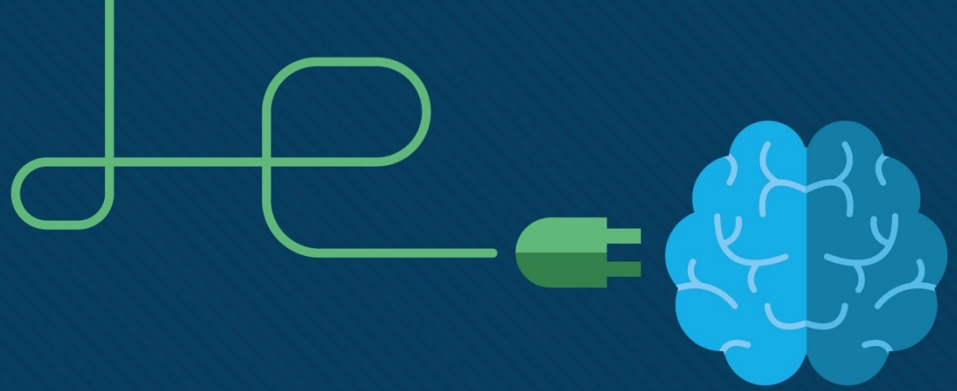


Module 8: Network Layer

Introduction to Networks v7.0
(ITN)

Module 8: Topics

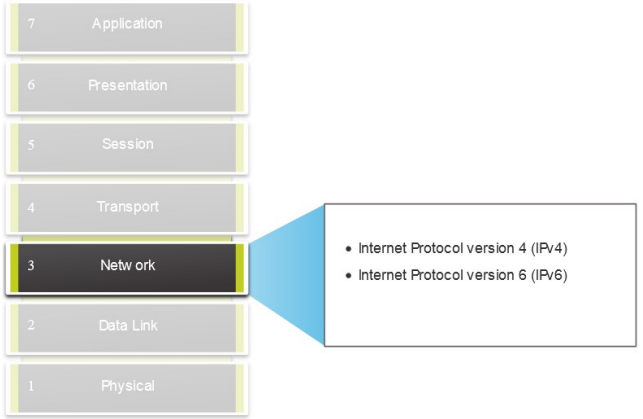
What will I learn to do in this module?

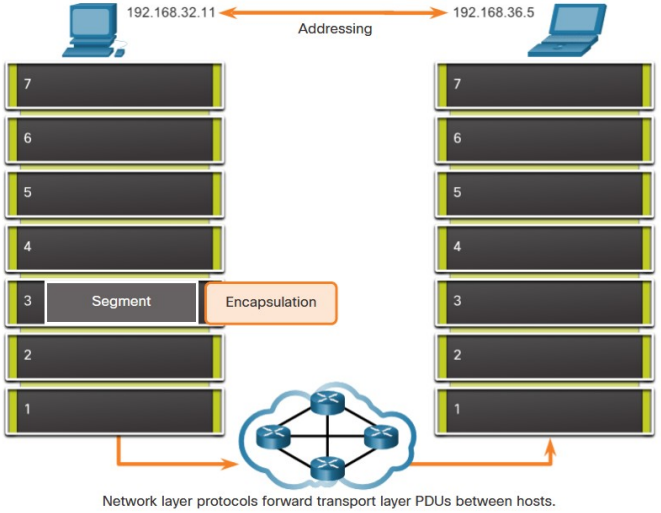
Topic Title	Topic Objective
Network Layer Characteristics	Explain how the network layer uses IP protocols for reliable communications.
IPv4 Packet	Explain the role of the major header fields in the IPv4 packet.
IPv6 Packet	Explain the role of the major header fields in the IPv6 packet.
How a Host Routes	Explain how network devices use routing tables to direct packets to a destination network.
Router Routing Tables	Explain the function of fields in the routing table of a router.

