Chapter 6: Network Layer

Introduction to Networks

Cisco Networking Academy®
Mind Wide Open™

Chapter 6: Objectives

In this chapter, you will be able to:

- Explain how network layer protocols and services support communications across data networks.
- Explain how routers enable end-to-end connectivity in a small-to-medium-sized business network.

Chapter 6

6.1 Network Layer Protocols

6.2 Routing

6.3 Routers

6.1 Network Layer Protocols

Cisco | Networking Academy®
Mind Wide Open™

Network Layer in Communication

The Network Layer

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network. To accomplish this end-to-end transport, the network layer uses four basic processes:

- Addressing end devices
- Encapsulation
- Routing
- De-encapsulating

Network Layer Protocols

Common network layer protocols include:

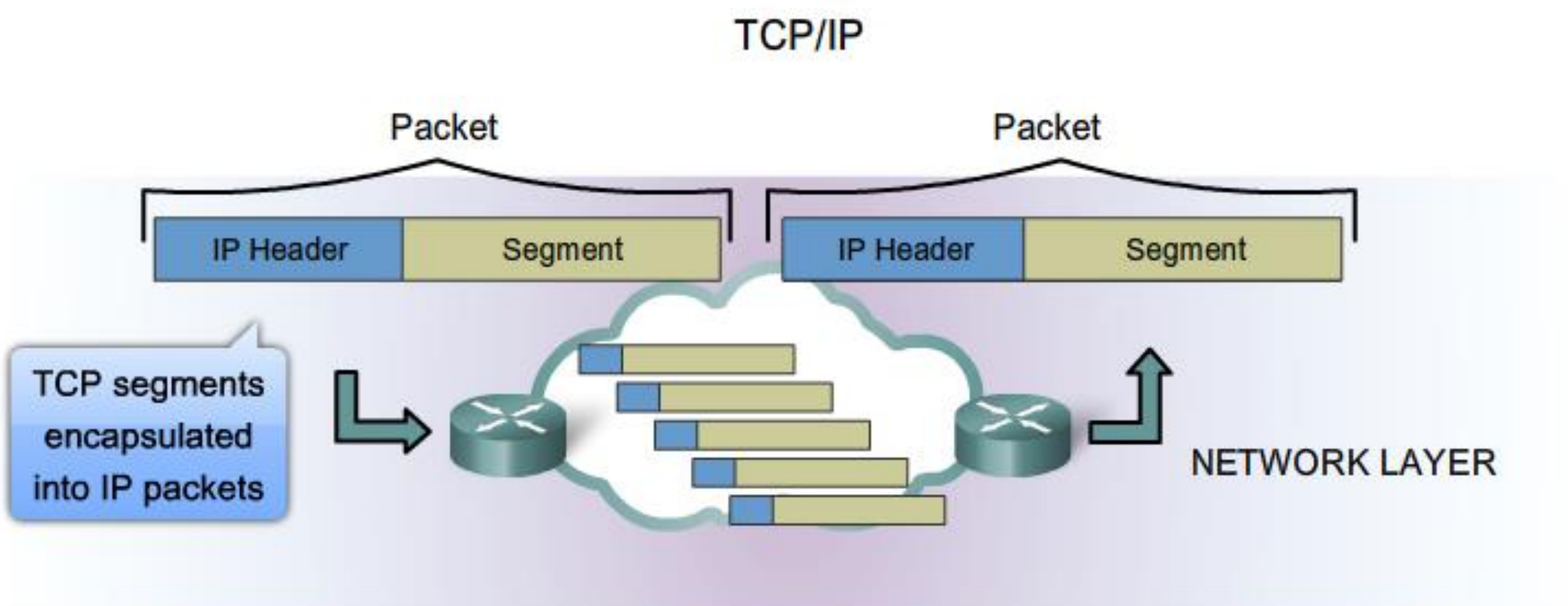
- IP version 4 (IPv4)
- IP version 6 (IPv6)

Legacy network layer protocols include:

- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

IP Characteristics

IP Components



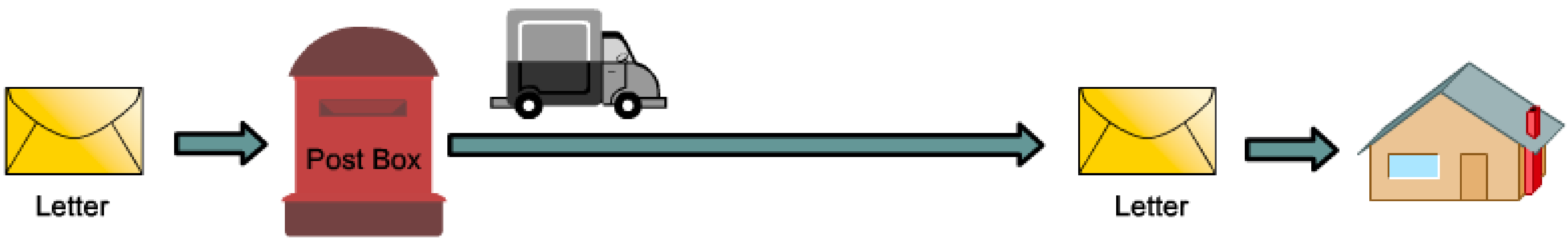
IP Packets flow through the internetwork.

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

Characteristics of the IP protocol

IP - Connectionless

Connectionless Communication



A letter is sent.

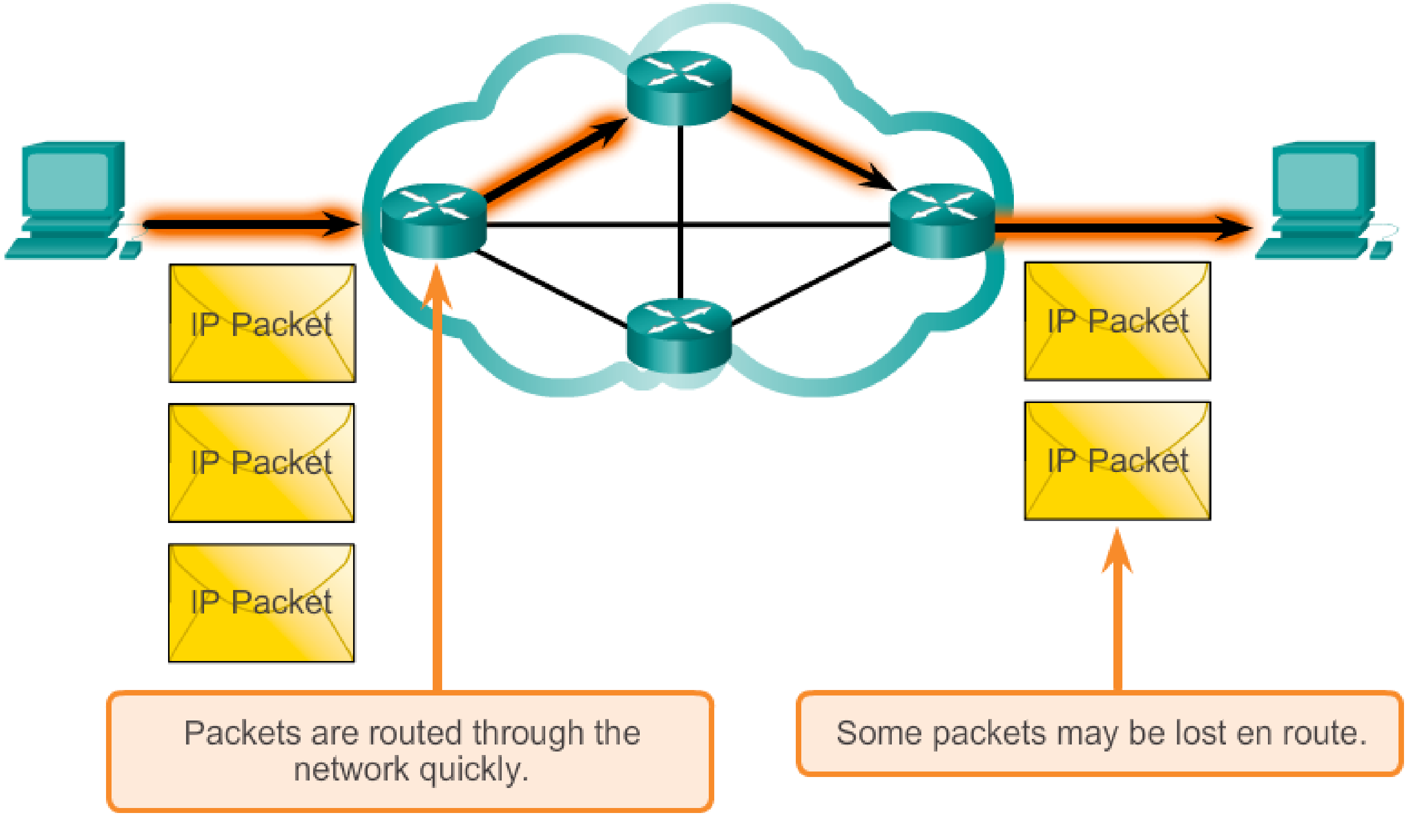
The sender doesn't know:

