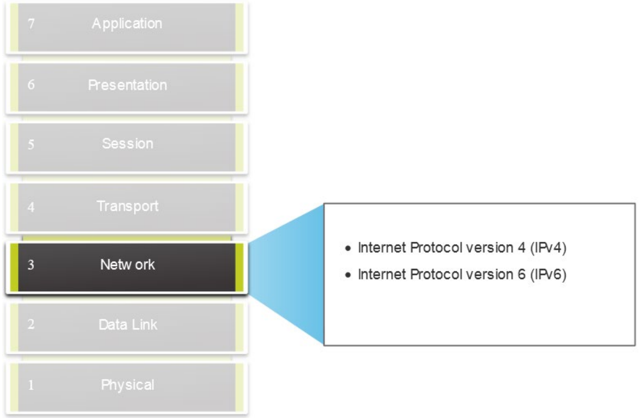
Module 5: Network Layer

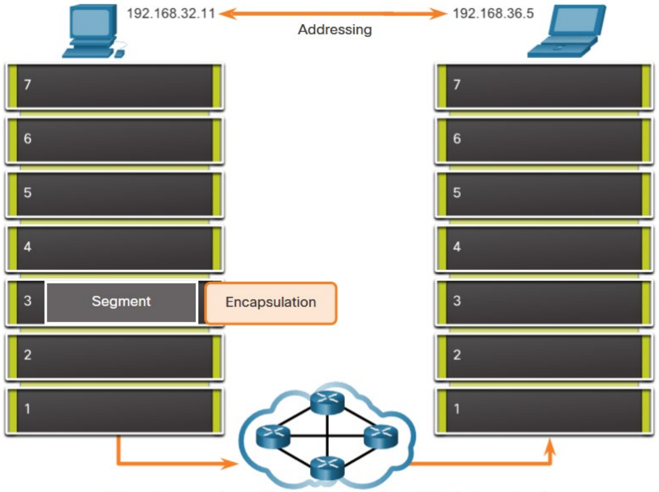
Introduction to Networks v7.0
(ITN)

Network Layer Characteristics

Network Layer Characteristics
The Network Layer

- Provides services to allow end devices to exchange data
- IP version 4 (IPv4) and IP version 6 (IPv6) are the principle network layer communication protocols.
- The network layer performs four basic operations:
  - Addressing end devices
  - Encapsulation
  - Routing
  - De-encapsulation



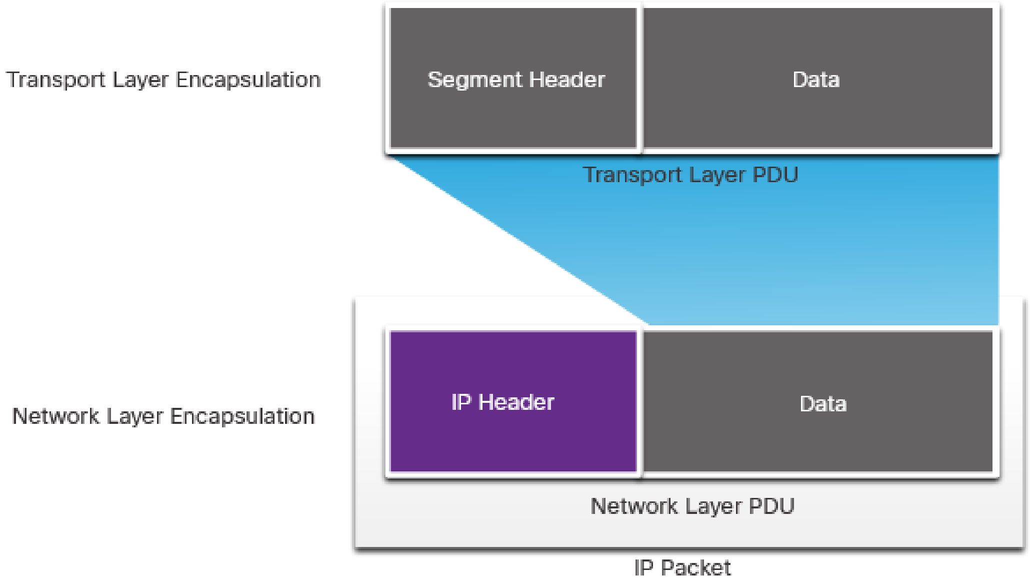


Network layer protocols forward transport layer PDUs between hosts.

IP Encapsulation

- IP encapsulates the transport layer segment.
- IP can use either an IPv4 or IPv6 packet and not impact the layer 4 segment.
- IP packet will be examined by all layer 3 devices as it traverses the network.
- The IP addressing does not change from source to destination.

Note: NAT will change addressing, but will be discussed in a later module.



Characteristics of IP

IP is meant to have low overhead and may be described as:

- Connectionless
- Best Effort
- Media Independent

Connectionless

IP is Connectionless

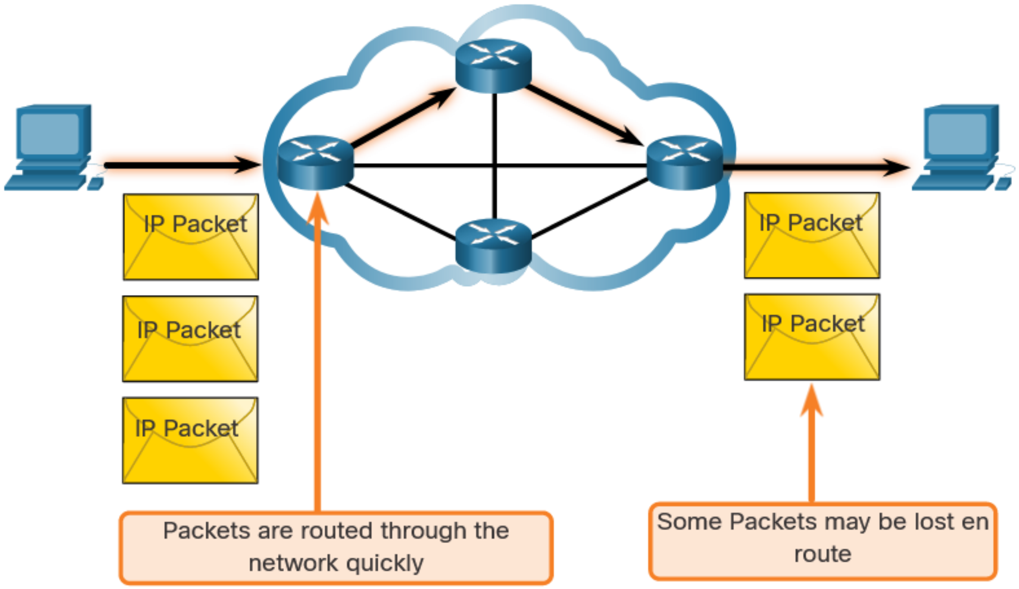
- IP does not establish a connection with the destination before sending the packet.
- There is no control information needed (synchronizations, acknowledgments, etc.).
- The destination will receive the packet when it arrives, but no pre-notifications are sent by IP.
- If there is a need for connection-oriented traffic, then another protocol will handle this (typically TCP at the transport layer).

A letter is sent.

Best Effort

IP is Best Effort

- IP will not guarantee delivery of the packet.
- IP has reduced overhead since there is no mechanism to resend data that is not received.
- IP does not expect acknowledgments.
- IP does not know if the other device is operational or if it received the packet.



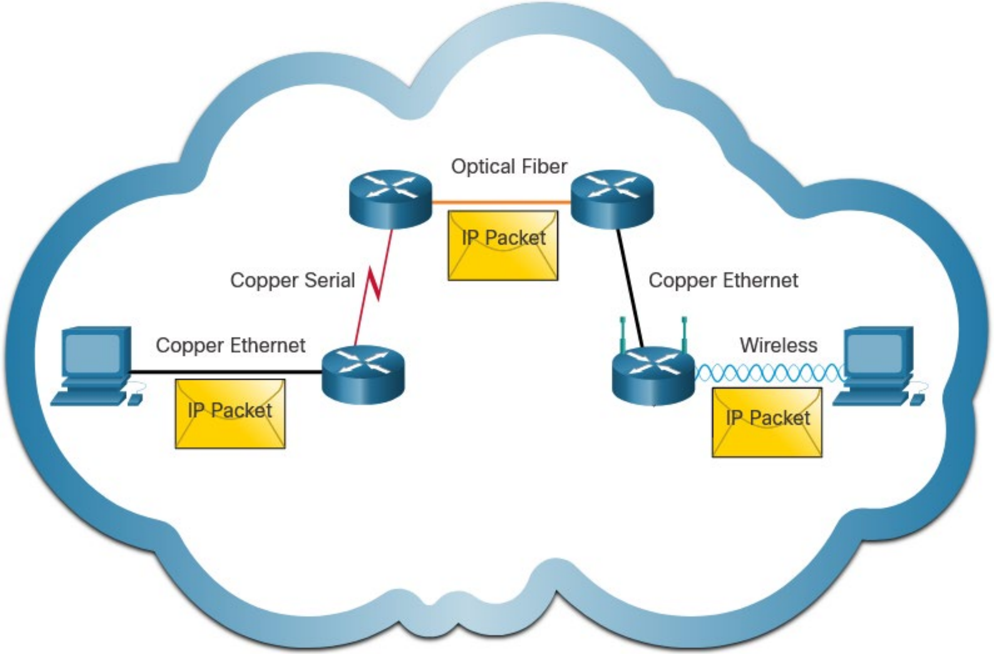
Media Independent

IP is unreliable:

- It cannot manage or fix undelivered or corrupt packets.
- IP cannot retransmit after an error.
- IP cannot realign out of sequence packets.
- IP must rely on other protocols for these functions.

IP is media Independent:

- IP does not concern itself with the type of frame required at the data link layer or the media type at the physical layer.
- IP can be sent over any media type: copper, fiber, or wireless.



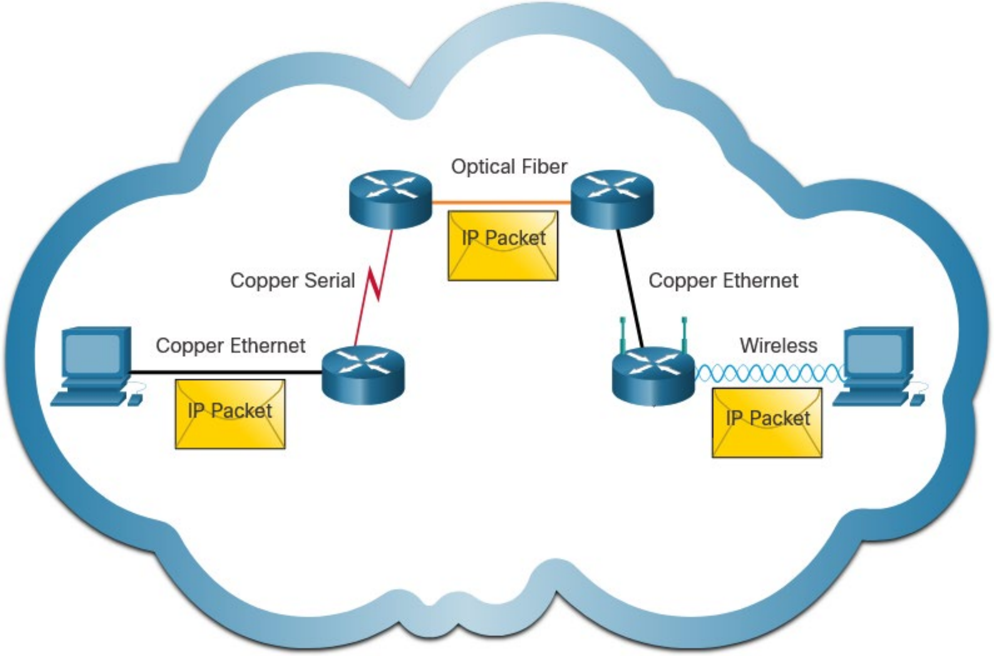
Media Independent (Contd.)

