Establishing Internet Connectivity

Interconnecting Cisco Networking Devices, Part 1 (ICND1) v2.0

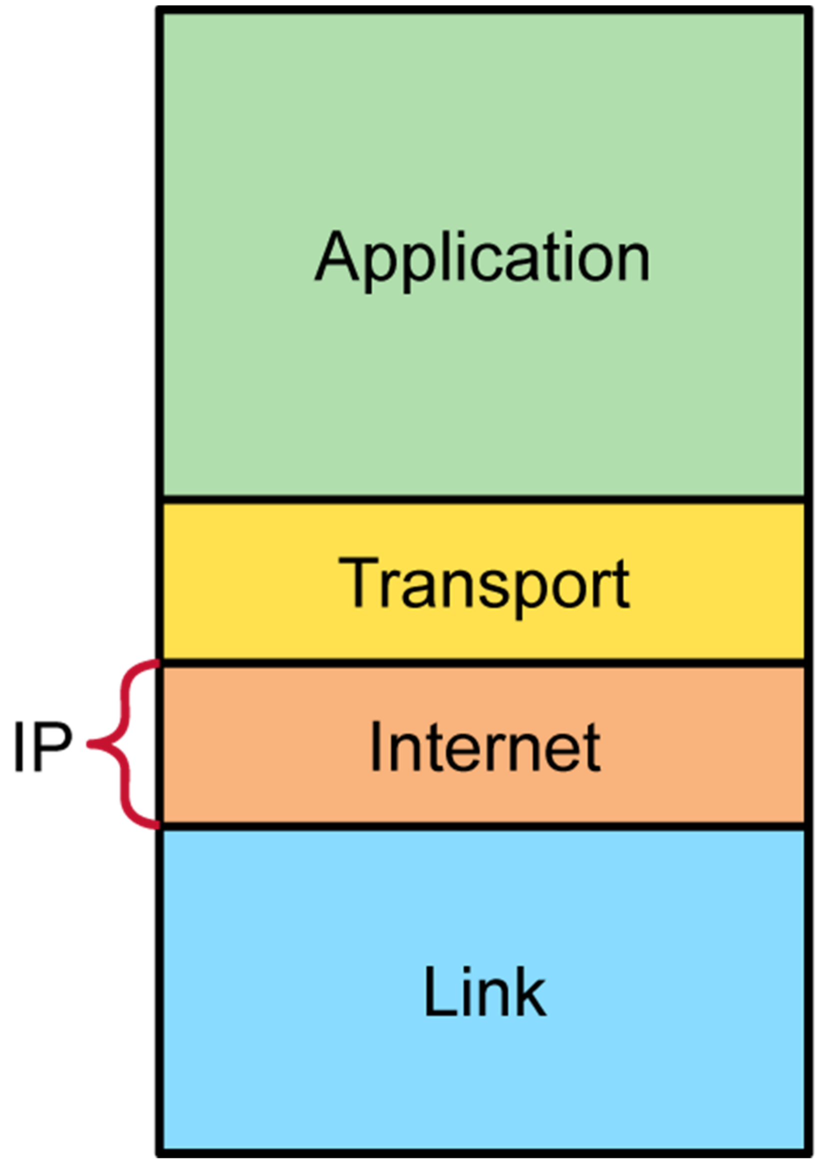
Understanding the TCP/IP Internet Layer

Establishing Internet Connectivity

Internet Protocol

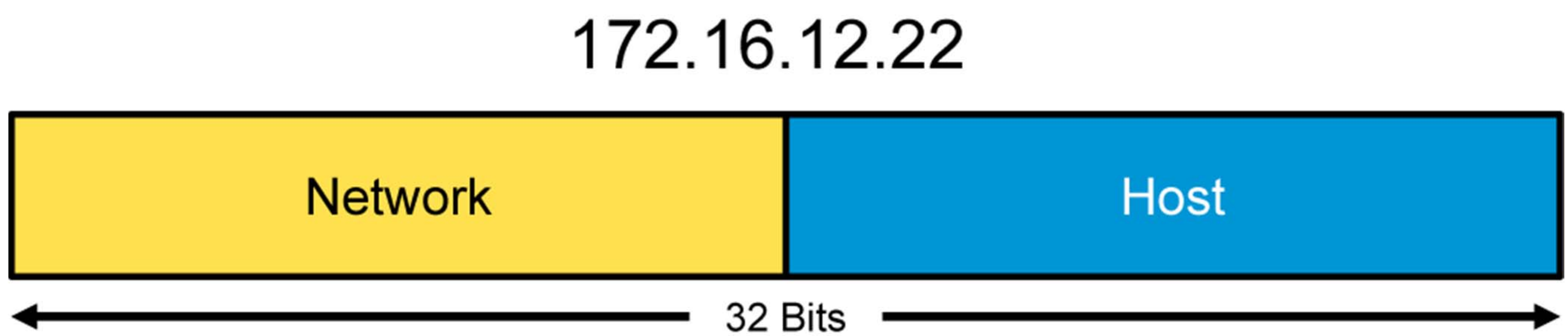
IP characteristics:

- Operates at the internet layer of the TCP/IP stack
- Connectionless protocol
- Packets treated independently
- Hierarchical addressing
- Best-effort delivery
- No data-recovery features
- Media-independent
- Two variants: IPv4 and IPv6



IPv4 Address Representation

- Every host (computer, networking device, peripheral) must have a unique address.
- An IP address consists of two parts:
  – Network ID:
    - Identifies the network of which the host is a part
    - Used by routers to maintain information about routes
  – Host ID:
    - Identifies the individual host
    - Assigned by organizations to individual devices



IPv4 Header Address Fields

<table>
<tr><td>Ver.</td><td>IHL</td><td colspan="2">Service Type</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td>Flag</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="7">Source Address</td></tr>
<tr><td colspan="7">Destination Address</td></tr>
<tr><td colspan="6">Options</td><td>Padding</td></tr>
</table>

Decimal and Binary Systems

- Decimal numbers are represented by the numbers 0 through 9.
- Binary numbers are represented by a series of 1s and 0s.

Decimal	Binary
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001

Decimal	Binary
10	1010
11	1011
12	1100
13	1101
14	1110
15	1111
16	10000
17	10001
18	10010
19	10011

Decimal-to-Binary Conversion

Base^{Exponent}	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Place Value	128	64	32	16	8	4	2	1
Example: Convert decimal 35 to binary	0	0	1	0	0	0	1	1
35 =	(2^7*0) +	(2^6*0) +	(2^5*1) +	(2^4*0) +	(2^3*0) +	(2^2*0) +	(2^1*1) +	(2^0*1)
35 =			(32*1)		+		(2*1) + (1*1)	
35 =	0 + 0 + 1 + 0 + 0 + 0 + 1 + 1							
35 = ***<u>00100011</u>***								

IP Address Classes

A B C … Easy as 1 2 3

Class A … First 1 Bit Fixed	0 x x x x x x x	Host	Host	Host
Class B … First 2 Bits Fixed	1 0 x x x x x x	Network	Host	Host
Class C … First 3 Bits Fixed	1 1 0 x x x x x	Network	Network	Host

IP Address Classes (Cont.)

IP Address Ranges			
IP Address Class	**First Octet Decimal Value**	**First Octet Binary Value**	**Possible Number of Hosts**
Class A	1–126	00000001 to 01111110*	16,777,214
Class B	128–191	10000000 to 10111111	65,534
Class C	192–223	11000000 to 11011111	254

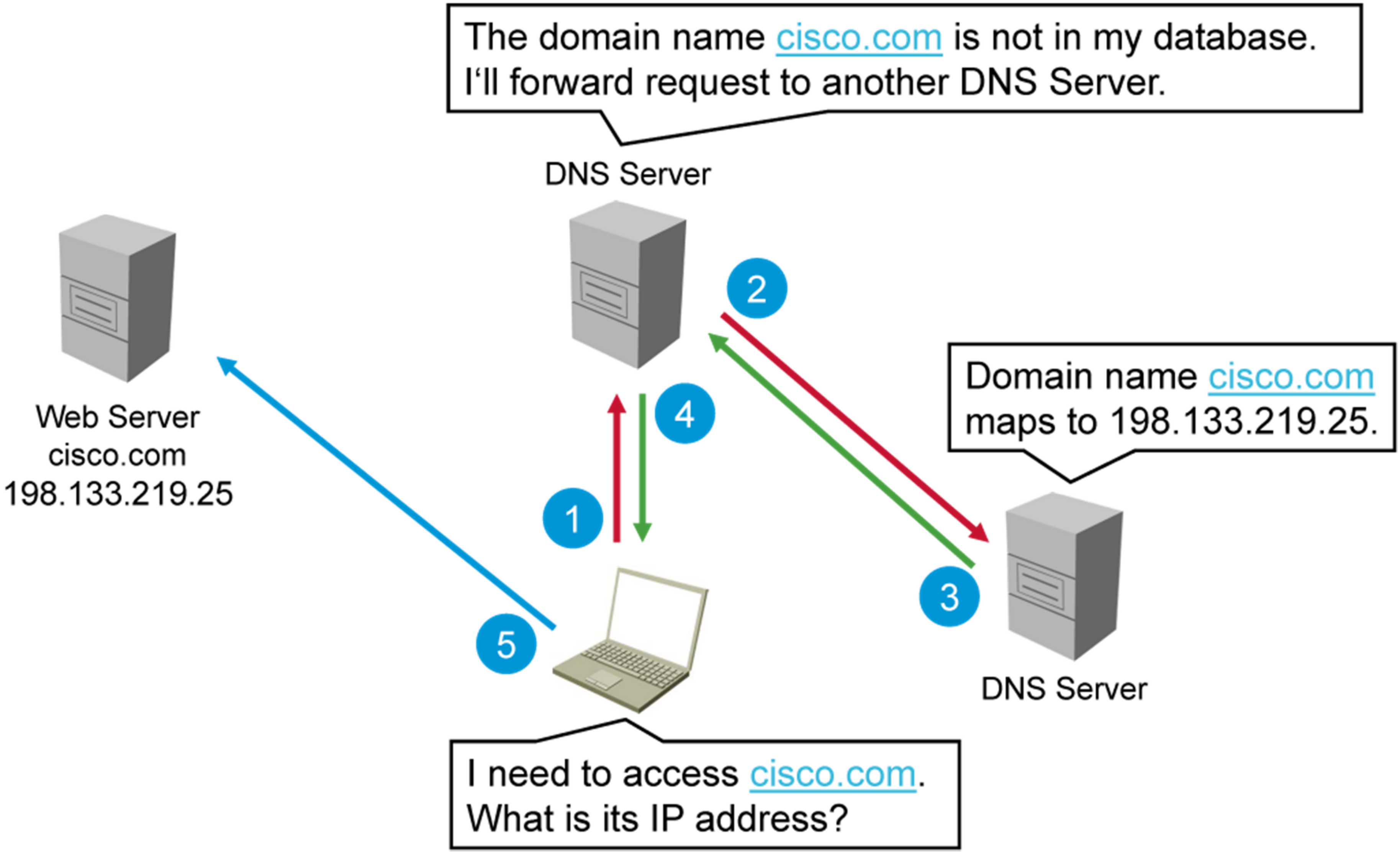
*127 (01111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.

Reserved IPv4 Address

These are reserved IPv4 addresses:

- Network address
- Directed broadcast address
- Local broadcast address
- Local loopback address
- All zeros address

Domain Name System



Verifying the IPv4 Address of a Host

Windows Platform

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : PCUSER
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . :

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/1000 PL Network Connection
        Physical Address. . . . . . . . . : 00-15-58-2F-21-E6
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.102
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 127.107.241.185
                                            127.135.250.69
        Lease Obtained. . . . . . . . . . : Wednesday, April 25, 2007 12:27:51 AM
        Lease Expires . . . . . . . . . . : Thursday, April 26, 2007 12:27:51 AM
```

Verifying the IPv4 Address of a Host (Cont.)

Verifying IP address of a switch