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

The receiver doesn't know:

- when it is coming

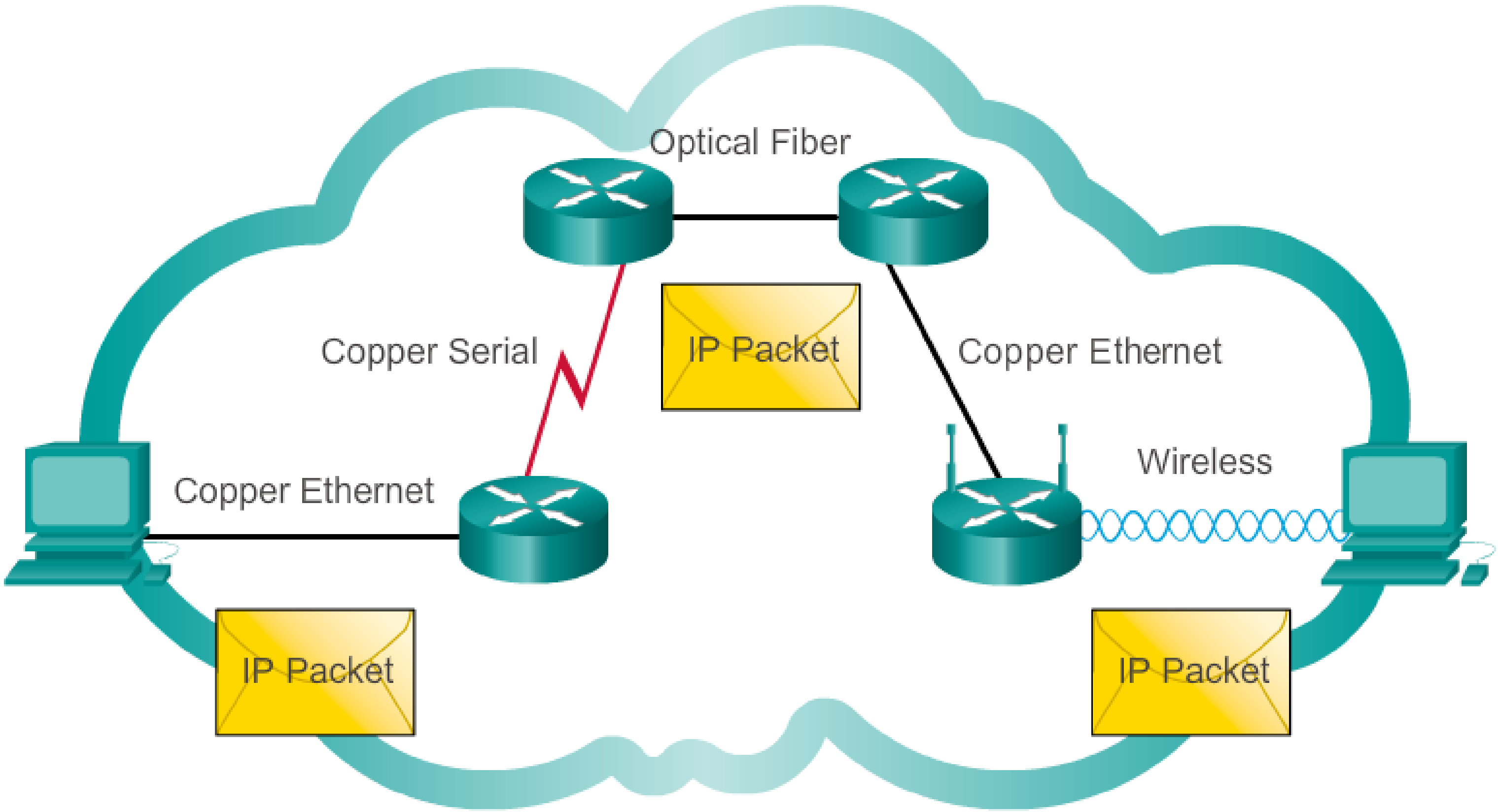
Characteristics of the IP protocol
Best Effort Delivery



As an unreliable network layer protocol, IP does not guarantee that all sent packets will be received. Other protocols manage the process of tracking packets and ensuring their delivery.

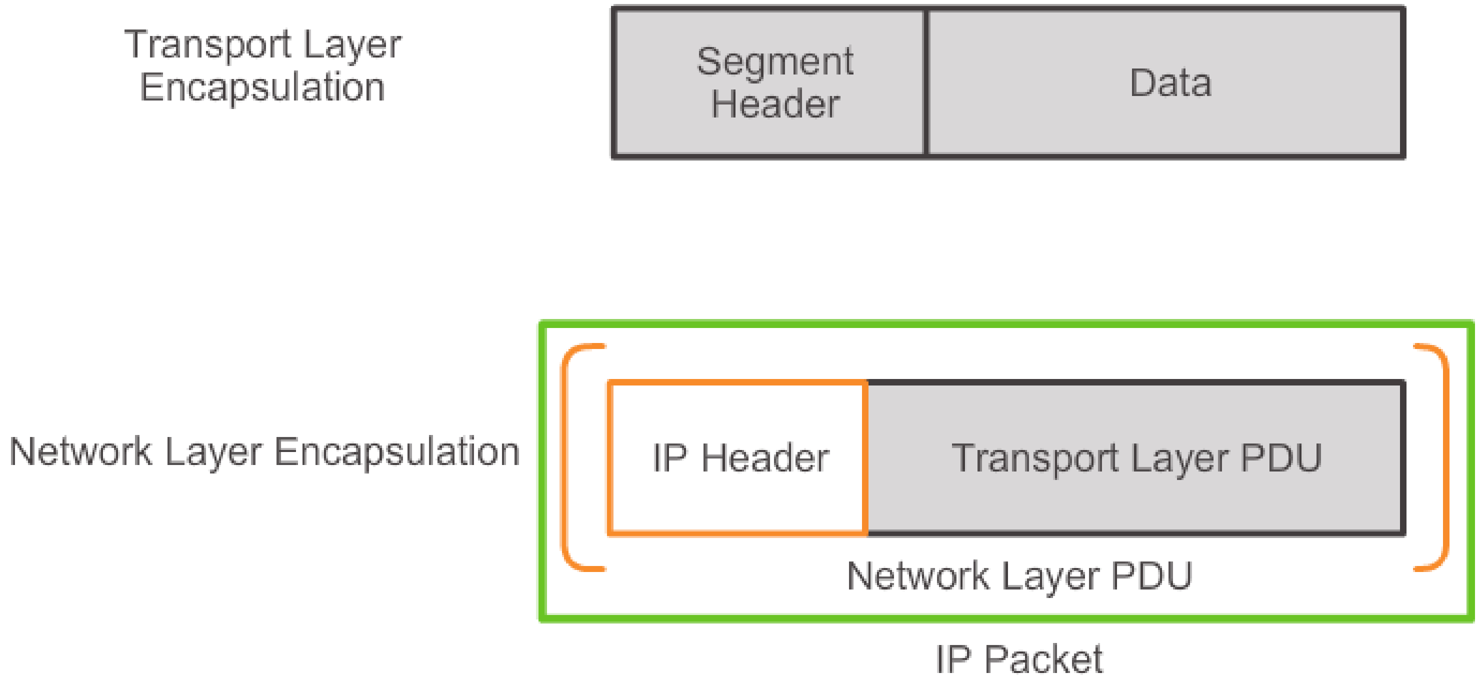
Characteristics of the IP protocol

IP – Media Independent



IP packets can travel over different media.

