Chapter 6:
Network Layer

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Network layer

- Transport segment from sending to receiving host
- On sending side encapsulates segments into datagrams
- On receiving side, delivers segments to transport layer
- Network layer protocols in *every* host and router
- Router examines header fields in all IP datagrams passing through it

Two key network-layer functions

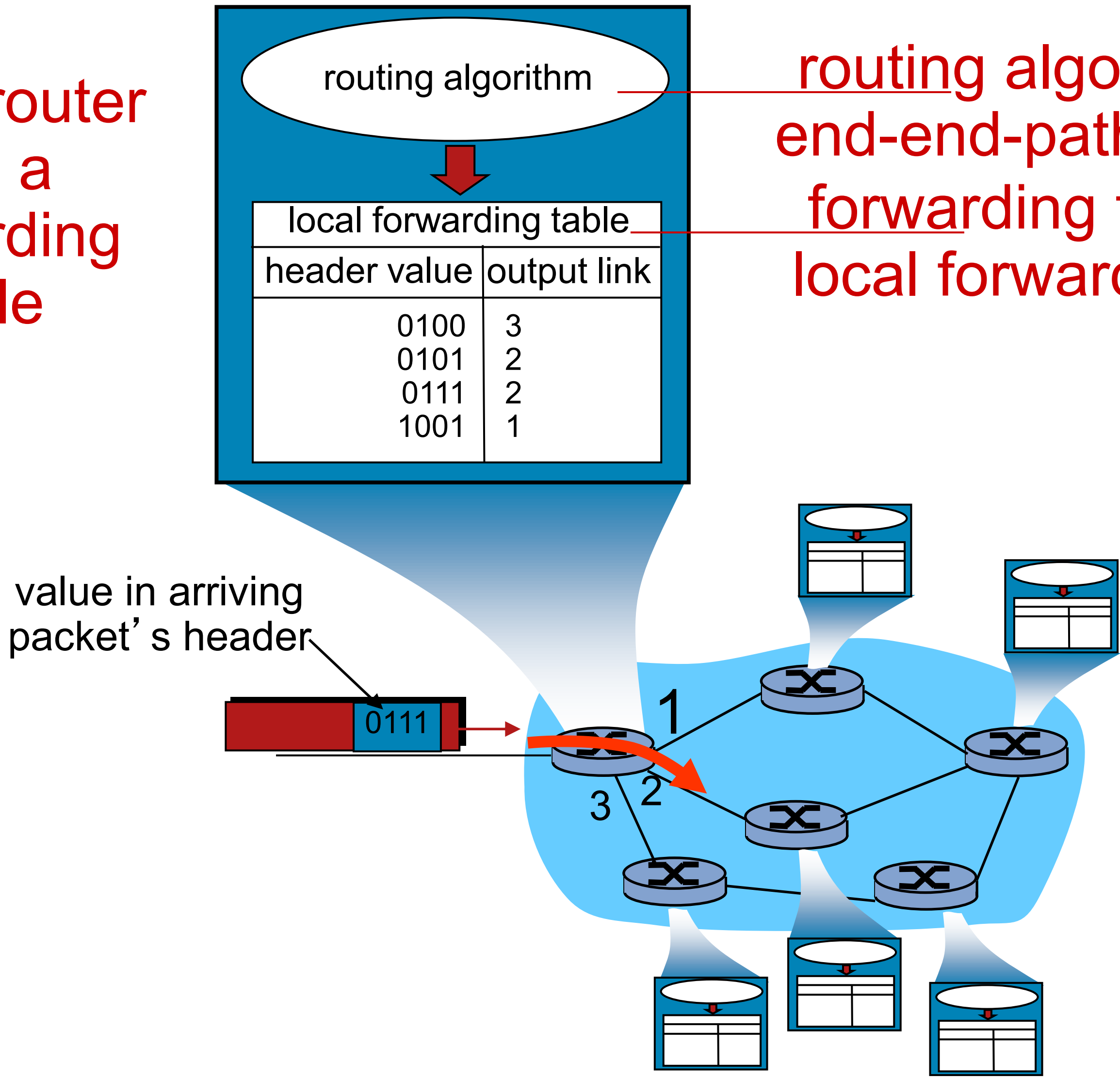
The role of the network layer is simple — to move packets from a sending host to a receiving host.

- *Forwarding:* When a packet arrives at a router's input link, the router must move the packet to the appropriate output link.
- *Routing:* Determine the route or path taken by packets as they flow from a sender to a receiver

  The algorithms that calculate these paths are referred to as **Routing Algorithms.**

Interplay between routing and forwarding

Every router has a forwarding table



routing algorithm determines end-end-path through network

forwarding table determines local forwarding at this router

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:

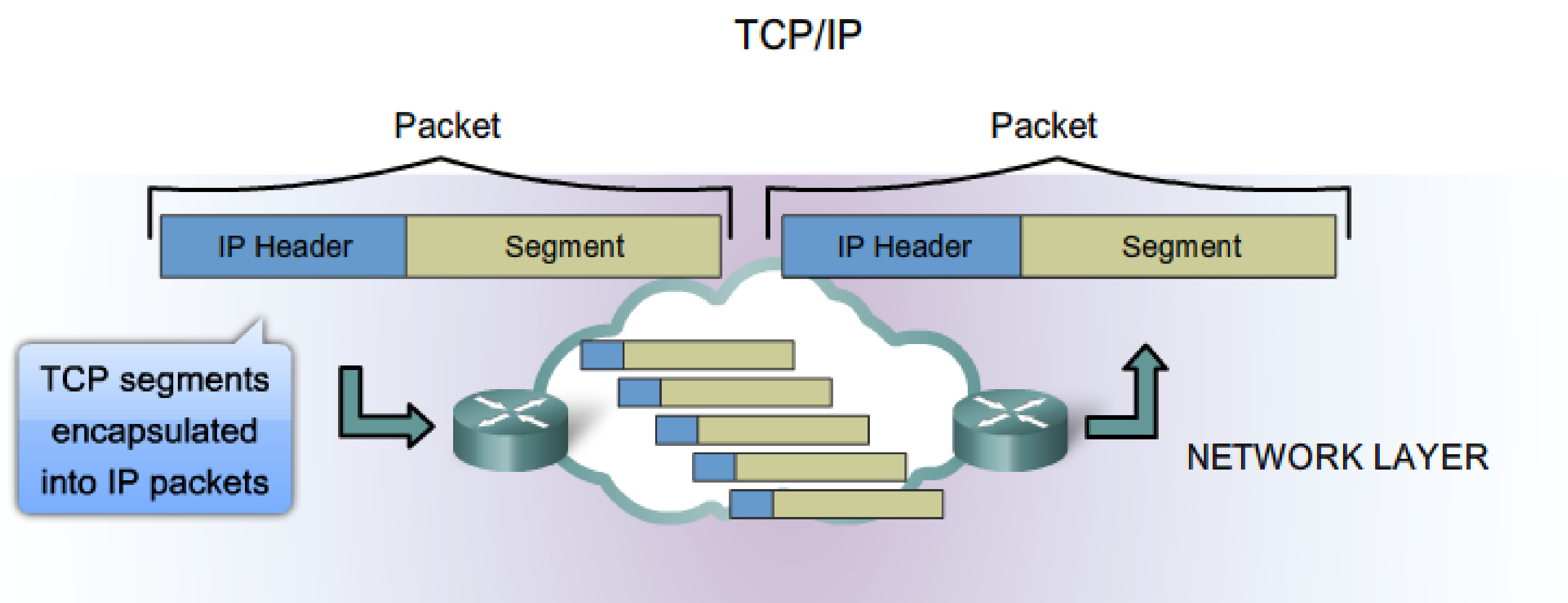
- IP version 4 (IPv4)
- IP version 6 (IPv6)

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:

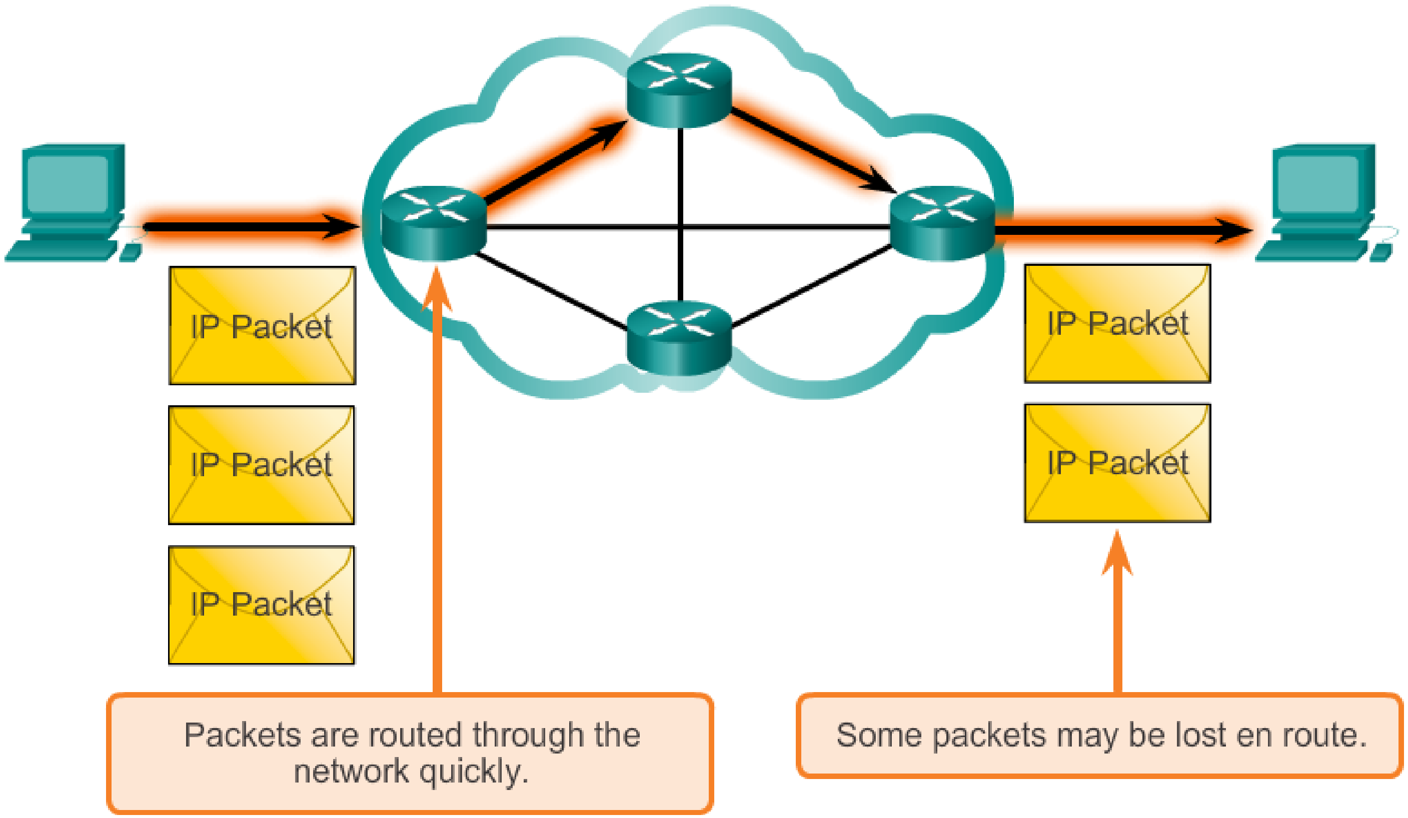
- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

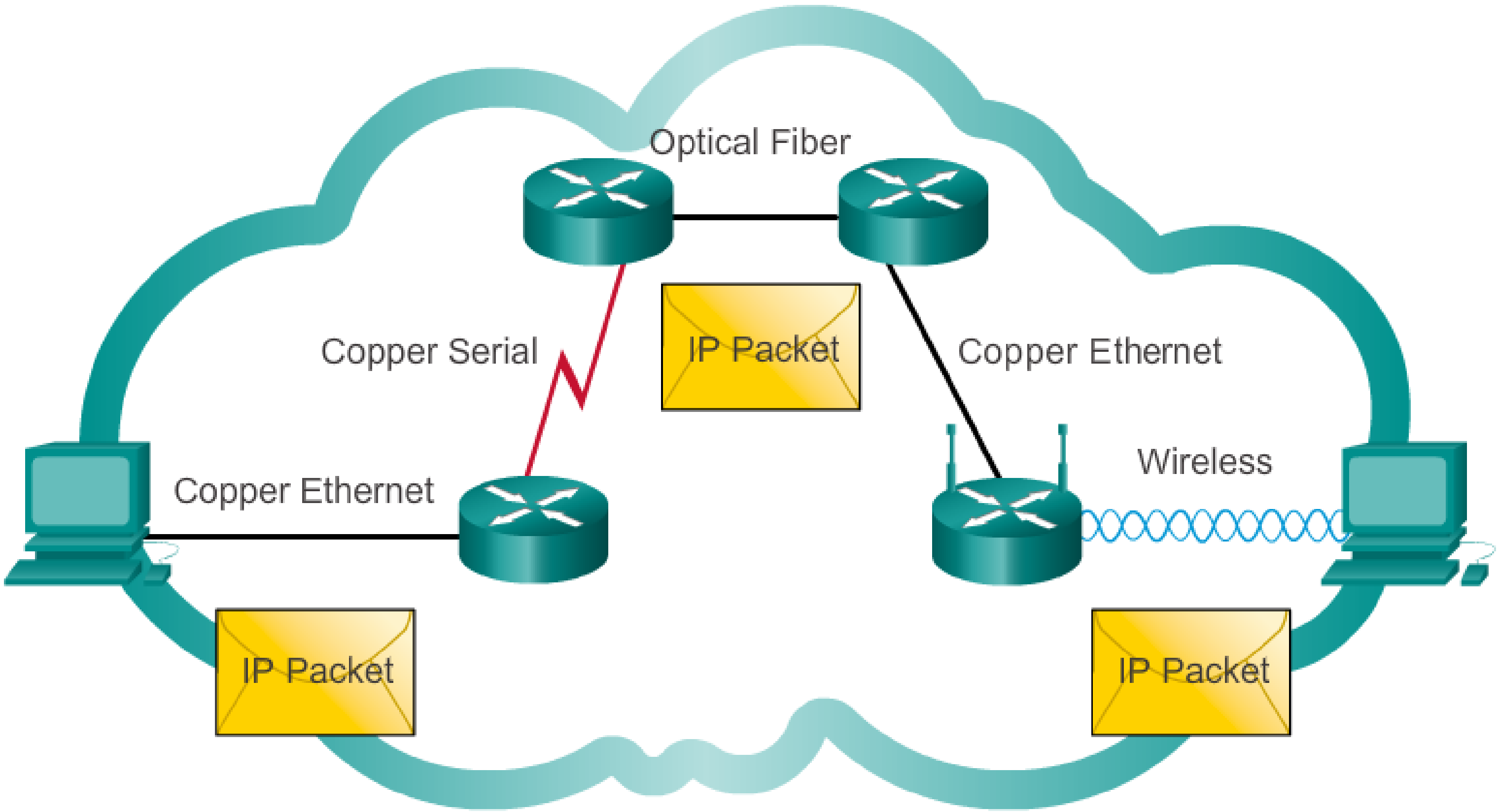
Characteristics of the IP protocol

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.