8.1 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

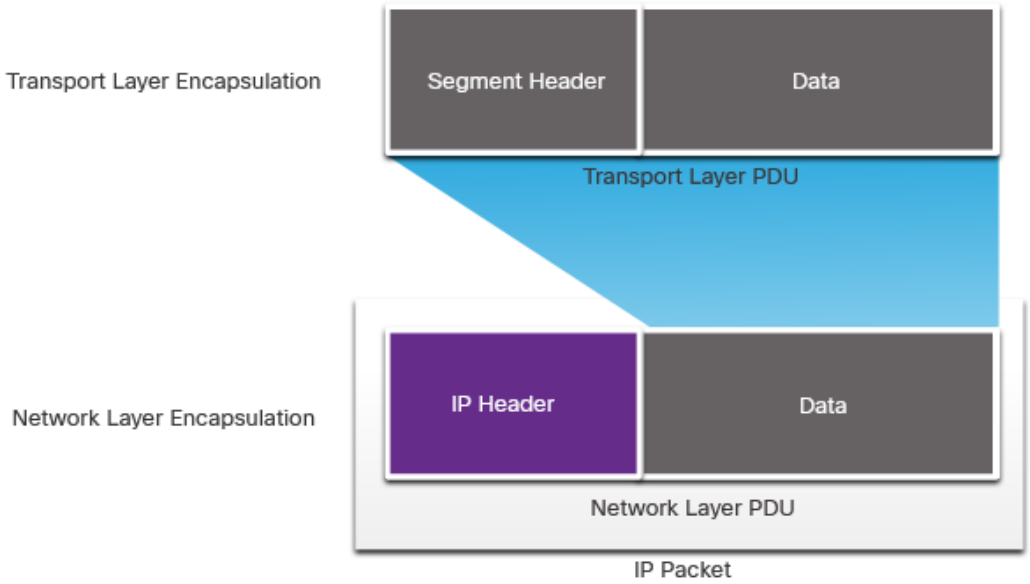




IP Encapsulation

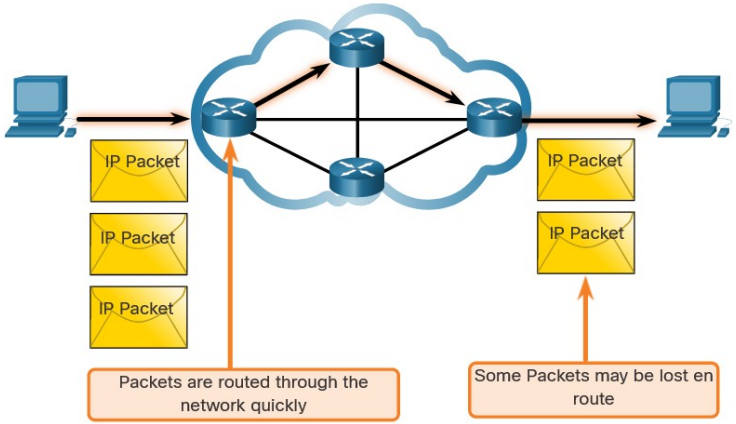
- IP encapsulates the transport layer segment.
- IP can use either an IPv4 or IPv6 packet and not impact the layer 4 segment.
- IP packet will be examined by all layer 3 devices as it traverses the network.
- The IP addressing does not change from source to destination.

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



IP – Internet Protocol

- IETF: RFC 791 (v4), RFC 8200 (v6)
- Unreliable, best effort delivery
- Addressing
  - Network interface
- Routing tables
  - Routing based on longest prefix match