IPv4 Packet
Encapsulating IP

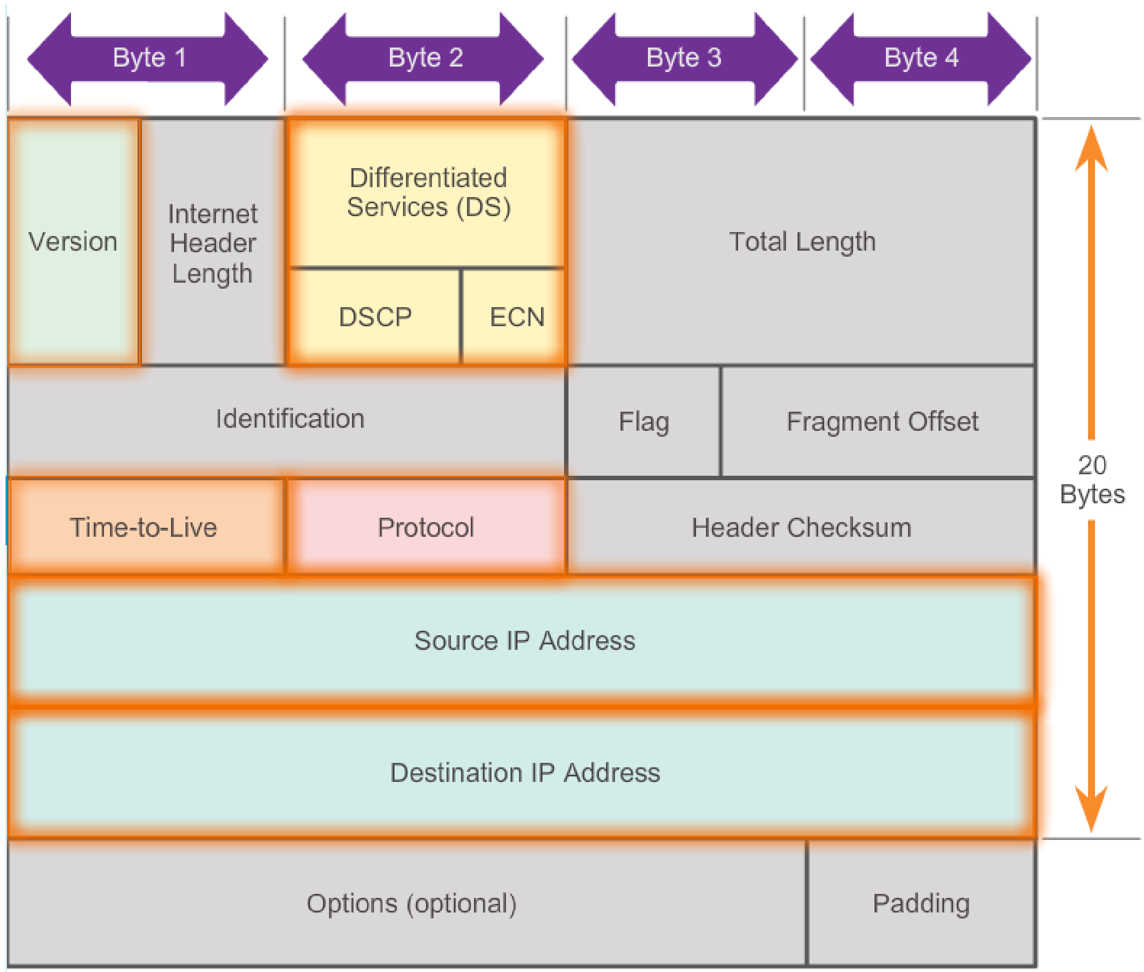


The network layer adds a header so packets can be routed through complex networks and reach their destination. In TCP/IP based networks, the network layer PDU is the IP packet.

IPv4 Packet

IPv4 Packet Header

Contents of the IPv4 packet header



IPv4 Packet

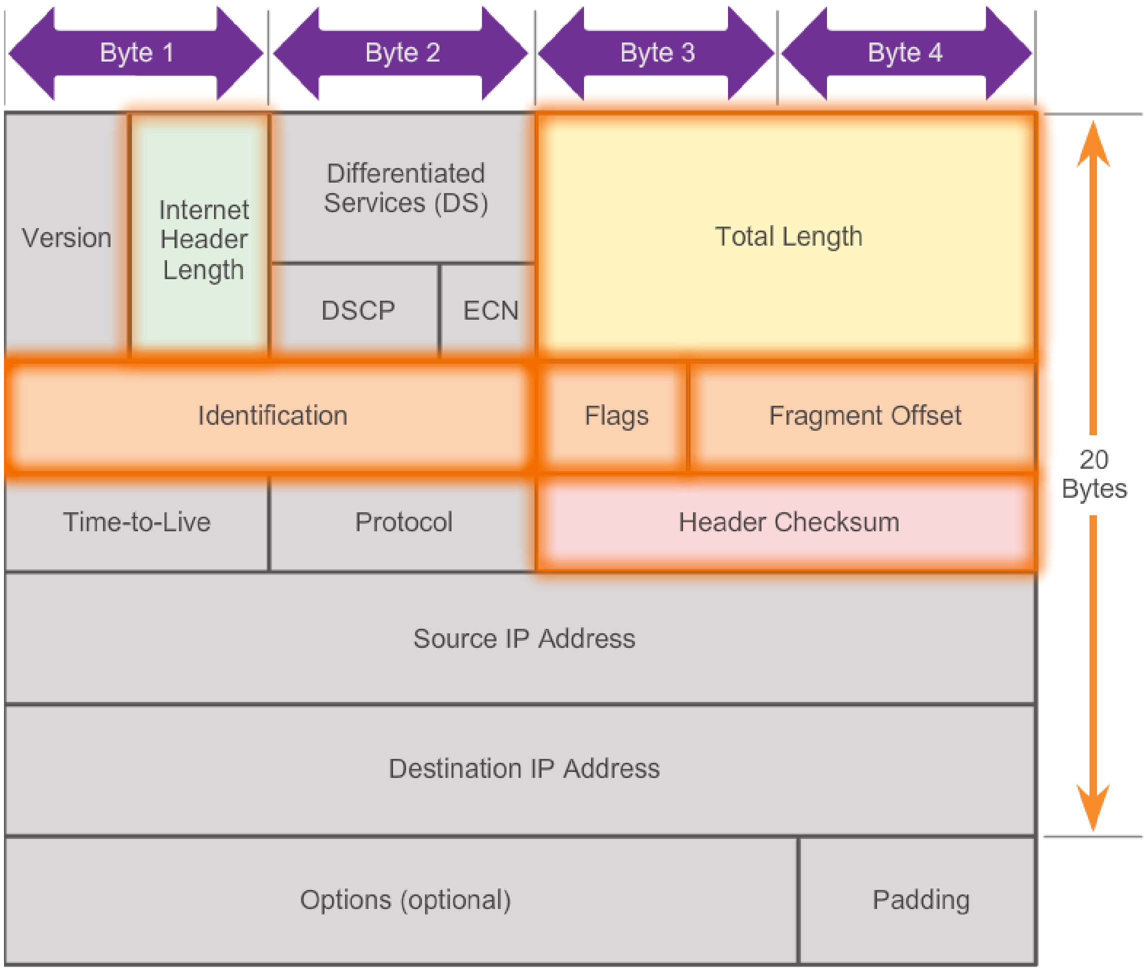
IPv4 Header Fields

IPv4 Header Fields

Version Always set to 0100 for IPv4	**Differentiated Services** Identifies the priority of each packet
Time-to-Live Commonly referred to as hop count	**Protocol** Identifies the upper-layer protocol to be used next
Source IP Address Identifies the IP address of the sending host	**Destination IP Address** Identifies the IP address of the recipient host

IPv4 Header Fields

Contents of the IPv4 header fields



IPv4 Header Fields

IPv4 Header Fields

Internet Header Length

Identifies the number of 32-bit words in the header

Total Length

Maximum value is 65,535 bytes

Header Checksum

Error-checks the IP header – if incorrect, the packet is discarded

IPv4 Header Fields

- Identification identifies each packet and its fragments, which keep the packet's original ID to enable defragmentation at the receiver computer.
- The More flag. If set, signifies that the packet has been fragmented and more fragments follow this current fragment. If not set, the flag signifies that either the packet was not fragmented or that this is the last of several fragments.
- The Do-Not-Fragment flag. If set, prevents fragmentation of the

packet; if the packet exceeds the outgoing link's Maximum Transmission Unit (MTU) it will be dropped.

- Fragment Offset signifies the position of the fragment within the original packet. If this is the first fragment, or the packet has not been fragmented then the offset will be zero.

Network Layer in Communication

Limitations of IPv4

- **IP Address depletion**
  - IPv4 has a limited number of unique public IP addresses available
- **Internet routing table expansion**
  - As the number of servers (nodes) connected to the Internet increases, so too does the number of network routes
- **Lack of end-to-end connectivity**
  - Network Address Translation (NAT) is a technology commonly implemented within IPv4 networks. NAT provides a way for multiple devices to share a single public IP address. However, because the public IP address is shared, the IP address of an internal network host is hidden.

