared data and information** through the use of shared storage devices
- **Shared software**, which is achieved by running applications on remote computers

Nguồn: https://www.techopedia.com/definition/5537/network

Components of a network

There are three categories of network components:

- Devices
- Media
- Services

Devices

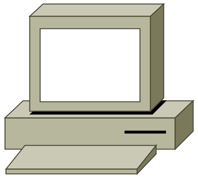
- **End devices**
  - Computers
  - Network printers
  - VoIP phones
  - Security camaras
  - Mobile handheld devices (such as smart phones, tablets,…)
- **Network infrastructure devices**
  - Network access devices (switches, wireless Access points)
  - Internetworking devices (routers)
  - Security devices (firewalls,…)

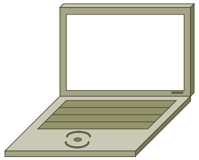
Network media

- Copper
- Fiber optic
- wireless

Network representations

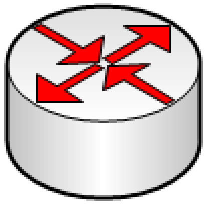
- End devices

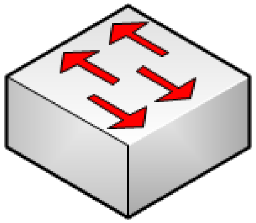

Computer


Laptop

IP phone

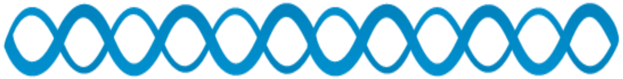
- Intermediary devices

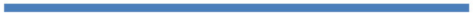

Router

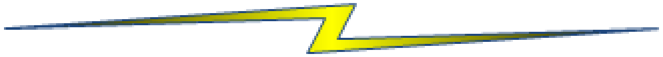

Switch

AP

- Network Media

Wireless


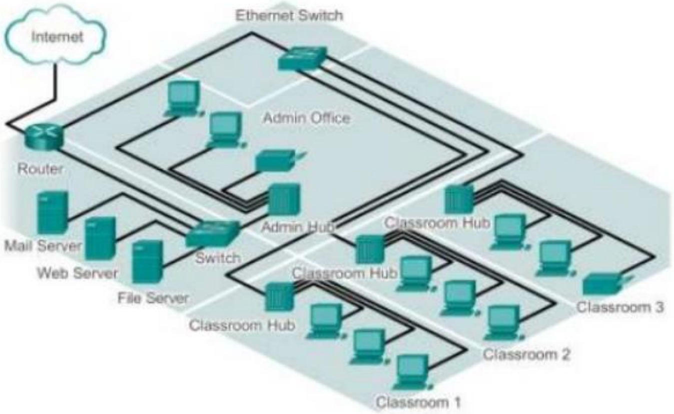
LAN


WAN


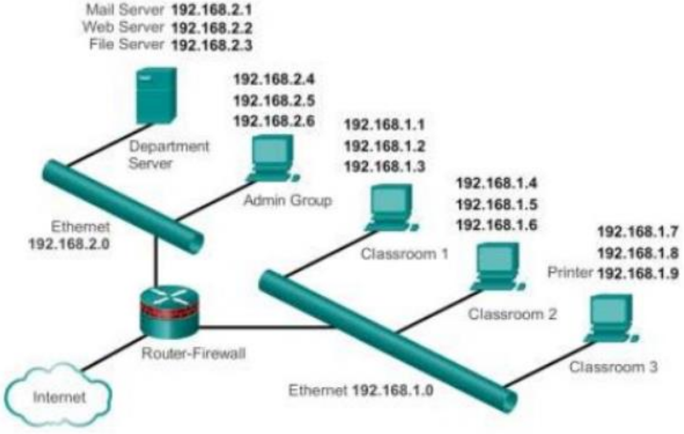
Network topology

- May also called “topology diagrams”

Physical Topology



Logical Topology



Types of networks

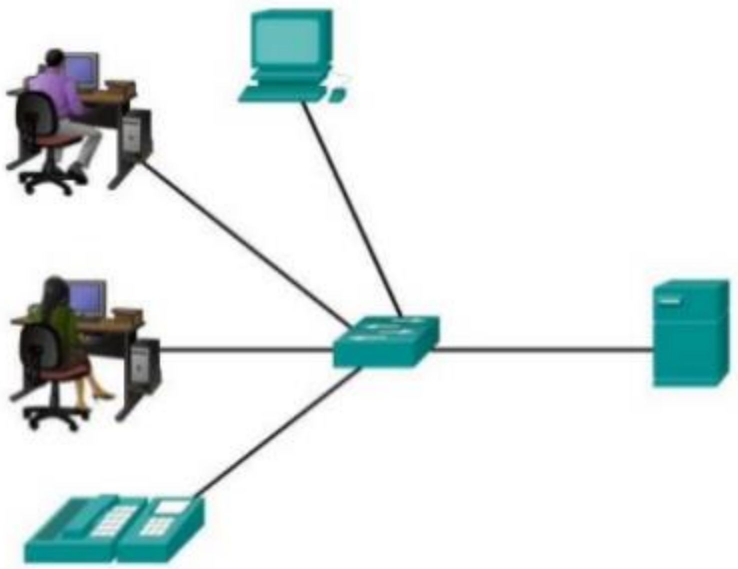
The two common types of network infrastructures are:

- Local Area Network (LAN)
- Wide Area Network (WAN)

Other types of networks include:

- Metropolitan Area Network (MAN)
- Wireless LAN (WLAN)
- Storage Area Network (SAN)

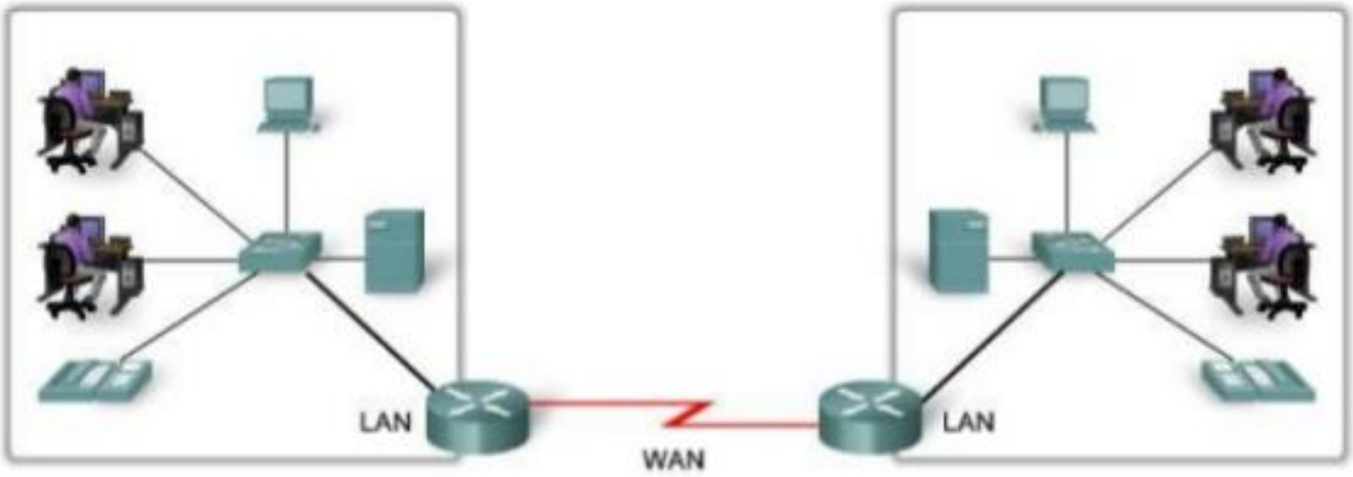
Local Area Network (LAN)



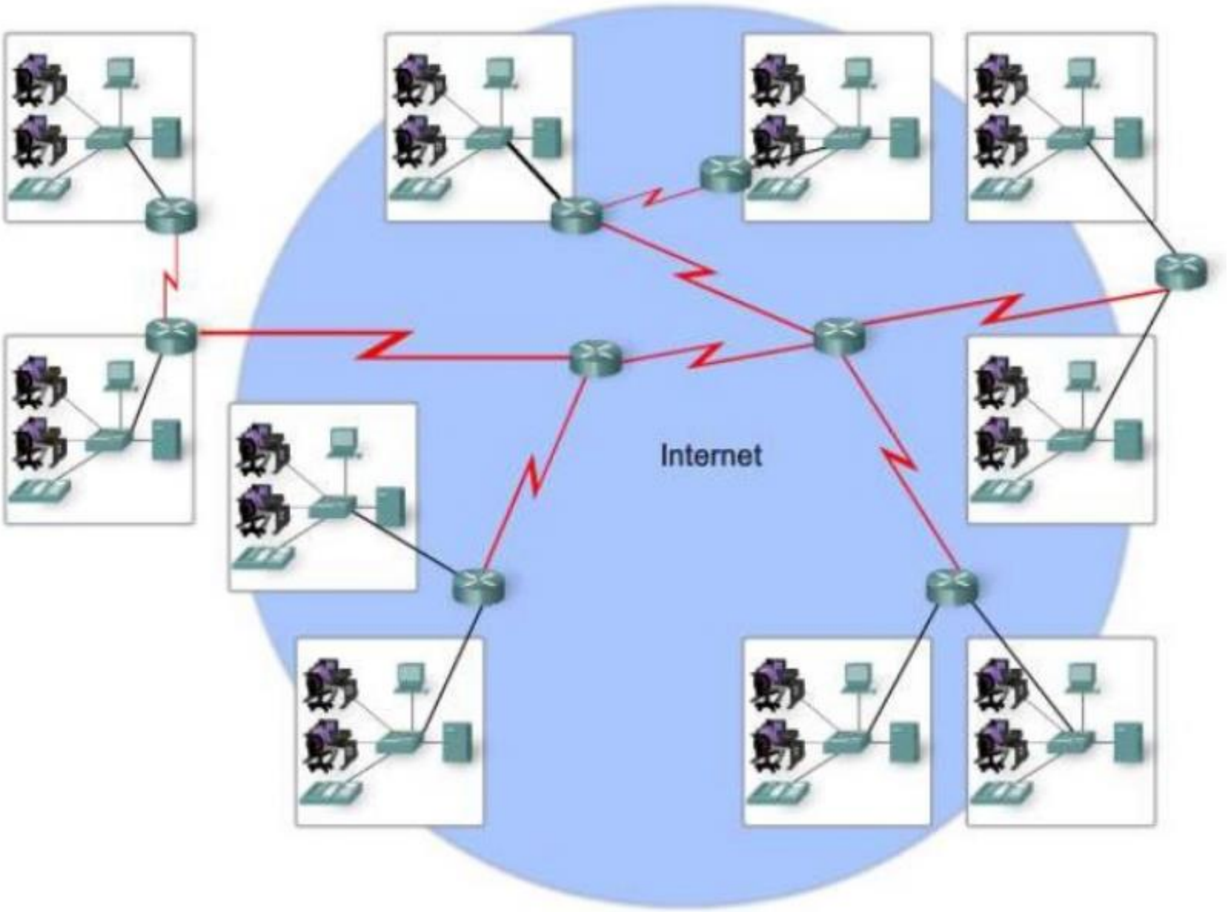
A network serving a home, building, or campus is considered a LAN

Wide Area Networks (WAN)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).

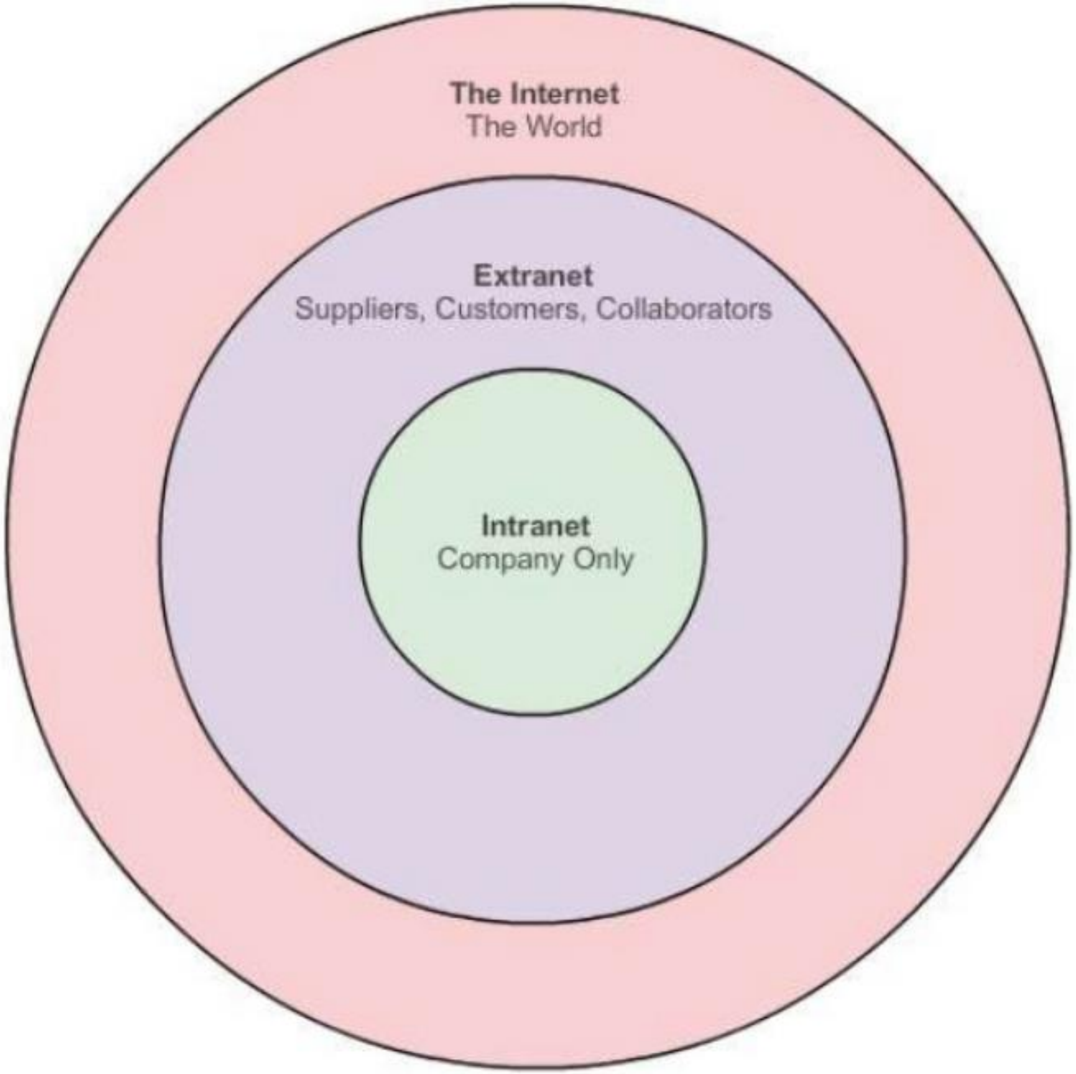


The Internet

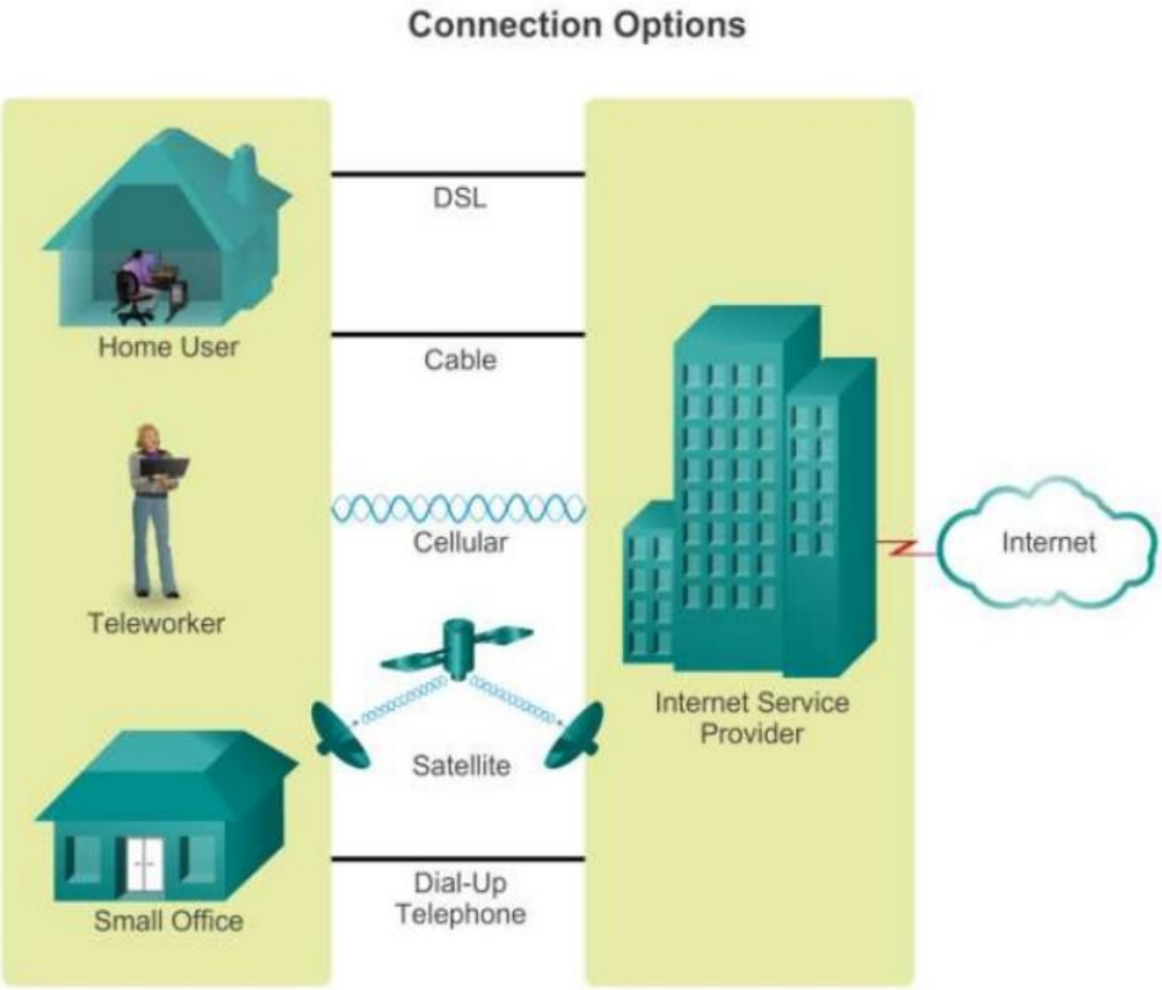


LANs and WANs may be connected into internetworks

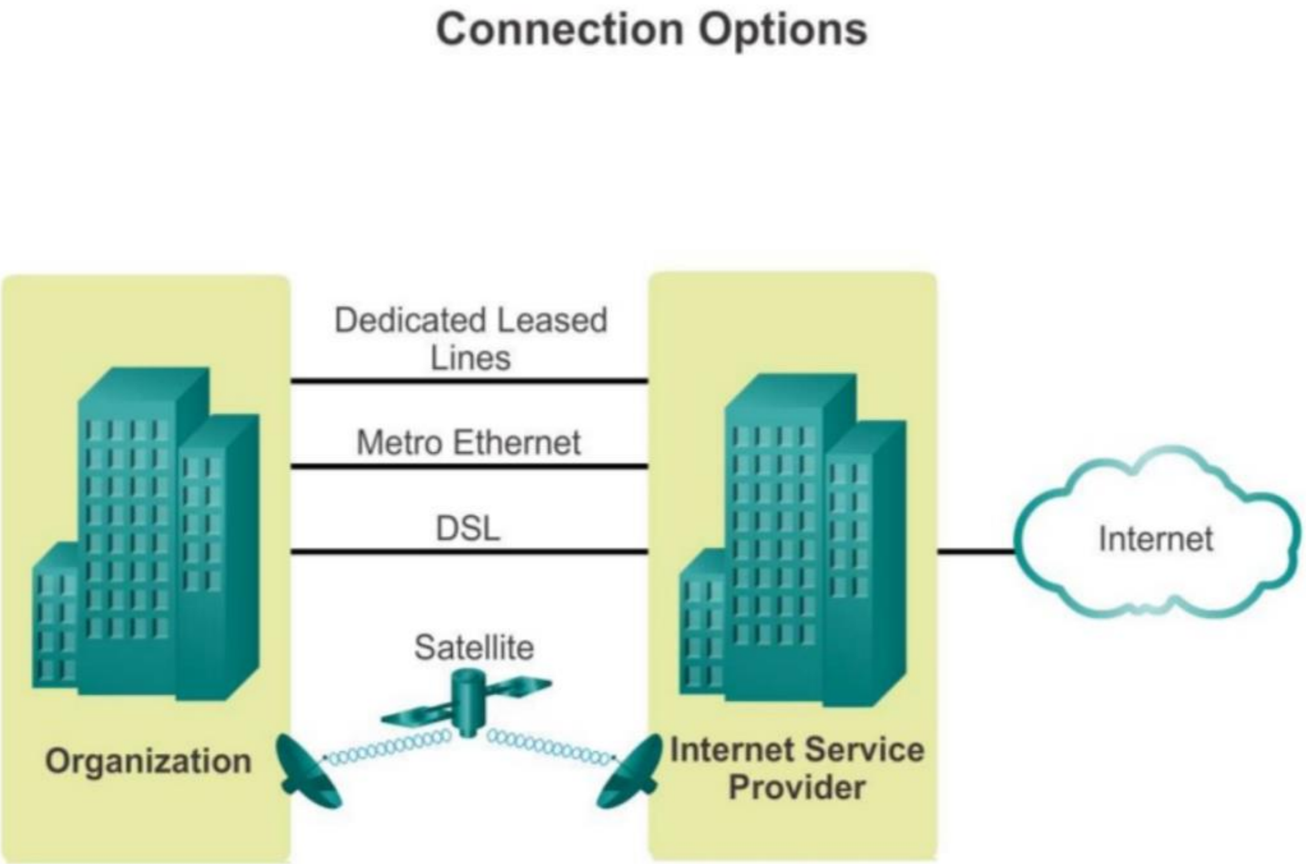
Intranet and Extranet



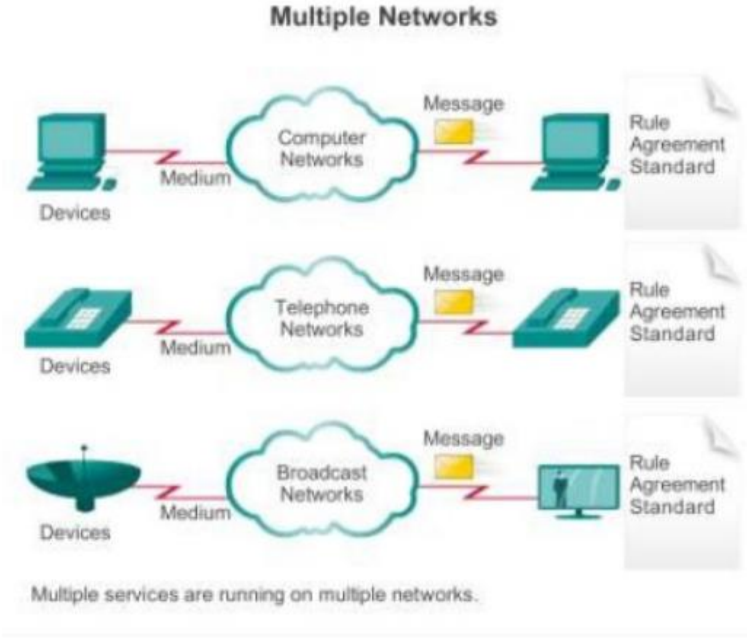
Connecting remote users to the Internet



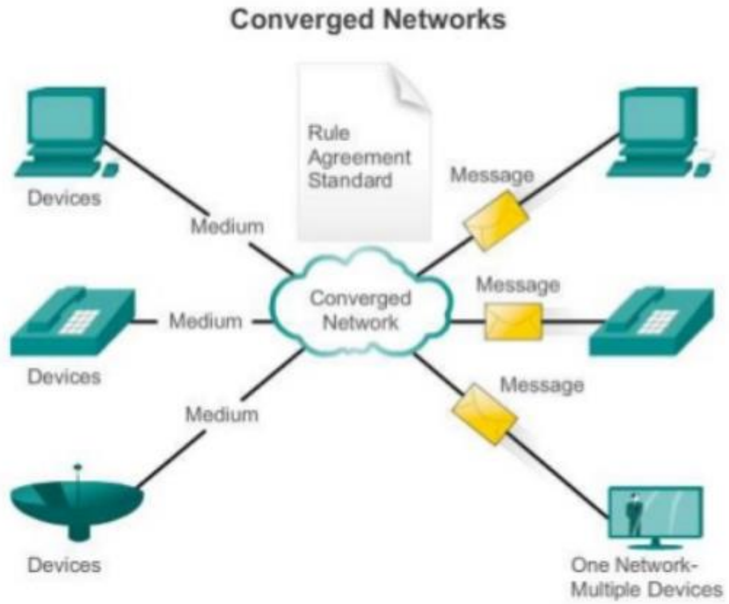
Connecting Businesses to the Internet



The converging network



Multiple services are running on multiple networks.



Converged data networks carry multiple services on one network.