```
Switch#show ip interface brief
Interface          IP-Address     OK?  Method  Status   Protocol
Vlan1              10.1.1.11      YES  manual  up       up
FastEthernet0/1    unassigned     YES  unset   up       up
FastEthernet0/2    unassigned     YES  unset   down     down
FastEthernet0/3    unassigned     YES  unset   up       up
FastEthernet0/4    unassigned     YES  unset   up       up
FastEthernet0/5    unassigned     YES  unset   down     down
<output omitted>
```

Summary

- IP is a Layer 3 media-independent connectionless protocol that uses hierarchical logical addressing and provides service in a best-effort manner.
- Every node that is connected to the Internet has a unique IP address that identifies it. An IP address consists of two parts: the network ID and the host ID.
- Every packet that travels through the network contains a source address and a destination address.
- Certain IP addresses (for example, network and broadcast addresses) are reserved and cannot be assigned to individual network devices.
- DNS is an application that is specified in the TCP/IP suite. It provides a means to translate human-readable names into IP addresses.

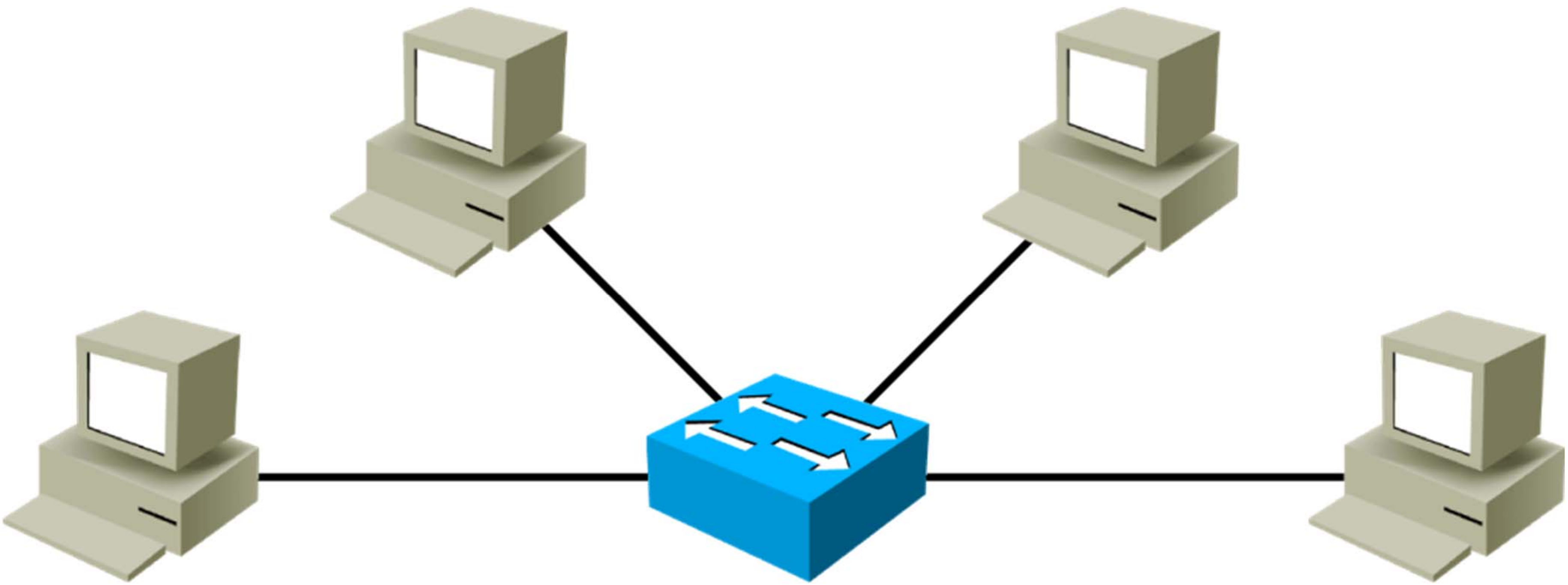
Understanding IP Addressing and Subnets

Establishing Internet Connectivity

Subnets

There can be problems within a single broadcast domain:

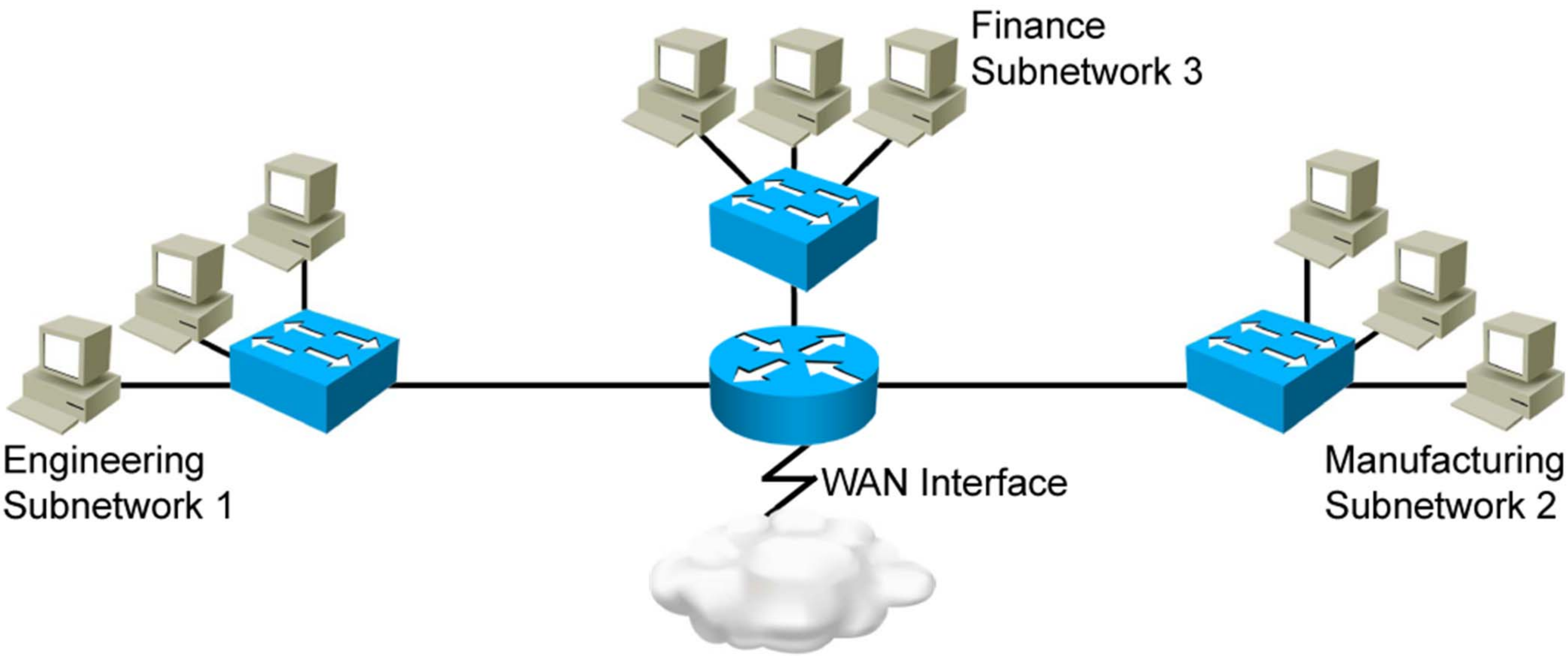
- The domain relies on MAC addresses for packet delivery.
- Larger amounts of broadcast traffic consume resources.
- All devices share the same broadcast domain.



Subnets (Cont.)

Solution: Subnetworks

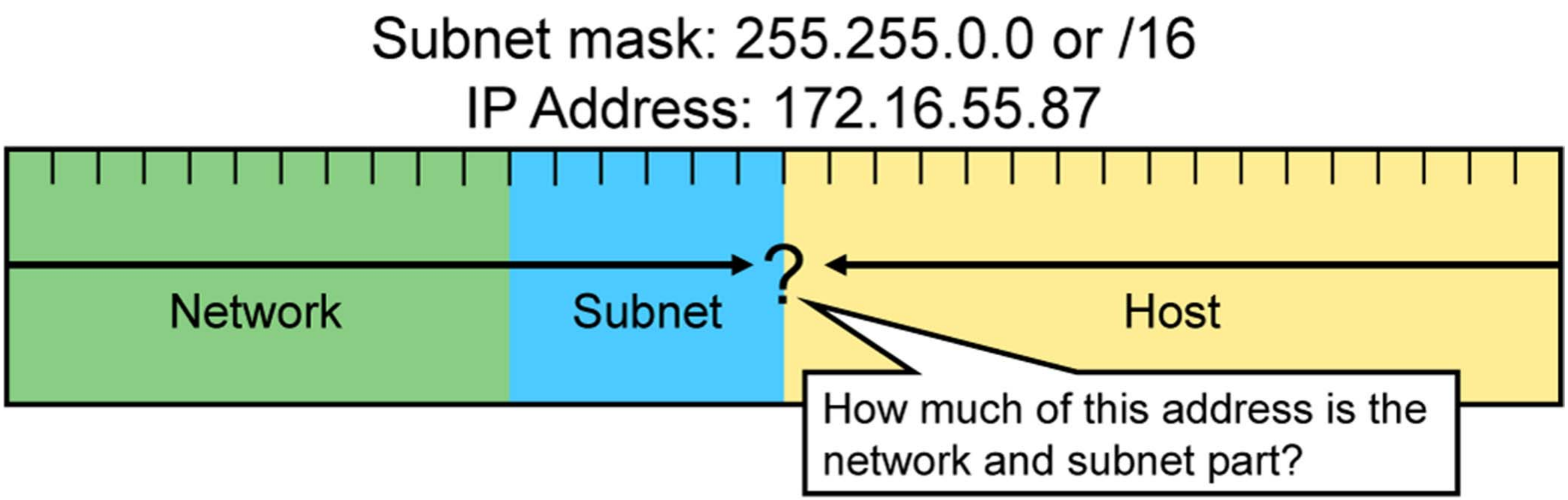
- Smaller networks are easier to manage.
- Overall traffic is reduced.
- You can apply network security policies more easily.



Subnet Masks

A subnet mask:

- Defines the number of bits that represent the network and subnet part of the address
- Used by end systems to identify the destination IP address as either local or remote
- Used by Layer 3 devices to determine network path



Octet Values of a Subnet Mask

- Subnet masks, like IP addresses, are represented in the dotted decimal format, such as 255.255.255.0.
- The binary 1 reflects the network and subnetwork part of the IP address.

Octet Values of a Subnet Mask (Cont.)

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

Octet Values of a Subnet Mask (Cont.)

Default Subnet Masks, Class A

Example Class A address (decimal):	10.0.0.0
Example Class A address (binary):	00001010.00000000.00000000.00000000
Default Class A mask (binary):	11111111.00000000.00000000.00000000
Default Class A mask (decimal):	255.0.0.0
Default classful prefix length:	/8

Octet Values of a Subnet Mask (Cont.)

Default Subnet Masks, Class B

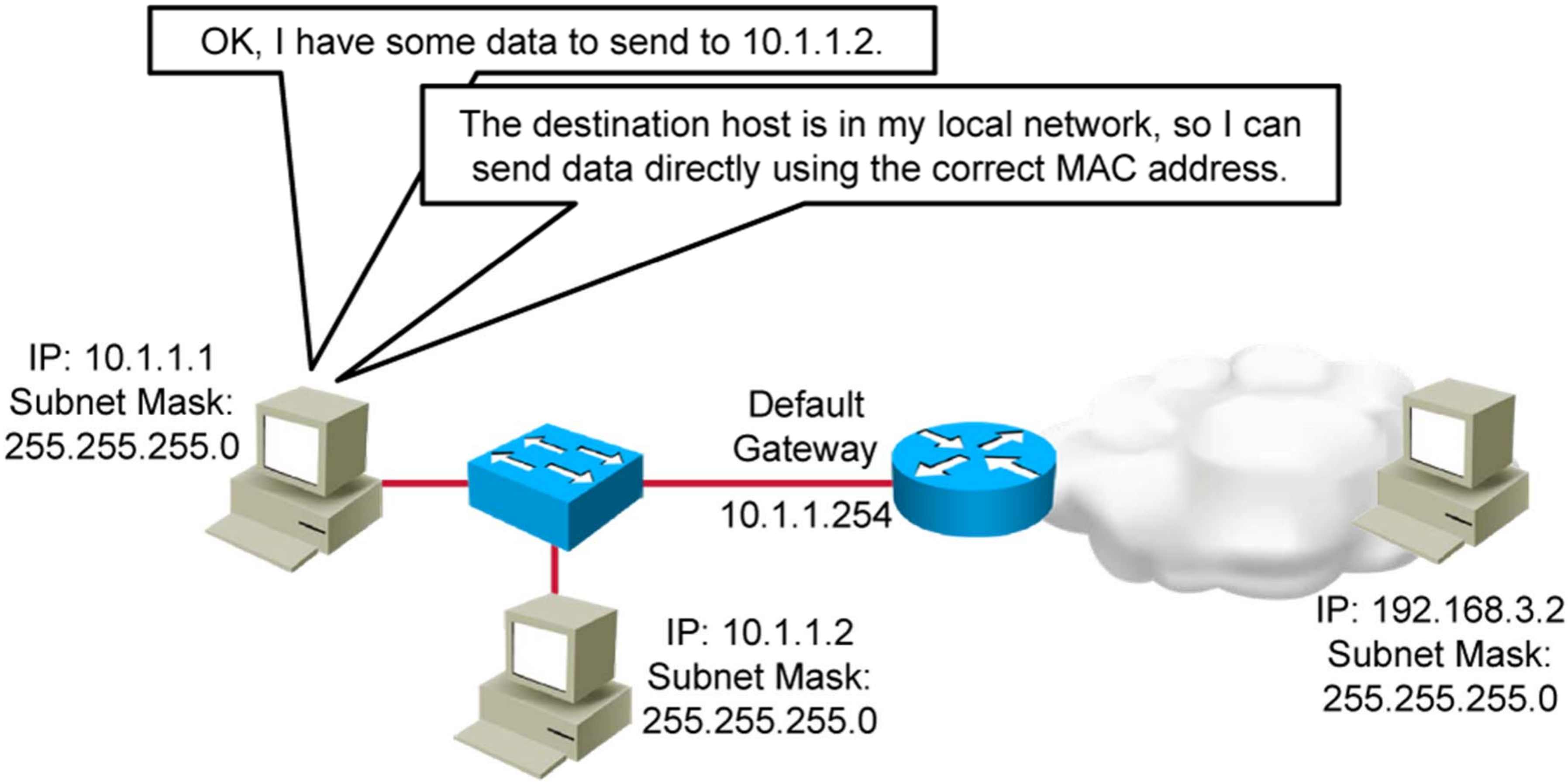
Example Class B address (decimal):	172.16.0.0
Example Class B address (binary):	10101100.00010000.00000000.00000000
Default Class B mask (binary):	11111111.11111111.00000000.00000000
Default Class B mask (decimal):	255.255.0.0
Default classful prefix length:	/16

Octet Values of a Subnet Mask (Cont.)

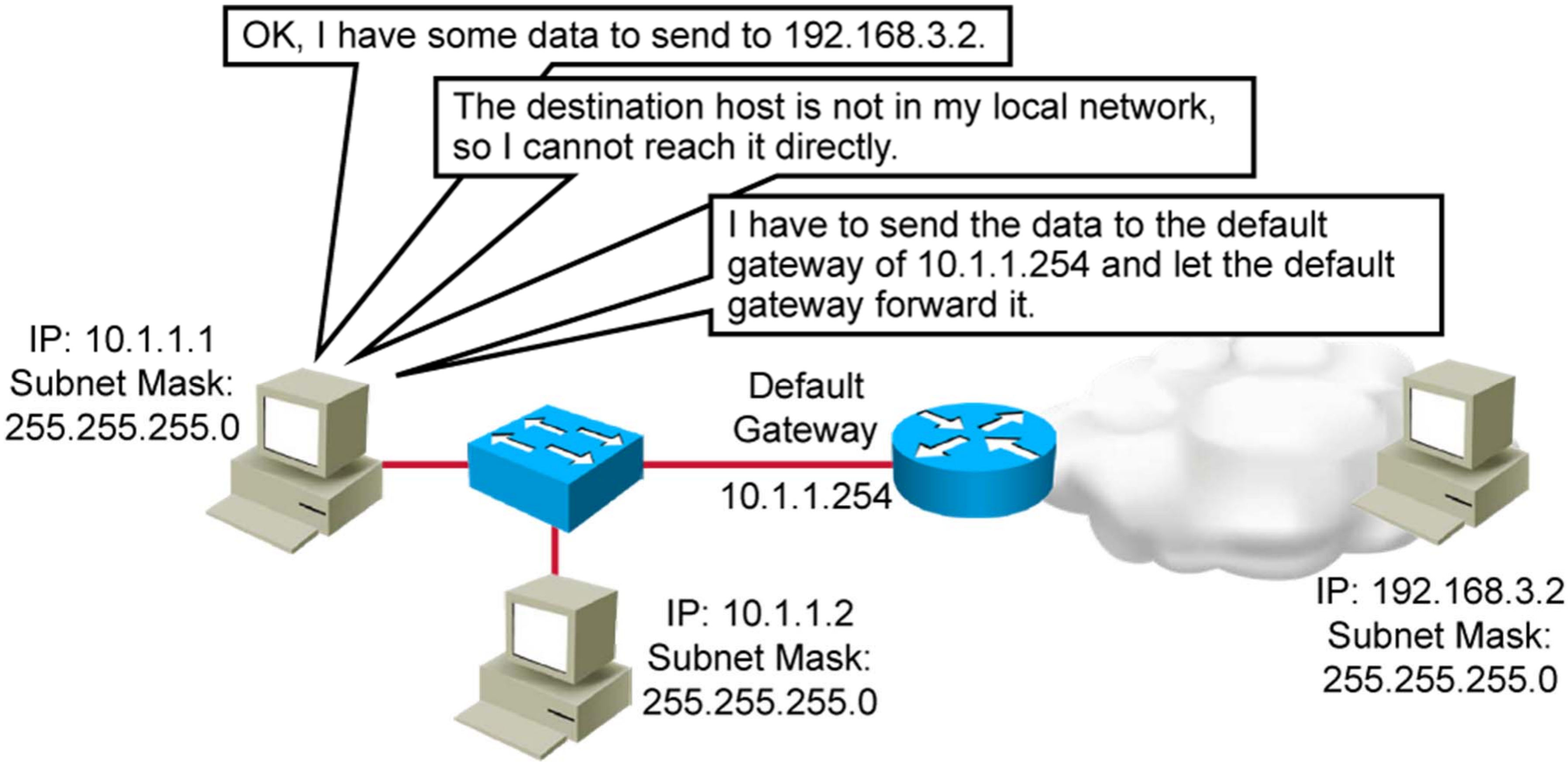
Default Subnet Masks, Class C

Example Class C address (decimal):	192.168.42.0
Example Class C address (binary):	11000000.10101000.00101010.00000000
Default Class C mask (binary):	11111111.11111111.11111111.00000000
Default Class C mask (decimal):	255.255.255.0
Default classful prefix length:	/24

Default Gateways



Default Gateways (Cont.)



Possible Subnets and Hosts for a Class B Network

Bits Borrowed (s)	Subnets Possible (2^s)	Bits Remaining in Host ID (h=16–s)	Hosts Possible per Subnet ($2^h–2$)
1	2	15	32,766
2	4	14	16,382
3	8	13	8,190
...	...	...	...
13	8192	3	6
14	16384	2	2
15	32768	1	0
16	65536	0	0

Applying Subnet Masks

Procedure for implementing subnets:

1. Determine the IP address space.
2. Based on the organizational and administrative structure, determine the number of subnets that are required.
3. Based on the address class and required number of subnets, determine the number of bits that you need to borrow from the host ID.
4. Determine the binary and decimal value of the subnet mask.
5. Apply the subnet mask to the network IP address to determine the subnet and host addresses.
6. Assign subnet addresses to specific interfaces for all devices that are connected to the network.

Determining the Network Addressing Scheme

Example 1: The IP address with subnet mask is 172.16.36.42/24.

The following tables show the eight steps that are used to determine the subnet addresses of a given IP address. In this example, the IP address and subnet mask are as follows:

- **IP address:** 172.16.36.42
- **Subnet mask:** 255.255.255.0

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
1	Write down the octet that is being split and all remaining octets on the right in binary.	**Third and fourth octet (36.42):** 00100100.00101010
2	Write down the mask or classful prefix length in binary.	**Assigned mask (/24):** 11111111.11111111.11111111.00000000
3	Draw a line to delineate the subnet and host bits in the assigned IP address. Write the IP address and the mask on top of each other so that you are able to identify the significant bits in the IP address.	**Split octet (binary):** 00100100 | 00101010 **Split mask (binary):** 11111111 | 00000000

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
4	Copy the subnet bits four times.	00100100.00000000 (subnet address) 00100100.00000001 (first address in subnet) 00100100.11111110 (last address in subnet) 00100100.11111111 (broadcast address)
5	In the first line, define the network address by placing all 0s in the host bits.	
6	In the last line, define the broadcast address by placing all 1s in the host bits.	
7	In the middle lines, define the first and last host number.	
8	Increment the subnet bits by 1 to determine the next subnet.	00100101.00000000

Determining the Network Addressing Scheme (Cont.)

After converting the addresses from binary to decimal, the addresses for the subnets are as follows:

- **Subnet address:** 172.16.36.0
- **First host address:** 172.16.36.1
- **Last host address:** 172.16.36.254
- **Broadcast address:** 172.16.36.255
- **Next subnet address:** 172.16.37.0

Determining the Network Addressing Scheme (Cont.)

Example 2: The IP address with subnet mask is 192.168.221.37/29.

The following tables show the eight steps that are used to determine the subnet addresses of a given IP address. In this example, the IP address and subnet mask are as follows:

- **IP address:** 192.168.221.37
- **Subnet mask:** 255.255.255.248

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
1	Write down the octet that is being split and all remaining octets on the right in binary.	**Fourth octet (37):** 00100101
2	Write down the mask or classful prefix length in binary.	**Assigned mask (/29):** 11111111.11111111.11111111.11111000
3	Draw a line to delineate the subnet and host bits in the assigned IP address. Write the IP address and the mask on top of each other so that you are able to identify the significant bits in the IP address.	**Split octet (binary):** 00100 | 101 **Split mask (binary):** 11111 | 000

Determining the Network Addressing Scheme (Cont.)

Step	Description	Example
4	Copy the subnet bits four times.	00100000 (network address) 00100001 (first address in subnet) 00100110 (last address in subnet) 00100111 (broadcast address)
5	In the first line, define the network address by placing all 0s in the host bits.	
6	In the last line, define the broadcast address by placing all 1s in the host bits.	
7	In the middle lines, define the first and last host number.	
8	Increment the subnet bits by 1 to determine the next subnet.	00101000

Determining the Network Addressing Scheme (Cont.)

After converting the addresses from binary to decimal, the addresses for the subnets are as follows:

- **Subnet address:** 192.168.221.32
- **First host address:** 192.168.221.33
- **Last host address:** 192.168.221.38
- **Broadcast address:** 192.168.221.39
- **Next subnet address:** 192.168.221.40

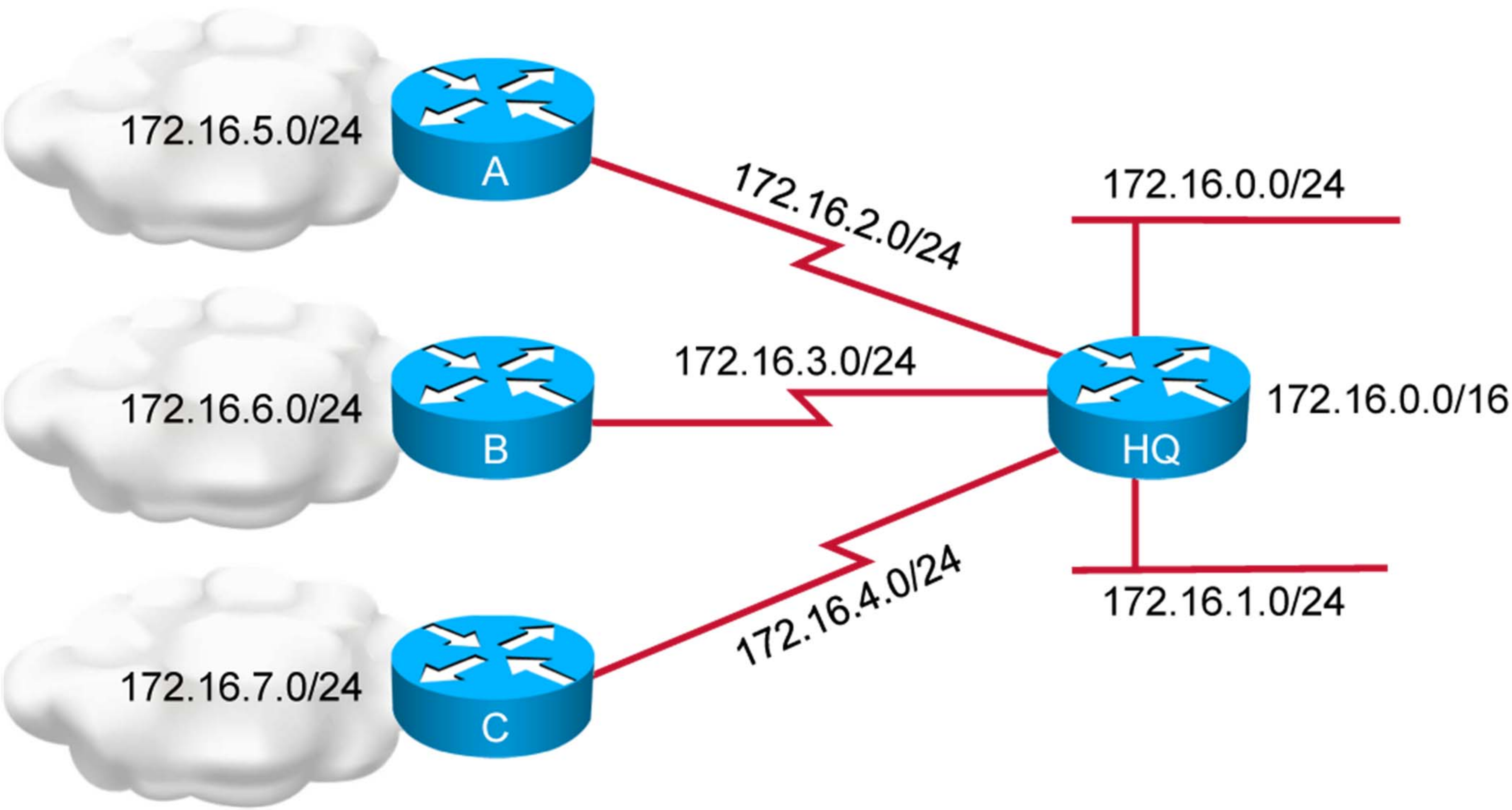
Example: Addressing Scheme

The IP address with subnet mask is 192.168.5.139/27.

IP Address	192	168	5	139
IP Address	11000000	10101000	00000101	100|01011
Subnet Mask	11111111	11111111	11111111	111|00000
Network (2)	11000000	10101000	00000101	100|00000
Network (10)	192	168	5	128
First Host	192	168	5	100|00001 = 129
Last Host	192	168	5	100|11110 = 158
Directed Broadcast	192	168	5	100|11111 = 159
Next Network	192	168	5	101|00000 = 160

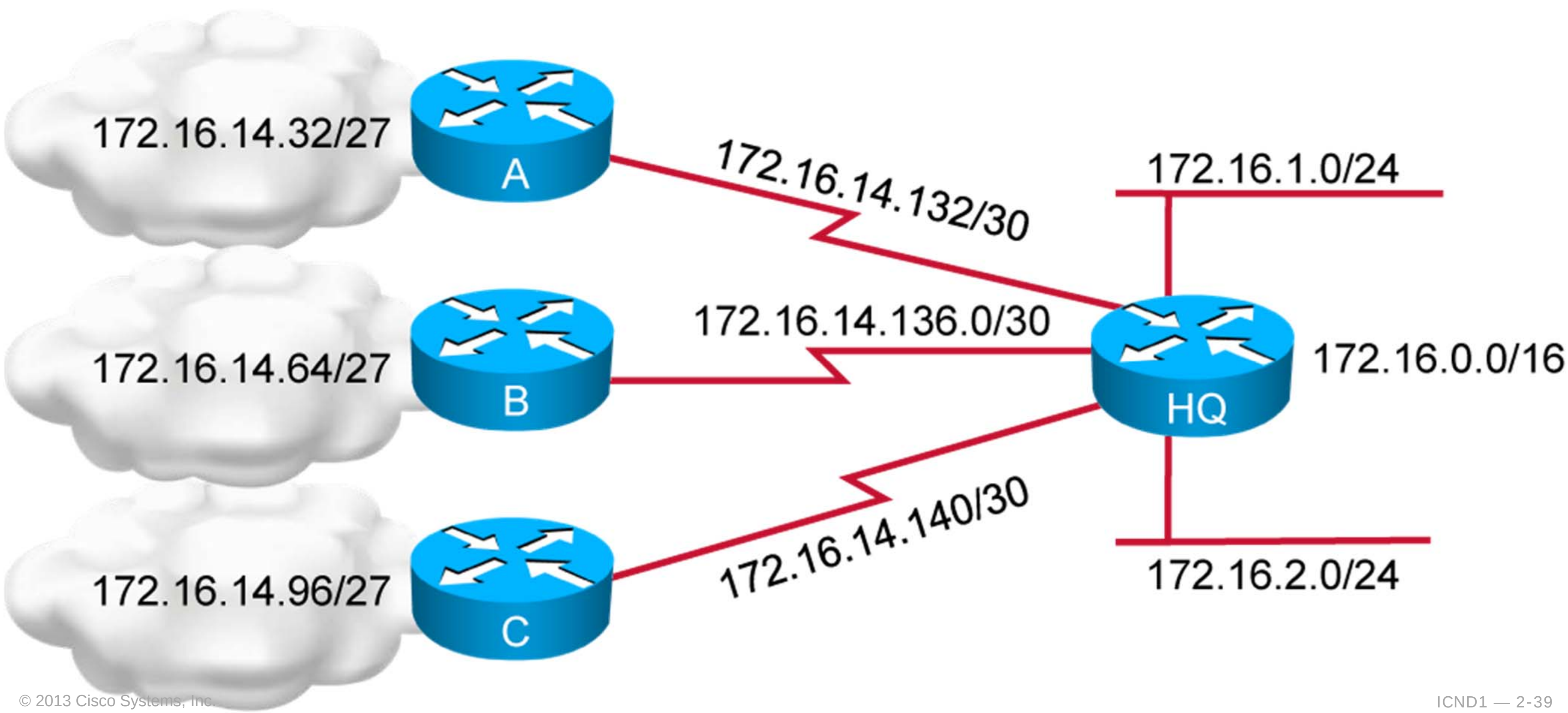
Variable-Length Subnet Masking

- Network using fixed-length subnet masking:



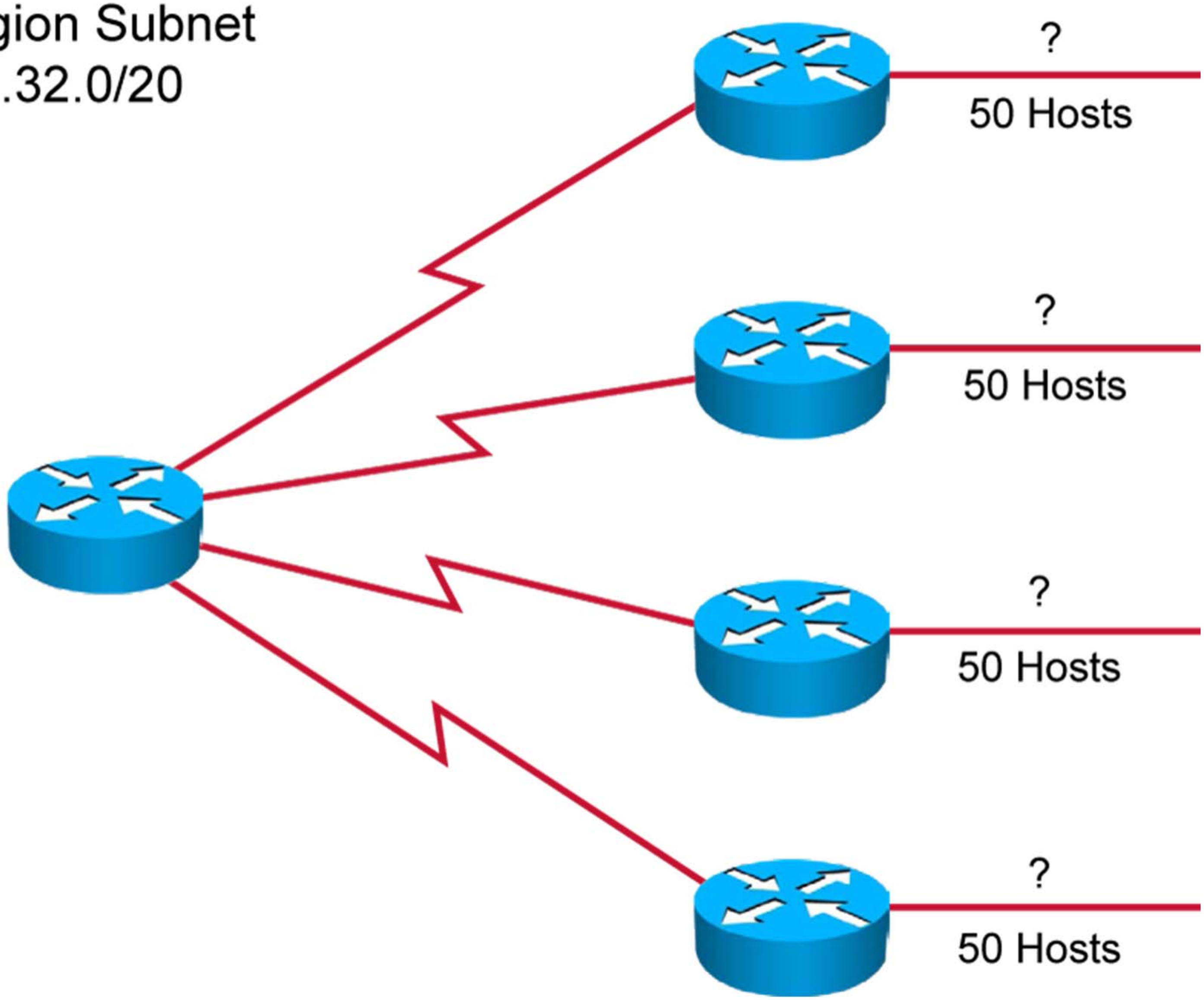
Variable-Length Subnet Masking (Cont.)

- Network using VLSM:
  - The subnet 172.16.14.0/24 is divided into smaller subnets.
  - One subnet has a subnet mask /27.
  - Further subnetting of one of the unused /27 subnets into multiple /30 subnets.



VLSM Example

Entire Region Subnet
172.16.32.0/20



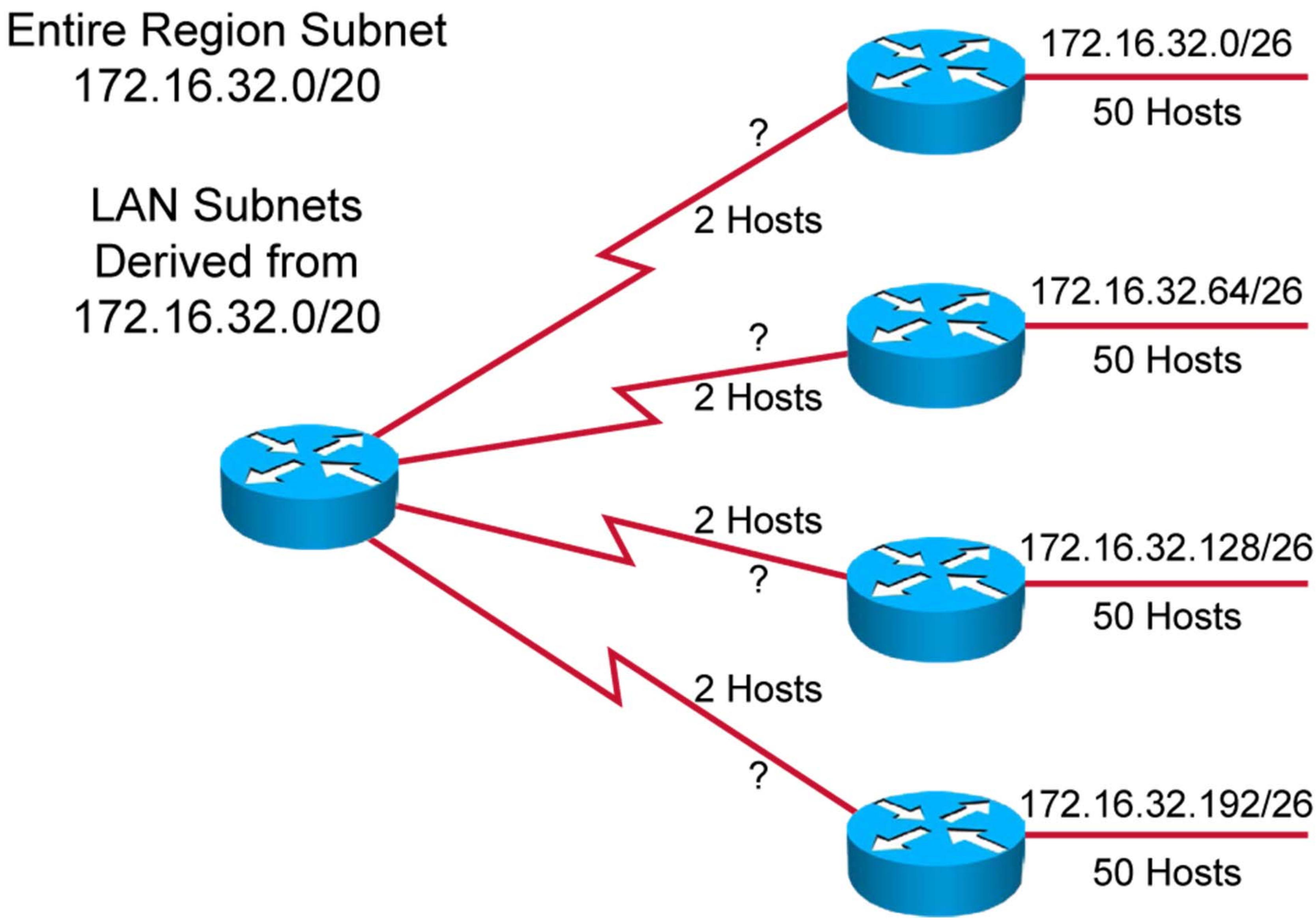
VLSM Example (Cont.)

Subnetted address: 172.16.32.0/20
In binary: 10101100.00010000.00100000.00000000

VLSM address: 172.16.32.0/26
In binary: 10101100.00010000.00100000.00000000

	Network			Subnet	VLSM Subnet	Host	
1st subnet:	172	.	16	.0010	0000.00	000000 =	172.16.32.0/26
2nd subnet:	172	.	16	.0010	0000.01	000000 =	172.16.32.64/26
3rd subnet:	172	.	16	.0010	0000.10	000000 =	172.16.32.128/26
4th subnet:	172	.	16	.0010	0000.11	000000 =	172.16.32.192/26
5th subnet:	172	.	16	.0010	0001.00	000000 =	172.16.33.0/26

VLSM Example (Cont.)



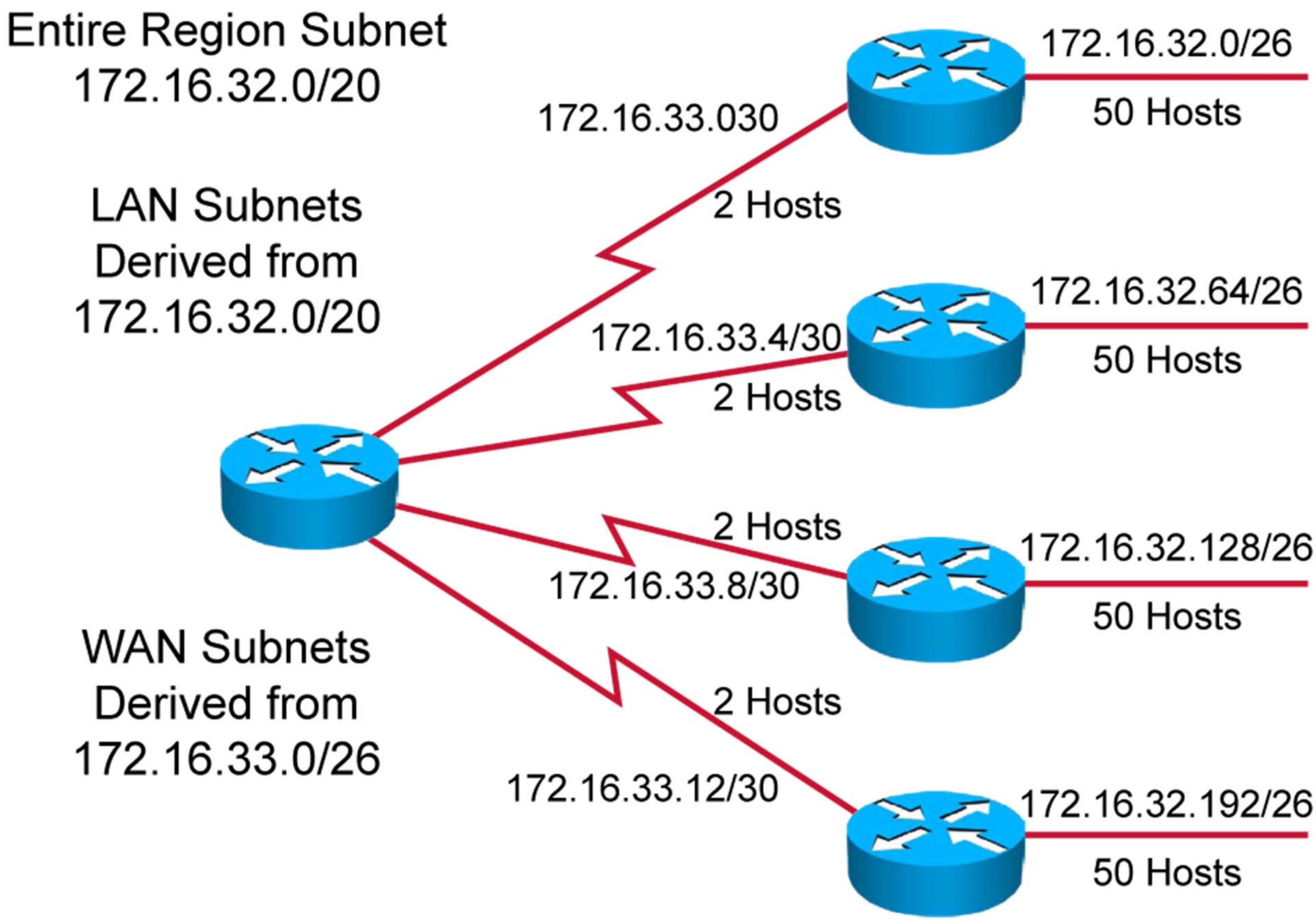
VLSM Example (Cont.)

Subnetted address: 172.16.33.0/26
In binary: 10101100.00010000.00100001.00000000

VLSM address: 172.16.33.0/30
In binary: 10101100.00010000.00100001.00000000

	Network		Subnet		VLSM Subnet	Host	
1st subnet:	172 .	16	.33	.0000	00	00 =	172.16.33.0/30
2nd subnet:	172 .	16	.33	.0000	01	00 =	172.16.33.4/30
3rd subnet:	172 .	16	.33	.0000	10	00 =	172.16.33.8/30
4th subnet:	172 .	16	.33	.0000	11	00 =	172.16.33.12/30

VLSM Example (Cont.)



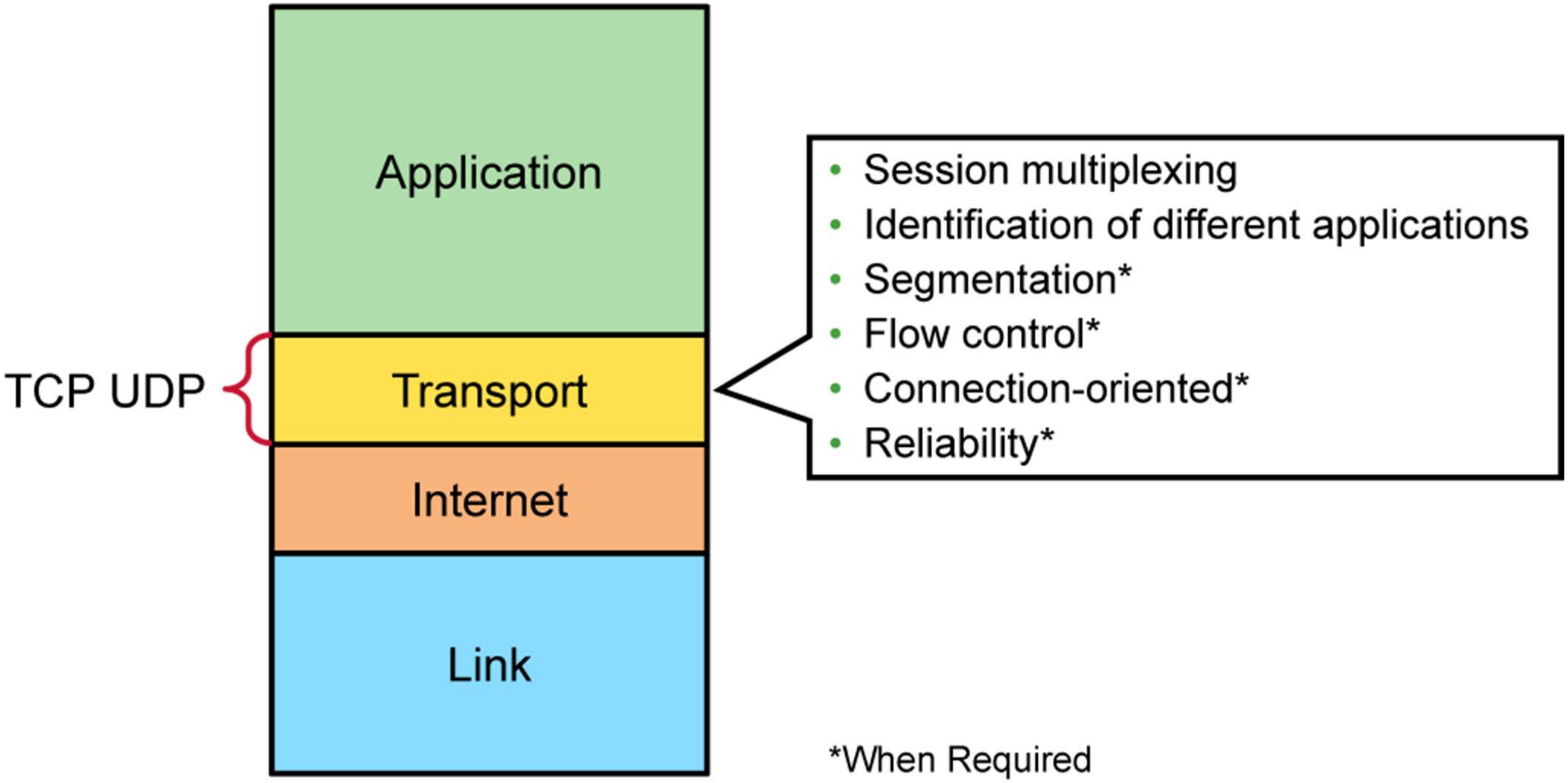
Summary

- Networks, particularly large networks, are often divided into smaller subnetworks, or subnets, which can improve network performance and control.
- The subnet mask defines the number of bits that represent the network part or subnet part of an IP address.
- End systems use subnet masks to identify the destination IP address as either local or remote.
- A default gateway is needed to send a packet out of the local network.
- Determining the optimal number of subnets and hosts depends on the type of network and the number of host addresses required.
- The algorithm for computing a number of subnets is 2^n, where *n* is the number of subnet bits.
- VLSM lets you allocate IP addresses more efficiently by adding multiple layers to the addressing hierarchy.

Understanding the TCP/IP Transport Layer

Establishing Internet Connectivity

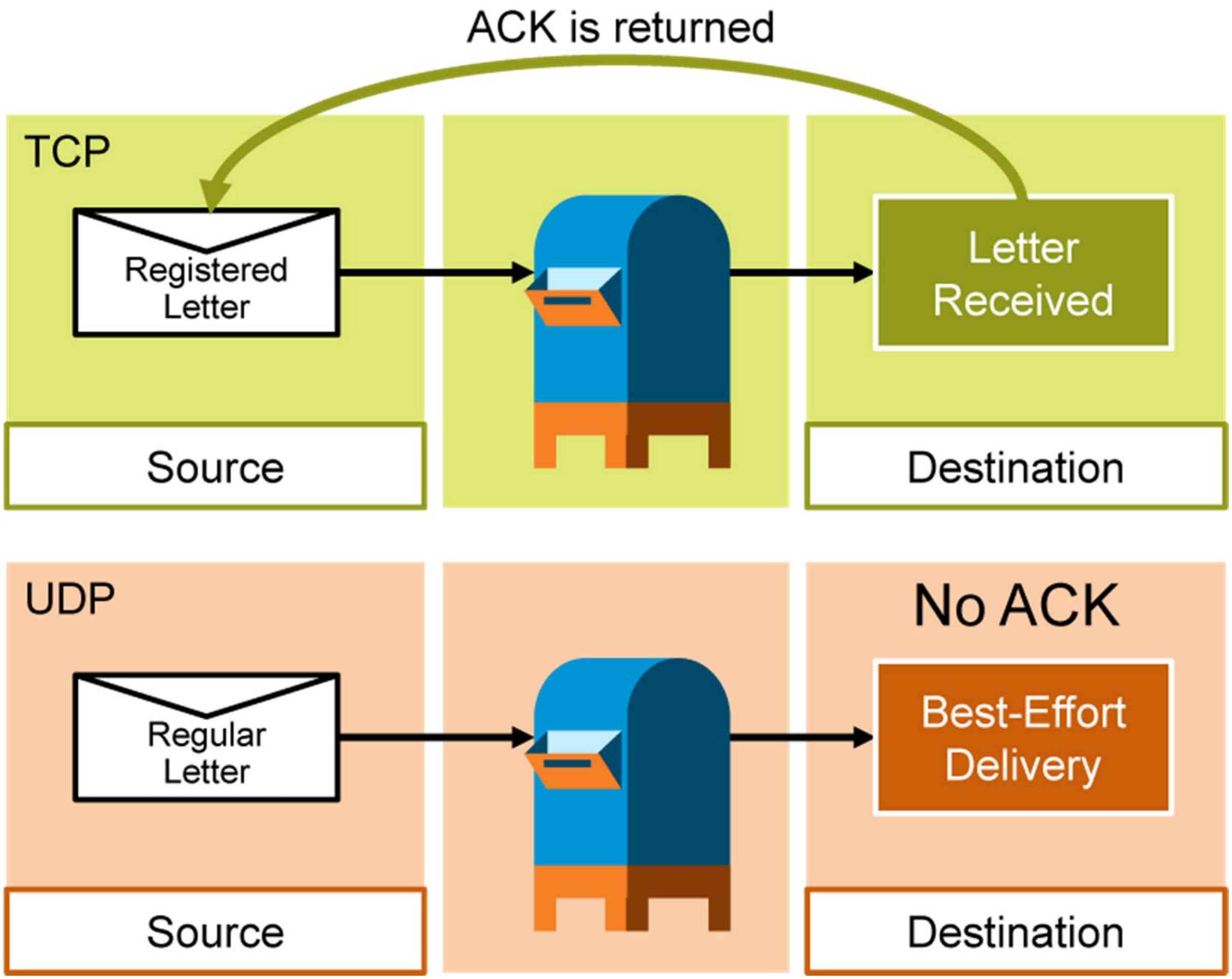
TCP/IP Transport Layer Functions



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

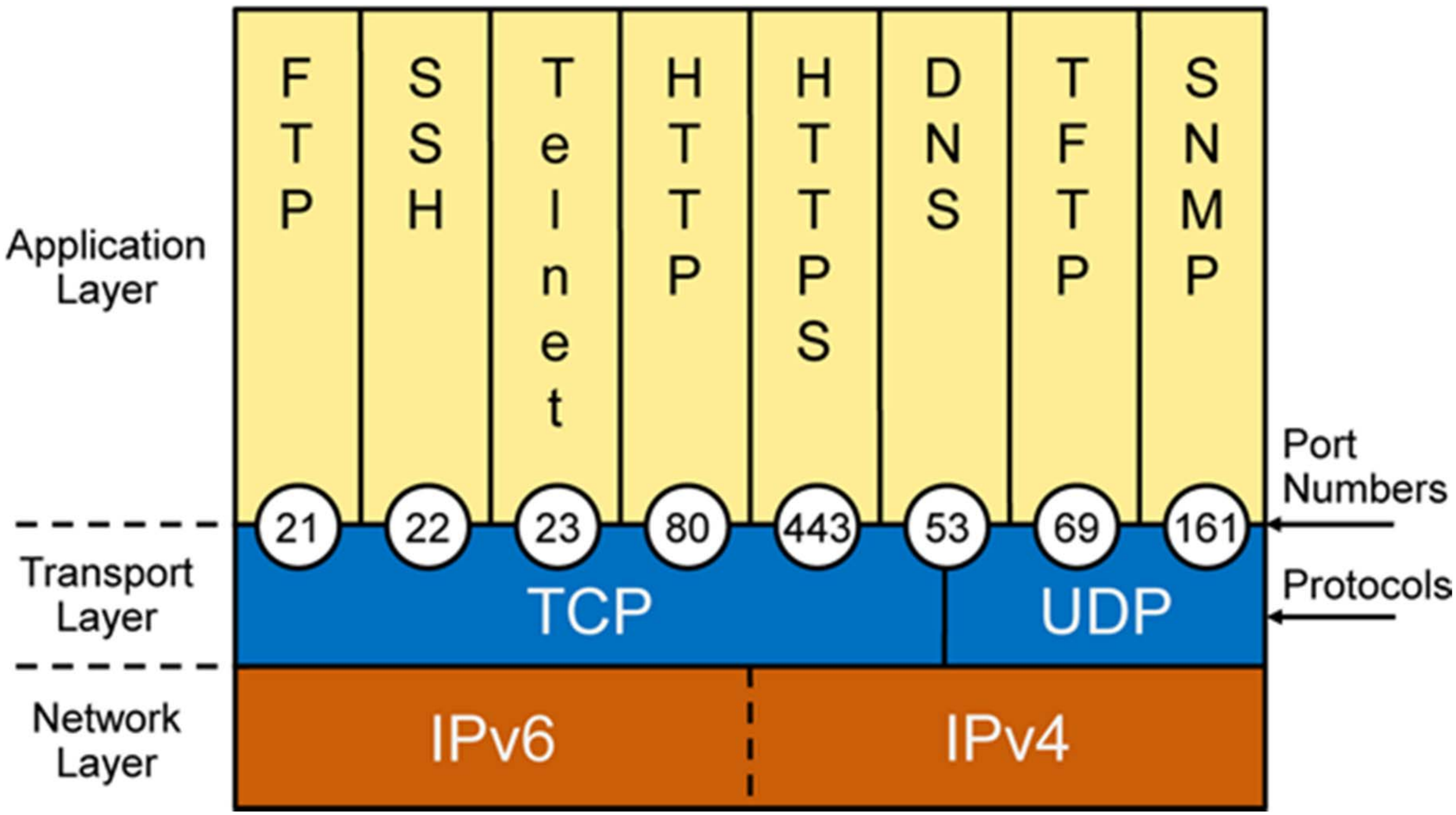
- Transport layer of the TCP/IP stack
- Access to the network layer for applications
- Connection-oriented protocol
- Full-duplex mode operation
- Error checking
- Sequencing of data packets
- Reliable delivery—acknowledgment of receipt
- Data recovery features
- Flow control

TCP Characteristics (Cont.)

The TCP header:

Source Port		Destination Port	
Sequence Number			
Acknowledgment Number			
Header Length	Reserved	Flags	Window Size
TCP Checksum		Urgent Pointer	
Options			
Data			

TCP/IP Applications



Summary

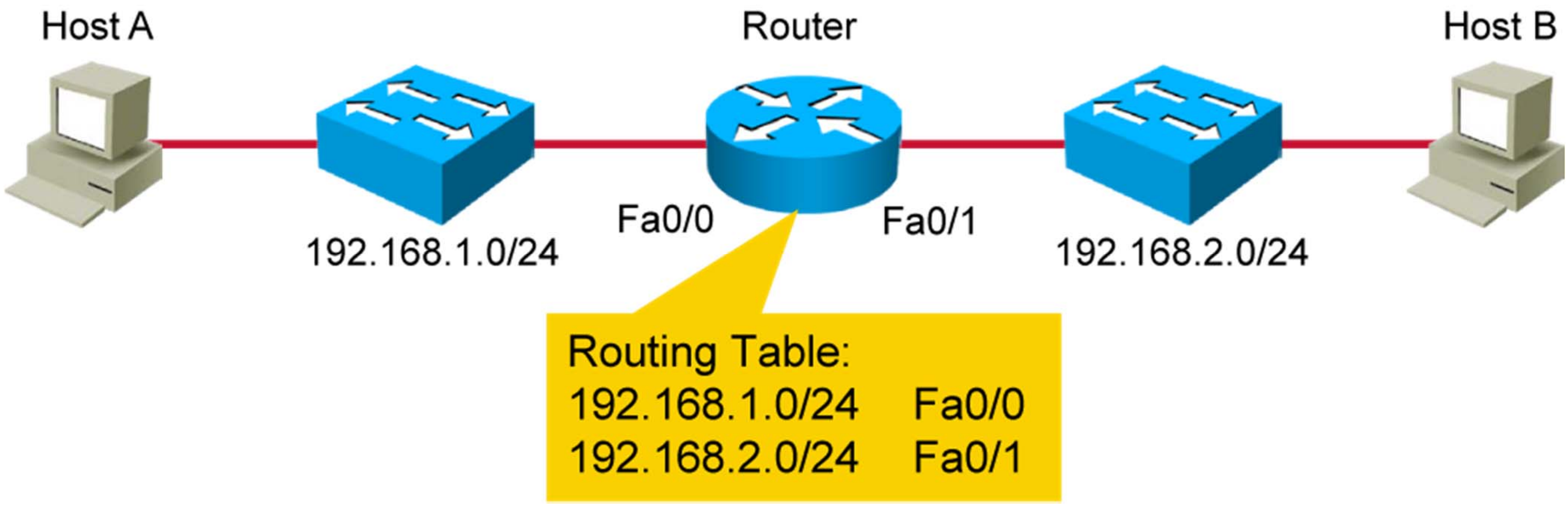
- The purpose of the transport layer is to hide the network requirements from the application layer and to ensure end-to-end transfer of application data.
- Connection-oriented transport provides reliable transport. Connectionless transport provides best-effort transport.
- UDP is a protocol that operates at the transport layer and provides applications with access to the network layer without the overhead of the reliability mechanisms of TCP. UDP is a connectionless, best-effort delivery protocol.
- TCP is a protocol that operates at the transport layer and provides applications with access to the network layer. TCP is connection-oriented and provides reliable transport.
- Port numbers identify applications.

Exploring the Functions of Routing

Establishing Internet Connectivity

Role of a Router

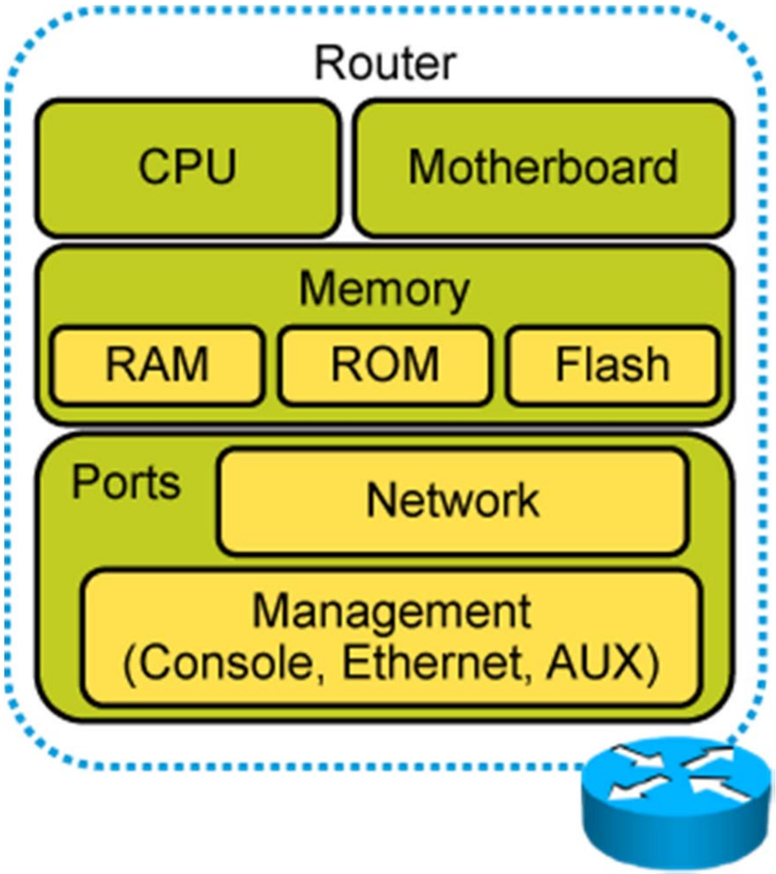
- Routers are required to reach hosts that are not in the local network.
- Routers use a routing table to route between networks.



Router Characteristics

Router components:

- CPU
- Motherboard
- Memory
- Ports
  - Management: For the connection of a terminal used for management
  - Network: Various LAN or WAN media ports



Router Functions

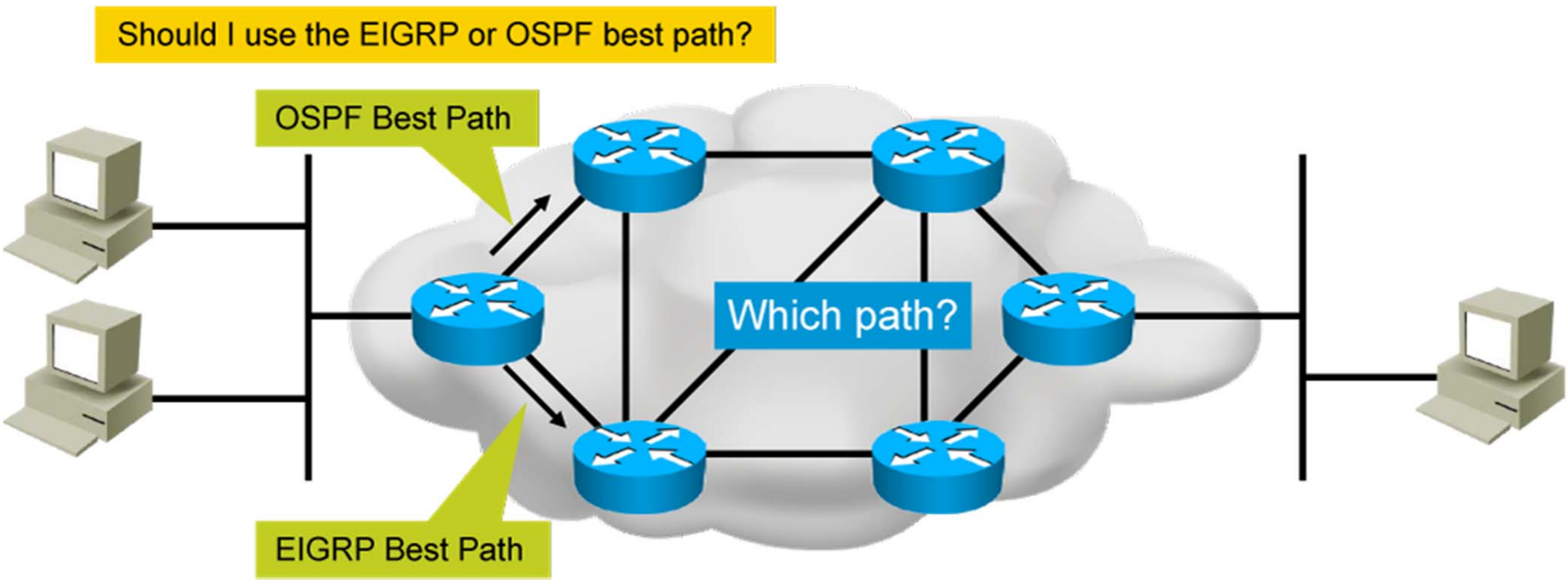
- Path determination
- Packet forwarding