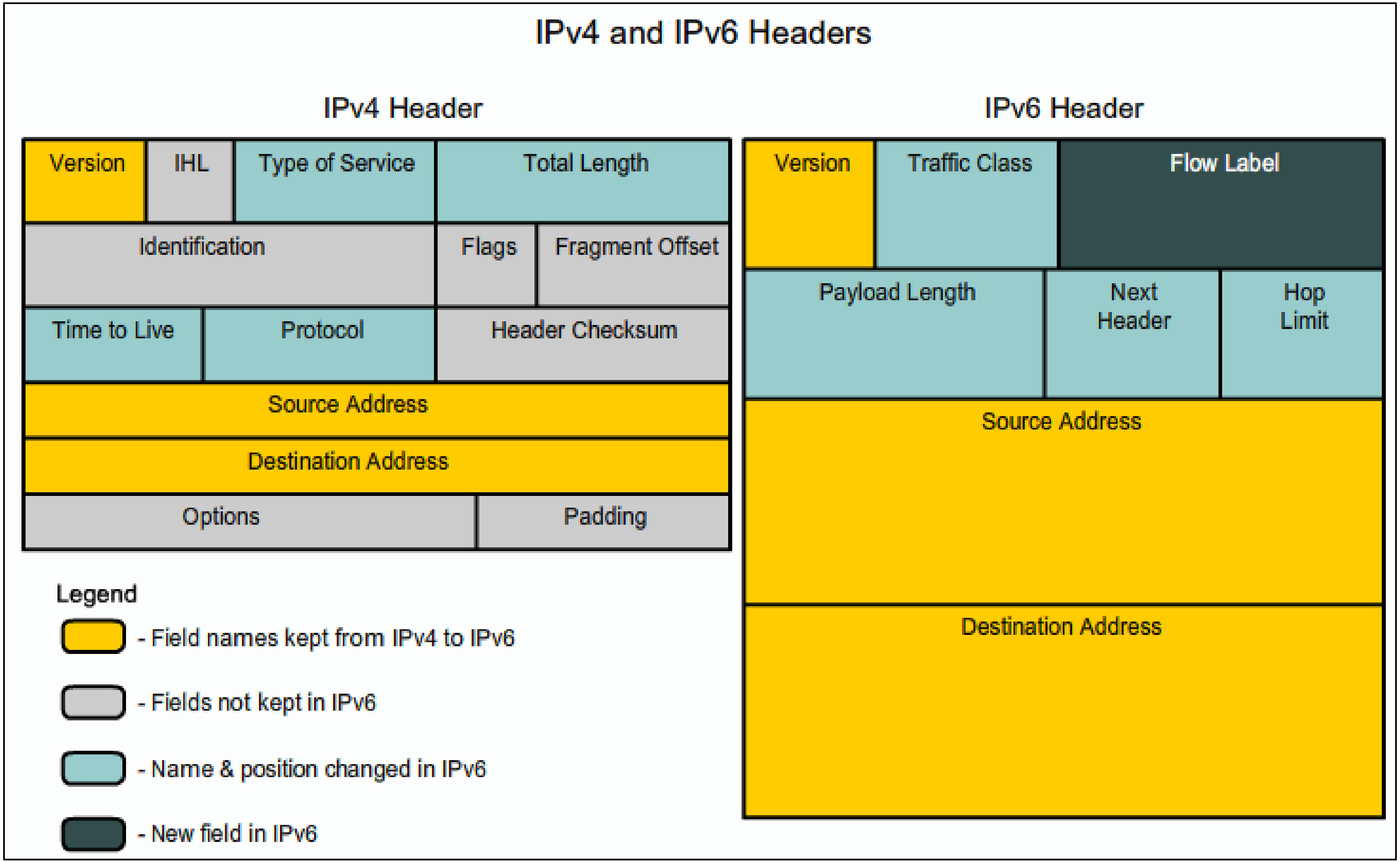
Network Layer in Communication

Introducing IPv6

- Increased address space
- Improved packet handling
- Eliminates the need for NAT
- Integrated security
- 4 billion IPv4 addresses
  4,000,000,000
- 340 undecillion IPv6 addresses
  340,000,000,000,000,000,000,000,000,000,000,000,000