The network layer will establish the Maximum Transmission Unit (MTU).

- Network layer receives this from control information sent by the data link layer.
- The network then establishes the MTU size.

Fragmentation is when Layer 3 splits the IPv4 packet into smaller units.

- Fragmenting causes latency.
- IPv6 does not fragment packets.
- Example: Router goes from Ethernet to a slow WAN with a smaller MTU



IPv4 Packet

IPv4 Packet Header

IPv4 is the primary communication protocol for the network layer.

The network header has many purposes:

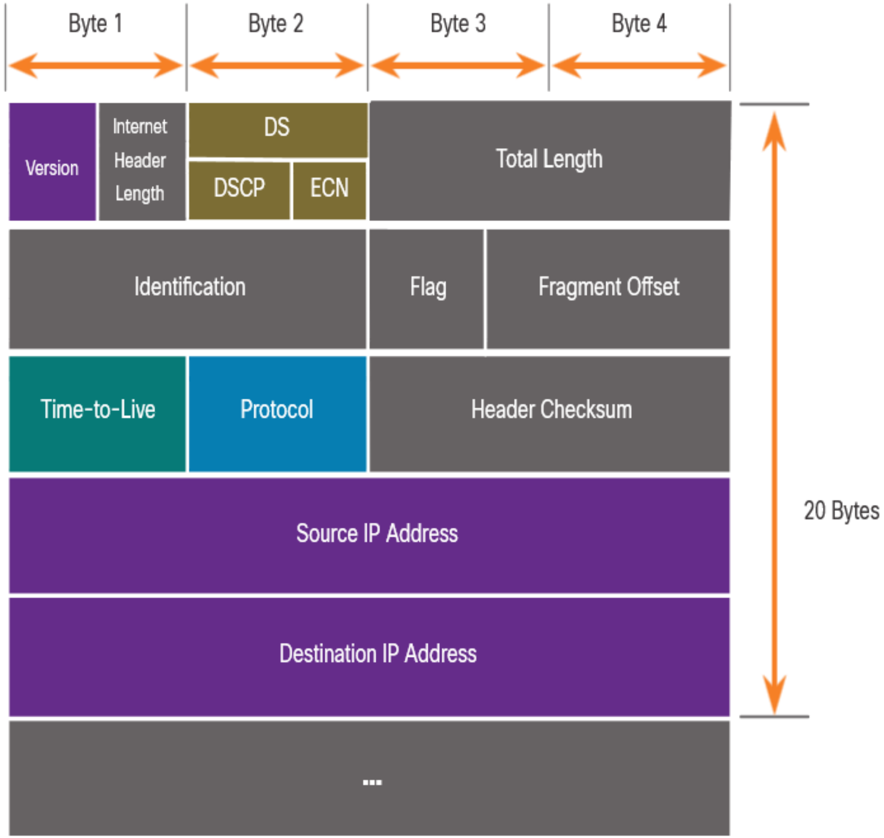
- It ensures the packet is sent in the correct direction (to the destination).
- It contains information for network layer processing in various fields.
- The information in the header is used by all layer 3 devices that handle the packet

IPv4 Packet Header Fields

The IPv4 network header characteristics:

- It is in binary.
- Contains several fields of information
- Diagram is read from left to right, 4 bytes per line
- The two most important fields are the source and destination.

Protocols may have one or more functions.



IPv4 Packet Header Fields

Significant fields in the IPv4 header:

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 Packets

Limitations of IPv4

IPv4 has three major limitations:

- IPv4 address depletion – We have basically run out of IPv4 addressing.
- Lack of end-to-end connectivity – To make IPv4 survive this long, private addressing and NAT were created. This ended direct communications with public addressing.
- Increased network complexity – NAT was meant as temporary solution and creates issues on the network as a side effect of manipulating the network headers addressing. NAT causes latency and troubleshooting issues.

IPv6 Overview

- IPv6 was developed by Internet Engineering Task Force (IETF).
- IPv6 overcomes the limitations of IPv4.
- Improvements that IPv6 provides:
  - **Increased address space** – based on 128 bit address, not 32 bits
  - **Improved packet handling** – simplified header with fewer fields
  - **Eliminates the need for NAT** – since there is a huge amount of addressing, there is no need to use private addressing internally and be mapped to a shared public address