```
RouterA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
     <output omitted>
Gateway of last resort is not set

     172.17.0.0/16 is variably subnetted, 8 subnets
O       172.17.14.0/24 [110/51] via 172.17.100.22, 1d05h
B       172.17.25.0/24 [200/0] via 172.17.100.22, 6d05h
D       172.17.43.0/24 [90/30720] via 172.17.50.4, 3d20h, GigabitEthernet0/0
C       172.17.50.0/24 is directly connected, GigabitEthernet0/0
L       172.17.50.2/32 is directly connected, GigabitEthernet0/0
S       172.17.92.0/24 [1/0] via 172.17.50.4
C       172.17.100.0/24 is directly connected, GigabitEthernet0/1
L       172.17.100.12/32 is directly connected, GigabitEthernet0/1
```

- Routing table on RouterA

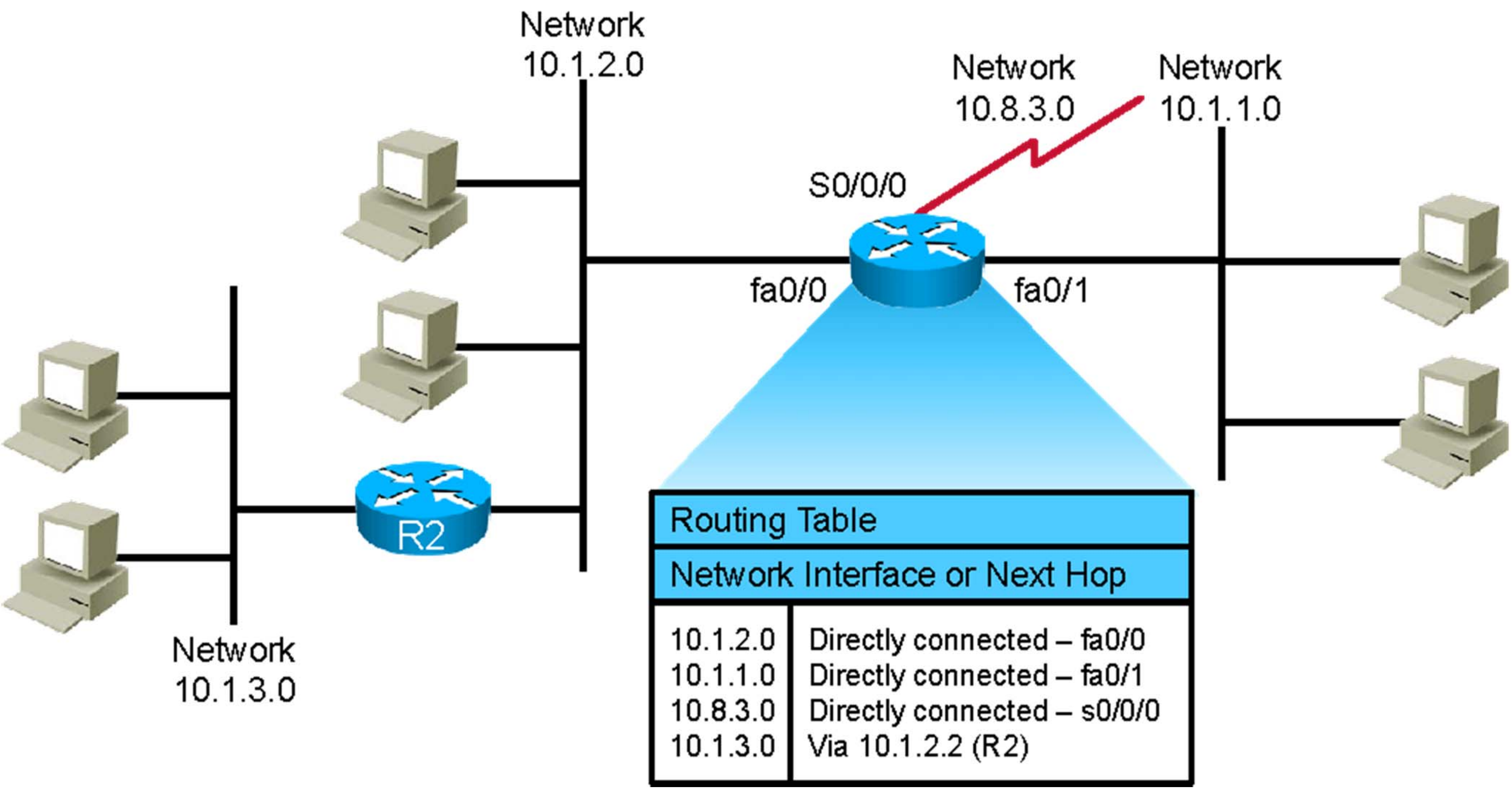
Path Determination

- Routers select the best path to the destination among various sources.
- Administrative distance defines the reliability of the route source.



Routing Table

A routing table lists all known destinations and information about how to reach them.



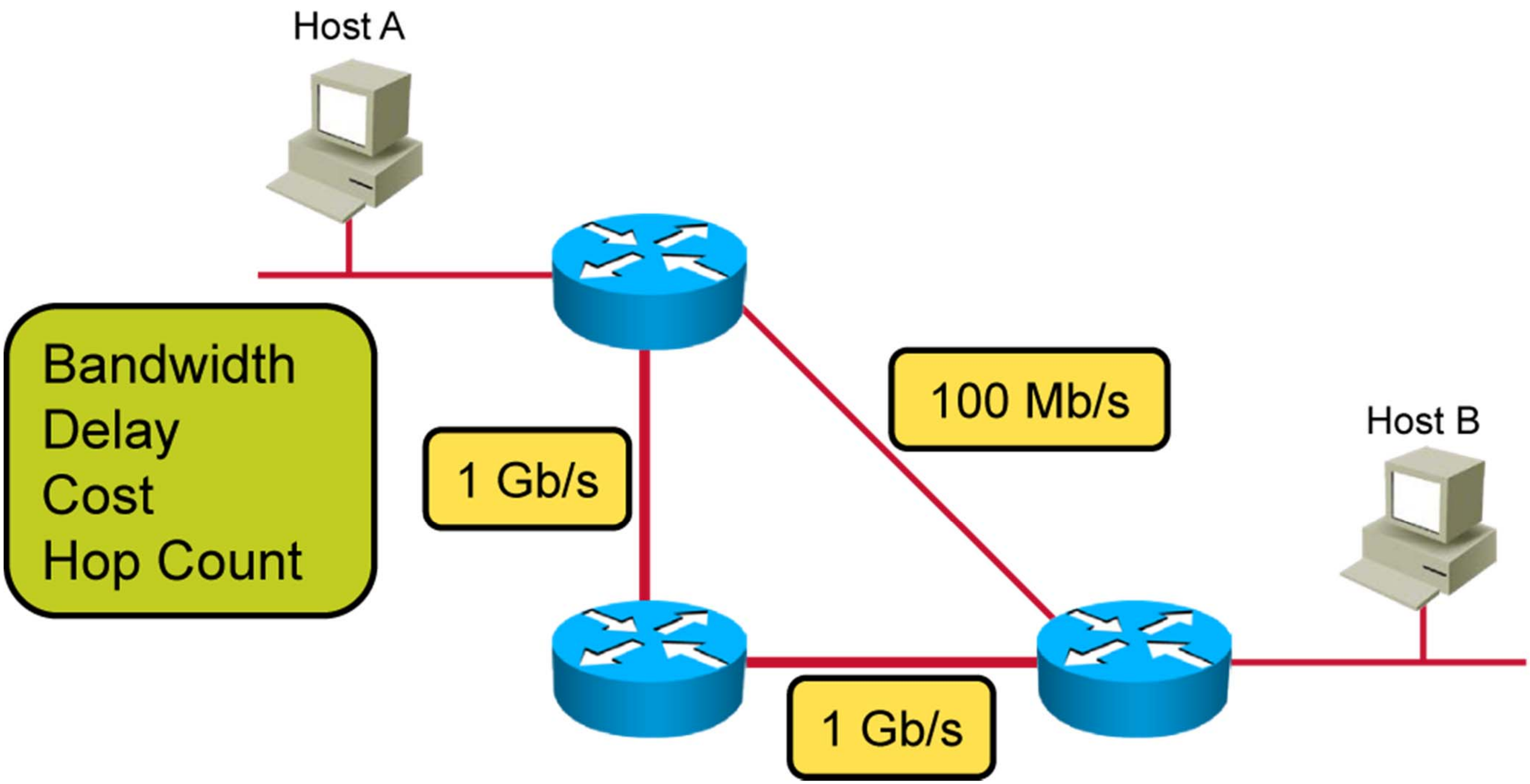
Routing Table	
Network	Interface or Next Hop
10.1.2.0	Directly connected – fa0/0
10.1.1.0	Directly connected – fa0/1
10.8.3.0	Directly connected – s0/0/0
10.1.3.0	Via 10.1.2.2 (R2)

Types of Routes

```
RouterA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-
2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.2/32 is directly connected, GigabitEthernet0/0
O 172.16.1.0/24 [110/2] via 192.168.10.2, 00:01:08, GigabitEthernet0/1
D 192.168.20.0/24 [90/156160] via 10.1.1.1, 00:01:23, GigabitEthernet0/0
S 192.168.30.0/24 [1/0] via 192.168.10.2
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 10.1.1.1
```

Dynamic Routing Protocols

Routing protocols choose different metrics to calculate best paths.



Distance Vector vs. Link State

Summary

- Routers enable internetwork communication.
- Routers include various ports and hardware similar to PCs.
- The primary functions of a router are path determination and packet forwarding.
- Routers select the best path from among different sources, based on administrative distance.
- Routing tables provide an ordered list of best paths to known networks.
- Routers use various types of routes: directly connected networks and static, dynamic, and default routes.
- Dynamic routing protocols use different metrics to calculate the best path.

Configuring a Cisco Router

Establishing Internet Connectivity

Initial Router Startup

Initial startup:

- Before you start the router, verify the power and cooling requirements, cabling, and console connection.
- Push the power switch to On.
- System startup routines initiate the router software.
- Cisco IOS Software output text appears on the console.

Initial Router Setup


```
RouterX con0 is now available

Press RETURN to get started.

RouterX>
```

- A configured router with an existing configuration displays a user EXEC mode prompt.

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

- A router without an existing configuration enters the system configuration dialog.

Configuring Router Interfaces

```
RouterX(config)#interface GigabitEthernet 0/0
RouterX(config-if)#
```

- Enters GigabitEthernet 0/0 interface configuration mode

```
RouterX(config)#interface Serial 0/0/0
RouterX(config-if)#description Link to ISP
```

- Enters Serial 0/0/0 interface configuration mode and adds descriptive text

Configuring Router Interfaces (Cont.)

```
RouterX#configure terminal
RouterX(config)#interface GigabitEthernet 0/0
RouterX(config-if)#no shutdown
%LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

- Enables an interface that is administratively shut down

```
RouterX#configure terminal
RouterX(config)#interface Serial 0/0/0
RouterX(config-if)#shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to down
```

- Administratively disables an interface

Configuring the Cisco Router IP Address

Each router interface needs a unique IP address.


```
RouterX#configure terminal
RouterX(config)#interface Serial 0/0/0
RouterX(config-if)#ip address 172.18.0.1 255.255.0.0
```

- Configures an IP address on the Serial 0/0/0 interface on router RouterX

Router **show ip interface brief** Command

```
RouterX#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down
down
GigabitEthernet0/0         10.1.1.1        YES manual up
up
GigabitEthernet0/1         209.165.200.226 YES manual up
up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down
down
Serial0/0/0                172.18.0.1      YES manual up
up
Serial0/0/1                unassigned      YES manual administratively down
down
```

- Verifies the status of all interfaces

Router **show ip interface brief** Command (Cont.)

```
Branch#show ip route
<output omitted>
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/24 is directly connected, GigabitEthernet0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0
      172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.18.0.0/16 is directly connected, Serial0/0/0
L        172.18.0.1/32 is directly connected, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.226/31 is directly connected, GigabitEthernet0/1
L        209.165.200.226/32 is directly connected, GigabitEthernet0/1
```

- Enabled interfaces populate the routing table

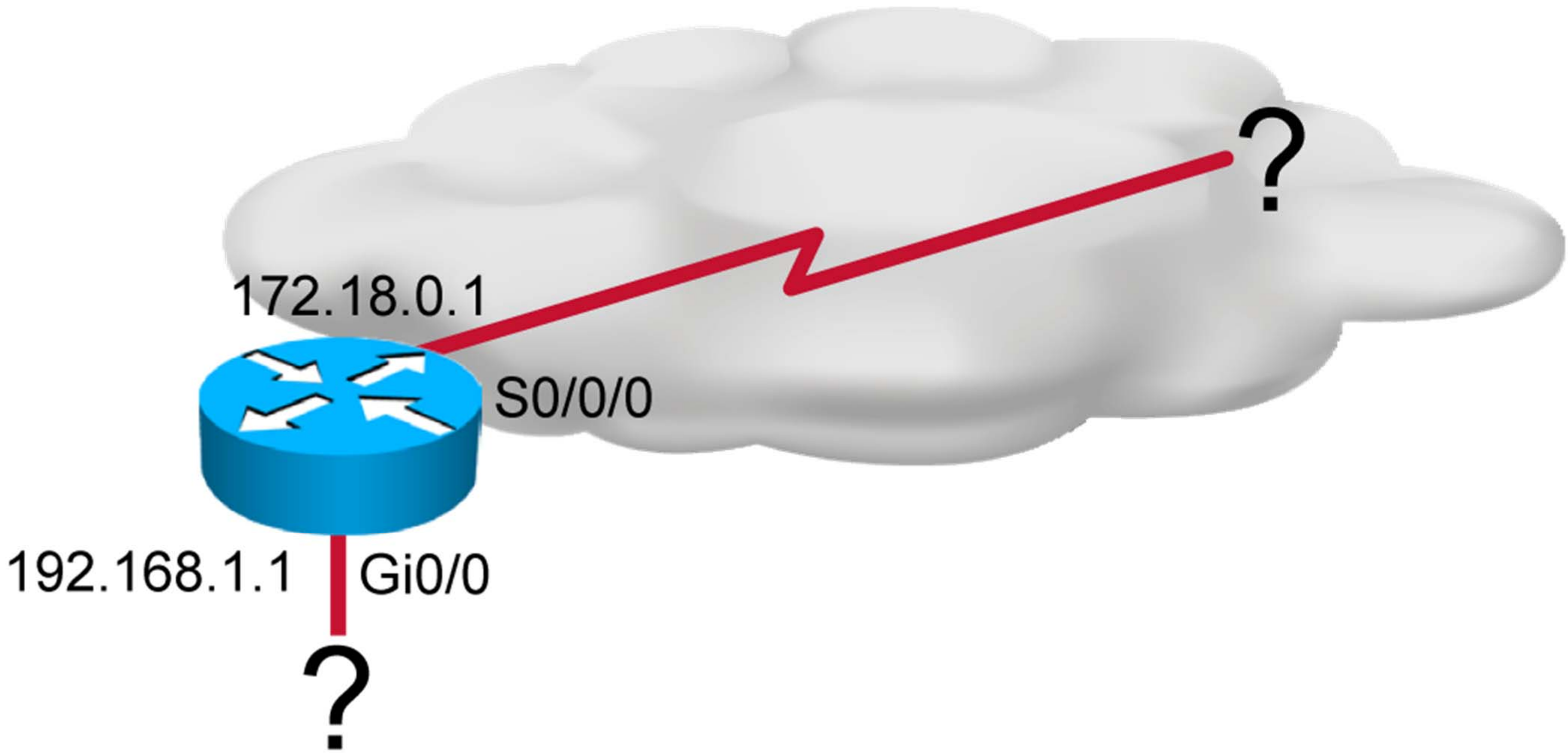
Router **show interfaces** Command

```
RouterX#show interfaces
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is f866.f231.7250 (bia
f866.f231.7250)
  Description: Link to LAN
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:53, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
<output omitted>
```

- Verifies the statistics for all interfaces that are configured on the router

Exploring Connected Devices

What are the neighboring devices of the router?

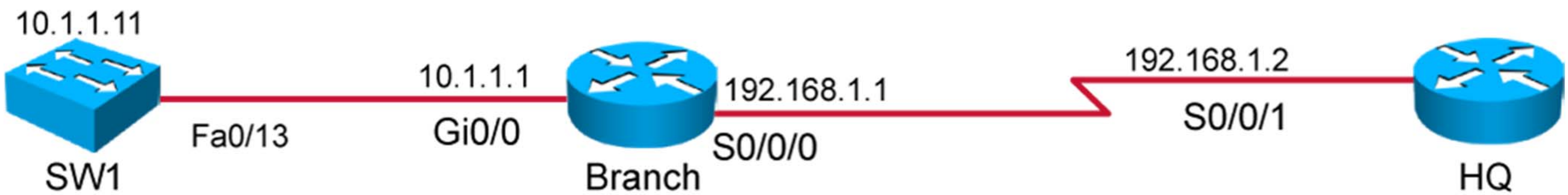


Cisco Discovery Protocol

- A proprietary utility that gathers information about directly connected Cisco switches, routers, and other Cisco devices
- Discovers neighboring devices, regardless of which protocol suite they are running
- LLDP—an alternative standards-based discovery protocol

Upper-layer entry addresses	**IPv4, IPv6, and others**
Cisco Discovery Protocol	Discovers and displays information about directly connected Cisco devices
Media	LAN, Frame Relay, ATM, others

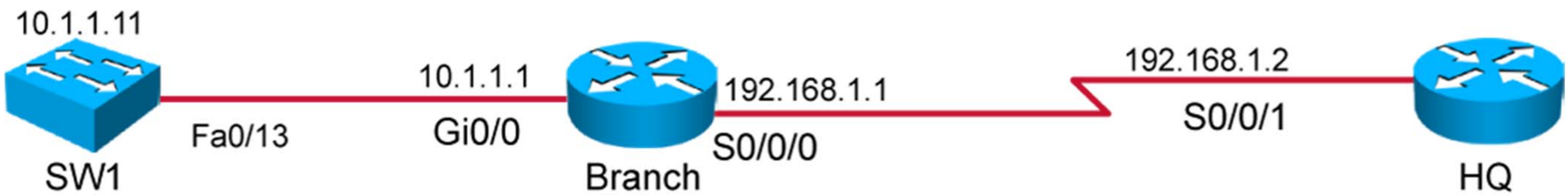
Discovering Neighbors Using Cisco Discovery Protocol




```
Branch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID    Local Intrfce    Holdtme Capability  Platform    Port ID
HQ           Ser 0/0/0        123     R S I       CISCO2901   Ser 0/0/1
SW1          Gig 0/0          124     S I         WS-C2960-   Fas 0/13
```

- Displays information about neighboring devices discovered with Cisco Discovery Protocol

Using the **show cdp neighbors detail** Command




```
Branch#show cdp neighbors detail
-------------------------
Device ID: HQ
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco CISCO2901/K9,  Capabilities: Router Switch IGMP
Interface: Serial0/0/0,  Port ID (outgoing port): Serial0/0/1
Holdtime: 132 sec
Version:  Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M),
Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 20-Mar-12 18:57 by prod_rel_team
<output omitted>
```

- Displays detailed information about neighboring devices

Summary

- The router startup sequence begins with POST, then the Cisco IOS image is found and loaded. Finally, the configuration file is loaded, if it exists.
- If a router starts without a configuration, the Cisco IOS Software executes a question-driven configuration dialog, which can be skipped.
- The main function of a router is to relay packets from one network device to another.
- Interface characteristics, such as the IP address and description, are configured using interface configuration mode.
- When you have completed router interface configuration, you can verify it by using the **show ip interface brief** and **show interfaces** commands

Summary (Cont.)

- Cisco Discovery Protocol is an information-gathering tool used by network administrators to obtain information about directly connected devices.
- Cisco Discovery Protocol exchanges hardware and software device information with its directly connected Cisco Discovery Protocol neighbors.
- The **show cdp neighbors** command displays information about the Cisco Discovery Protocol neighbors of a router.
- The **show cdp neighbors detail** command displays detailed Cisco Discovery Protocol information on a Cisco device.

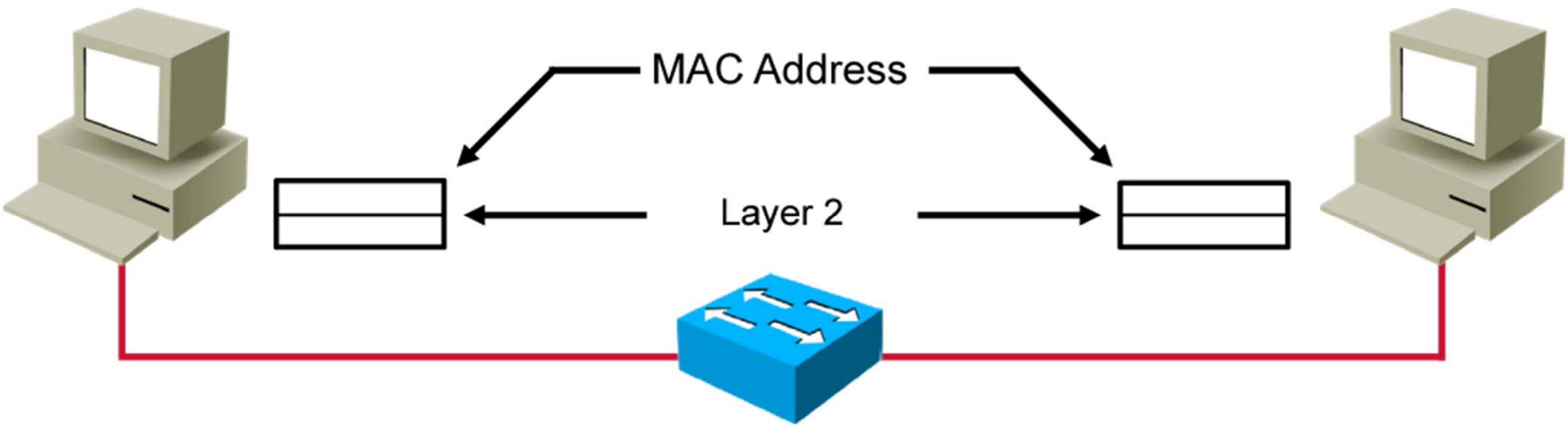
Exploring the Packet Delivery Process

Establishing Internet Connectivity

Layer 2 Addressing

Layer 2 characteristics:

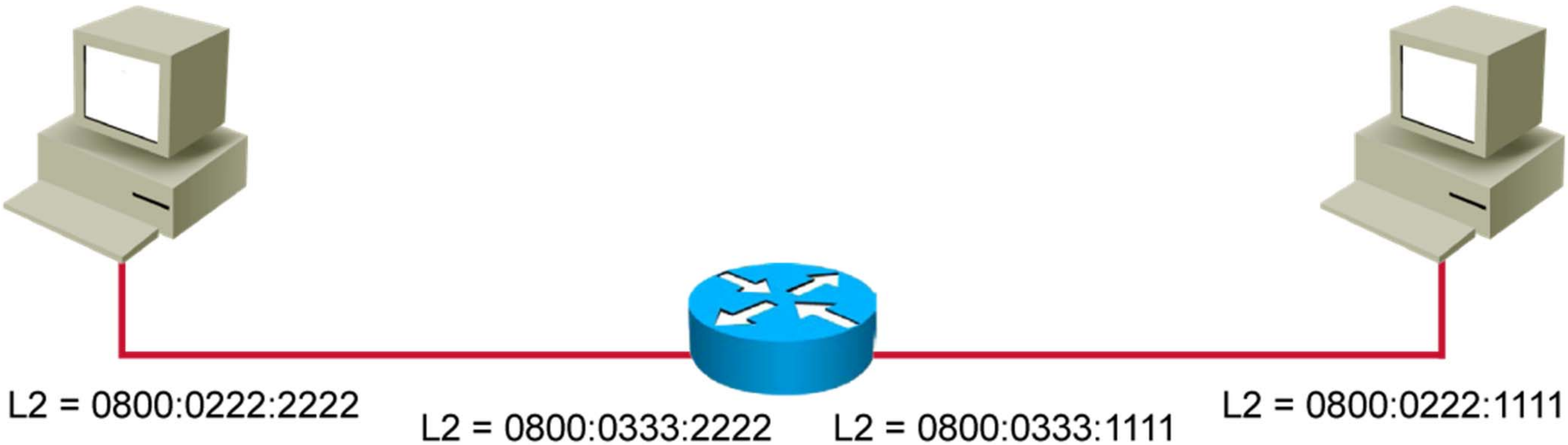
- Ethernet uses MAC addresses.
- Identifies end devices in the LAN.
- Enables the packet to be carried by the local media across each segment.



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.