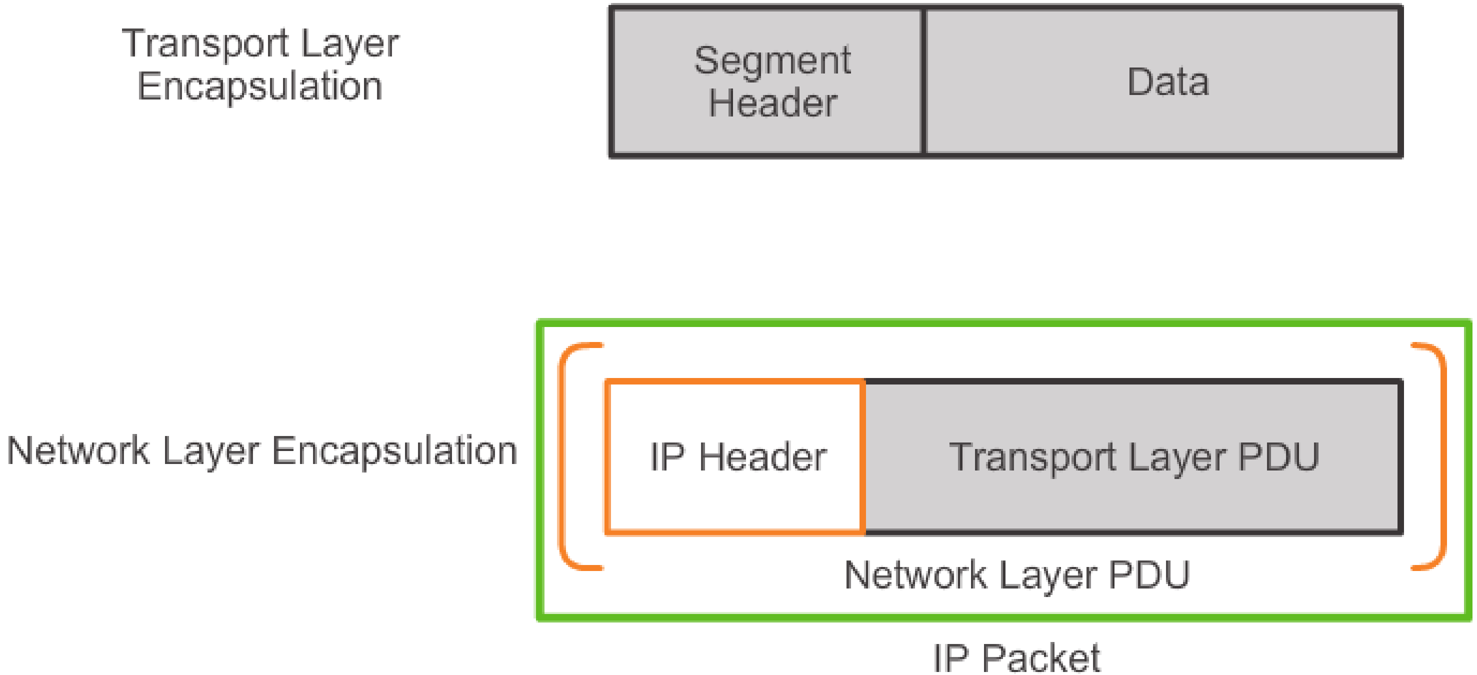
IP – Media Independent



IP packets can travel over different media.

IPv4 Packet

Encapsulating IP

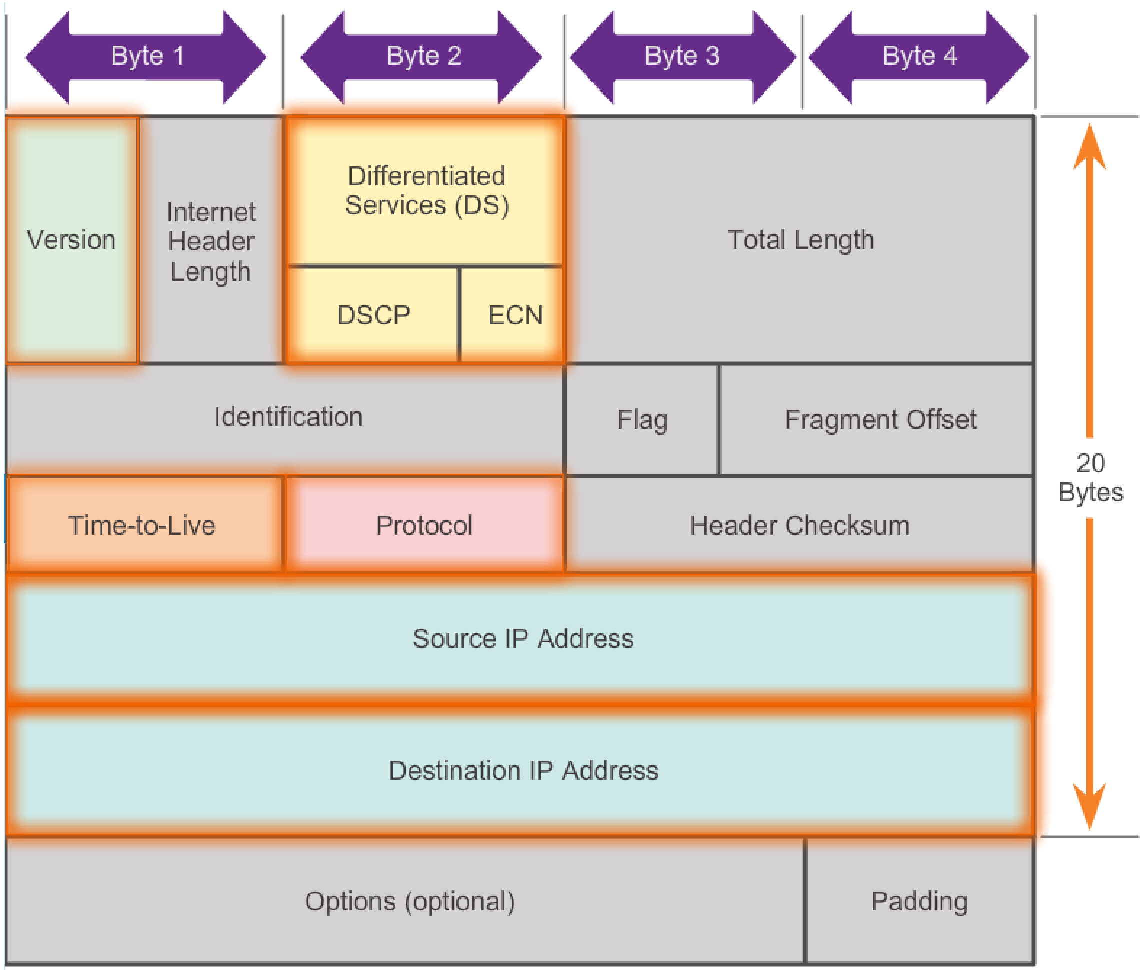


The network layer adds a header so packets can be routed through complex networks and reach their destination. In TCP/IP based networks, the network layer PDU is the IP packet.

