8.1.1
The Network Layer

The network layer, or OSI Layer 3, provides services to allow end devices to exchange data across networks.

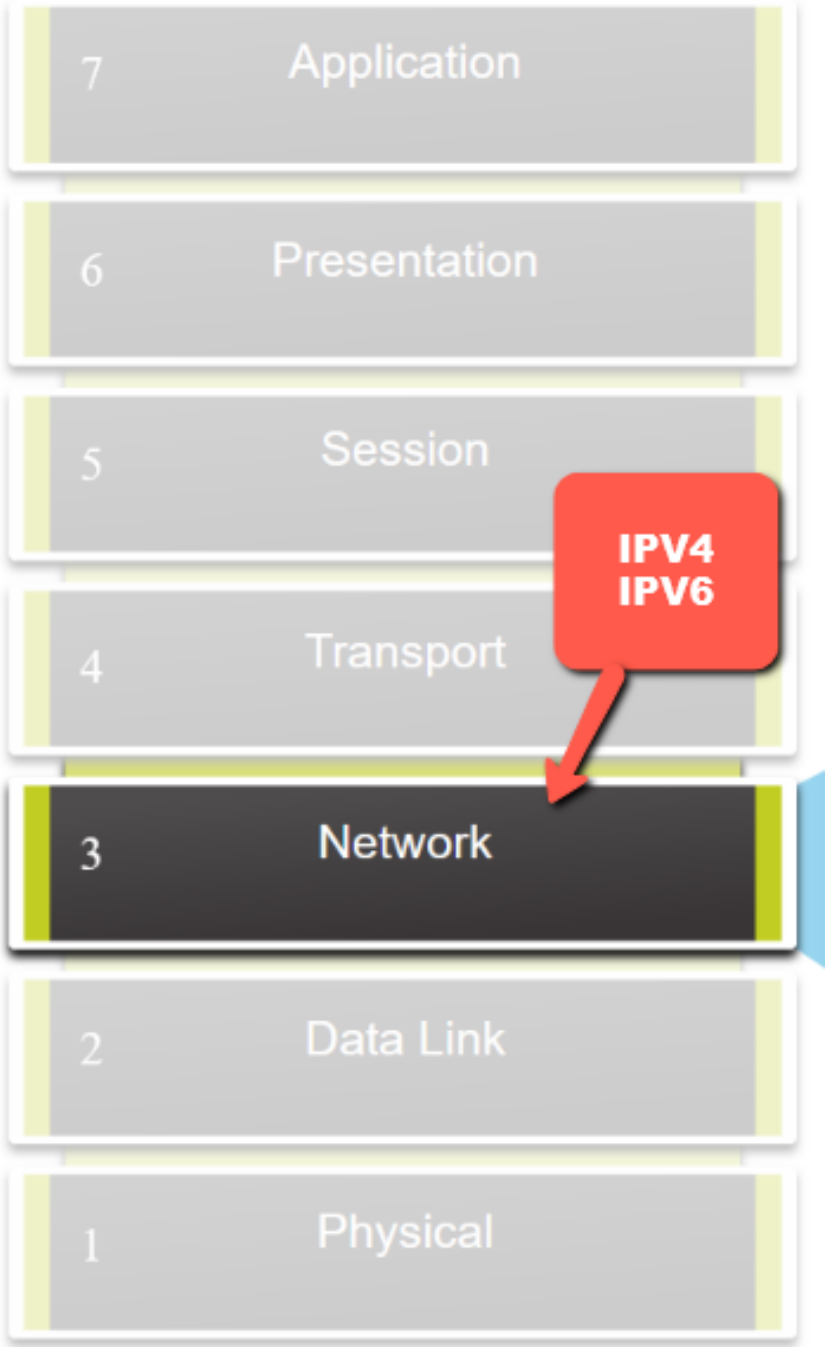
Created by Frank Schneemann, MS EdTech
Bonita Vista H.S.
Southwestern College, Chula Vista CA.
www.edtechnology.com

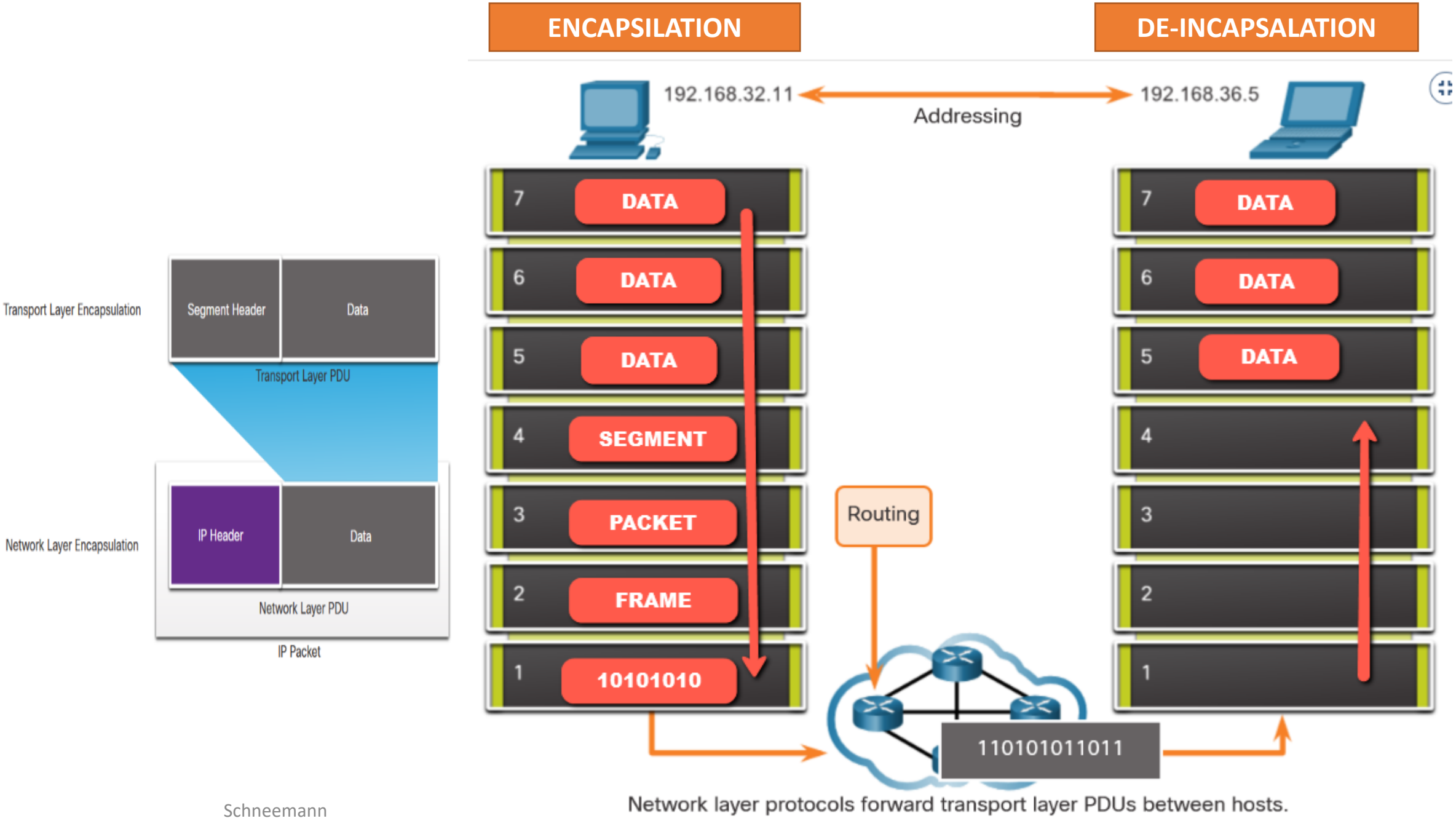
This presentation is in no way intended to substitute for the regular Netacad lessons.
It is only meant to explain parts of the Netacad curriculum that students may need help understanding
The regular Netacad curriculum contains many teaching tools such as Packet Tracers, Quizzes, Video's, reviews, chapter summaries and other concepts not included in these tutorials.