IPv4 and IPv6 Address Space Comparison

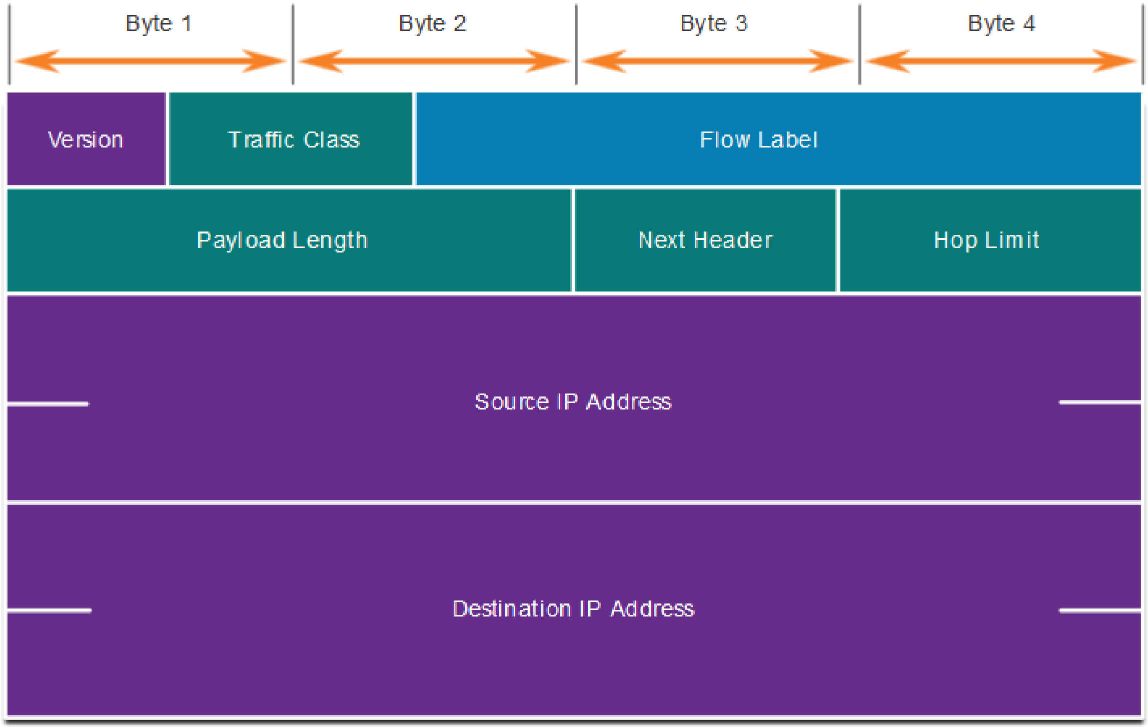
Number Name	Scientific Notation	Number of Zeros
1 Thousand	10^3	1,000
1 Million	10^6	1,000,000
1 Billion	10^9	1,000,000,000
1 Trillion	10^12	1,000,000,000,000
1 Quadrillion	10^15	1,000,000,000,000,000
1 Quintillion	10^18	1,000,000,000,000,000,000
1 Sextillion	10^21	1,000,000,000,000,000,000,000
1 Septillion	10^24	1,000,000,000,000,000,000,000,000
1 Octillion	10^27	1,000,000,000,000,000,000,000,000,000
1 Nonillion	10^30	1,000,000,000,000,000,000,000,000,000,000
1 Decillion	10^33	1,000,000,000,000,000,000,000,000,000,000,000
1 Undecillion	10^36	1,000,000,000,000,000,000,000,000,000,000,000,000

Legend

- There are 4 billion IPv4 addresses
- There are 340 undecillion IPv6 addresses

IPv4 Packet Header Fields in the IPv6 Packet Header

- The IPv6 header is simplified, but not smaller.
- The header is fixed at 40 Bytes or octets long.
- Several IPv4 fields were removed to improve performance.
- Some IPv4 fields were removed to improve performance:
  - Flag
  - Fragment Offset
  - Header Checksum



IPv6 Packet Header

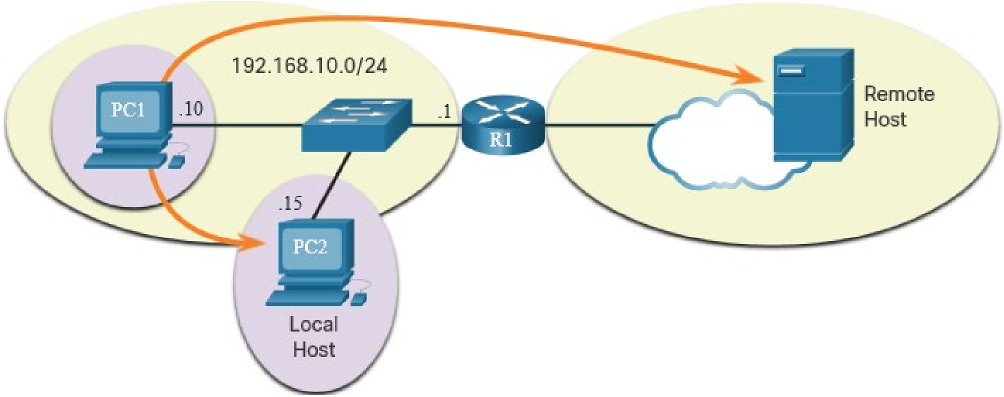
Significant fields in the IPv6 header:

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 IPv4 Address	128 bit source address
Destination IPV4 Address	128 bit destination address

How a Host Routes

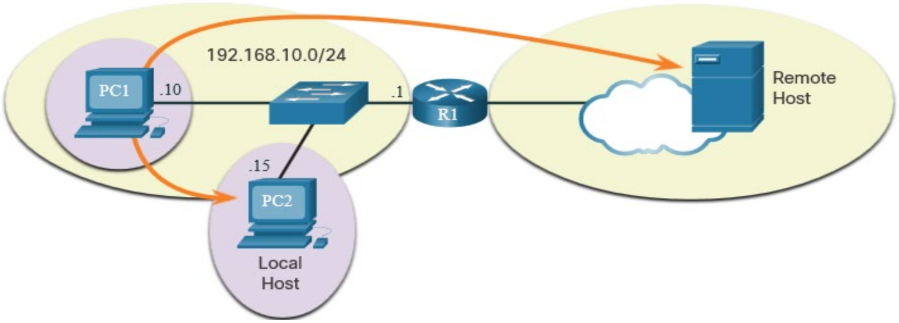
Host Forwarding Decision

- Packets are always created at the source.
- Each host devices creates their own routing table.
- A host can send packets to the following:
  - Itself – 127.0.0.1 (IPv4), ::1 (IPv6)
  - Local Hosts – destination is on the same LAN
  - Remote Hosts – devices are not on the same LAN



Host Forwarding Decision (Cont.)

