

Network Layer







CCNA1v7 Module 8 Network Layer



Pedro Durán

Network Layer

- Provides services to allow end devices to exchange data.
- Network Layer Protocols: **IPv4 and IPv6**.
- The network layer performs four **basic operations**:
 -  **Addressing end devices**
 -  **Encapsulation**
 -  **Routing**
 -  **De-encapsulation**
- 🤔 The IP addressing does not change from source to destination.

Network Layer Characteristics

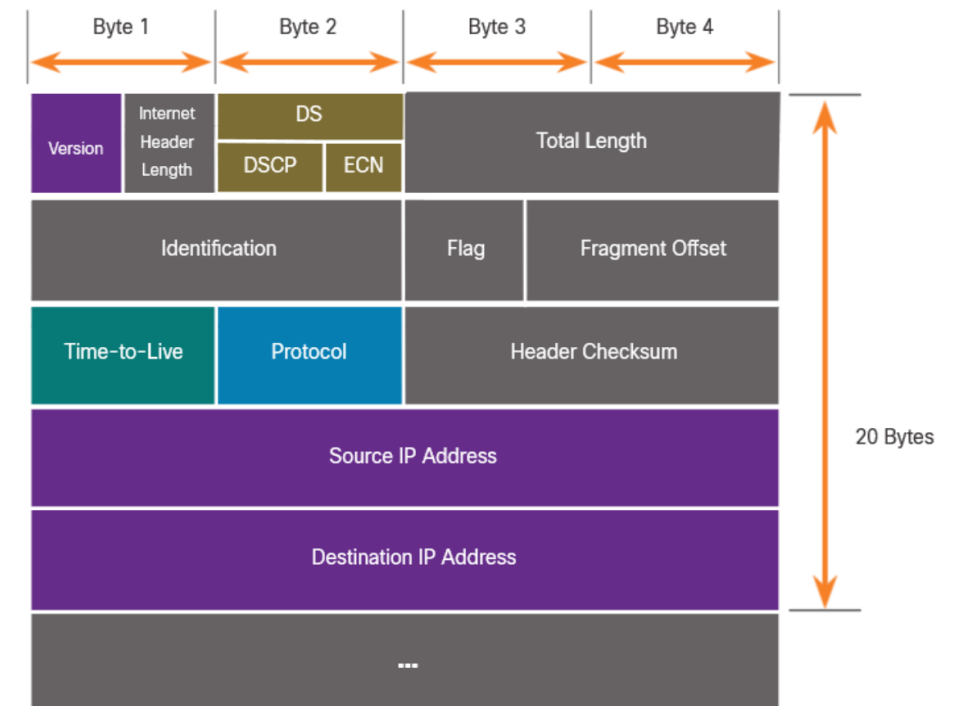
IP have low overhead and may be described as:

- **Connectionless:** does not establish a connection before sending a packet. There is no control information needed.
- **Best effort:** will not guarantee delivery of the packet. Reduced overhead and no acknowledgments.
- **Media Independent:**
 - IP is unreliable: cannot manage or fix undelivered or corrupt packets
 - IP is media independent: can be sent over any media type.

Layer 3 splits the IPv4 into smaller units (Fragmentation, **MTU**: Maximum Transport Unit)

IPv4 Packet Header Fields

Function	Description
Version	This will be for v4, as opposed to v6, a 4 bit field= 0100
Differentiated Services	Used for QoS: DiffServ – DS field or the older IntServ – ToS or Type of Service
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32 bit source address
Destination IPv4 Address	32 bit destination address



IPv6 Overview

IPv4 has 3 major limitations:

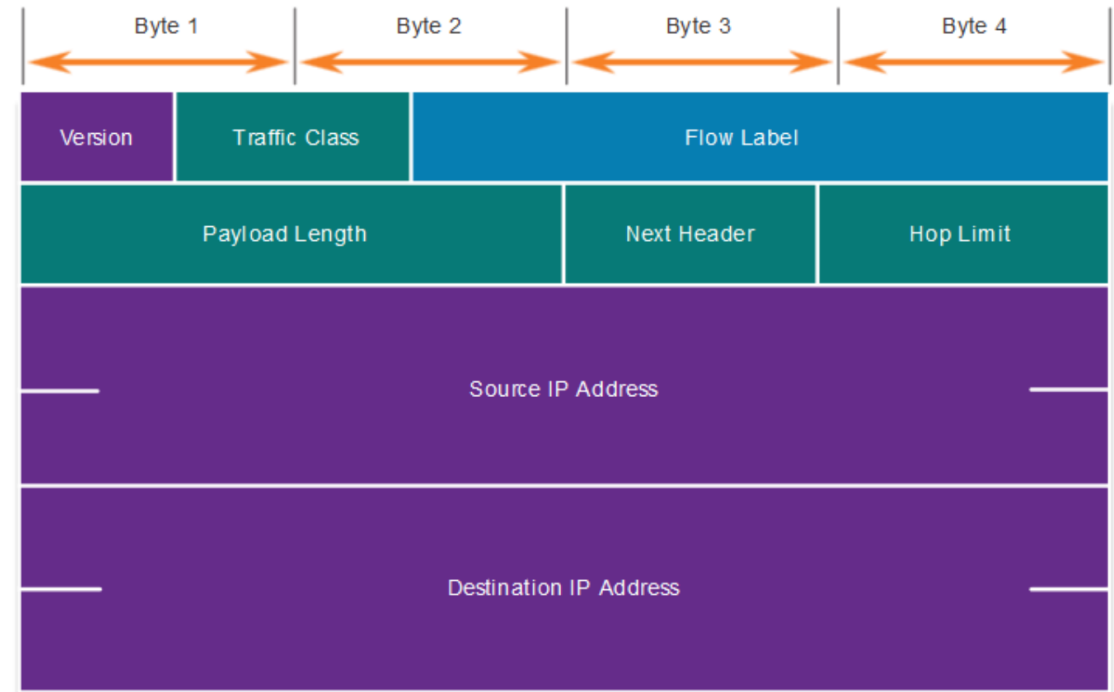
- **1** IPv4 address depletion: run out of IPv4 addressing
- **2** Lack of end-to-end connectivity: private addressing and NAT were created
- **3** Increased network complexity: NAT was a temporary solution, create issues and causes latency.

IPv6 overcomes the limitation of IPv4:

- **1** Increased address space: based on 128 bit address instead of 32 bit
- **2** Improved packet handling: simplified header with fewer fields
- **3** Eliminates the need for NAT: no need to use private addressing internally

IPv6 Packet Header Fields

Function	Description
Version	This will be for v6, as opposed to v4, a 4 bit field= 0110
Traffic Class	Used for QoS: Equivalent to DiffServ – DS field
Flow Label	Informs device to handle identical flow labels the same way, 20 bit field
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet
Next Header	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Hop Limit	Replaces TTL field Layer 3 hop count
Source IPv6 Address	128 bit source address
Destination IPv6 Address	128 bit destination address



Host Forwarding Decision

- Each host devices creates their own routing table.
- A host can send packets to:
 - **Itself:** 127.0.0.1 (IPv4), ::1 (IPv6)
 - **Local hosts:** destination on the same LAN. Traffic handled by intermediary device.
 - **Remote hosts:** devices are not on the same LAN. Traffic forwarded directly to LAN default gateway.
- The source device determines whether the destination is local or remote:
 - **IPv4:** Source IP address and network mask < > Destination IP address
 - **IPv6:** Source uses the network address and prefix advertised by local router

Default Gateway

A Router or Layer 3 Switch can be a default gateway.

- It must have an IP address in the same range as the rest of the LAN.
- It can route to other networks.

A default gateway is static route which will be a last resort route in the routing table. All device on the LAN will need the default gateway of the router if they intend to send traffic remotely. If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

Host will know the default gateway:

- IPv4: statically or through DHCP
- IPv6: through RS (Router Solicitation) or manually

Host Routing Tables

Display the PC routing table:

- Windows: `route print` or `netstat -r`
- Linux: `ip route`



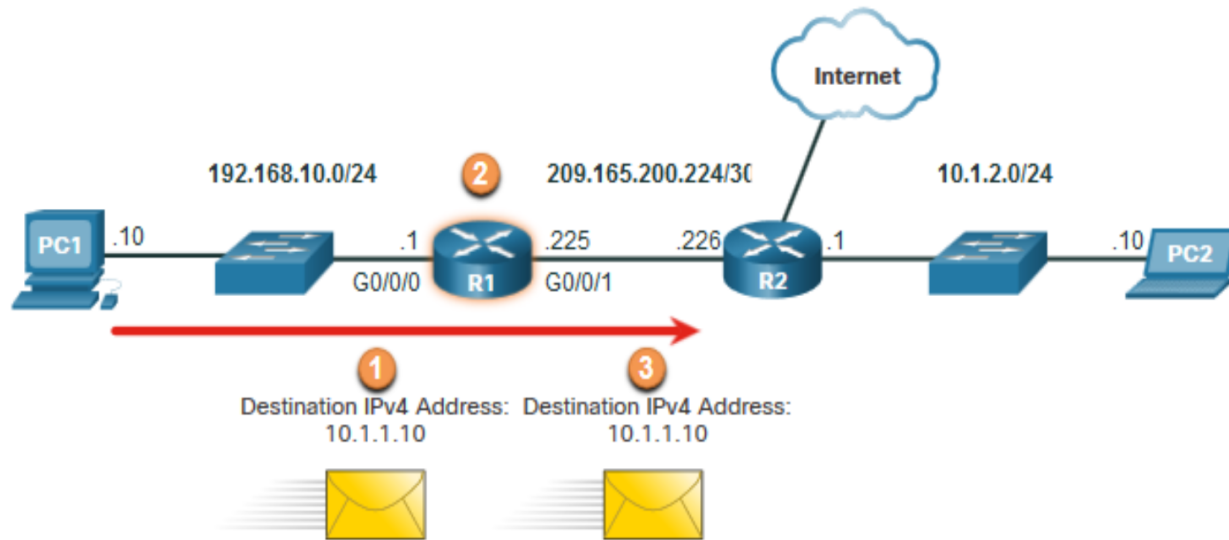
IPv4 Routing Table for PC1

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

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
```

Router Packet Forwarding Decision

What happens when the router receives the frame from the host device?



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-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.

IP Routing Table

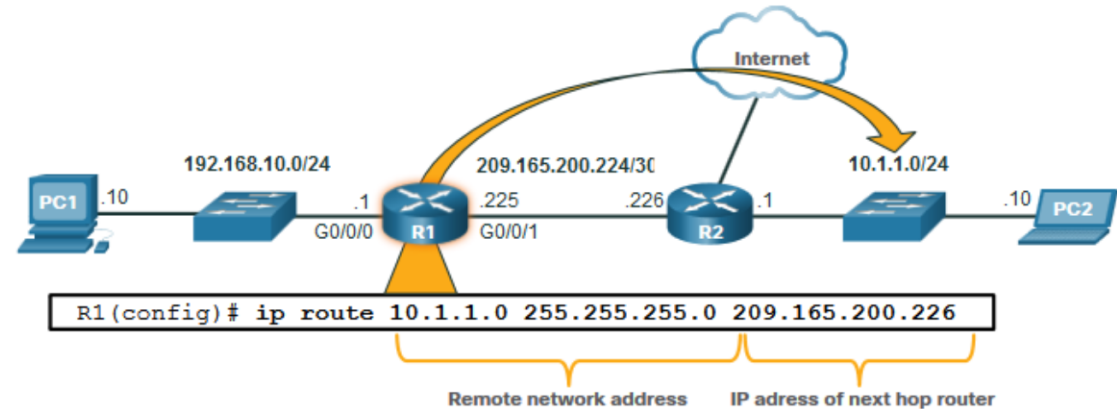
3 types of routes in a router's routing table:

- **1 Directly Connected:** These routes are automatically added by the router, provided the interface is active and has addressing.
- **2 Remote:** These are the routes the router does not have a direct connection and may be learned:
 - Manually – with a static route
 - Dynamically – by using a routing protocol to have the routers share their information with each other
- **3 Default Route:** this forwards all traffic to a specific direction when there is not a match in the routing table

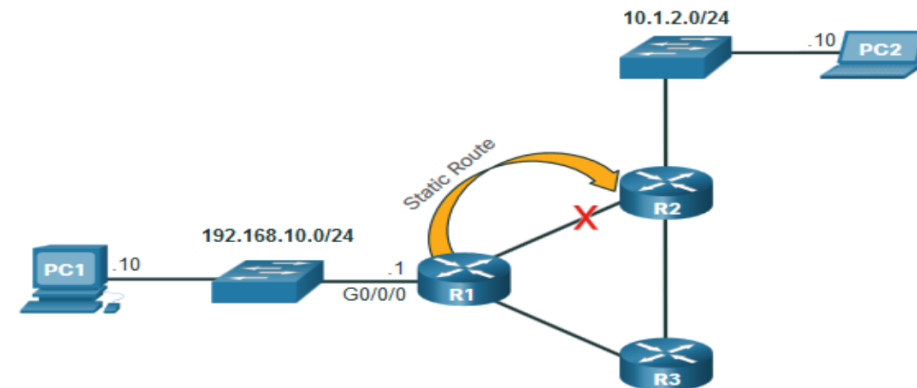
Static Routing

Static Route Characteristics:

- Must be configured manually
- Must be adjusted manually by the administrator when there is a change in the topology