Please avail yourself of the regular Netacad lessons

To accomplish end-to-end communications across network boundaries, network layer protocols perform four basic operations:

- **Addressing** end devices - End devices must be configured with a unique IP address for identification on the network.
- **Encapsulation** - The network layer encapsulates the protocol data unit (PDU) from the transport layer into a packet. The encapsulation process adds IP header information, such as the IP address of the source (sending) and destination (receiving) hosts. The encapsulation process is performed by the source of the IP packet.
- **Routing** - To travel to other networks, the packet must be processed by a router. The role of the router is to select the best path and direct packets toward the destination host in a process known as routing. A packet may cross many routers before reaching the destination host.
- **De-encapsulation** - When the packet arrives at the network layer of the destination host, the host checks the IP header of the packet. If the destination IP address within the header matches its own IP address, the IP header is removed from the packet. After the packet is de-encapsulated by the network layer, the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer. The de-encapsulation process is performed by the destination host of the IP packet.

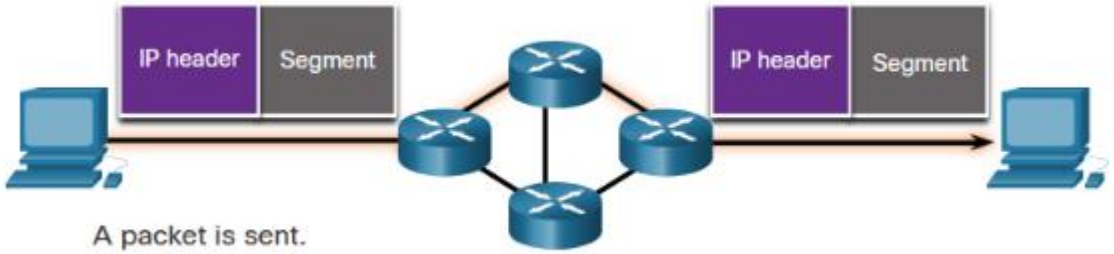



ENCAPSILATION
DE-INCAPSALATION
192.168.32.11
Addressing
192.168.36.5
7 DATA
6 DATA
5 DATA
4 SEGMENT
3 PACKET
2 FRAME
1 10101010
Routing
110101011011
Transport Layer Encapsulation
Segment Header
Data
Transport Layer PDU
Network Layer Encapsulation
IP Header
Data
Network Layer PDU
IP Packet
Network layer protocols forward transport layer PDUs between hosts.

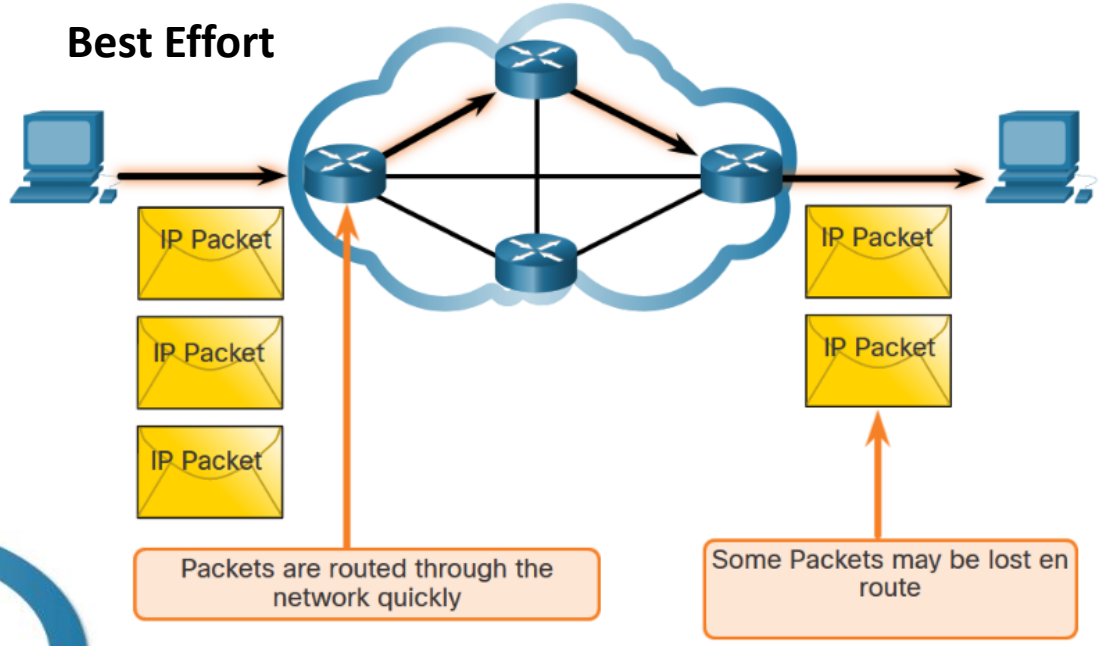
Characteristics of IP

Connectionless - There is no connection with the destination established before sending data packets.
Best Effort - IP is inherently unreliable because packet delivery is not guaranteed.
Media Independent - Operation is independent of the medium (i.e., copper, fiber-optic, or wireless) carrying the data.