IPv4 Packet

IPv4 Packet Header

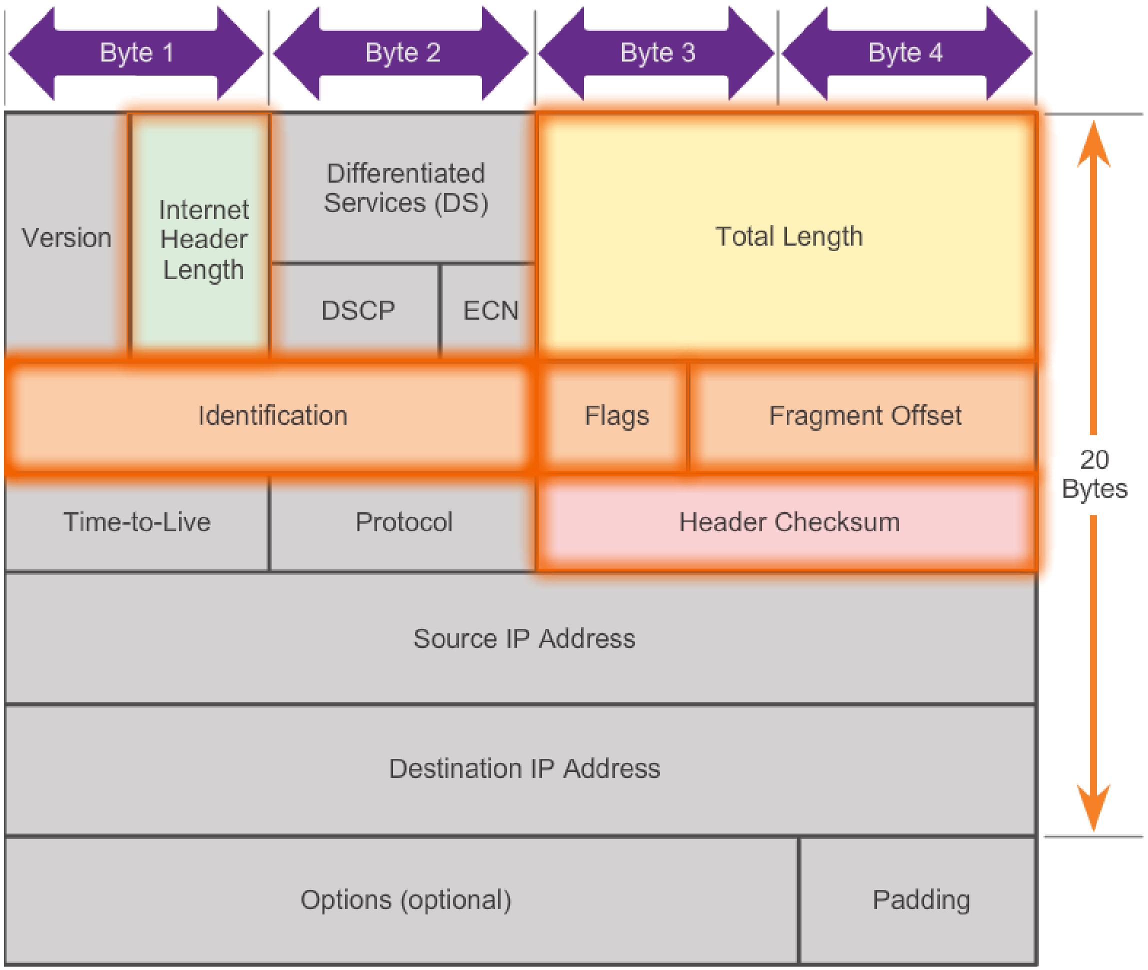
Contents of the IPv4 packet header

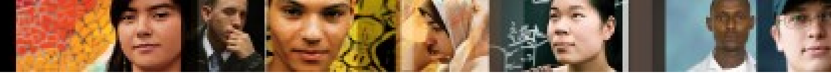


IPv4 Packet

IPv4 Header Fields

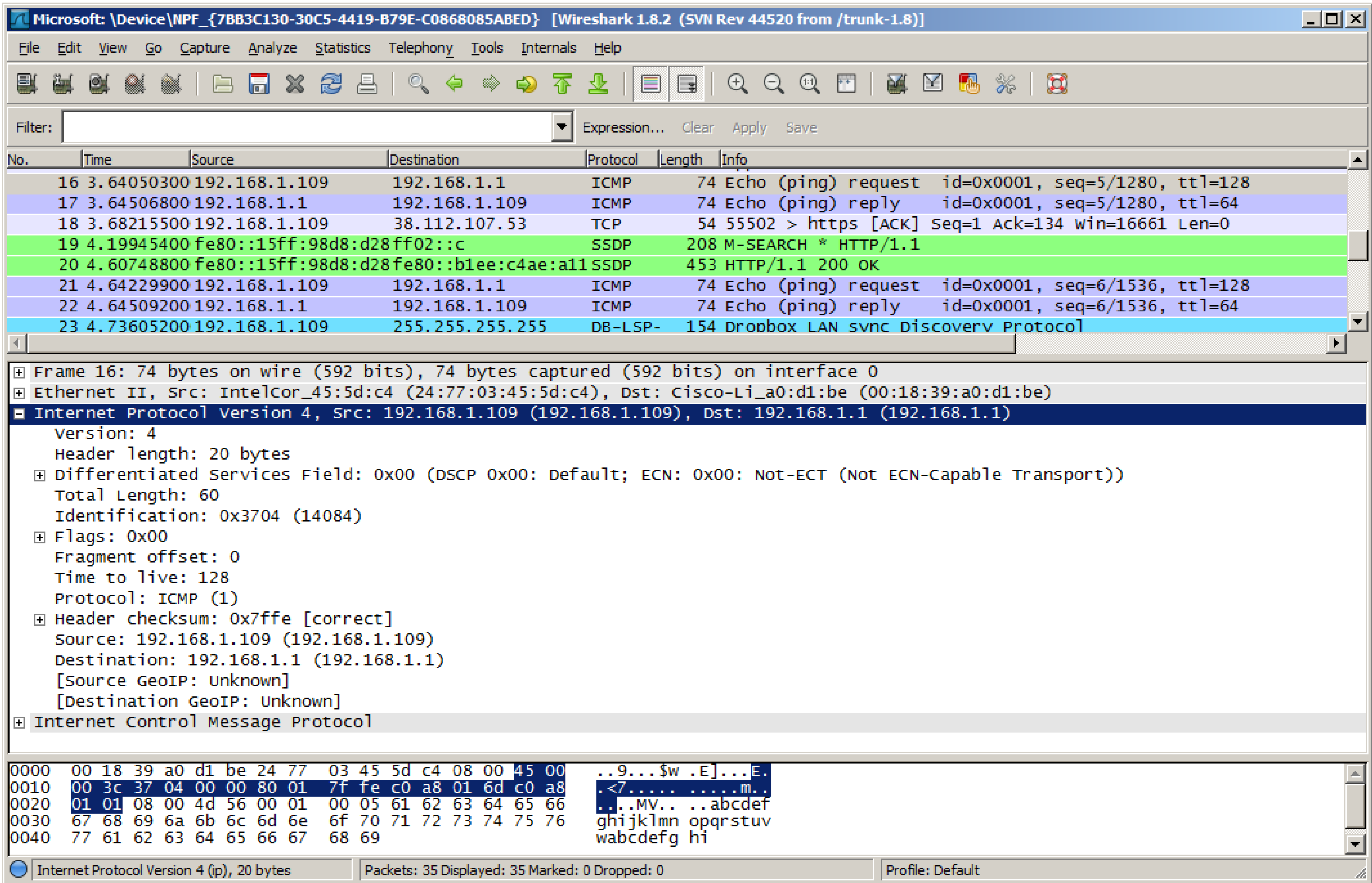
Contents of the IPv4 header fields





IPv4 Packet

Sample IPv4 Headers



Network Layer in Communication

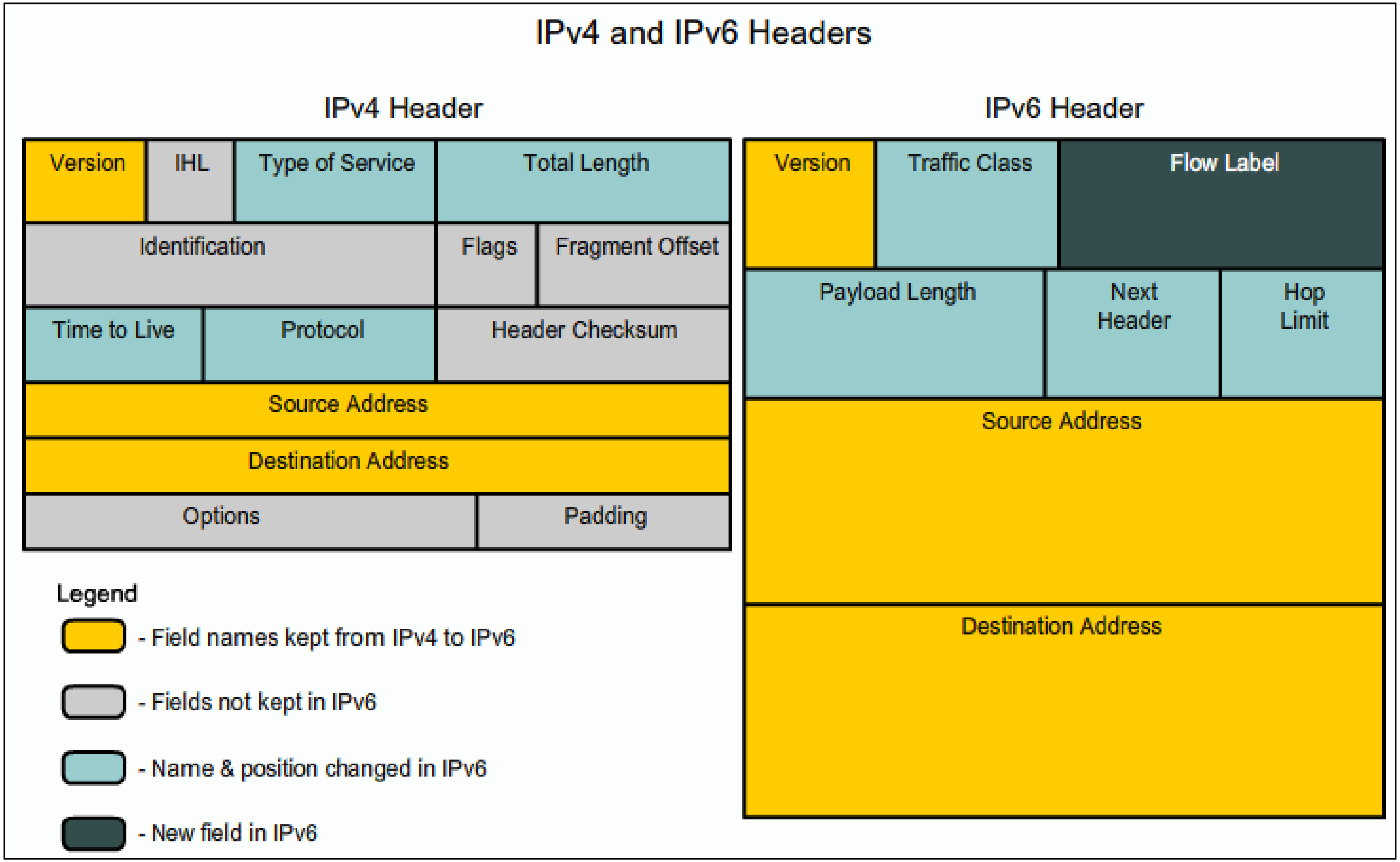
Limitations of IPv4

- IP Address depletion
- Internet routing table expansion
- Lack of end-to-end connectivity

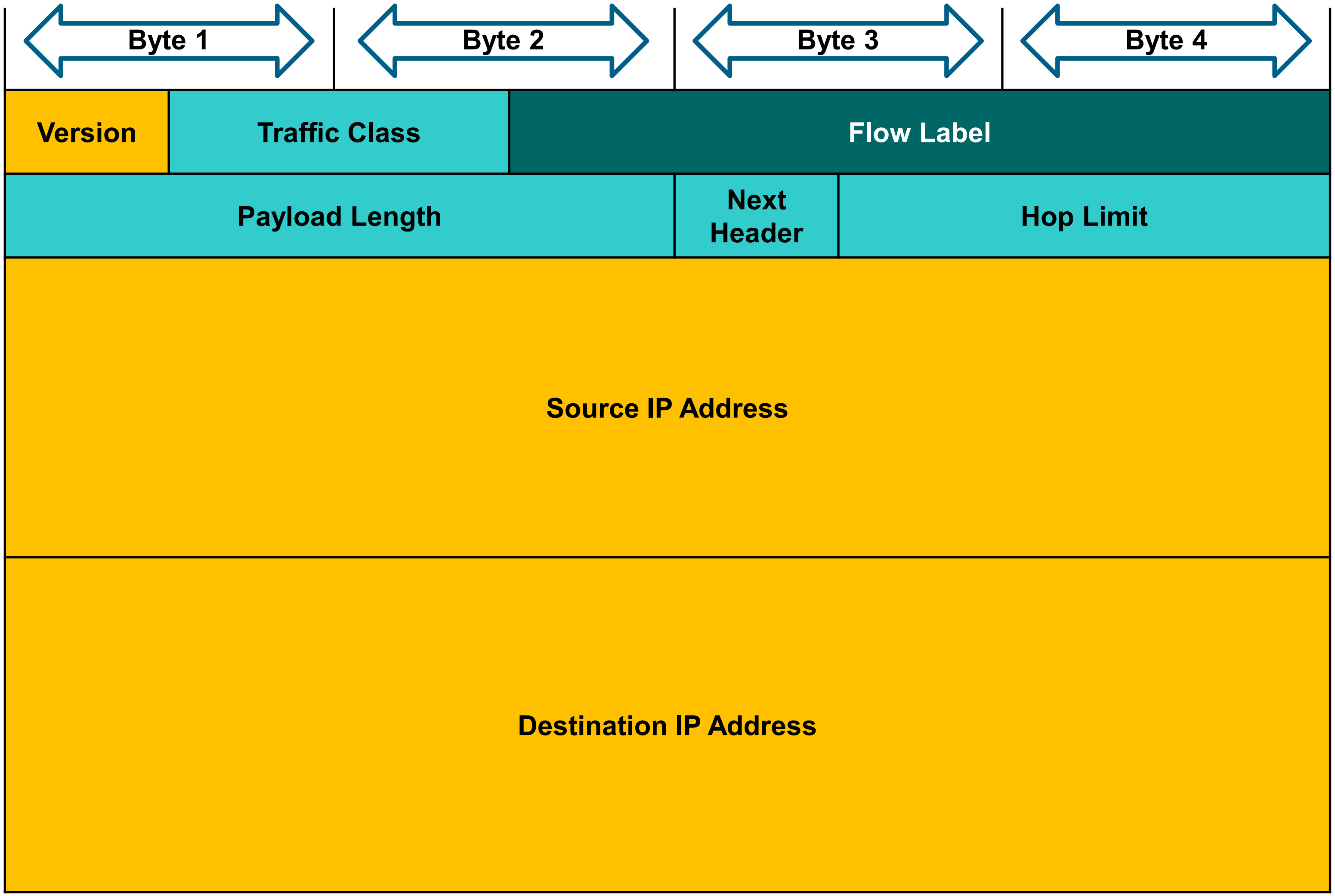
Introducing IPv6

- 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

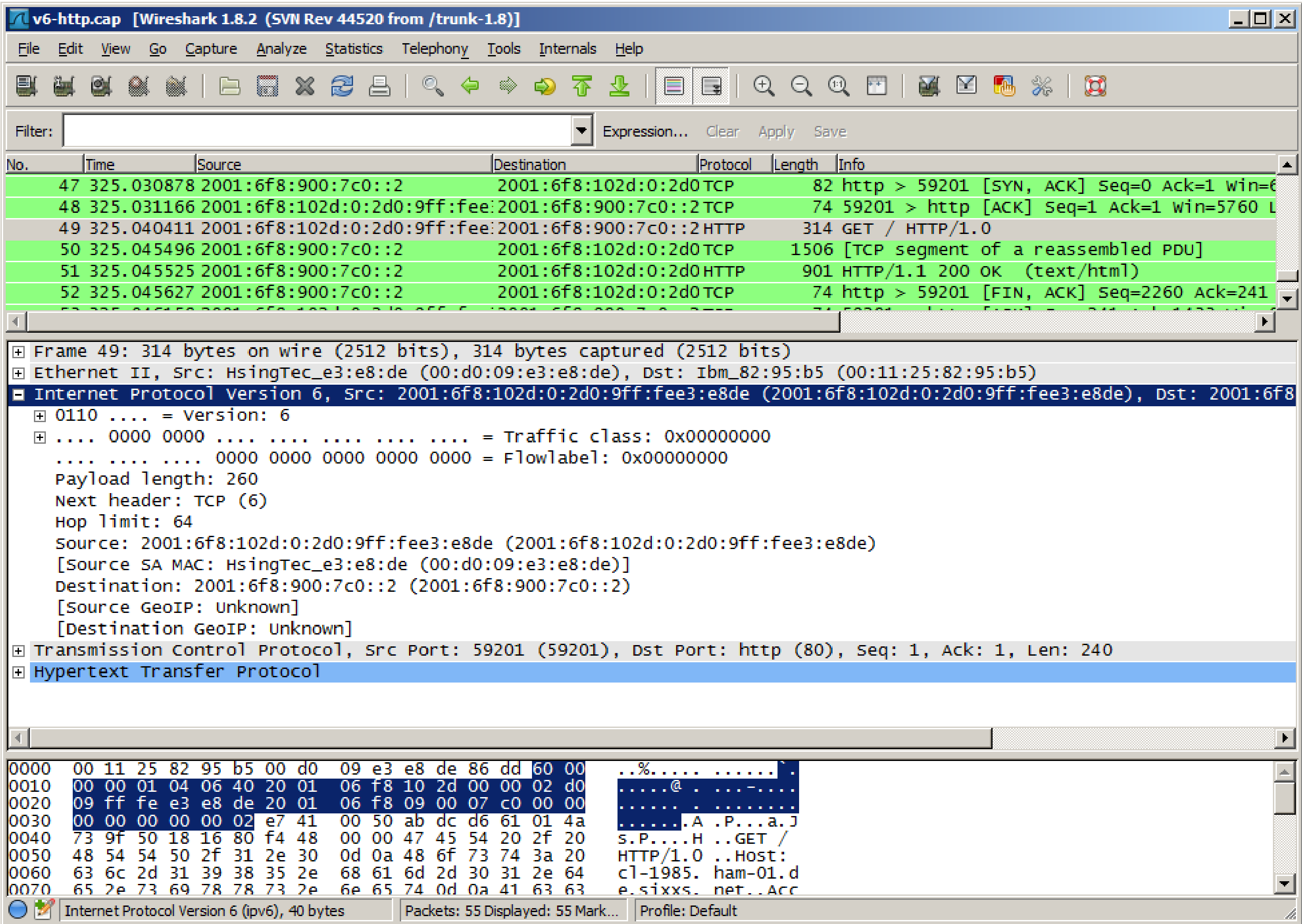
IPv6 Packet
Encapsulating IPv6



IPv6 Packet Header



Sample IPv6 Header



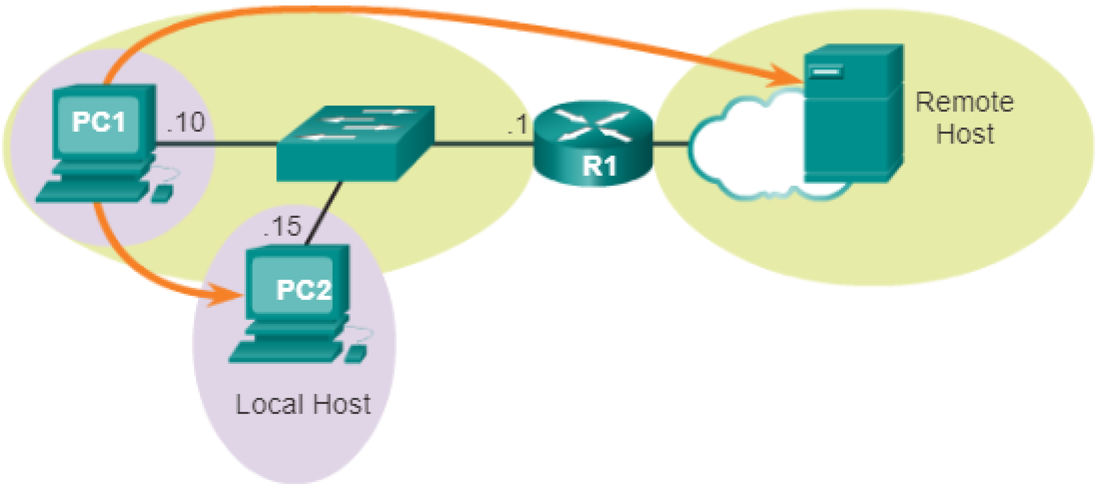
6.2 Routing

Cisco | Networking Academy®
Mind Wide Open™

How a host routes

A host can send a packet to:

- **Itself**
- **Local host**
- **Remote host**



Host Routing Tables

How a host routes

A host can send a packet to:

- **Itself** - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1 which is referred to as the ***loopback interface***. This loopback address is automatically assigned to a host when TCP/IP is running. The ability for a host to send a packet to itself using network functionality is useful for testing purposes. Any IP within the network 127.0.0.0/8 refers to the local host.
- **Local host** - This is a host on the same network as the sending host. The hosts share the same network address.
- **Remote host** - This is a host on a remote network. The hosts do not share the same network address.

Host Routing Tables

How a host routes

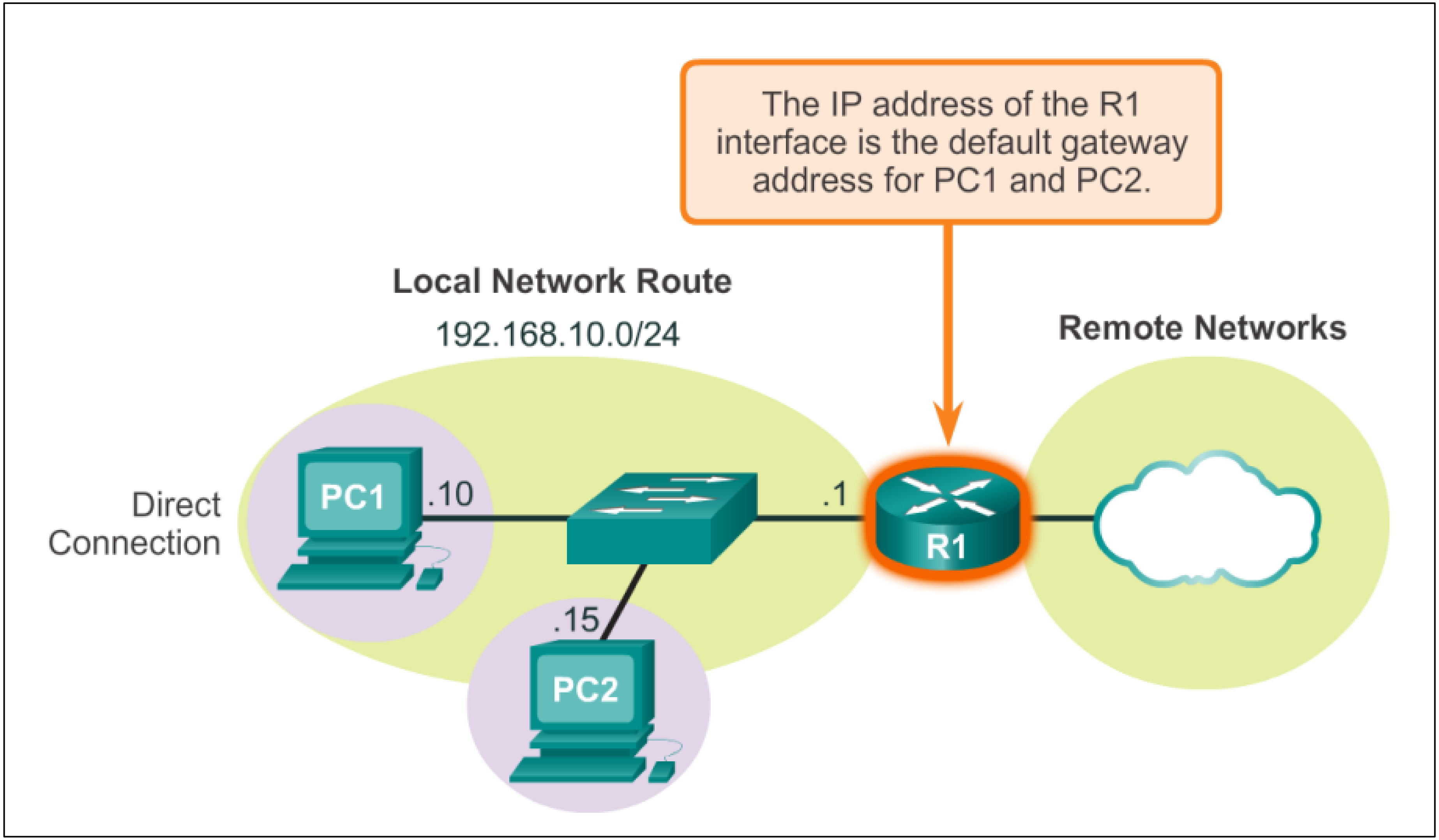
- Devices that are beyond the local network segment are known as remote hosts.
- When a source device sends a packet to a remote destination device, then the help of routers and routing is needed.
- Routing is the process of identifying the best path to a destination.
- The router connected to the local network segment is referred to as the **default gateway**.