Reliable network

- As networks evolve, we are discovering that there are four basic characteristics that underlying architectures need to address in order to meet user expectations:
  - Fault Tolerance
  - Scalability
  - Quality of service (QoS)
  - Security

Security Threats

- The common external threats to networks include:
  - Virueses, worms, and trojan horses
  - Spyware and adware
  - Zero-day attacks
  - Hacker attacks
  - Denial of service (DoS) attacks
  - Data interception and theft
  - Identity theft

Security solution

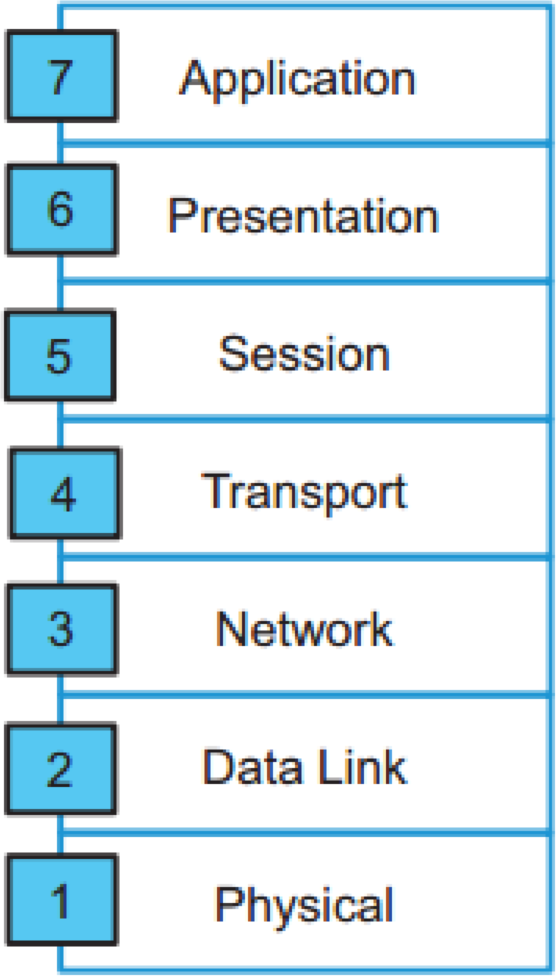
- Network security components often include:
  - Antivirus and antispyware
  - Firewall filtering
  - Access Control Lists (ACL)
  - Intrusion prevention systems (IPS)
  - Virtual Private Networks (VPN)

OSI & TCP/IP models

Two different types of host-to-host models:

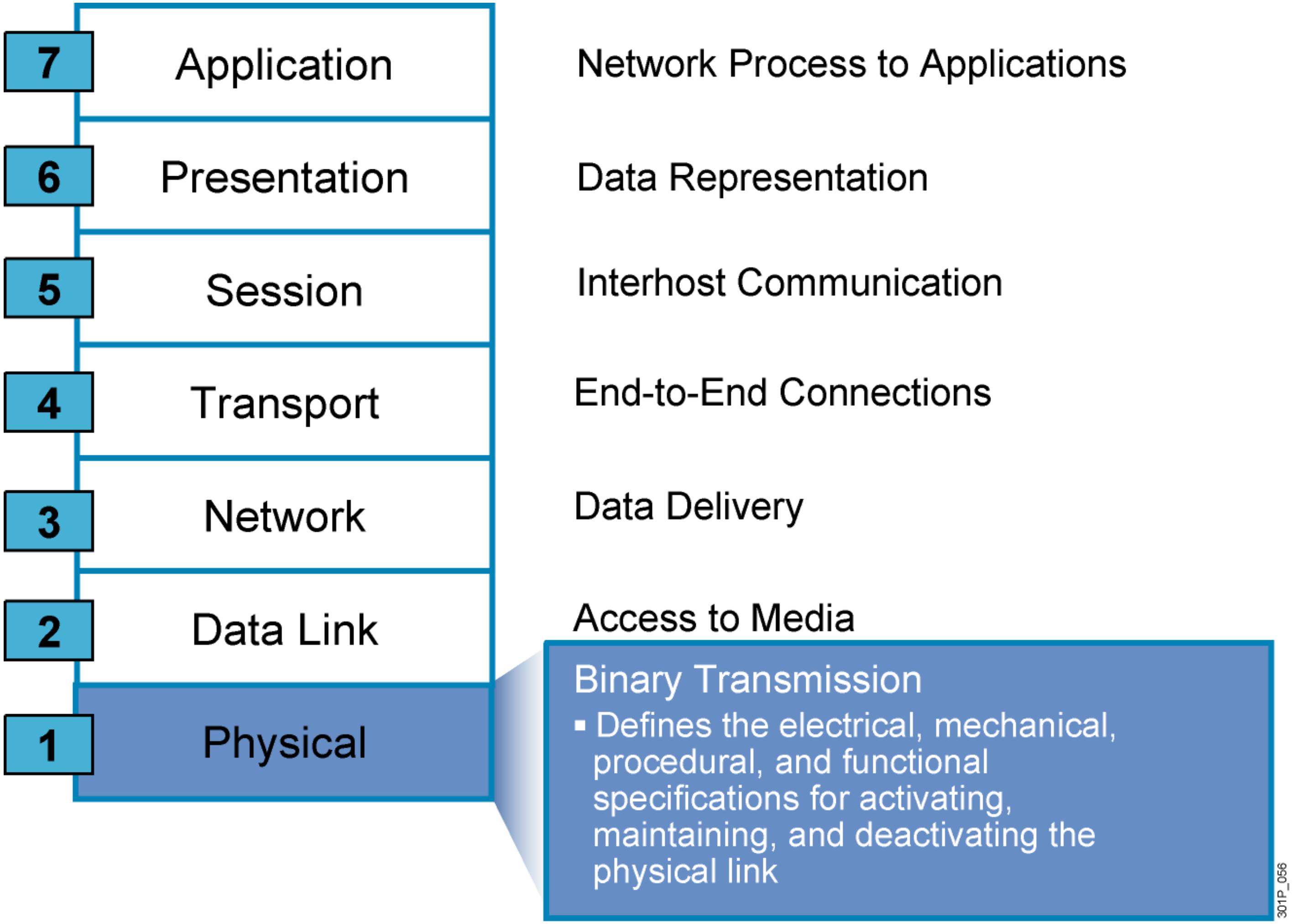
- **Older model**
  - Proprietary
  - Applications and combination of software controlled by one vendor.
- **Standards-based model**
  - Multivendor software
  - Leyered approach
  - Examples: OSI, TCP/IP

OSI Reference Model



7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

The Seven Layers of the OSI Model

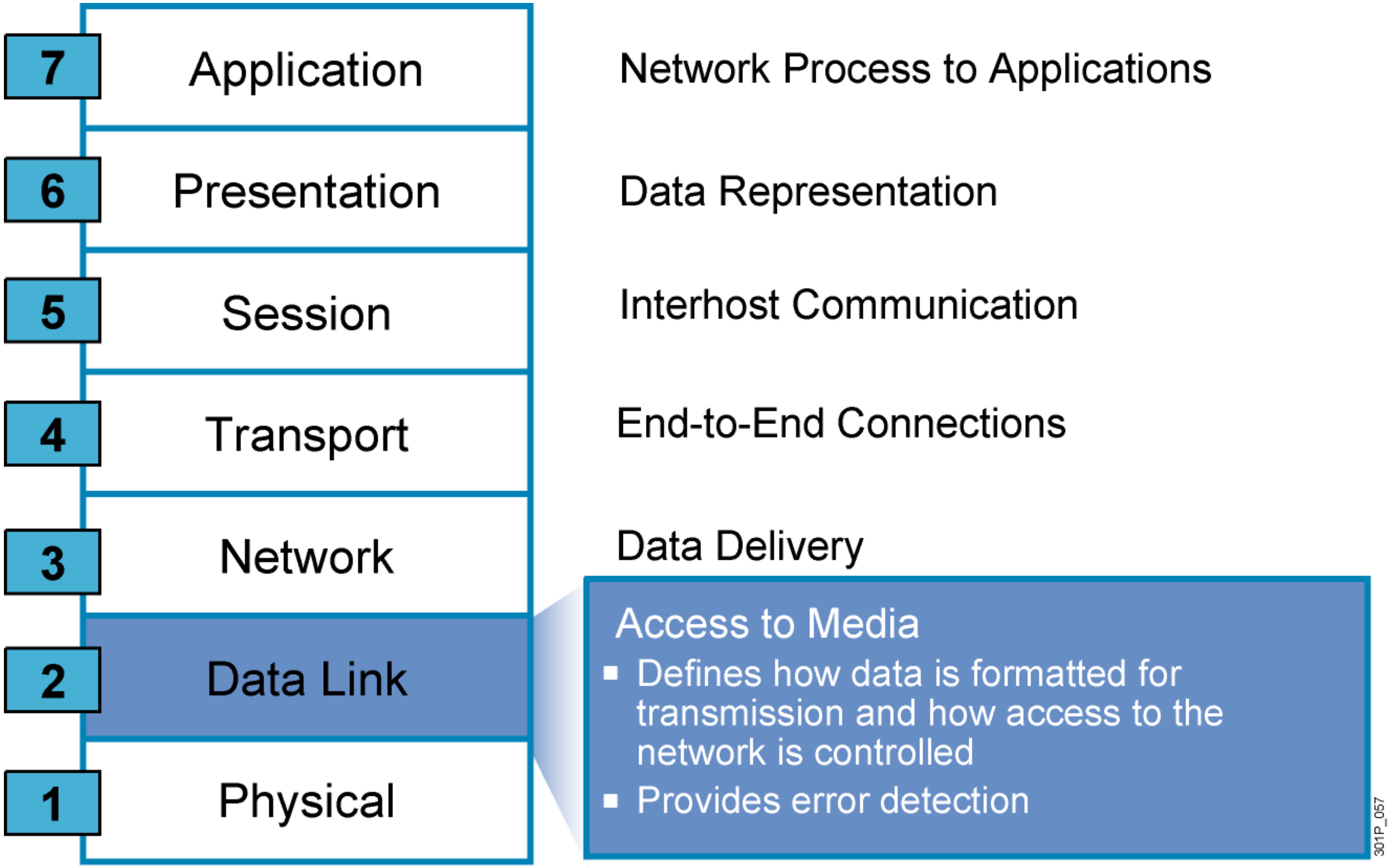


7	Application	Network Process to Applications
6	Presentation	Data Representation
5	Session	Interhost Communication
4	Transport	End-to-End Connections
3	Network	Data Delivery
2	Data Link	Access to Media
1	Physical	Binary Transmission

Binary Transmission

- Defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link

The Seven Layers of the OSI Model (Cont.)



7 Application — Network Process to Applications

6 Presentation — Data Representation

5 Session — Interhost Communication

4 Transport — End-to-End Connections

3 Network — Data Delivery

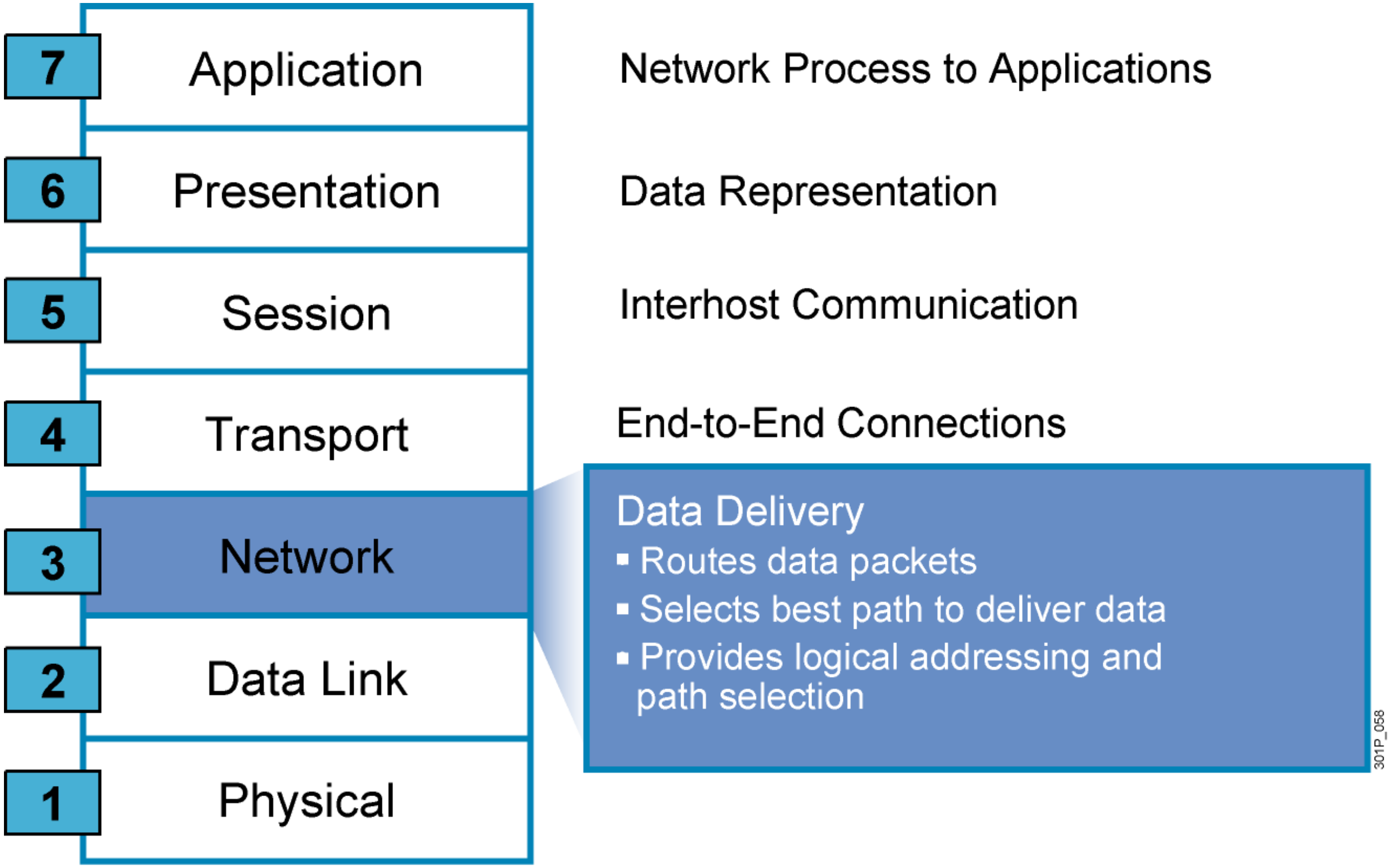
2 Data Link

1 Physical

Access to Media

- Defines how data is formatted for transmission and how access to the network is controlled
- Provides error detection

The Seven Layers of the OSI Model (Cont.)



Network Process to Applications

Data Representation

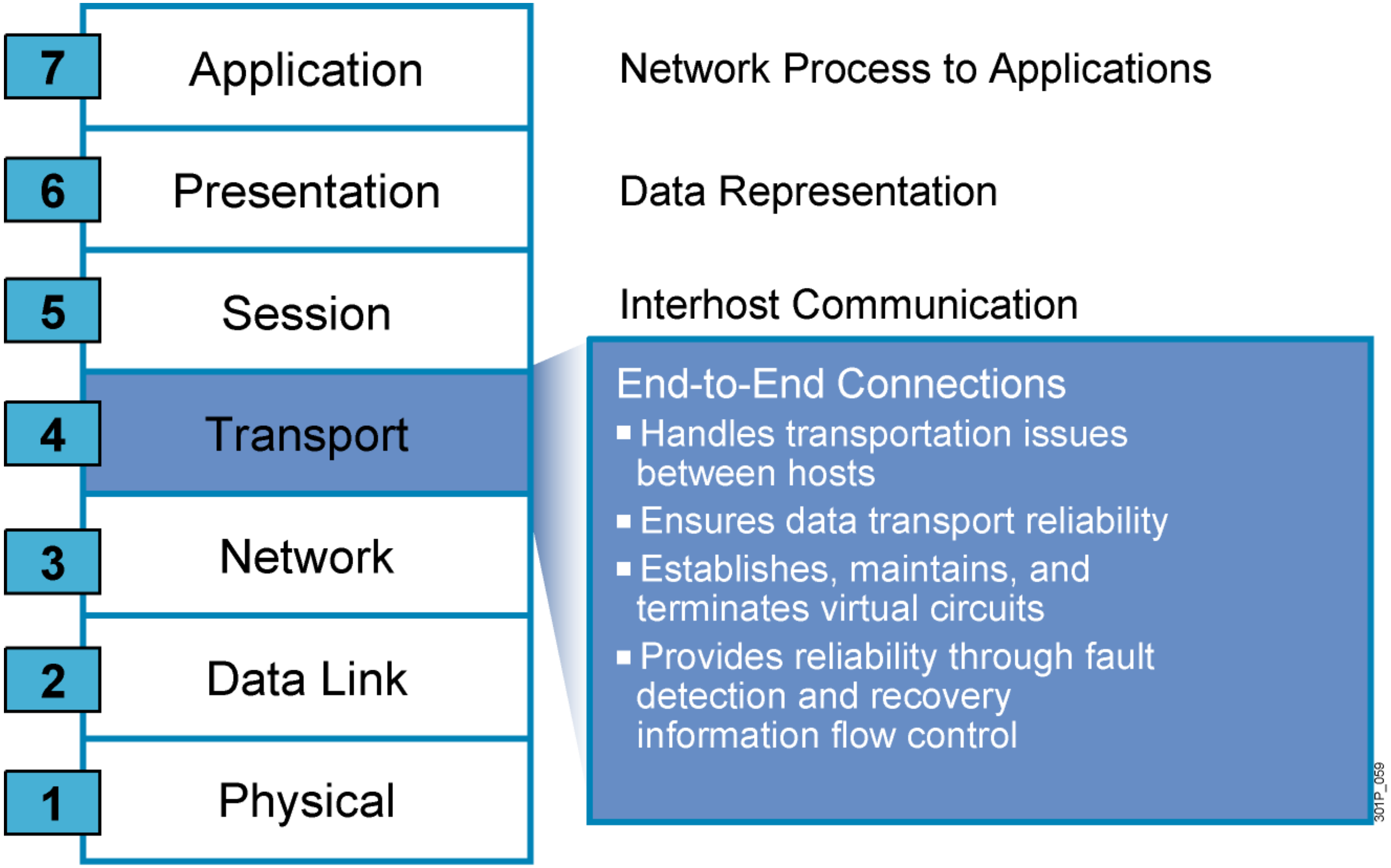
Interhost Communication

End-to-End Connections

Data Delivery

- Routes data packets
- Selects best path to deliver data
- Provides logical addressing and path selection

The Seven Layers of the OSI Model (Cont.)



7 Application — Network Process to Applications

6 Presentation — Data Representation

5 Session — Interhost Communication

4 Transport

3 Network

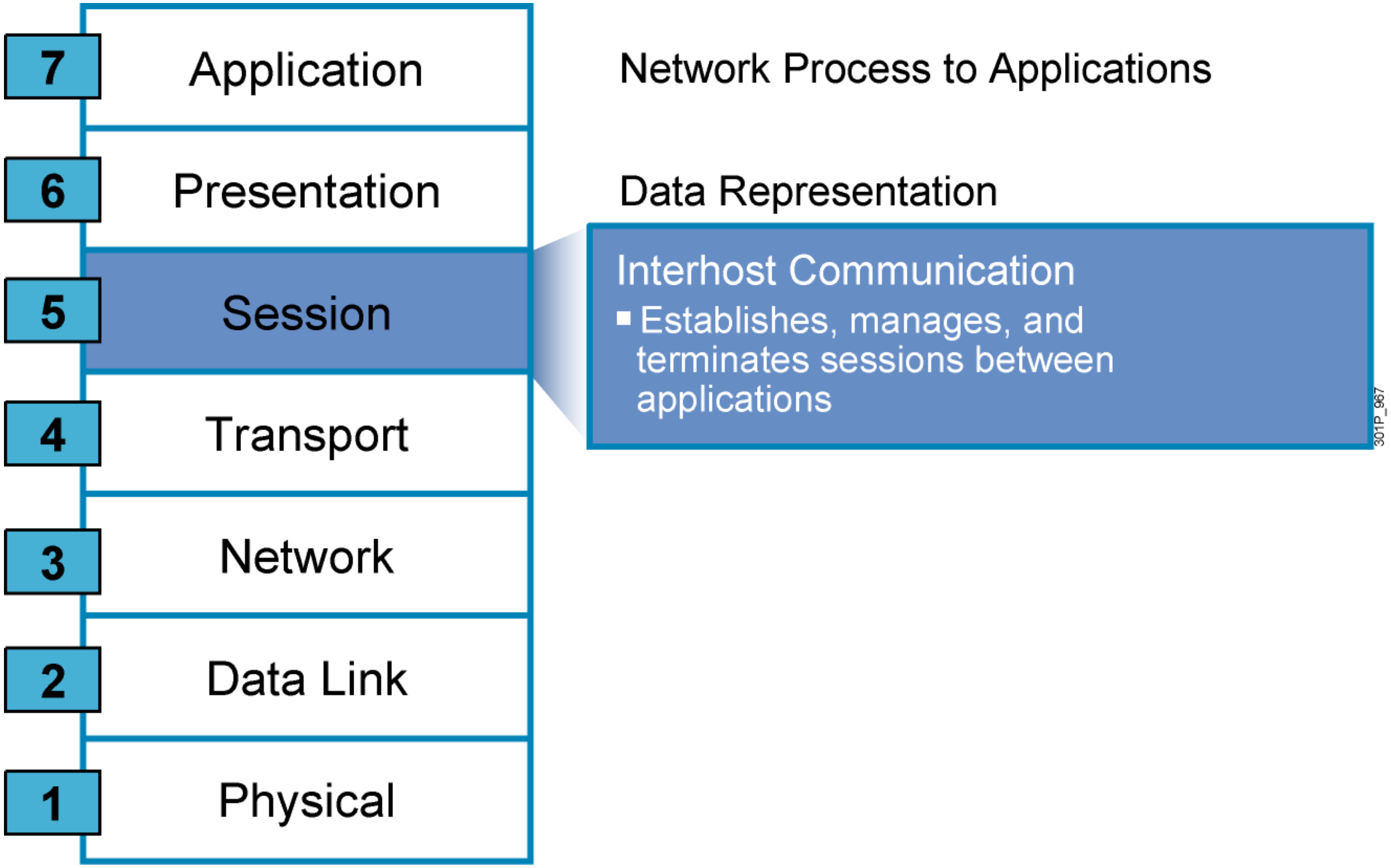
2 Data Link

1 Physical

End-to-End Connections

- Handles transportation issues between hosts
- Ensures data transport reliability
- Establishes, maintains, and terminates virtual circuits
- Provides reliability through fault detection and recovery information flow control

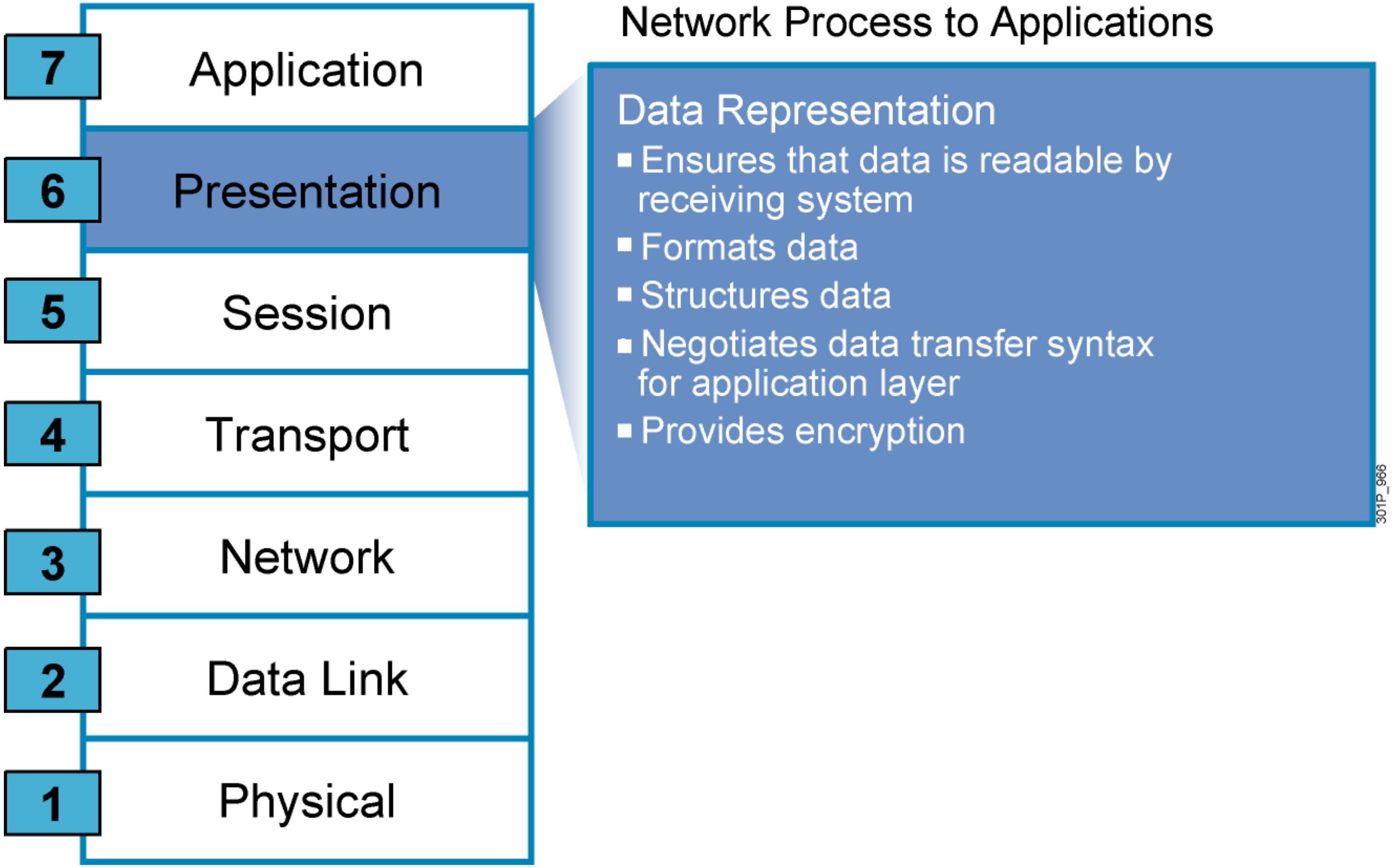
The Seven Layers of the OSI Model (Cont.)



Interhost Communication

- Establishes, manages, and terminates sessions between applications

The Seven Layers of the OSI Model (Cont.)



7 Application

6 Presentation

5 Session

4 Transport

3 Network

2 Data Link

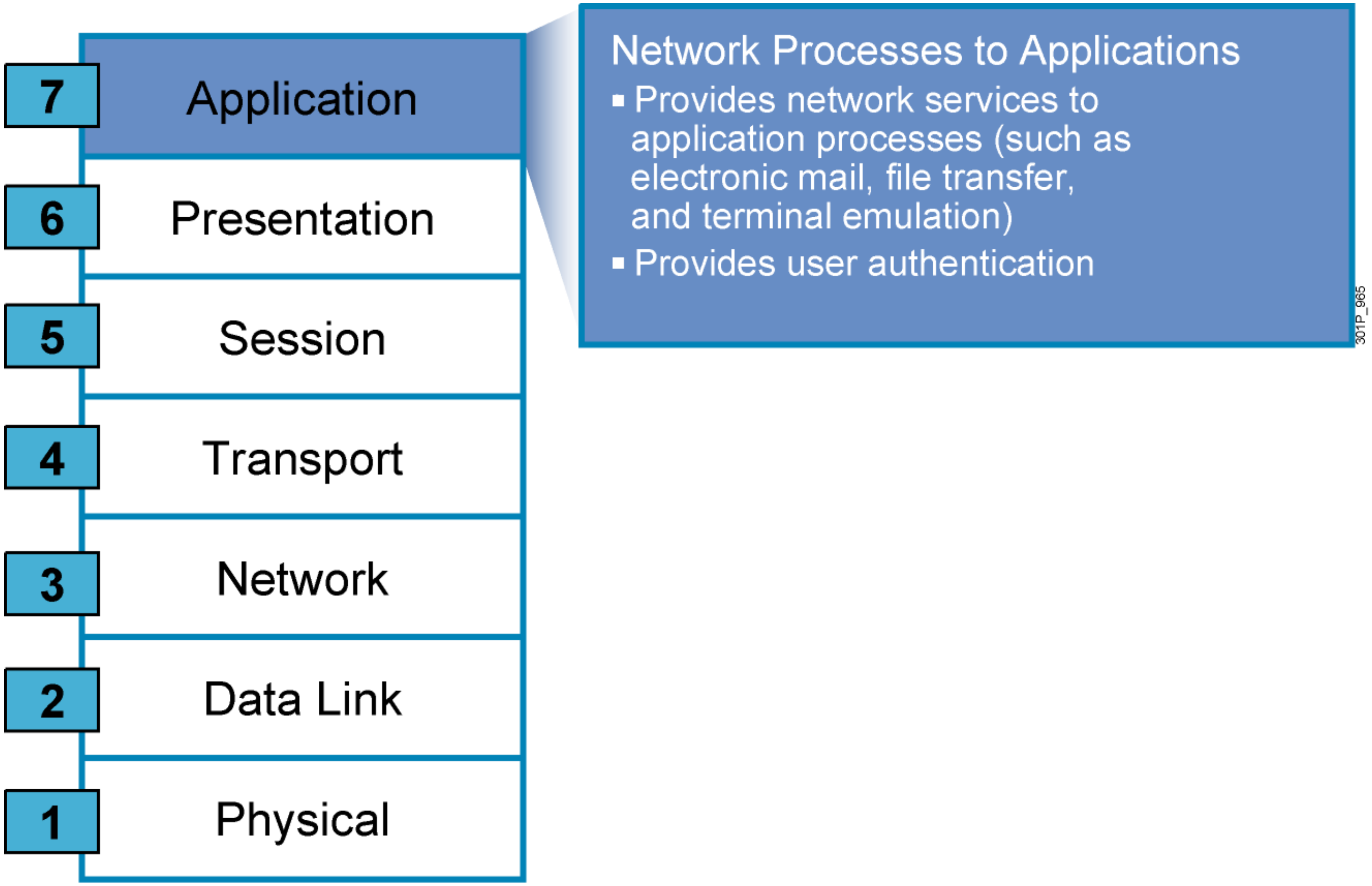
1 Physical

Network Process to Applications

Data Representation

- Ensures that data is readable by receiving system
- Formats data
- Structures data
- Negotiates data transfer syntax for application layer
- Provides encryption

The Seven Layers of the OSI Model (Cont.)