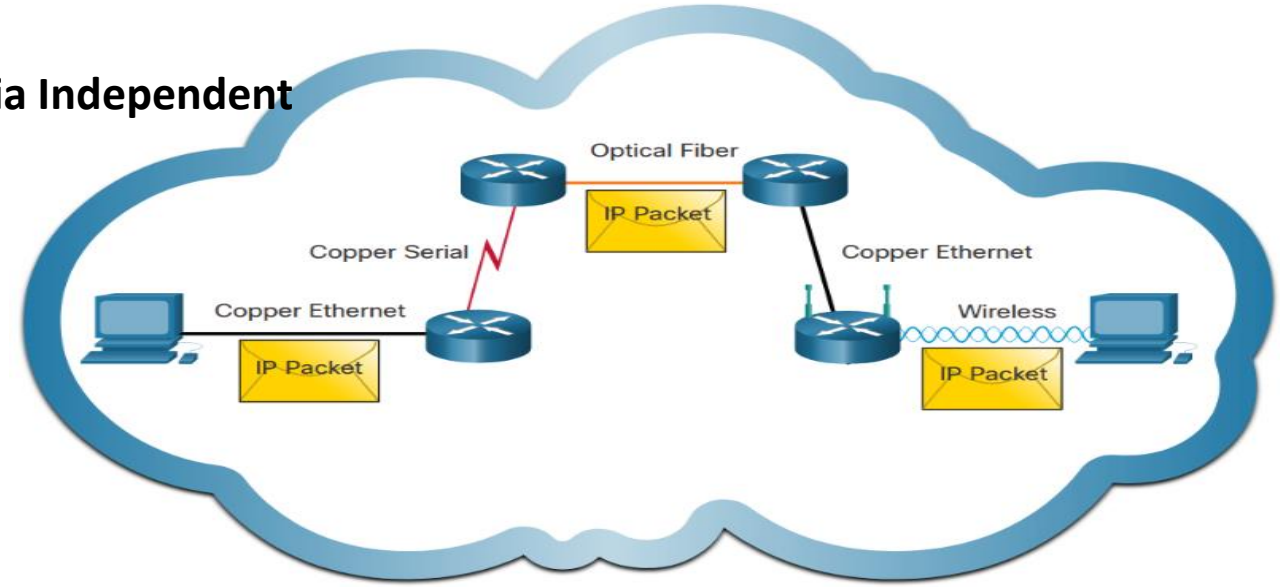
Connectionless - Network



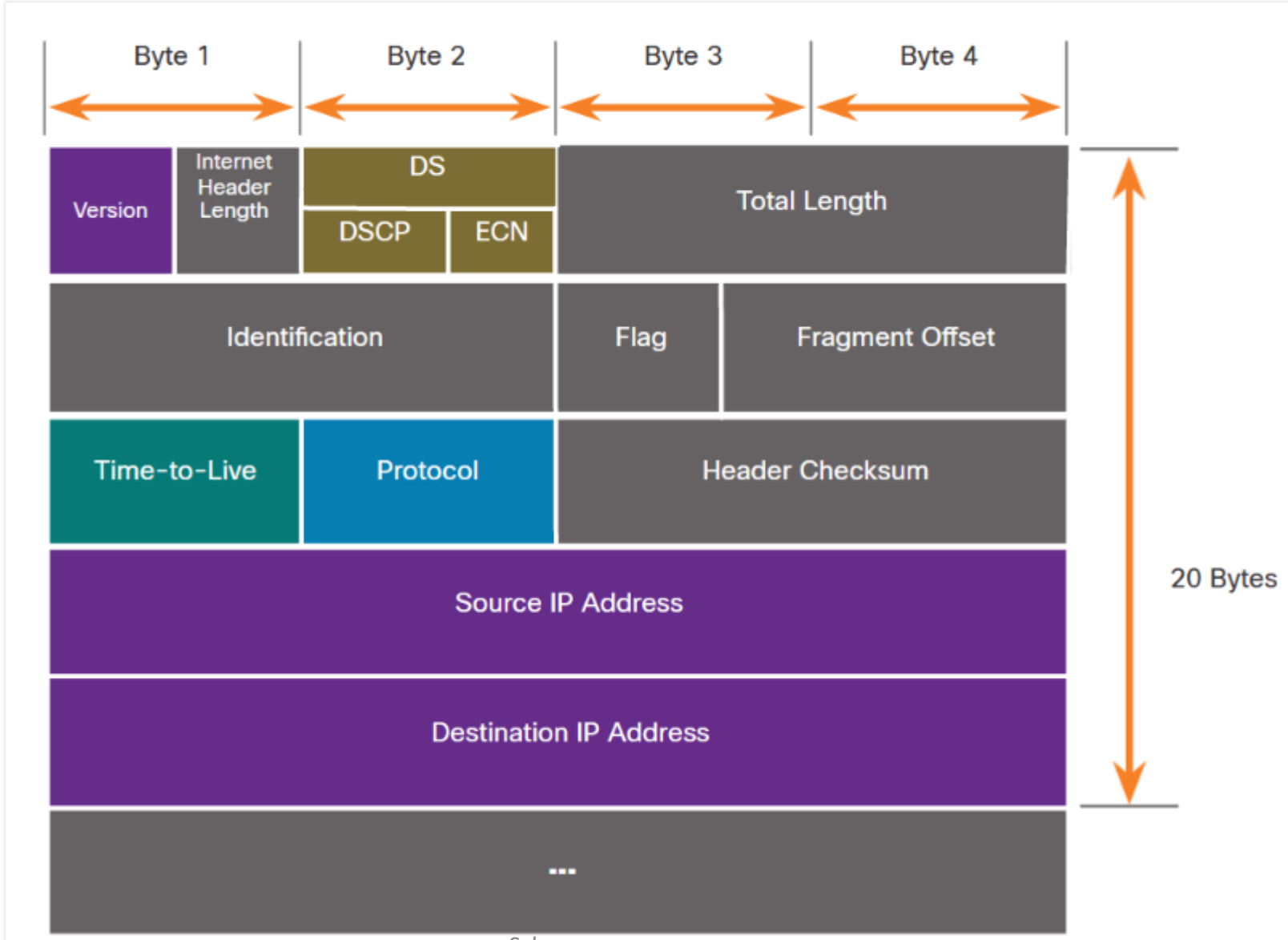
Best Effort



Media Independent



Fields in the IPv4 Packet Header

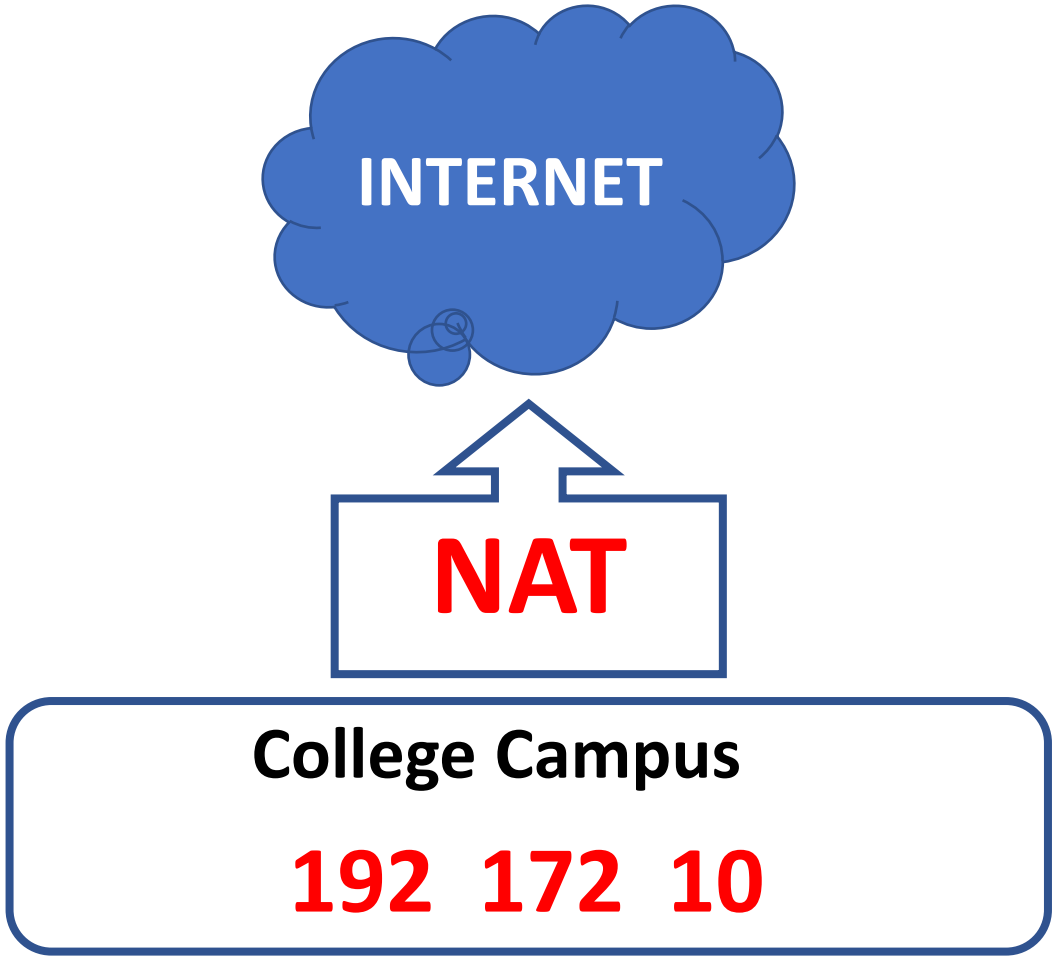


Limitations of IPv4

IPv4 address depletion - IPv4 has a limited number of unique public addresses available

Lack of end-to-end connectivity - Network Address Translation (NAT) is a technology commonly implemented

Increased network complexity –NAT creates additional complexity in the network, creating latency and making troubleshooting more difficult.