Host Routing Tables

Default Gateway

- The default gateway is the device that routes traffic from the local network to devices on remote networks.
- In a home or small business environment, the default gateway is often used to connect the local network to the Internet.
- 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

Host Packet Forwarding Decision



Host Routing Tables

Displaying the Routing Table

- **netstat -r** command can be used to display the host routing table.
- It displays three sections related to the current TCP/IP network connections:
- **Interface List -** Lists the Media Access Control (MAC) address and assigned interface number of every network-capable interface on the host including Ethernet, Wi-Fi, and Bluetooth adapters.
- **IPv4 Route Table -** Lists all known IPv4 routes, including direct connections, local network, and local default routes.
- **IPv6 Route Table -** Lists all known IPv6 routes, including direct connections, local network, and local default routes.

Host Routing Tables

Displaying the Routing Table


```
C:\Users\PC1>netstat -r

<Output omitted>

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     192.168.10.0    255.255.255.0         On-link     192.168.10.10    281
    192.168.10.10  255.255.255.255         On-link     192.168.10.10    281
   192.168.10.255  255.255.255.255         On-link     192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.10.10    281
===========================================================================

<Output omitted>
```

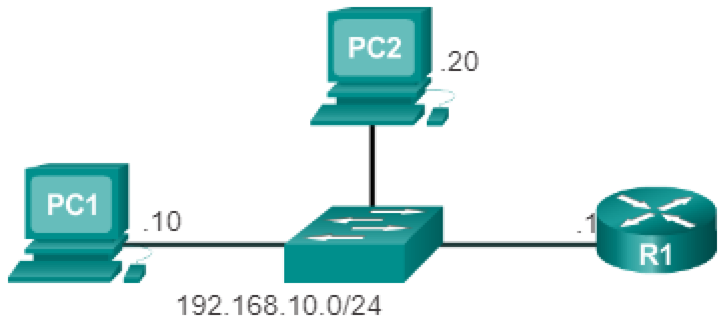
Host Routing Tables

Displaying the Routing Table

- The figure displays the IPv4 Route Table section of the output.
- The output is divided into five columns which identify.
- **Network Destination -** Lists the reachable networks.
- **Netmask -** Lists a subnet mask that informs the host how to determine the network and the host portions of the IP address.
- **Gateway -** Lists the address used by the local computer to get to a remote network destination. If a destination is directly reachable, it will show as “on-link” in this column.
- **Interface -** Lists the address of the physical interface used to send the packet to the gateway that is used to reach the network destination.
- **Metric -** Lists the cost of each route and is used to determine the best route to a destination.

Host Routing Tables

Displaying the Routing Table



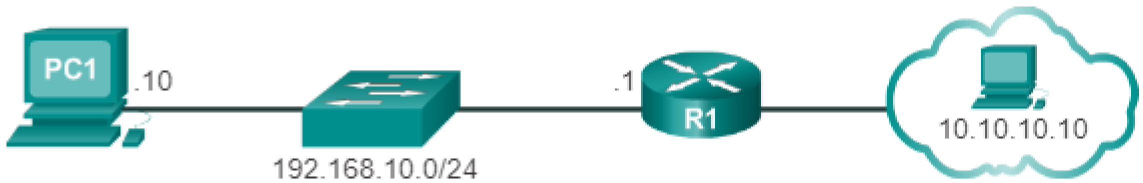

```
C:\Users\PC1> netstat -r
<Output omitted>
IPv4 Route Table
======================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     192.168.10.0    255.255.255.0         On-link     192.168.10.10    281
    192.168.10.10  255.255.255.255         On-link     192.168.10.10    281
   192.168.10.255  255.255.255.255         On-link     192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.10.10    281
======================================================================
<Output omitted>
```

For example, if PC1 wanted to send a packet to 192.168.10.20, it would:

1. Consult the IPv4 Route Table.
2. Match the destination IP address with the 192.168.10.0 Network Destination entry to reveal that the host is on the same network (On-link).
3. PC1 would then send the packet toward the final destination using its local interface (192.168.10.10).

Host Routing Tables

Displaying the Routing Table




```
C:\Users\PC1> netstat -r
<Output omitted>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
     192.168.10.0    255.255.255.0         On-link     192.168.10.10    281
    192.168.10.10  255.255.255.255         On-link     192.168.10.10    281
   192.168.10.255  255.255.255.255         On-link     192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.10.10    281
===========================================================================
<Output omitted>
```

If PC1 wanted to send a packet to a remote host located at 10.10.10.10, it would:

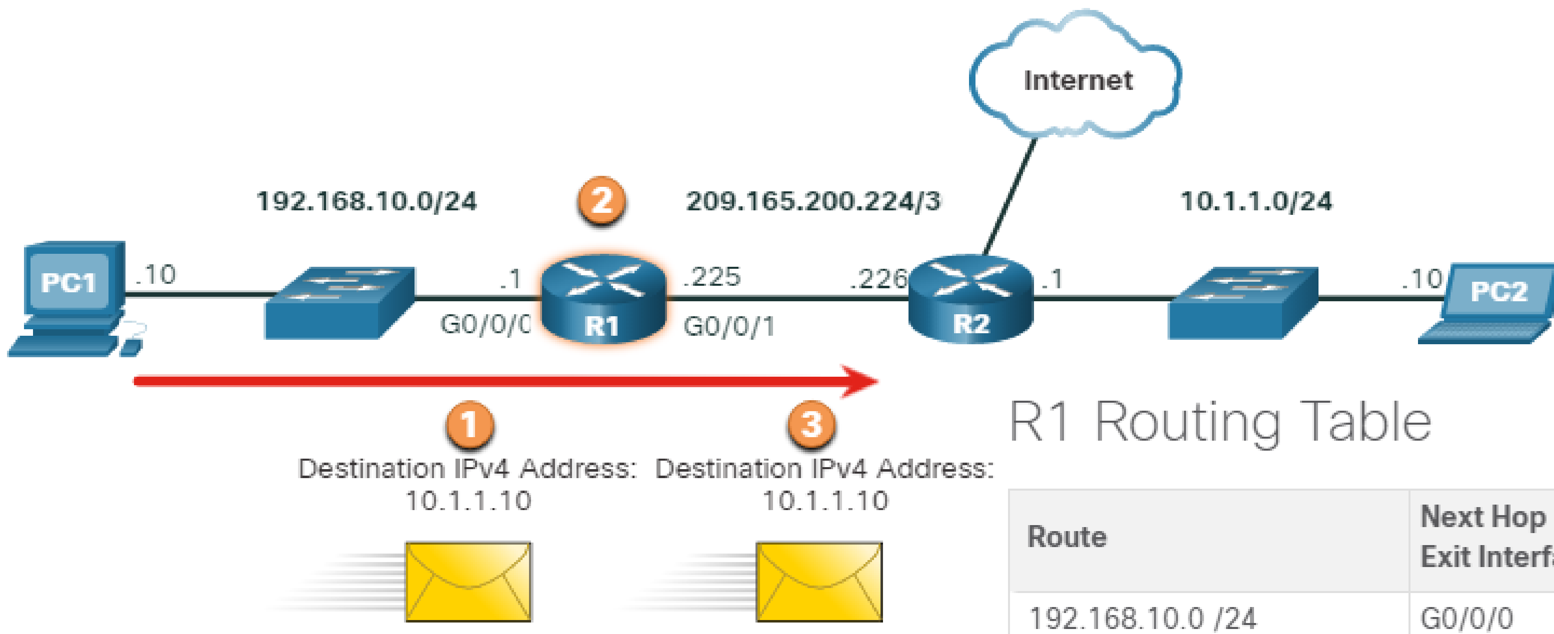
1. Consult the IPv4 Route Table.
2. Find that there is no exact match for the destination IP address.
3. Choose the local default route (0.0.0.0) to reveal that it should forward the packet to the 192.168.10.1 gateway address.
4. PC1 then forwards the packet to the gateway for using its local interface (192.168.10.10). The gateway device then determines the next path for the packet to reach the final destination address of 10.10.10.10.

Router Packet Forwarding Decision

What happens when a packet arrives on a router interface?

- The router examines the destination IP address of the packet and searches its routing table to determine where to forward the packet.
- The routing table contains a list of all known network addresses (prefixes) and where to forward the packet.
- These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry.

Router Packet Forwarding Decision



R1 Routing Table

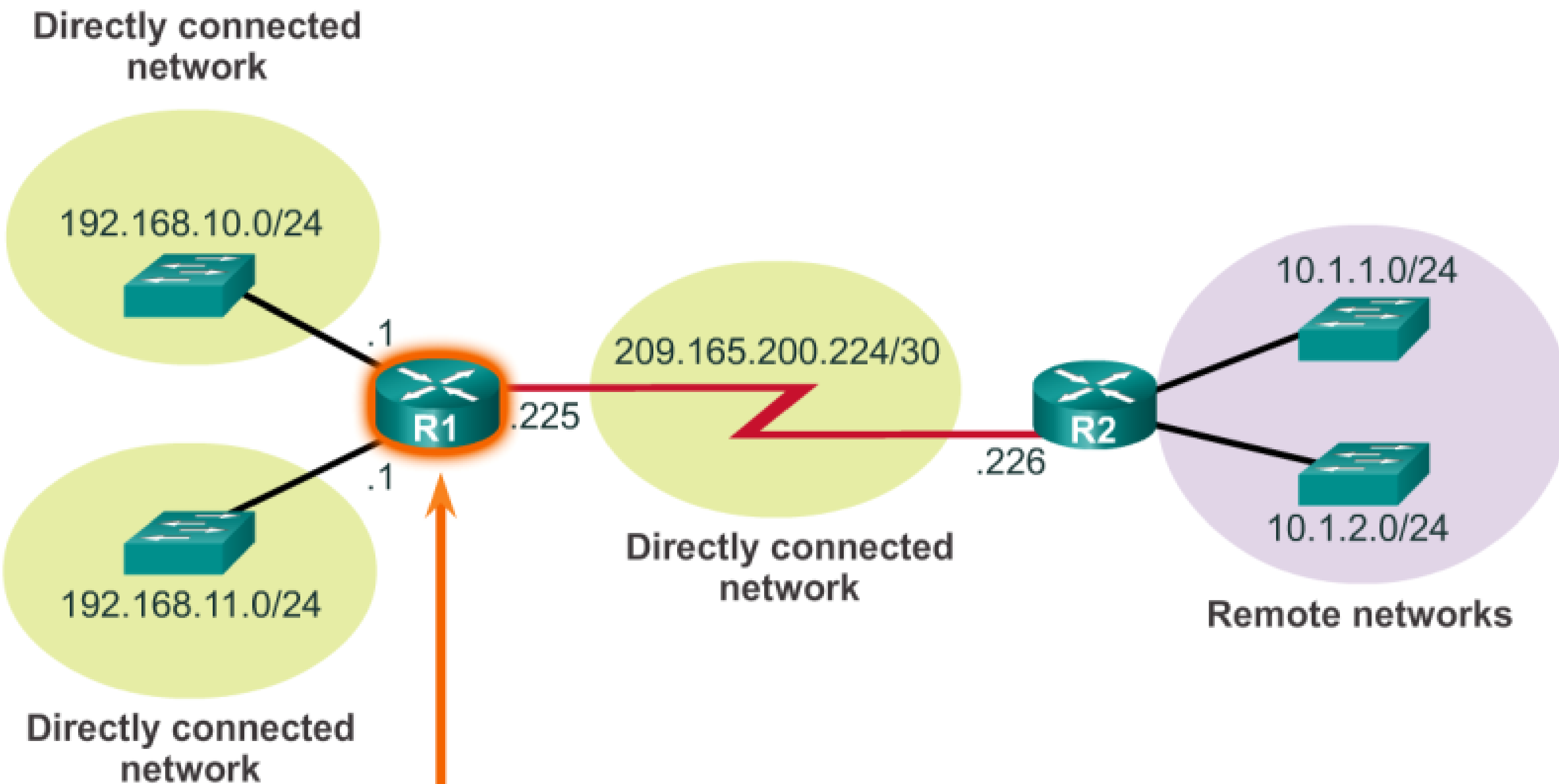
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2

1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-e trailer.
2. Router R1 examines the destination IPv4 address of the packet and searche The route entry indicates that this packet is to be forwarded to router R2.
3. Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

Router Routing Tables

- The routing table stores three types of route entries:
- **Directly-connected networks -** These network route entries are active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated. Each router interface is connected to a different network segment.
- **Remote networks -** These network route entries are connected to other routers. Routers learn about remote networks either by being explicitly configured by an administrator or by exchanging route information using a dynamic routing protocol.
- **Default route** – Like a host, most routers also include a default route entry, a ***gateway of last resort***. The default route is used when there is no better (longer) match in the IP routing table.