7 Application

6 Presentation

5 Session

4 Transport

3 Network

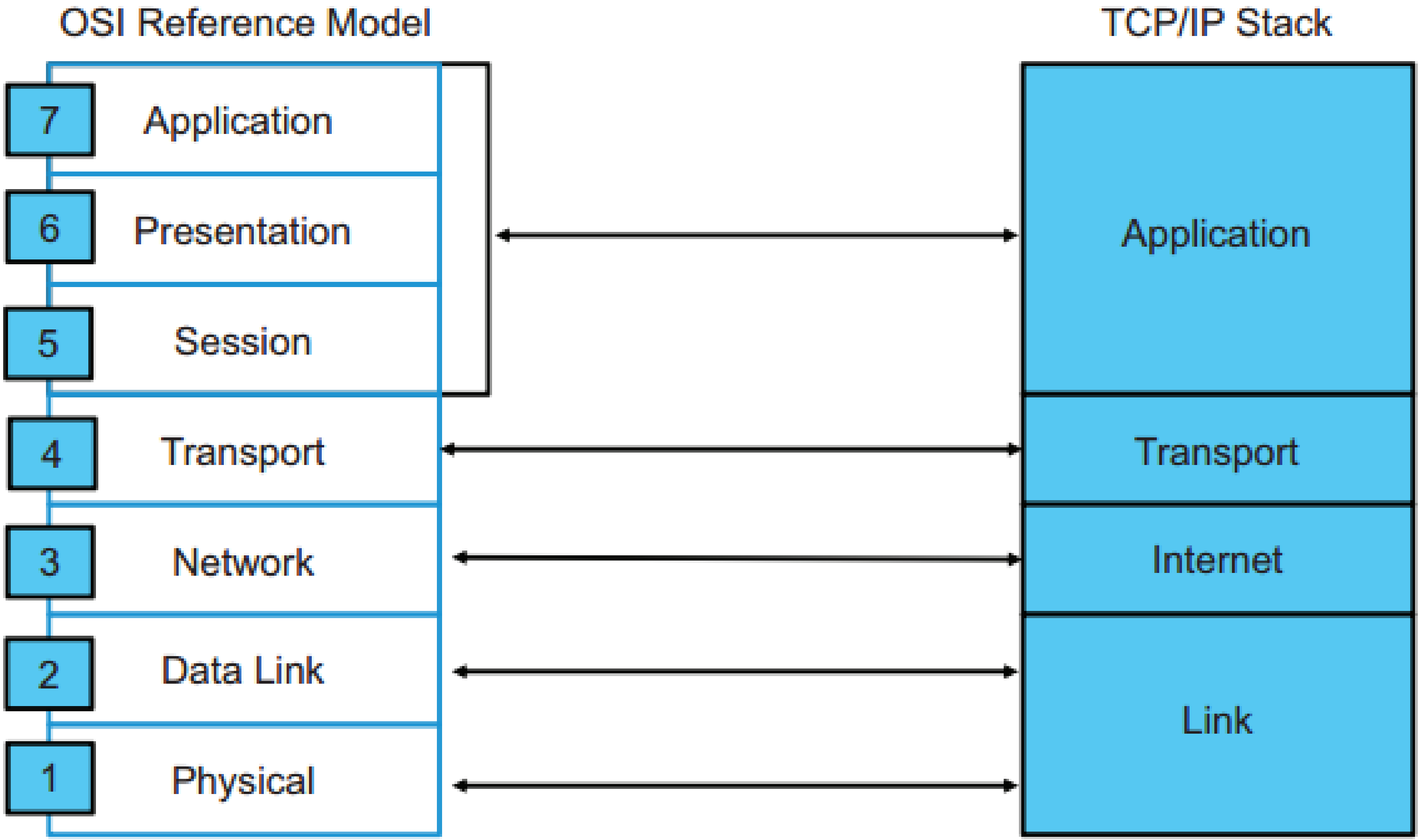
2 Data Link

1 Physical

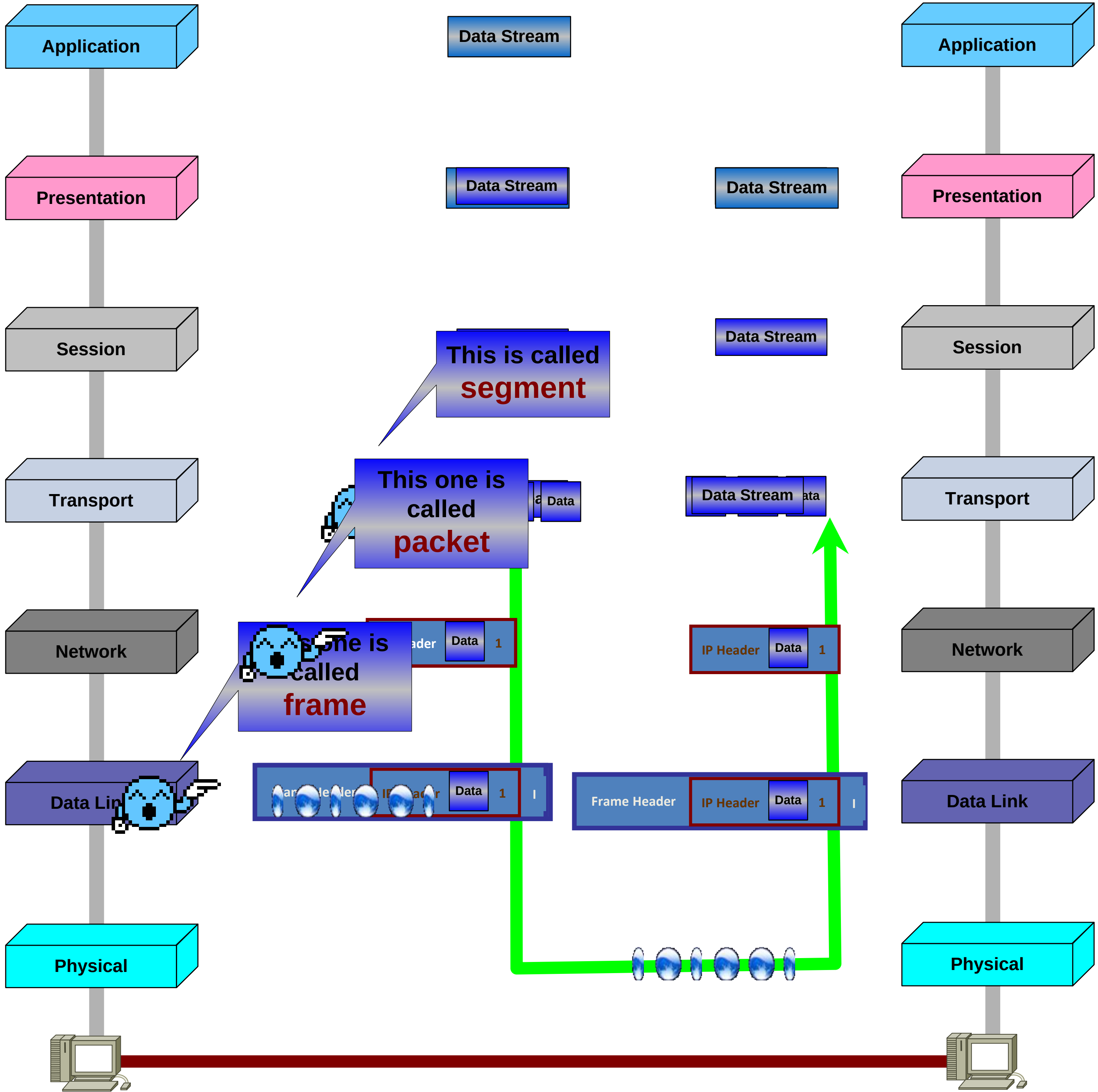
Network Processes to Applications

- Provides network services to application processes (such as electronic mail, file transfer, and terminal emulation)
- Provides user authentication

TCP/IP Protocol Suite



Data encapsualtion & De-encapsulation

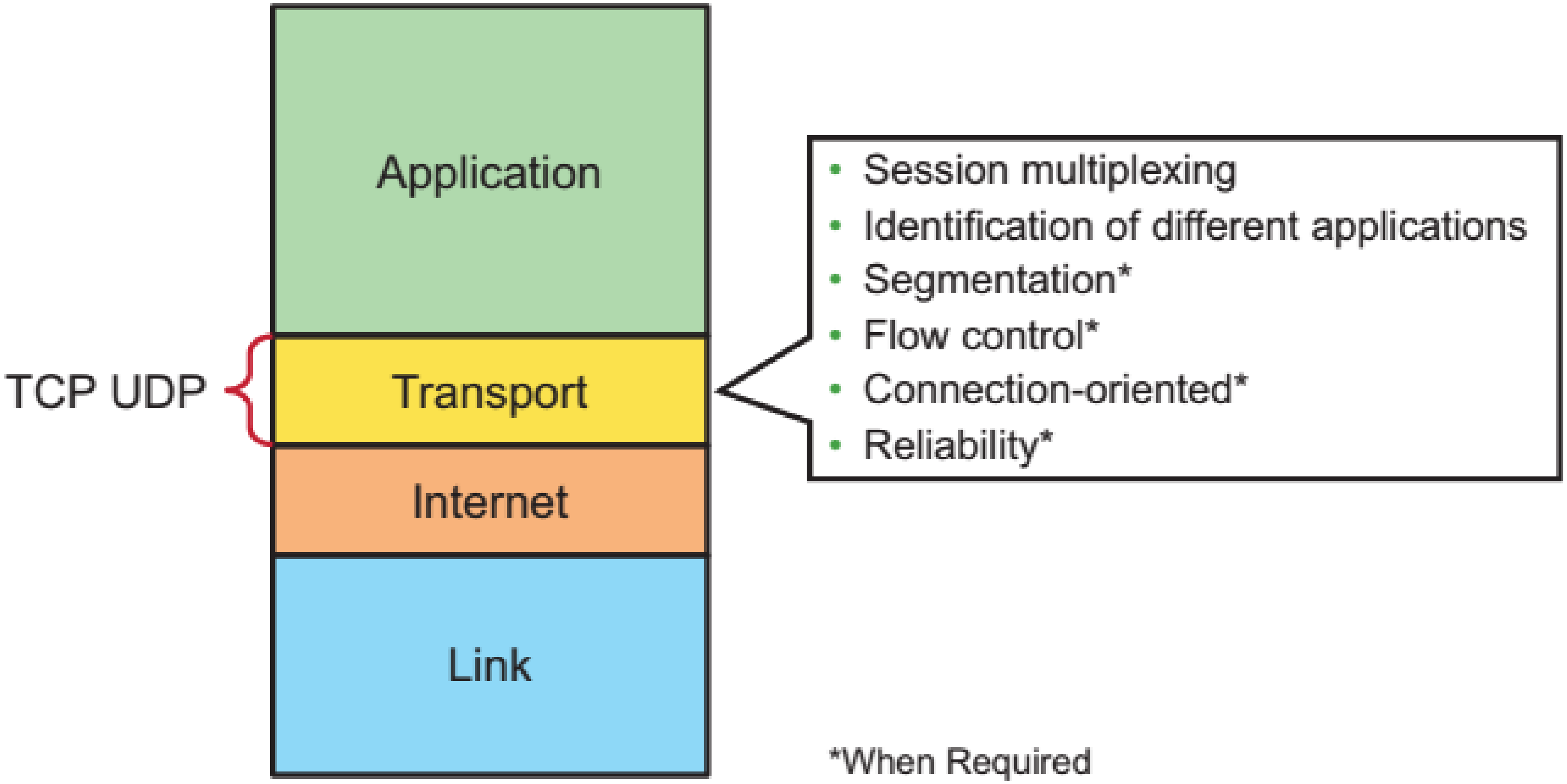


This is called **segment**

This one is called **packet**

This one is called **frame**

TCP/IP Transport Layer Functions



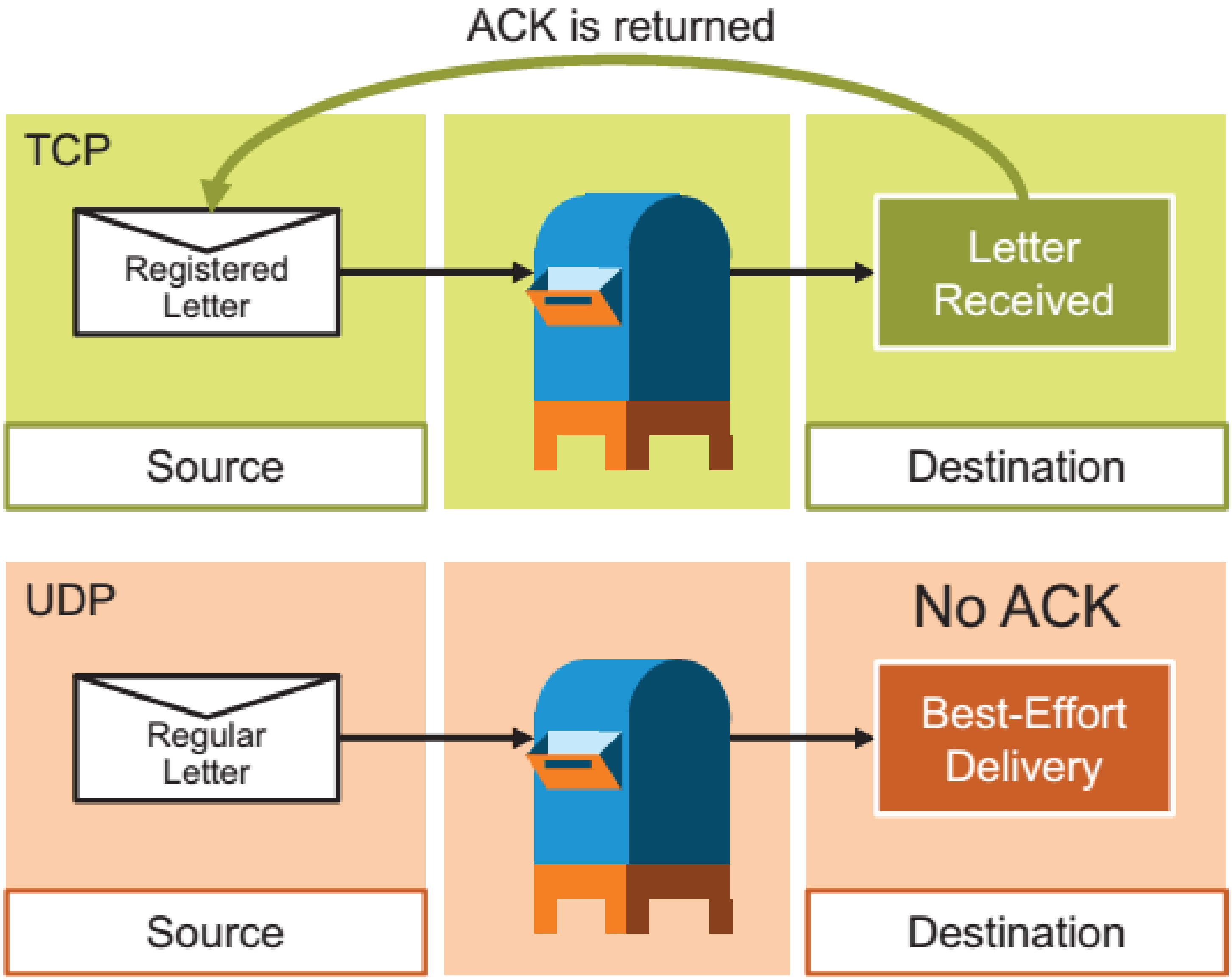
- Session multiplexing
- Identification of different applications
- Segmentation*
- Flow control*
- Connection-oriented*
- Reliability*

*When Required

Reliable vs. Best-Effort Transport

	Reliable	Best Effort
Protocol	TCP	UDP
Connection Type	Connection-oriented	Connectionless
Sequencing	Yes	No
Uses	• Email • File sharing • Downloading	• Voice streaming • Video streaming

TCP vs. UDP Analogy

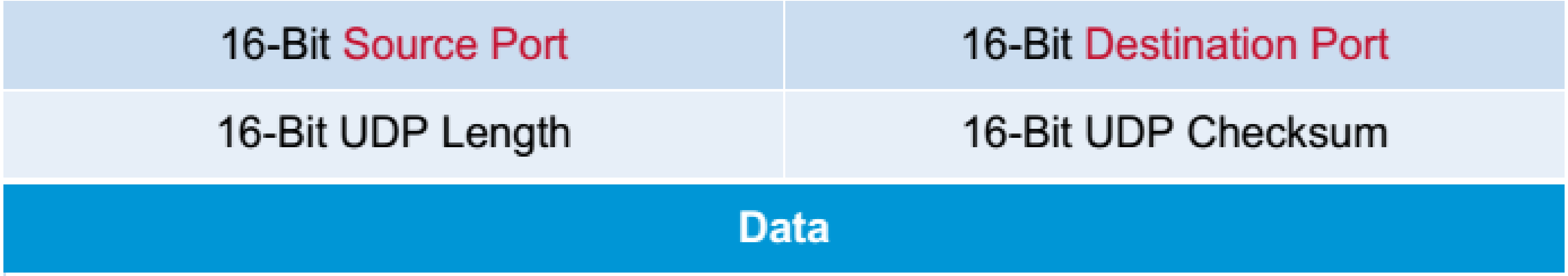


UDP Characteristics

- Operates at the transport layer of the TCP/IP stack
- Provides applications with access to the network layer without the overhead of reliability mechanisms
- Operates as a connectionless protocol
- Provides limited error checking
- Provides best-effort delivery
- Provides no data recovery features

UDP Characteristics (Cont.)

The UDP header:



16-Bit Source Port	16-Bit Destination Port
16-Bit UDP Length	16-Bit UDP Checksum
Data	

TCP Characteristics

- Transport layer of the TCP/IP stack
- Access to the network layer for applications
- Connection-oriented protocol
- Full-duplex mode operation
- Error checking
- Sequencing of data packets
- Reliable delivery—acknowledgment of receipt
- Data recovery features
- Flow control

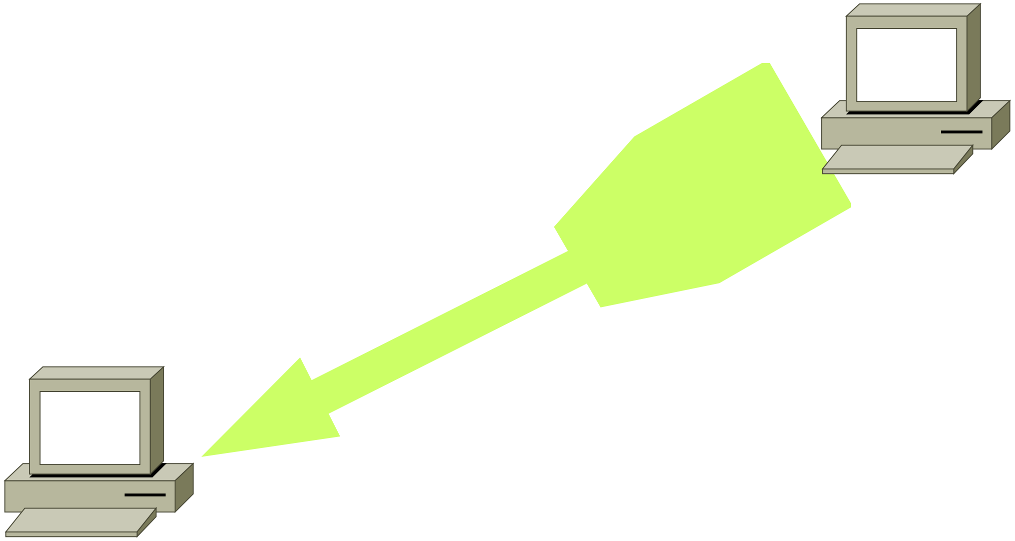
TCP Characteristics (Cont.)

The TCP header:

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgment Number</td></tr>
<tr><td>Header Length</td><td>Reserved</td><td>Flags</td><td>Window Size</td></tr>
<tr><td colspan="3">TCP Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">Options</td></tr>
<tr><td colspan="4"><b>Data</b></td></tr>
</table>

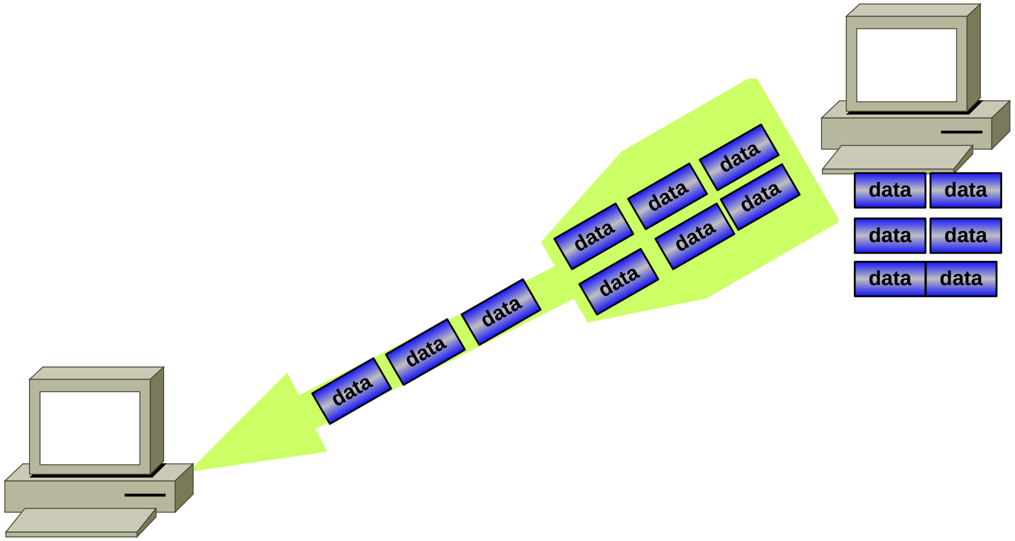
Flow Control

- Once data transfer is in progress, congestion can occur for two reasons.



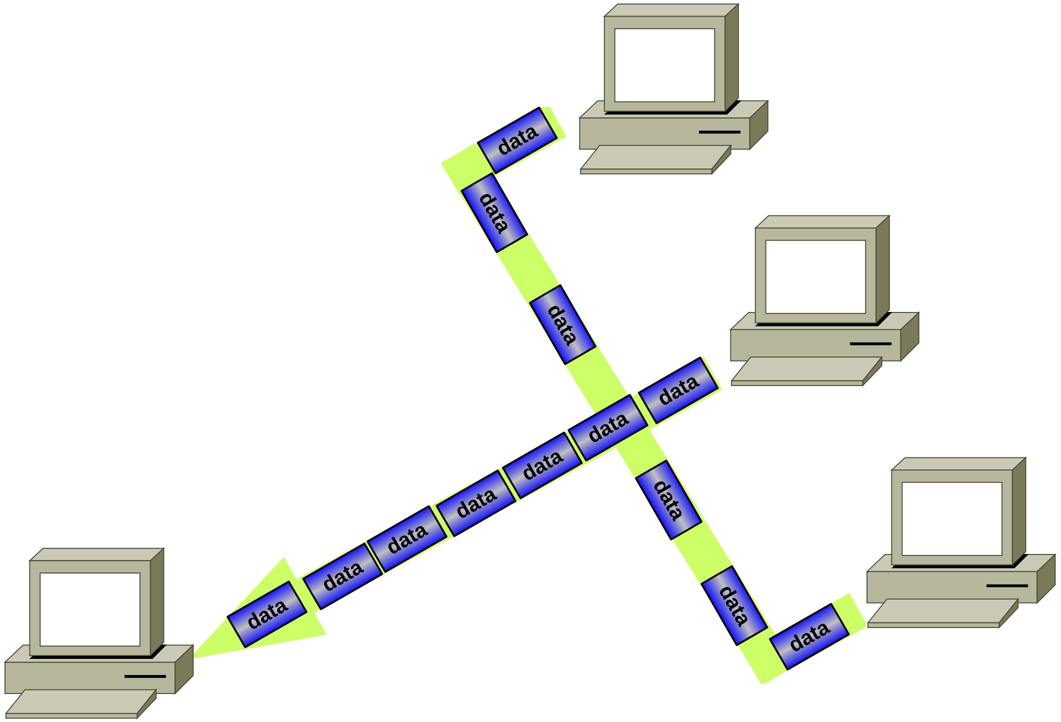
Flow Control (tt)

- First, the sending device might be able to generate traffic faster than the network can transfer it.



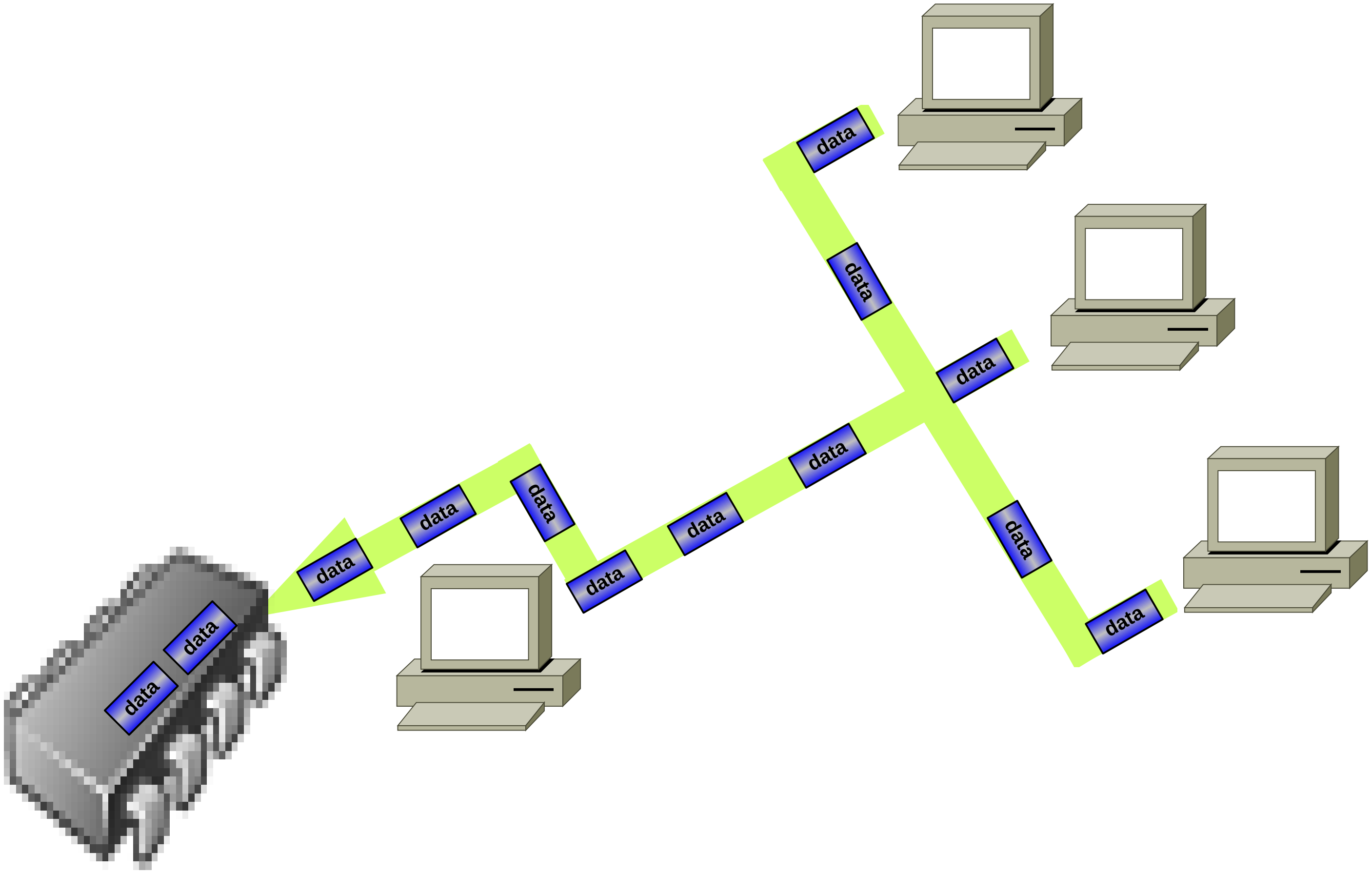
Flow Control (tt)

- The second reason is that multiple devices need to send data to the same destination.



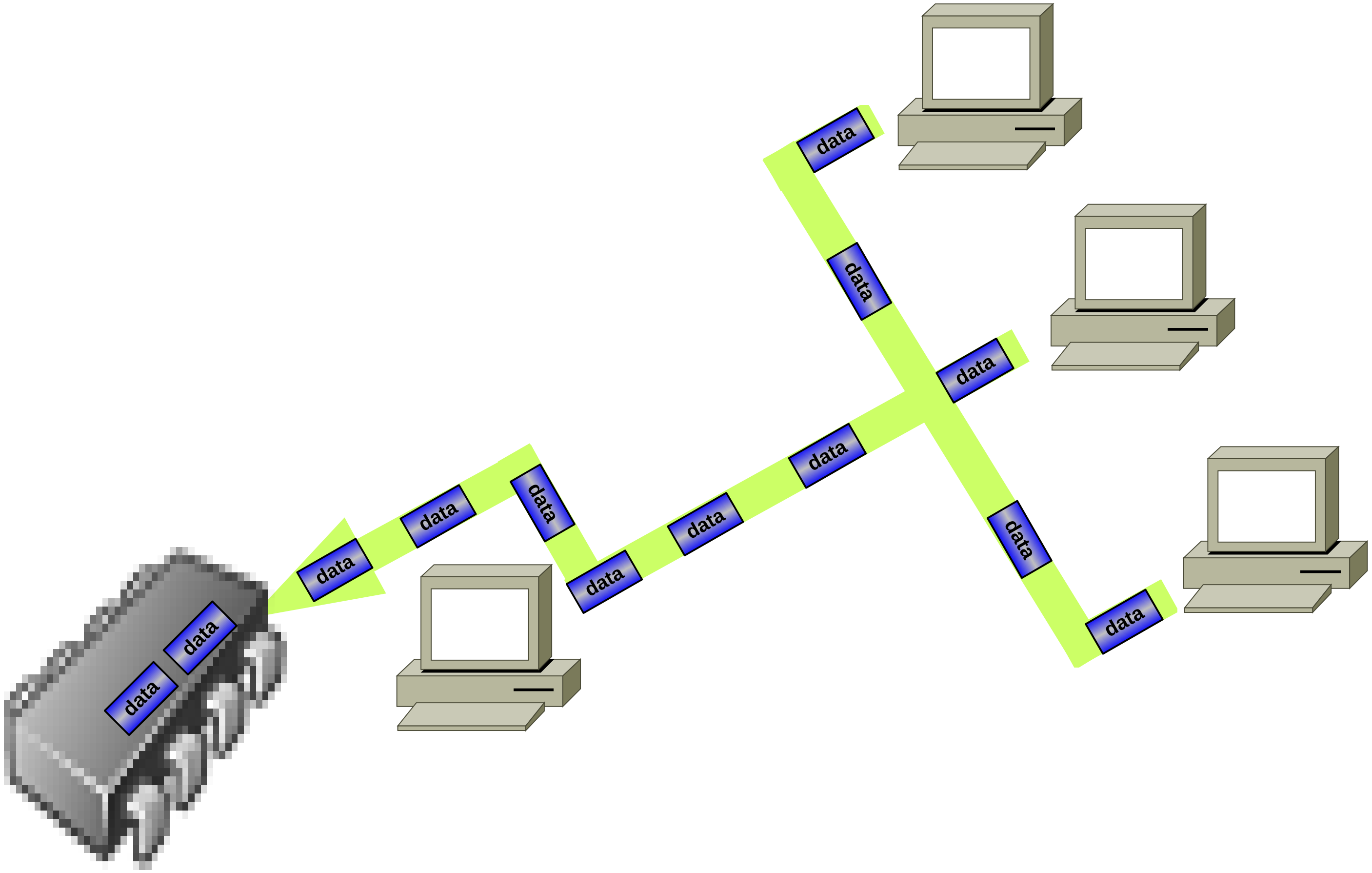
Flow Control (tt)

- When datagram arrive too quickly for a device to process, it temporarily stores them in memory.