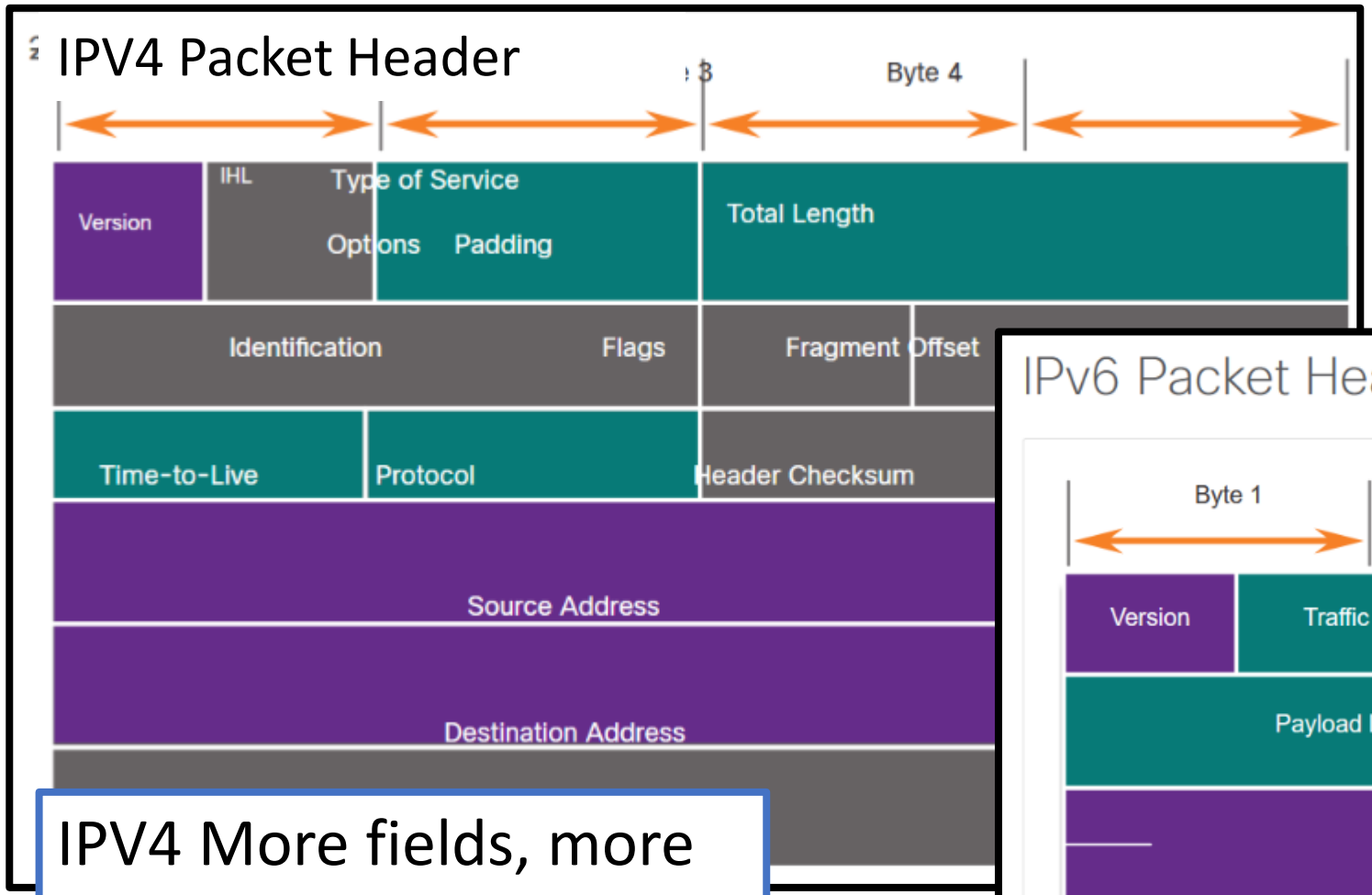


INTERNAL ADDRESSES – Never use on internet

192. NNNNNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH = 255 HOSTS

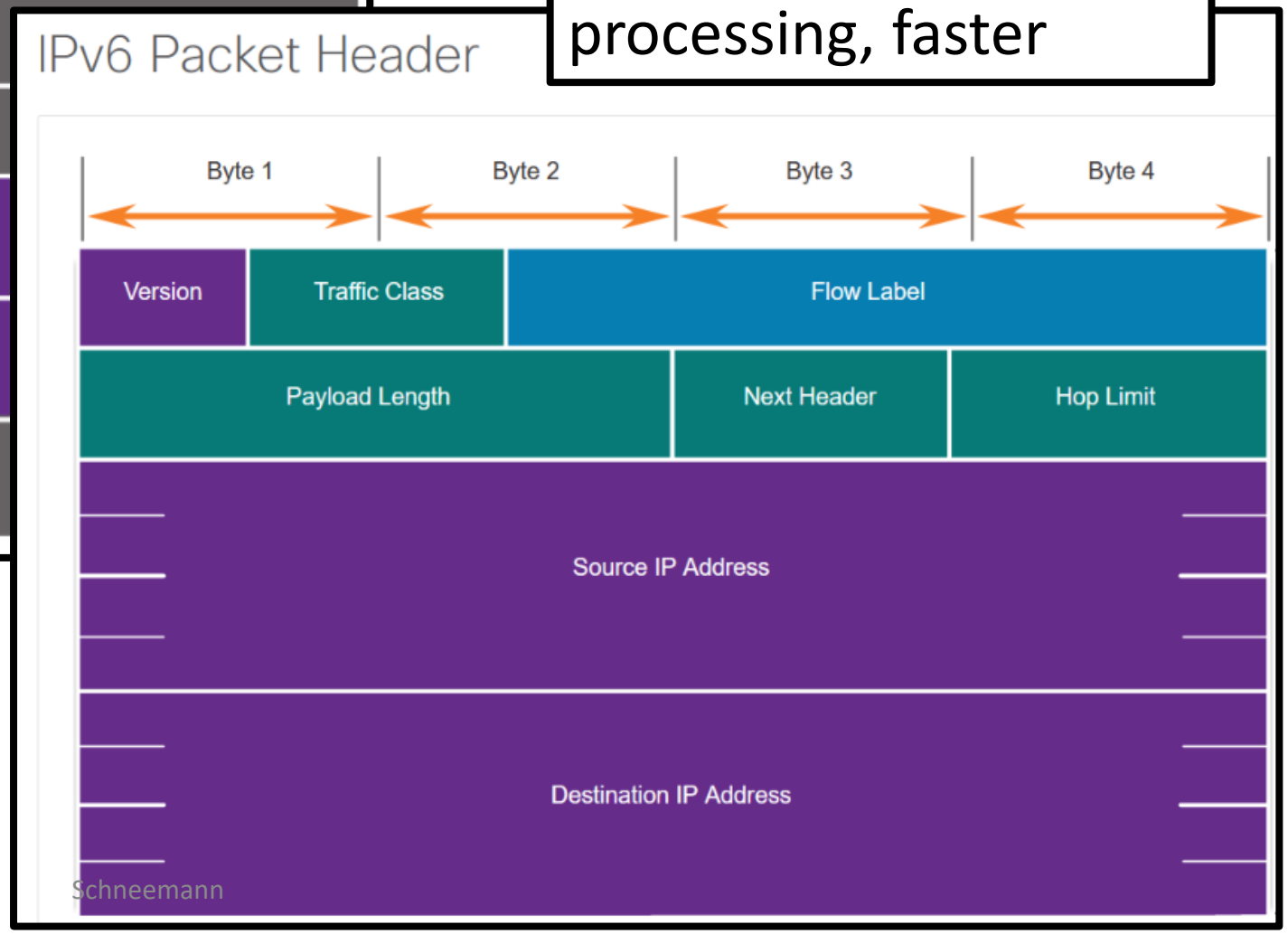
172. NNNNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH = 65,536 HOSTS

10. NNNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH = 16,777,216 HOSTS



IPV4 More fields, more processing, slower

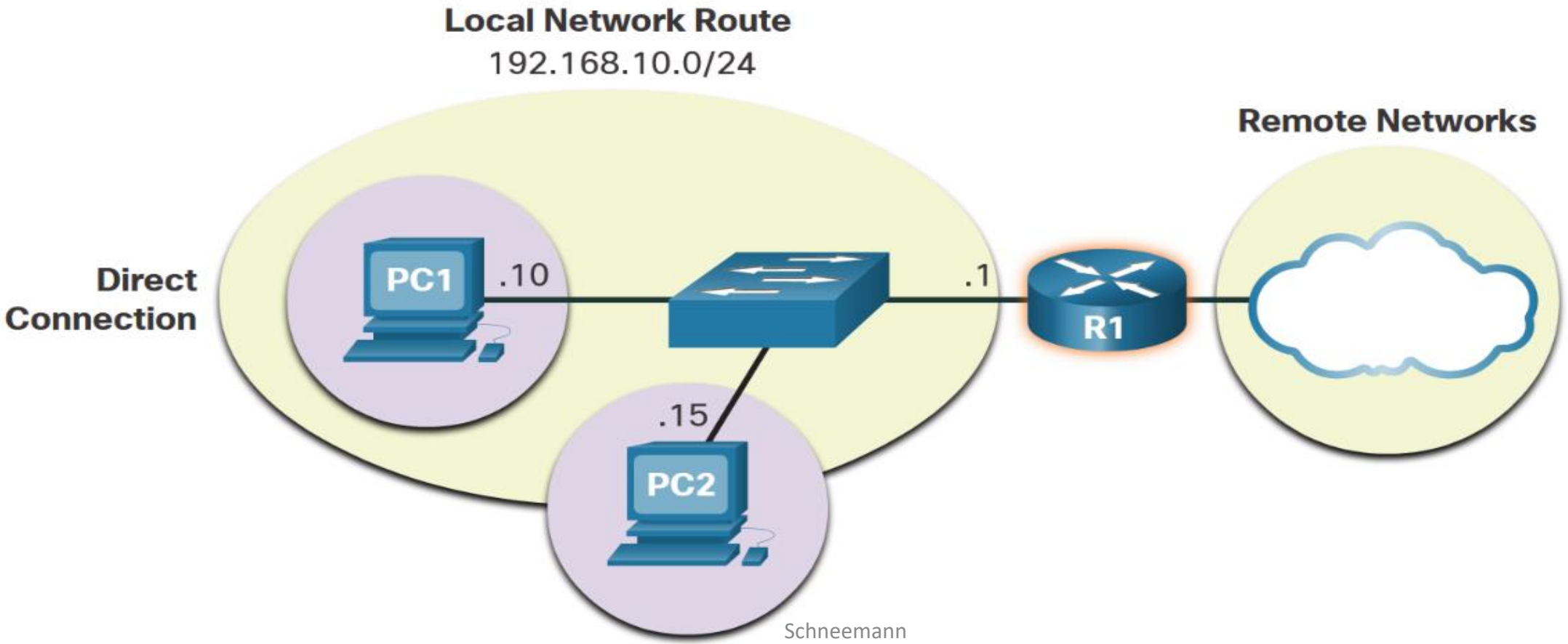
IPV6 Fewer fields, less processing, faster



A Host Routes to the Default Gateway

A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically from Dynamic Host Configuration Protocol (DHCP) or configured manually. In IPv6, the router advertises the default gateway address or the host can be configured manually.

In the figure, PC1 and PC2 are configured with the IPv4 address of 192.168.10.1 as the default gateway



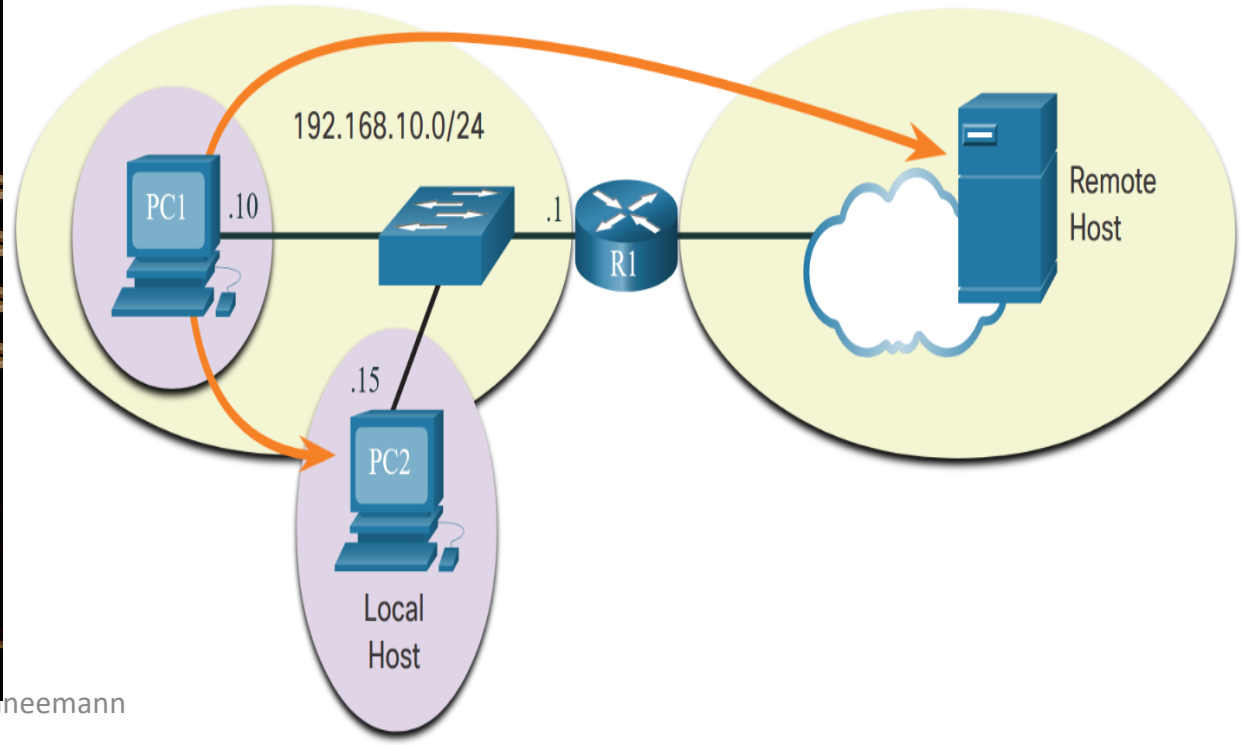
Another role of the network layer is to direct packets between hosts. A host can send a packet to the following:

Itself - A host can ping itself by sending a packet to a special IPv4 address of 127.0.0.1 or an IPv6 address ::1.

Local host - This is a destination host that is on the same local network as the sending host.

Remote host - This is a destination host on a remote network

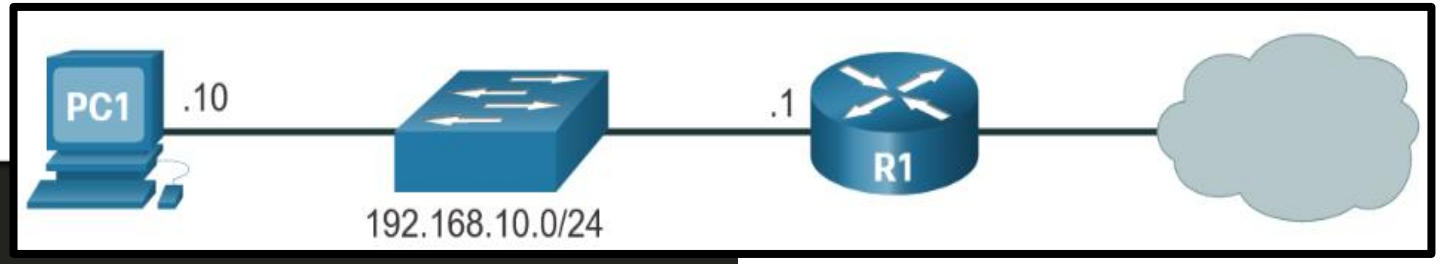
```
C:\Users\schne>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



Host Routing Tables

On a Windows host, the route print or netstat -r command can be used to display the host routing table. Both commands generate the same output. The output may seem overwhelming at first, but is fairly simple to understand.

IPv4 Routing Table for PC1