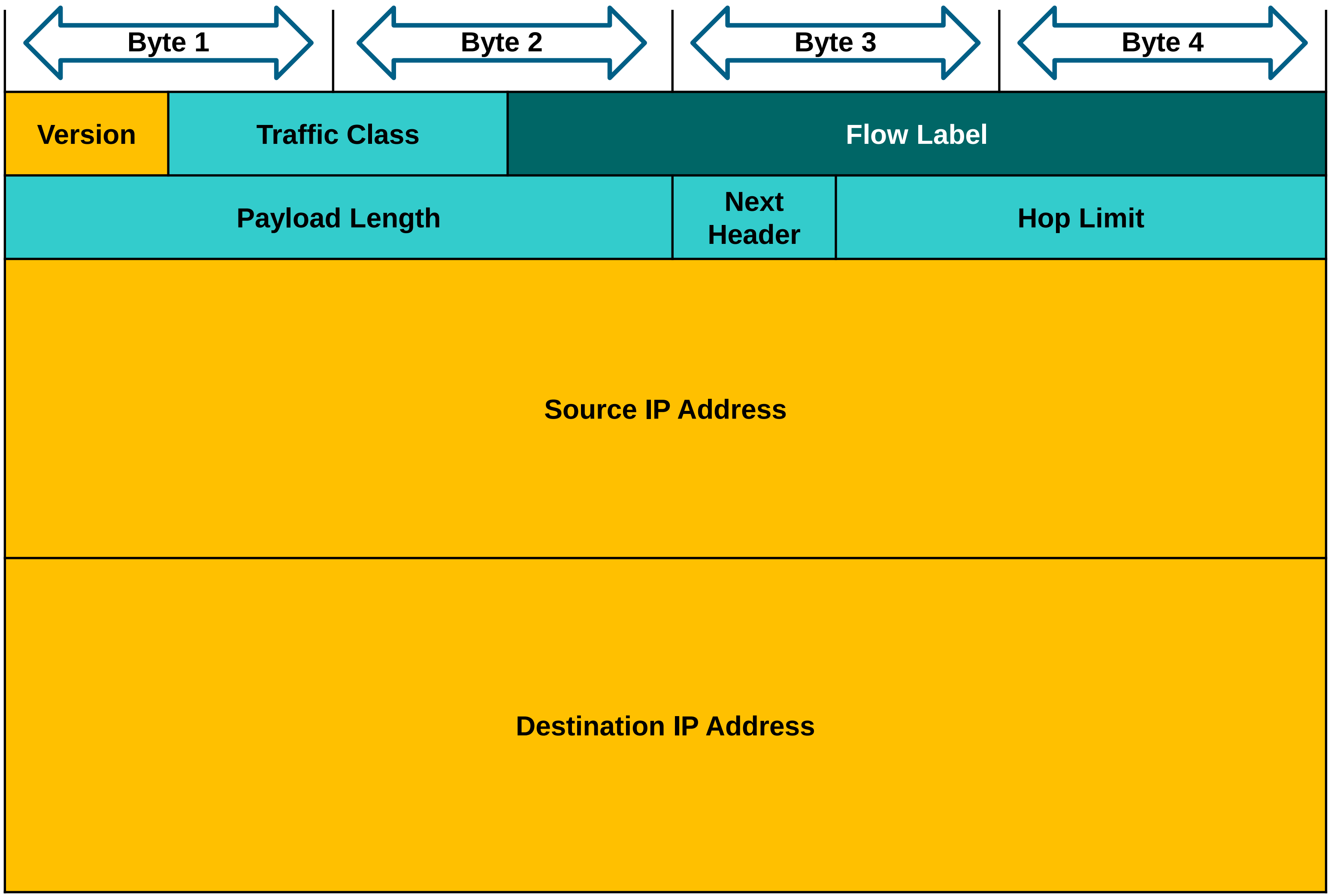
IPv6 Packet

Encapsulating IPv6



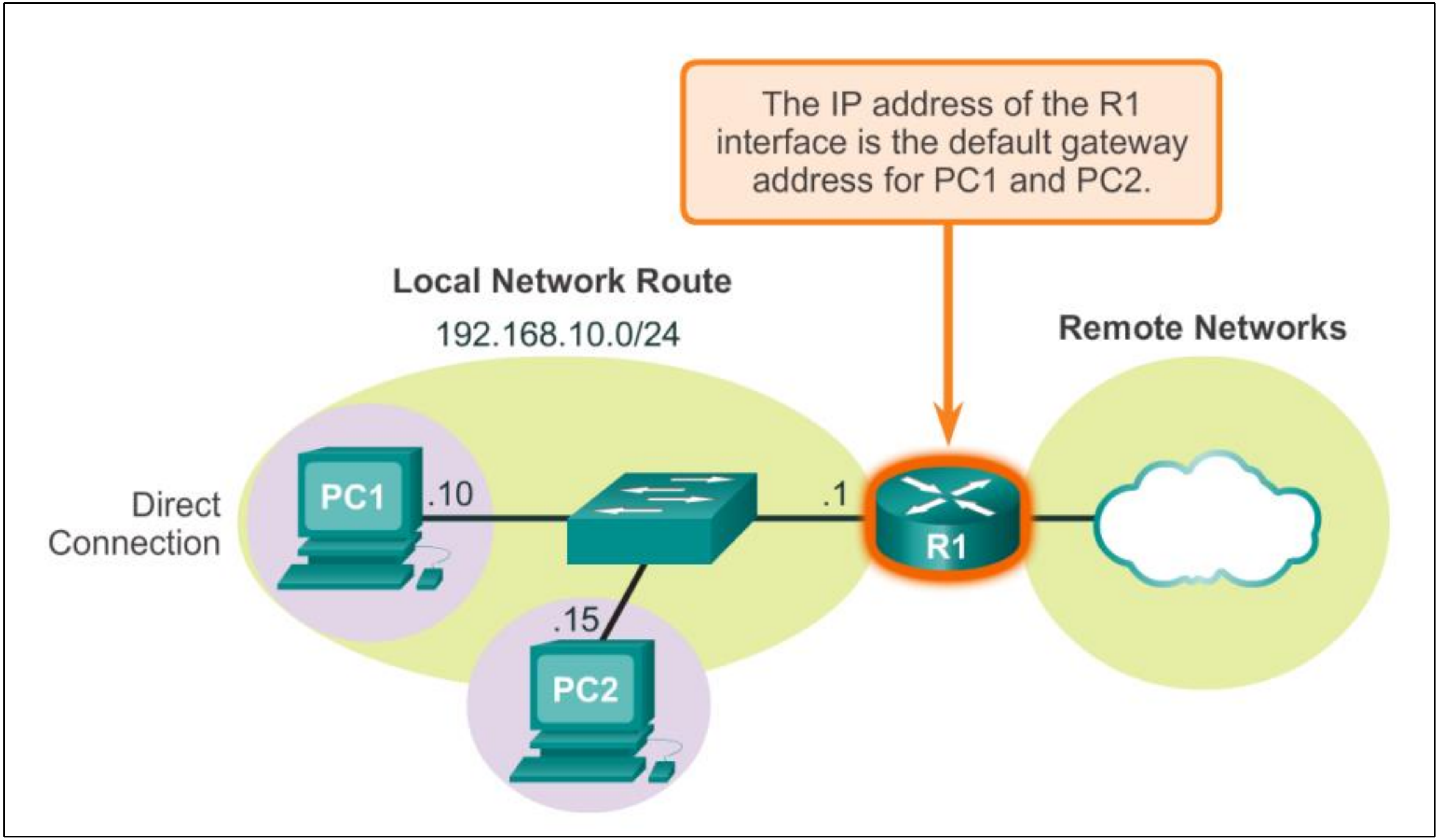
IPv6 Packet

IPv6 Packet Header



6.2 Routing

Host Packet Forwarding Decision



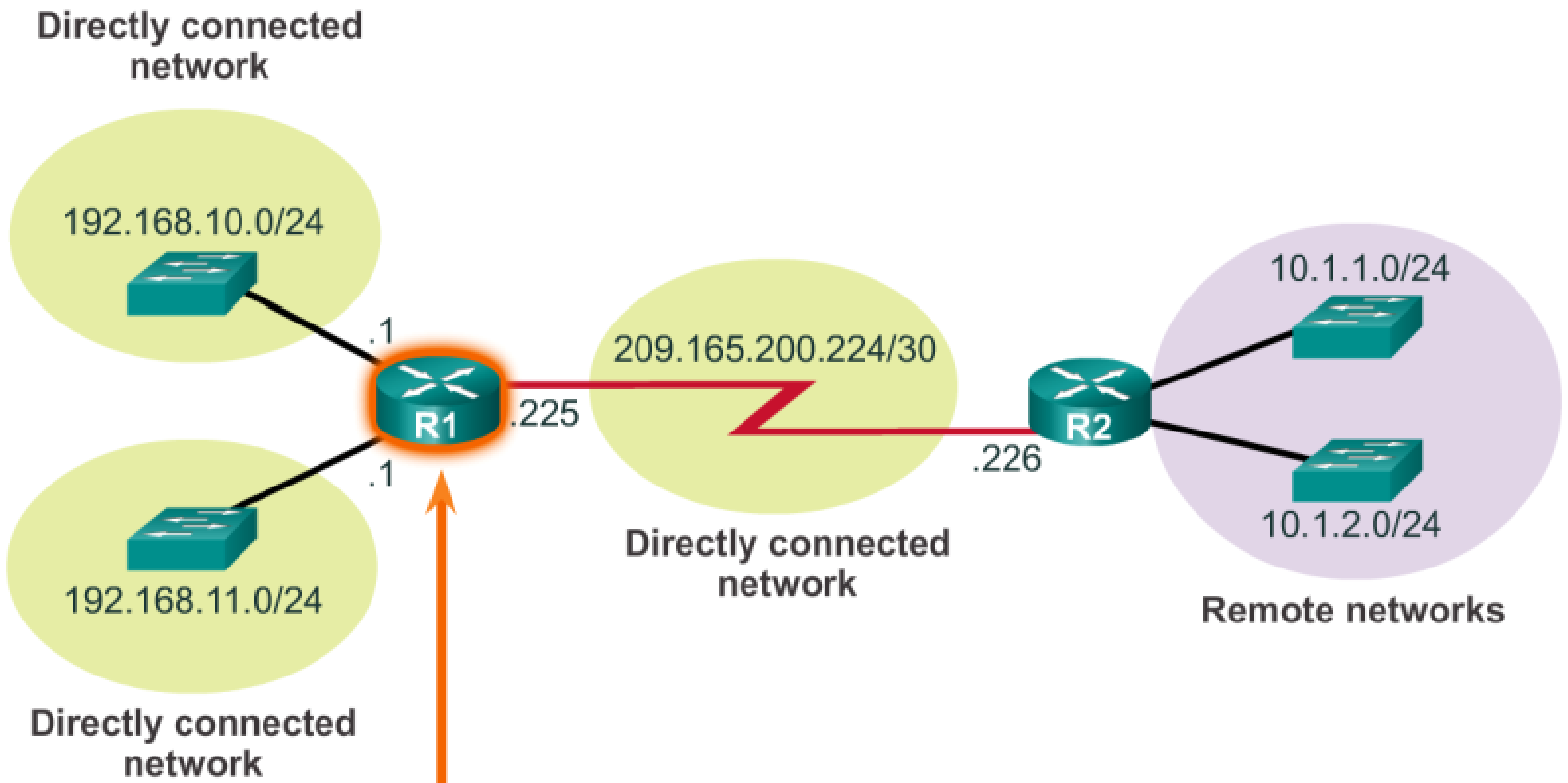
Default Gateway

Hosts must maintain their own, local, routing table to ensure that network layer packets are directed to the correct destination network. The local table of the host typically contains:

- Direct connection
- Local network route
- Local default route

Router Routing Tables

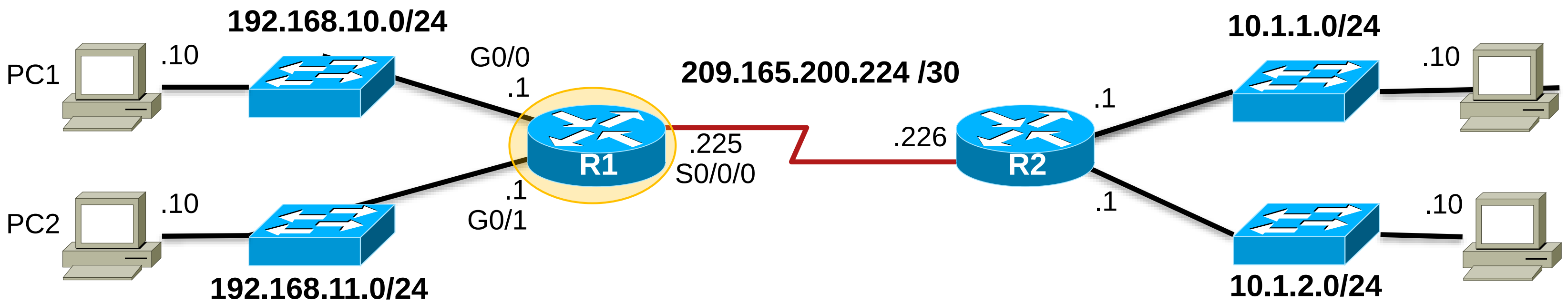
Router Packet Forwarding Decision



R1 has three directly connected networks: 192.168.10.0/24, 192.168.11.0/24, and 209.165.200.224/30. R1 also has two remote networks that it can learn about from R2: 10.1.1.0/24 and 10.1.2.0/24.