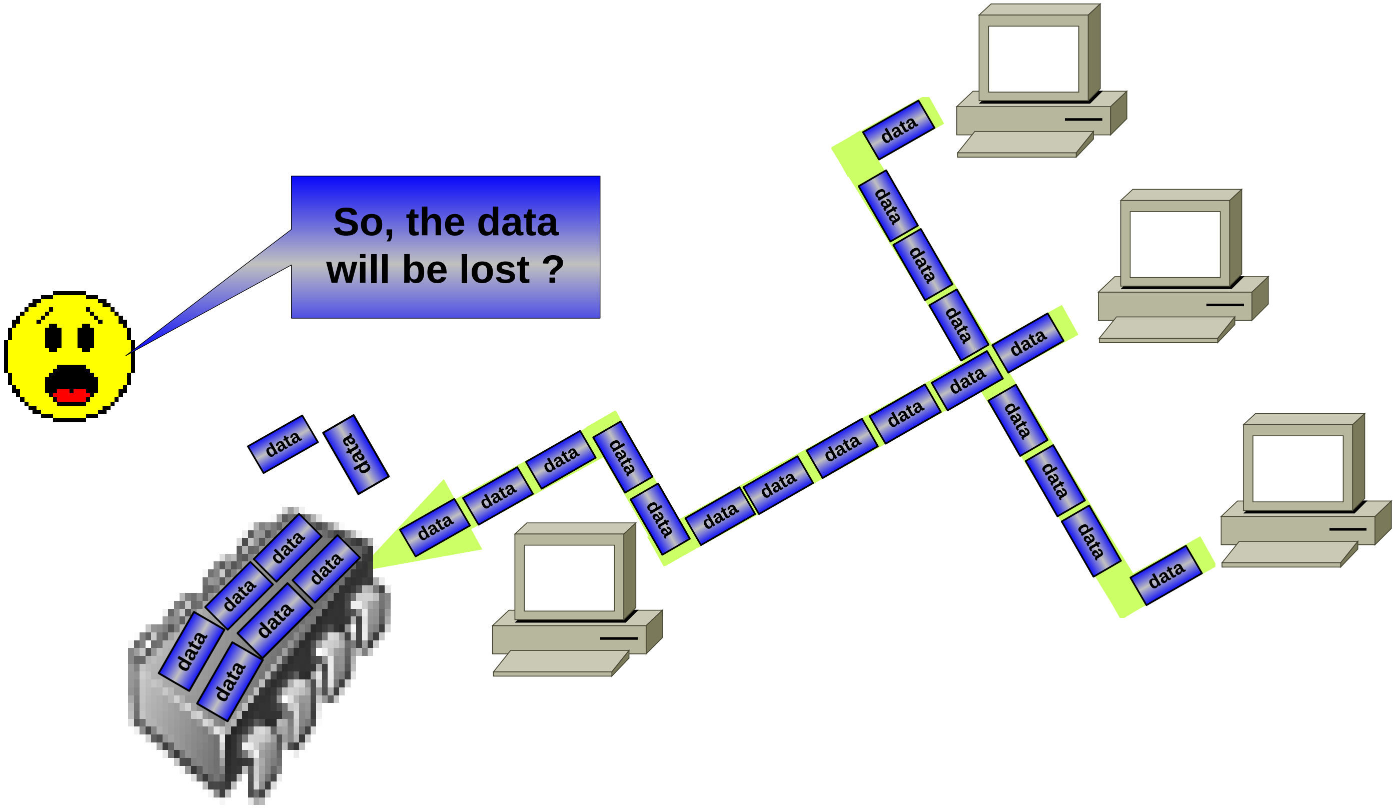
Flow Control (tt)

- If the datagrams are part of a small burst, this buffering solves the problem.



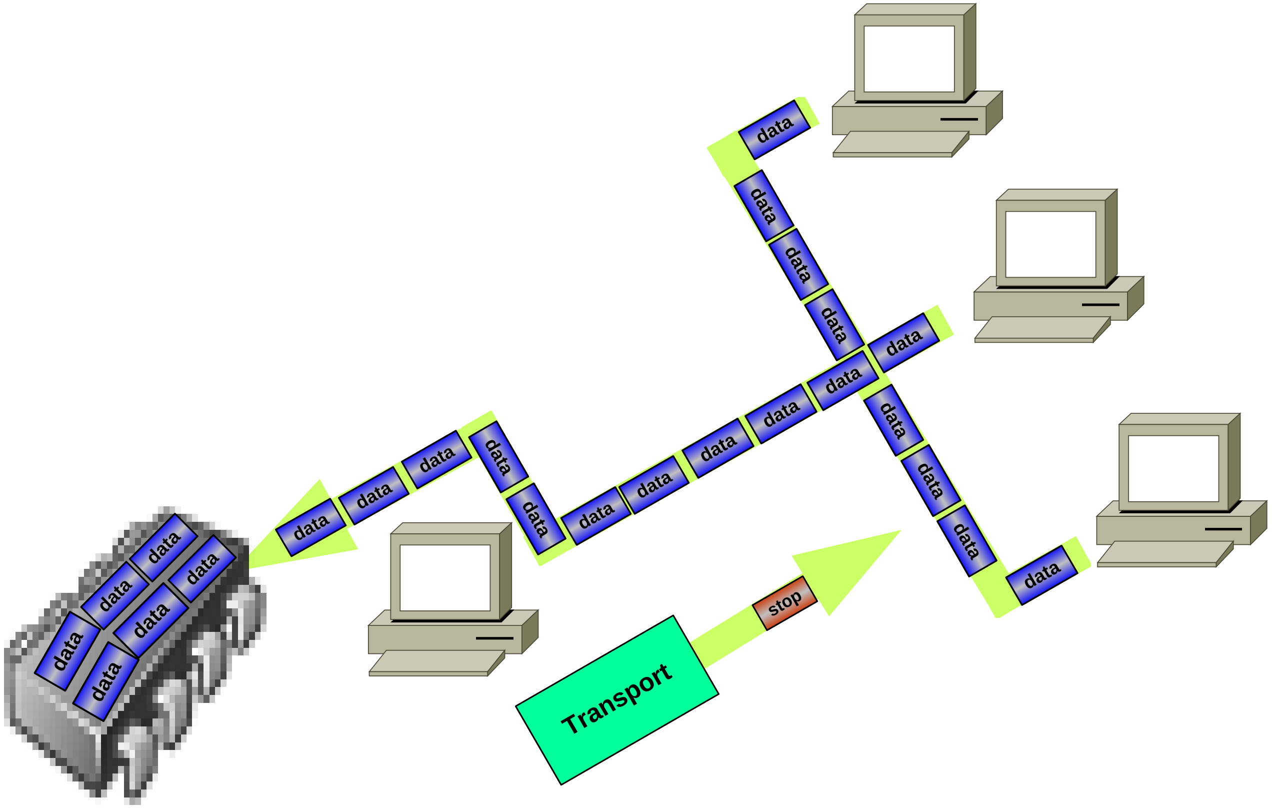
Flow Control (tt)

- However, if the traffic continues at this rate, the device eventually exhausts its memory and must discard additional datagrams that arrive.



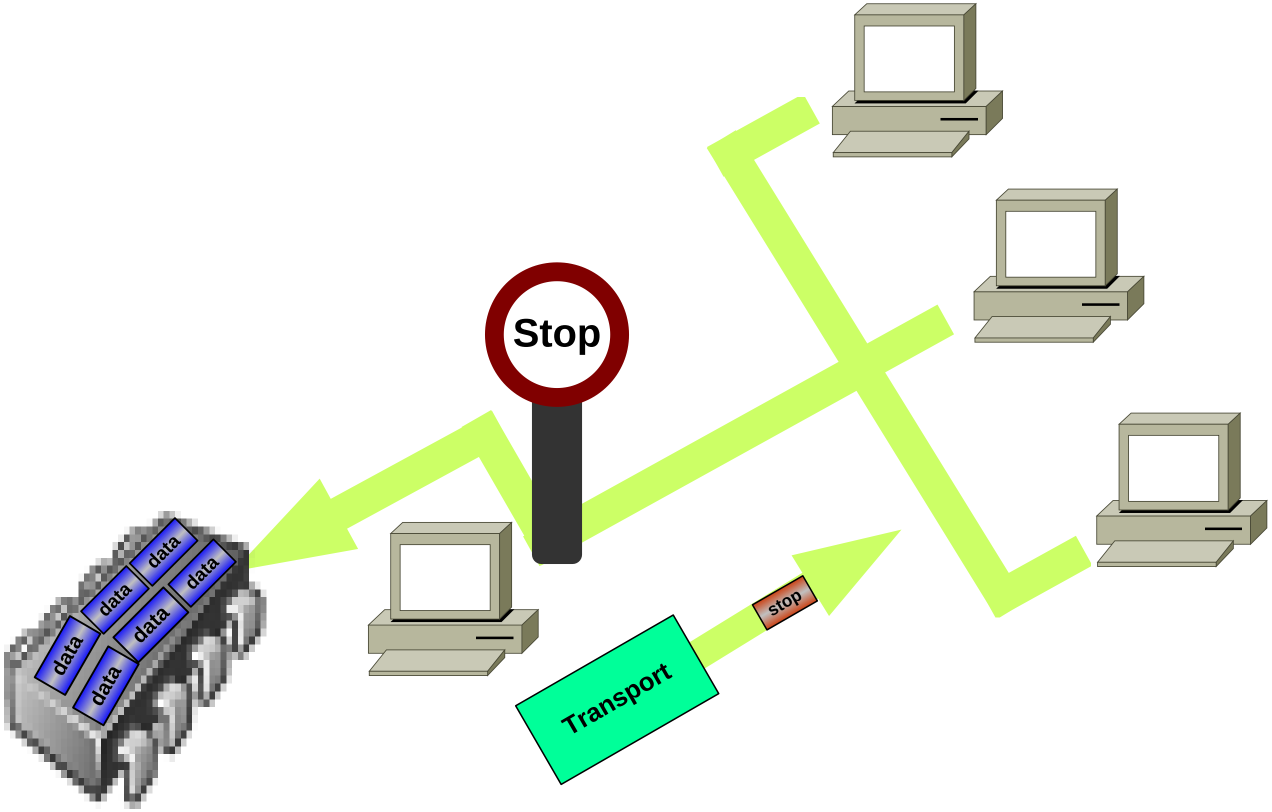
Flow Control (tt)

- Instead of losing the data, the transport function can issue a “not ready” indicator to the sender.



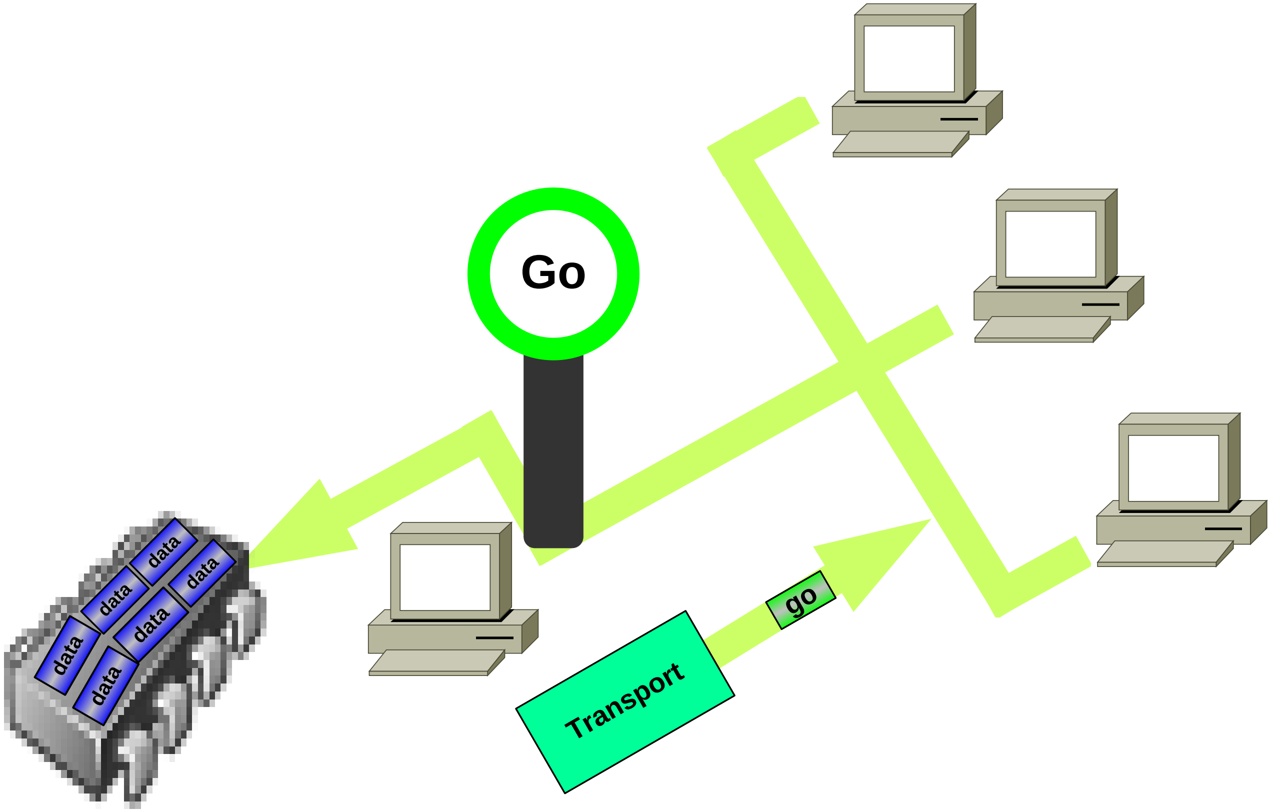
Flow Control (tt)

- This acts like a stop sign and signal the sender to discontinue sending segment traffic to the receiver.



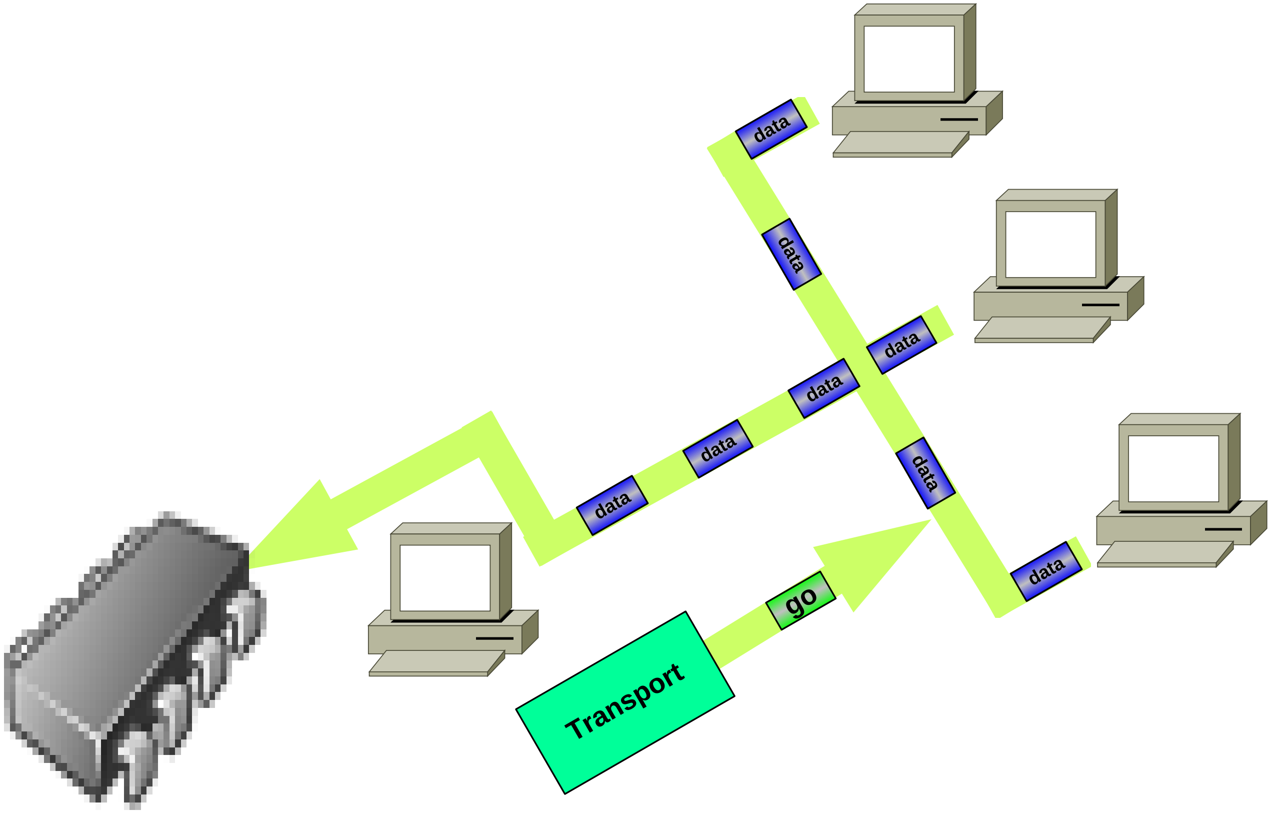
Flow Control (tt)

- After the receiving device has processed sufficient segments to free space in its buffer, the receiver sends a “ready transport “ indicator – which is like a go signal.

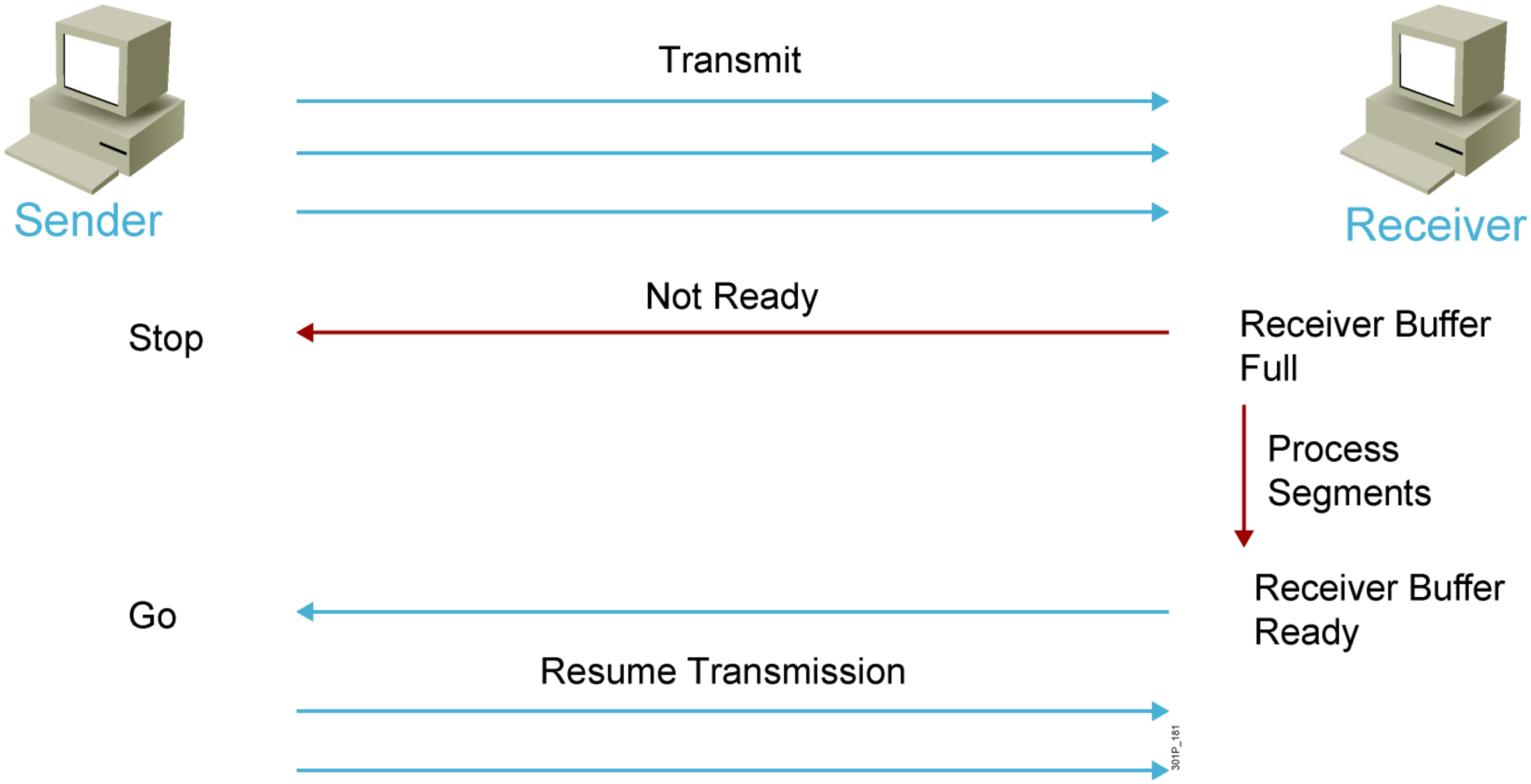


Flow Control (tt)

- When they receives this indicator, the senders can resume segment transmission.



Flow Control (tt)