```
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)
```

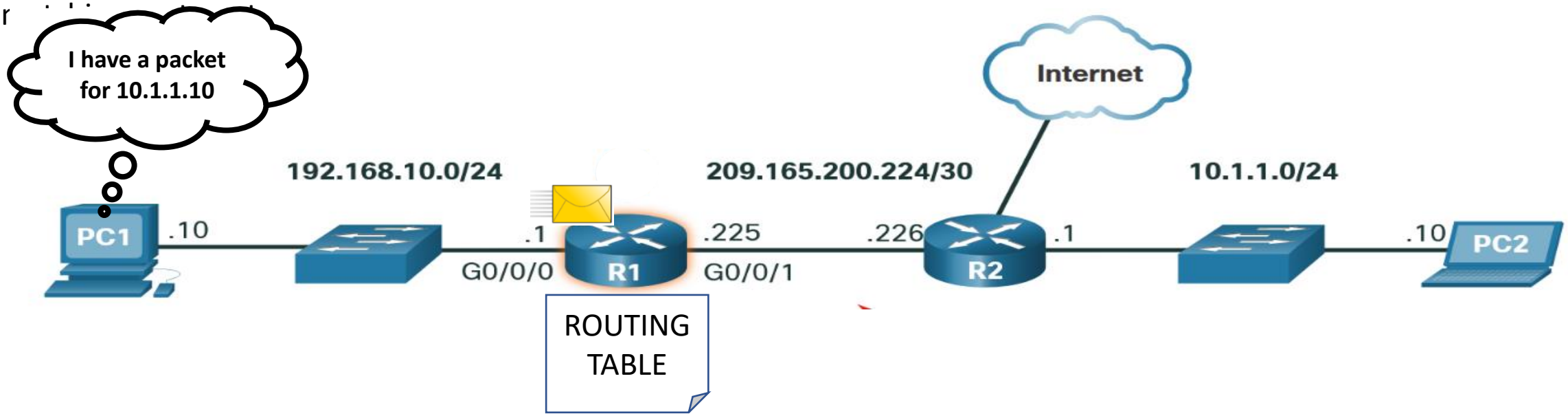
netstat -r

Introduction to Routing

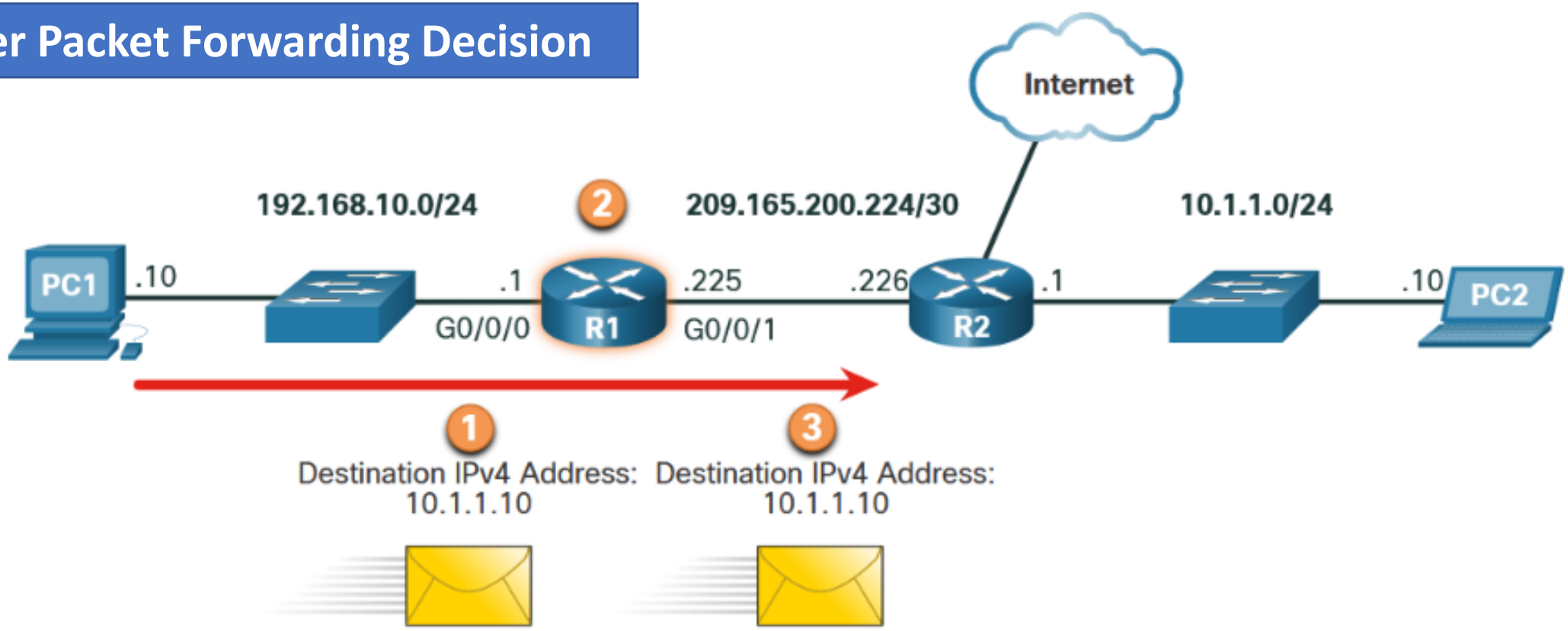
Router Packet Forwarding Decision

Most networks also contain routers, which are intermediary devices. Routers also contain routing tables. When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway, which is usually the local router.

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)



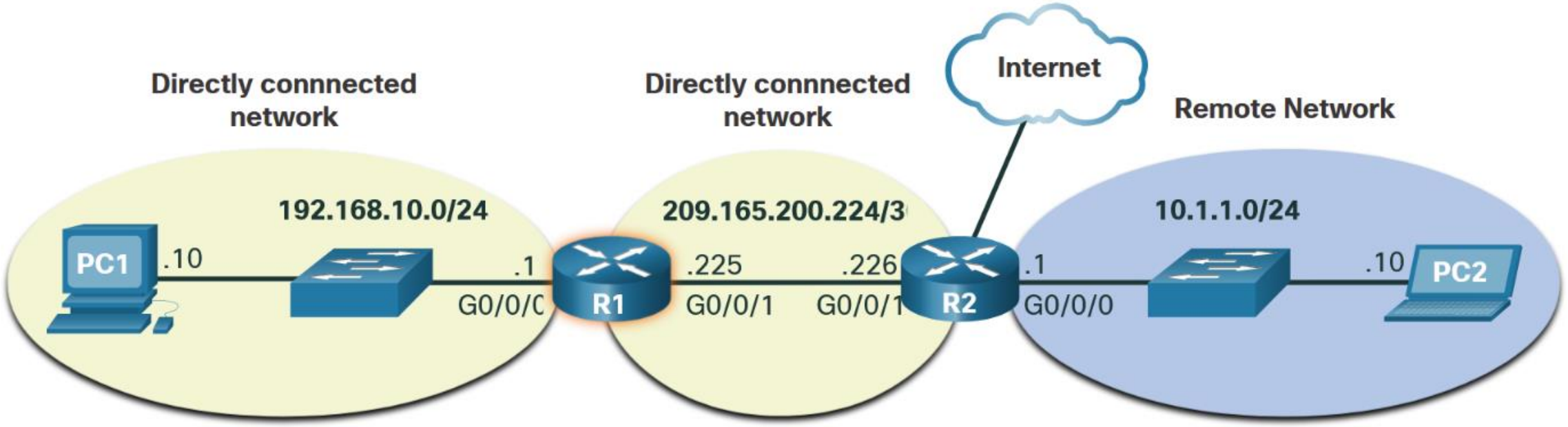
Router Packet Forwarding Decision



1. Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
2. Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. 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.

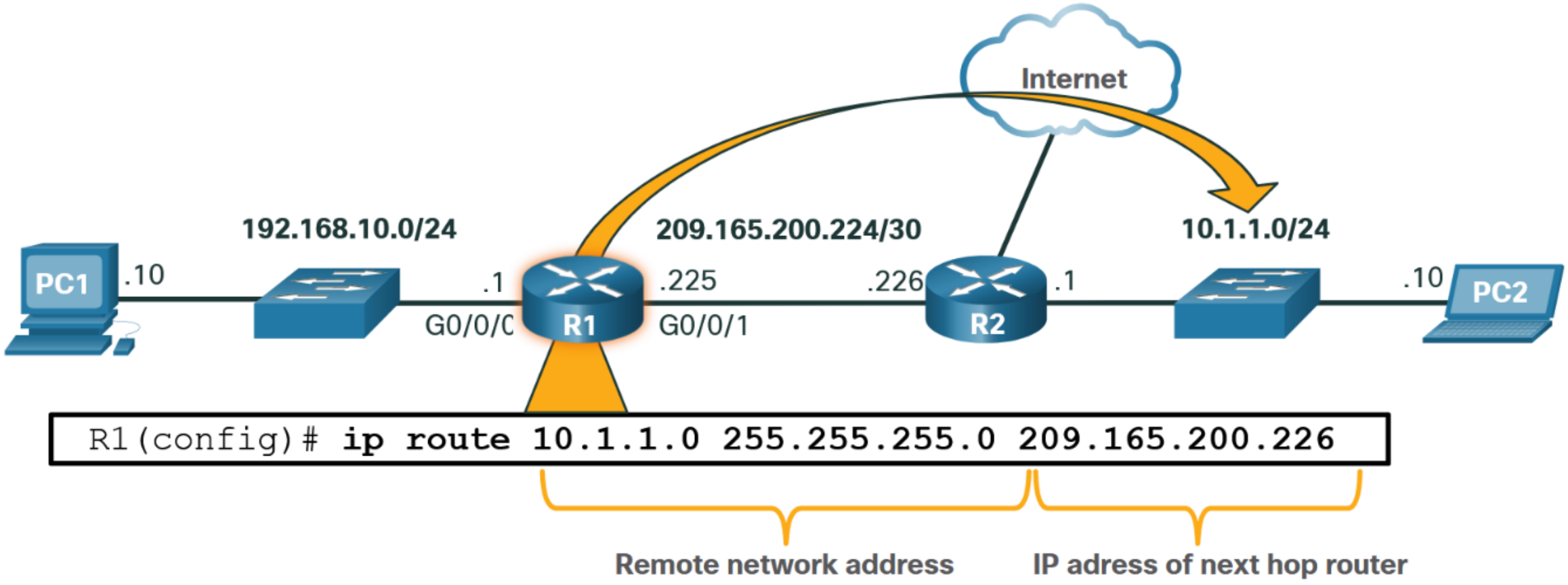
The routing table stores three types of route entries:

- **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. In the figure, the directly-connected networks in the R1 IPv4 routing table would be 192.168.10.0/24 and 209.165.200.224/30.
- **Remote networks** - 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. In the figure, the R1 IPv4 routing table would most likely include a default route to forward all packets to router R2.



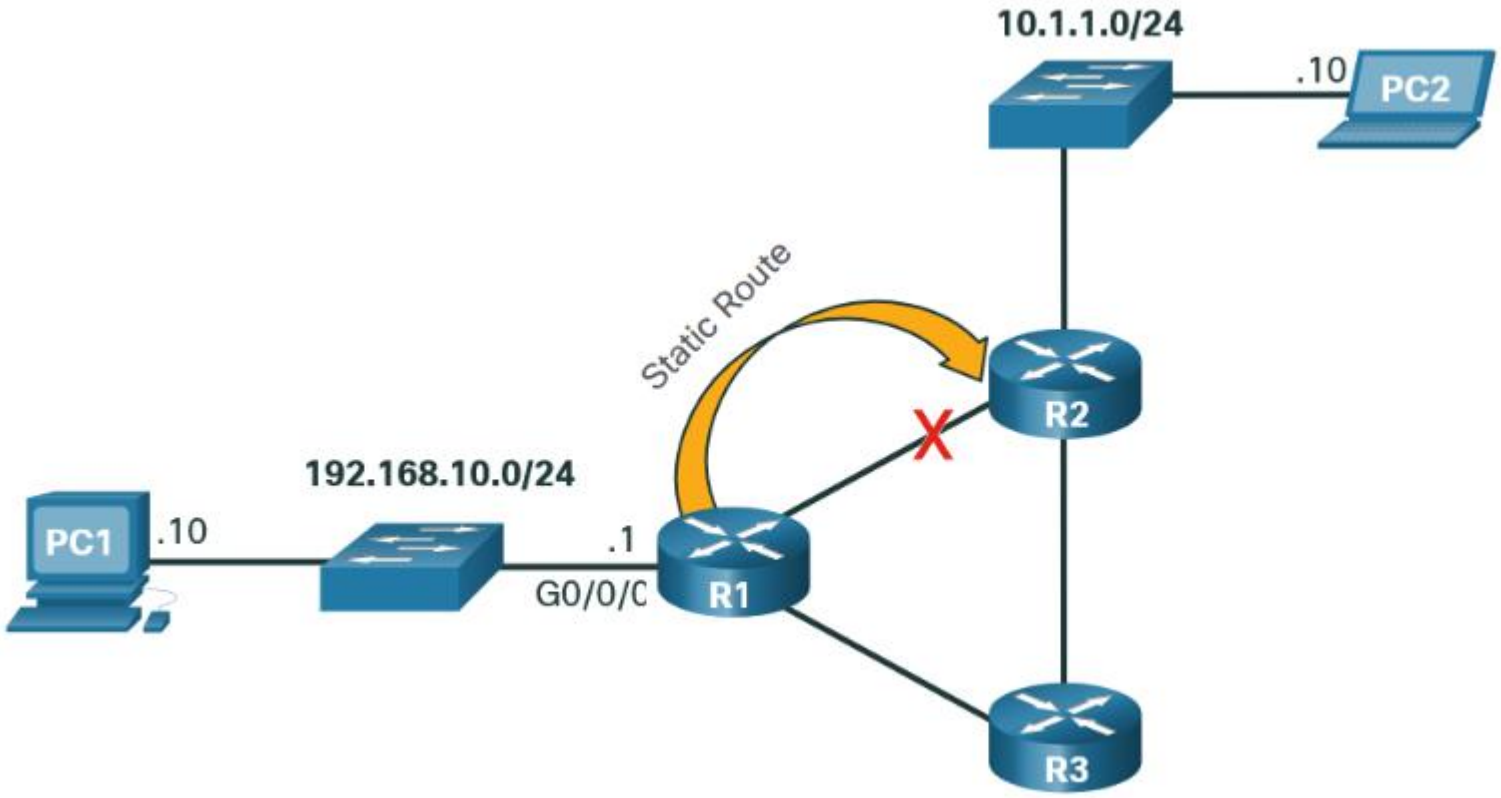
Static Routing

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.



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.

If there is a change in the network topology, the static route is not automatically updated and must be manually reconfigured. For example, in the figure 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 R3. Router R3 would therefore need to have a route entry in its routing table to send packets destined for 10.1.1.0/24 to R2.