Router Routing Tables

IPv4 Router Routing Table



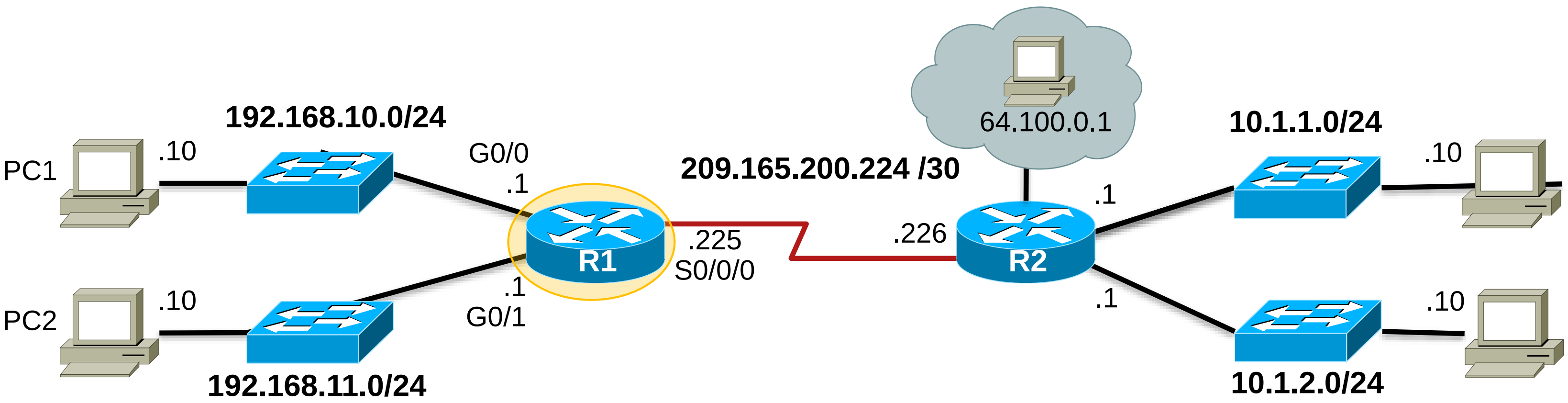

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05, Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C       209.165.200.224/30 is directly connected, Serial0/0/0
L       209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

Router Routing Tables

Directly Connected Routing Table Entries

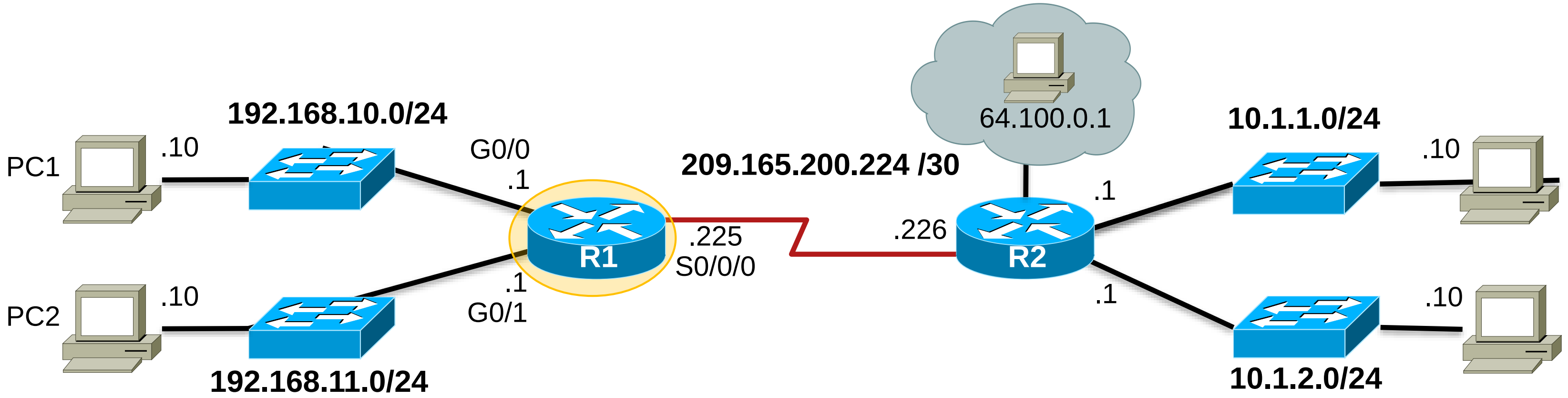


A		B	C
C		192.168.10.0/24 is directly connected,	GigabitEthernet0/0
L		192.168.10.1/32 is directly connected,	GigabitEthernet0/0

A	Identifies how the network was learned by the router.
B	Identifies the destination network and how it is connected.
C	Identifies the interface on the router connected to the destination network.

Router Routing Tables

Remote Network Routing Table Entries



D		10.1.1.0/24	[90	/2170112]	via	209.165.200.226,	00:00:05,	Serial0/0/0	

A	Identifies how the network was learned by the router.
B	Identifies the destination network.
C	Identifies the administrative distance (trustworthiness) of the route source.
D	Identifies the metric to reach the remote network.
E	Identifies the next hop IP address to reach the remote network.
F	Identifies the amount of elapsed time since the network was discovered.
G	Identifies the outgoing interface on the router to reach the destination network.

Activity

A	B	C	D	E	F
D	192.168.1.0/24	[90/3072]	via 192.168.3.1,	00:06:03,	GigabitEthernet0/0

	A	B	C	D	E	F
1. The elapsed time since the network was discovered.						
2. The administrative distance (source) and metric to reach the remote network.						
3. How the network was learned by the router.						
4. Shows the destination network.						
5. The next hop IP address to reach the remote network.						

Activity Solution

```
A       B               C          D                  E            F
----------------------------------------------------------------------------
D   192.168.1.0/24   [90/3072]   via 192.168.3.1,   00:06:03,   GigabitEthernet0/0
```

	A	B	C	D	E	F
1. The elapsed time since the network was discovered.					✓	
2. The administrative distance (source) and metric to reach the remote network.			✓			
3. How the network was learned by the router.	✓					
4. Shows the destination network.		✓				
5. The next hop IP address to reach the remote network.				✓		