Sender

Transmit

Receiver

Stop

Not Ready

Receiver Buffer Full

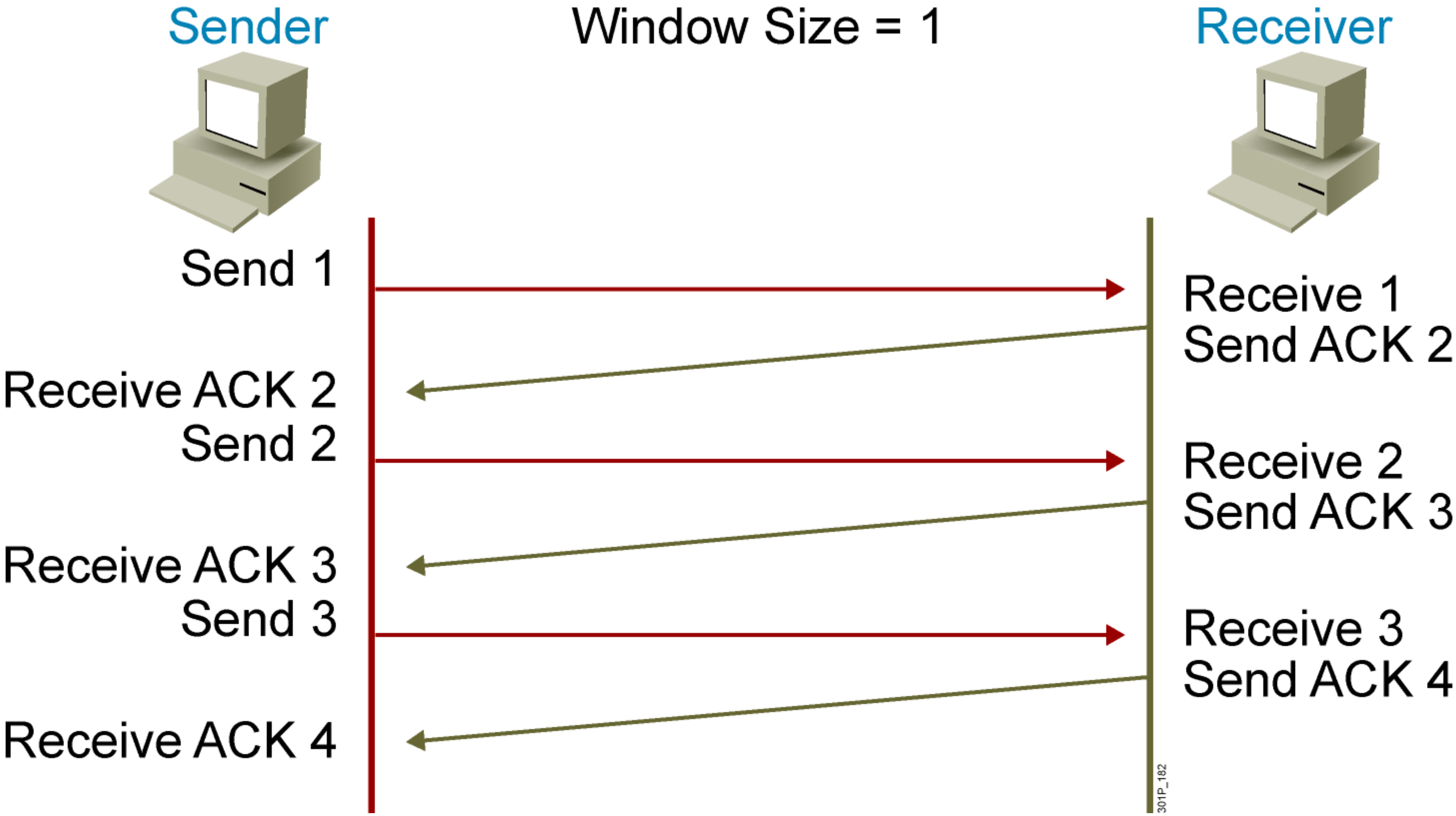
Process Segments

Go

Receiver Buffer Ready

Resume Transmission

TCP Acknowledgment



Sender

Window Size = 1

Receiver

Send 1

Receive 1
Send ACK 2

Receive ACK 2
Send 2

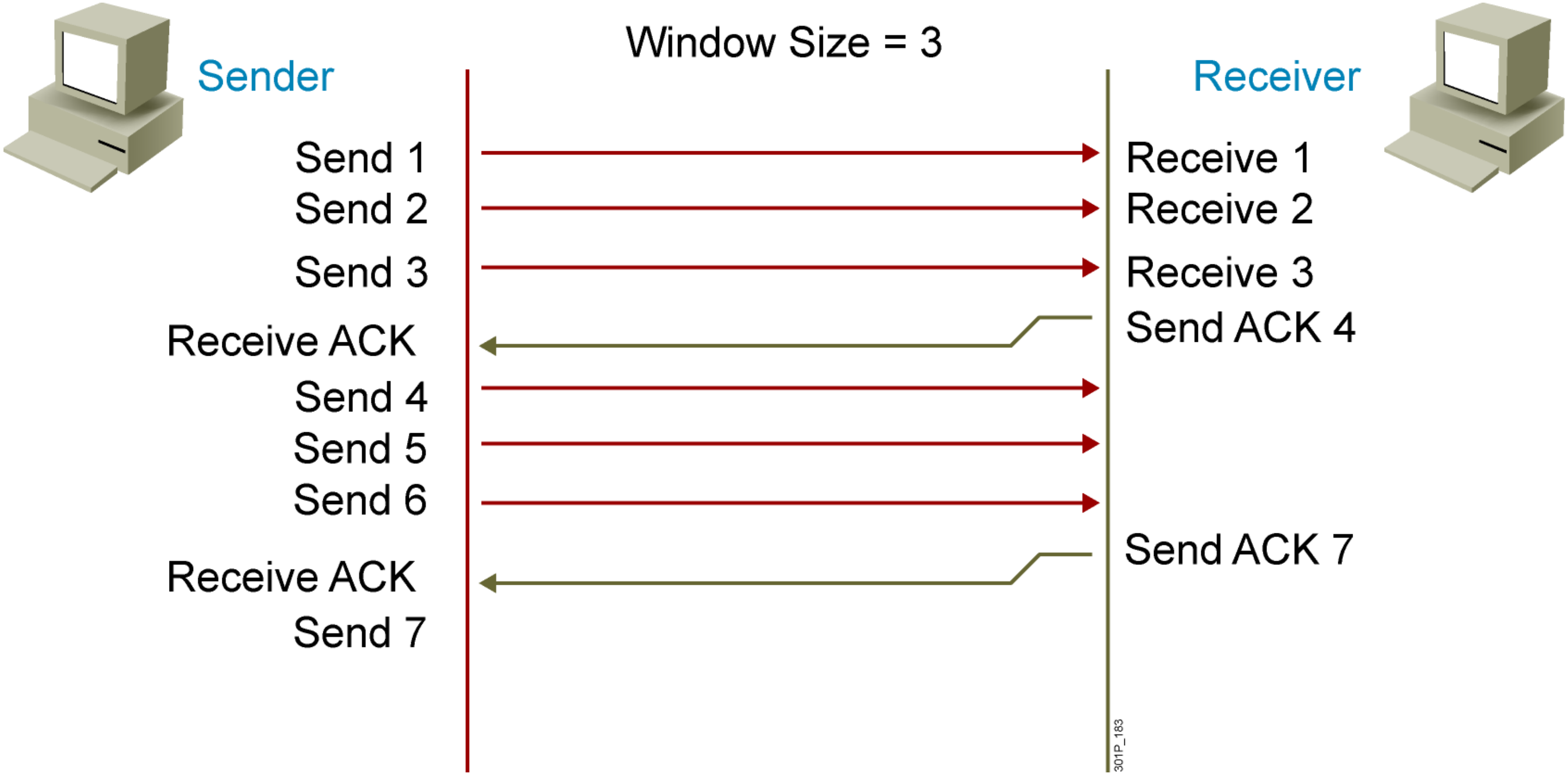
Receive 2
Send ACK 3

Receive ACK 3
Send 3

Receive 3
Send ACK 4

Receive ACK 4

Fixed Windowing



Window Size = 3

Sender

Receiver

Send 1

Receive 1

Send 2

Receive 2

Send 3

Receive 3

Send ACK 4

Receive ACK

Send 4

Send 5

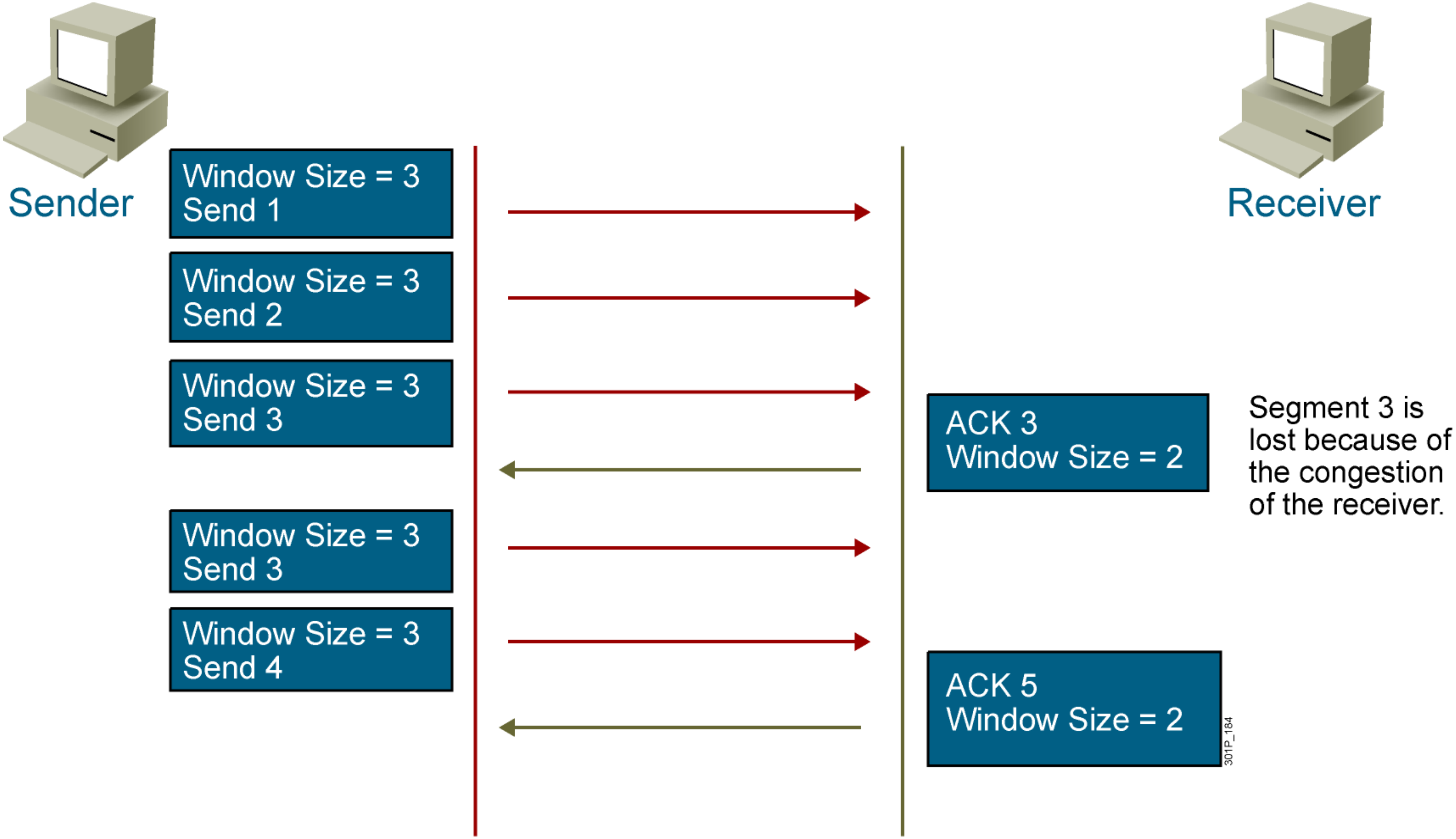
Send 6

Send ACK 7

Receive ACK

Send 7

TCP Sliding Windowing



Sender

Receiver

Window Size = 3
Send 1

Window Size = 3
Send 2

Window Size = 3
Send 3

ACK 3
Window Size = 2

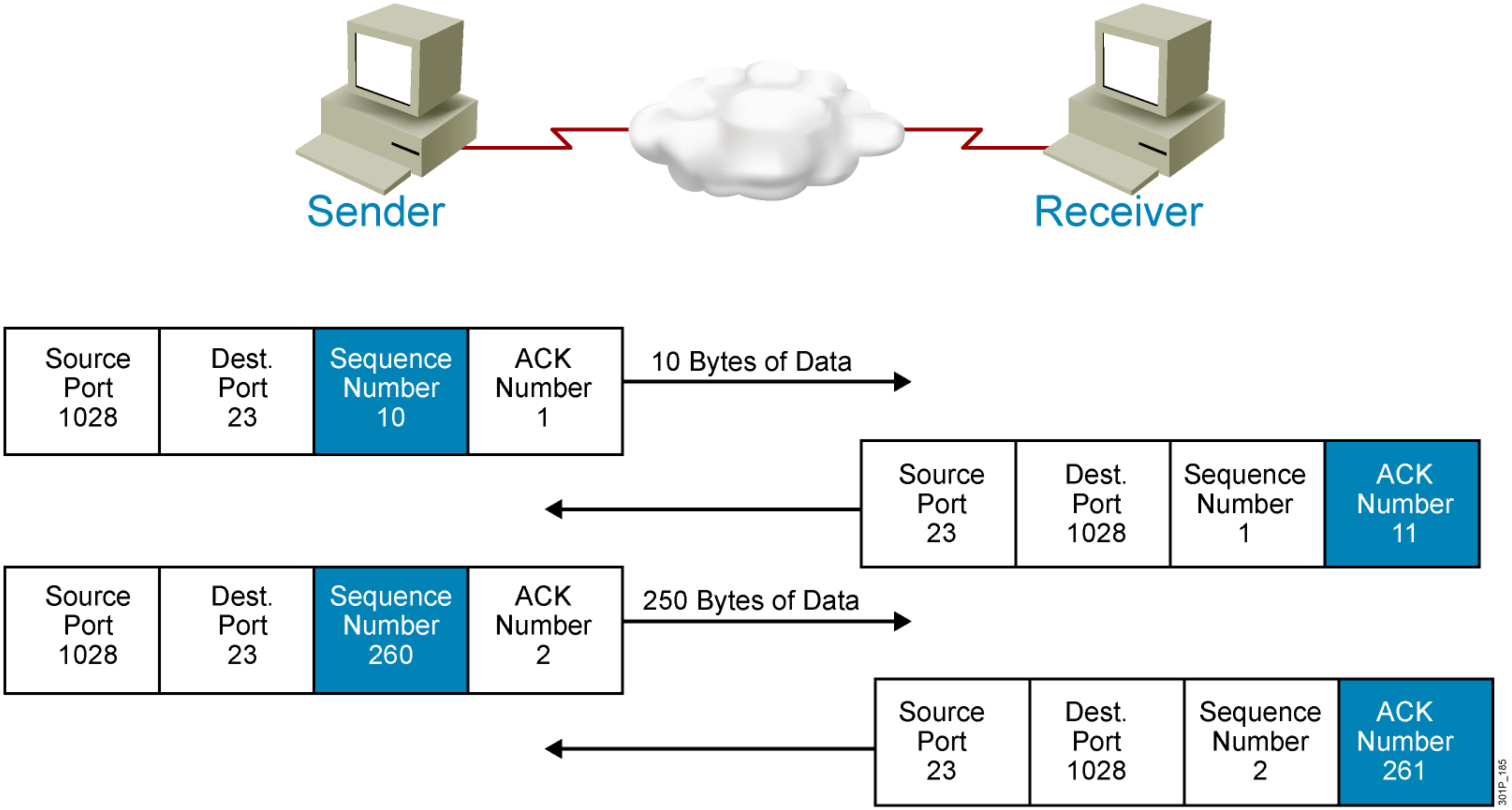
Segment 3 is lost because of the congestion of the receiver.

Window Size = 3
Send 3

Window Size = 3
Send 4

ACK 5
Window Size = 2

TCP Sequence and Acknowledgment Numbers



Source Port	Dest. Port	Sequence Number	ACK Number
1028	23	10	1

10 Bytes of Data

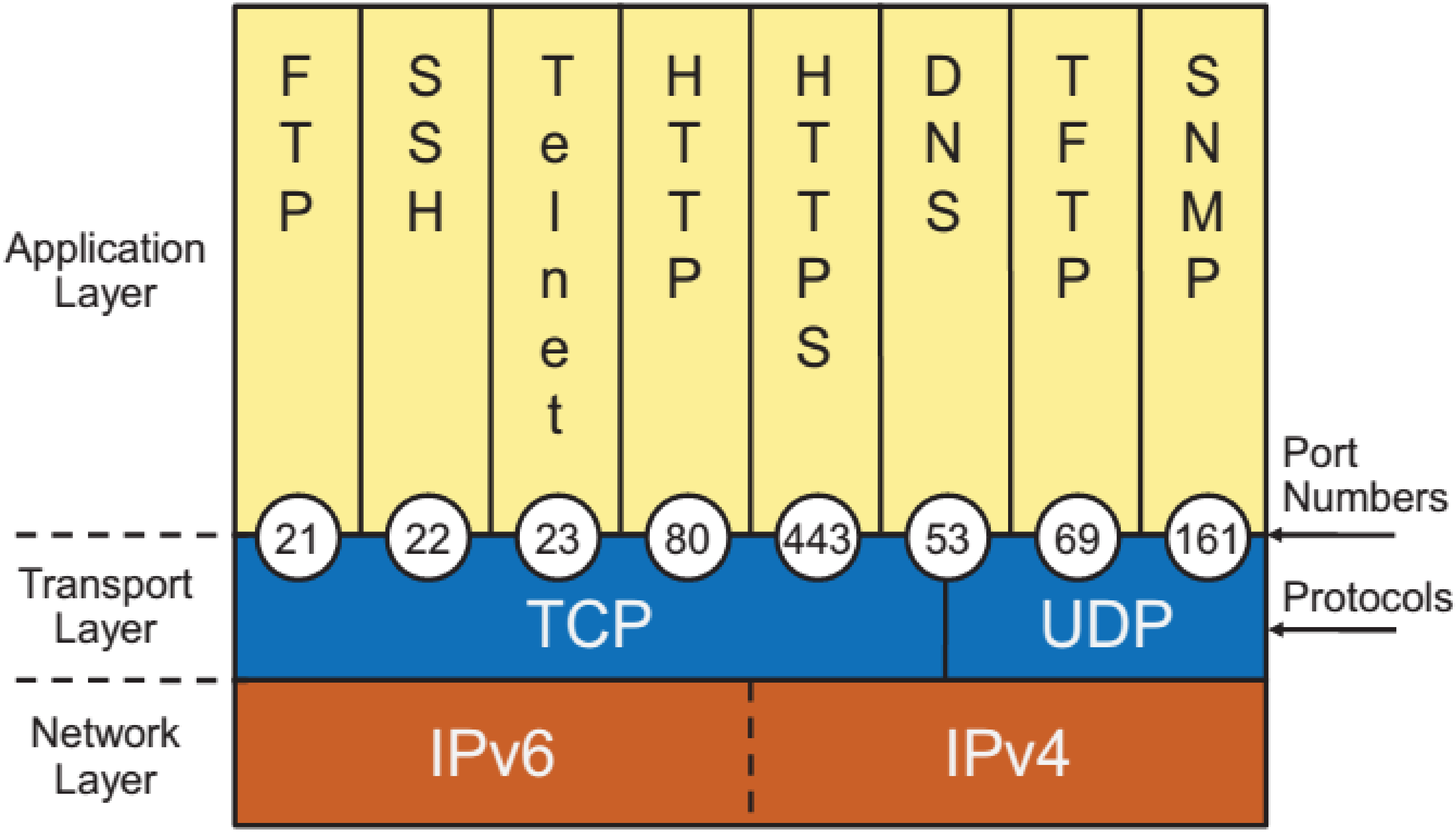
Source Port	Dest. Port	Sequence Number	ACK Number
23	1028	1	11

Source Port	Dest. Port	Sequence Number	ACK Number
1028	23	260	2

250 Bytes of Data

Source Port	Dest. Port	Sequence Number	ACK Number
23	1028	2	261

TCP/IP Applications

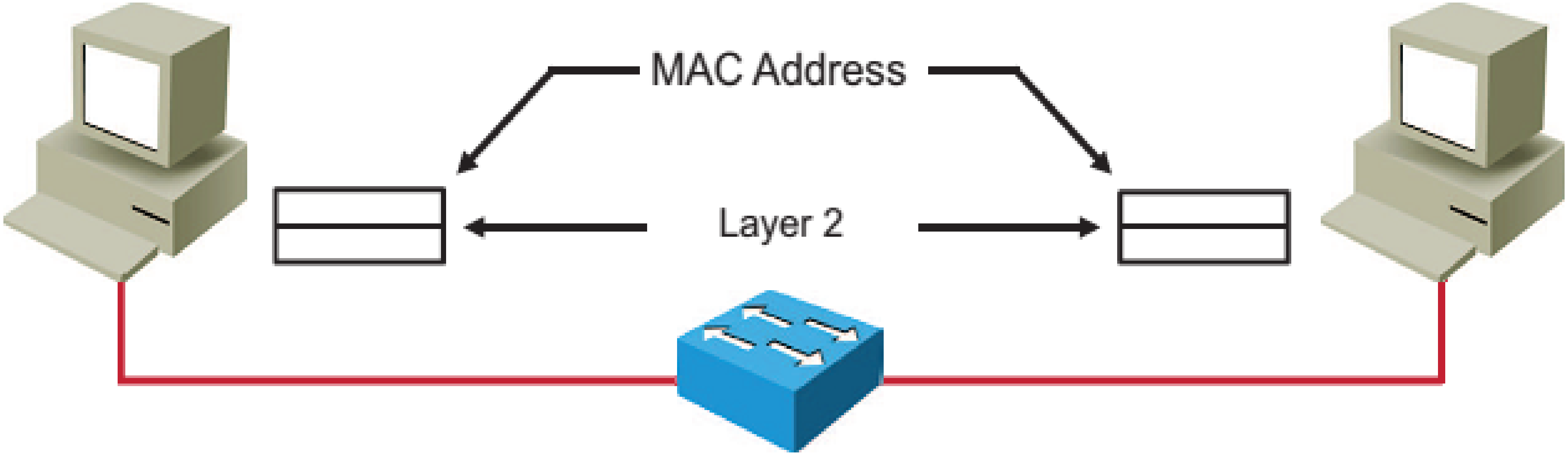


Exploring the Packet Delivery Process

Layer 2 Addressing

Layer 2 characteristics:

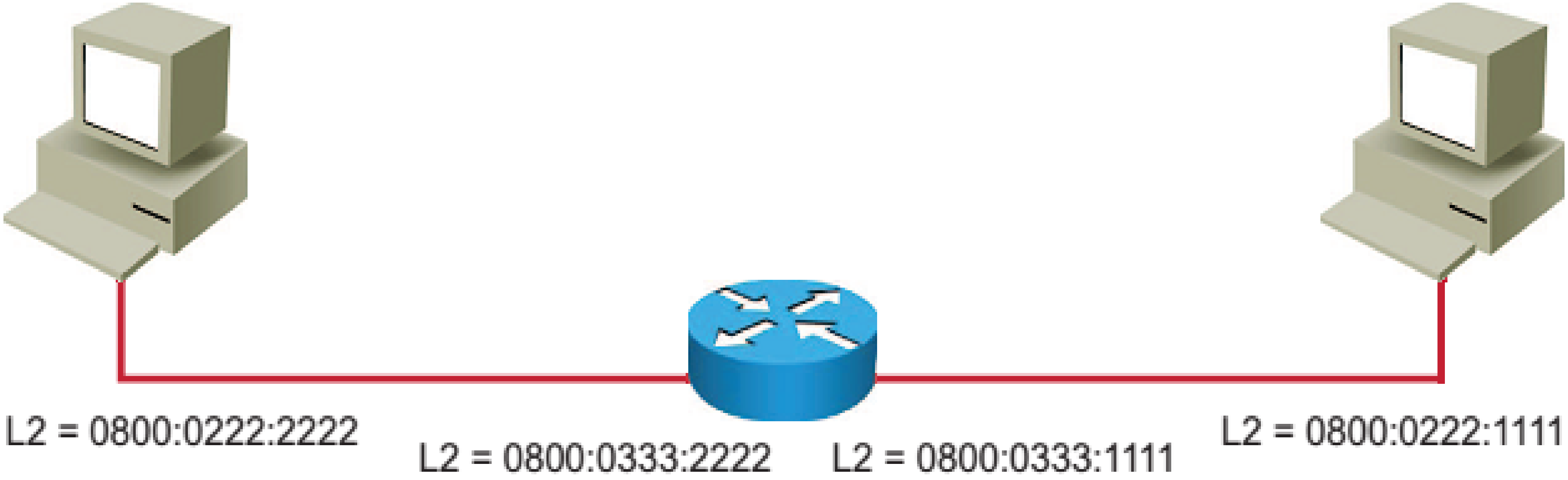
- Ethernet uses MAC addresses.
- Identifies end devices in the LAN.
- Enables the packet to be carried by the local media across each segment.



Layer 2 Addressing (Cont.)

Layer 2 addressing:

- The router has two interfaces directly connected to two PCs.
- Each PC and each router interface has its own unique MAC address.



L2 = 0800:0222:2222

L2 = 0800:0333:2222

L2 = 0800:0333:1111

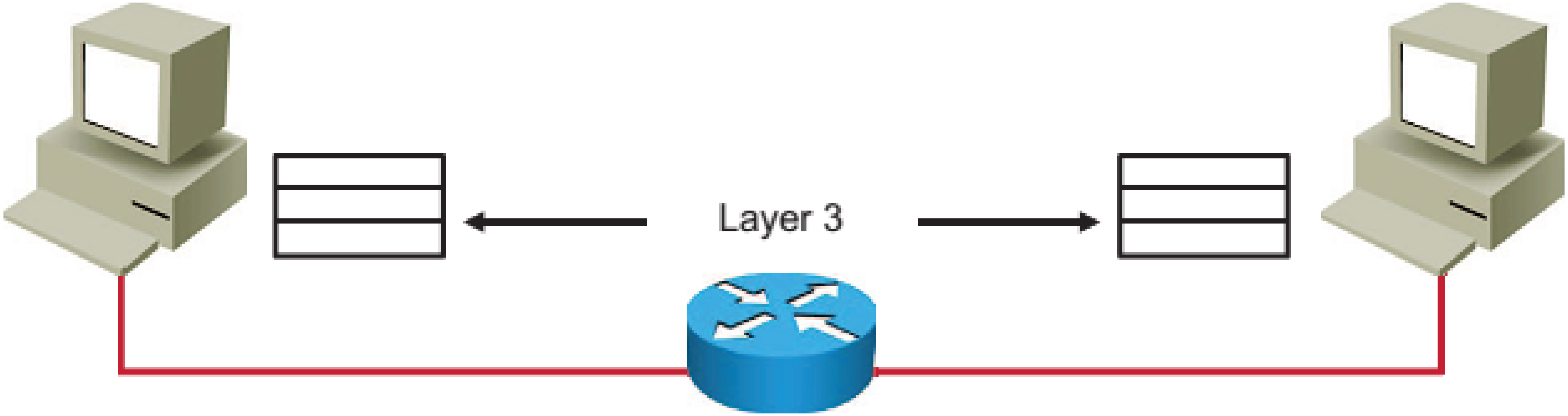
L2 = 0800:0222:1111

L2 = Layer 2

Layer 3 Addressing

Layer 3 devices and functions:

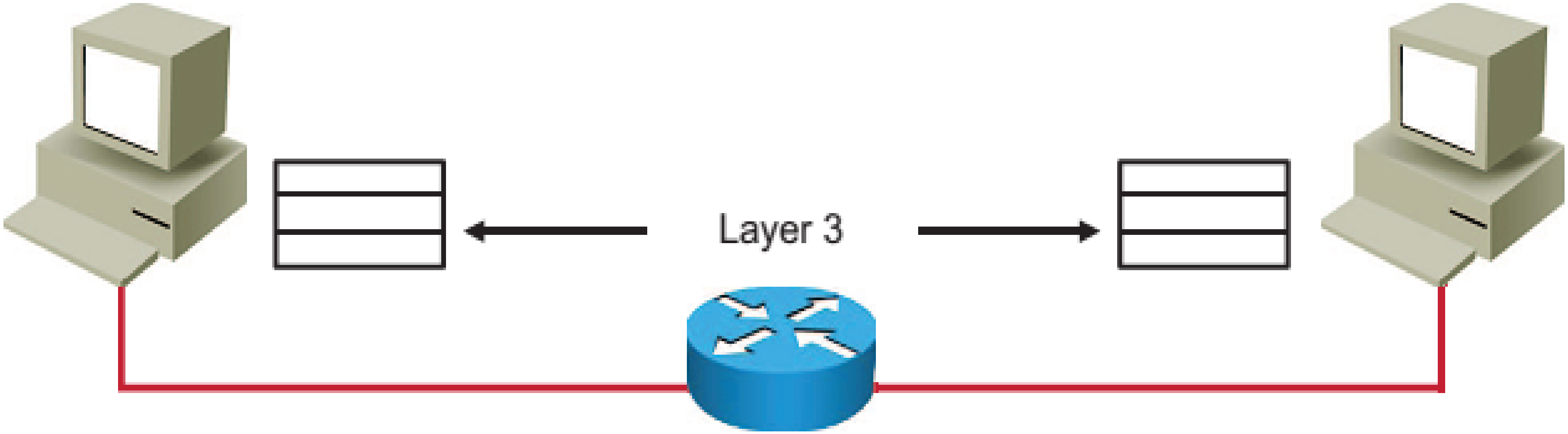
- The network layer provides connectivity and path selection between two host systems.
- In the host, this is the path between the data link layer and the upper layers.
- In the router, it is the actual path across the network.



Layer 3 Addressing (Cont.)

Layer 3 addressing:

- Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks.
- TCP/IP protocol stack uses IP.

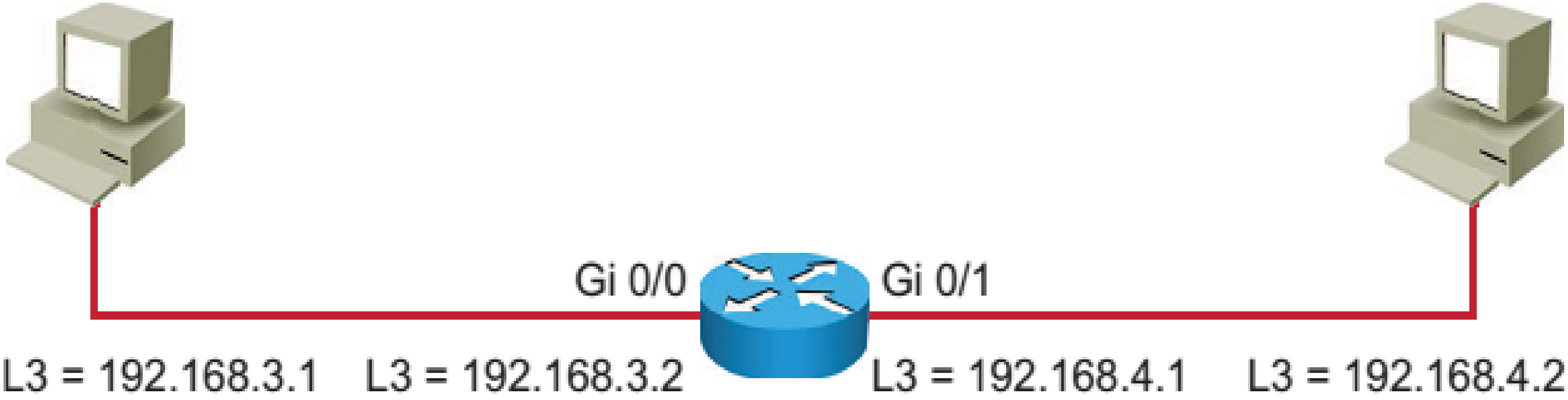


Layer 3 Addressing (Cont.)

- Layer 3 addresses are assigned to hosts and network devices that provide Layer 3 functions.
- Network devices maintain a routing table.

Routing Table

192.168.3.0/24	Interface Gi0/0
192.168.4.0/24	Interface Gi0/1



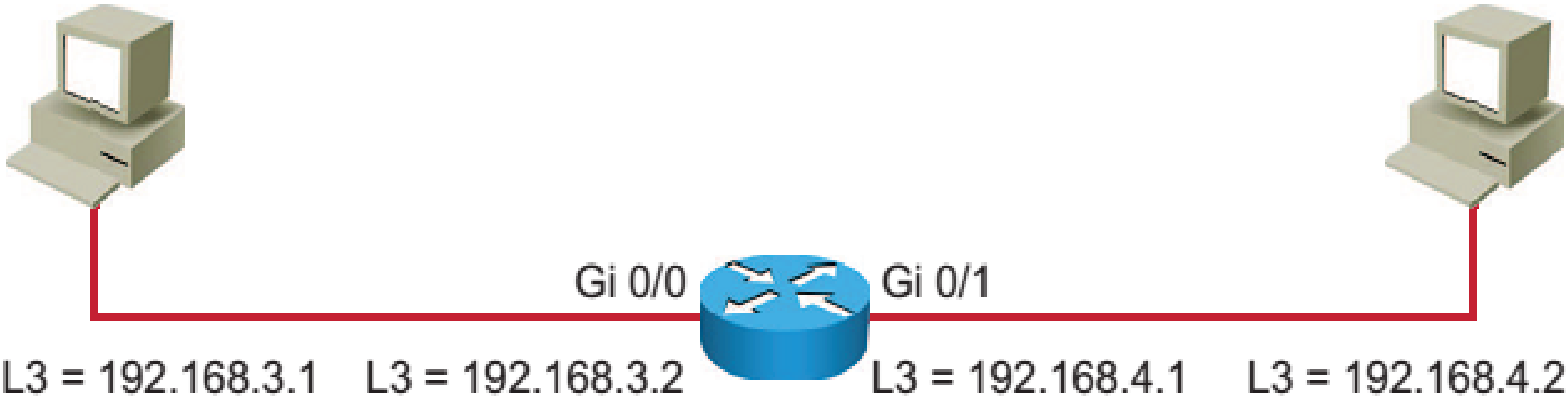
L3 = Layer 3

Layer 3 Addressing (Cont.)

- Layer 3 addresses are assigned to hosts and network devices that provide Layer 3 functions.
- Network devices maintain a routing table.

Routing Table

192.168.3.0/24	Interface Gi0/0
192.168.4.0/24	Interface Gi0/1



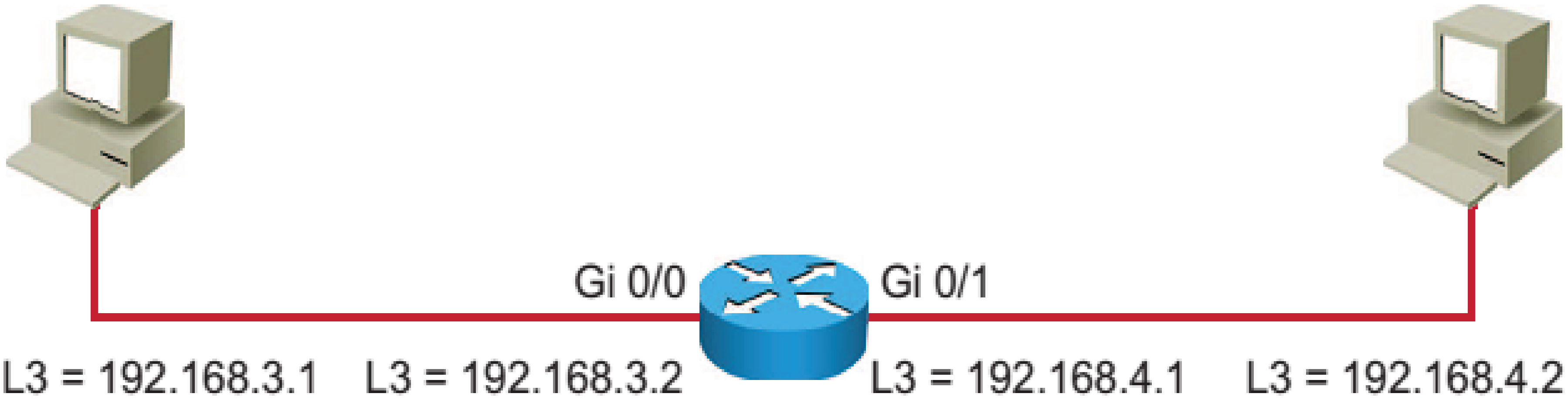
L3 = Layer 3

Layer 3 Addressing (Cont.)