A static route must be configured manually.

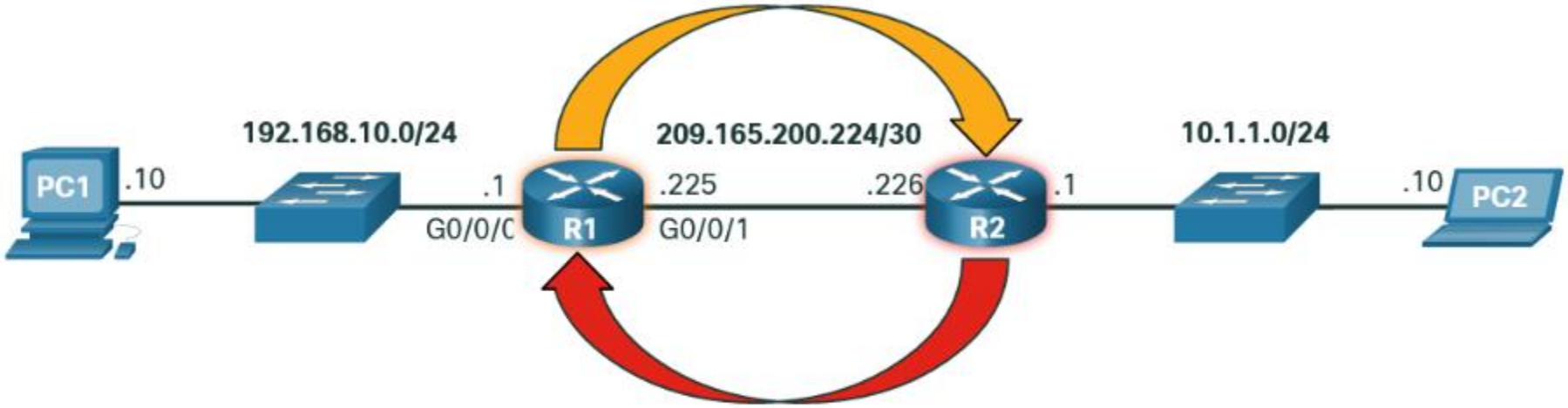
- **The administrator needs to reconfigure a static route if there is a change in the topology and the static route is no longer viable.**
- **A static route is appropriate for a small network and when there are few or no redundant links.**
- **A static route is commonly used with a dynamic routing protocol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

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.

Dynamic Routing

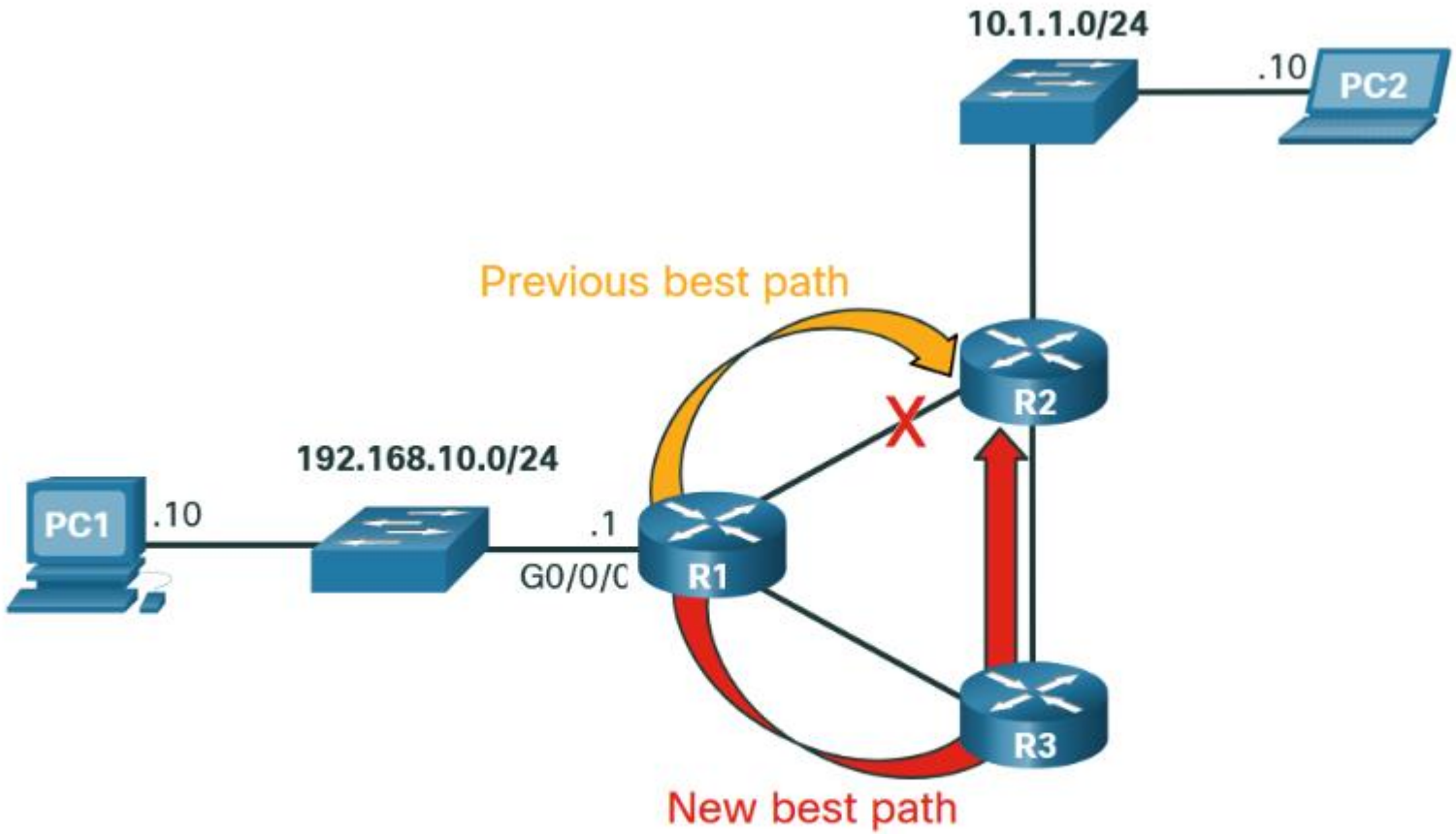
A dynamic routing protocol allows the routers to automatically learn about remote networks, including a default route, from other routers. Routers that use dynamic routing protocols automatically share routing information with other routers and compensate for any topology changes without involving the 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). 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.

When a router is manually configured with a static route or learns about a remote network dynamically using a dynamic routing protocol, the remote network address and next hop address are entered into the IP routing table. 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

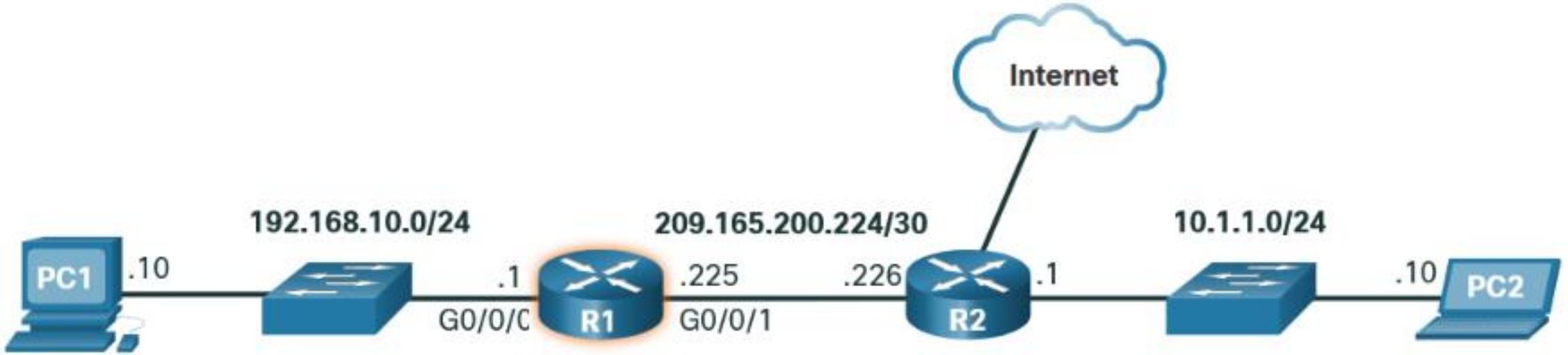


R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

GREAT VIDEO THAT EXPLAINS THE IPV4 ROUTING TABLE
Watch it in your Netacad curriculum

Introduction to an IPv4 Routing Table

Notice in the figure that R2 is connected to the internet. Therefore, the administrator configured R1 with a default static route sending packets to R2 when there is no specific entry in the routing table that matches the destination IP address. R1 and R2 are also using OSPF routing to advertise directly connected networks



SEE ROUTING TABLE FOR R1 ON NEXT SLIDE

The show ip route privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. The example shows the IPv4 routing table of router R1. 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:

```
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#
```


- L - Directly connected local interface IP address
- C – Directly connected network
- S – Static route was manually configured by an administrator

O - OSPF
D - EIGRP

A default route has a network address of all zeroes. For example, the IPv4 network address is 0.0.0.0. A static route entry in the routing table begins with a code of S*, as highlighted in the example


```
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#
```

L - Directly connected local interface IP address

C – Directly connected network

S – Static route was manually configured by an administrator

O - OSPF

D - EIGRP

L - Directly connected local interface IP address

C – Directly connected network

S – Static route was manually configured by an administrator

O - OSPF

D - EIGRP

8.6.1 Module Practice and Quiz

What did I learn in this module?

- Network Layer Characteristics
  - IPv4 Packet
  - IPv6 Packet
- How a Host Routes
- Introduction to Routing

Thanks!

Frank Schneemann, MS EdTech
www.edtechnology.com