- The Source device determines whether the destination is local or remote
- Method of determination:
  - IPv4 – Source uses its own IP address and Subnet mask, along with the destination IP address
  - IPv6 – Source uses the network address and prefix advertised by the local router
- Local traffic is dumped out the host interface to be handled by an intermediary device.
- Remote traffic is forwarded directly to the default gateway on the LAN.



Default Gateway

A router or layer 3 switch can be a default-gateway.

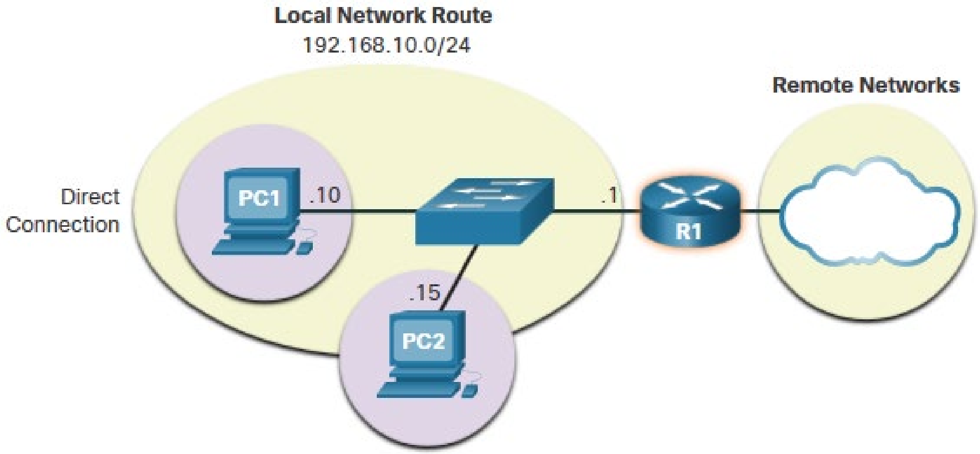
Features of a default gateway (DGW):

- It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic off of the LAN.
- It can route to other networks.

If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

A Host Routes to the Default Gateway

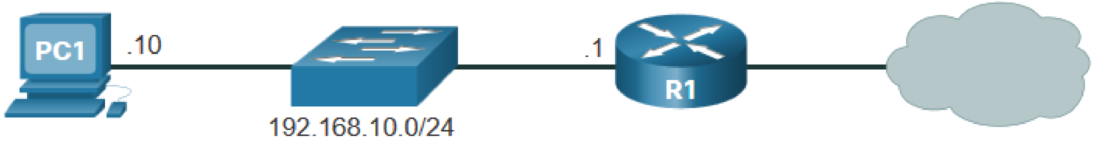
- The host will know the default gateway (DGW) either statically or through DHCP in IPv4.
- IPv6 sends the DGW through a router solicitation (RS) or can be configured manually.
- A DGW is static route which will be a last resort route in the routing table.
- All device on the LAN will need the DGW of the router if they intend to send traffic remotely.



How a Host Routes

Host Routing Tables

- On Windows, route print or netstat -r to display the PC routing table
- Three sections displayed by these two commands:
  - Interface List – all potential interfaces and MAC addressing
  - IPv4 Routing Table
  - IPv6 Routing Table



IPv4 Routing Table for PC1

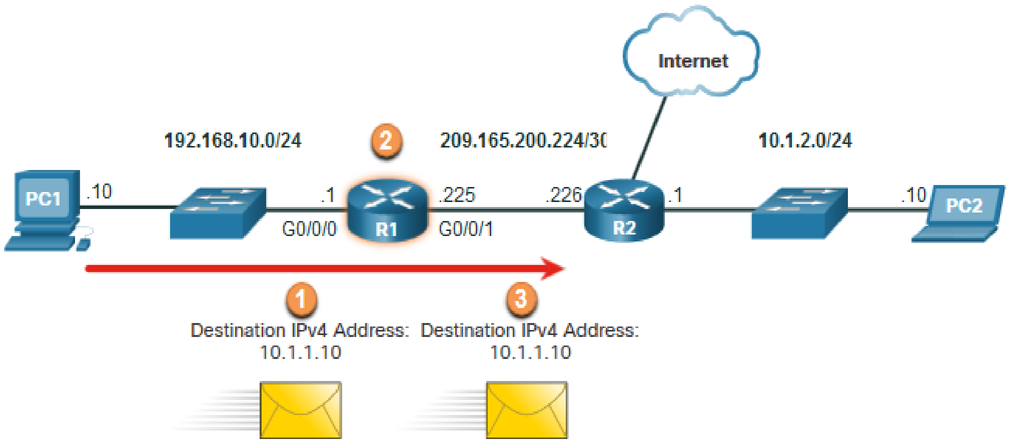
```
C:\Users\PC1> netstat -r

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
```