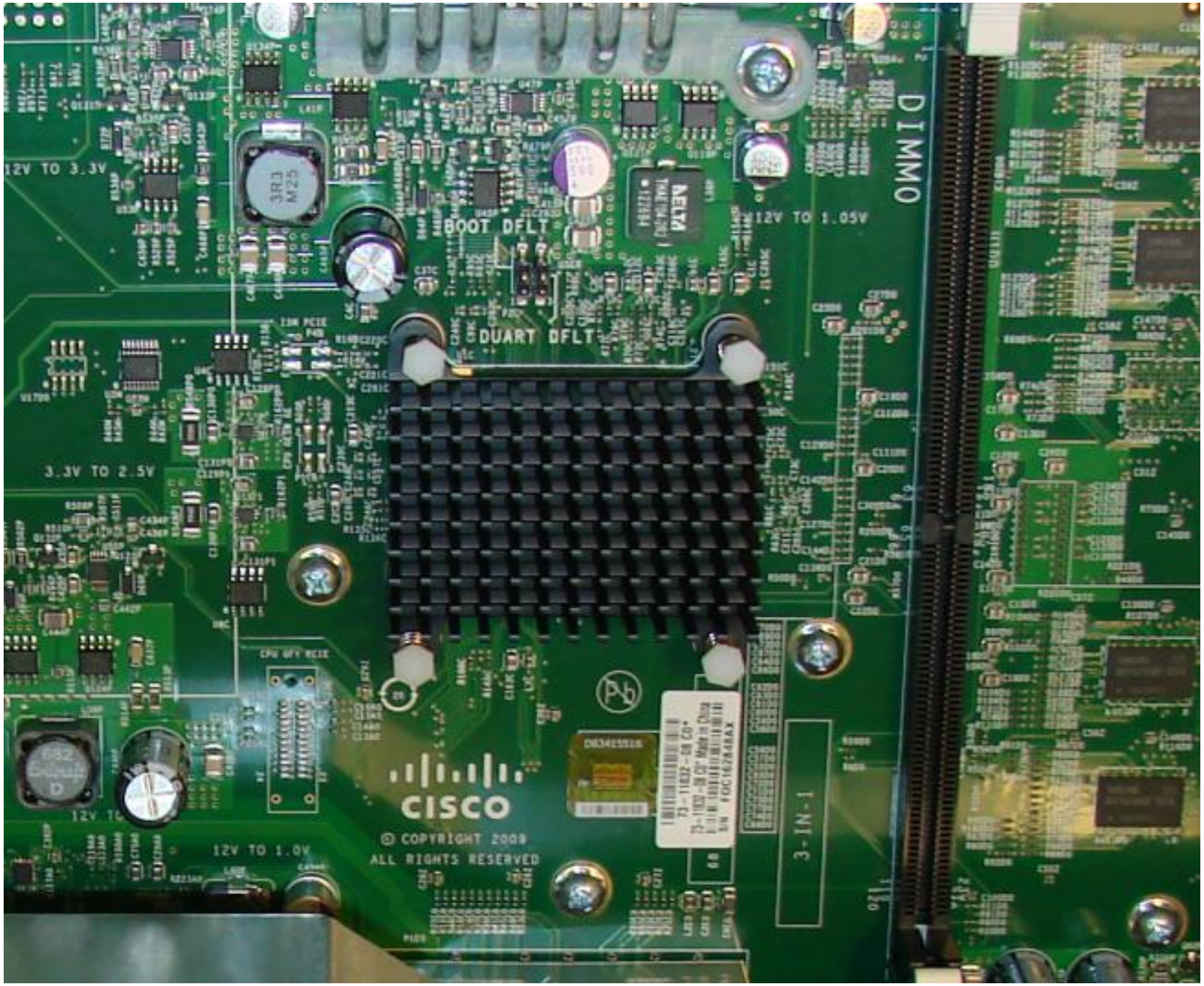
6.3 Routers

Anatomy of a Router

A Router is a Computer

Anatomy of a Router

Router CPU and OS



Router Memory

Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	• Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
ROM	Non-Volatile	• Bootup instructions • Basic diagnostic software • Limited IOS
NVRAM	Non-Volatile	• Startup configuration file
Flash	Non-Volatile	• IOS • Other system files

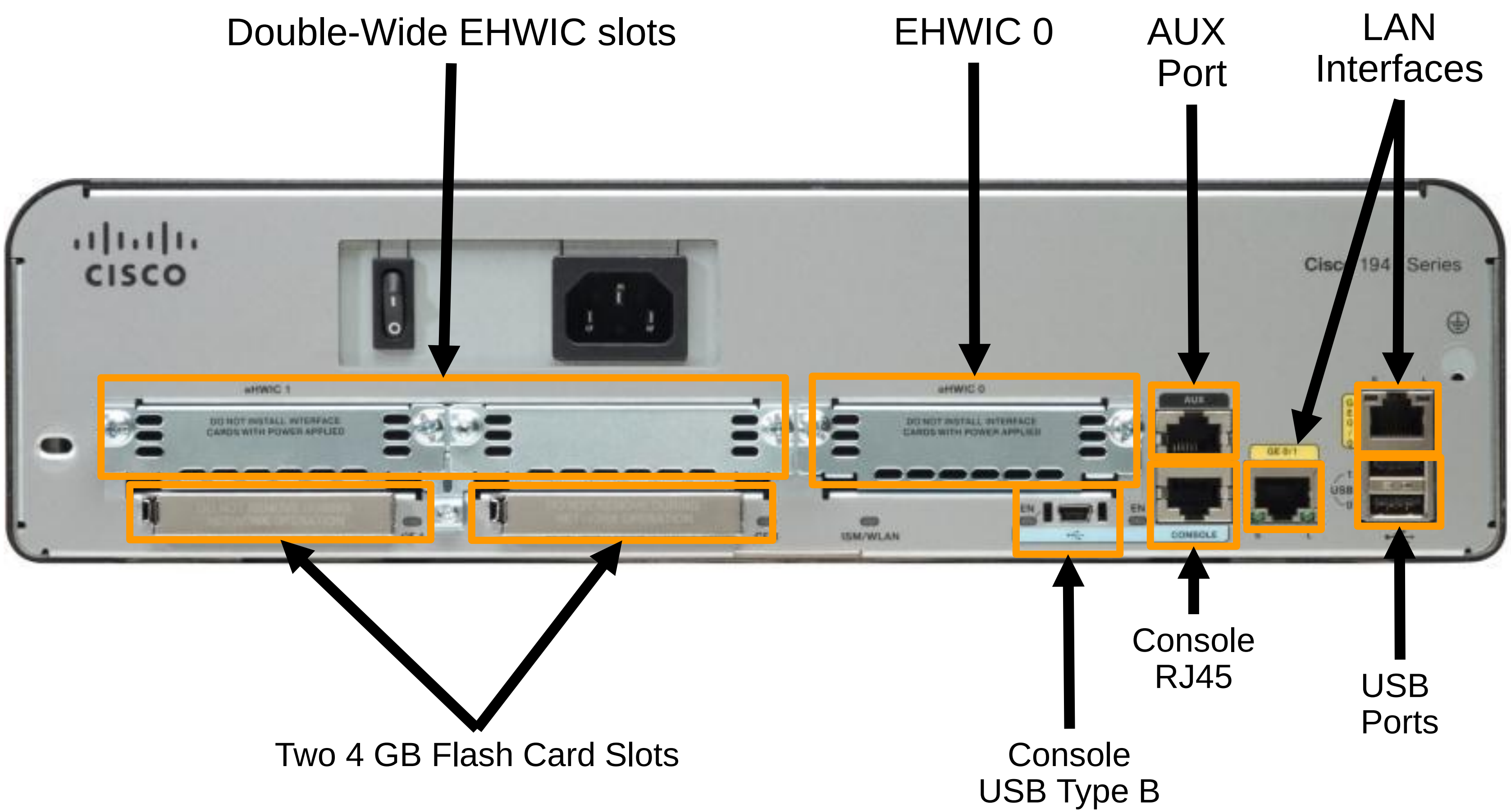
Anatomy of a Router

Inside a Router

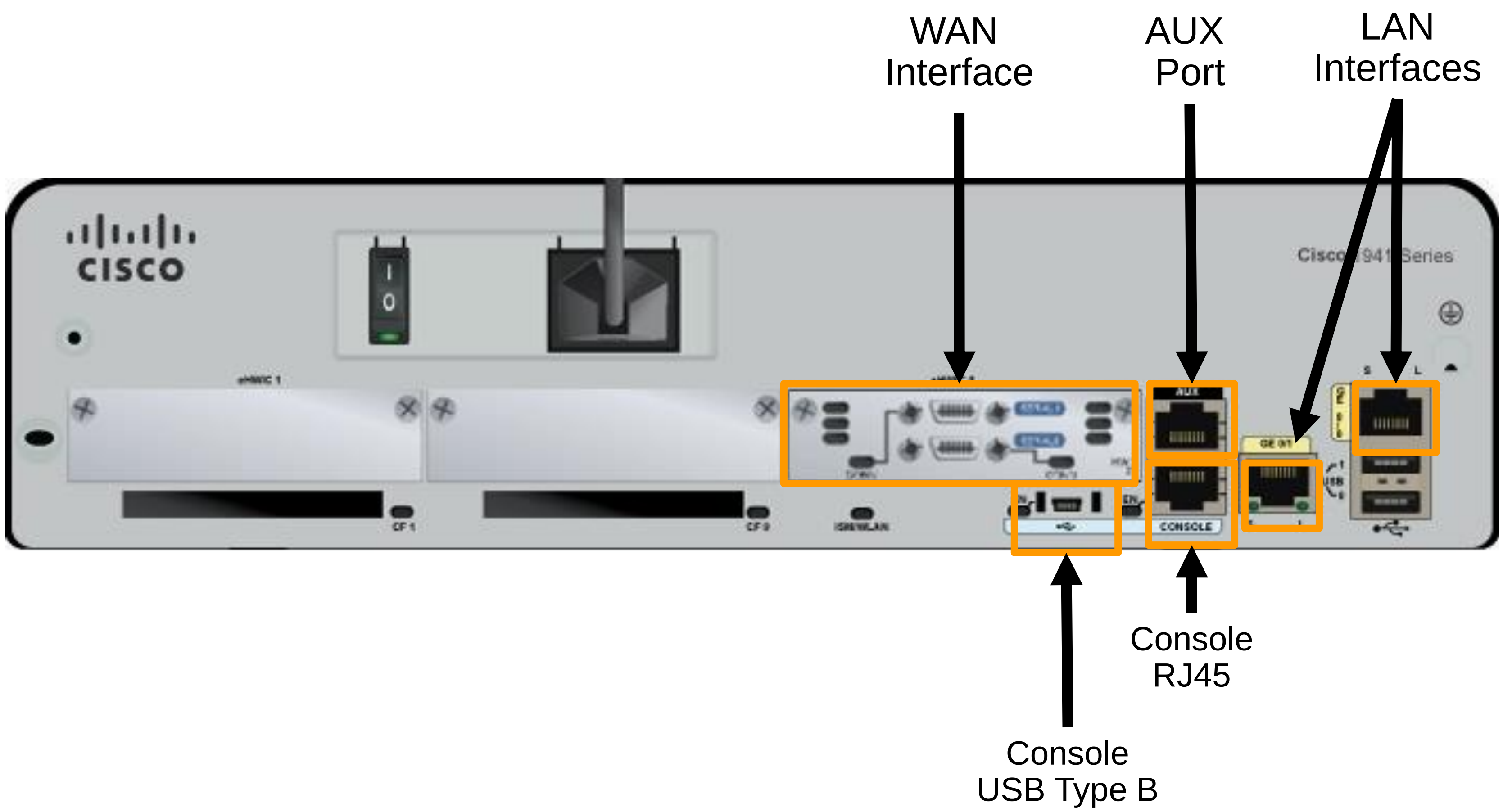
1. Power Supply
2. Shield for WIC (WAN Interface Card)
3. Fan
4. SDRAM
5. NVRAM
6. CPU
7. Advanced Integration Module (AIM)