Router Routing Tables



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

- The **show ip route** command is used to view the IPv4 routing table on a Cisco IOS router.
- At the beginning of each routing table entry is a code that is used to identify the type of route or how the route was learned.
- Common route sources (codes) include these:

  L – Directly connected local interface IP address

  C – Directly connected network

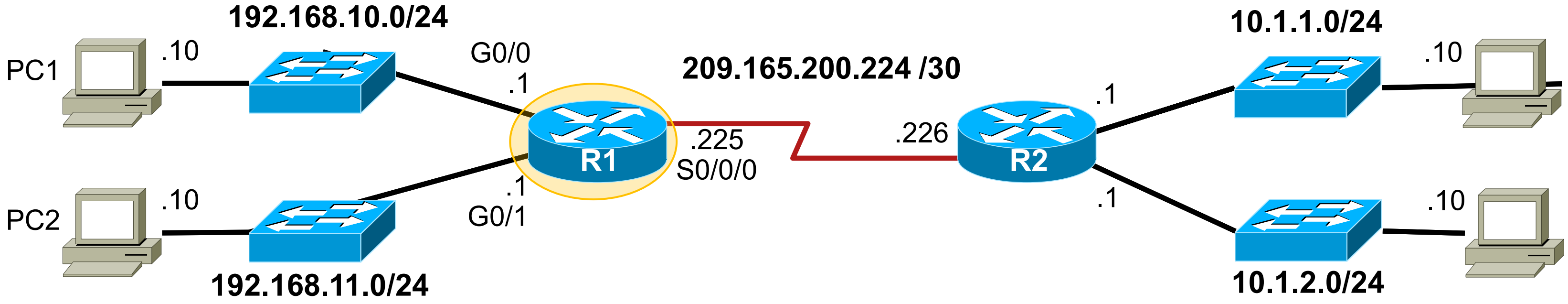
  S – Static route was manually configured by an administrator

  O – OSPF

  D – EIGRP

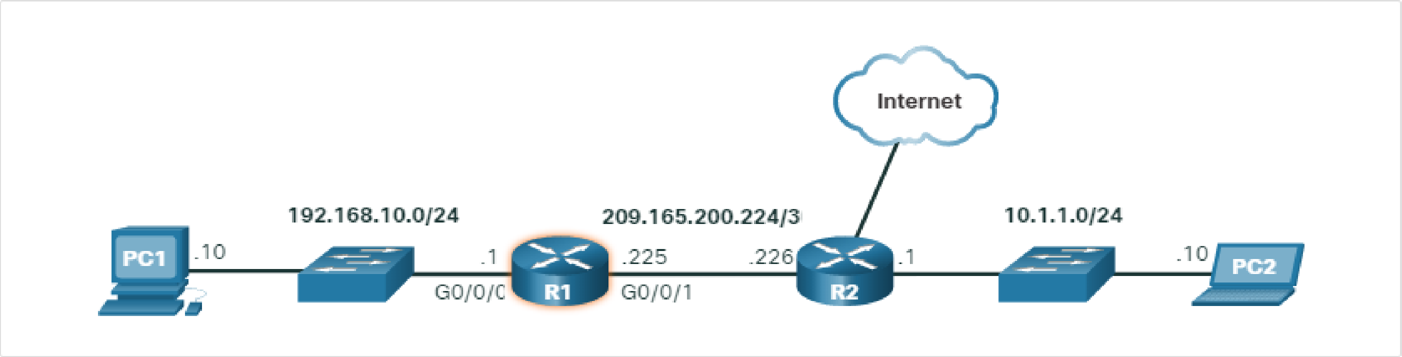
Router Routing Tables

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#
```

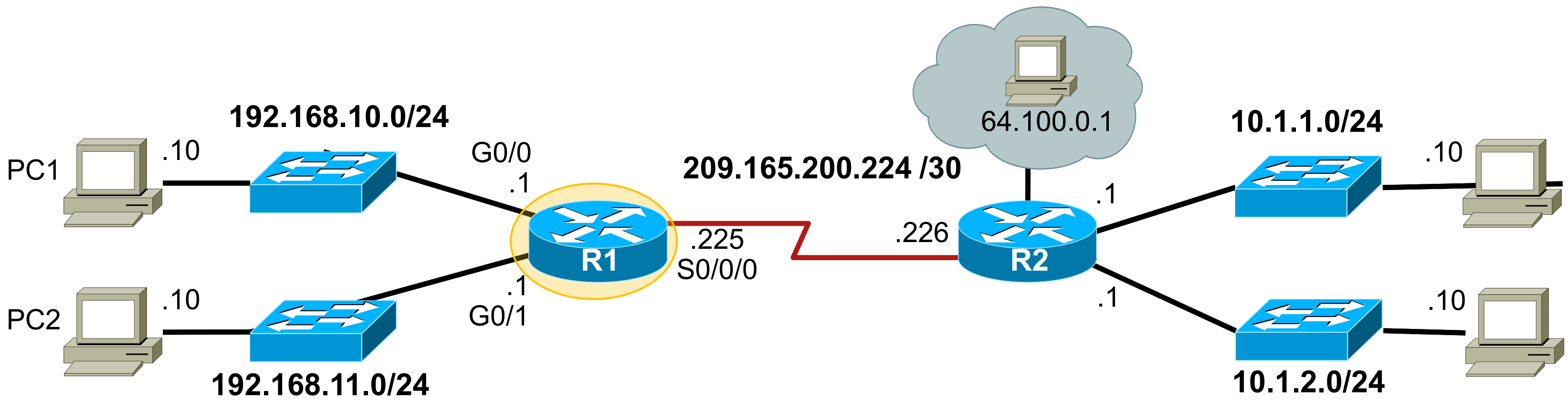
IPv4 Router Routing Table




```
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
       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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

Router Routing Tables

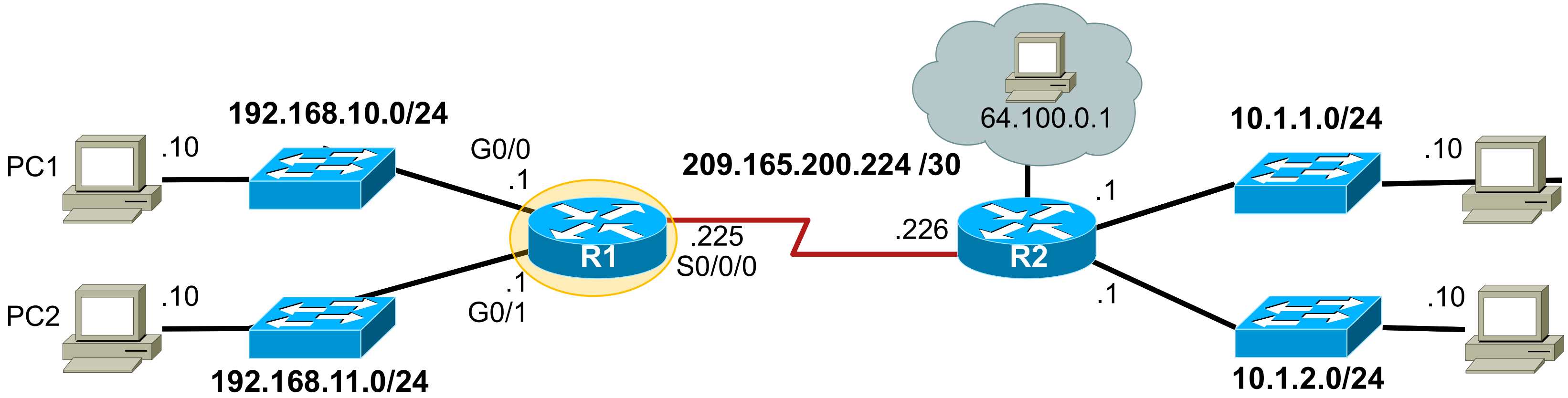
Directly Connected Routing Table Entries



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.

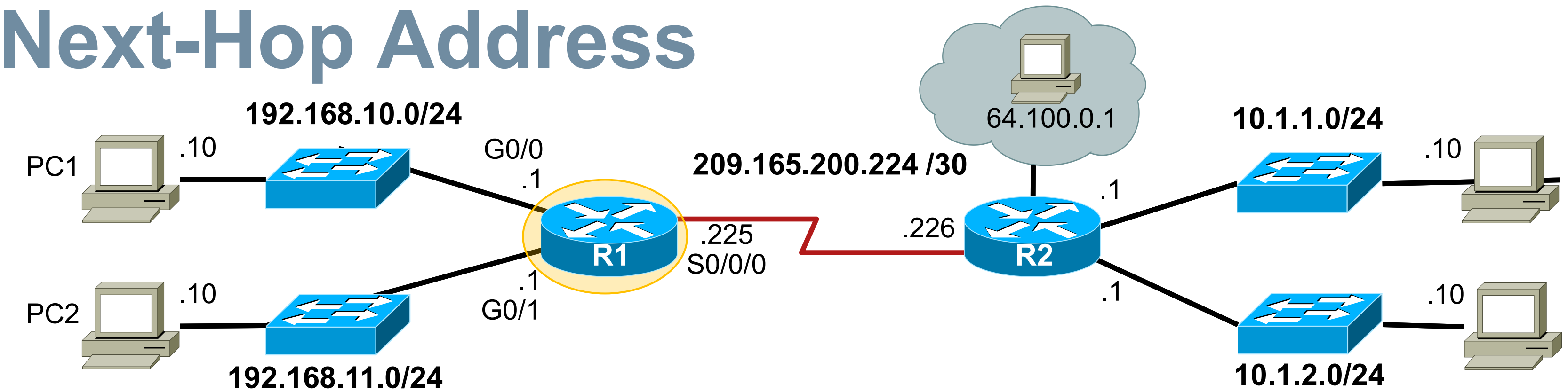
Remote Network Routing Table Entries




```
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.

Next-Hop Address