- Layer 3 addresses are assigned to hosts and network devices that provide Layer 3 functions.
- Network devices maintain a routing table.

Routing Table

192.168.3.0/24	Interface Gi0/0
192.168.4.0/24	Interface Gi0/1

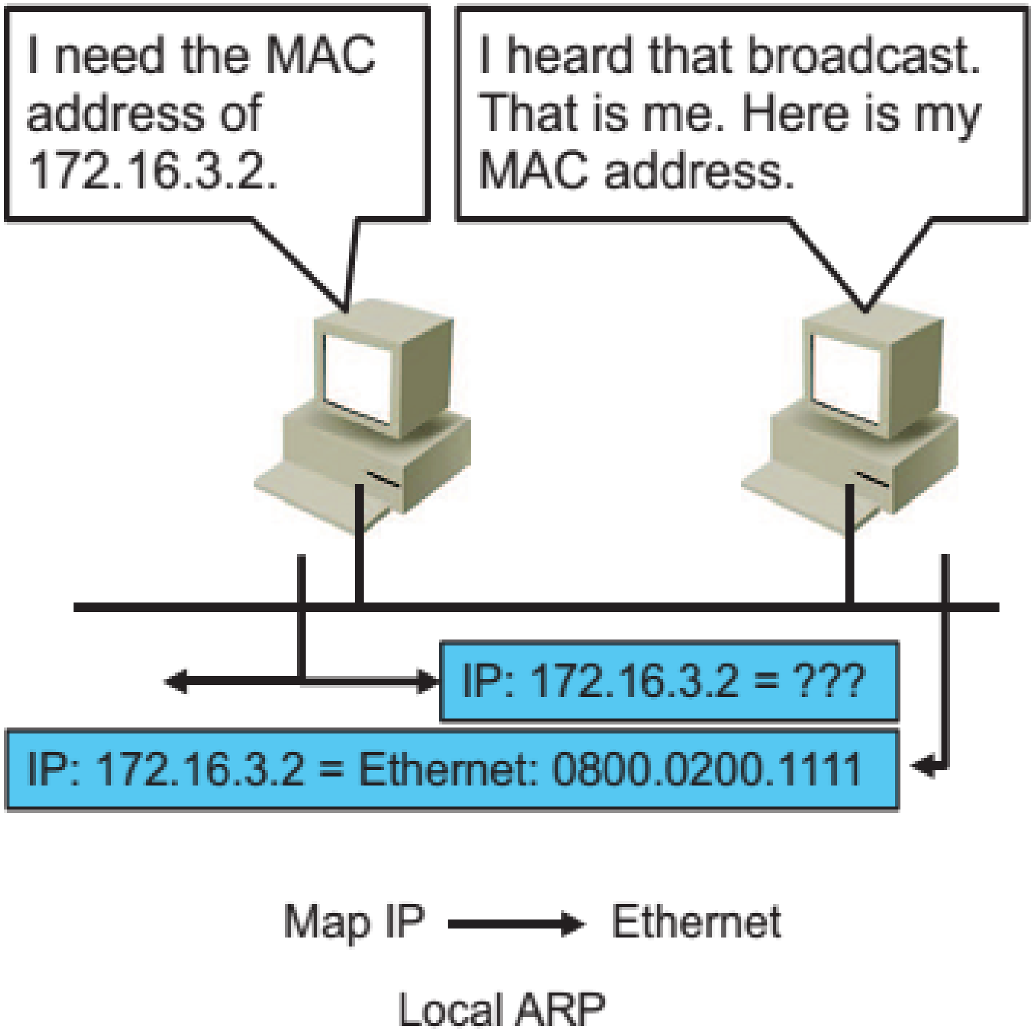


L3 = Layer 3

Address Resolution Protocol

ARP provides two basic functions:

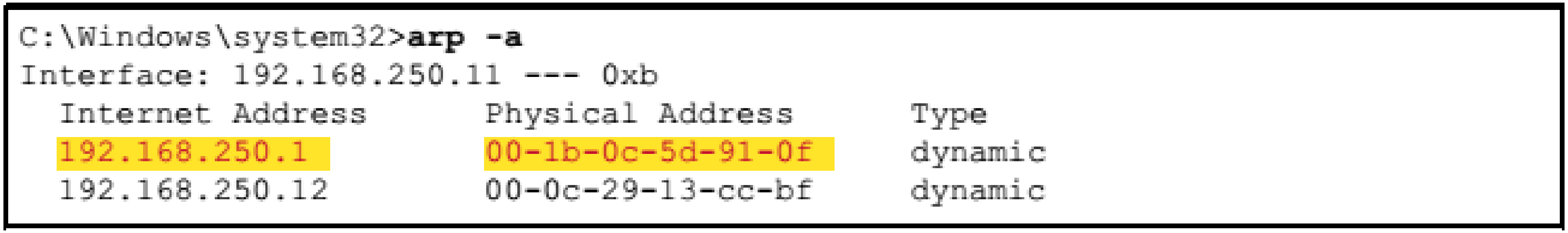
- Resolving IP addresses to MAC addresses
- Maintaining a cache of mappings


I need the MAC address of 172.16.3.2.
I heard that broadcast. That is me. Here is my MAC address.
IP: 172.16.3.2 = ???
IP: 172.16.3.2 = Ethernet: 0800.0200.1111
Map IP → Ethernet
Local ARP

Address Resolution Protocol (Cont.)

The ARP table keeps a record of recent bindings of IP addresses to MAC addresses.

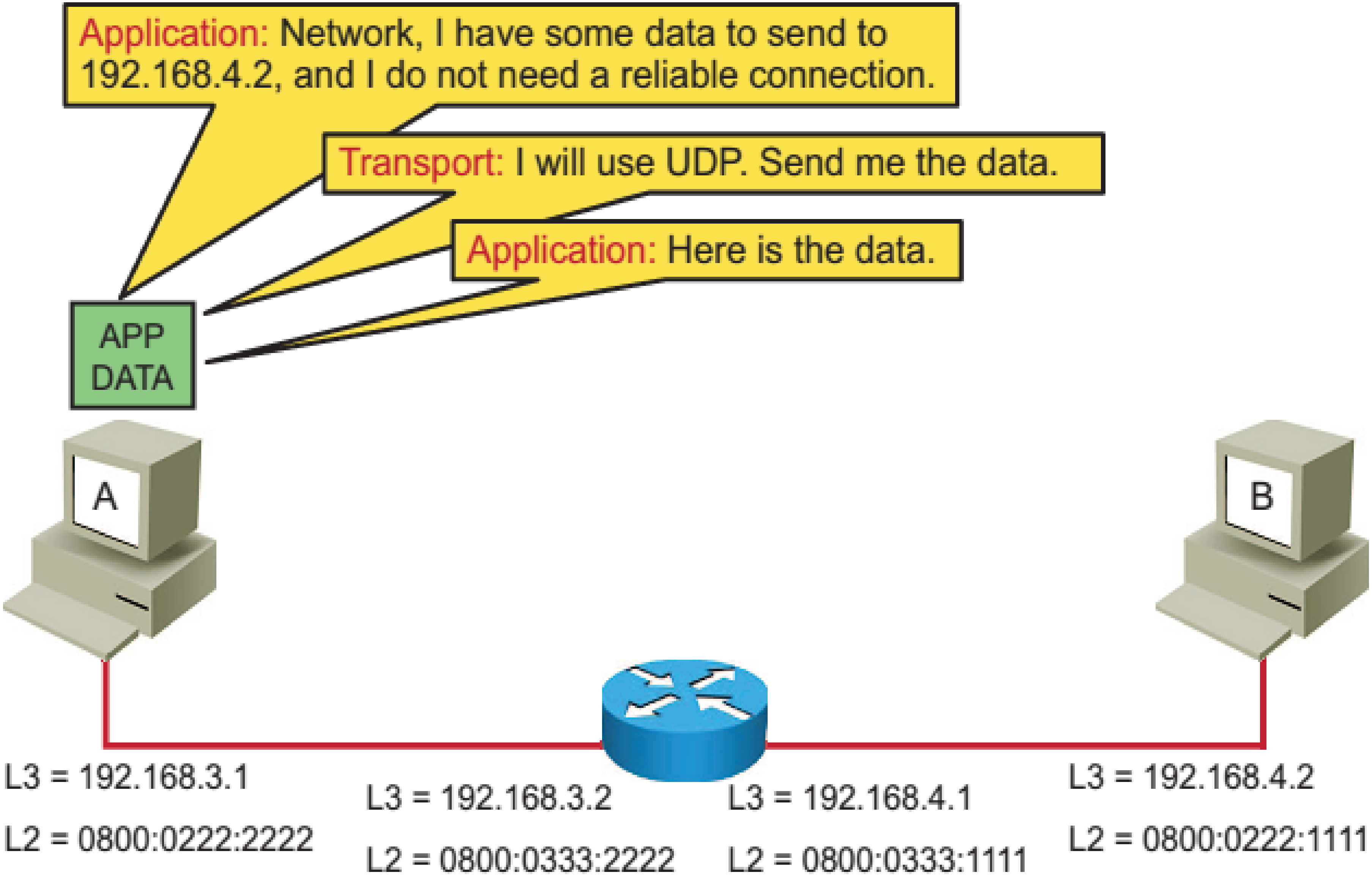
On the PC:



```
C:\Windows\system32>arp -a
Interface: 192.168.250.11 --- 0xb
  Internet Address      Physical Address      Type
  192.168.250.1         00-1b-0c-5d-91-0f     dynamic
  192.168.250.12        00-0c-29-13-cc-bf     dynamic
```

Host – to –Host packet delivery

Host-to-Host Packet Delivery (Step 1 of 16)



Application: Network, I have some data to send to 192.168.4.2, and I do not need a reliable connection.

Transport: I will use UDP. Send me the data.

Application: Here is the data.

L3 = 192.168.3.1

L2 = 0800:0222:2222

L3 = 192.168.3.2

L2 = 0800:0333:2222

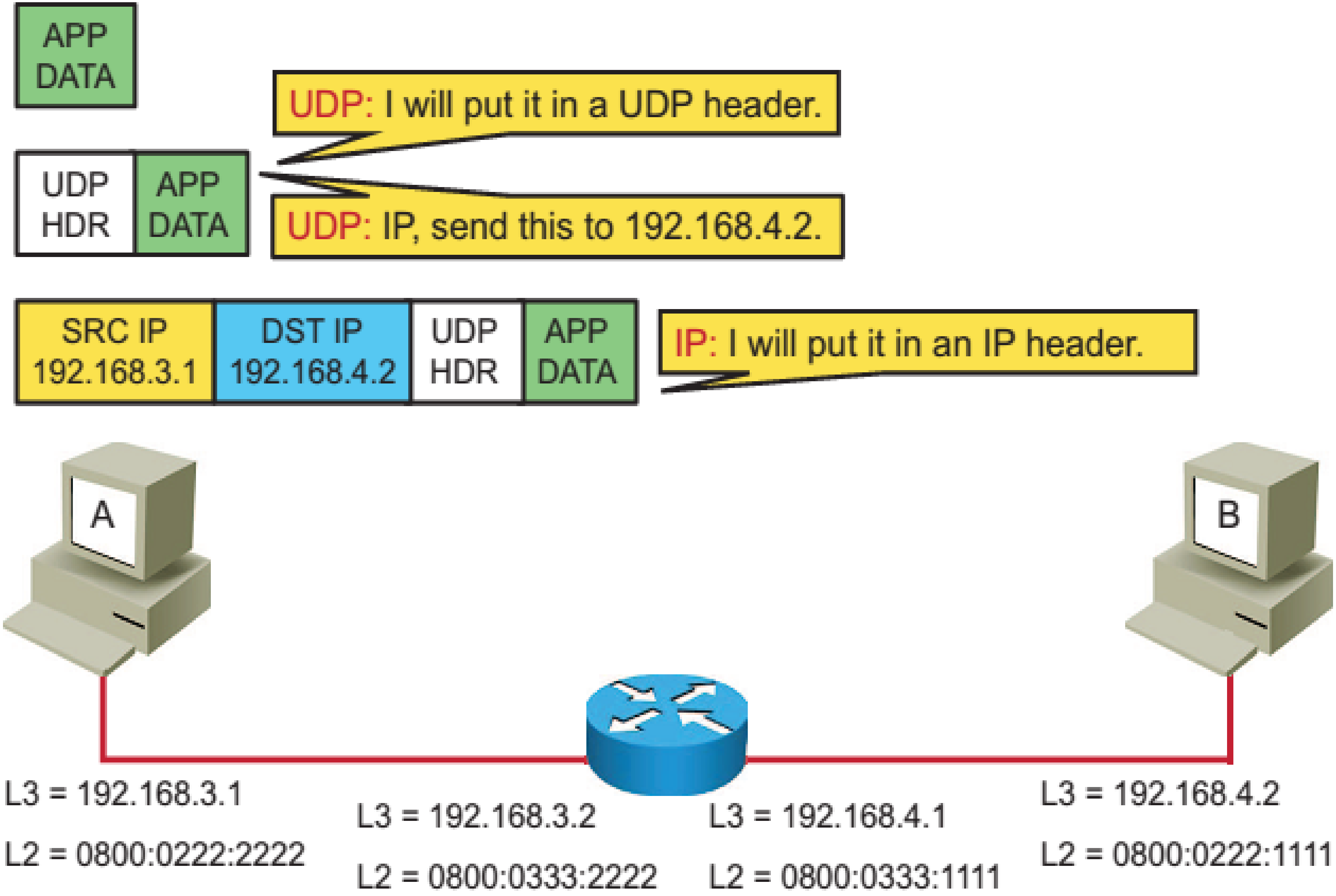
L3 = 192.168.4.1

L2 = 0800:0333:1111

L3 = 192.168.4.2

L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 2 of 16)



APP DATA

UDP: I will put it in a UDP header.

UDP HDR | APP DATA

UDP: IP, send this to 192.168.4.2.

SRC IP 192.168.3.1 | DST IP 192.168.4.2 | UDP HDR | APP DATA

IP: I will put it in an IP header.

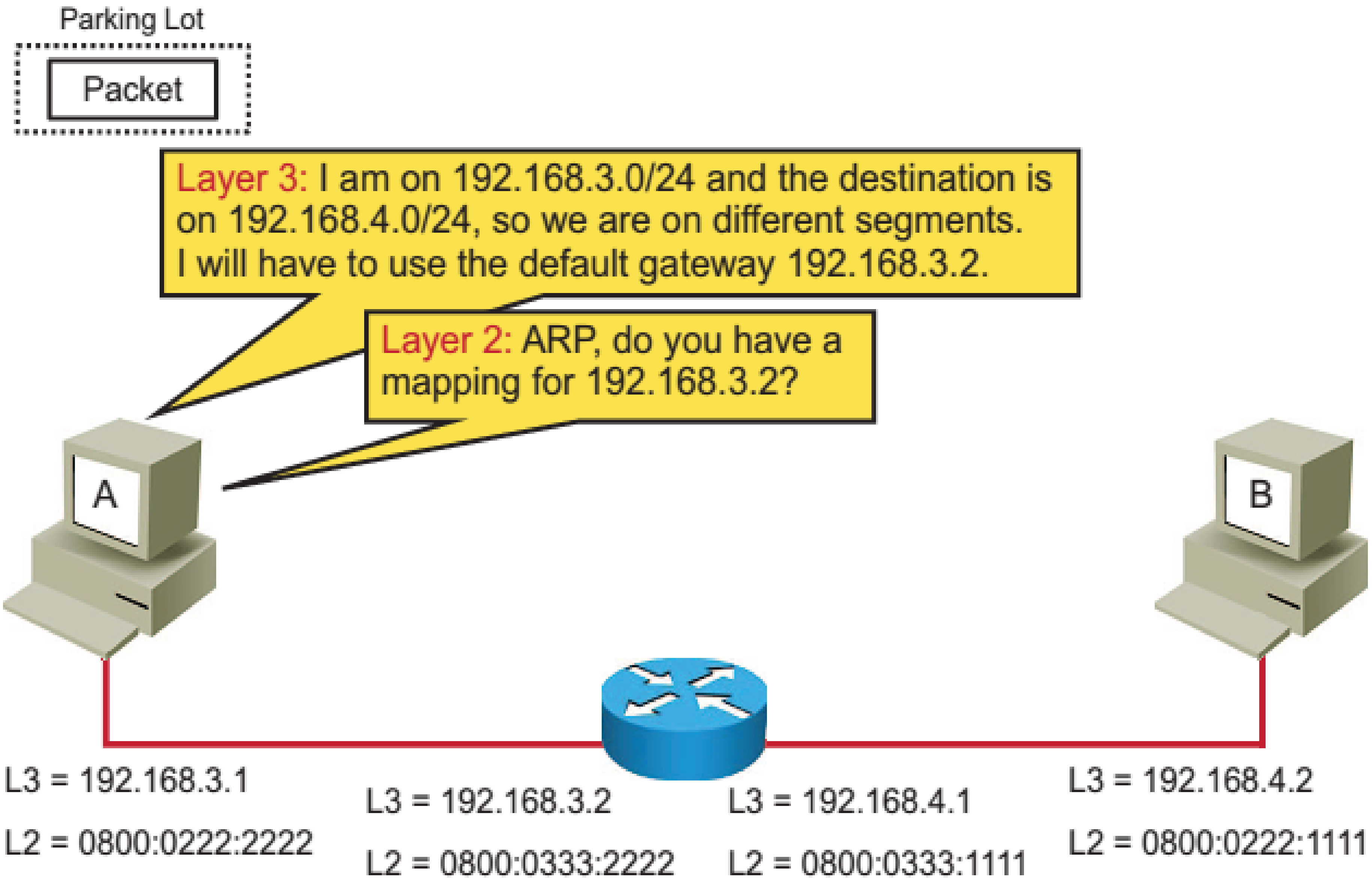
L3 = 192.168.3.1
L2 = 0800:0222:2222

L3 = 192.168.3.2
L2 = 0800:0333:2222

L3 = 192.168.4.1
L2 = 0800:0333:1111

L3 = 192.168.4.2
L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 3 of 16)



Parking Lot

Packet

Layer 3: I am on 192.168.3.0/24 and the destination is on 192.168.4.0/24, so we are on different segments. I will have to use the default gateway 192.168.3.2.

Layer 2: ARP, do you have a mapping for 192.168.3.2?

A

B

L3 = 192.168.3.1

L2 = 0800:0222:2222

L3 = 192.168.3.2

L2 = 0800:0333:2222

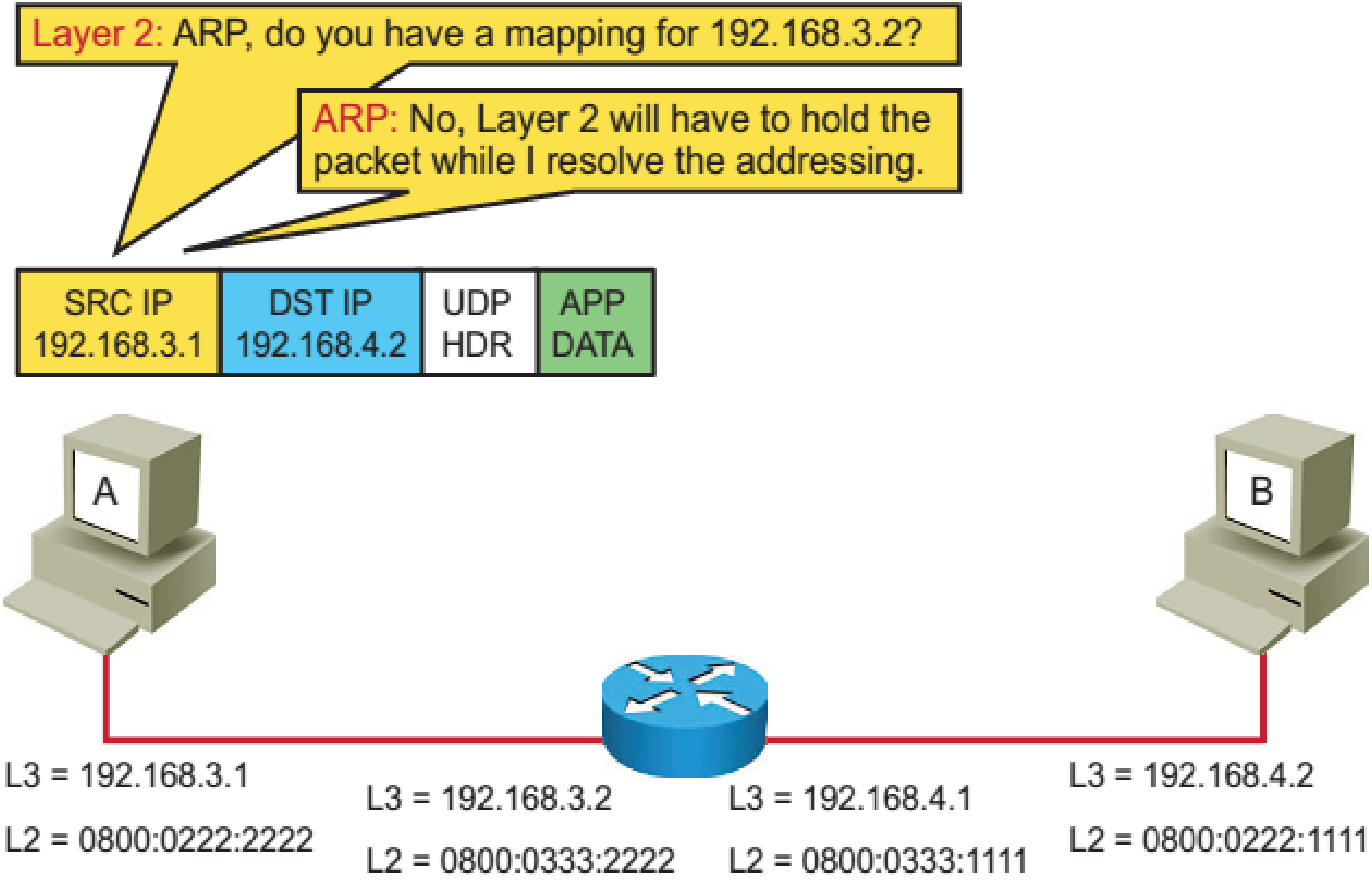
L3 = 192.168.4.1

L2 = 0800:0333:1111

L3 = 192.168.4.2

L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 4 of 16)

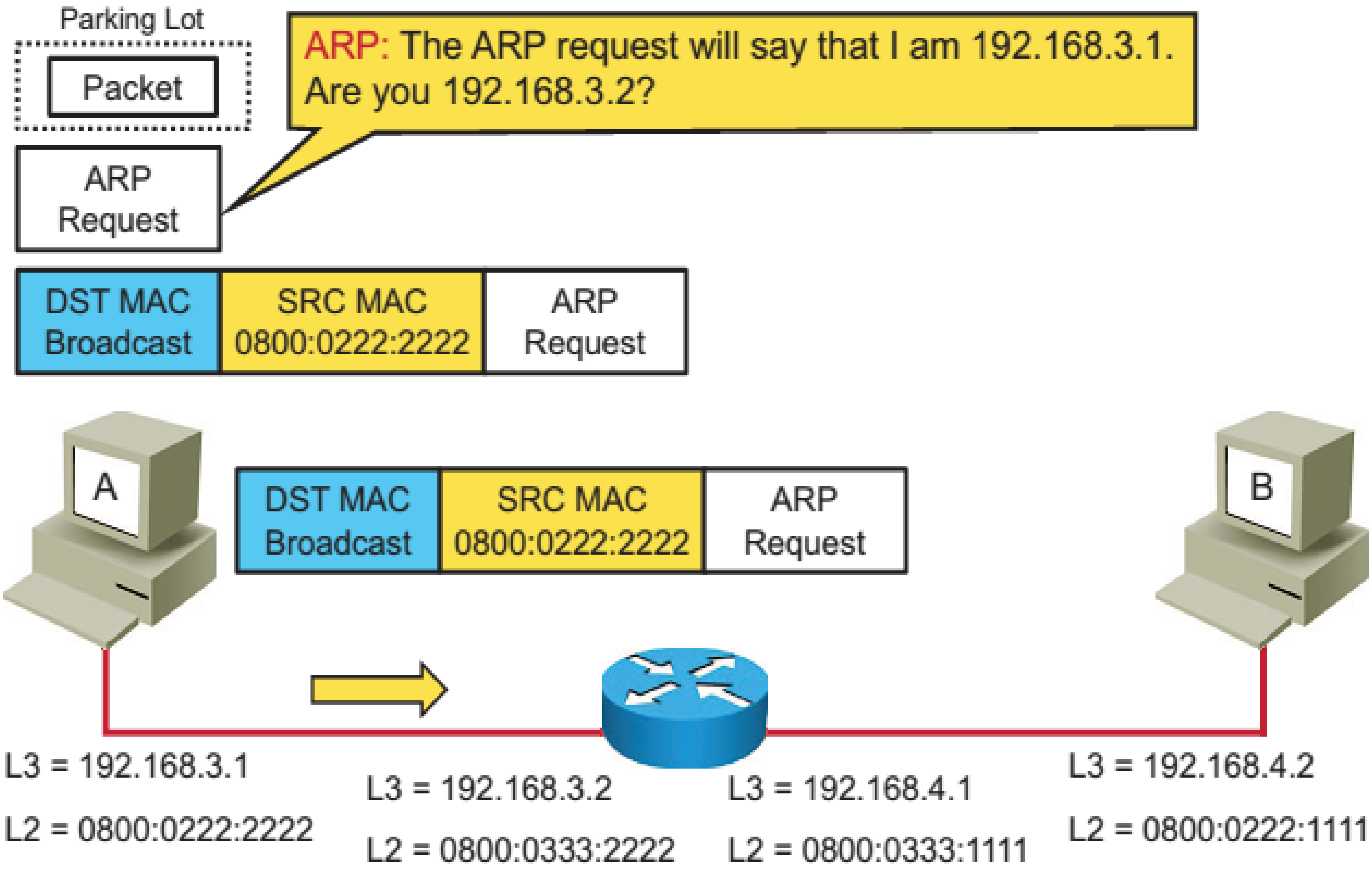


Layer 2: ARP, do you have a mapping for 192.168.3.2?

ARP: No, Layer 2 will have to hold the packet while I resolve the addressing.

SRC IP 192.168.3.1	DST IP 192.168.4.2	UDP HDR	APP DATA

Host-to-Host Packet Delivery (Step 5 of 16)



Parking Lot

Packet

ARP: The ARP request will say that I am 192.168.3.1. Are you 192.168.3.2?