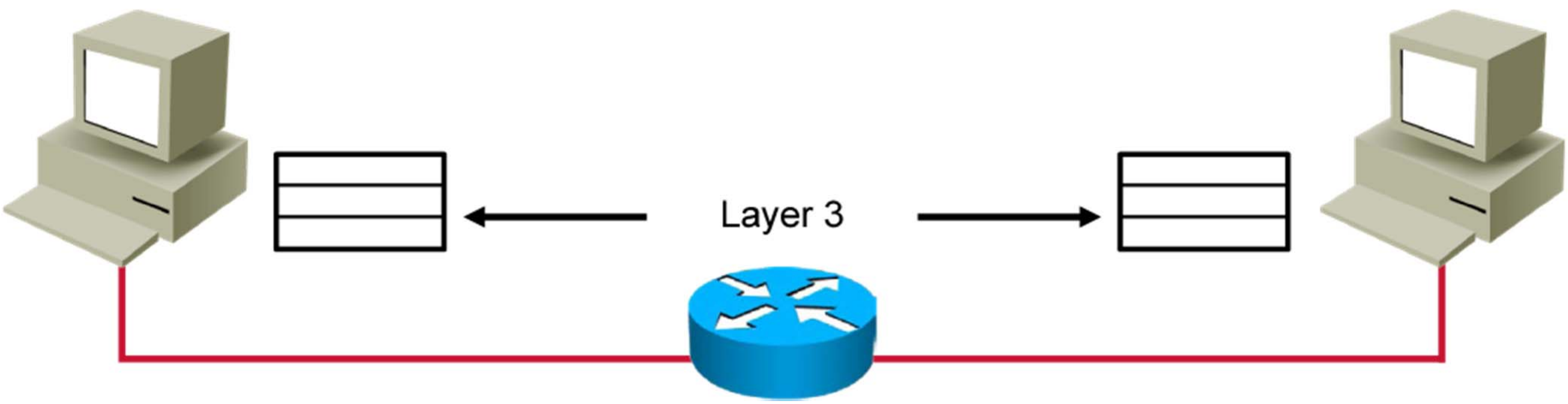


L2 = Layer 2

Layer 3 Addressing

Layer 3 devices and functions:

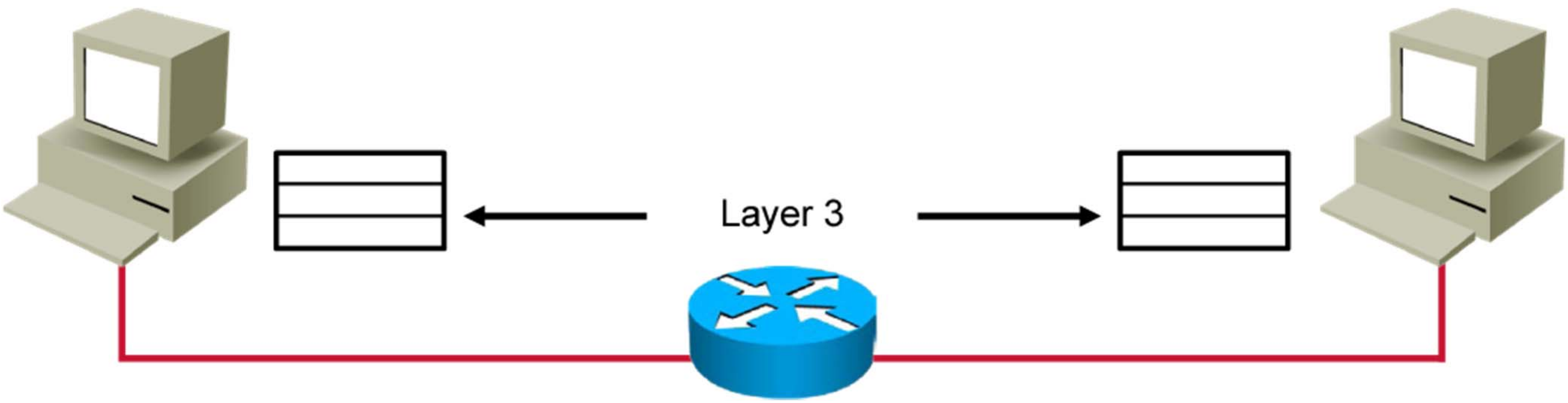
- The network layer provides connectivity and path selection between two host systems.
- In the host, this is the path between the data link layer and the upper layers.
- In the router, it is the actual path across the network.



Layer 3 Addressing (Cont.)

Layer 3 addressing:

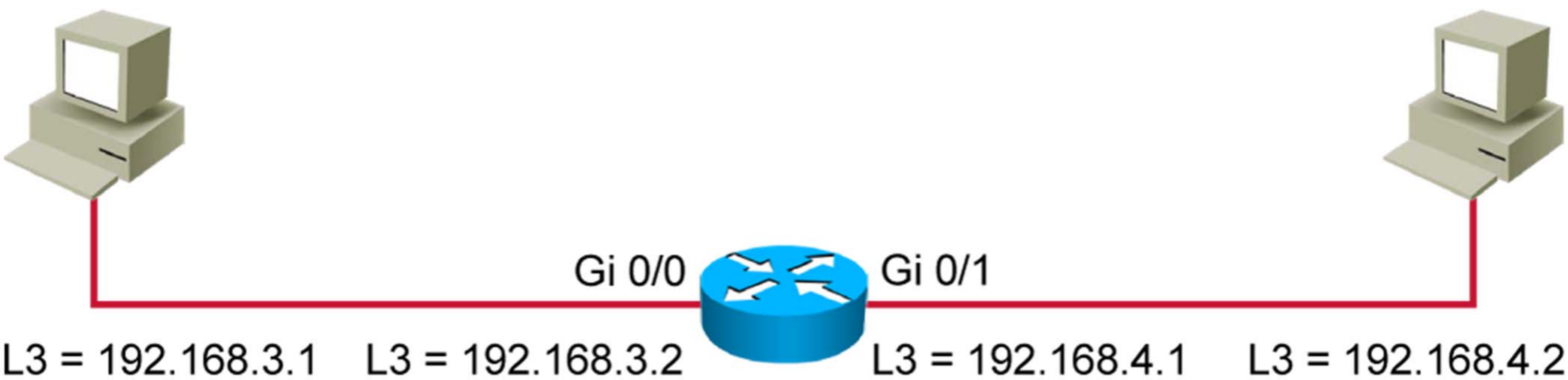
- Layer 3 addresses must include identifiers that enable intermediary network devices to locate hosts on different networks.
- TCP/IP protocol stack uses IP.



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

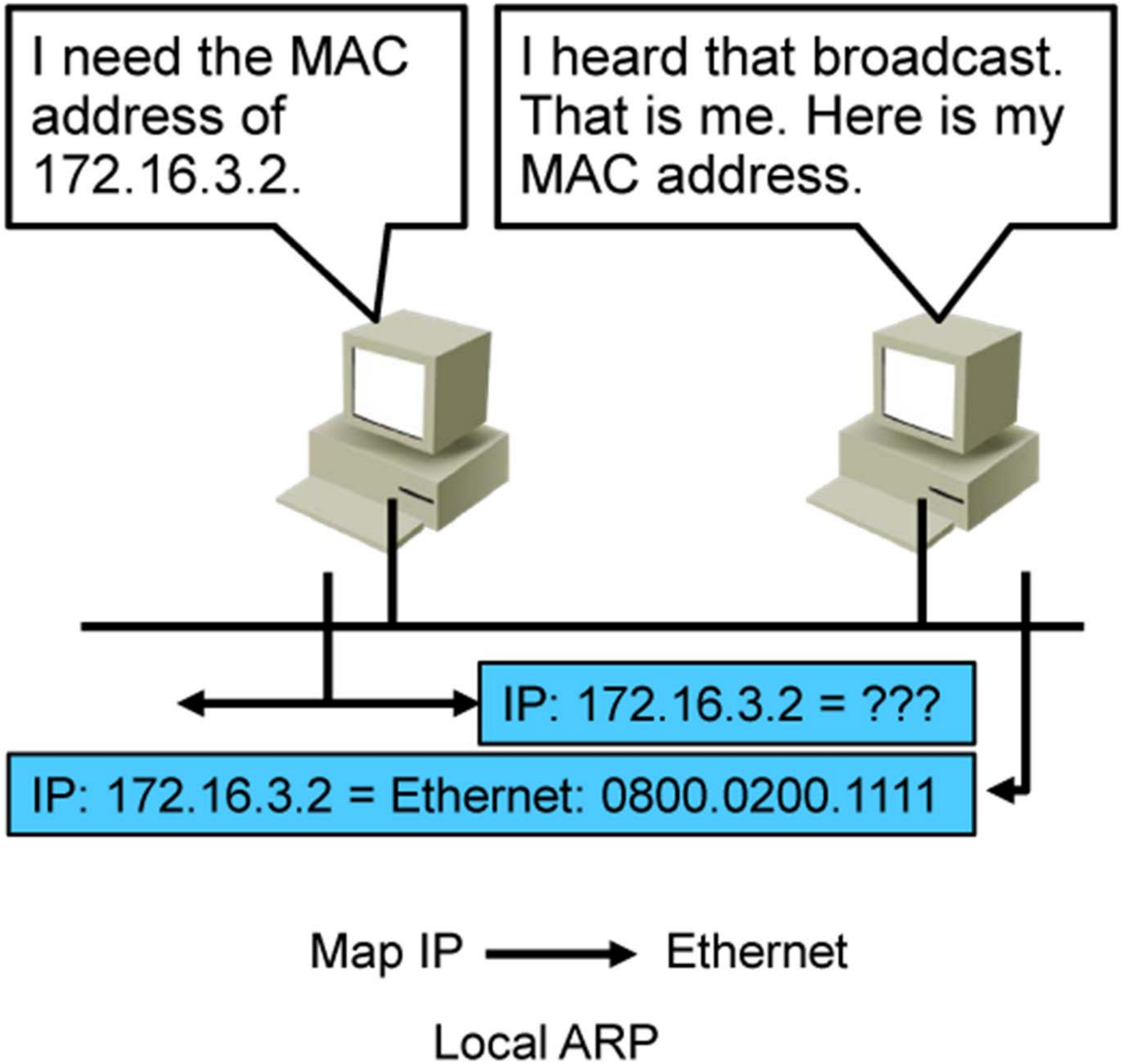


L3 = Layer 3

Address Resolution Protocol

ARP provides two basic functions:

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



Address Resolution Protocol (Cont.)

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

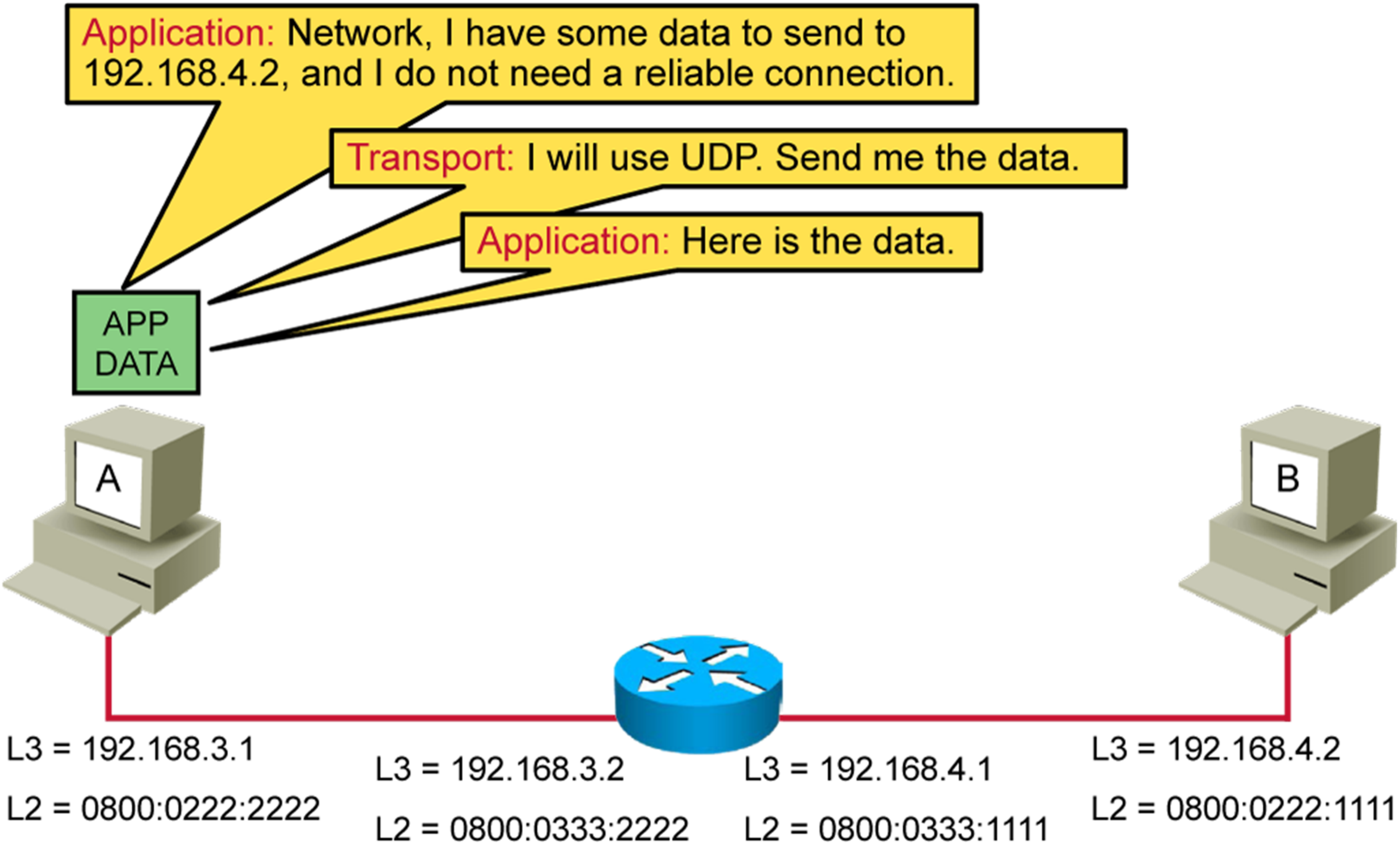
On the PC:

```
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
```

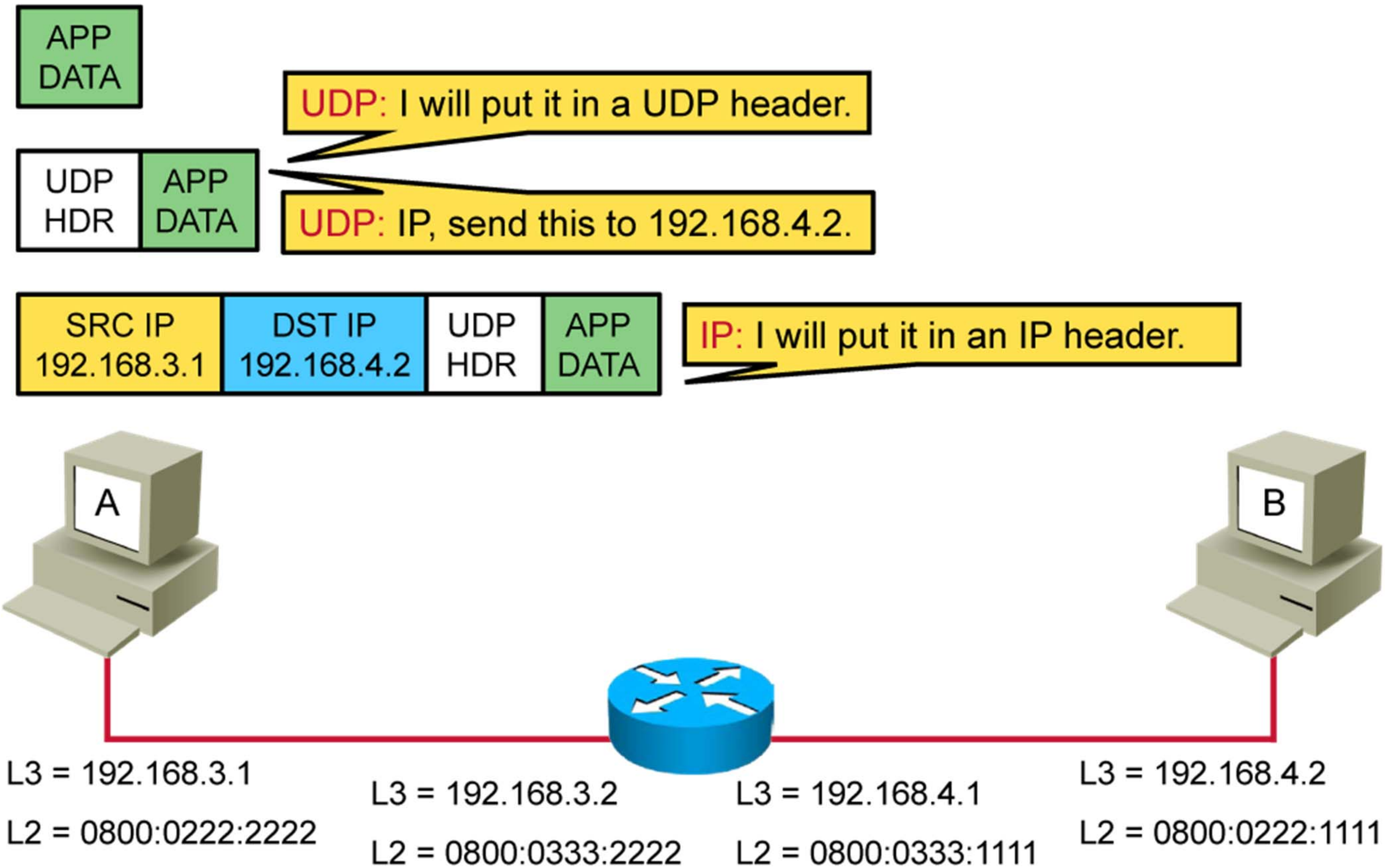
On the router:

```
Branch#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.1.100              5   000c.2993.6a84  ARPA
GigabitEthernet0/0
Internet  10.1.1.101              4   000c.2913.ccc9  ARPA
GigabitEthernet0/0
```

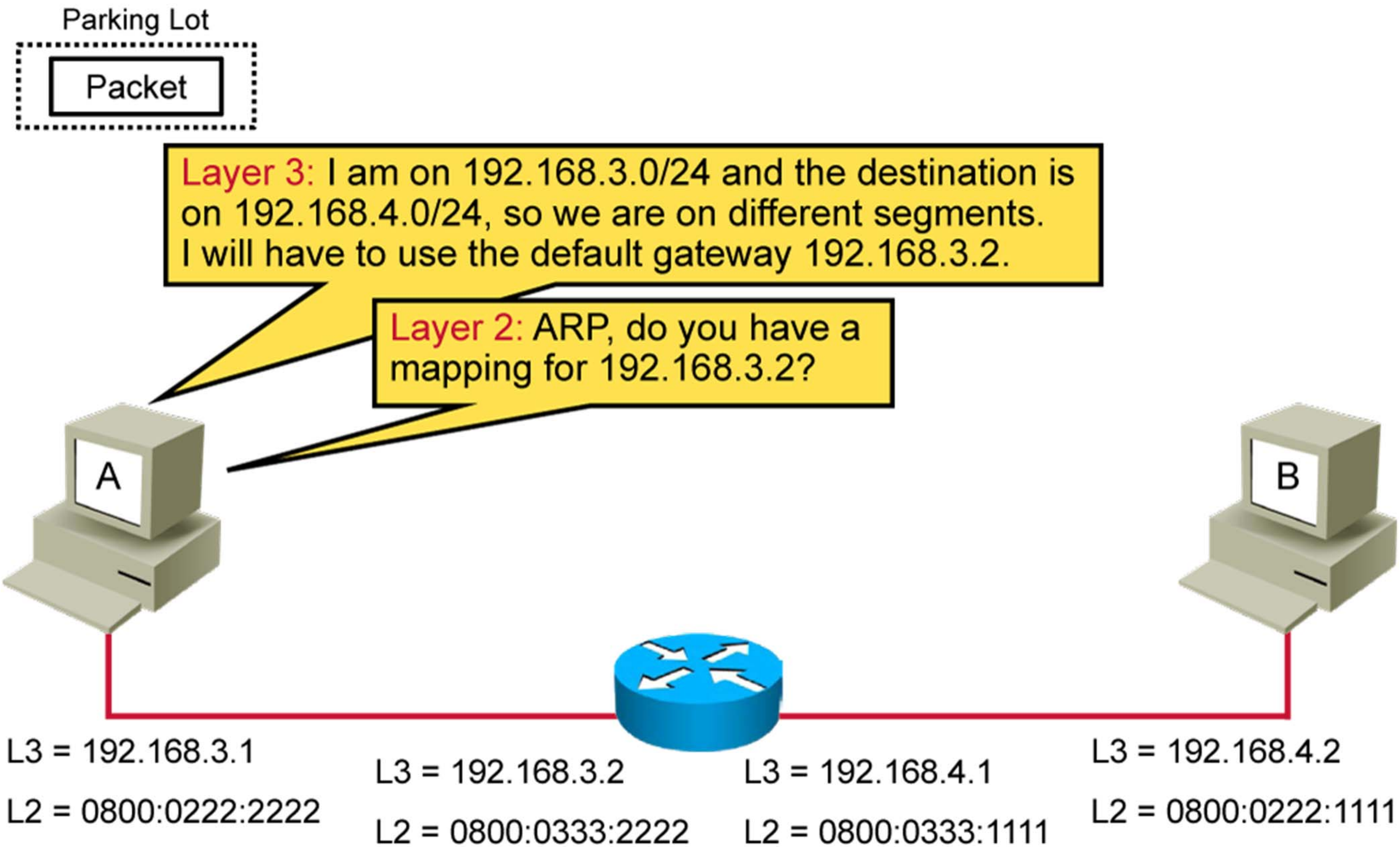
Host-to-Host Packet Delivery (Step 1 of 16)



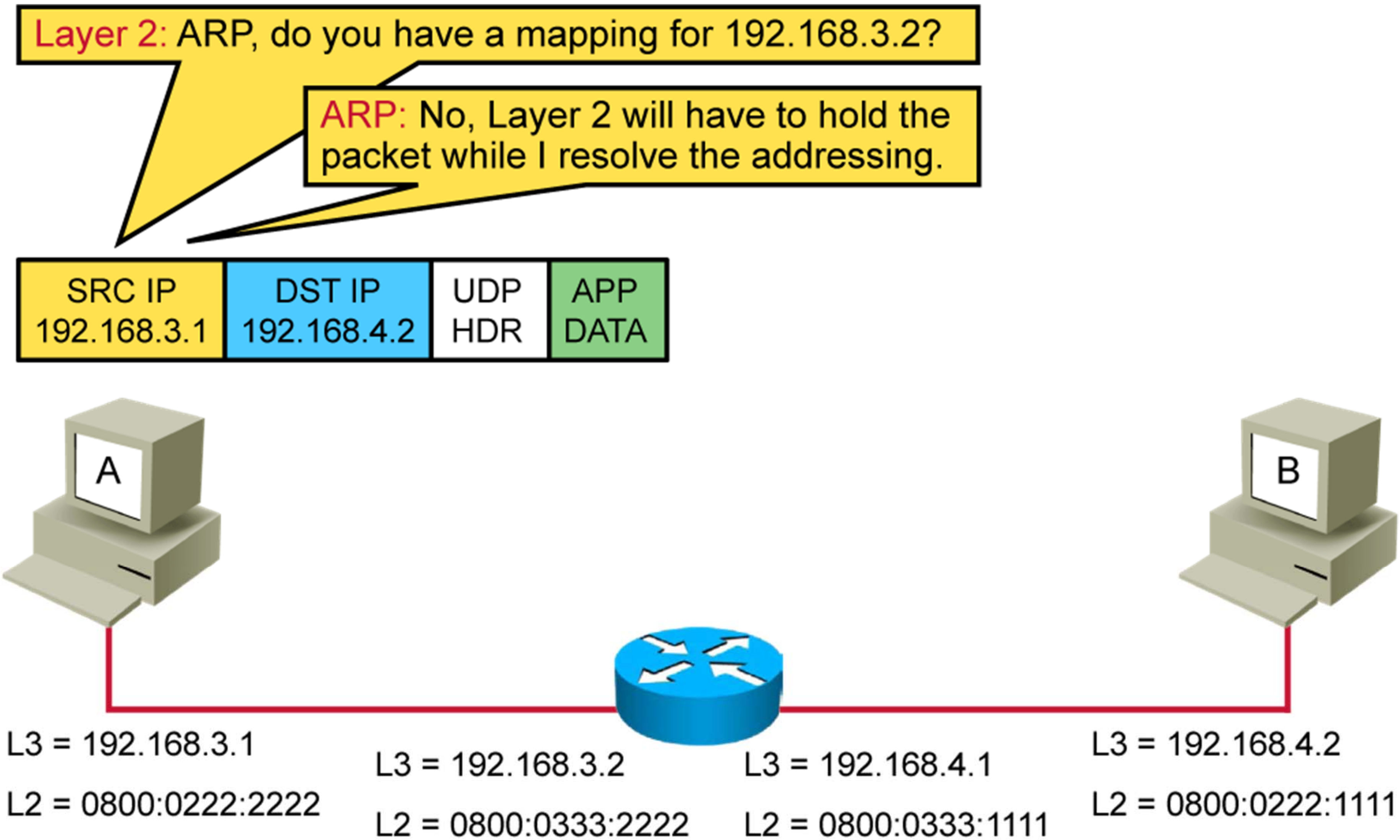
Host-to-Host Packet Delivery (Step 2 of 16)



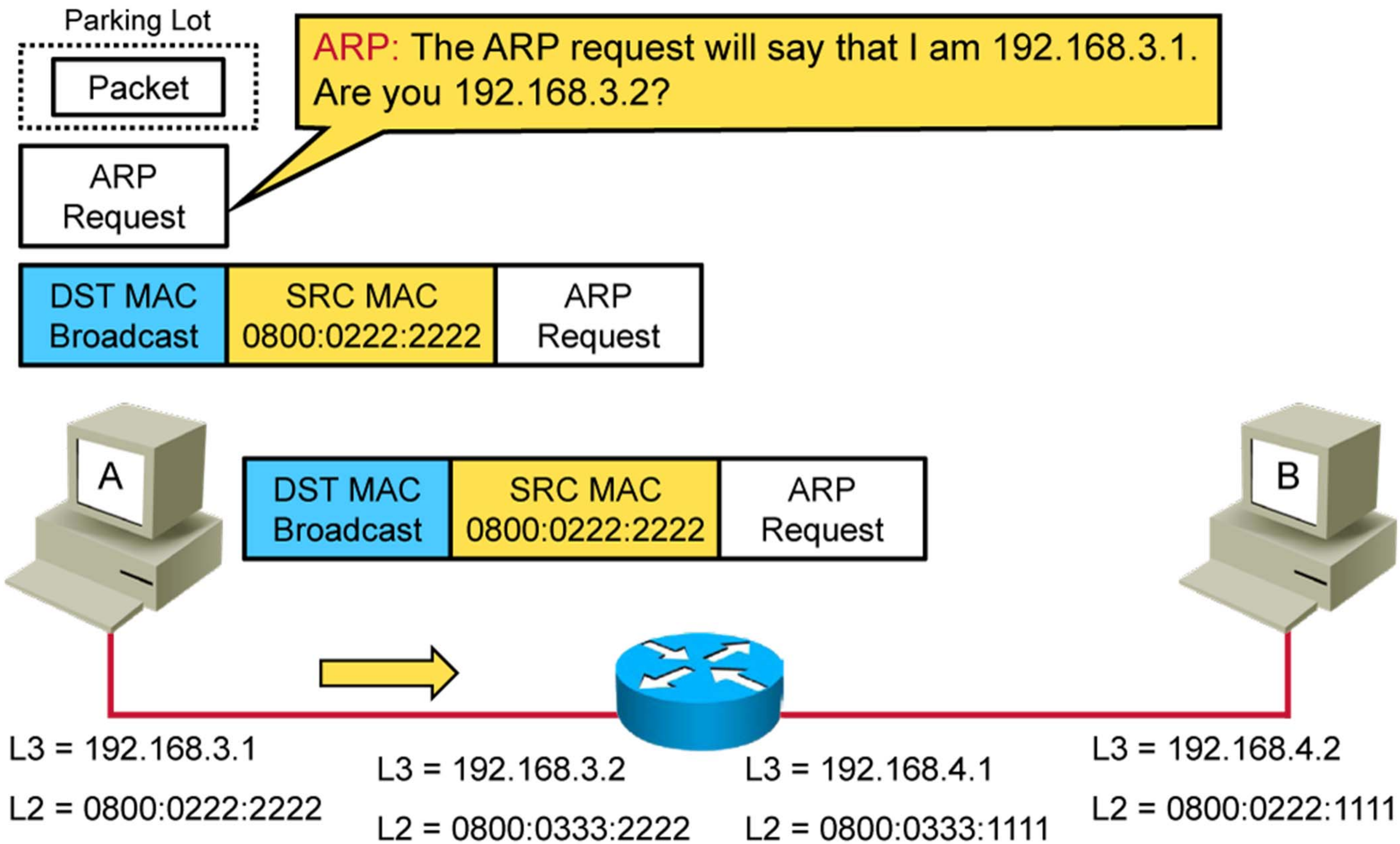
Host-to-Host Packet Delivery (Step 3 of 16)



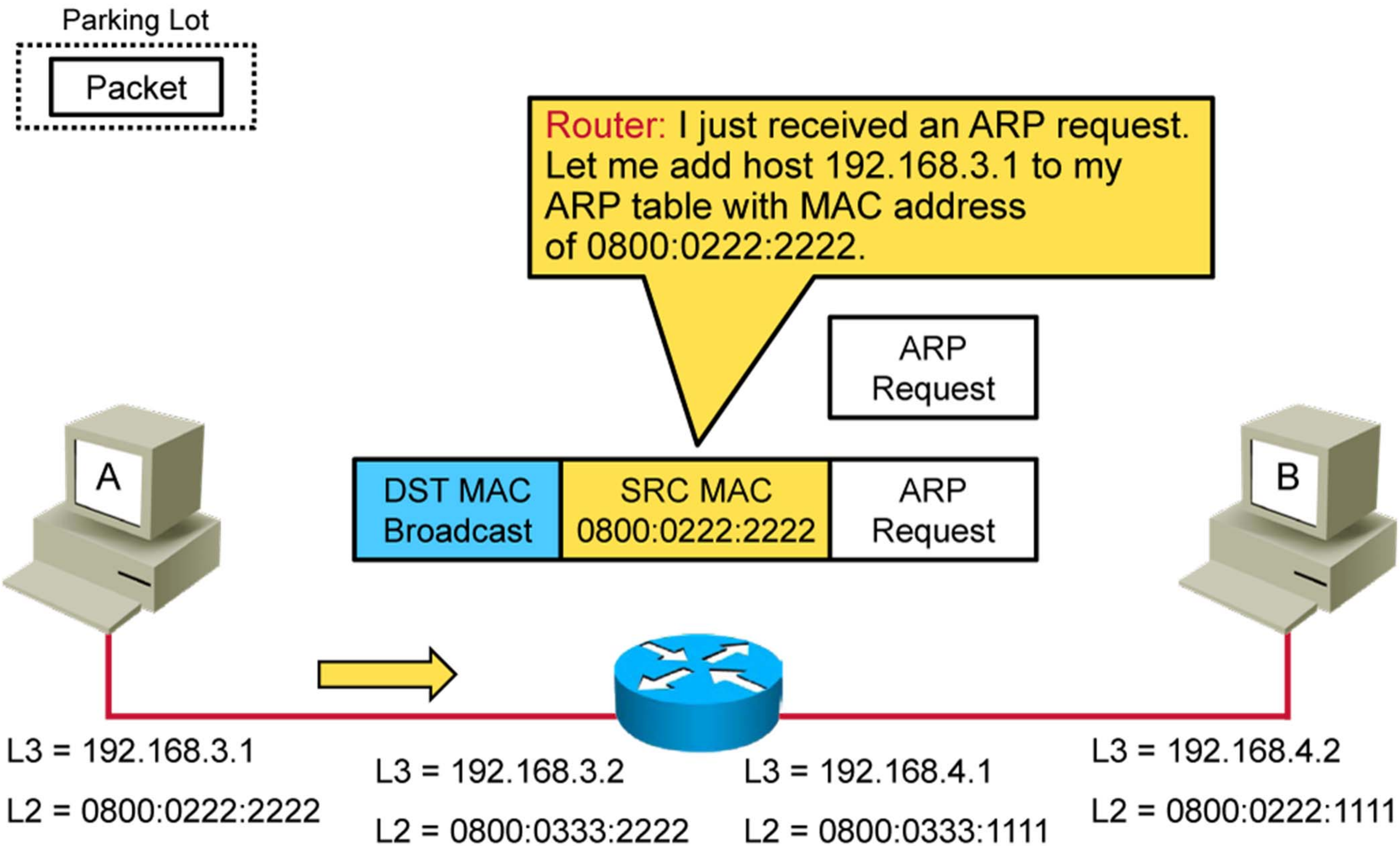
Host-to-Host Packet Delivery (Step 4 of 16)