```
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#
```

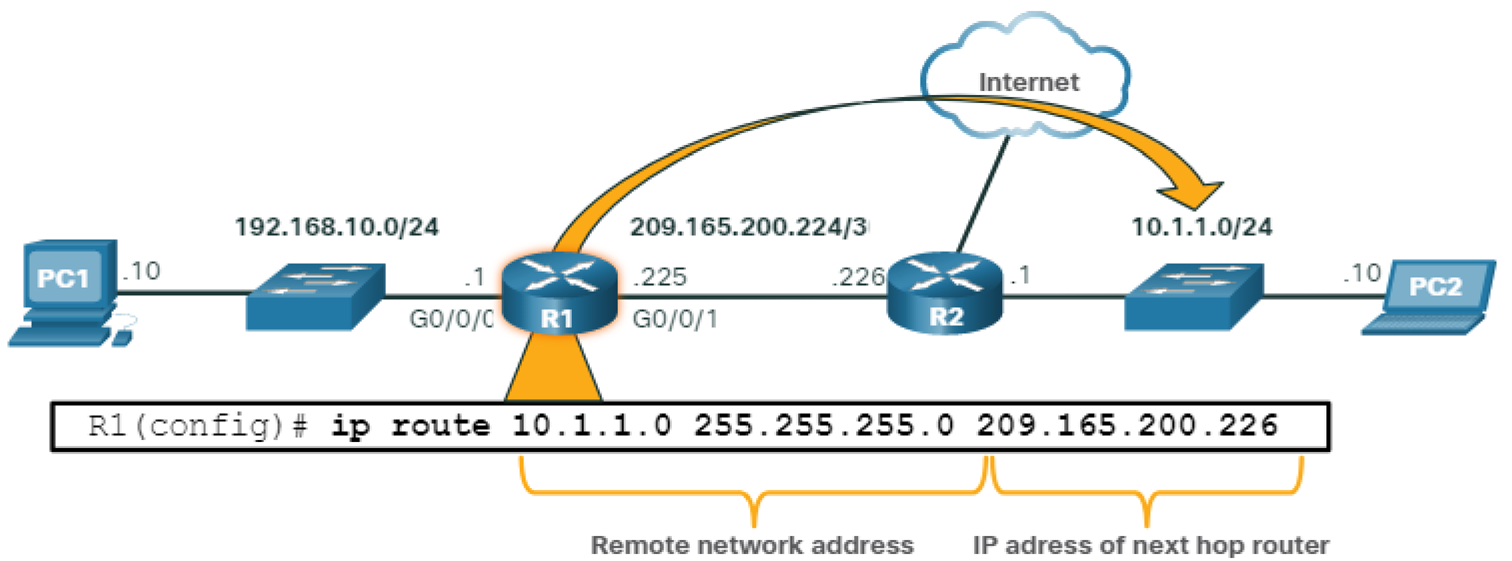
IPv4 Router Routing Tables

A router can learn about remote networks in one of two ways:

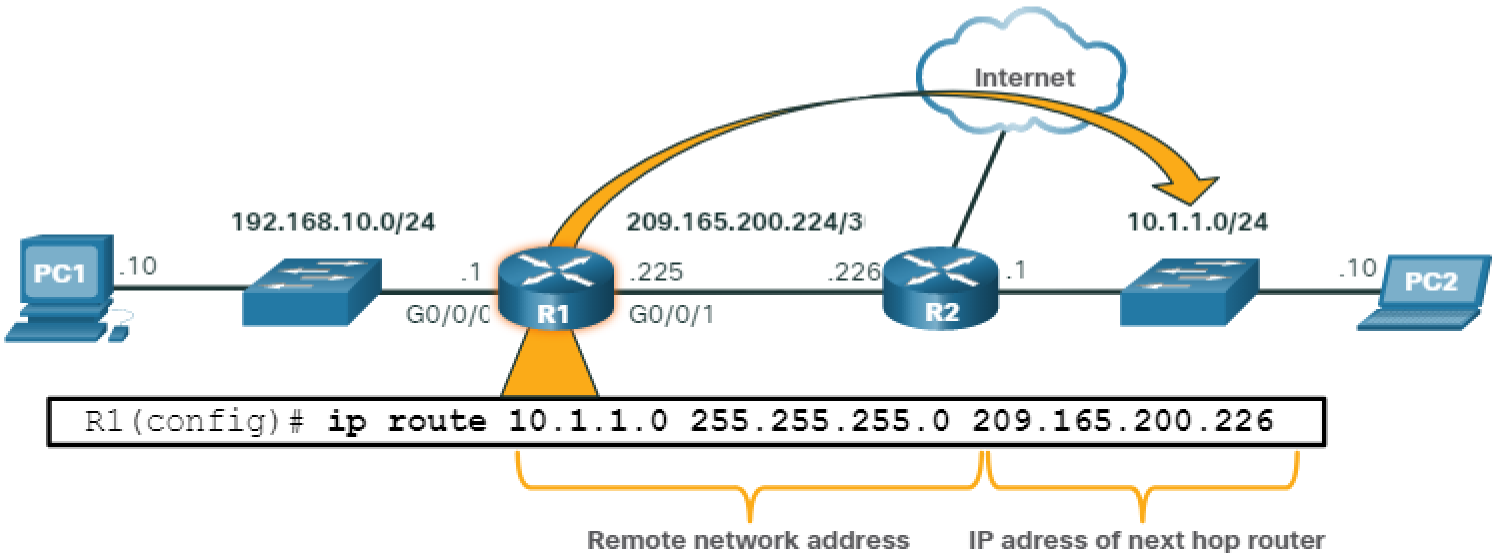
- **Manually** - Remote networks are manually entered into the route table using static routes.
- **Dynamically** - Remote routes are automatically learned using a dynamic routing protocol.

Router Routing Tables
Static Routing

- Static routes are route entries that are manually configured.
- The figure shows an example of a static route that was manually configured on router R1.
- The static route includes the remote network address and the IP address of the next hop router.

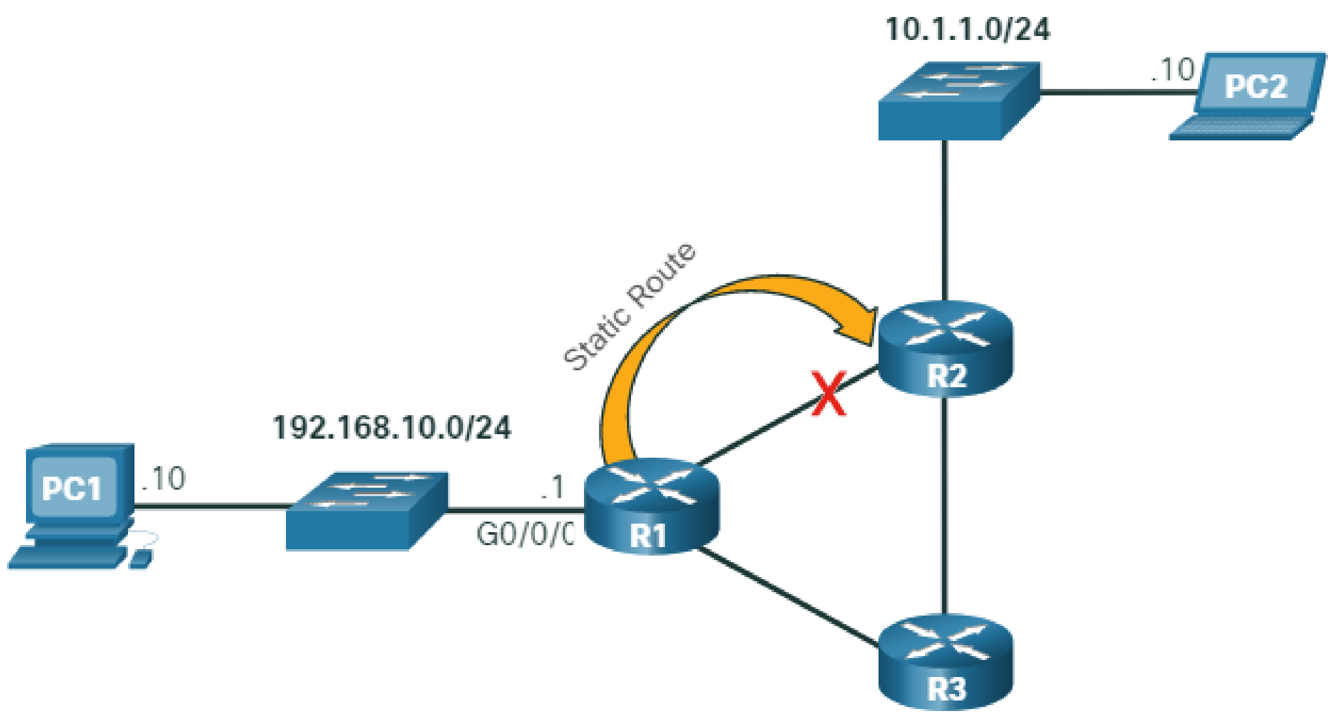


Router Routing Tables
Static Routing



- If there is a change in the network topology, the static route is not automatically updated and must be manually reconfigured.
- R1 has a static route to reach the 10.1.1.0/24 network via R2.
- If that path is no longer available, R1 would need to be reconfigured with a new static route to the 10.1.1.0/24 network via another router.

Static Routing



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

Static Routing

Static routing has the following characteristics:

- A static route must be configured manually.
- The administrator needs to reconfigure a static route if there is a change in the topology and the static route is no longer viable.
- A static route is appropriate for a small network and when there are few or no redundant links.
- A static route is commonly used with a dynamic routing protocol for configuring a default route.

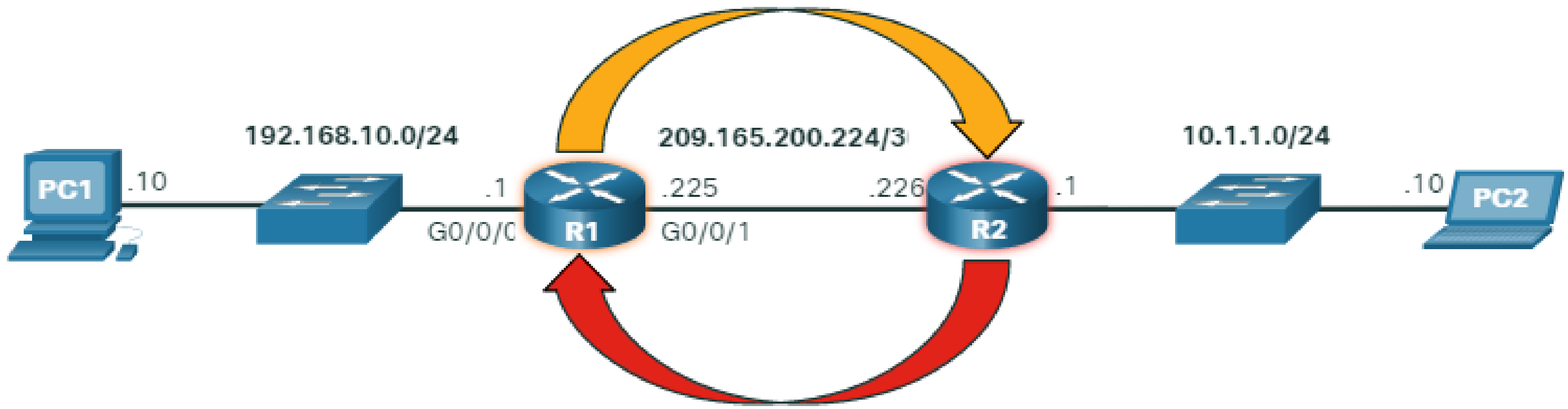
Dynamic Routing

- A dynamic routing protocol allows the routers to automatically learn about remote networks, including a default route, from other routers.
- Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the network administrator.
- If there is a change in the network topology, routers share this information using the dynamic routing protocol and automatically update their routing tables.
- Dynamic routing protocols include OSPF and Enhanced Interior Gateway Routing Protocol (EIGRP).