- Good for small non-redundant networks
- Often used in conjunction with a dynamic routing protocol for configuring a default route



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.



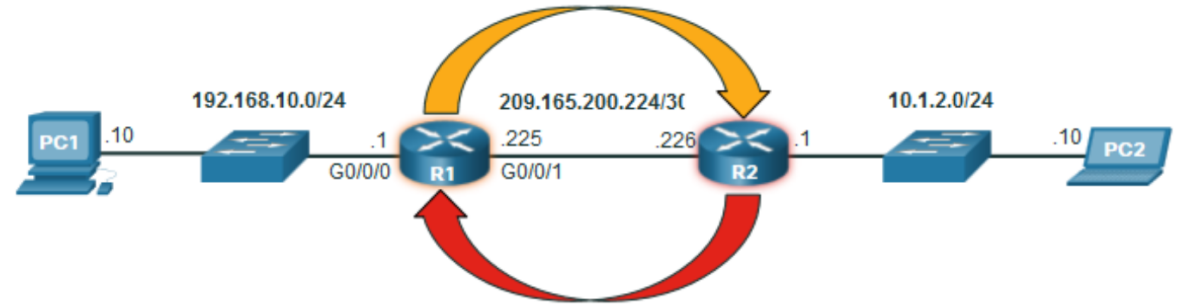
If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

Dynamic Routing

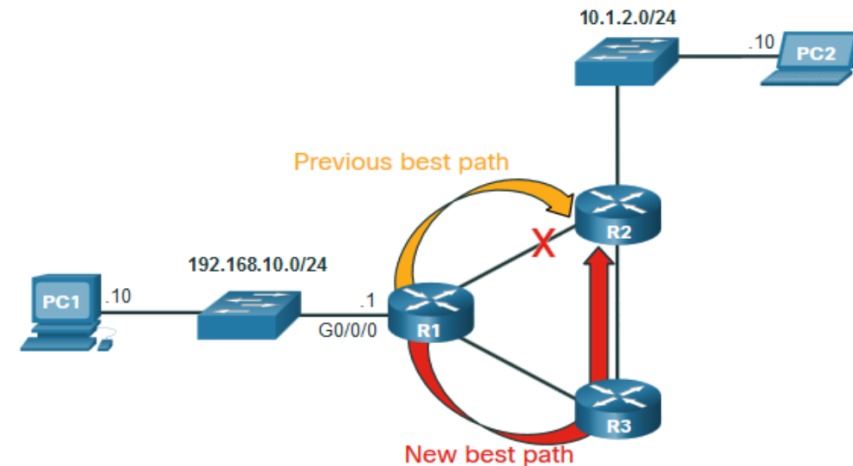
Dynamic Routes Automatically:

- Discover remote networks
- Maintain up-to-date information
- Choose the best path to the destination
- Find new best paths when there is a topology change

Dynamic routing can also share static default routes with the other routers.



- 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.



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.

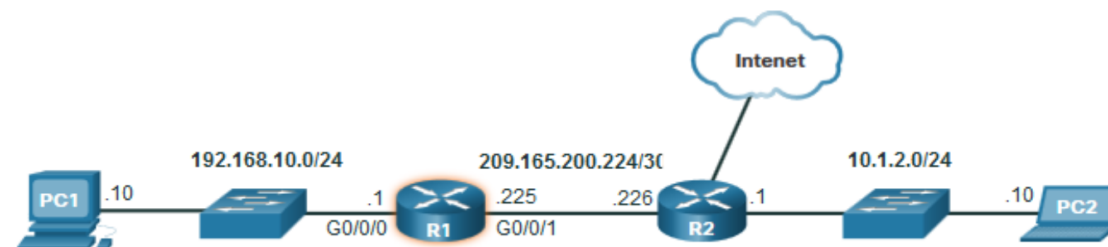
Introduction to an IPv4 Routing Table

The **show ip route** command shows the following route sources:

- **L** - Directly connected local interface IP address
- **C** - Directly connected network
- **S** - Static route was manually configured by an administrator
- **O** - OSPF
- **D** - EIGRP

This command shows types of routes:

- Directly Connected – C and L
- Remote Routes – O, D, etc.
- Default Routes – S*



```
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#
```