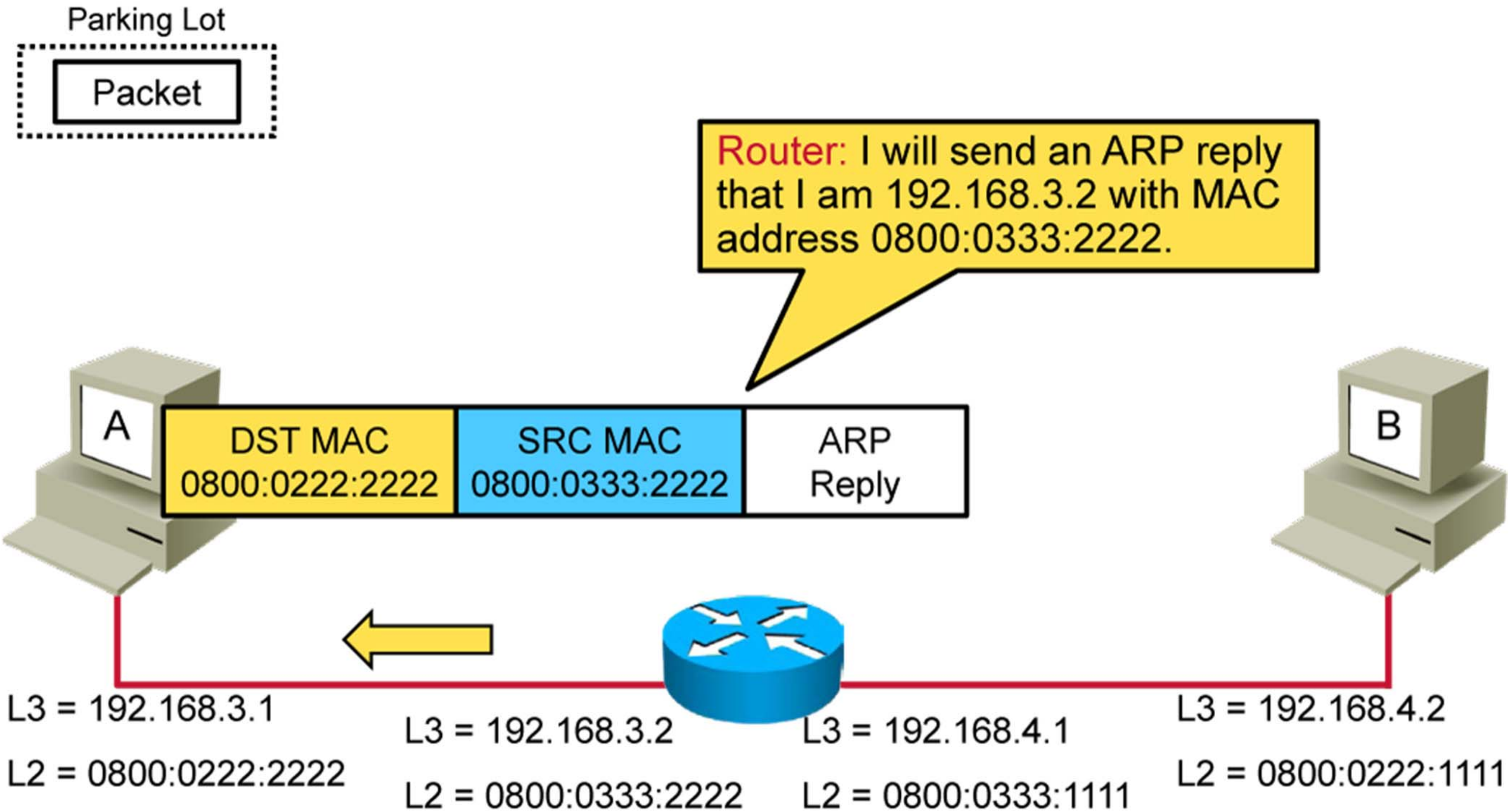
Host-to-Host Packet Delivery (Step 5 of 16)



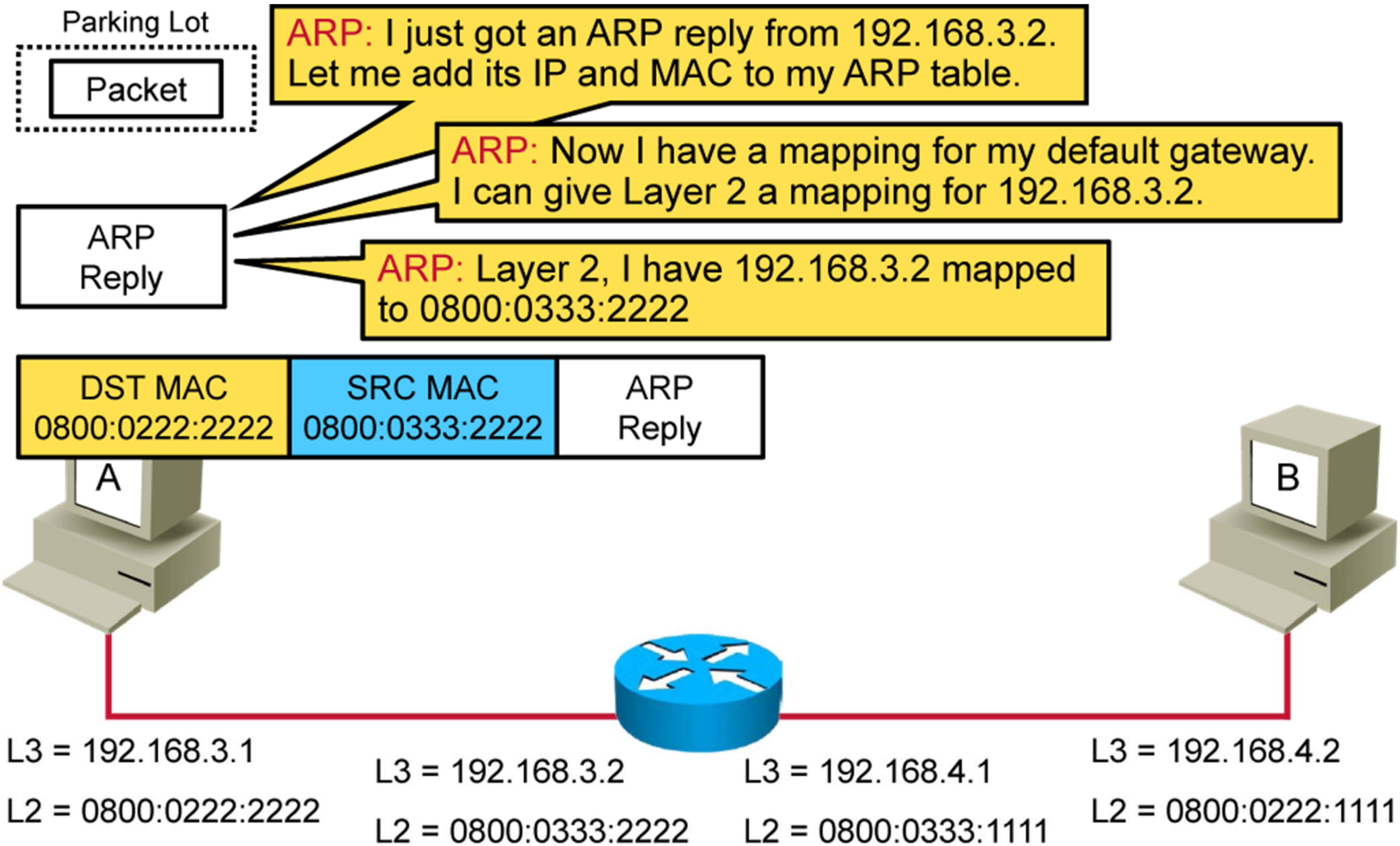
Host-to-Host Packet Delivery (Step 6 of 16)



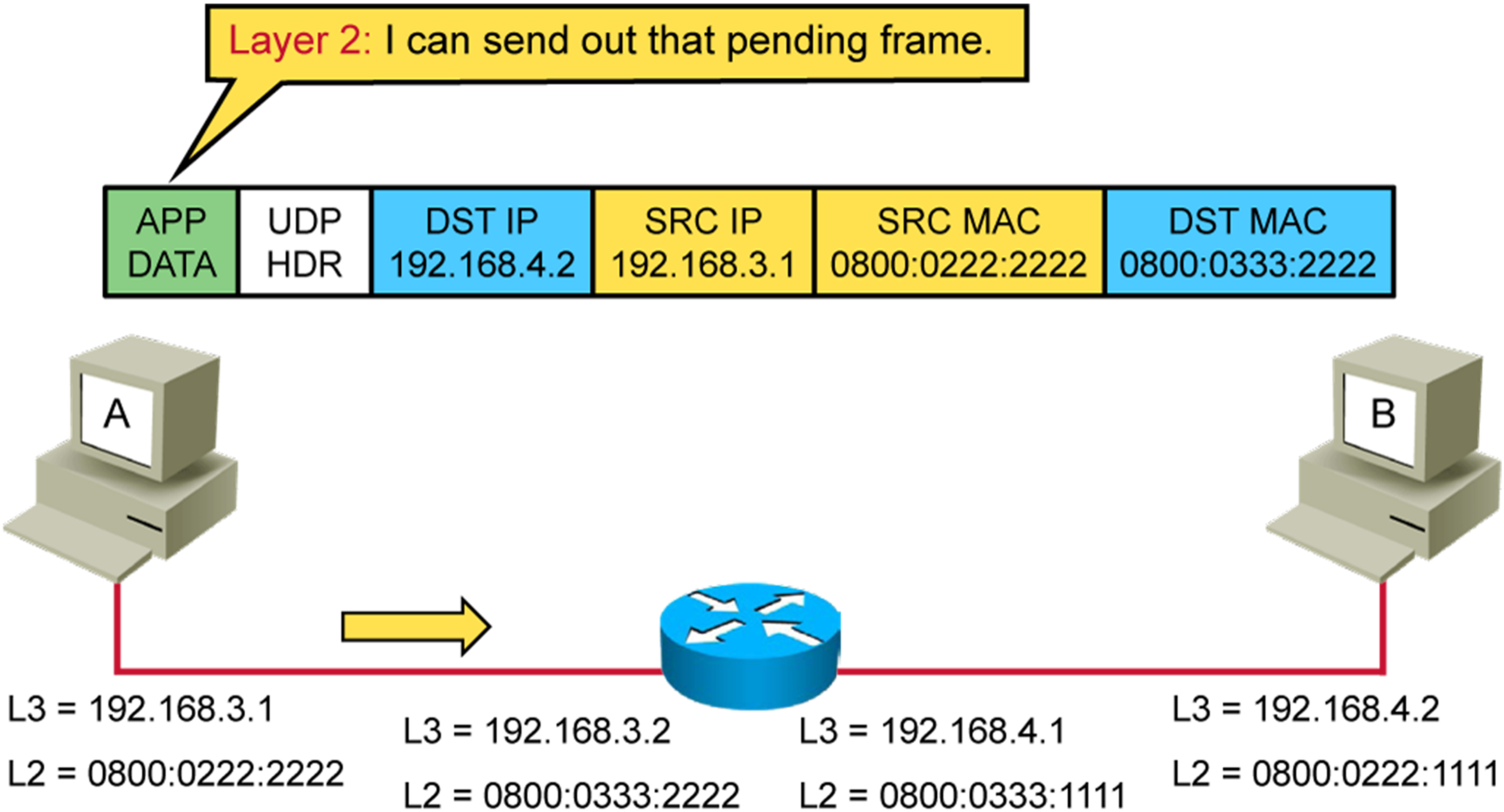
Host-to-Host Packet Delivery (Step 7 of 16)



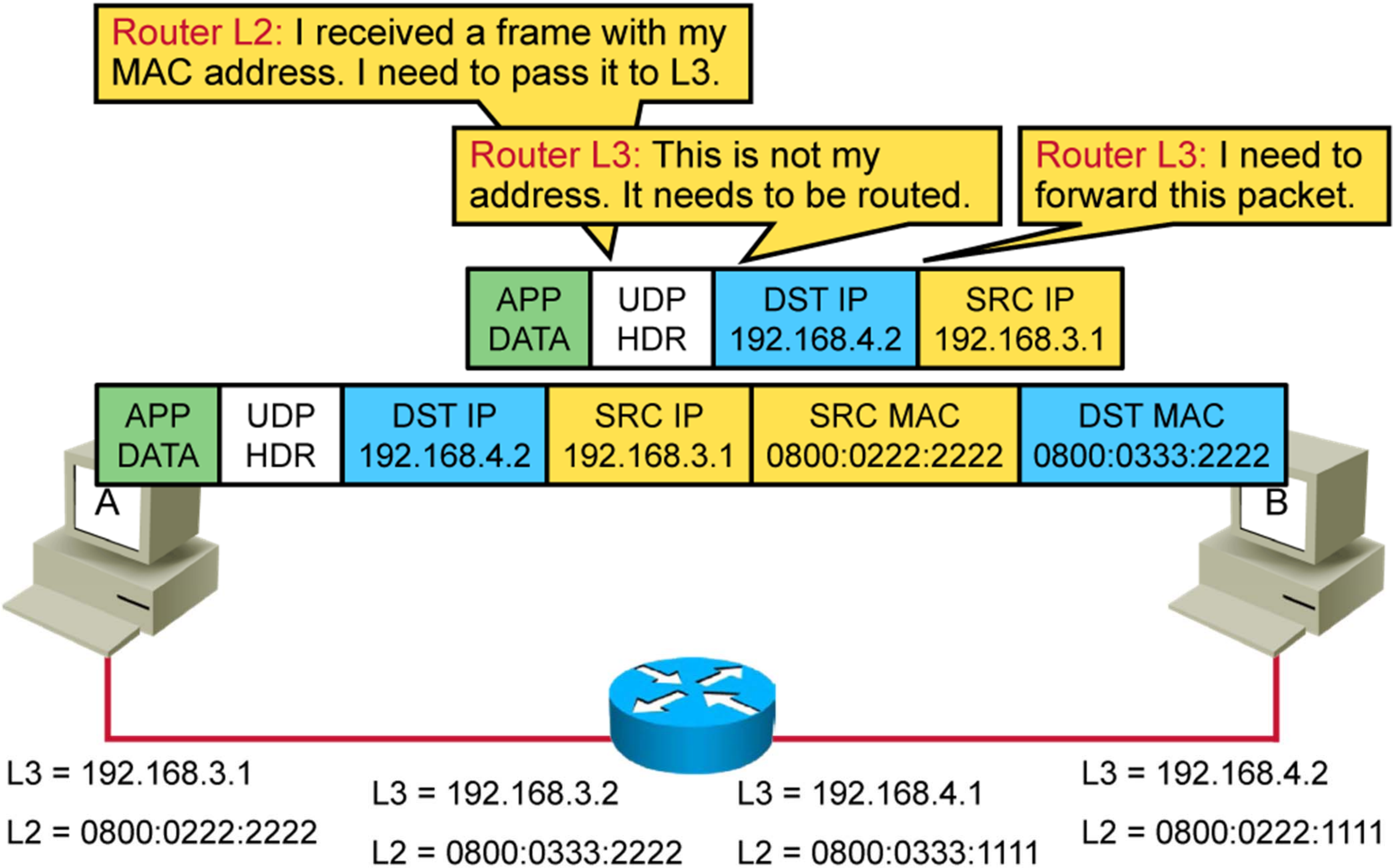
Host-to-Host Packet Delivery (Step 8 of 16)



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

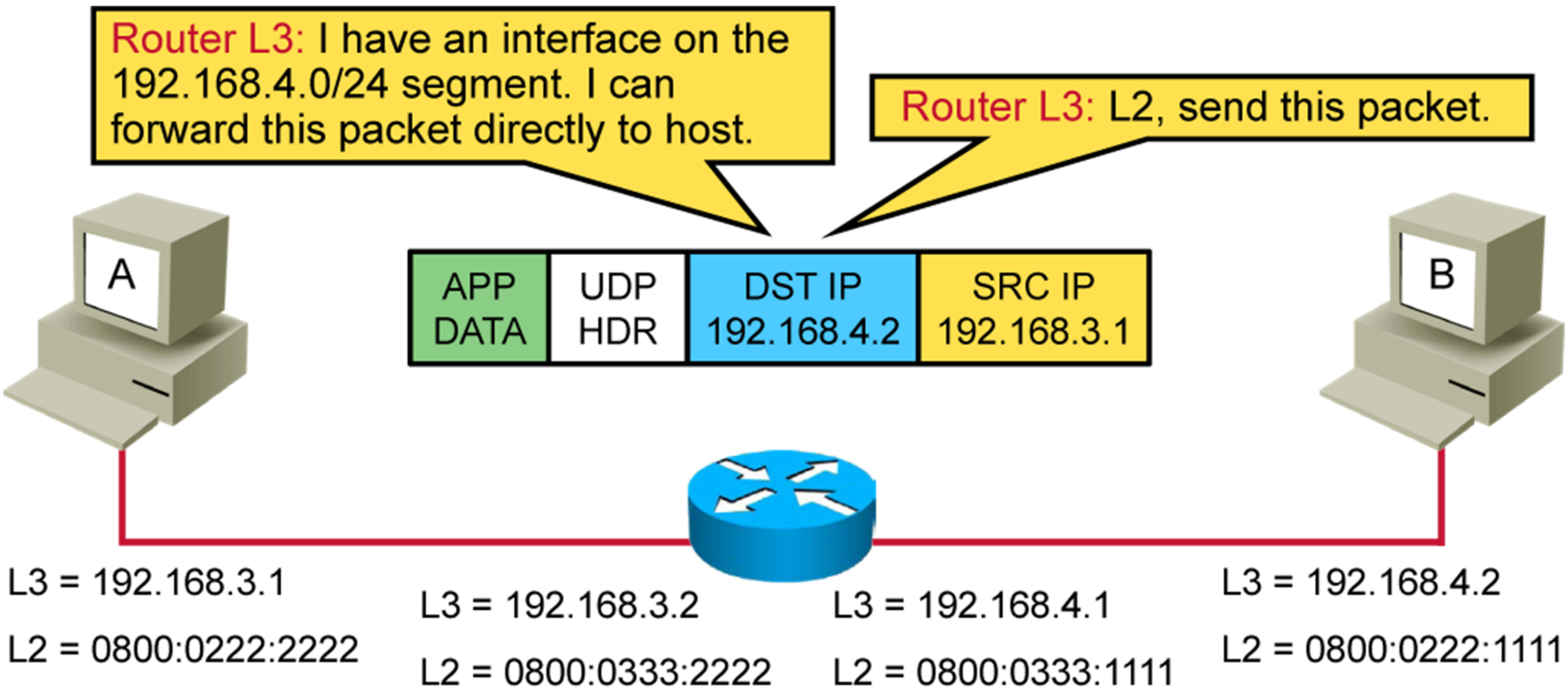


Host-to-Host Packet Delivery (Step 10 of 16)

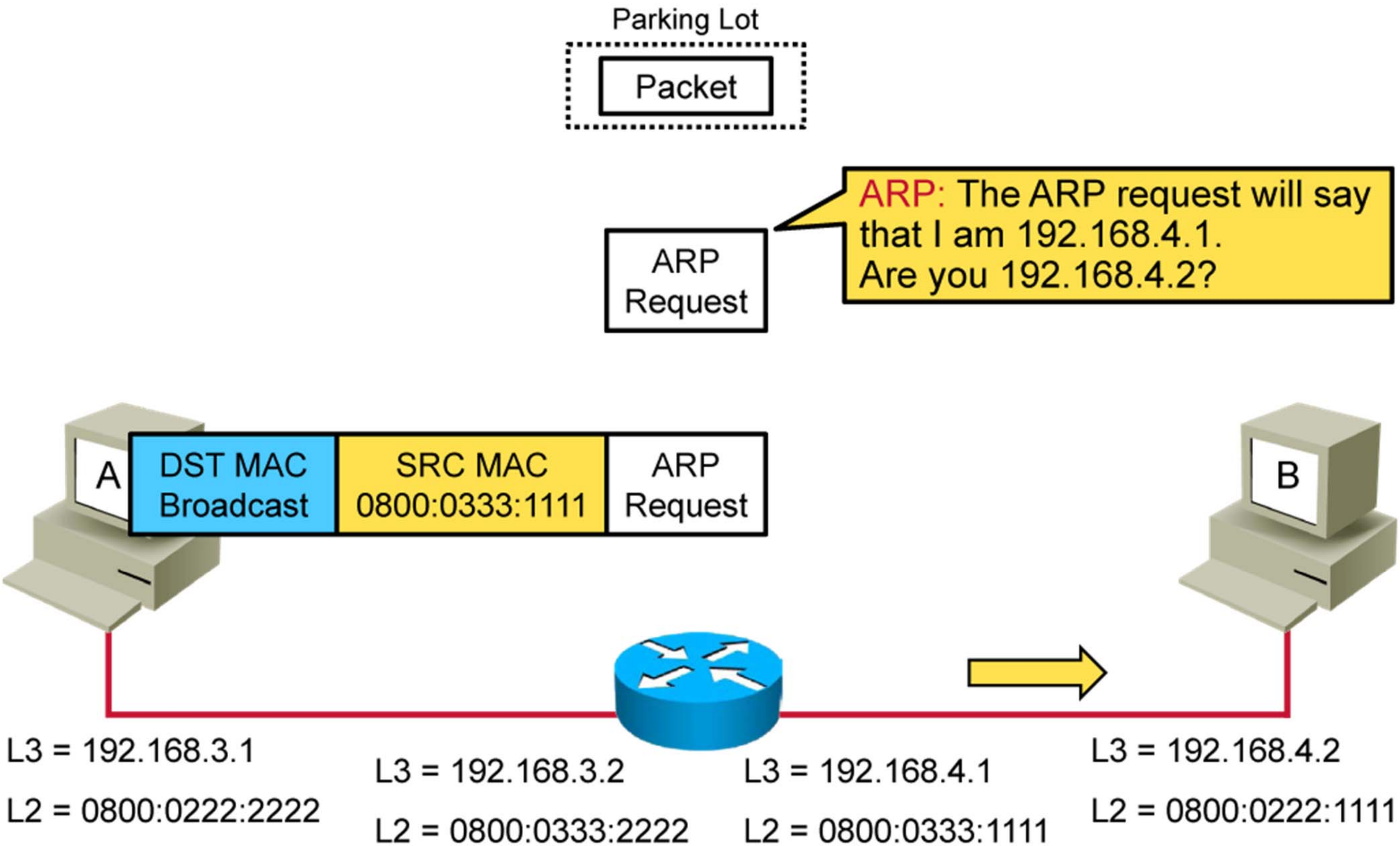


Host-to-Host Packet Delivery (Step 11 of 16)

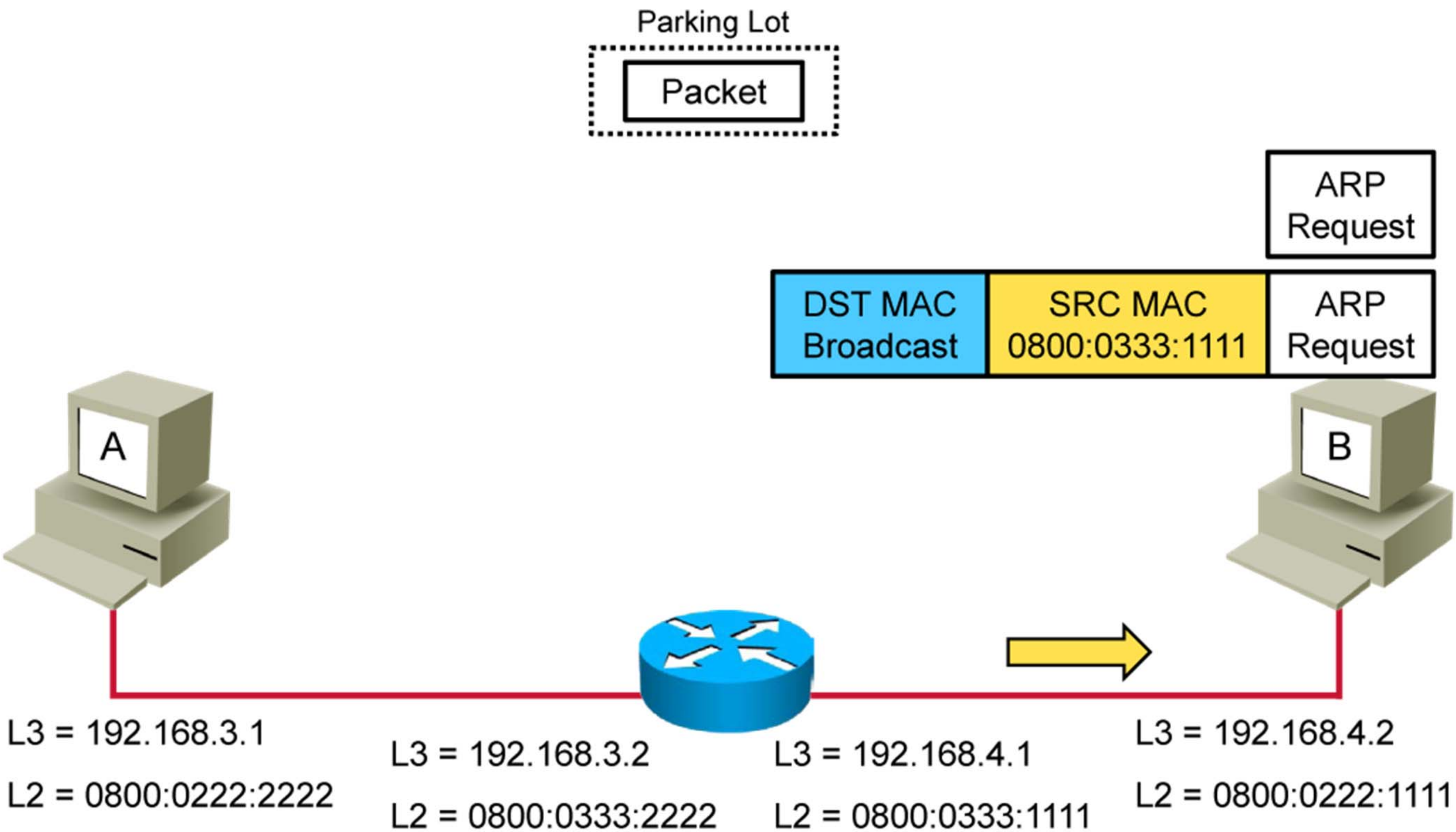
Destination	Next Hop	Interface
192.168.3.0/24	Connected	Gi 0/0
192.168.4.0/24	Connected	Gi 0/1



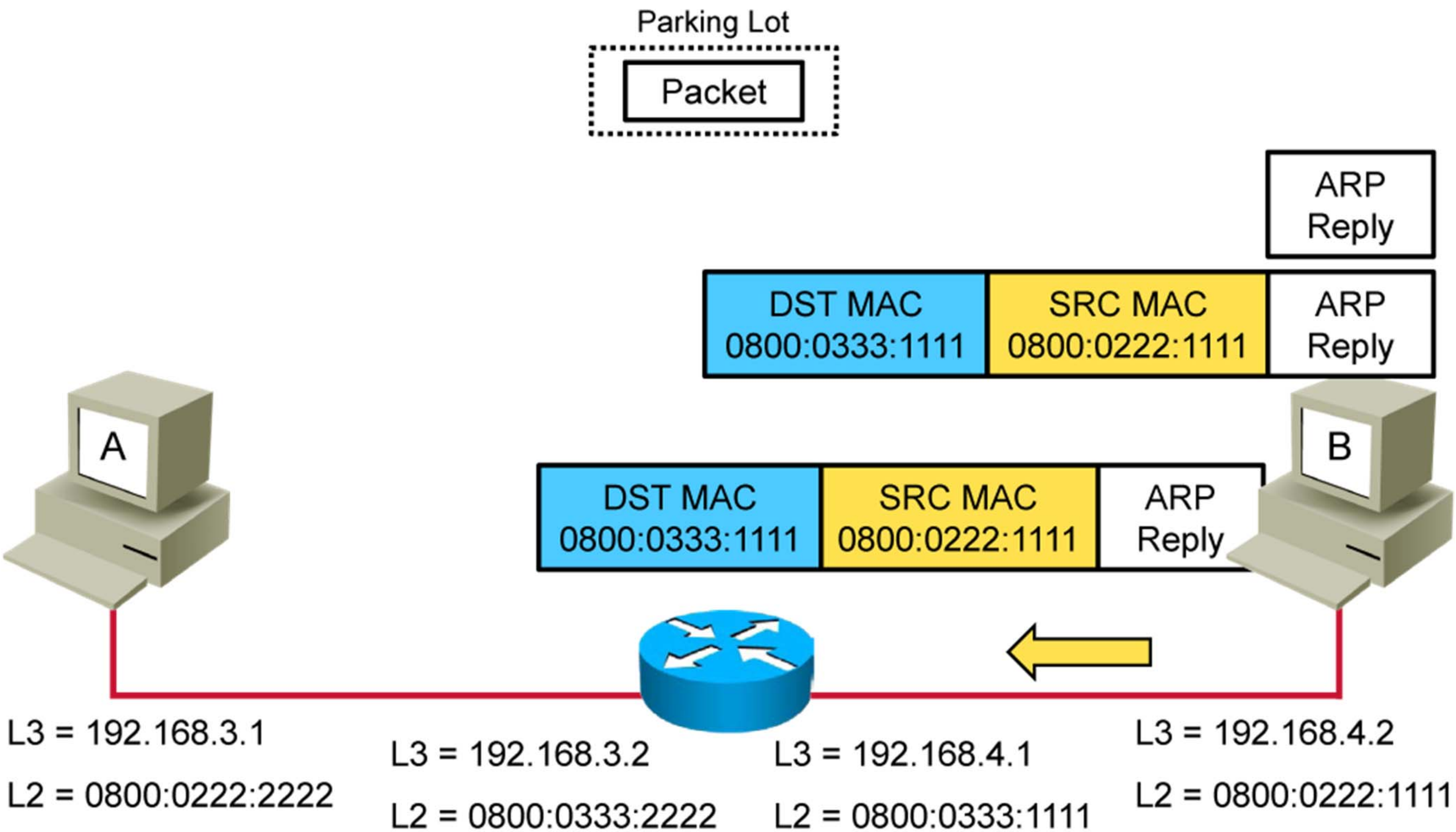
Host-to-Host Packet Delivery (Step 12 of 16)



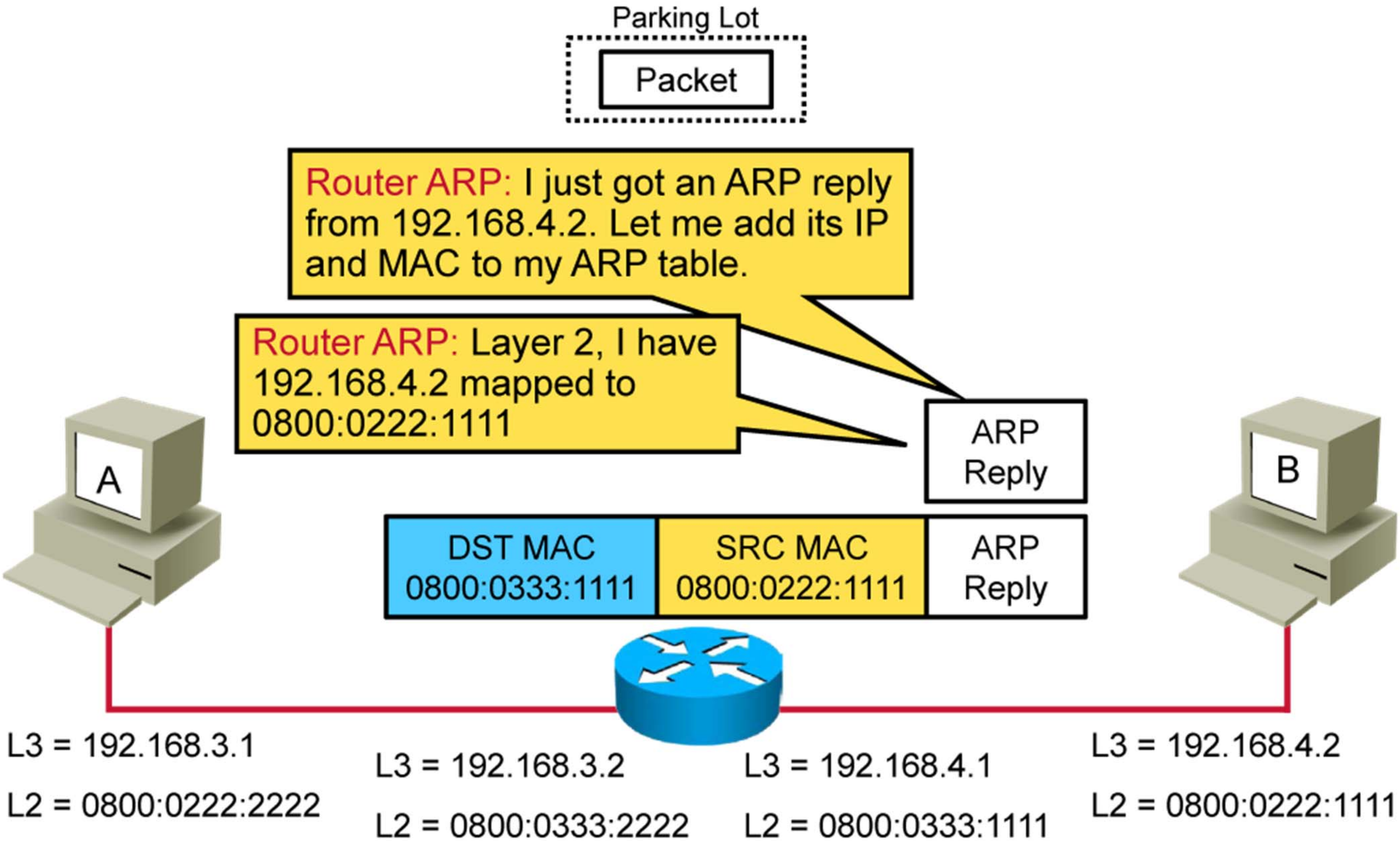
Host-to-Host Packet Delivery (Step 13 of 16)