ARP Request

DST MAC Broadcast	SRC MAC 0800:0222:2222	ARP Request

DST MAC Broadcast	SRC MAC 0800:0222:2222	ARP Request

L3 = 192.168.3.1

L2 = 0800:0222:2222

L3 = 192.168.3.2

L2 = 0800:0333:2222

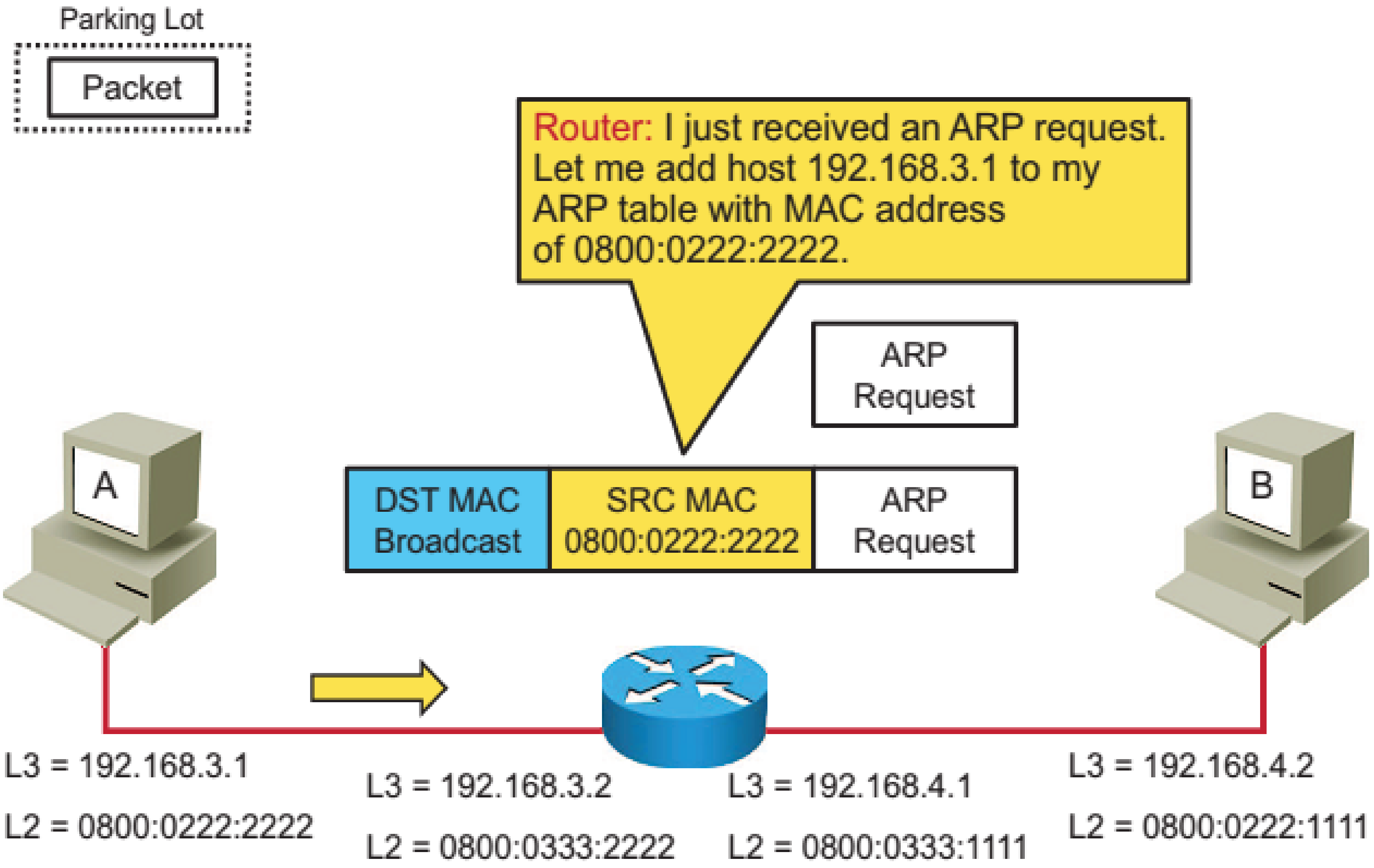
L3 = 192.168.4.1

L2 = 0800:0333:1111

L3 = 192.168.4.2

L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 6 of 16)



Parking Lot

Packet

Router: I just received an ARP request. Let me add host 192.168.3.1 to my ARP table with MAC address of 0800:0222:2222.

ARP Request

DST MAC Broadcast	SRC MAC 0800:0222:2222	ARP Request

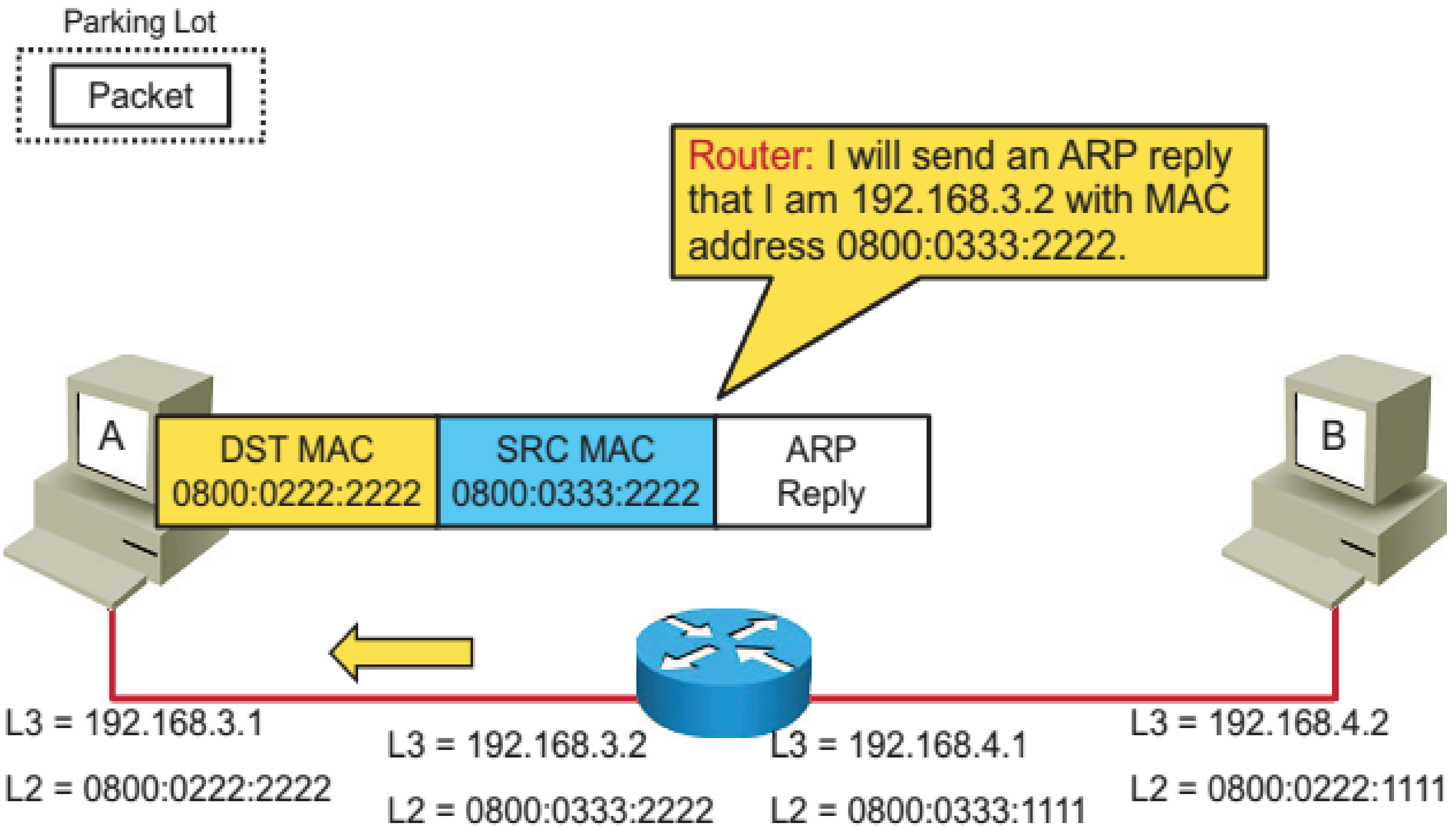
L3 = 192.168.3.1
L2 = 0800:0222:2222

L3 = 192.168.3.2
L2 = 0800:0333:2222

L3 = 192.168.4.1
L2 = 0800:0333:1111

L3 = 192.168.4.2
L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 7 of 16)



Parking Lot

Packet

Router: I will send an ARP reply that I am 192.168.3.2 with MAC address 0800:0333:2222.

A

DST MAC	SRC MAC	ARP
0800:0222:2222	0800:0333:2222	Reply

B

L3 = 192.168.3.1

L2 = 0800:0222:2222

L3 = 192.168.3.2

L2 = 0800:0333:2222

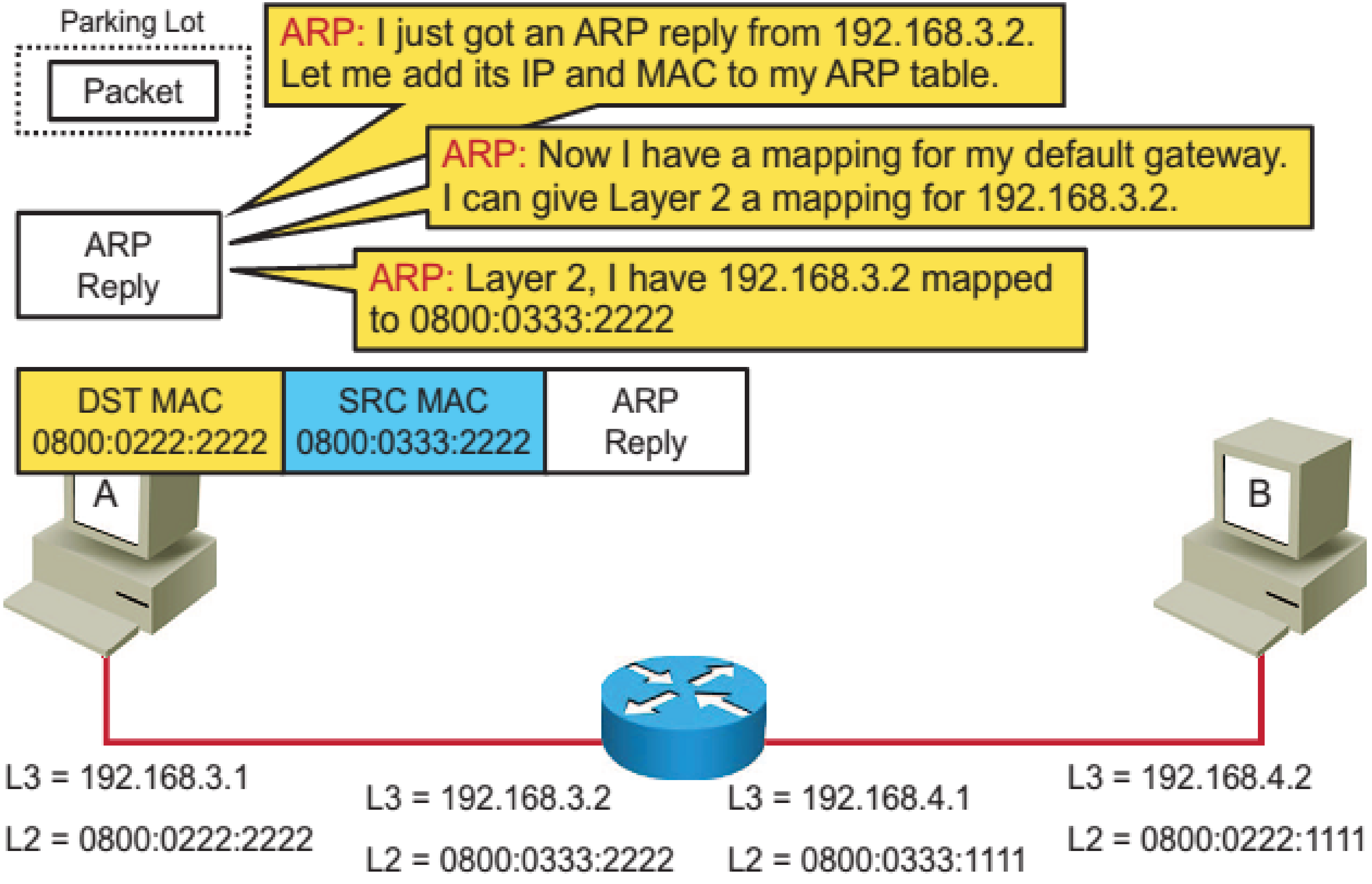
L3 = 192.168.4.1

L2 = 0800:0333:1111

L3 = 192.168.4.2

L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 8 of 16)



Parking Lot

Packet

ARP Reply

ARP: I just got an ARP reply from 192.168.3.2. Let me add its IP and MAC to my ARP table.

ARP: Now I have a mapping for my default gateway. I can give Layer 2 a mapping for 192.168.3.2.

ARP: Layer 2, I have 192.168.3.2 mapped to 0800:0333:2222

DST MAC	SRC MAC	ARP
0800:0222:2222	0800:0333:2222	Reply

L3 = 192.168.3.1
L2 = 0800:0222:2222

L3 = 192.168.3.2
L2 = 0800:0333:2222

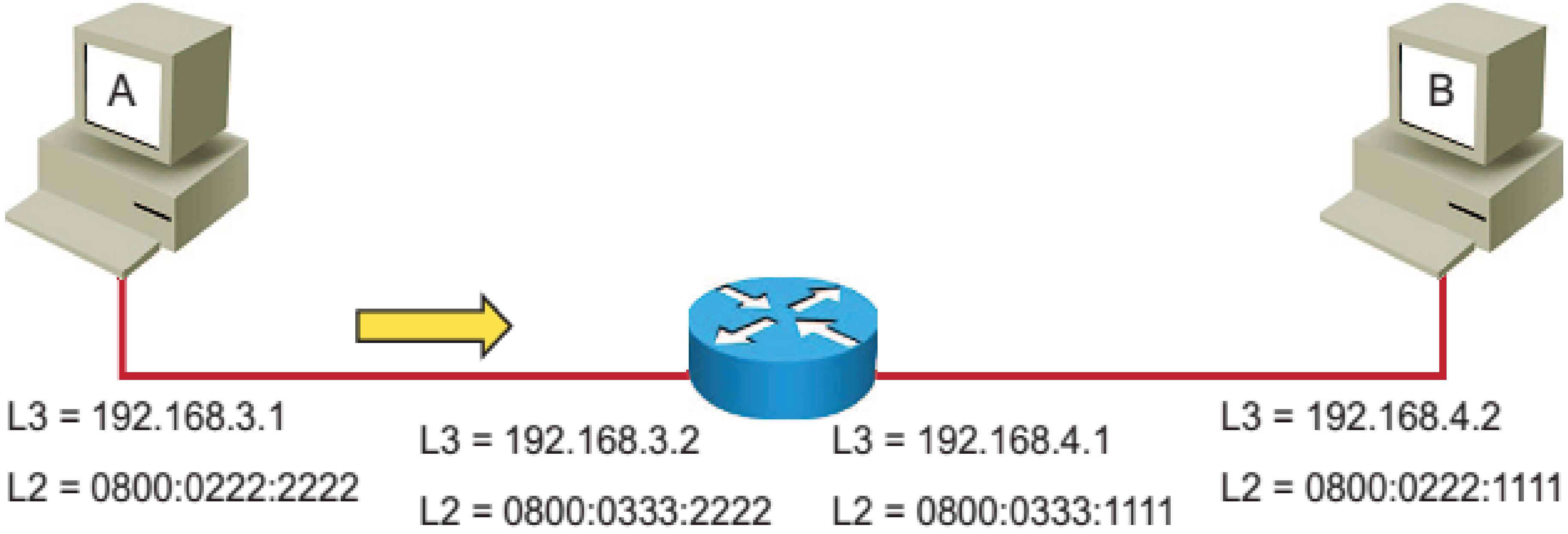
L3 = 192.168.4.1
L2 = 0800:0333:1111

L3 = 192.168.4.2
L2 = 0800:0222:1111

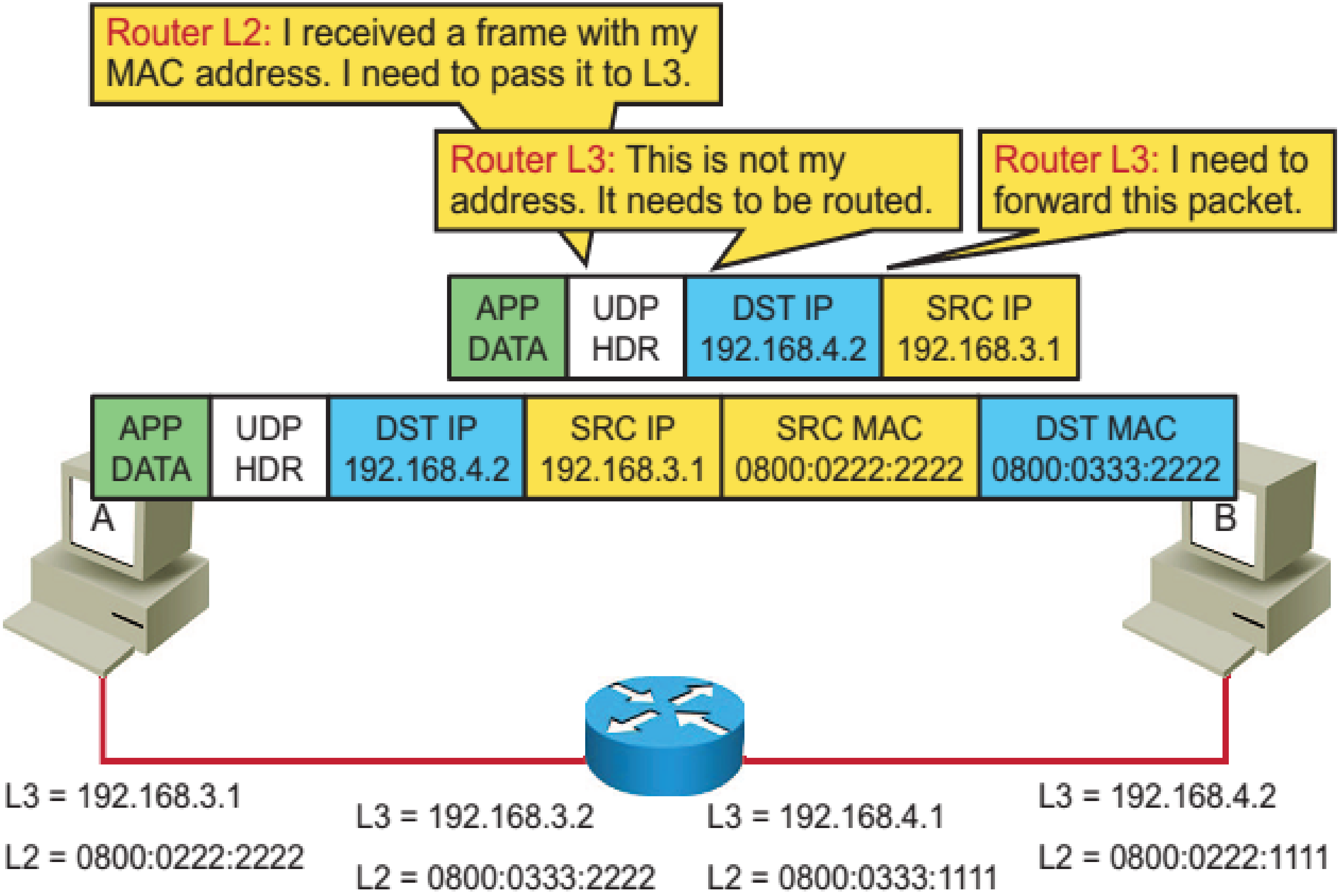
Host-to-Host Packet Delivery (Step 9 of 16)

Layer 2: I can send out that pending frame.

APP DATA	UDP HDR	DST IP 192.168.4.2	SRC IP 192.168.3.1	SRC MAC 0800:0222:2222	DST MAC 0800:0333:2222



Host-to-Host Packet Delivery (Step 10 of 16)



Router L2: I received a frame with my MAC address. I need to pass it to L3.

Router L3: This is not my address. It needs to be routed.

Router L3: I need to forward this packet.

APP DATA	UDP HDR	DST IP	SRC IP
		192.168.4.2	192.168.3.1

APP DATA	UDP HDR	DST IP	SRC IP	SRC MAC	DST MAC
		192.168.4.2	192.168.3.1	0800:0222:2222	0800:0333:2222

L3 = 192.168.3.1
L2 = 0800:0222:2222

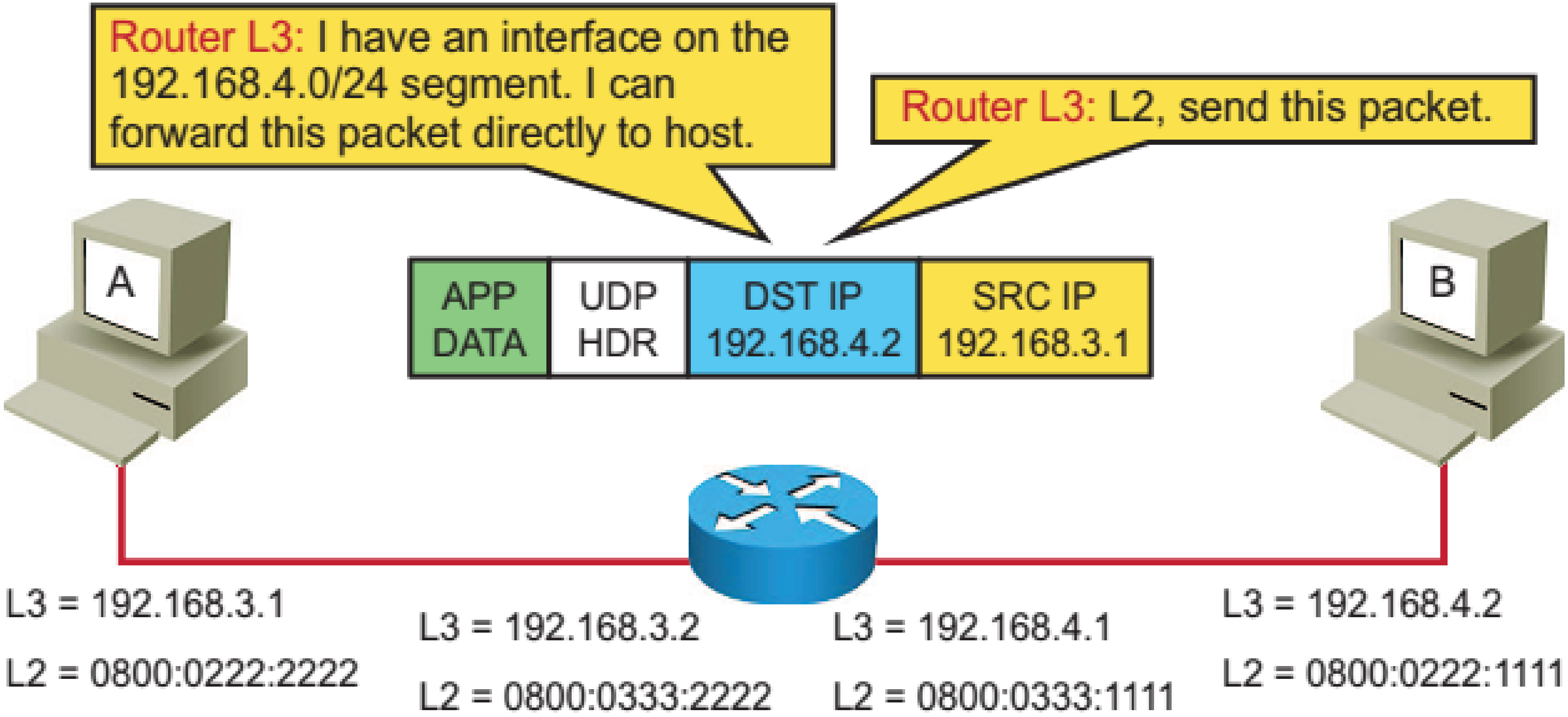
L3 = 192.168.3.2
L2 = 0800:0333:2222

L3 = 192.168.4.1
L2 = 0800:0333:1111

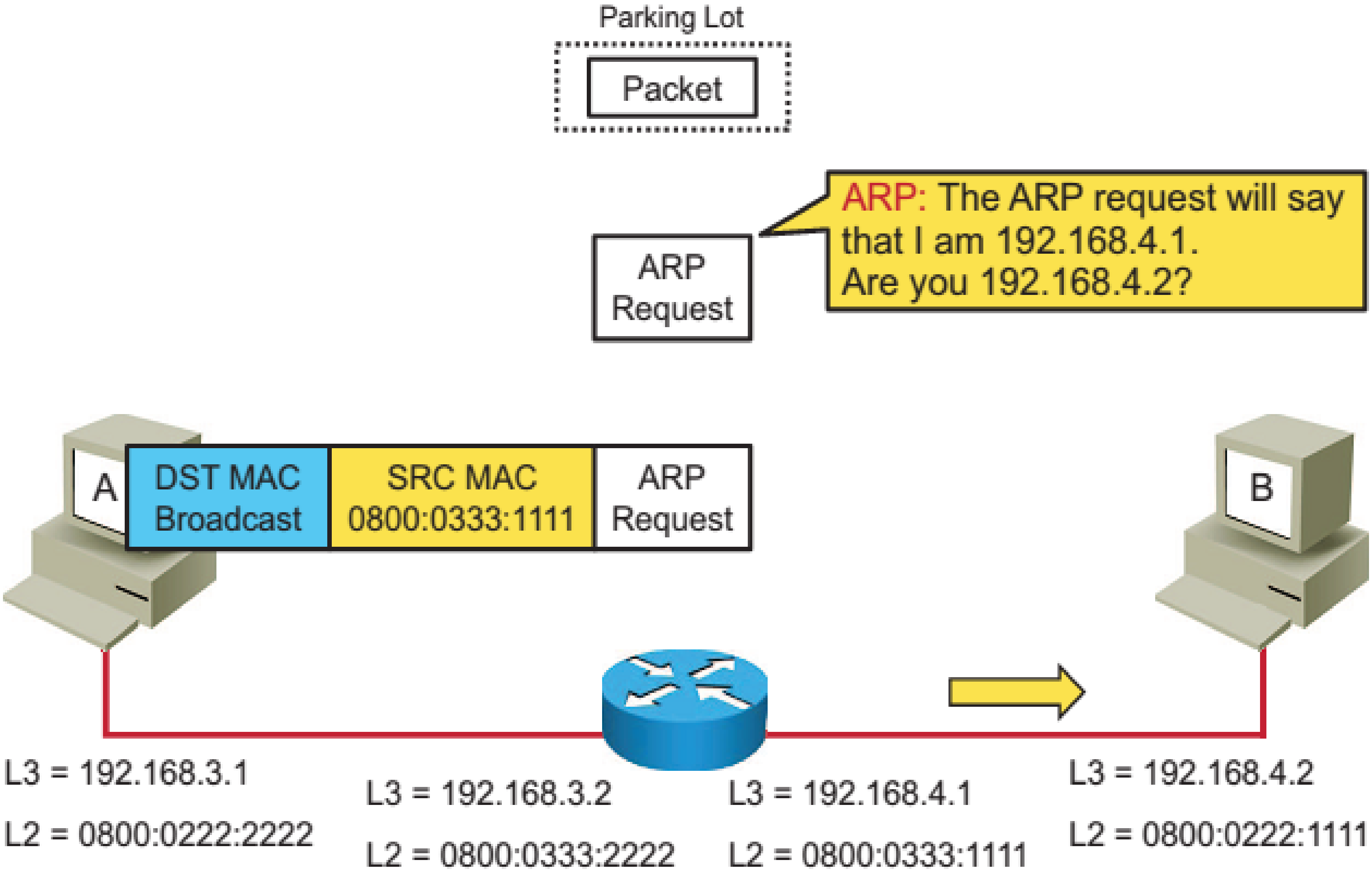
L3 = 192.168.4.2
L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 11 of 16)

Destination	Next Hop	Interface
192.168.3.0/24	Connected	Gi 0/0
192.168.4.0/24	Connected	Gi 0/1

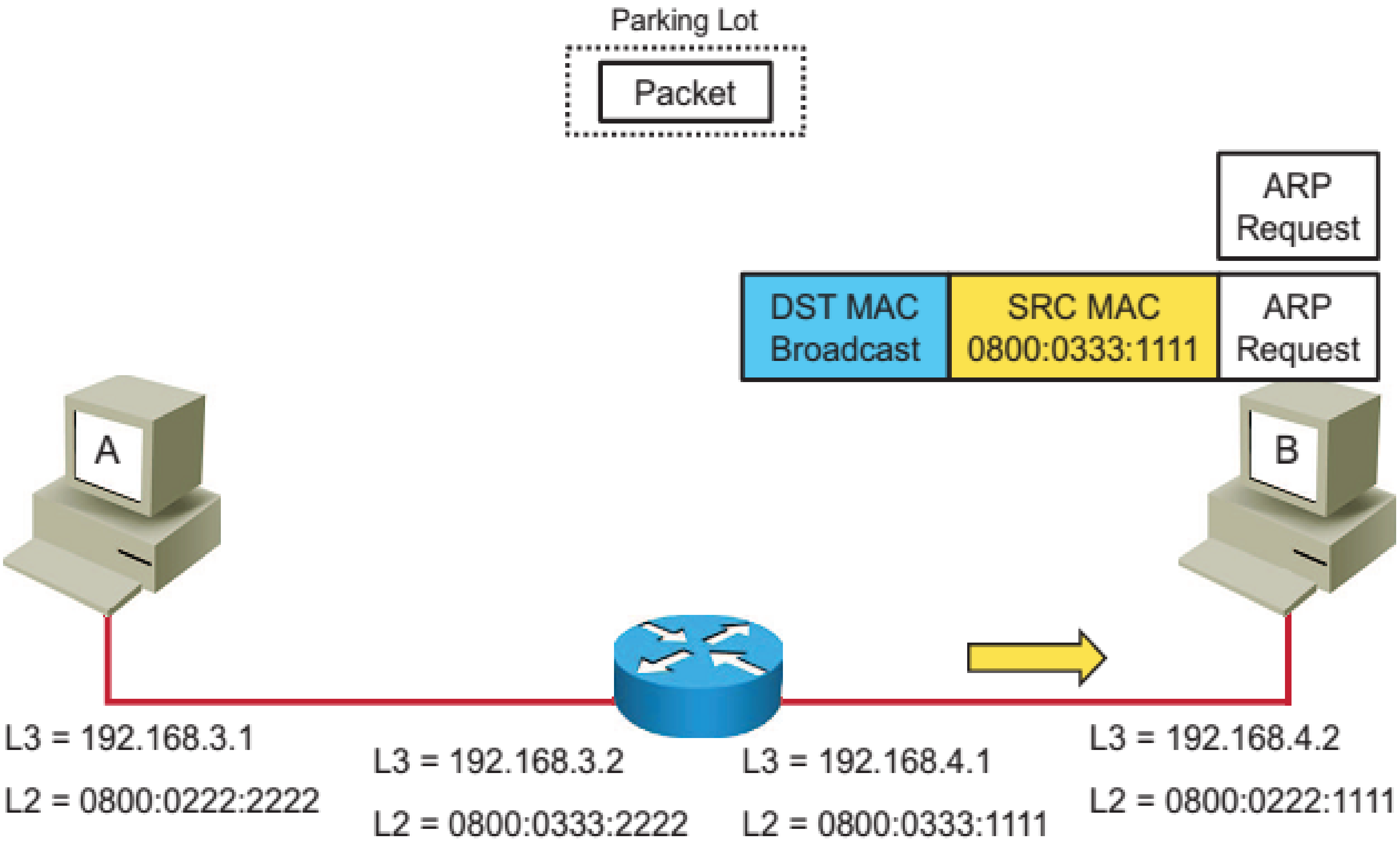


Host-to-Host Packet Delivery (Step 12 of 16)