Introduction to Routing

Router Packet Forwarding Decision

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



R1 Routing Table

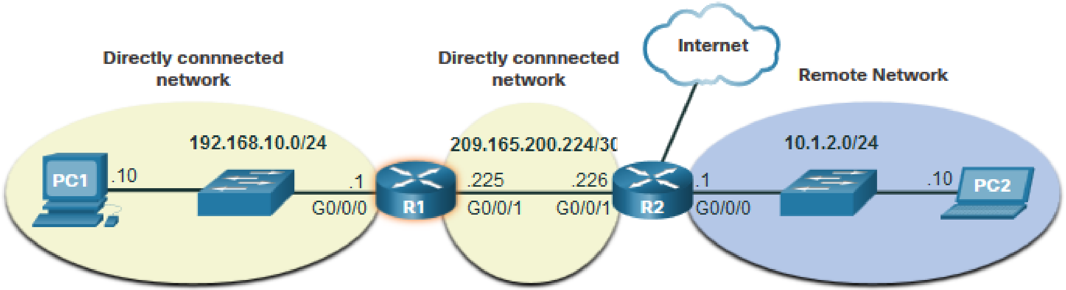
Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
10.1.1.0/24	**via R2**
Default Route 0.0.0.0/0	via R2

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 Router Routing Table

There three types of routes in a router's routing table:

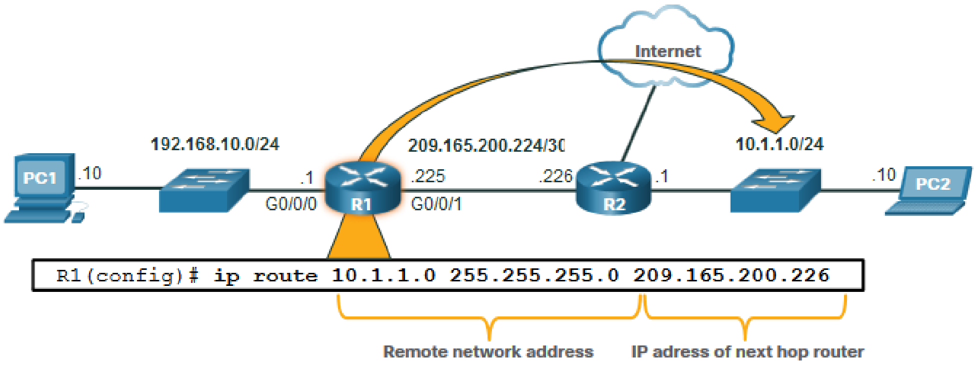
- **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
- **Remote** – These are the routes the router does not have a direct connection and may be learned:
  - Manually – with a static route
  - Dynamically – by using a routing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



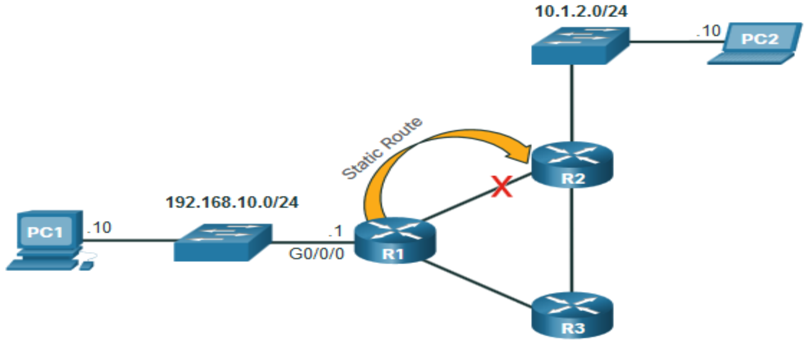
Static Routing

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.



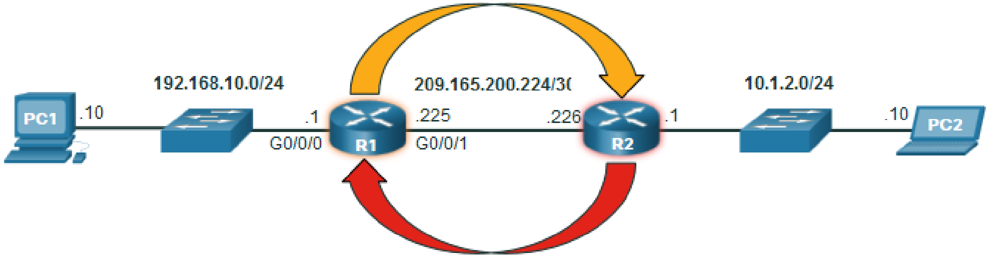
If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

Dynamic Routing

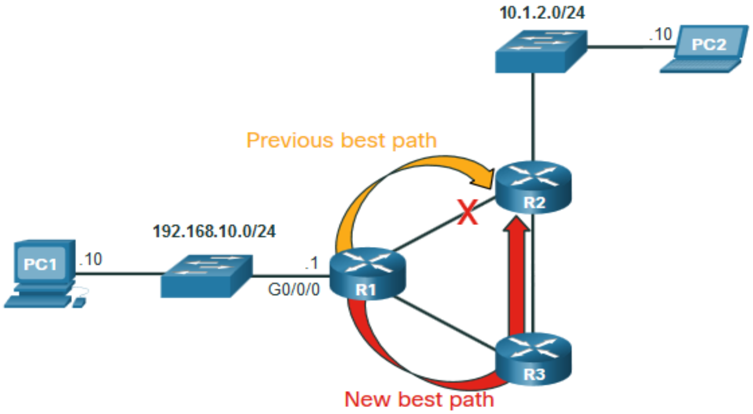
Dynamic Routes Automatically:

- 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.