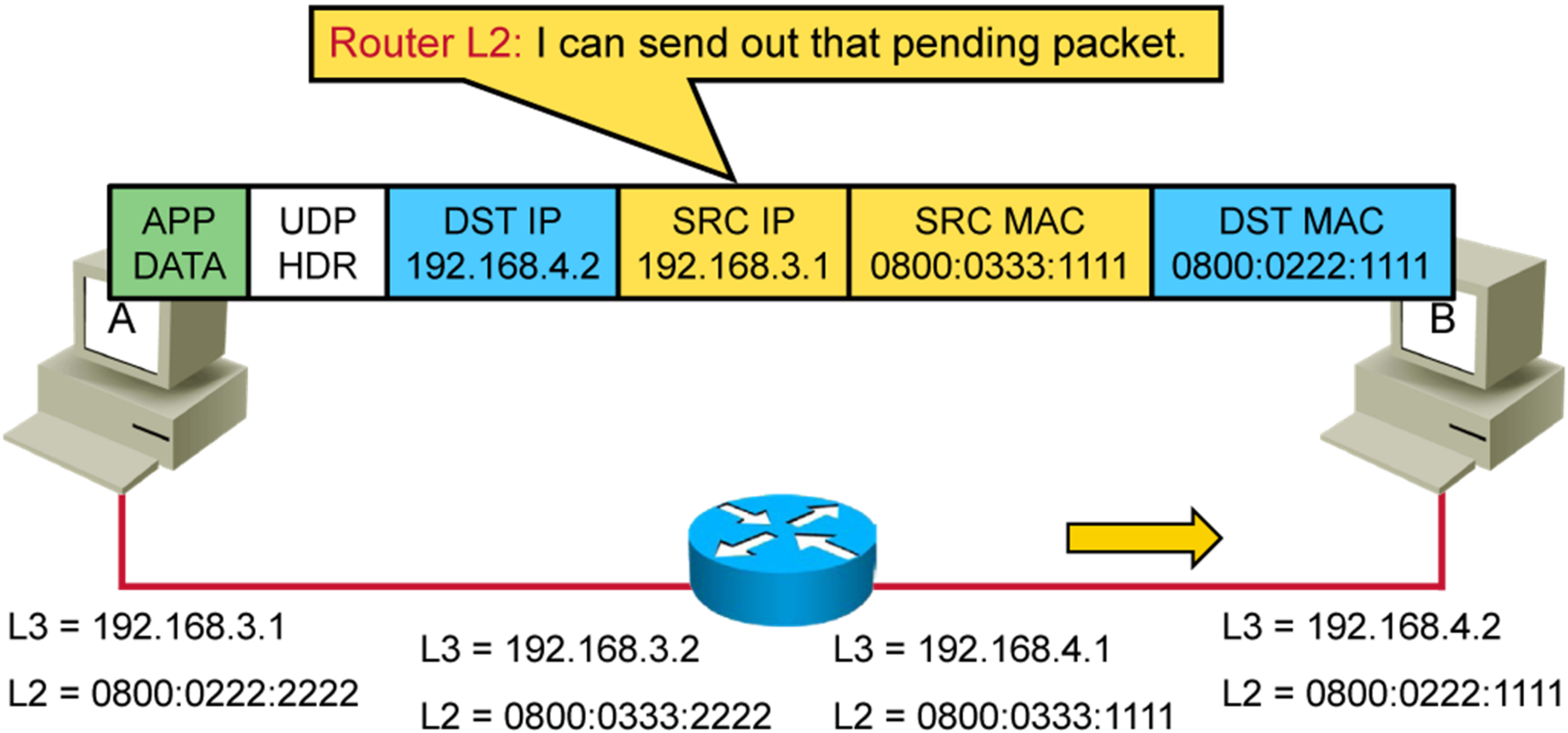
Host-to-Host Packet Delivery (Step 14 of 16)



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

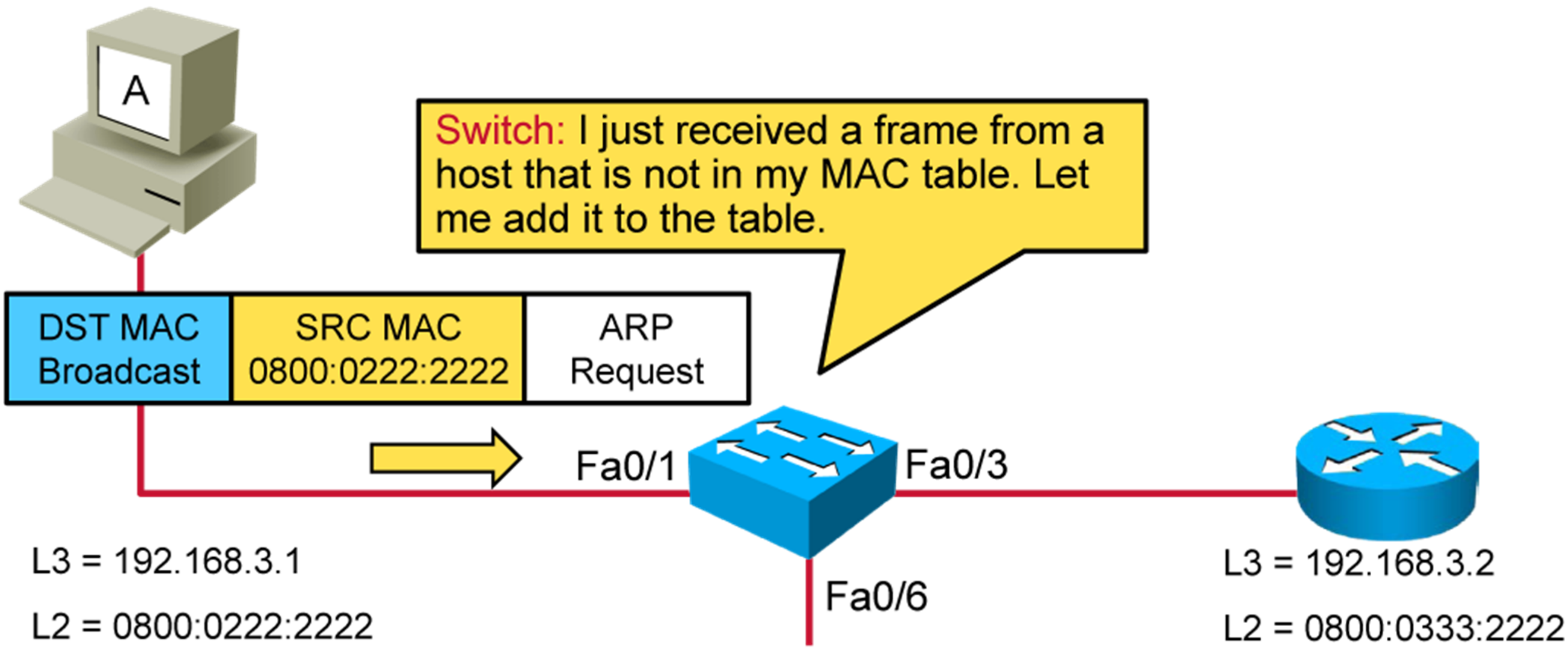


Host-to-Host Packet Delivery (Step 16 of 16)



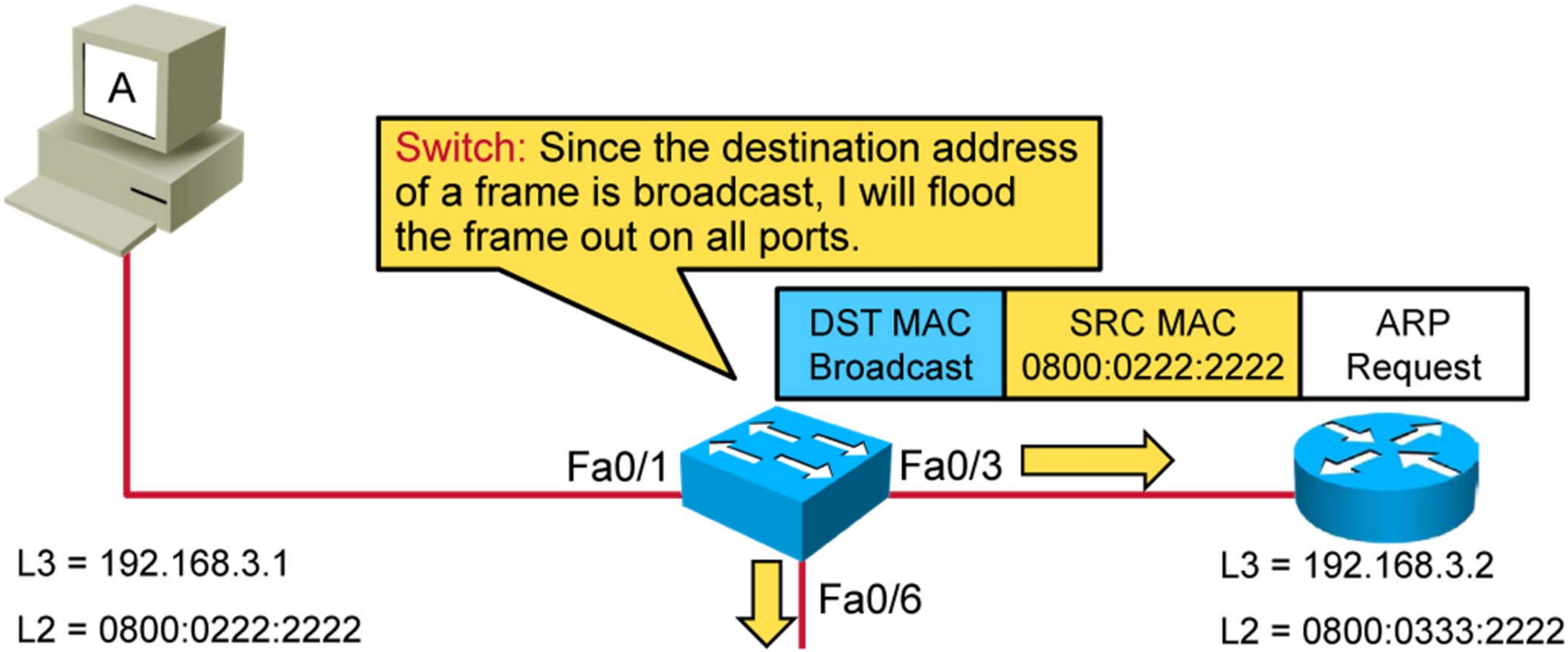
Role of a Switch in Packet Delivery (Step 1 of 4)

MAC	Port
0800:0222:2222	Fa0/1



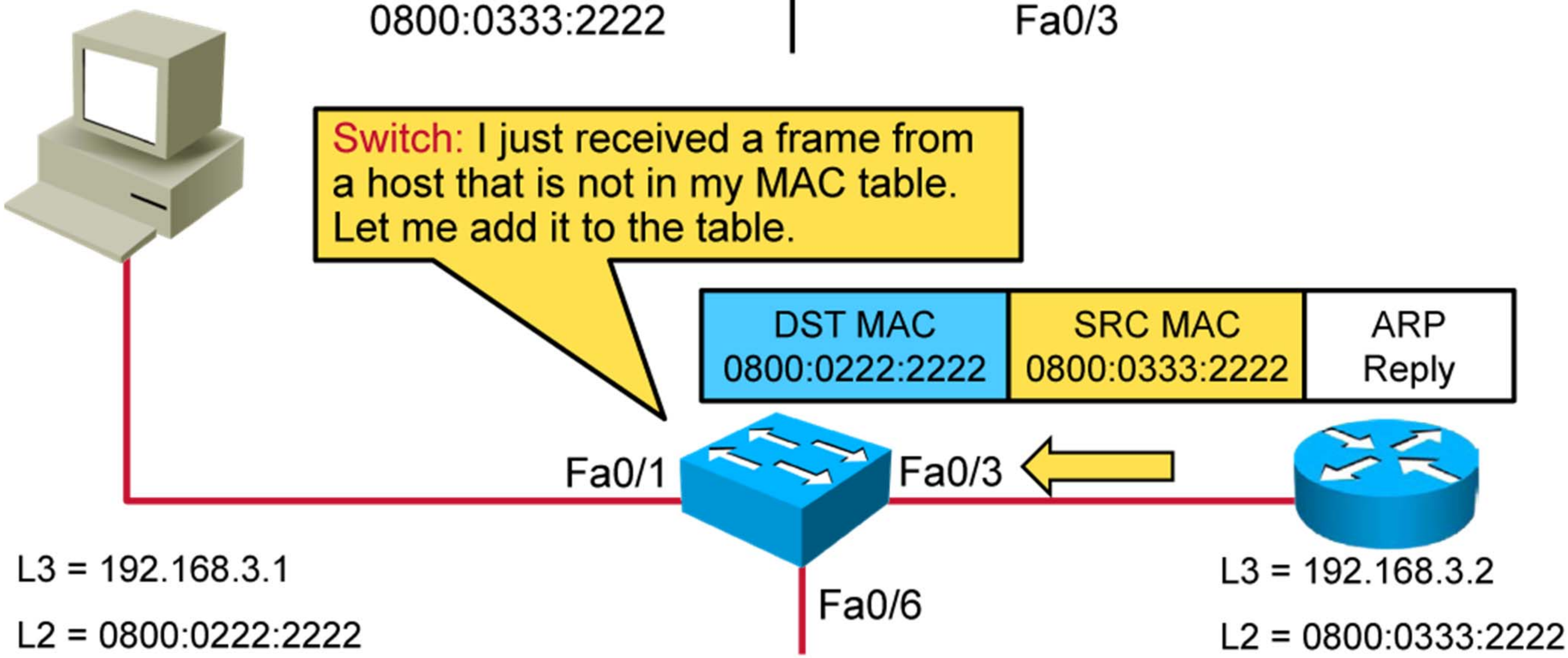
Role of a Switch in Packet Delivery (Step 2 of 4)

MAC	Port
0800:0222:2222	Fa0/1



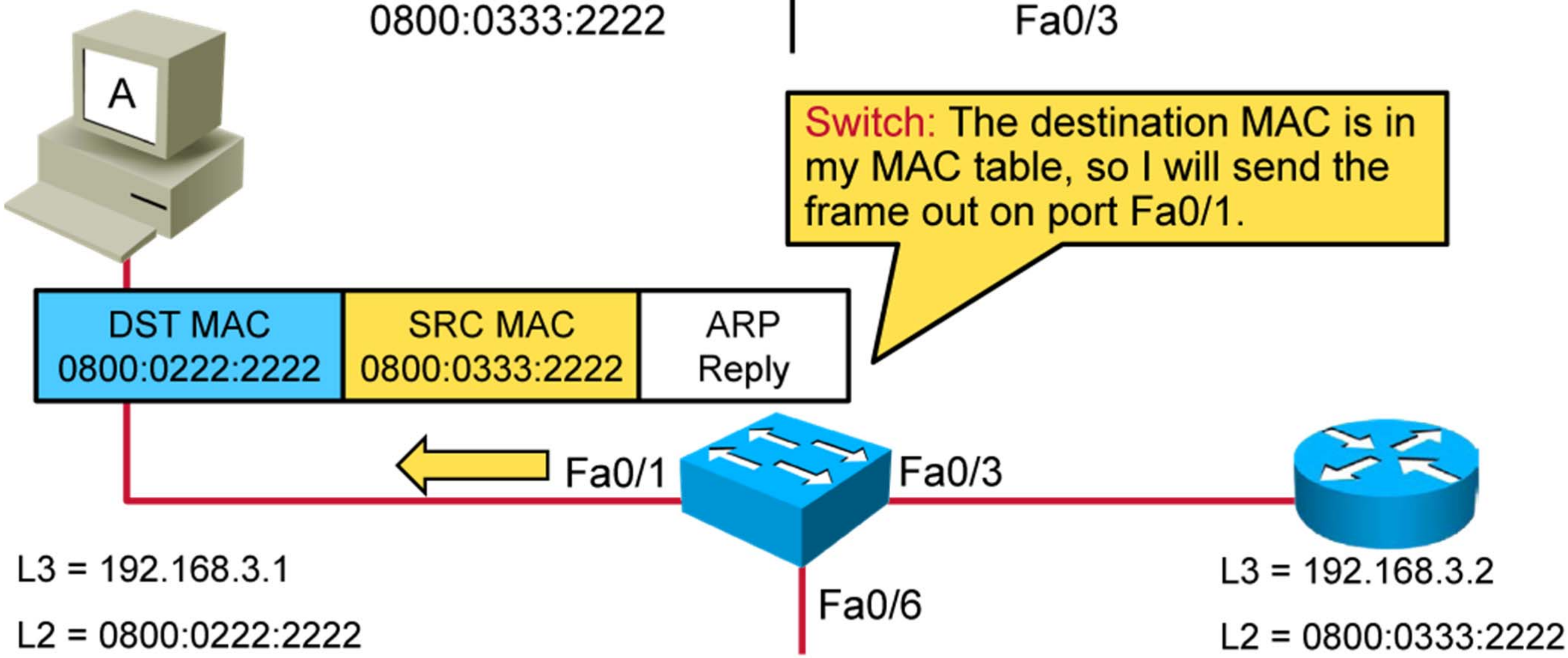
Role of a Switch in Packet Delivery (Step 3 of 4)

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



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

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



Summary

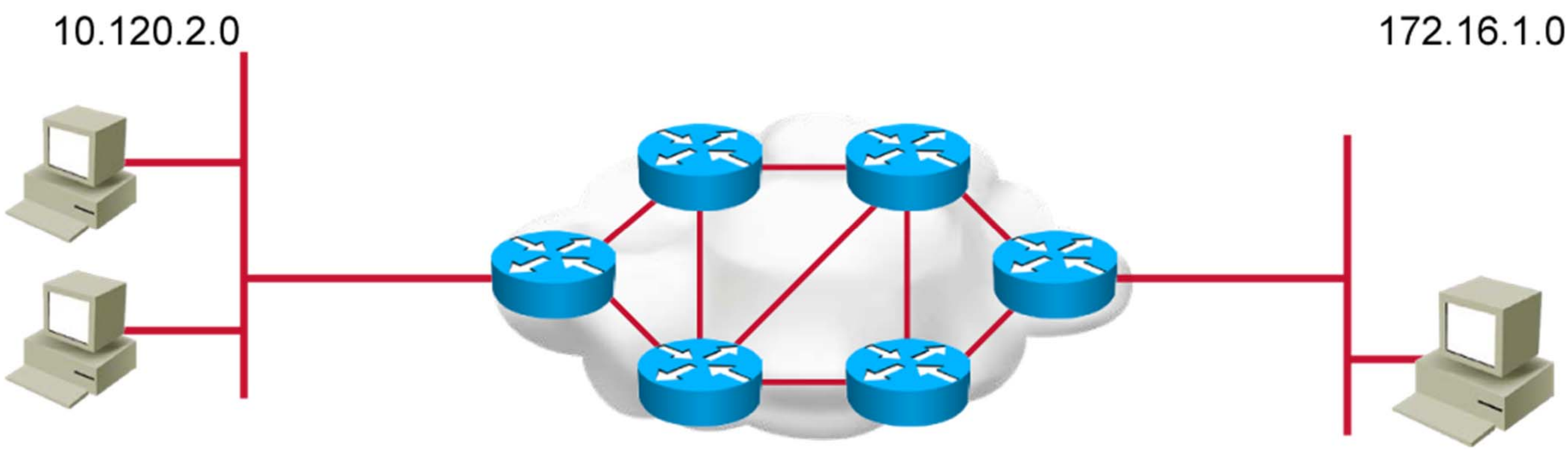
- If hosts are not in the same network, the frame is sent to the default gateway.
- Frames sent to the default gateway have the local host source MAC address and the default gateway destination MAC address.
- A router changes the Layer 2 address as needed, but it does not change the Layer 3 address.
- The switch does not change the frame in any way, it just forwards the frame out on the proper port according to the MAC address table.

Enabling Static Routing

Establishing Internet Connectivity

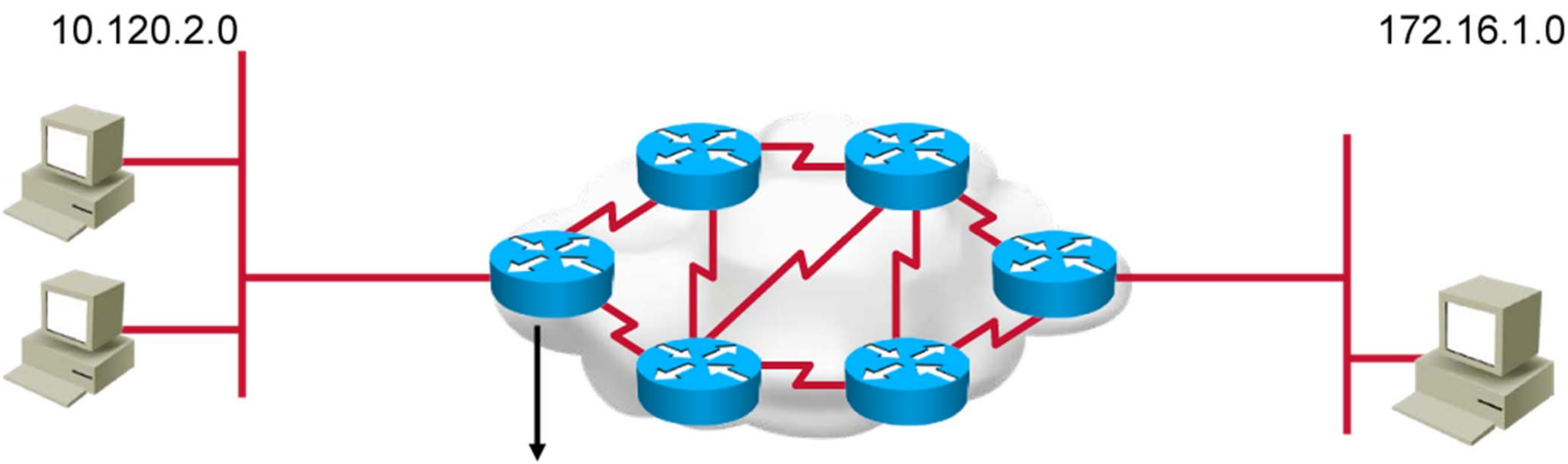
Routing Operations

- Path identification and selection:
  - Discovers possible routes to the intended destination
  - Selects the best route
  - Maintains and verifies the routing information
- Packet forwarding:
  - Router identifies the destination address



Routing Operations (Cont.)

- A router must learn about destinations that are not directly connected to it.
- The routing table is used to determine the best path to the destination.



Network Protocol	Destination Network	Exit Interface	Next Hop
Connected	10.120.2.0	fa0/0	
Learned	172.16.1.0	s0/0/0	172.20.1.2

Static and Dynamic Routing Comparison

Static routes:

- A network administrator manually enters static routes into the router.
- A network topology change requires a manual update to the route.
- Routing behavior can be precisely controlled.

Dynamic routes:

- A network routing protocol automatically adjusts dynamic routes when the topology or traffic changes.
- Routers learn and maintain routes to the remote destinations by exchanging routing updates.
- Routers discover new networks by sharing routing table information.

When to Use Static Routing

Use static routes:

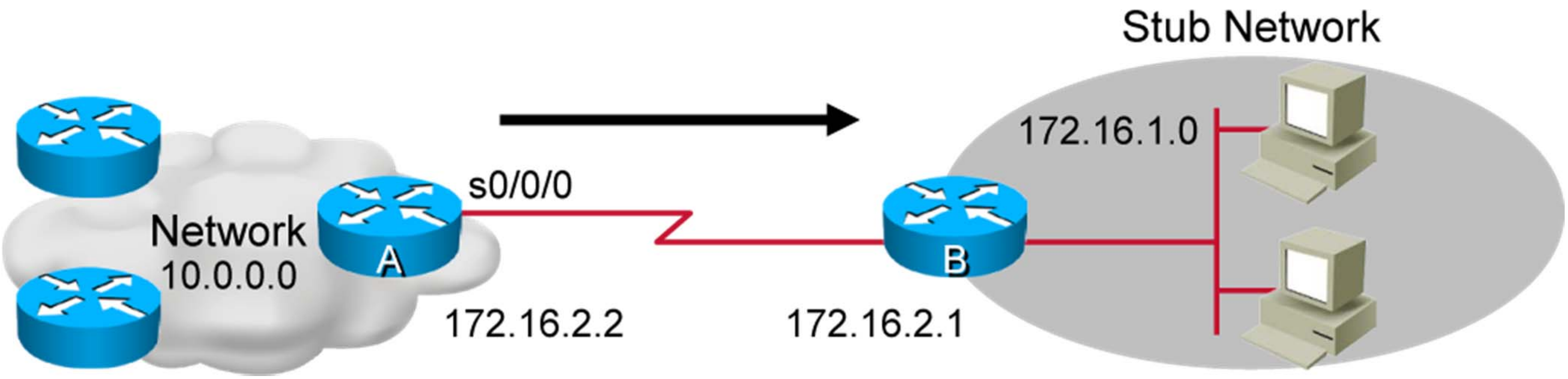
- In a small network that requires only simple routing
- In a hub-and-spoke network topology
- When you want to create a quick ad hoc route

Do *not* use static routes:

- In a large network
- When the network is expected to scale

Static Route Configuration

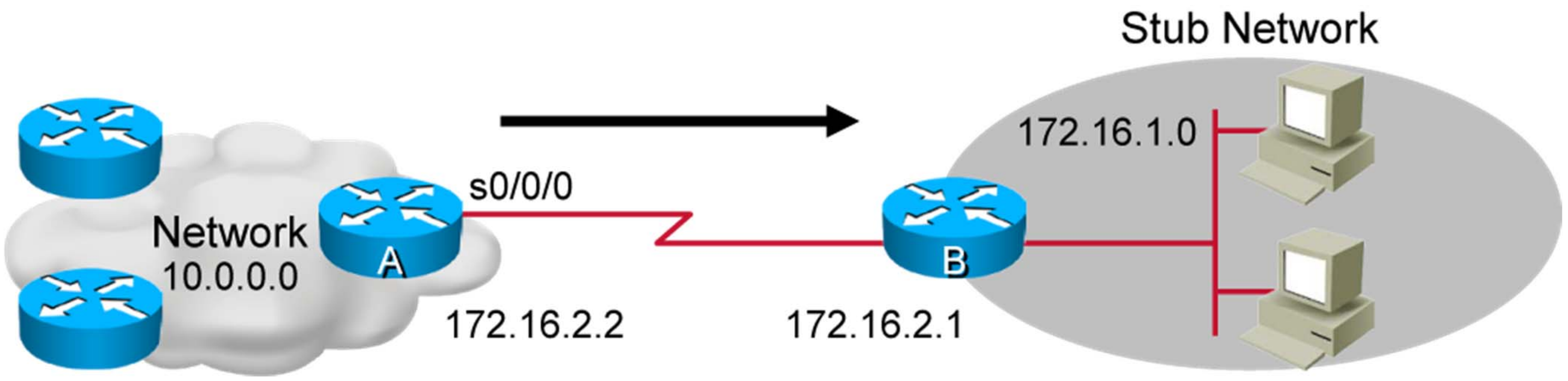
Configure unidirectional static routes to and from a stub network to allow communication to occur.



Static Route Configuration (Cont.)

Static route configuration steps:

- Define a path to an IP destination network (172.16.1.0 255.255.255.0).
- Use the IP address of the next-hop router (172.16.2.1).
- Or, use the outbound interface of the local router (serial 0/0/0).

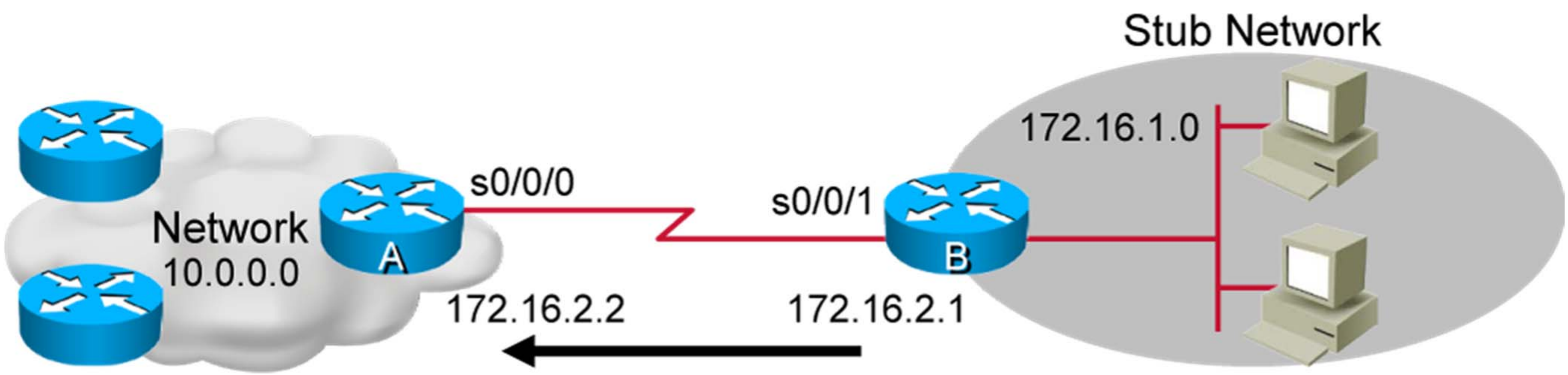


Static route pointing to next-hop IP.

```
RouterA(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

Default Routes

This route allows the stub network to reach all known networks beyond Router A.



Default route pointing to next-hop IP.

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

Default route pointing to exit interface.

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

Static Route Configuration Verification

```
RouterA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

<output omitted>

Gateway of last resort is not set

   10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, FastEthernet0/0
   172.16.0.0/24 is subnetted, 2 subnets
S    172.16.1.0/24 [1/0] via 172.16.2.1
C    172.16.2.0/24 is directly connected, Serial0/0/0
L    172.16.2.2/32 is directly connected, Serial0/0/0
```

Static Route Configuration Verification (Cont.)

To verify static routes in the routing table, examine the routing table with the **show ip route** command:

- Includes network address and subnet mask as well as IP address of next-hop router or exit interface
- Denoted with the code "*S*" in the routing table

Routing tables must contain directly connected networks that are used to connect remote networks before static or dynamic routing can be used.

Verifying the Default Route Configuration

To verify the default route configuration, examine the routing table on RouterB:

```
RouterB#show ip route
Codes: L - local, C - connected, S - static,
R - RIP, M - mobile, B - BGP