Router Routing Tables

Dynamic Routing

The figure shows an example of routers R1 and R2 automatically sharing network information using the routing protocol OSPF.



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.

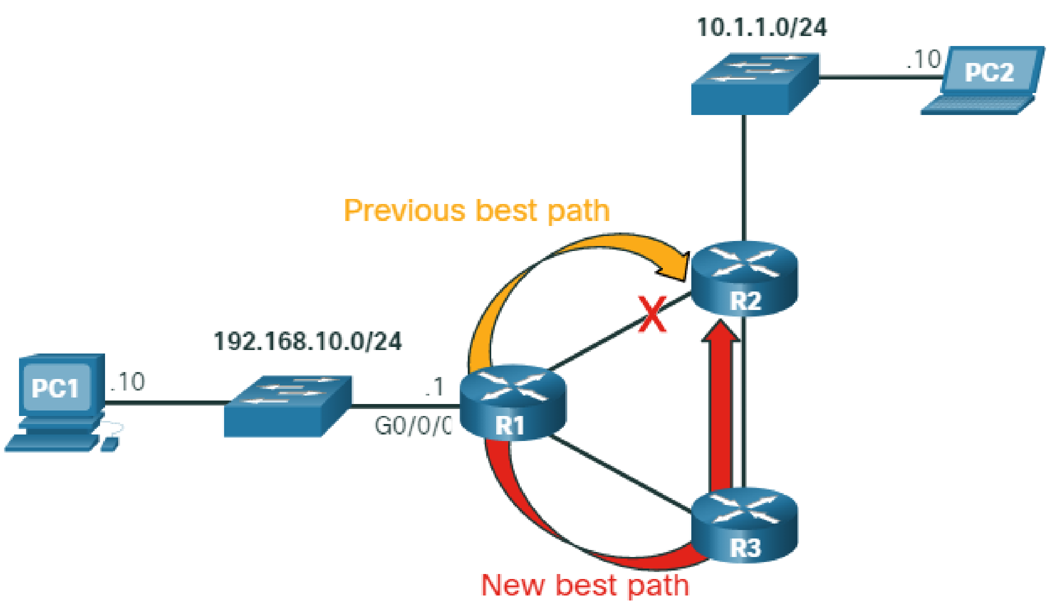
Router Routing Tables

Dynamic Routing

- Basic configuration only requires the network administrator to enable the directly connected networks within the dynamic routing protocol.
- The dynamic routing protocol will automatically do as follows:
  - Discover remote networks
  - Maintain up-to-date routing information
  - Choose the best path to destination networks
  - Attempt to find a new best path if the current path is no longer available

Dynamic Routing

- As shown in the figure, if there is a change in the network topology, the routers will automatically adjust and attempt to find a new best path.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

6.3 Routers

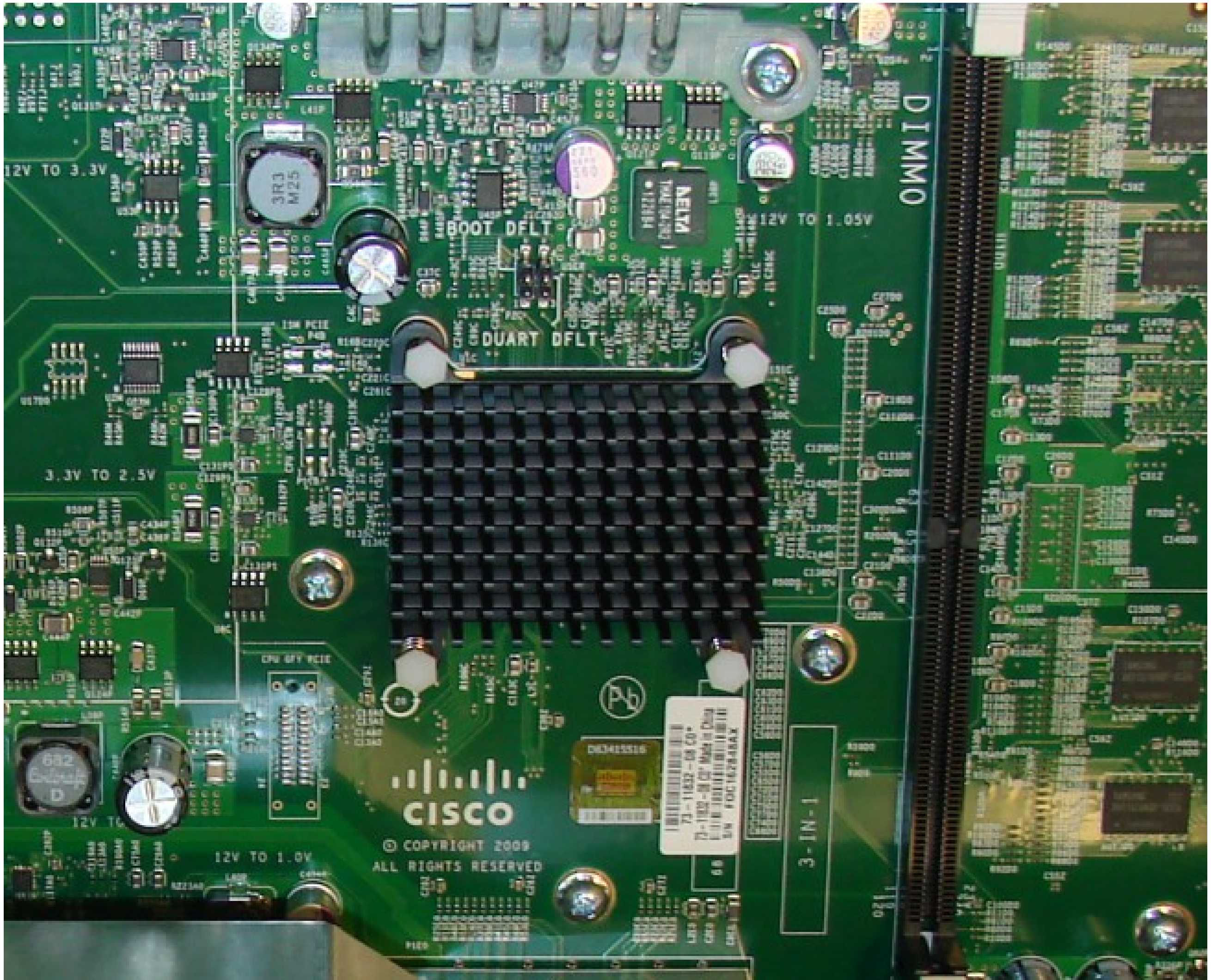
Cisco | Networking Academy®
Mind Wide Open™

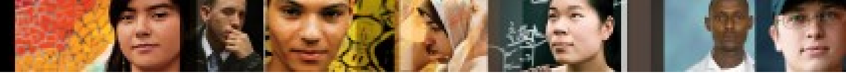
Anatomy of a Router

A Router is a Computer

Anatomy of a Router

Router CPU and OS



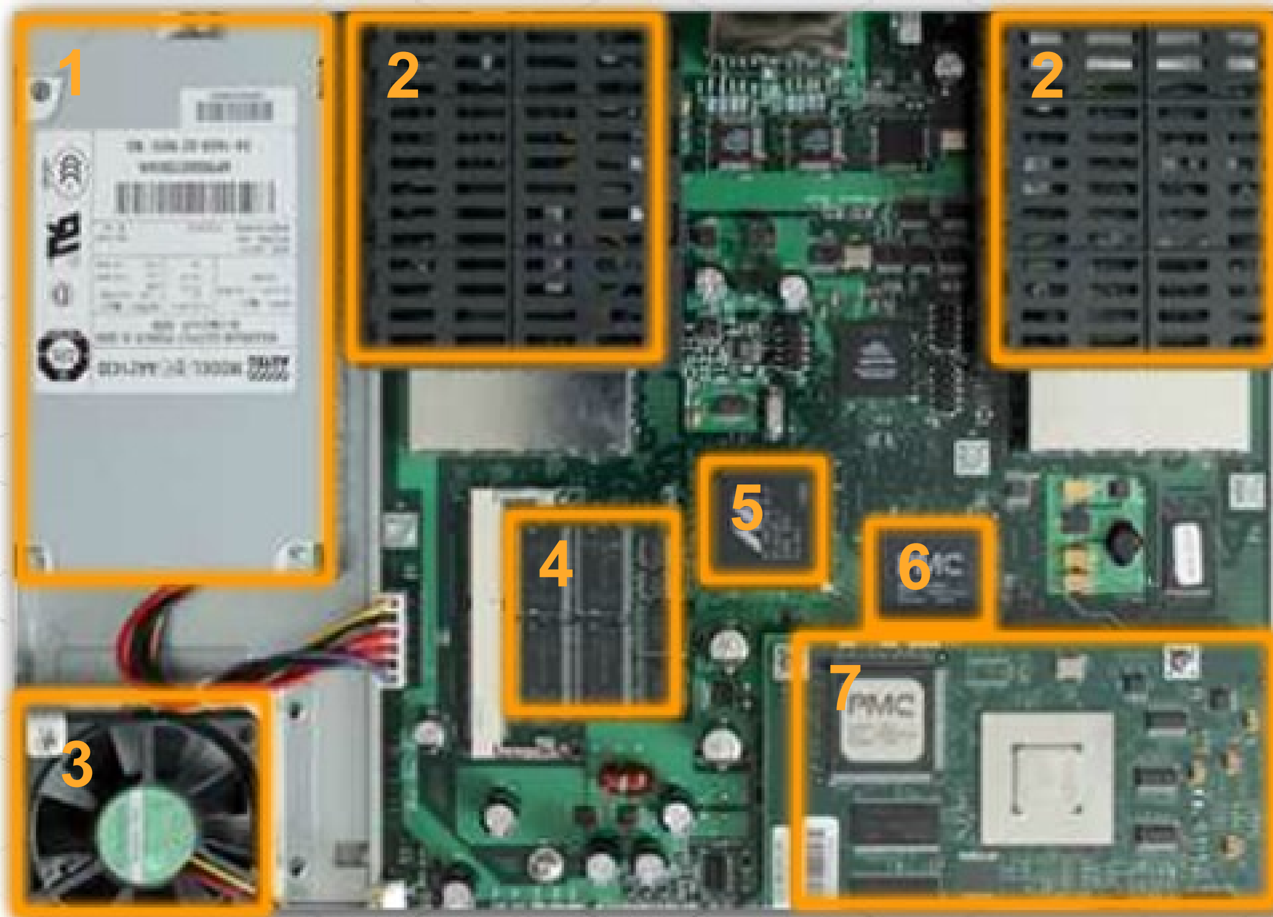


Router Memory

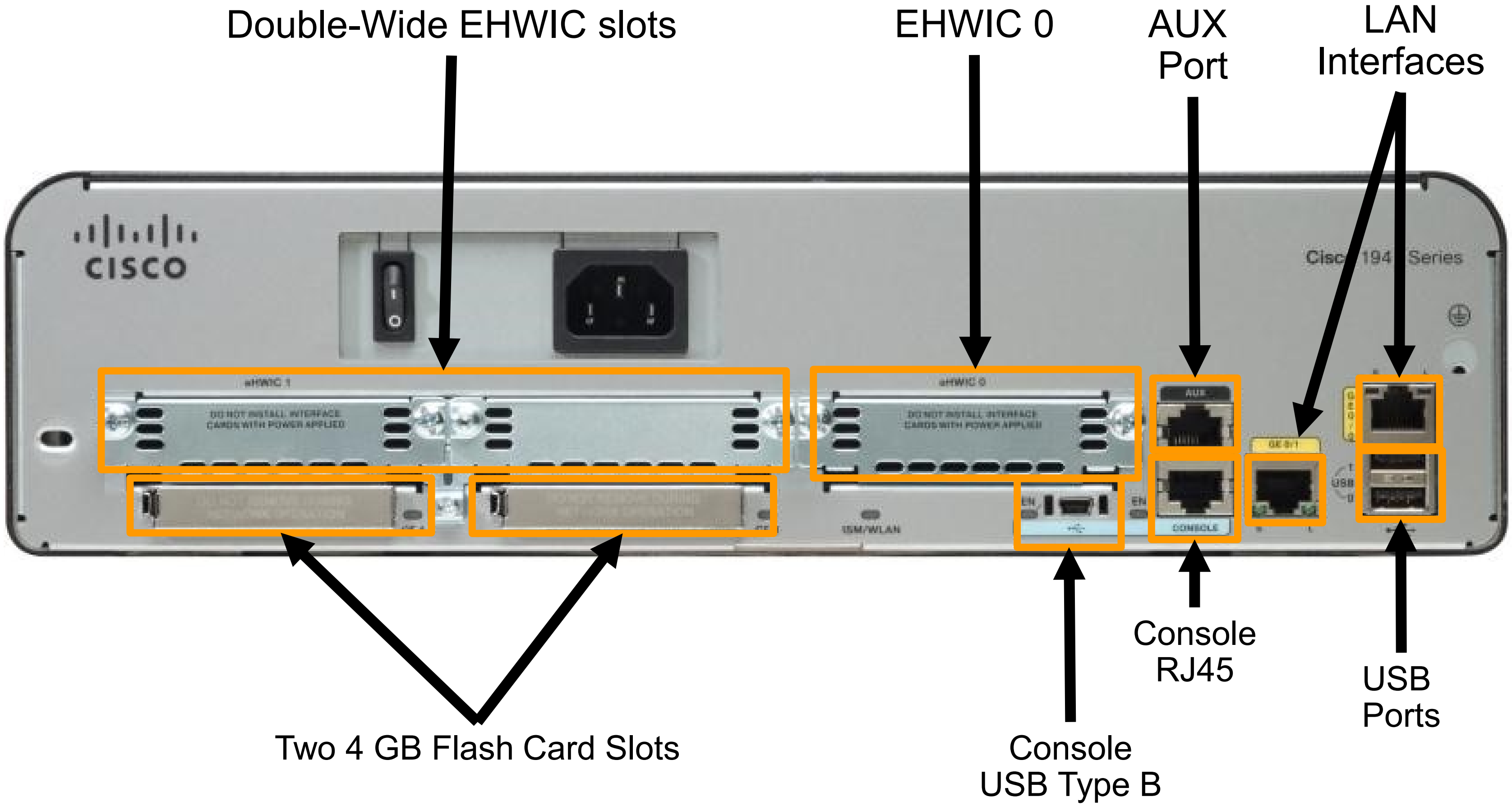
Memory	Volatile / Non-Volatile	Stores
RAM	Volatile	• Running IOS • Running configuration file • IP routing and ARP tables • Packet buffer
ROM	Non-Volatile	• Bootup instructions • Basic diagnostic software • Limited IOS
NVRAM	Non-Volatile	• Startup configuration file
Flash	Non-Volatile	• IOS • Other system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

Inside a Router

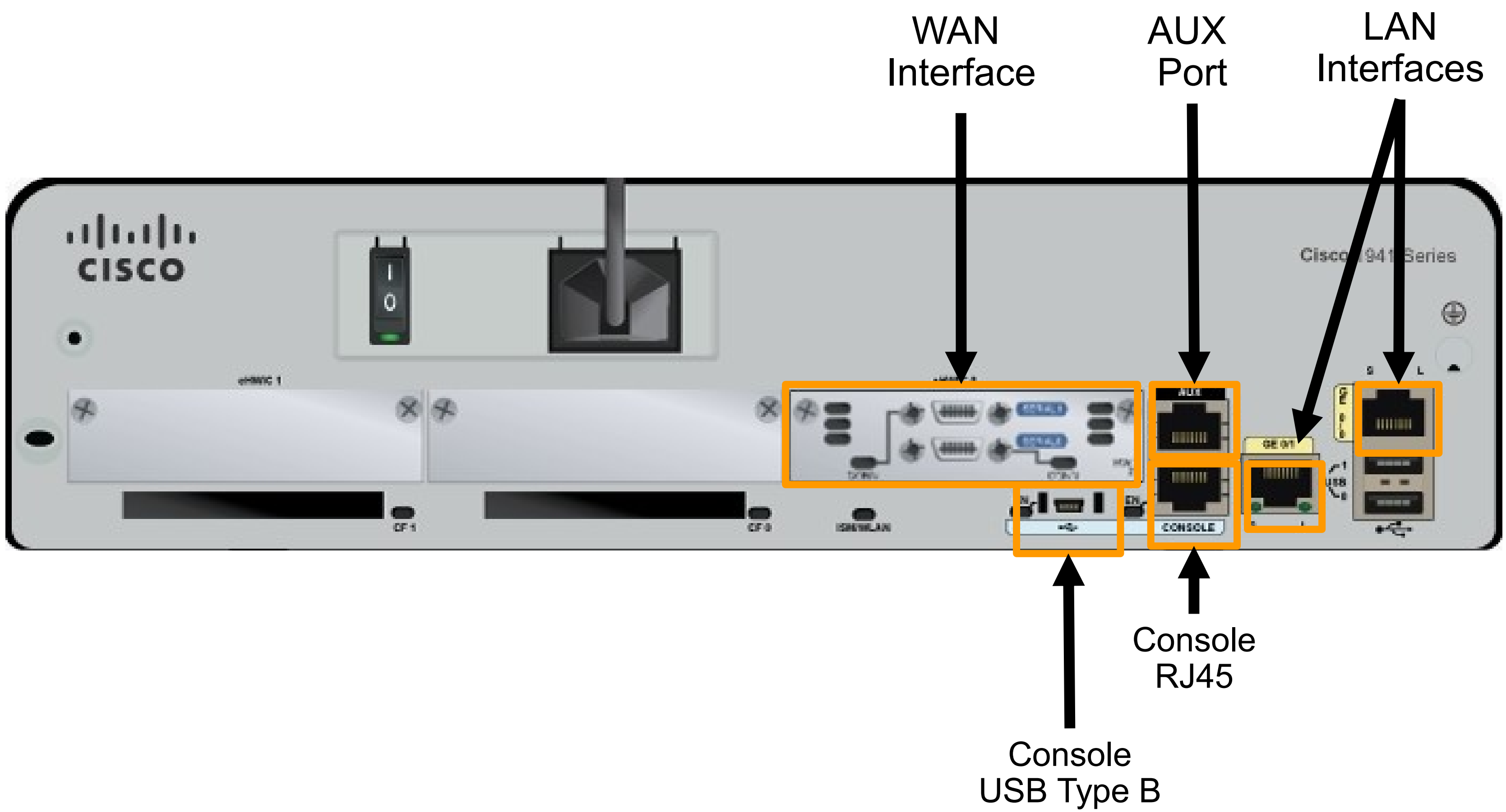
1. Power Supply
2. Shield for WIC
3. Fan
4. SDRAM
5. NVRAM
6. CPU
7. Advanced Integration Module (AIM)



Router Backplane

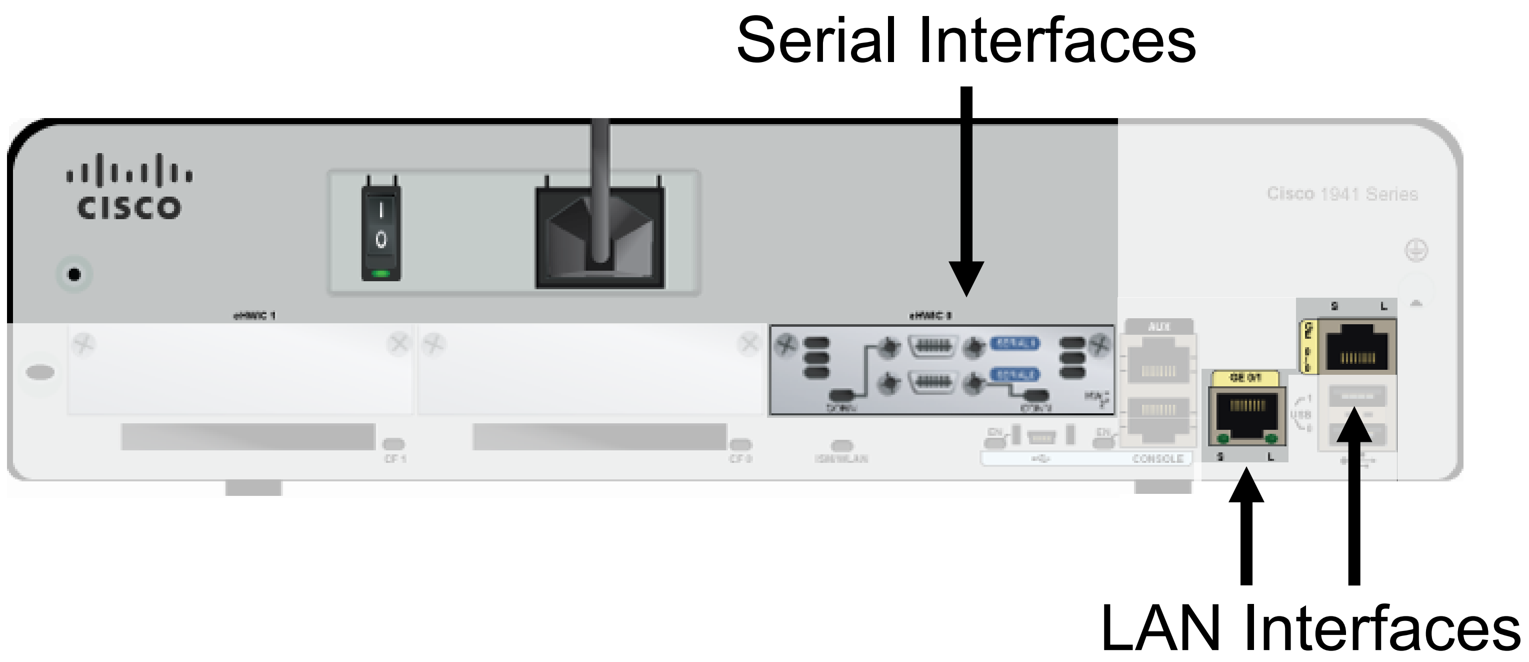


Connecting to a Router



Anatomy of a Router

LAN and WAN Interfaces



Router Boot-up

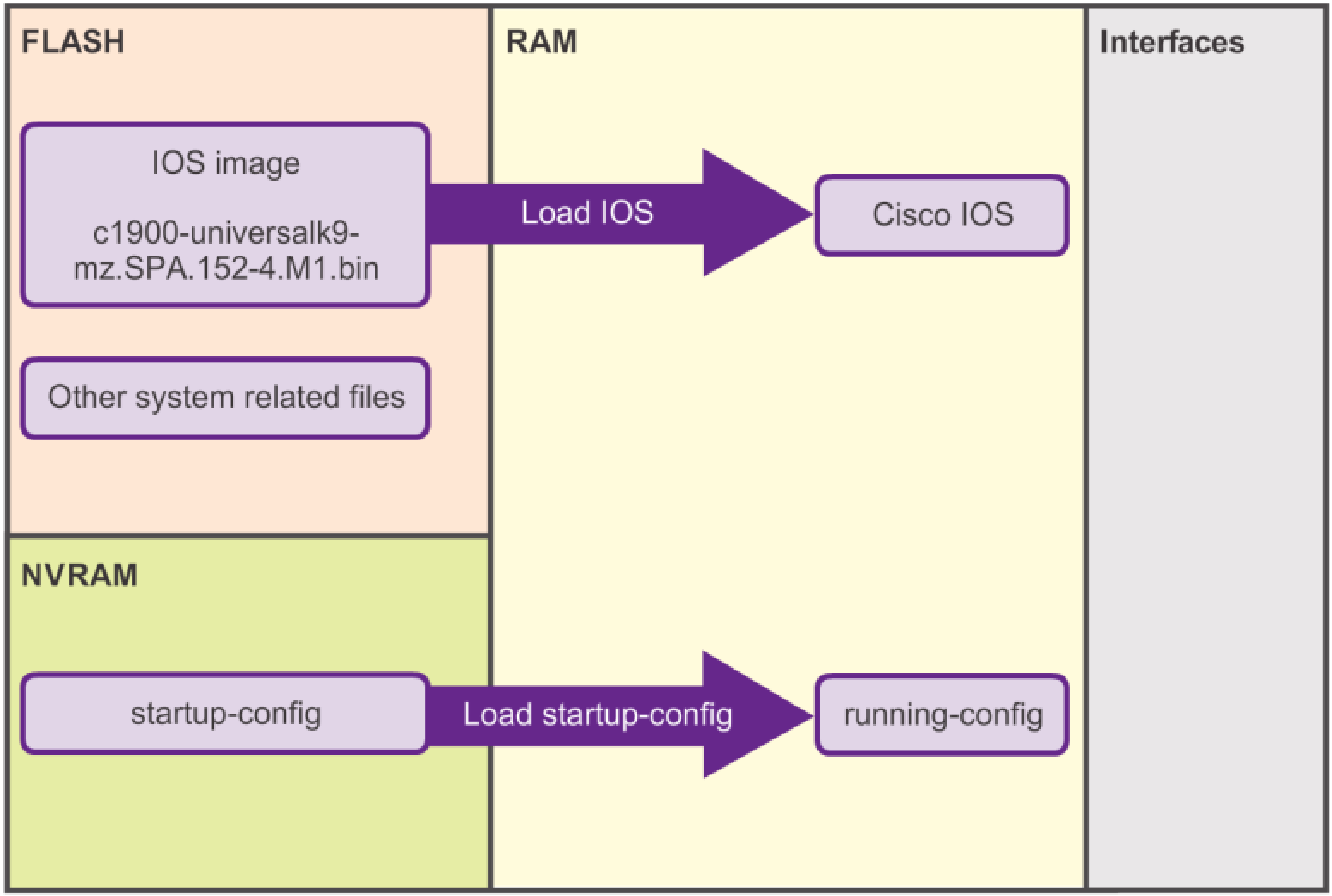
Cisco IOS

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

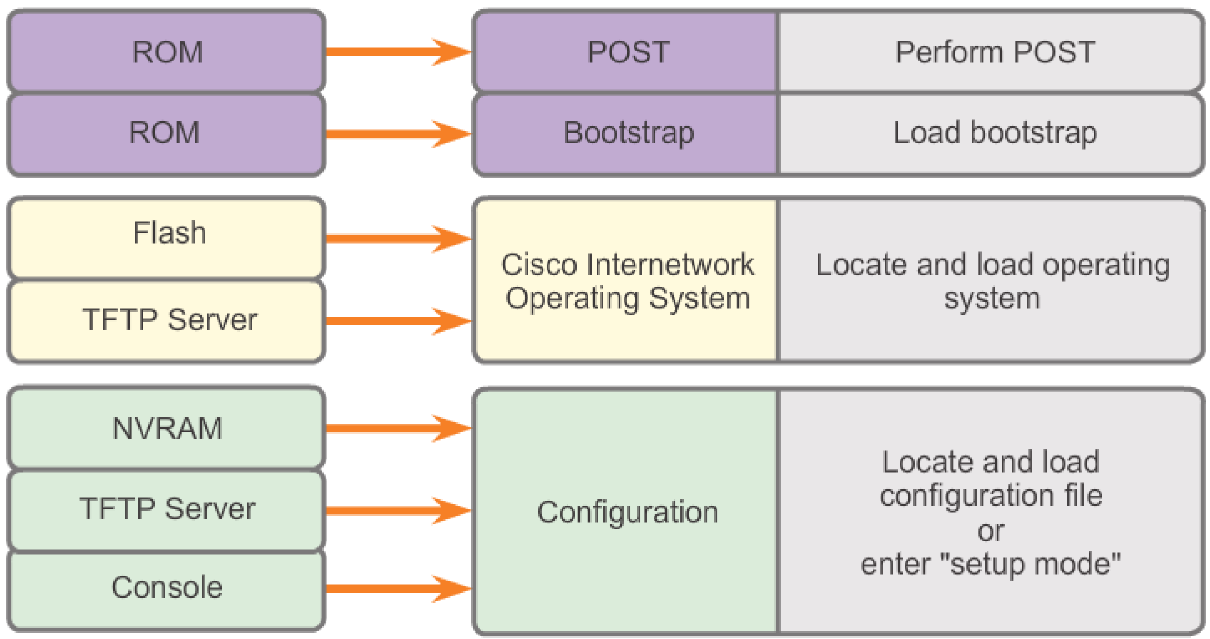
Bootset Files



Router Boot-up

Router Bootup Process

How a Router Boots Up