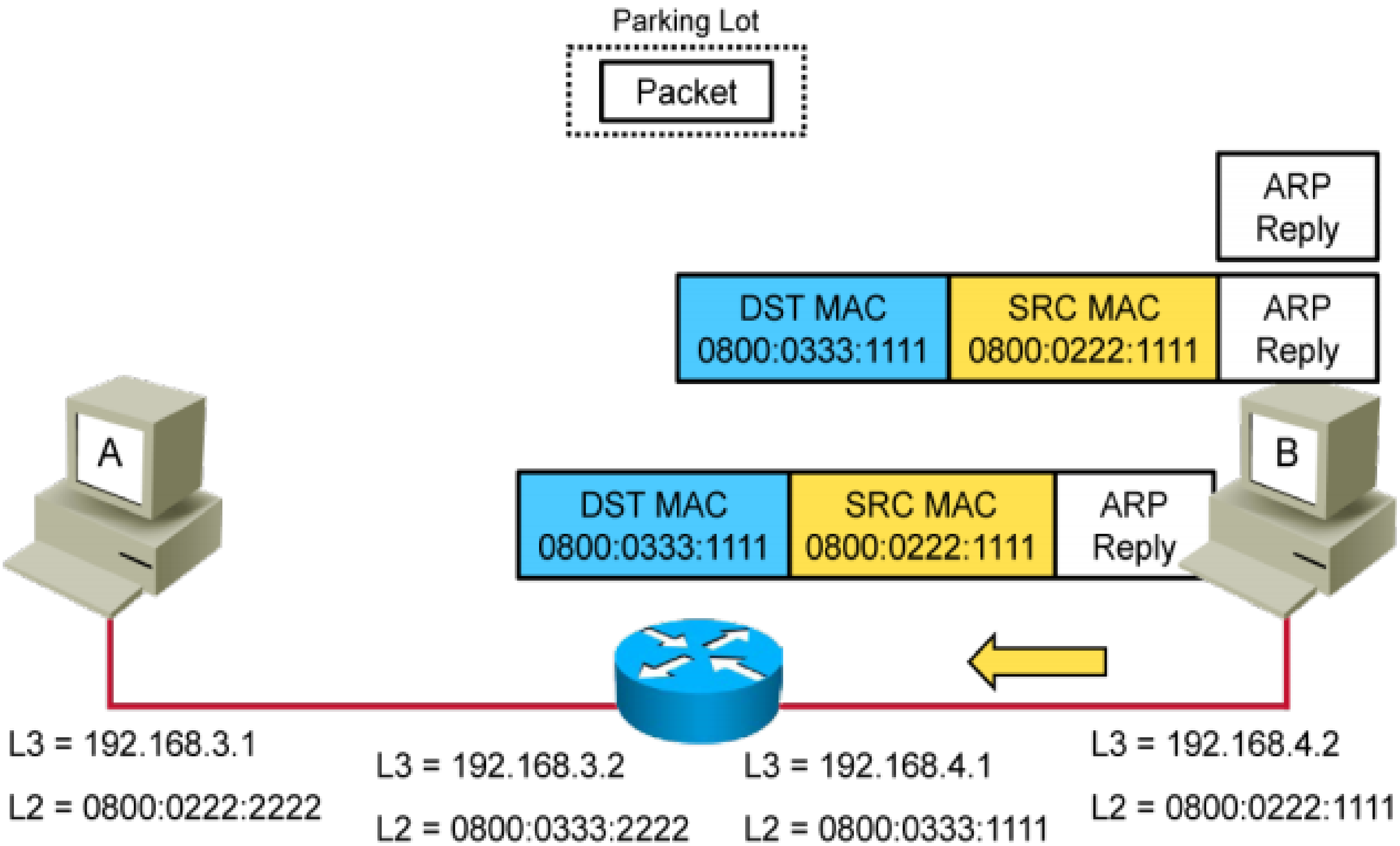


ARP: The ARP request will say that I am 192.168.4.1. Are you 192.168.4.2?

Host-to-Host Packet Delivery (Step 13 of 16)



Host-to-Host Packet Delivery (Step 14 of 16)



Parking Lot

Packet

ARP Reply

DST MAC 0800:0333:1111 | SRC MAC 0800:0222:1111 | ARP Reply

DST MAC 0800:0333:1111 | SRC MAC 0800:0222:1111 | ARP Reply

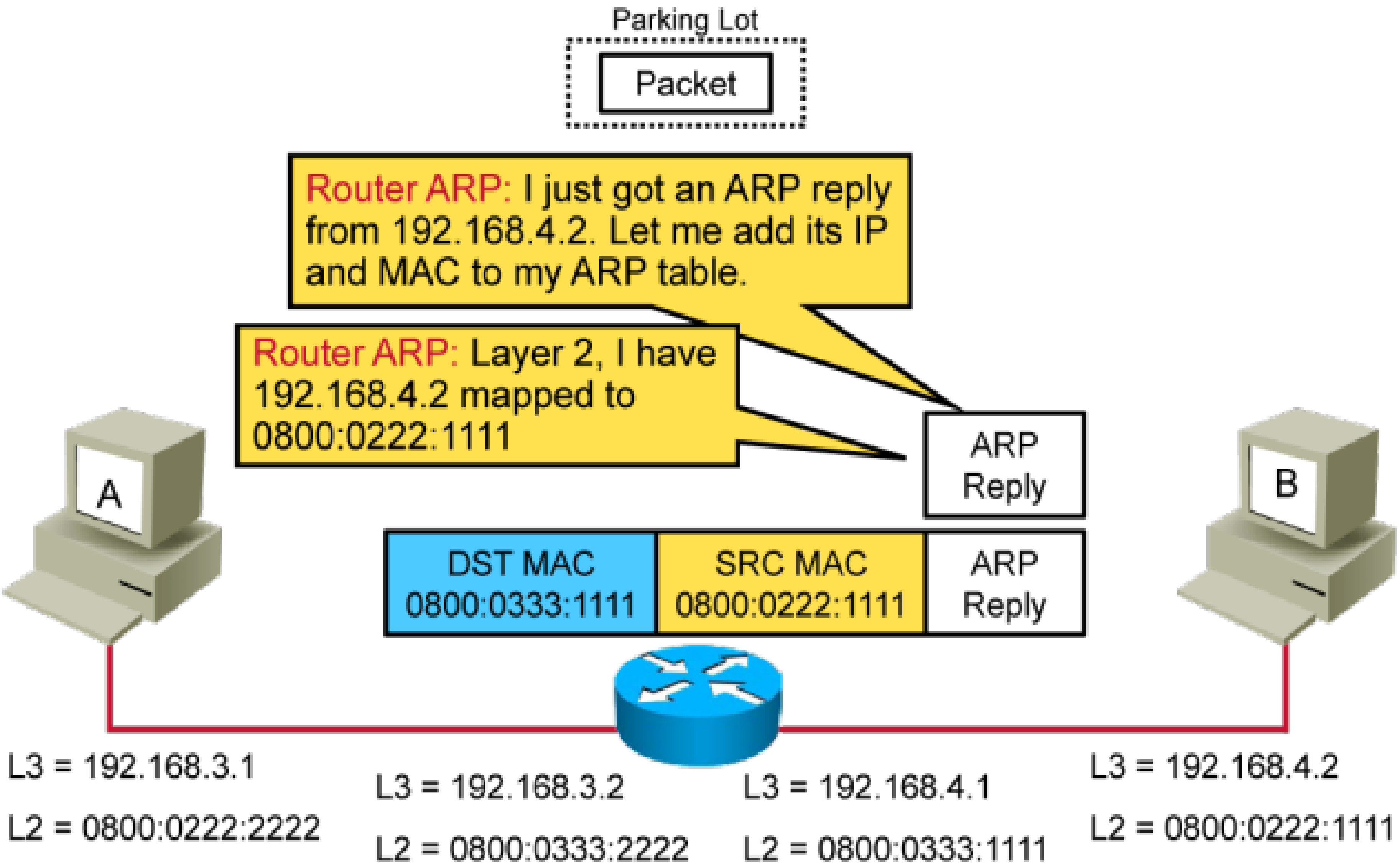
L3 = 192.168.3.1
L2 = 0800:0222:2222

L3 = 192.168.3.2
L2 = 0800:0333:2222

L3 = 192.168.4.1
L2 = 0800:0333:1111

L3 = 192.168.4.2
L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 15 of 16)



Parking Lot

Packet

Router ARP: I just got an ARP reply from 192.168.4.2. Let me add its IP and MAC to my ARP table.

Router ARP: Layer 2, I have 192.168.4.2 mapped to 0800:0222:1111

ARP Reply

DST MAC 0800:0333:1111	SRC MAC 0800:0222:1111	ARP Reply

A

B

L3 = 192.168.3.1

L2 = 0800:0222:2222

L3 = 192.168.3.2

L2 = 0800:0333:2222

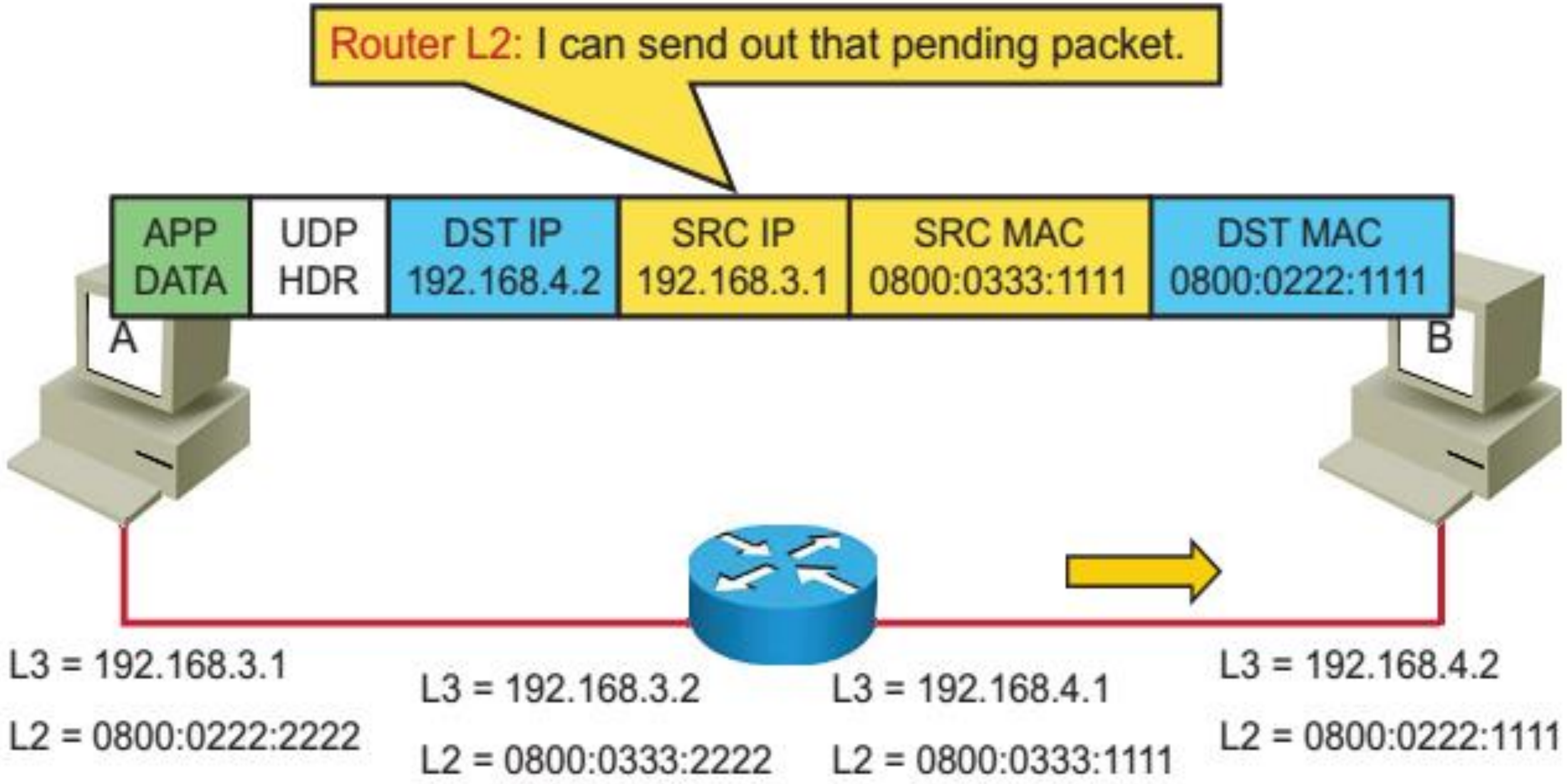
L3 = 192.168.4.1

L2 = 0800:0333:1111

L3 = 192.168.4.2

L2 = 0800:0222:1111

Host-to-Host Packet Delivery (Step 16 of 16)



Router L2: I can send out that pending packet.

APP DATA	UDP HDR	DST IP	SRC IP	SRC MAC	DST MAC
		192.168.4.2	192.168.3.1	0800:0333:1111	0800:0222:1111

L3 = 192.168.3.1
L2 = 0800:0222:2222

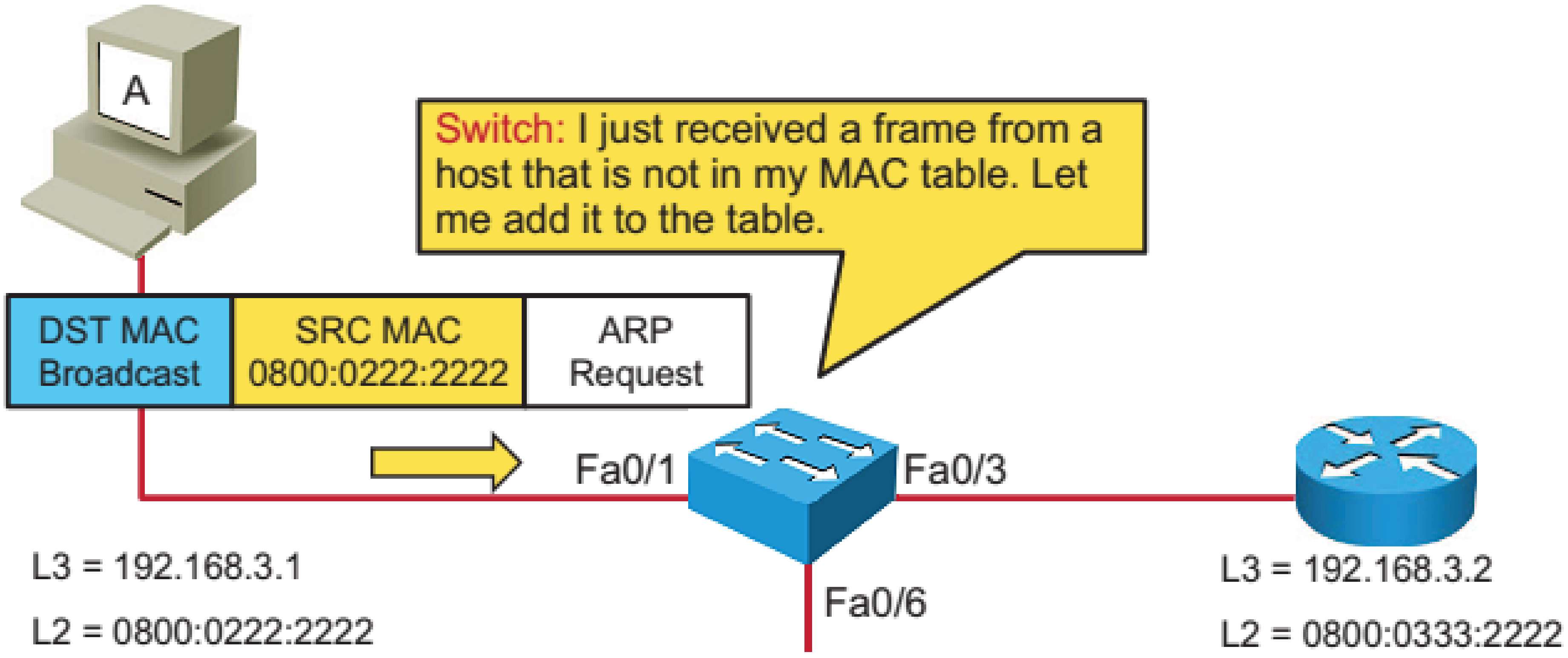
L3 = 192.168.3.2
L2 = 0800:0333:2222

L3 = 192.168.4.1
L2 = 0800:0333:1111

L3 = 192.168.4.2
L2 = 0800:0222:1111

Role of a Switch in Packet Delivery (Step 1 of 4)

MAC	Port
0800:0222:2222	Fa0/1



Switch: I just received a frame from a host that is not in my MAC table. Let me add it to the table.

DST MAC	SRC MAC	ARP
Broadcast	0800:0222:2222	Request

L3 = 192.168.3.1

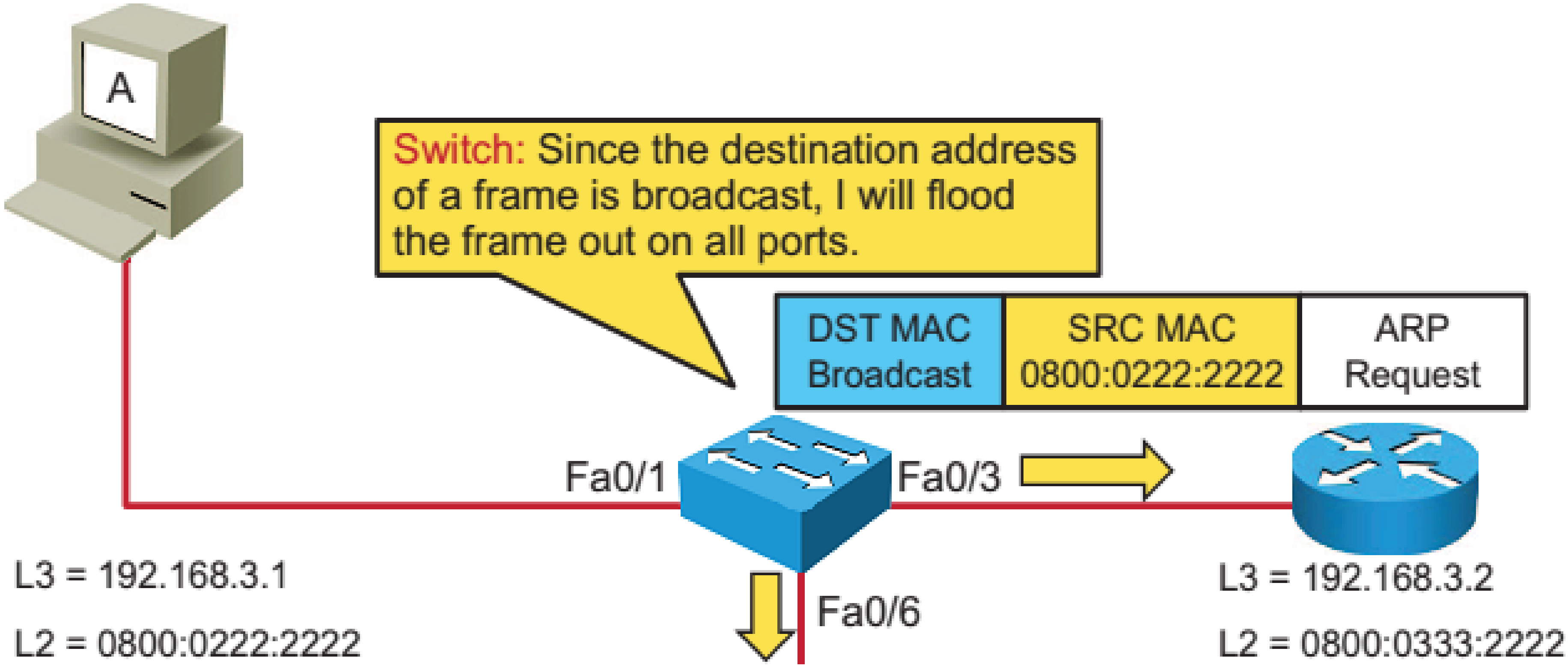
L2 = 0800:0222:2222

L3 = 192.168.3.2

L2 = 0800:0333:2222

Role of a Switch in Packet Delivery (Step 2 of 4)

MAC	Port
0800:0222:2222	Fa0/1

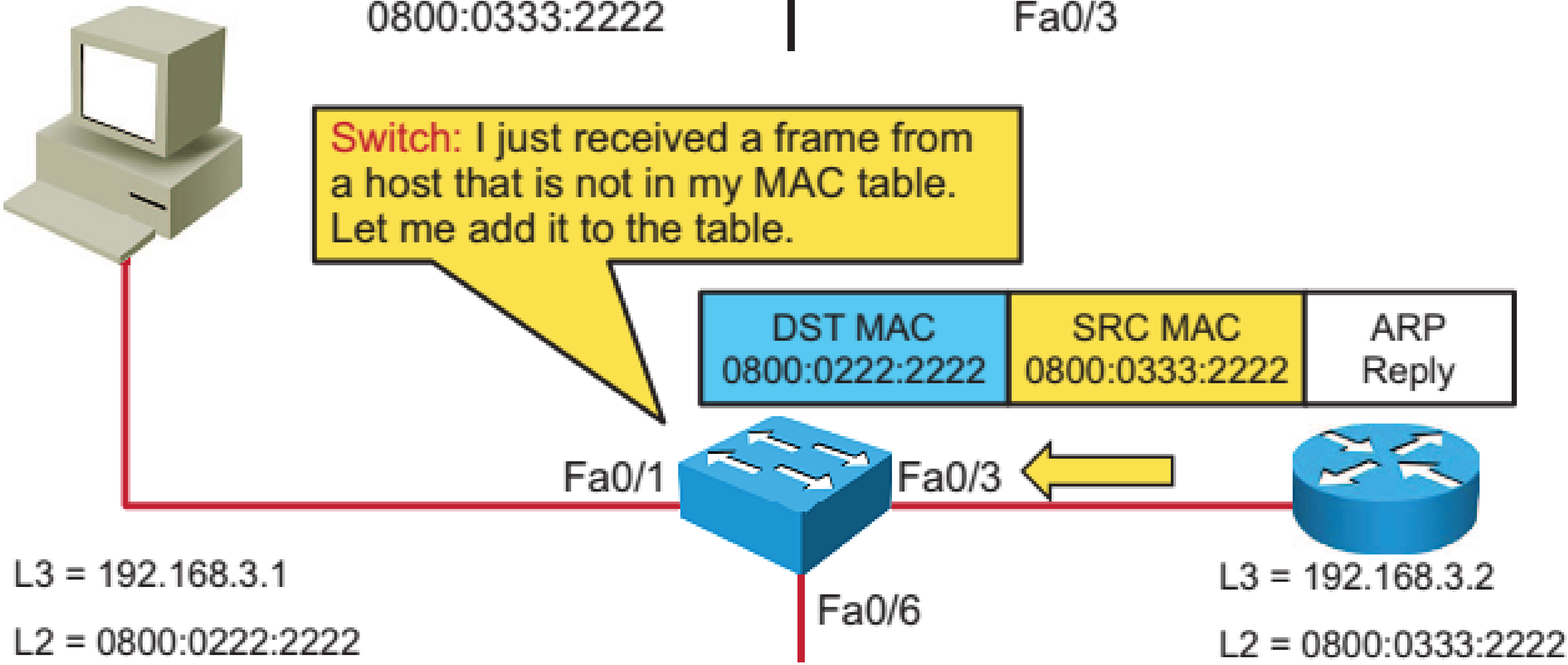


Switch: Since the destination address of a frame is broadcast, I will flood the frame out on all ports.

DST MAC	SRC MAC	ARP
Broadcast	0800:0222:2222	Request

Role of a Switch in Packet Delivery (Step 3 of 4)

MAC	Port
0800:0222:2222	Fa0/1
0800:0333:2222	Fa0/3

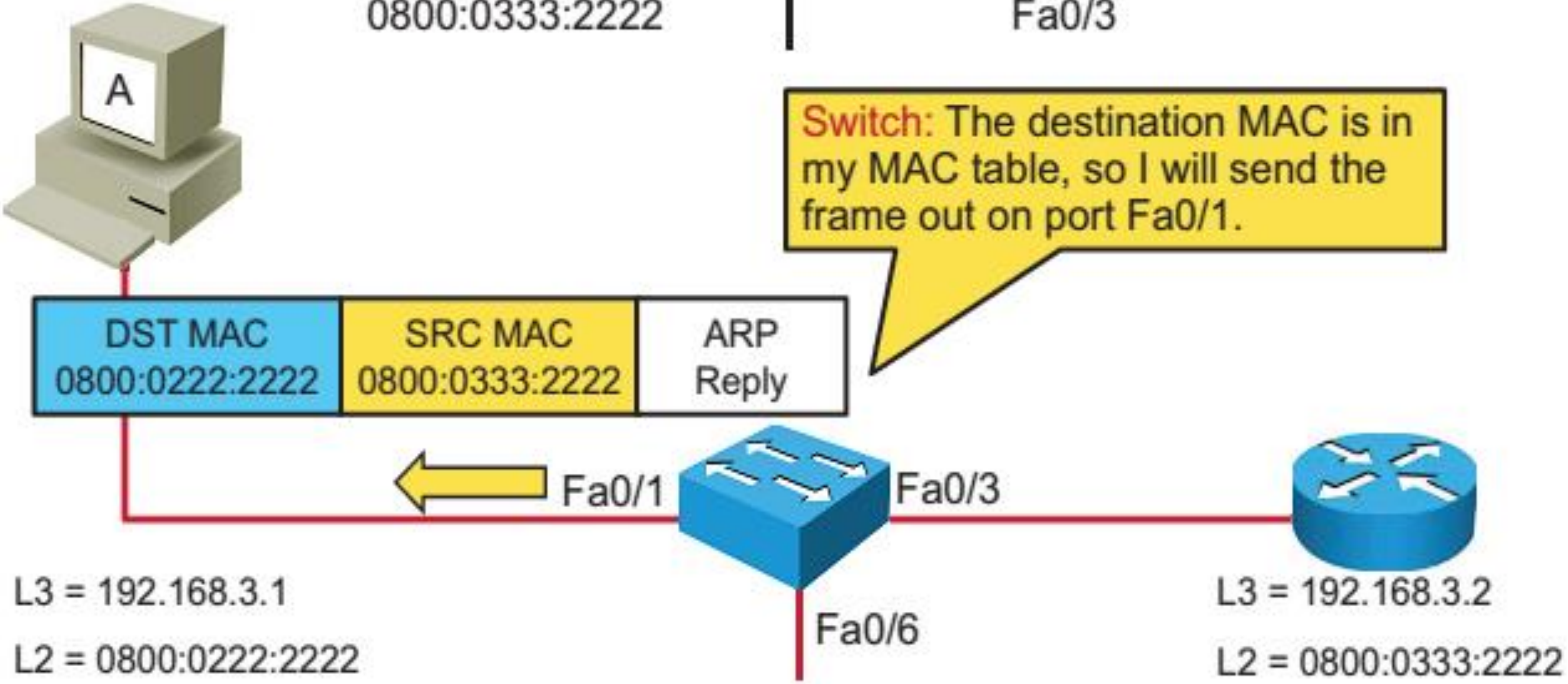


Switch: I just received a frame from a host that is not in my MAC table. Let me add it to the table.

DST MAC	SRC MAC	ARP
0800:0222:2222	0800:0333:2222	Reply

Role of a Switch in Packet Delivery (Step 4 of 4)

MAC	Port
0800:0222:2222	Fa0/1
0800:0333:2222	Fa0/3



Switch: The destination MAC is in my MAC table, so I will send the frame out on port Fa0/1.