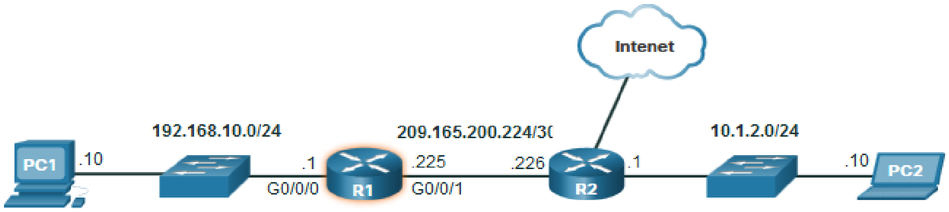
Introduction to an IPv4 Routing Table

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#
```

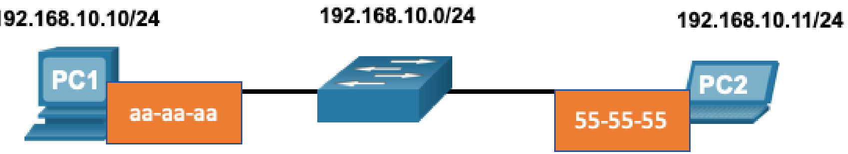
MAC and IP

MAC and IP
Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.

Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network. If a destination IP address is on the same network, the destination MAC address will be that of the destination device.

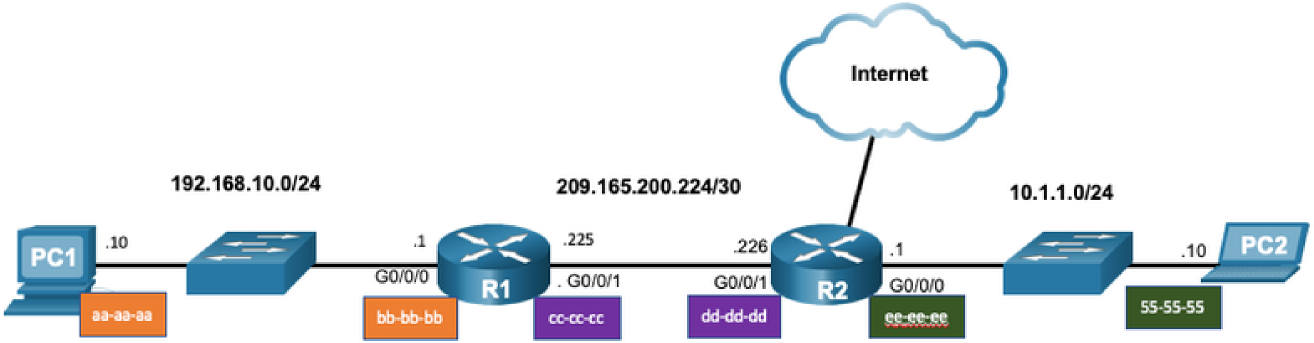


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Destination on Remote Network

When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.

- ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
- ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

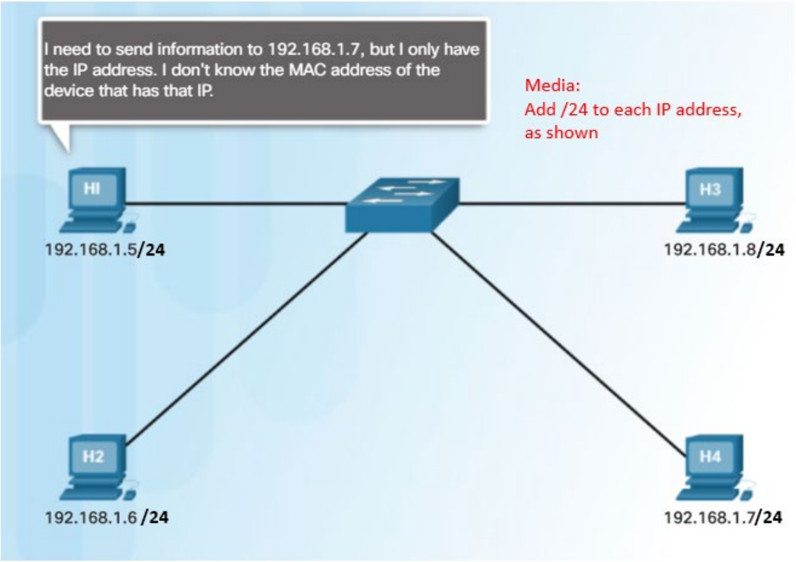
ARP

ARP Overview

A device uses ARP to determine the destination MAC address of a local device when it knows its IPv4 address.

ARP provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining an ARP table of IPv4 to MAC address mappings

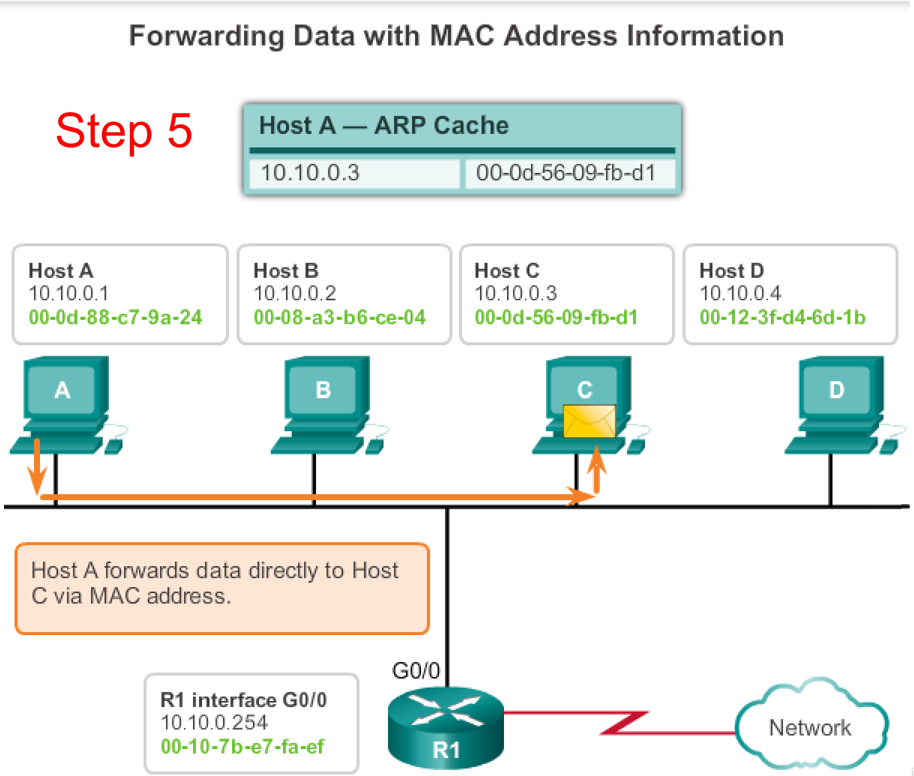


ARP Functions

To send a frame, a device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

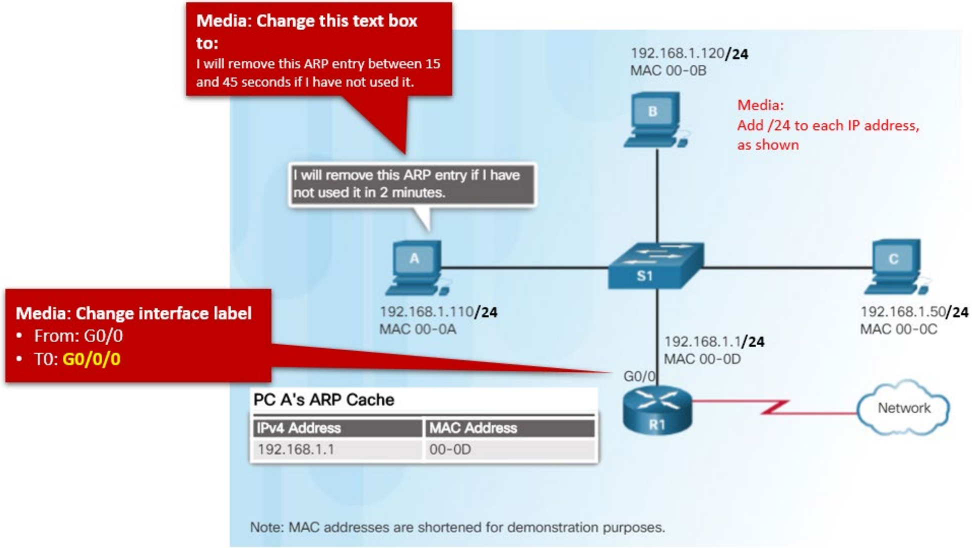