<output omitted>

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0/24 is directly connected, FastEthernet0/0
C       172.16.2.0/24 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 172.16.2.2
```

Summary

- Routing is the process by which items get from one location to another. Routers can forward packets over static routes or dynamic routes.
- Static routes are entered manually by a network administrator. Dynamic routes are learned by a routing protocol, and dynamic routes change automatically when circumstances in the network change.
- Unidirectional static routes must be configured to and from a stub network to allow communication to occur.
- The **ip route** command can be used to configure default route forwarding.
- The **show ip route** command is used to verify that static routing is properly configured. Static routes are signified in the command output by “S” in the first position.

Managing Traffic Using ACLs

Establishing Internet Connectivity

Understanding ACLs

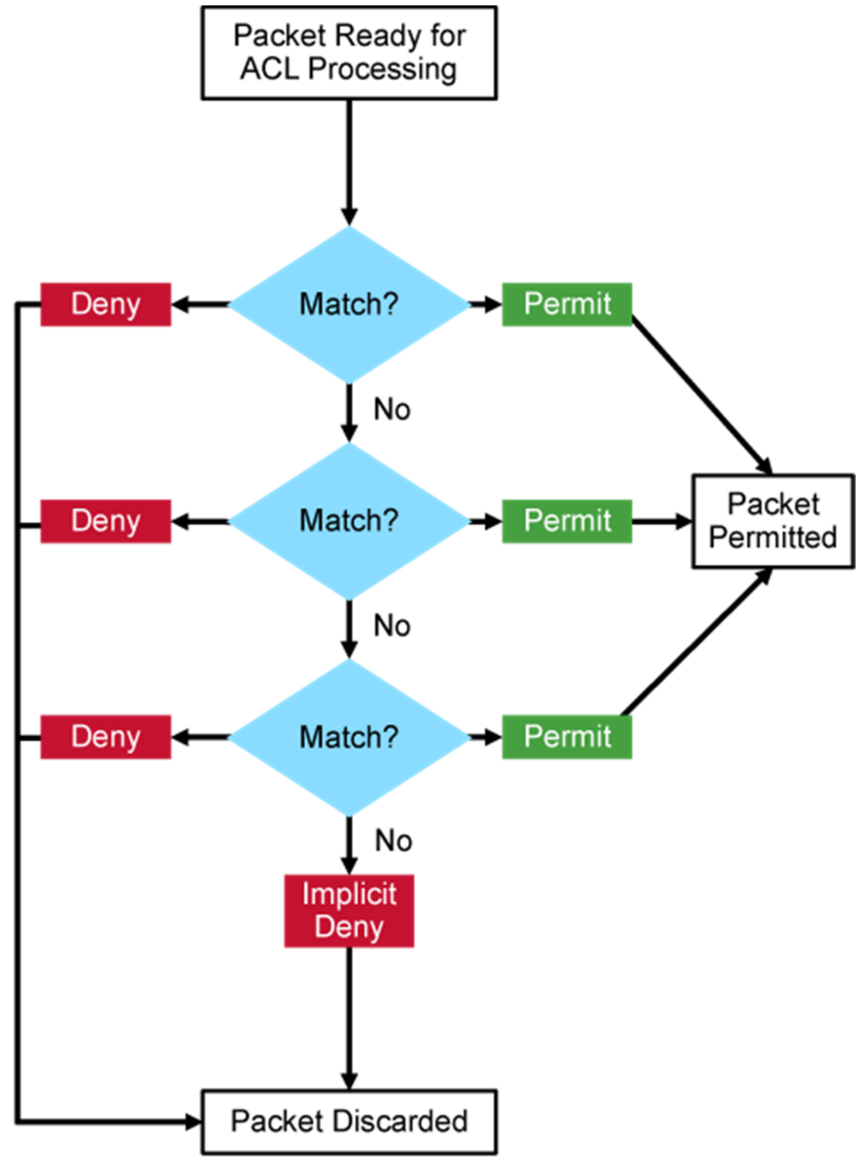
What is an ACL?

- An ACL is a Cisco IOS tool for traffic identification.
- An ACL is a list of permit and deny statements.
- An ACL identifies traffic based on the information within the IP packet.
- After traffic is identified, different actions can be taken.
- ACLs can be used on routers and switches.

ACL Operation

ACL tests:

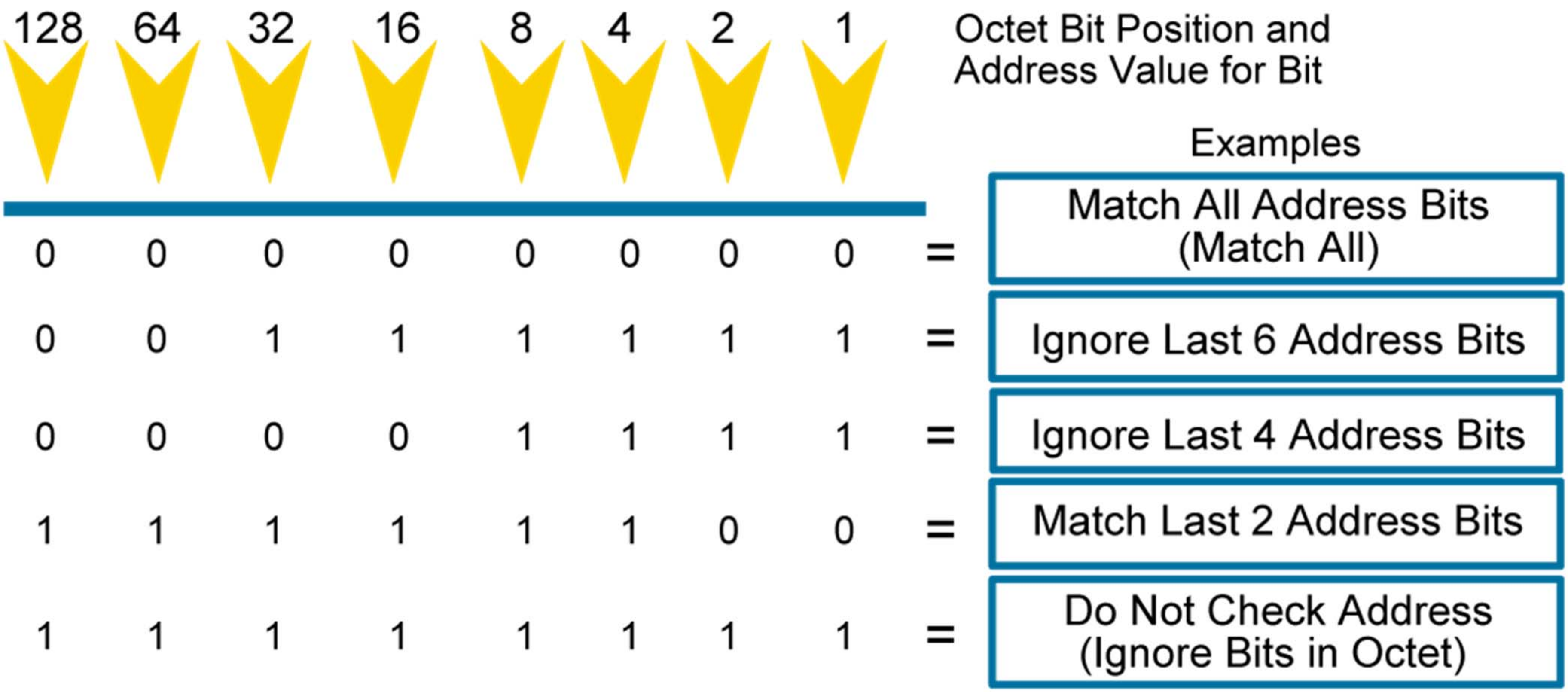
- An ACL consists of a series of permit and deny statements.
- An ACL is consulted in top-down order.
- The first match executes the permit or deny action and stops further ACL matching.
- There is an implicit deny all statement at the end of each ACL.



ACL Wildcard Masking

Wildcard bits—how to check the corresponding address bits:

- 0 means to match the value of the corresponding address bit.
- 1 means to ignore the value of the corresponding address bit.



ACL Wildcard Masking (Cont.)

Filter for IP subnets 170.30.**16**.0/24 to 172.30.**31**.0/24.

Address and wildcard mask:

172.30.16.0 0.0.15.255

ACL Wildcard Masking (Cont.)

This example shows the wildcard masking process for IP subnets.

Network.Host

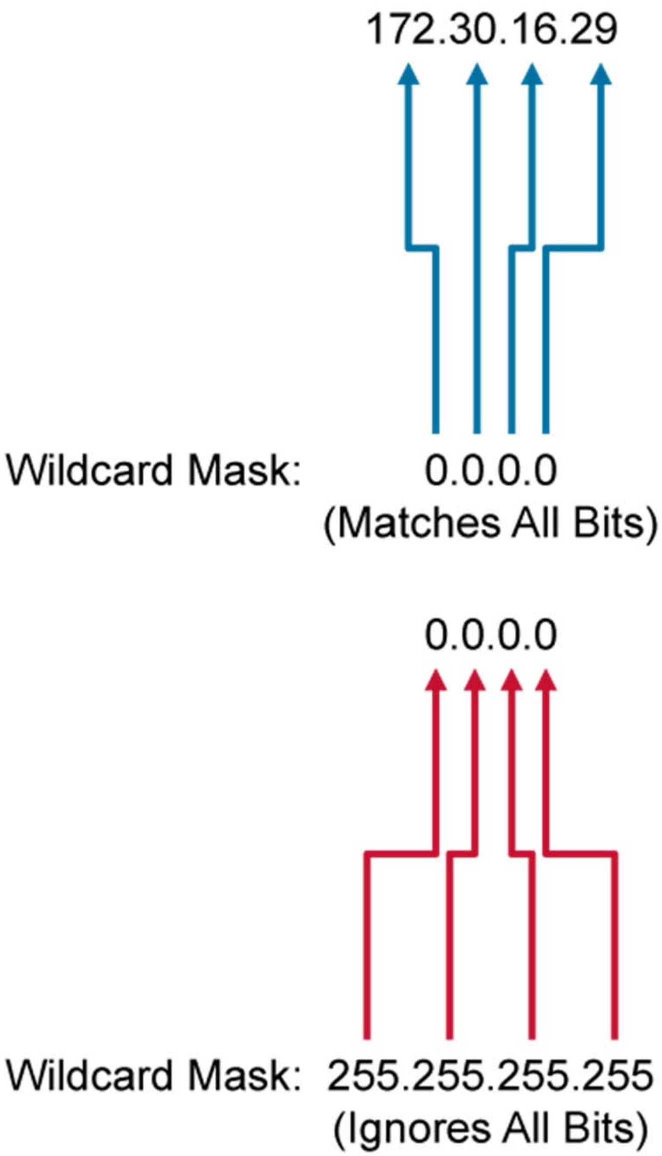
172.30.16.0

	0	0	0	1	0	0	0	0		
Wildcard Mask:	0	0	0	0	1	1	1	1		
	|<---- Match			---- >|	< ---- Don't Care			---->|		
	0	0	0	1	0	0	0	0	=	16
	0	0	0	1	0	0	0	1	=	17
	0	0	0	1	0	0	1	0	=	18
				:						:
	0	0	0	1	1	1	1	1	=	31

Wildcard Bit Mask Abbreviations

Using wildcard bit mask abbreviations:

- 172.30.16.29 0.0.0.0 matches all of the address bits.
- Abbreviate this wildcard mask using the IP address preceded by the keyword **host** (**host 172.30.16.29**).
- 0.0.0.0 255.255.255.255 ignores all address bits.
- Abbreviate *expression* with the keyword ***any***.



Types of ACLs

Two main types of ACLs:

- Standard ACL:
  - Checks source IP address
  - Permits or denies entire protocol suite
- Extended ACL:
  - Checks source and destination IP address
  - Generally permits or denies specific protocols and applications

Two methods that you can use to identify standard and extended ACLs:

- Numbered ACLs
- Named ACLs

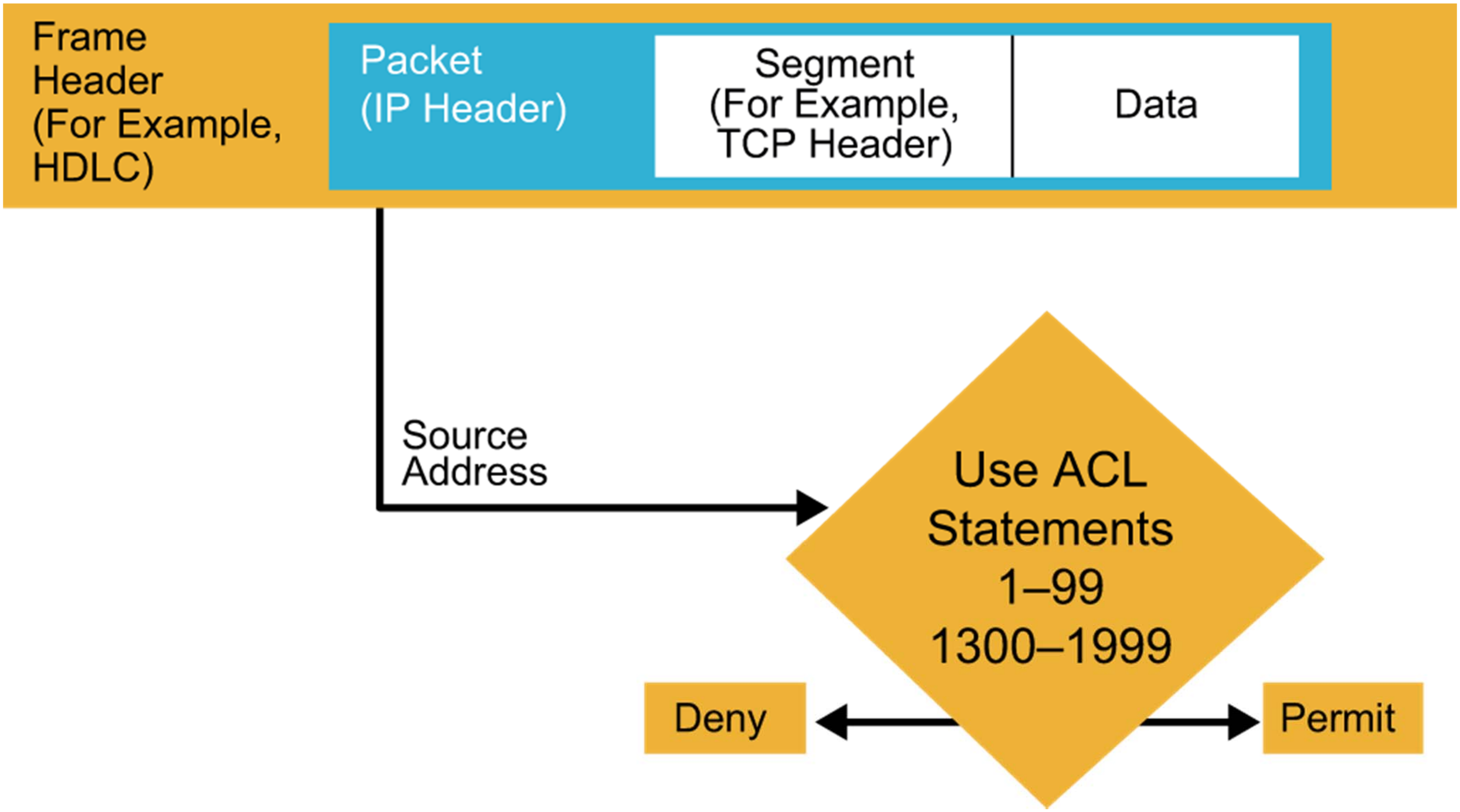
Types of ACLs (Cont.)

How to identify ACLs:

- Numbered standard IPv4 ACLs (1 to 99) test conditions of all IP packets for source addresses. The expanded range is 1300 to 1999.
- Numbered extended IPv4 ACLs (100 to 199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports. The expanded range is 2000 to 2699.
- Named ACLs identify IP standard and extended ACLs with an alphanumeric string (name).

IPv4 ACL Type	Number Range or Identifier
Numbered Standard	1–99, 1300–1999
Numbered Extended	100–199, 2000–2699
Named (Standard and Extended)	Name

Testing An IP Packet Against a Numbered Standard Access List



Basic Configuration of Numbered Standard IPv4 ACLs

Configure a numbered standard IPv4 ACL:

- Standard ACL configuration uses 1 to 99, or 1300 to 1999, for the ACL number (1 in the example).

```
RouterX(config)#access-list 1 permit 172.16.0.0 0.0.255.255
```

- The default wildcard mask is 0.0.0.0 (only standard ACL).

Display the current ACLs configured on RouterX:

```
RouterX#show access-lists
Standard IP access list 1
     10 permit 172.16.0.0, wildcard bits 0.0.255.255
```

Basic Configuration of Numbered Standard IPv4 ACLs (Cont.)

Delete a numbered standard IPv4 ACL:

```
RouterX(config)#no access-list 1
RouterX(config)#exit
RouterX#show access-lists
RouterX#
```

- Use the **no access-list 1** command to remove the entire ACL 1.

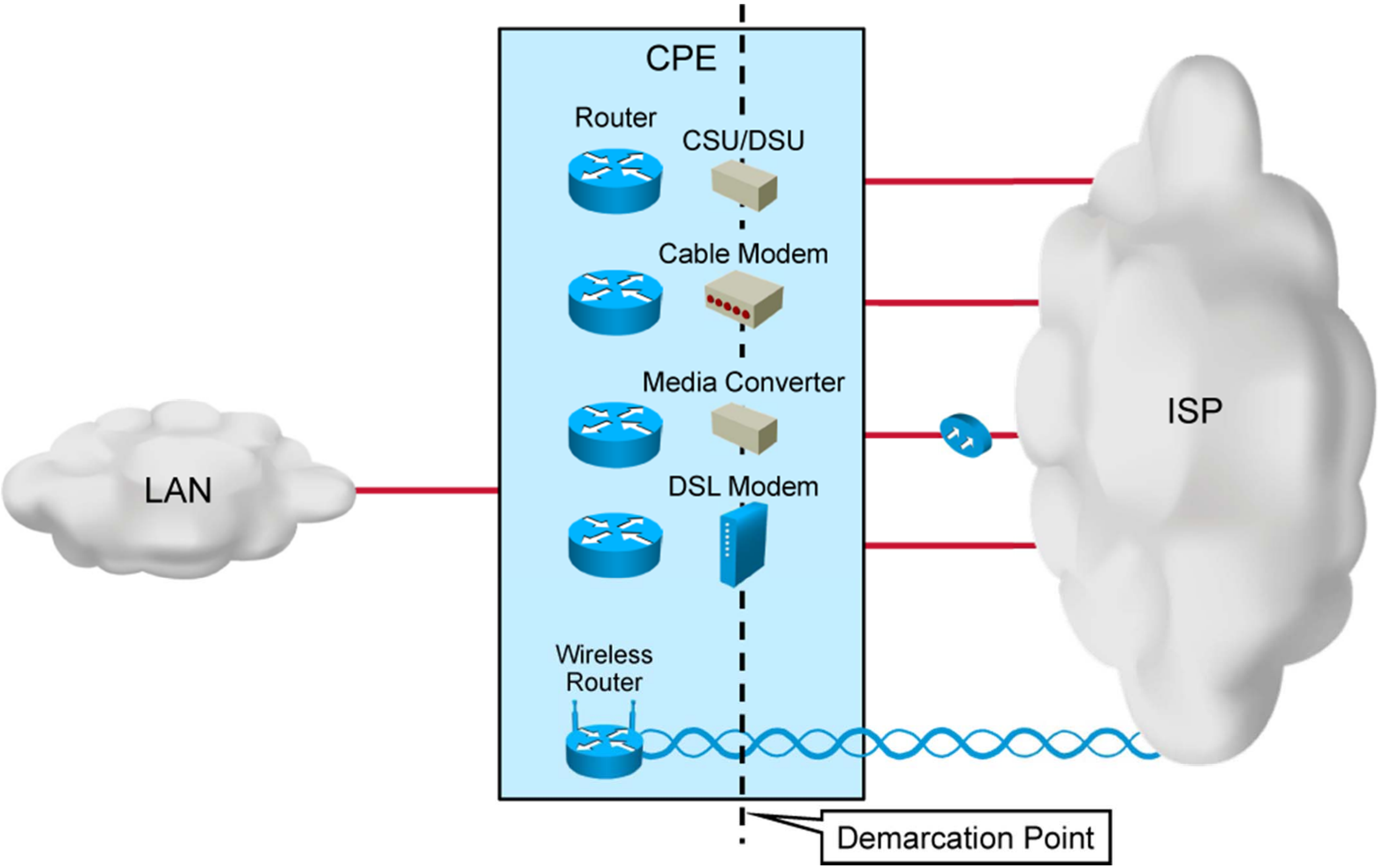
Summary

- An ACL is a tool to identify traffic for special handling.
- ACLs perform top-down processing and can be configured for incoming or outgoing traffic.
- In a wildcard bit mask, a 0 bit means to match the corresponding address bit and a 1 bit means to ignore the corresponding address bit.
- You can create an ACL using a named or numbered ACL. Named or numbered ACLs can be configured as standard or extended ACLs, which determines what they can filter.

Enabling Internet Connectivity

Establishing Internet Connectivity

The Demarcation Point



Dynamic Host Configuration Protocol

Understanding DHCP:

- DHCP is a client-server model.
- A DHCP server allocates network addresses and delivers configurations.
- A DHCP client is a host that requests an IP address and configuration from a DHCP server.

Dynamic Host Configuration Protocol (Cont.)

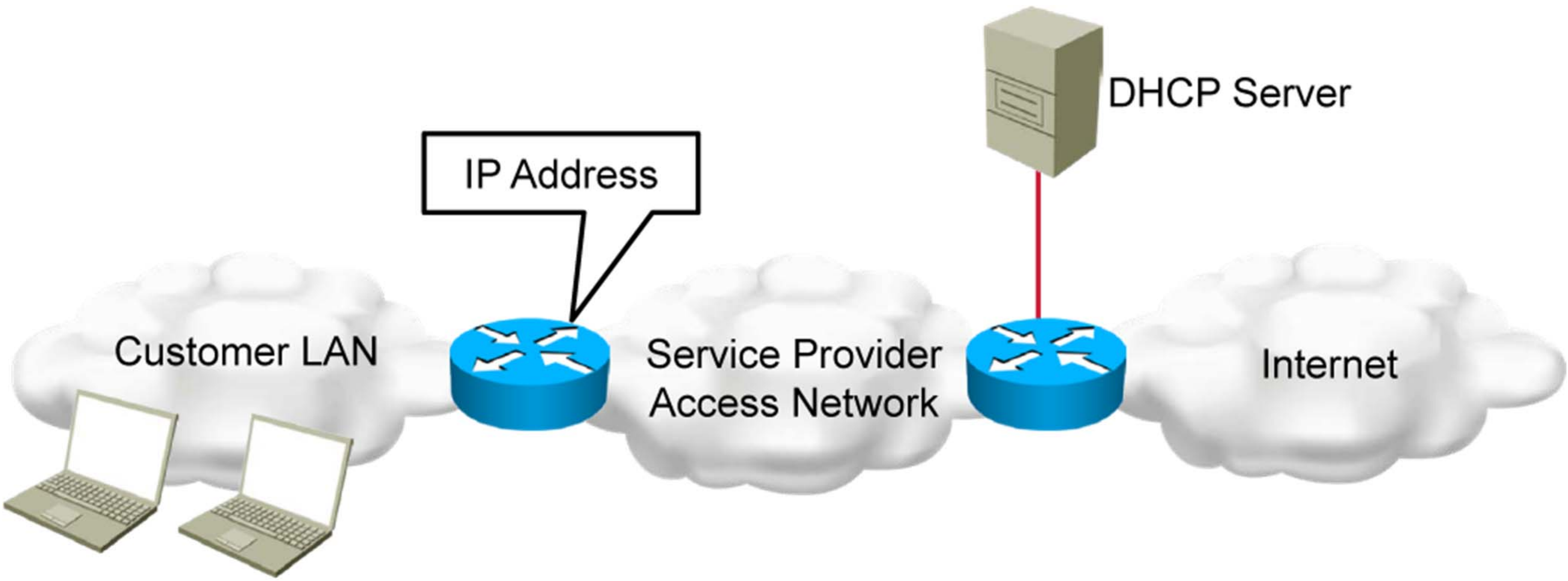
DHCP IP address allocation mechanisms:

- **Automatic allocation:** A permanent IP address is assigned to a client.
- **Dynamic allocation:** A client is assigned an IP address for a limited time.
- **Manual allocation:** A client is assigned an IP address by the network administrator.

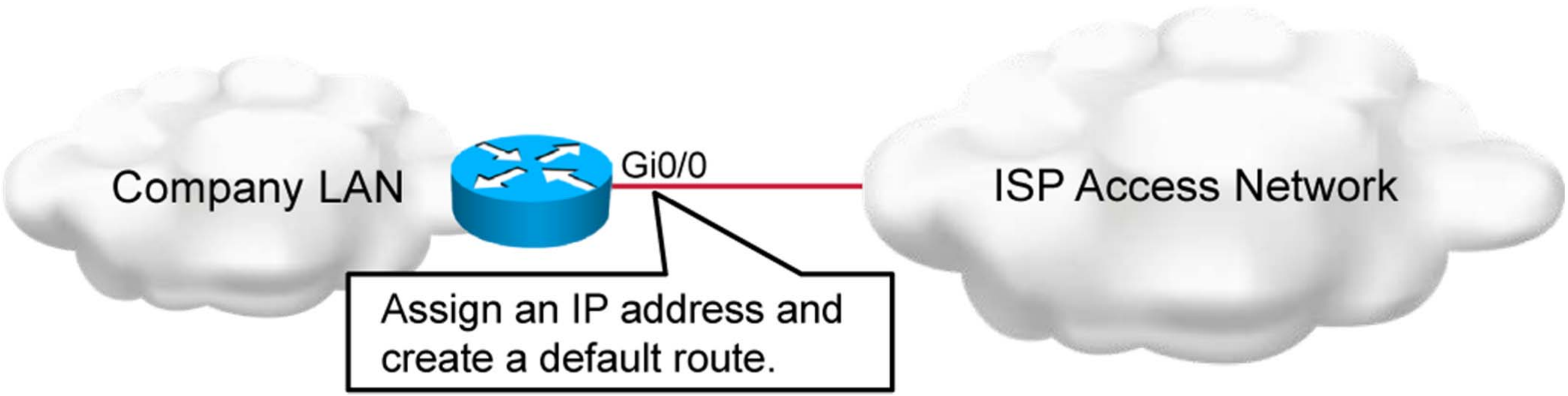
Options for Configuring a Provider-Assigned IP Address

Options for configuring IP addresses:

- Statically assigned
- Dynamically assigned through DHCP



Configuring a Static Provider-Assigned IP Address



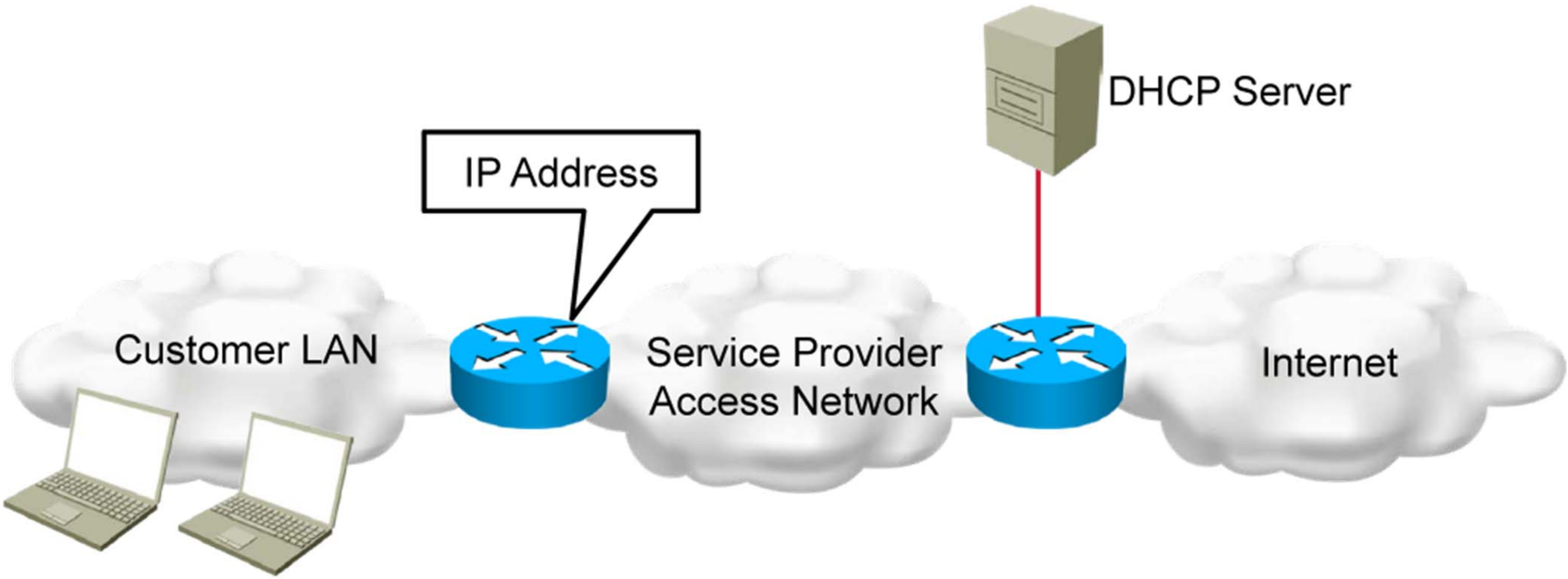

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shutdown
```

- Configures a public IP address

```
Router(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

- Creates a default route that points toward the next-hop IP address

Configuring a DHCP Client




```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address dhcp
```

- Router automatically injects default route based on optional default gateway parameter received with assigned IP address

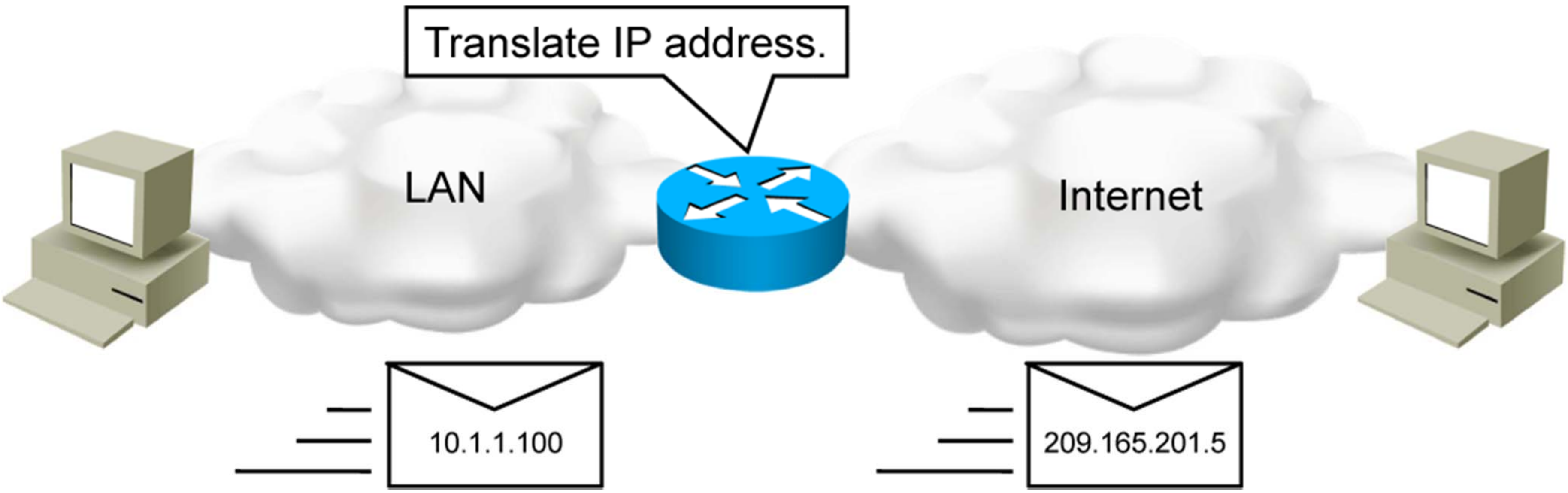
Public vs. Private IPv4 Addresses

Class	Private 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

Class	Public Address Range
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

Introducing NAT

NAT allows private users to access the Internet by sharing one or more public IP addresses.

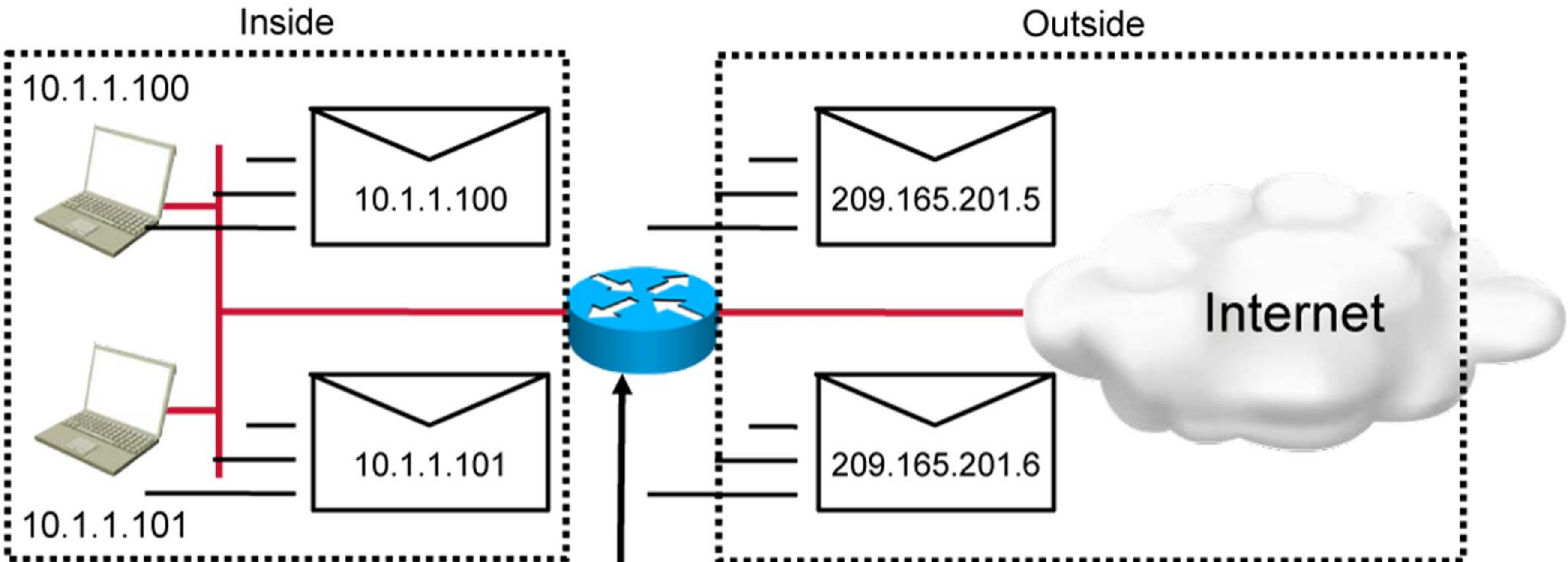


Types of Addresses in NAT

These are the most important types of addresses in NAT:

- **Inside local:** Host on the inside network
- **Inside global:** Usually assigned by an ISP and allows the customer outside access
- **Outside global:** Host on the outside network

Types of Addresses in NAT (Cont.)



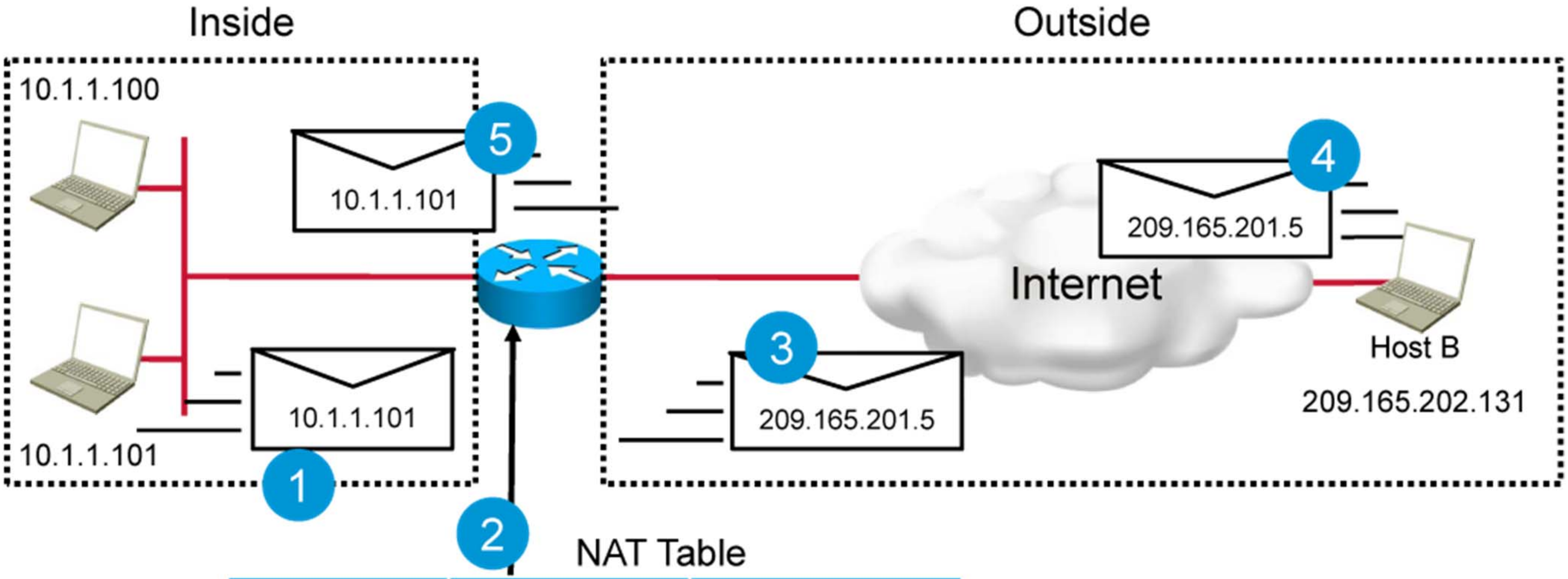
Inside Local IPv4 Address	Outside Global IPv4 Address
10.1.1.100	209.165.201.5
10.1.1.101	209.165.201.6

Types of NAT

These are the types of NAT:

- **Static NAT:** One-to-one address mapping
- **Dynamic NAT:** Many-to-many address mapping
- **PAT:** Many-to-one address mapping

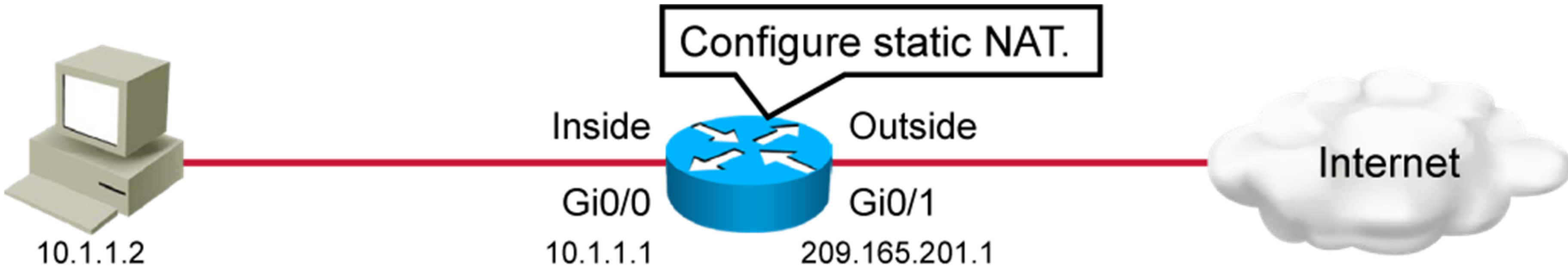
Understanding Static NAT



Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.1.1.101	209.165.201.5	209.165.202.131

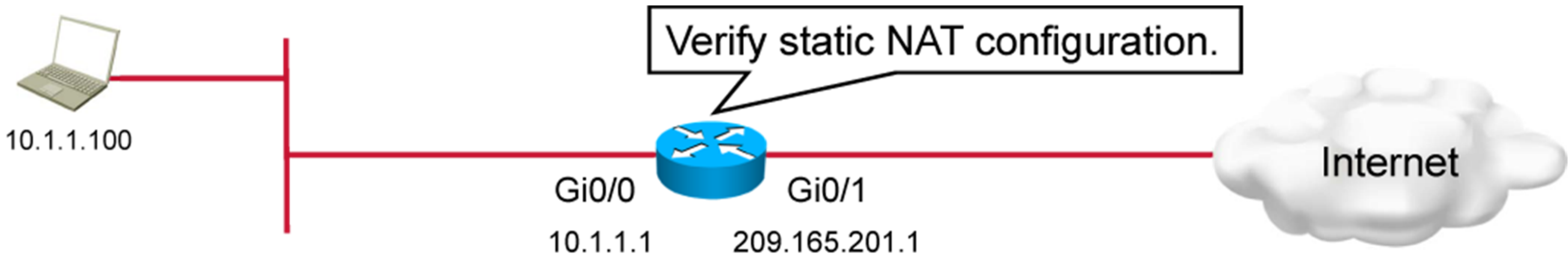
Configuring Static NAT

Example: Configuring static NAT



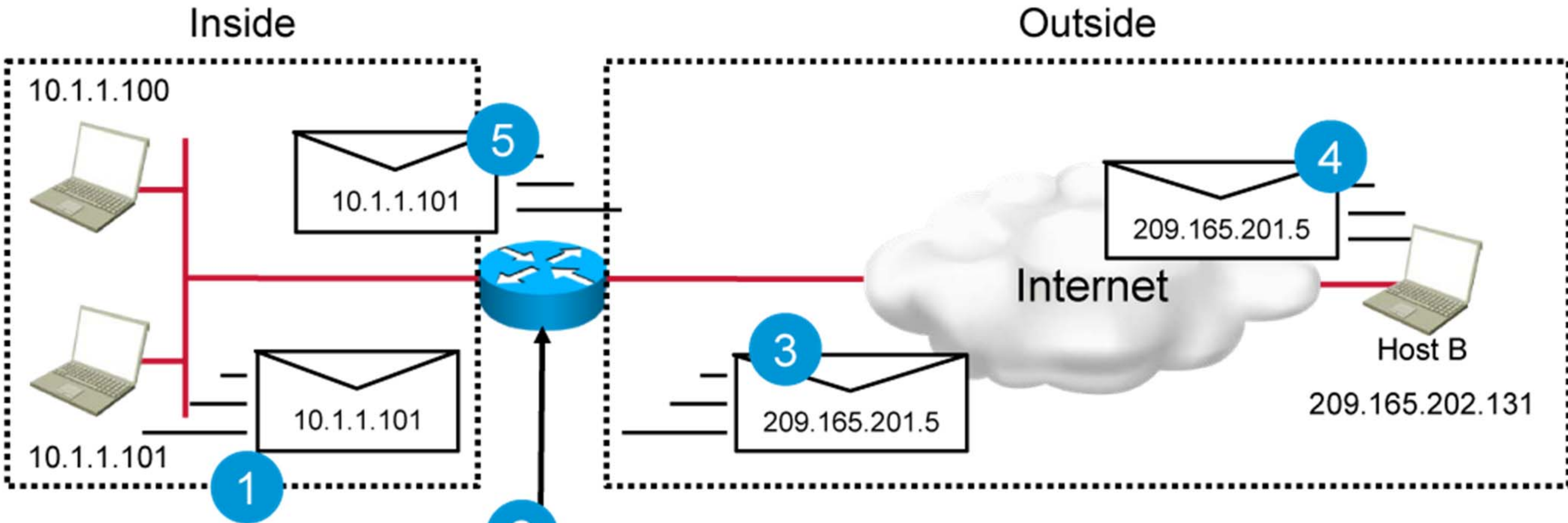