Anatomy of a Router

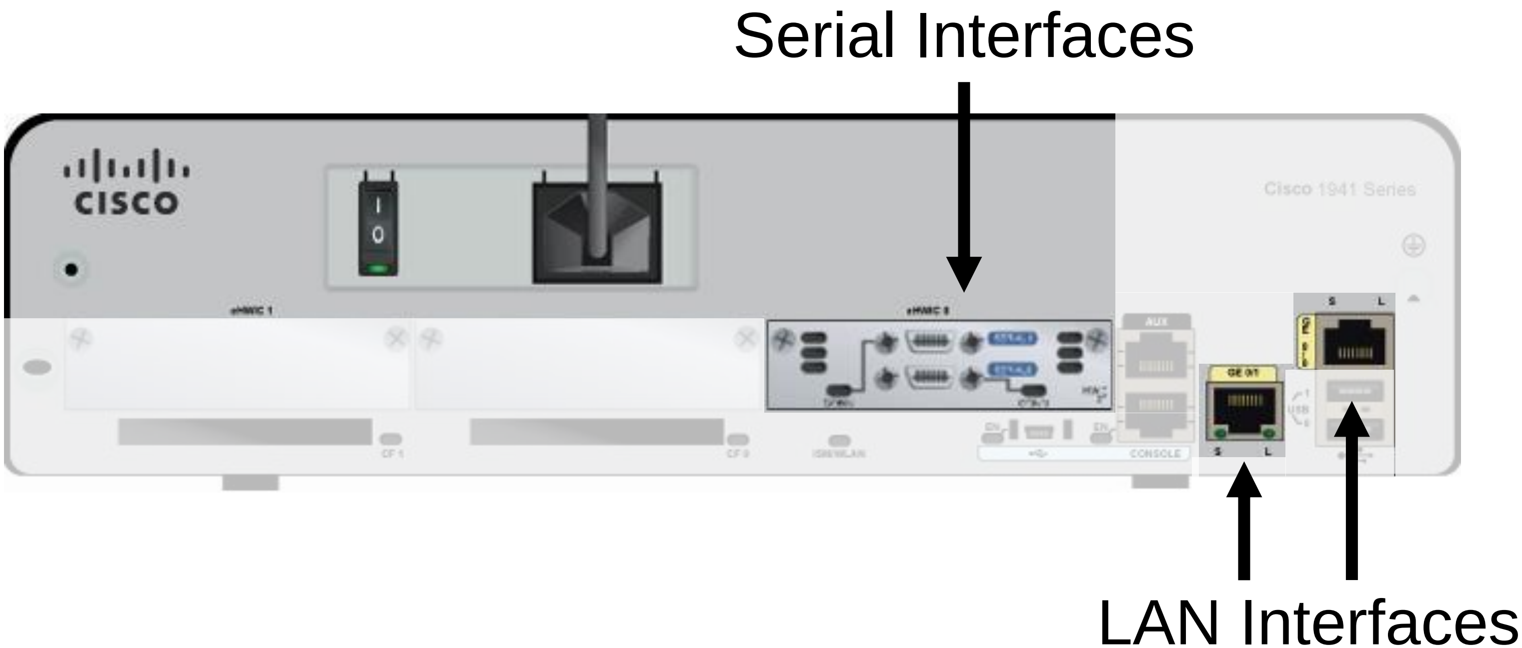
Router Backplane



Connecting to a Router



LAN and WAN Interfaces



Router Boot-up

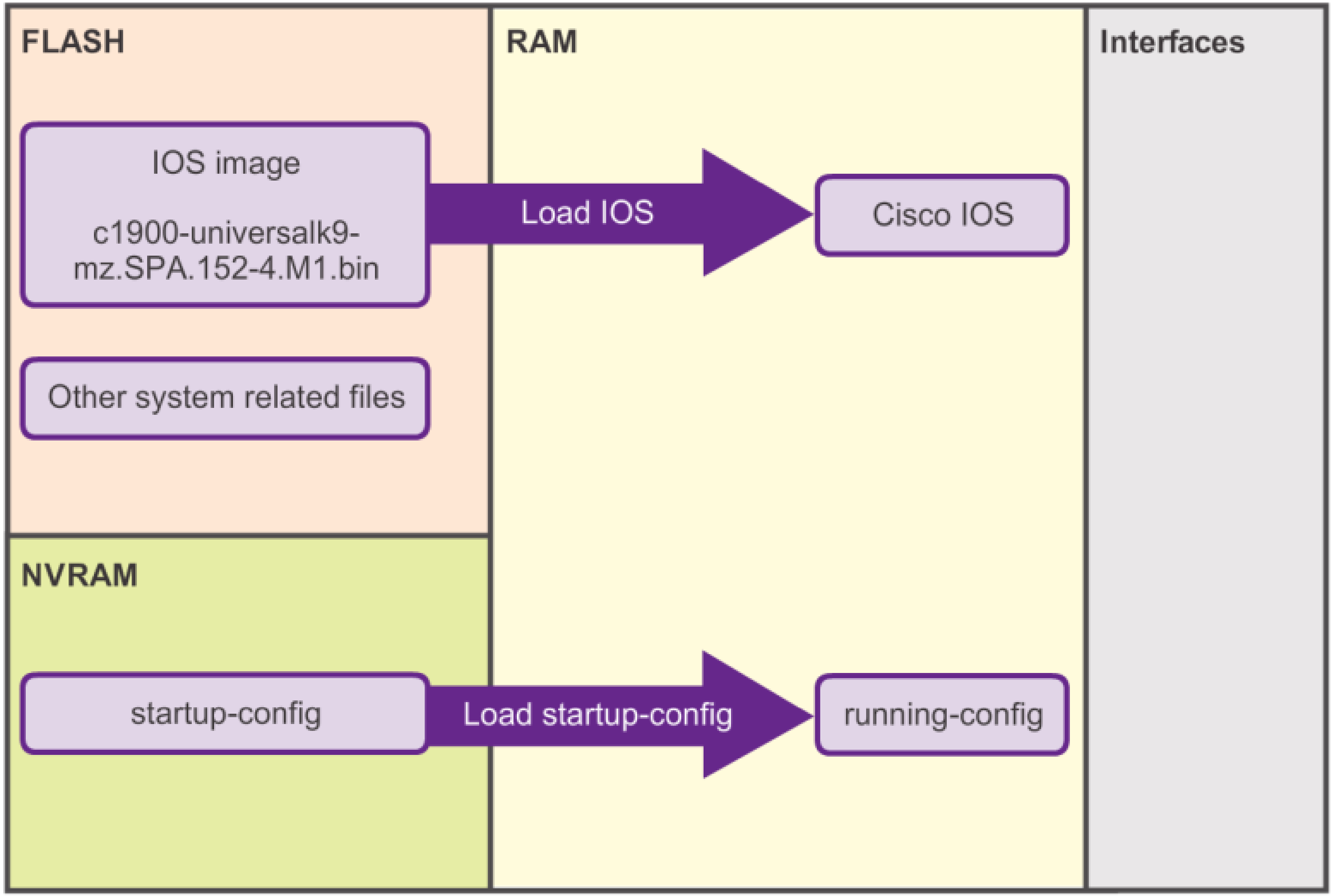
Cisco IOS

The Cisco IOS operational details vary on different internetworking devices, depending on the device's purpose and feature set. However, Cisco IOS for routers provides the following:

- Addressing
- Interfaces
- Routing
- Security
- QoS
- Resources Management

Router Boot-up

Bootset Files



Cisco | Networking Academy®
Mind Wide Open™