```
System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport


<output omitted>
```

Router Boot-up
Show Versions Output

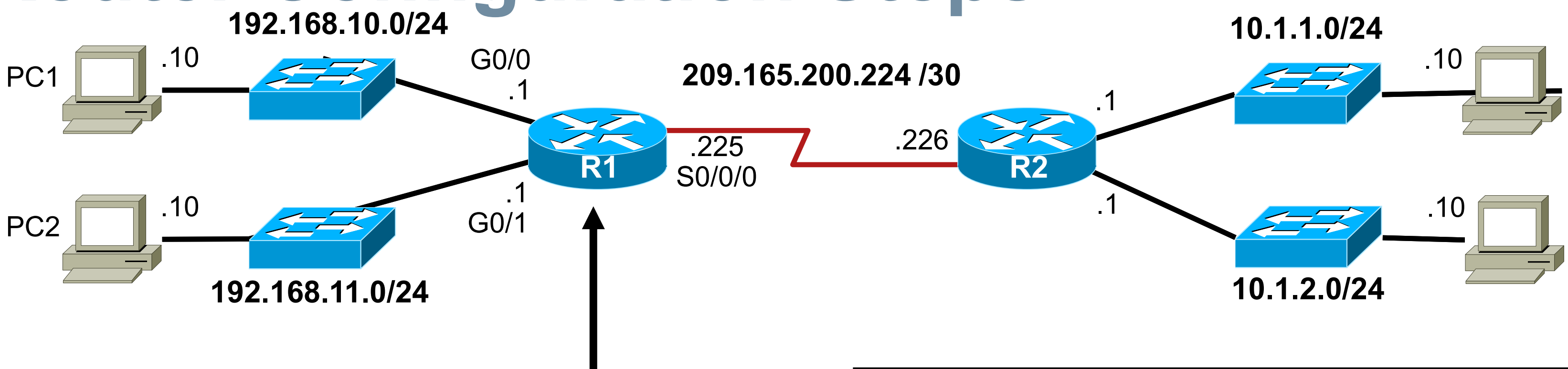
```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on

<Output omitted>

Cisco CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

<Output omitted>

Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      None          None           None
data          None          None           None

Configuration register is 0x2142 (will be 0x2102 at next reload)

Router#
```

6.4 Configuring a Cisco Router

Cisco | Networking Academy®
Mind Wide Open™

Configure Initial Settings

Router Configuration Steps




```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

OR

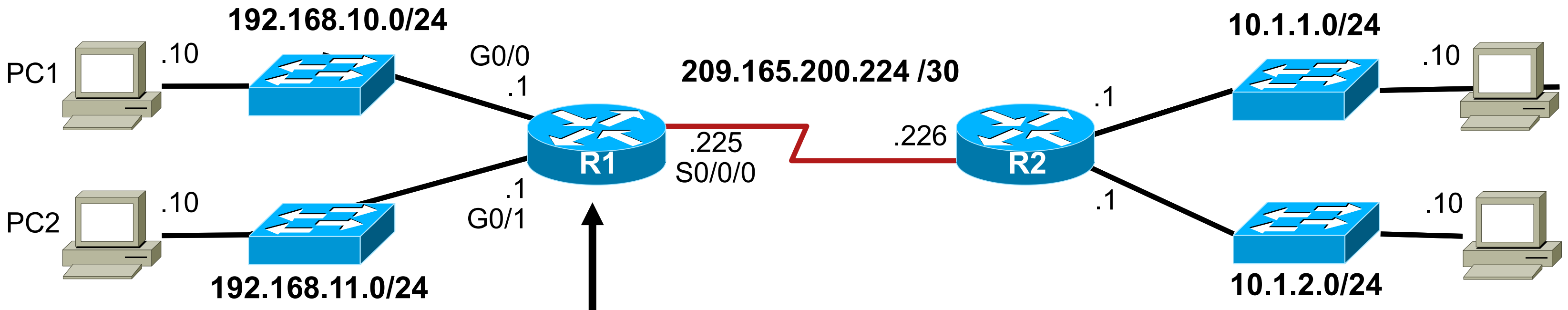
```
Router> en
Router# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# ho R1
R2(config)#
```

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

```
R1(config)# banner motd #
Enter TEXT message.  End with the character '#'.
    ***********************************************
      WARNING: Unauthorized access is prohibited!
    ***********************************************
#

R1(config)#
```

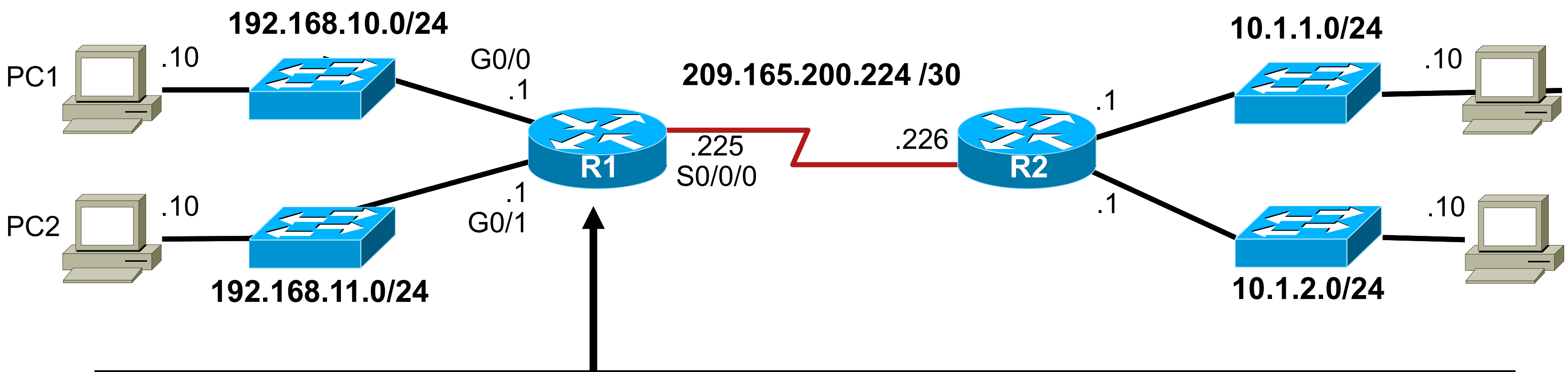
```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Configure LAN Interfaces




```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# exit
R1(config)#
R1(config)# int g0/1
R1(config-if)# ip add 192.168.11.1 255.255.255.0
R1(config-if)# des Link to LAN-11
R1(config-if)# no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)# exit
R1(config)#
```

Verify Interface Configuration

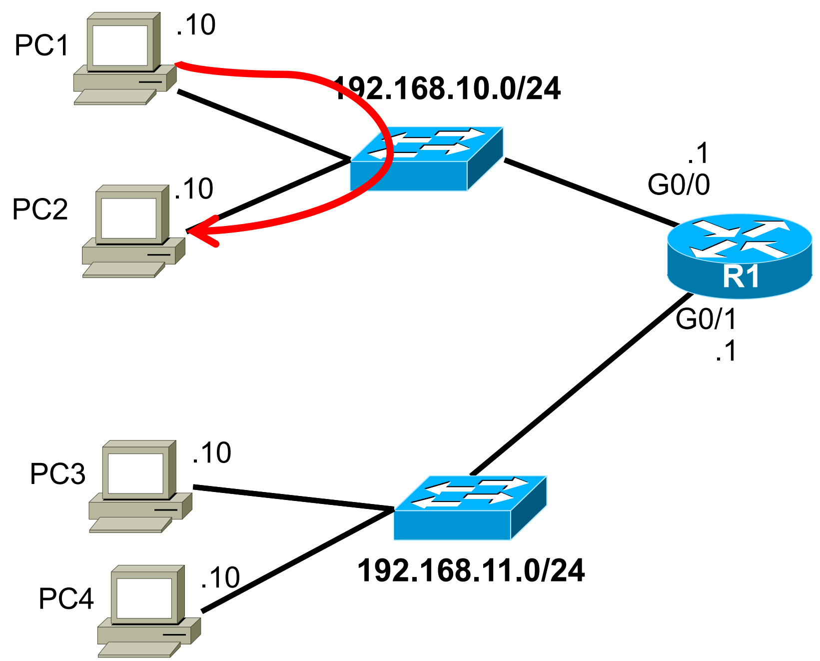



```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     192.168.11.1    YES manual up                    up
Serial0/0/0            209.165.200.225 YES manual up                    up
Serial0/0/1            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

R1#
```

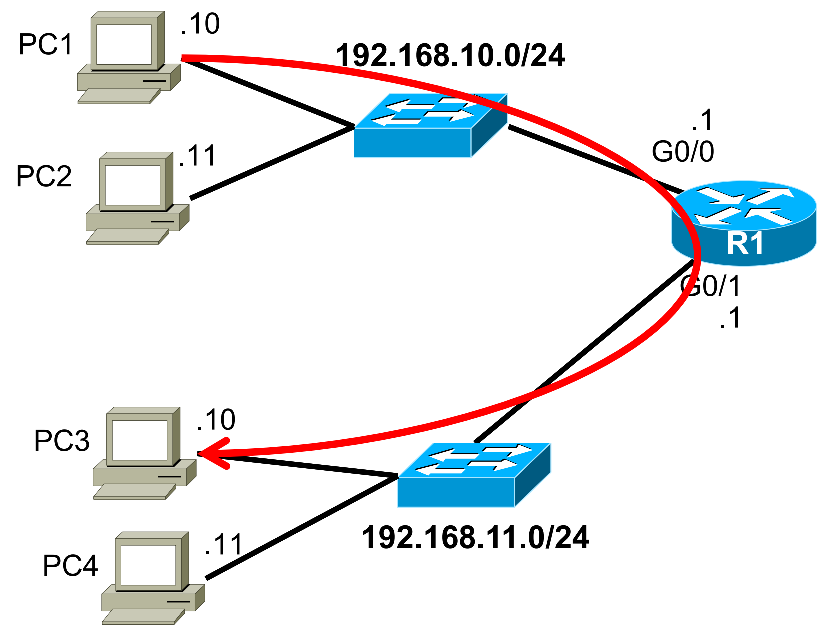
Configuring the Default Gateway

Default Gateway on a Host

Default Gateway
not needed

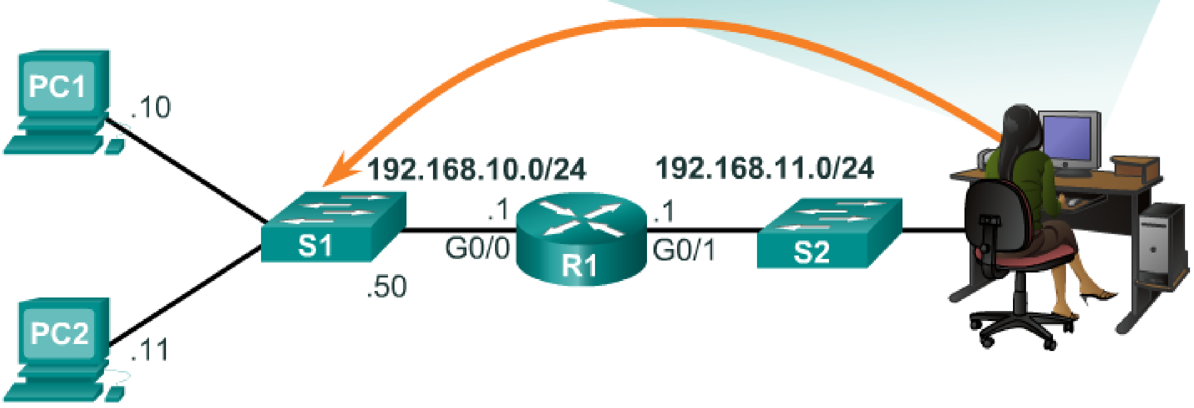


Default Gateway
needed



Default Gateway on a Switch

```
S1# show running-config
Building configuration...
!
<output omitted>
service password-encryption
!
hostname S1
!
Interface Vlan1
ip address 192.168.10.50
!
ip default-gateway 192.168.10.1
<output omitted>
```



If the default gateway was not configured on S1, response packets from S1 would not be able to reach the administrator at 192.168.11.10. The administrator would not be able to manage the device remotely.

Network Layer
Summary

In this chapter, you learned:

- The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across the network.
- The network layer uses four basic processes: IP addressing for end devices, encapsulation, routing, and de-encapsulation.
- The Internet is largely based on IPv4, which is still the most widely-used network layer protocol.
- An IPv4 packet contains the IP header and the payload.
- The IPv6 simplified header offers several advantages over IPv4, including better routing efficiency, simplified extension headers, and capability for per-flow processing.

Summary (cont.)

- In addition to hierarchical addressing, the network layer is also responsible for routing.
- Hosts require a local routing table to ensure that packets are directed to the correct destination network.
- The local default route is the route to the default gateway.
- The default gateway is the IP address of a router interface connected to the local network.
- When a router, such as the default gateway, receives a packet, it examines the destination IP address to determine the destination network.

Network Layer

Summary (cont.)

- The routing table of a router stores information about directly-connected routes and remote routes to IP networks. If the router has an entry in its routing table for the destination network, the router forwards the packet. If no routing entry exists, the router may forward the packet to its own default route, if one is configured or it will drop the packet.
- Routing table entries can be configured manually on each router to provide static routing or the routers may communicate route information dynamically between each other using a routing protocol.
- For routers to be reachable, the router interface must be configured.

Cisco | Networking Academy®
Mind Wide Open™