```
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip address 209.165.201.1 255.255.255.240
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#ip nat inside source static 10.1.1.2 209.165.201.5
```

Verifying Static NAT Configuration




```
Router#show ip nat translations
Pro Inside global        Inside local       Outside local         Outside global
tcp 209.165.201.5:1031 10.1.1.100:1031  209.165.202.155:23
209.165.202.155:23
--- 209.165.201.5      10.1.1.100         ---                   ---
```

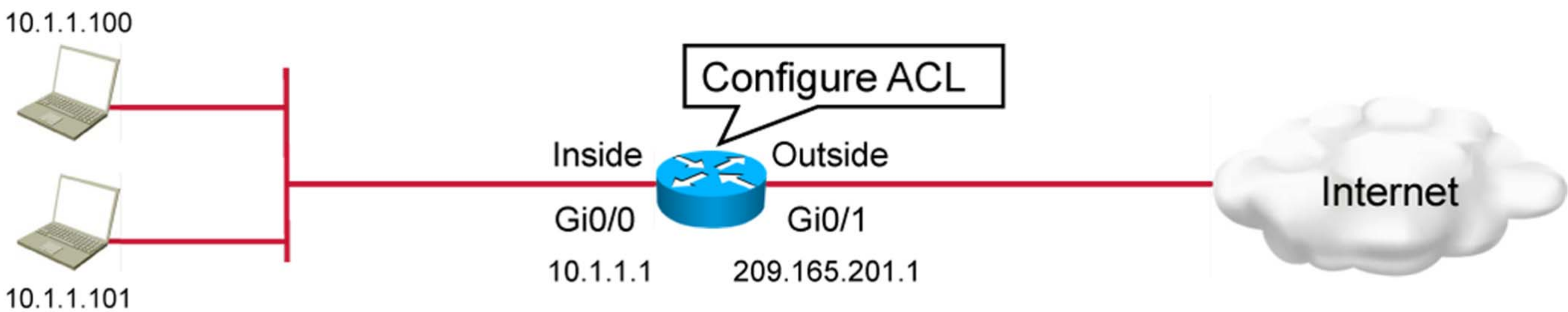
Understanding Dynamic NAT



NAT Table

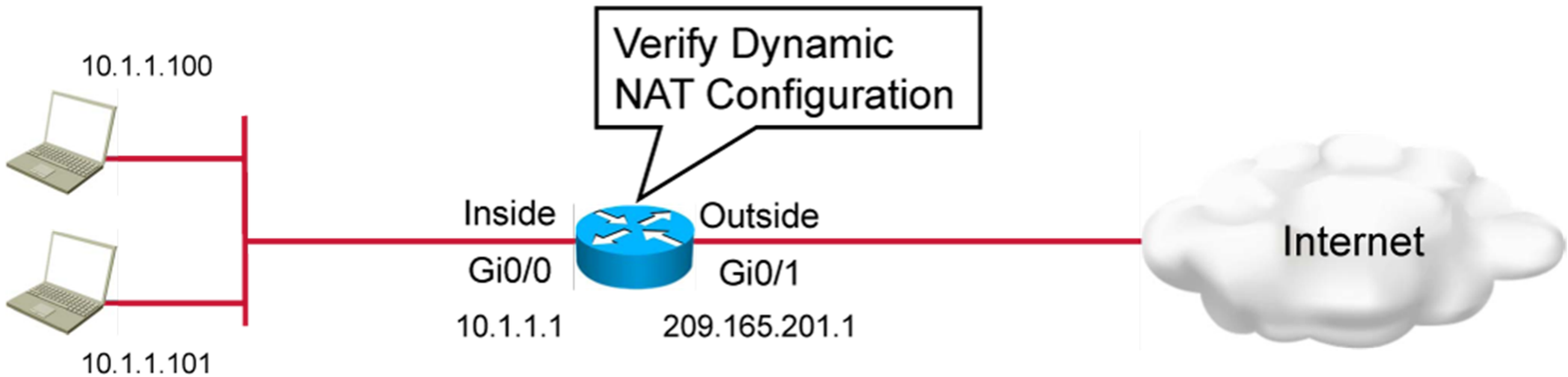
Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.1.1.101	209.165.201.5	209.165.202.131
10.1.1.100	209.165.201.6	209.165.202.131

Configuring Dynamic NAT



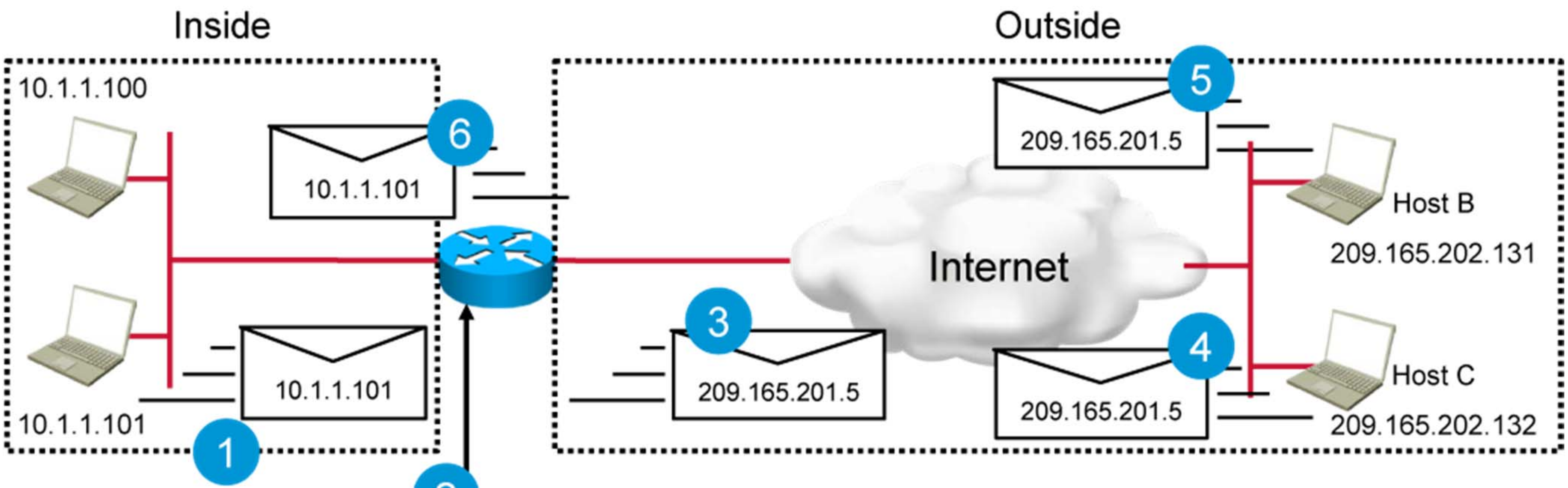

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#ip nat pool NAT-POOL 209.165.201.5 209.165.201.10 netmask
255.255.255.240

Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip address 209.165.201.1 255.255.255.240
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#ip nat inside source list 1 pool NAT-POOL
```

Verifying Dynamic NAT Configuration




```
Router#show ip nat translations
Pro Inside global       Inside local     Outside local       Outside global
icmp 209.165.201.5:3    10.1.1.100:3     209.165.202.155:3   209.165.202.155:3
--- 209.165.201.5       10.1.1.100       ---                 ---
icmp 209.165.201.6:1    10.1.1.101:1     209.165.201.125:1   209.165.201.125:1
tcp 209.165.201.6:1030 10.1.1.101:1030 209.165.201.125:23
209.165.201.125:23
--- 209.165.201.6       10.1.1.101       ---                ---
```

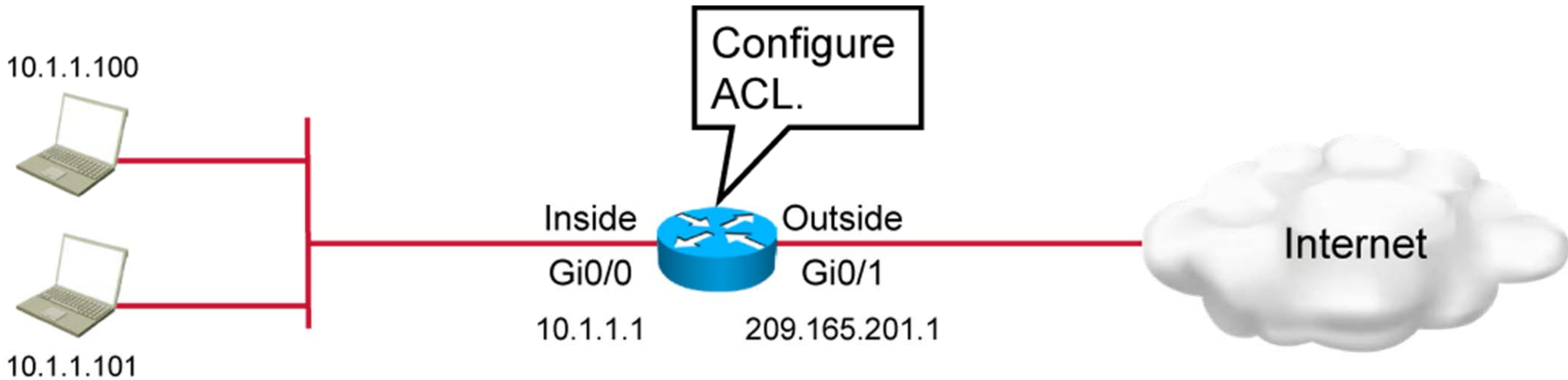
Understanding PAT



NAT Table

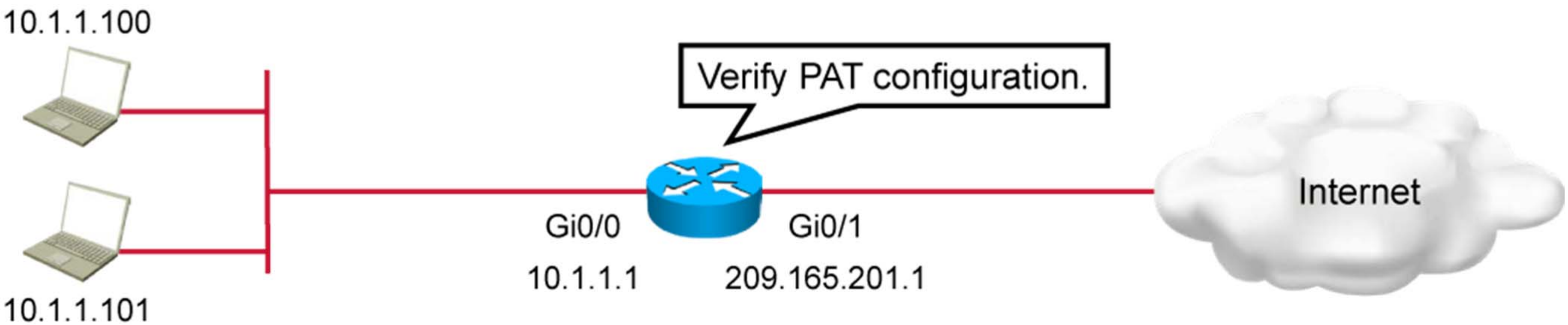
Protocol	Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
TCP	10.1.1.100:1723	209.165.201.5:1723	209.165.202.131:23
TCP	10.1.1.101:1927	209.165.201.5:1927	209.165.202.132:23
TCP	10.1.1.101:1723	209.165.201.5:1724	209.165.202.131:23

Configuring PAT



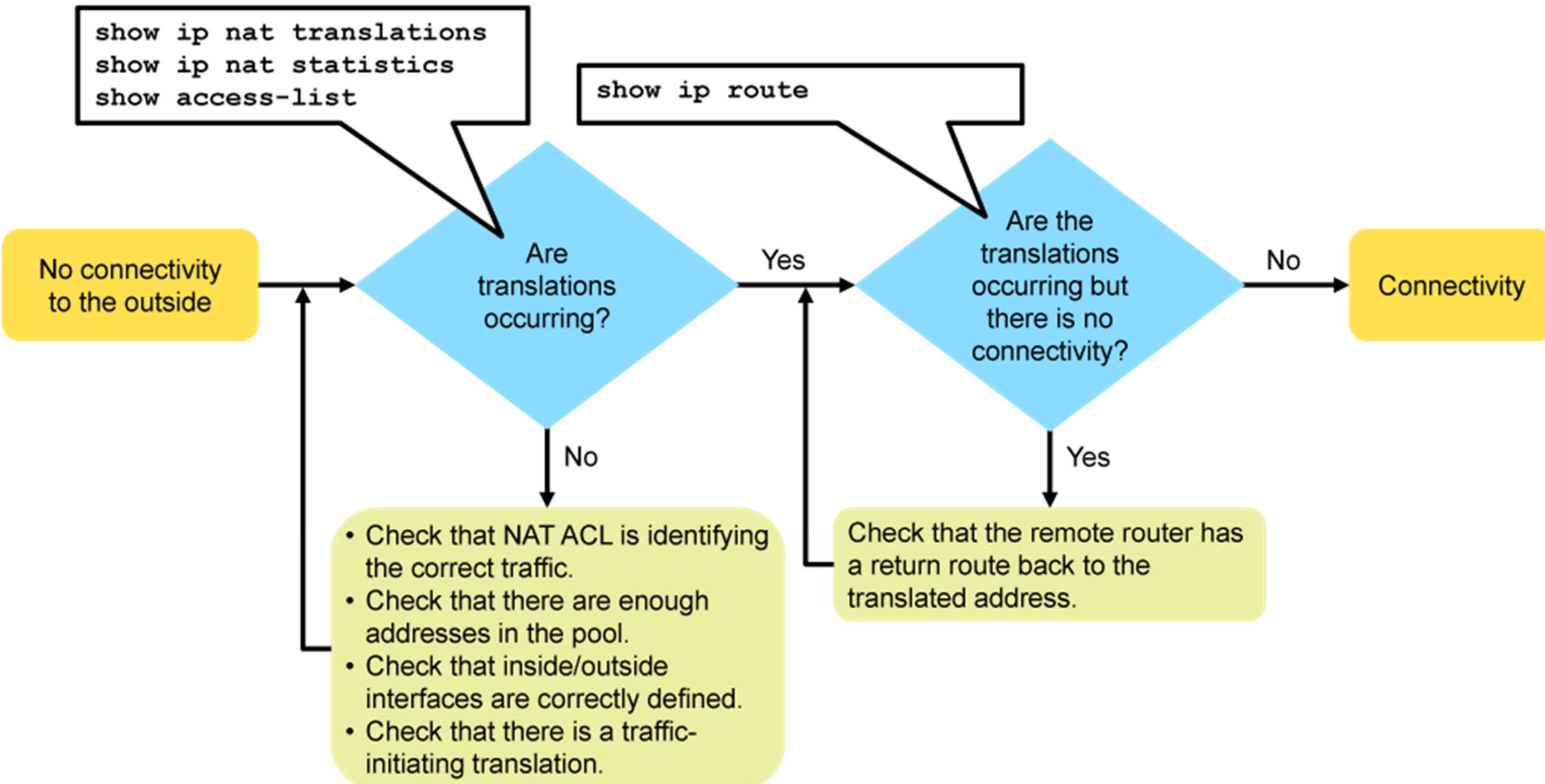

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside

Router(config-if)#interface GigabitEthernet 0/1
Router(config-if)#ip address 209.165.201.1 255.255.255.240
Router(config#ip nat outside

Router(config)#ip nat inside source list 1 interface Gi 0/1 overload
```

Verifying PAT Configuration




```
Router#show ip nat translations
Pro Inside global         Inside local       Outside local         Outside global
tcp 209.165.201.5:27497 10.1.1.100:27497 209.165.202.155:80
209.165.202.155:80
tcp 209.165.201.5:2597  10.1.1.100:2597  209.165.201.125:443
209.165.201.125:443
```

Troubleshooting NAT



Troubleshooting NAT (Cont.)

Are Addresses Being Translated?

```
Router#show ip nat statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: Serial0
Inside Interfaces: Ethernet0 , Ethernet1
Hits: 42 Misses: 44
<output omitted>
```

- Monitors NAT statistics

```
Router#show access-list
access-list 1 permit 10.1.1.100 0.0.0.255
```

- Verifies that the NAT ACL is permitting all necessary networks

Troubleshooting NAT (Cont.)

- To display detailed dynamic data and events, you can use **debug** commands.
  - A **debug** command can intensively use device resources. Use carefully on production equipment.
  - Always turn off **debug** after troubleshooting with the **no debug all** command.

```
Router#debug ip nat
NAT*: s=10.1.1.100->209.165.201.1, d=172.16.1.100 [103]
NAT*: s=172.16.1.100, d=209.165.201.1->10.1.1.100 [103]
NAT*: s=10.1.1.100->209.165.201.1, d=172.16.1.100 [104]
NAT*: s=172.16.1.100, d=209.165.201.1->10.1.1.100 [104]
<output omitted>
```

- Displays information about every packet that is translated by the router

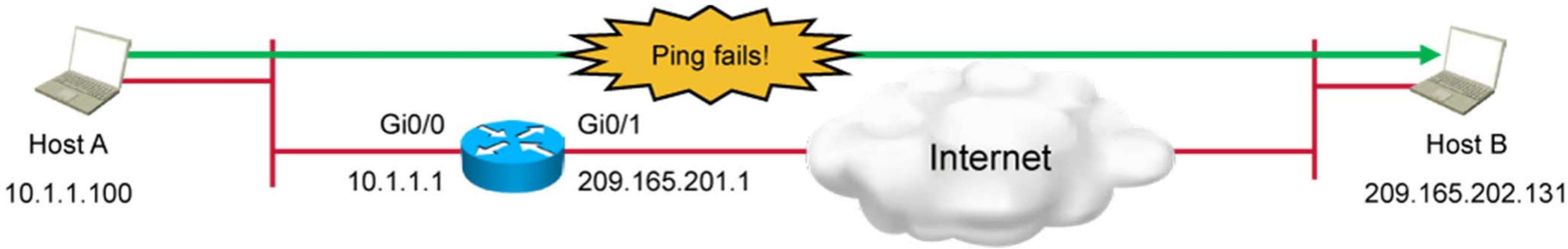
Troubleshooting NAT (Cont.)

If translations are occurring, but there is no connectivity, verify that the remote router has a route to the translated address.


```
Branch#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
   E1 - OSPF external type 1, E2 - OSPF external type 2
   i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
   ia - IS-IS inter area, * - candidate default, U - per-user static route
   o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 209.165.201.1 to network 0.0.0.0
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.2/32 is directly connected, GigabitEthernet0/0
C 209.165.201.0/27 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.201.1
```

Troubleshooting NAT Case Study

Host A and host B are unable to ping after a new NAT configuration is put in place.

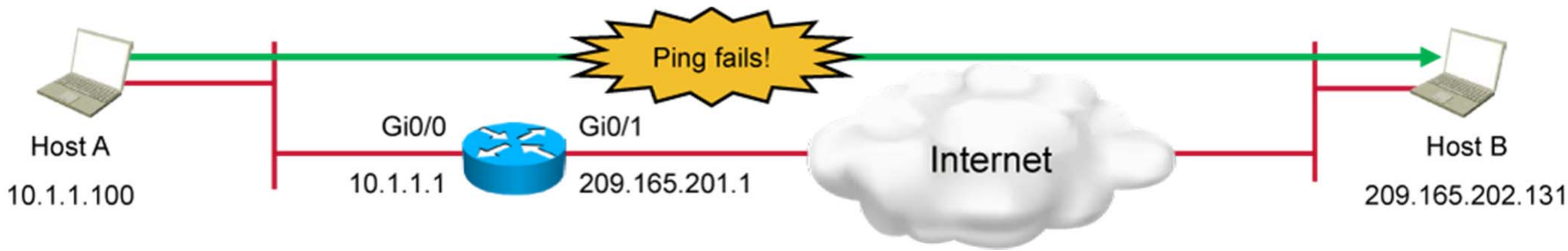


Troubleshooting NAT Case Study (Cont.)

```
Router#show running-config
<output omitted>
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
access-list 20 permit 0.0.0.0 255.255.255.0
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
!
interface GigabitEthernet0/1
 ip address 209.165.200.1 255.255.255.254
 ip nat inside
!
ip nat inside source list 20 interface GigabitEthernet0/1 overload
```

Troubleshooting NAT Case Study (Cont.)

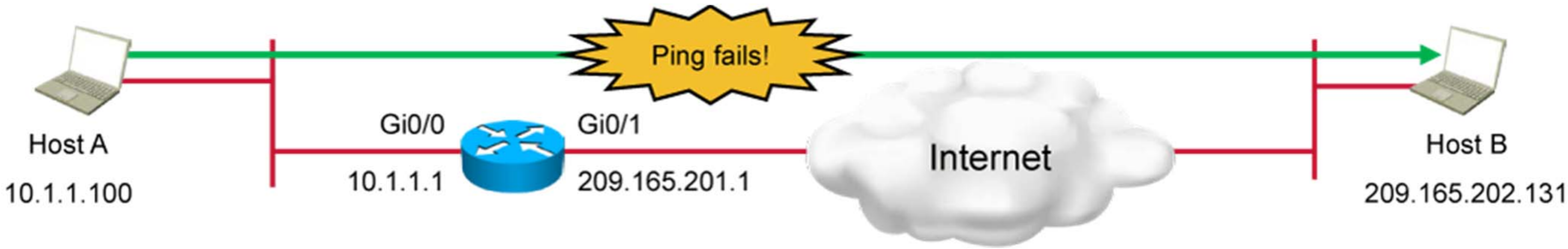
Translations are not occurring.




```
Router#show ip nat translations
   Pro Inside global    Inside local    Outside local    Outside global
```

Troubleshooting NAT Case Study (Cont.)

The router interfaces are incorrectly defined as NAT inside and NAT outside.




```
Router#show ip nat statistics
      Total active translations: 0 (0 static, 0 dynamic; 0 extended)
      Outside interfaces:
      GigabitEthernet0/0
      Inside interfaces:
      GigabitEthernet0/1
<output omitted>
```

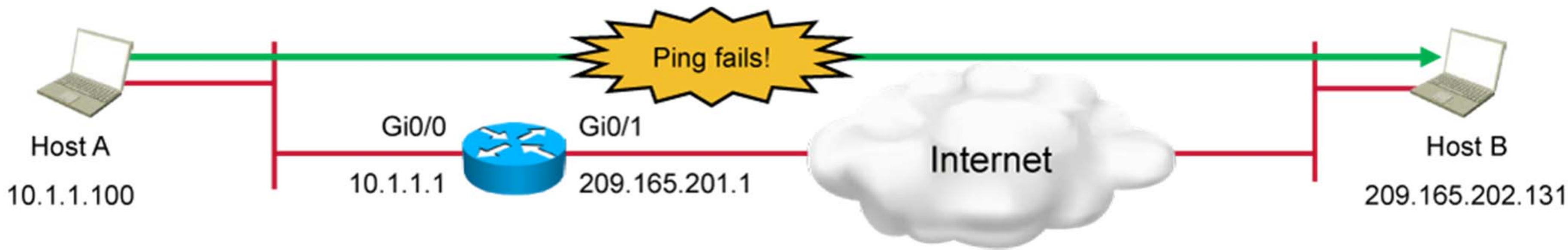
Troubleshooting NAT Case Study (Cont.)

How to fix configuration:

```
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface GigabitEthernet 0/1
Router(config-if)#ip nat outside
```

Troubleshooting NAT Case Study (Cont.)

Verify that the access list is correct.



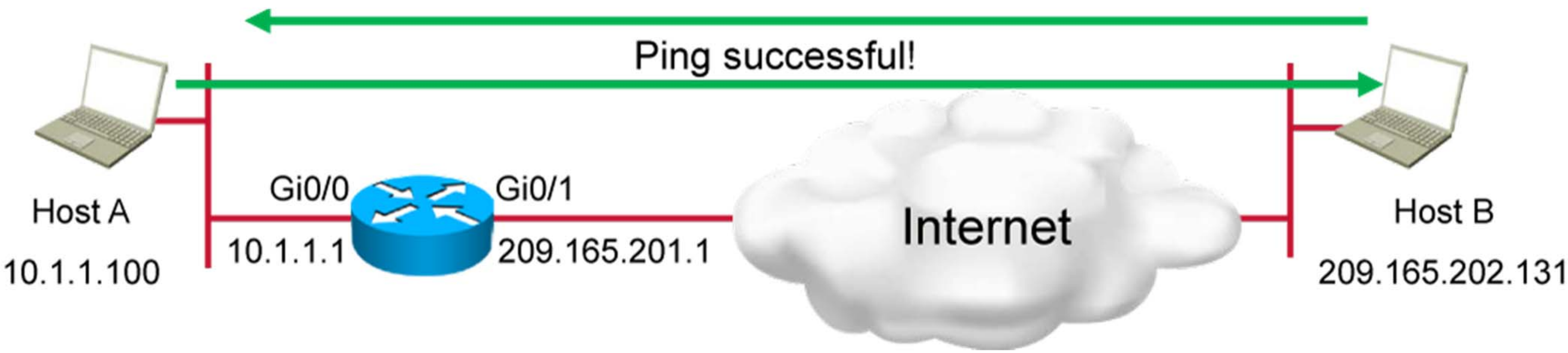

```
RouterA#show access-list

Standard IP access list 20
   10 permit 0.0.0.0, wildcard bits 255.255.255.0
```

How to fix access list:

```
Router#config terminal
Router(config)#no access-list 20
Router(config)#access-list 20 permit 10.1.1.0 0.0.0.255
```

Troubleshooting NAT Case Study (Cont.)

Verify that translations are occurring and you have connectivity to the remote network.




```
C:\>ping 209.165.202.131
Pinging 209.165.202.131 with 32 bytes of data:
Reply from 209.165.202.131: bytes=32 time=107ms TTL=127
Reply from 209.165.202.131: bytes=32 time=70ms TTL=127
<output omitted>
```

```
Router#show ip nat translations
Pro Inside global      Inside local        Outside local         Outside global
icmp 209.165.201.1:1  10.1.1.100:1   209.165.202.131:1  209.165.202.131:1
```

Summary

- Provider-assigned IP addresses can be configured on a router statically or can be dynamically assigned through DHCP.
- A DHCP client is a host that requests an IP address and configuration from a DHCP server.
- A DHCP server allocates network addresses and delivers configurations.

Summary (Cont.)

- NAT enables private IP internetworks that use private IP addresses to connect to the Internet. PAT, or NAT overload, a feature of NAT, enables several internal addresses to be translated to only one or a few external addresses.
- Static NAT is one-to-one address mapping. Dynamic NAT addresses are picked from a pool.
- PAT allows you to map many inside addresses to one outside address.
- Use the **show ip nat translations** command to display the translation table and verify that translation has occurred.
- To determine whether a current translation entry is being used, use the **show ip nat statistics** command to check the hits counter.

Module Summary

- IP is a Layer 3 media-independent connectionless protocol that uses hierarchical logical addressing and provides best-effort service.
- Internet hosts require a unique public IP address. Hosts in private networks can have any valid private IP address that is unique locally in each network.
- Networks, particularly large networks, are often divided into smaller subnetworks, or subnets. Subnets can improve network performance and control.
- TCP is a connection-oriented protocol that provides reliable transport. UDP is a connectionless transport protocol that provides best-effort transport.

Module Summary (Cont.)

- The main function of a router is to relay packets from one network device to another. To do this, you must define the characteristics of the interfaces through which packets are received and sent. Interface characteristics, such as the IP address, are configured in interface configuration mode.
- Cisco Discovery Protocol is an information-gathering tool that is used by network administrators to obtain information about directly connected devices.
- Static routers use a route that a network administrator manually enters into the router. Dynamic routers use a route that a network routing protocol adjusts automatically for topology or traffic changes.

Module Summary (Cont.)

- ACLs can be used as a Cisco IOS tool to identify traffic that receives special handling.
- NAT enables private IP internetworks that use private IP addresses to connect to the Internet. PAT, a feature of NAT, enables several internal addresses to be translated to one external address or a few external addresses.