- If the packet's destination IPv4 address is on the same network, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network, the device will search the ARP table for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If there is no ARP table entry is found, then the device sends an ARP request.

ARP Operation



Removing Entries from an ARP Table

- Entries in the ARP table are not permanent and are removed when an ARP cache timer expires after a specified period of time.
- The duration of the ARP cache timer differs depending on the operating system.
- ARP table entries can also be removed manually by the administrator.



ARP Tables on Networking Devices

- The **`show ip arp`** command displays the ARP table on a Cisco router.
- The **`arp –a`** command displays the ARP table on a Windows 10 PC.

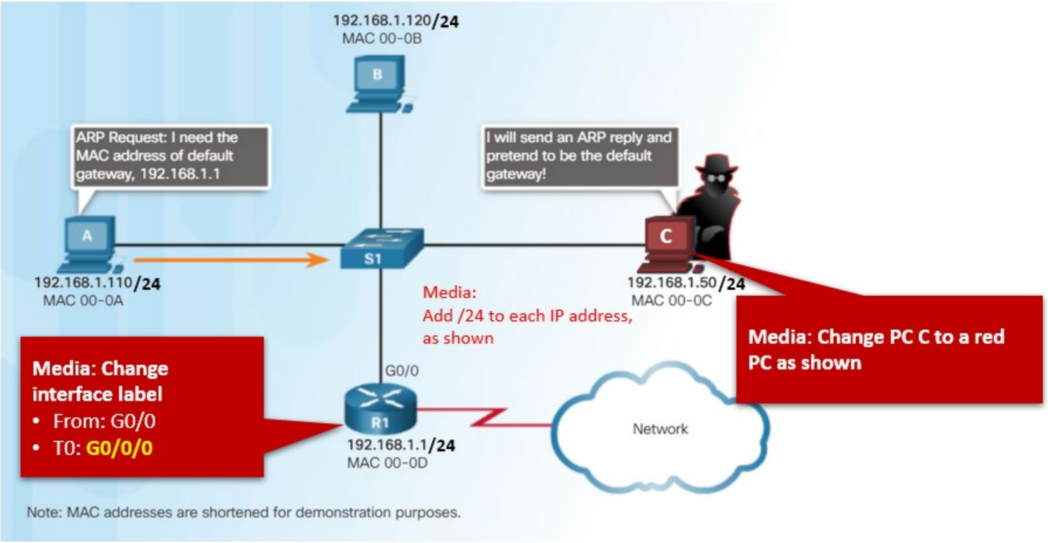
```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

ARP Issues – ARP Broadcasting and ARP Spoofing

- ARP requests are received and processed by every device on the local network.
- Excessive ARP broadcasts can cause some reduction in performance.
- ARP replies can be spoofed by a threat actor to perform an ARP poisoning attack.
- Enterprise level switches include mitigation techniques to protect against ARP attacks.



cisco