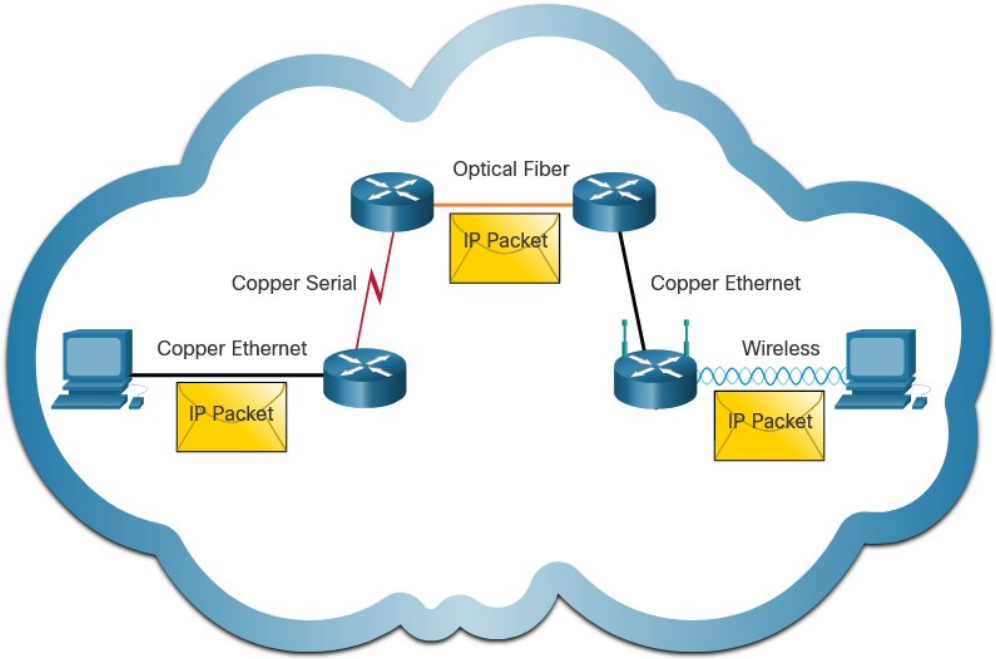
Media Independent

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.

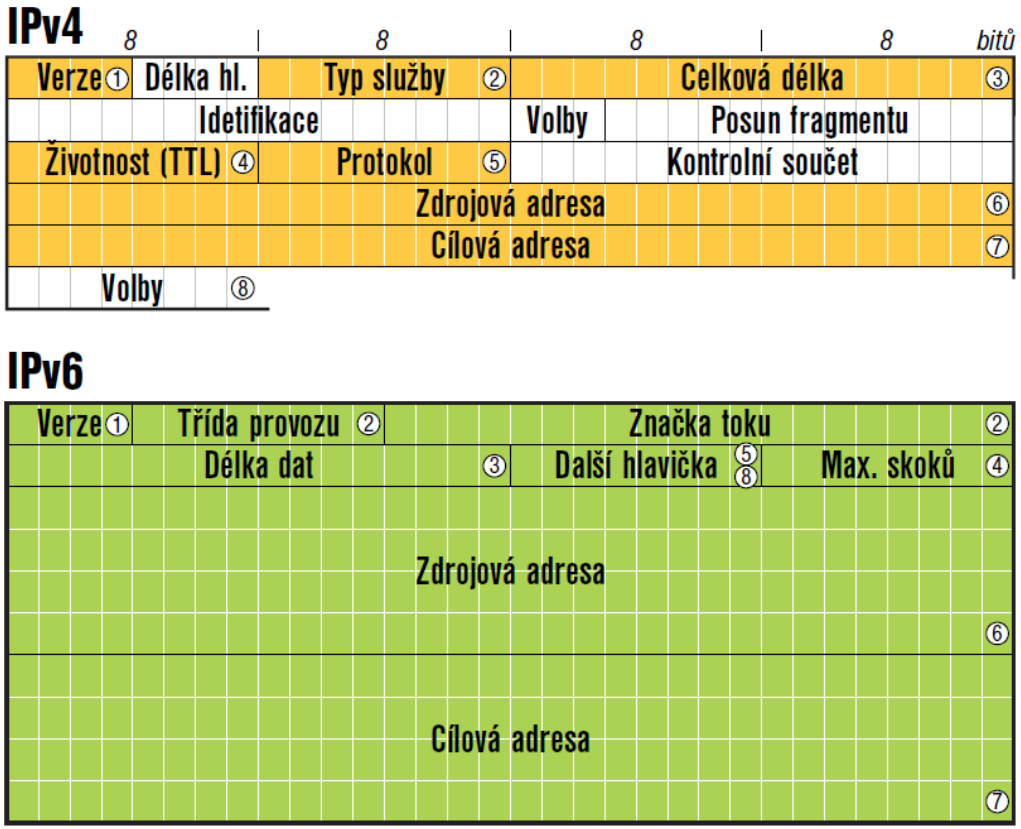
IP is media Independent:

- 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.



8.2 IPv4 Packet
8.3 IPv6 Packets

IPv4 and IPv6 datagram

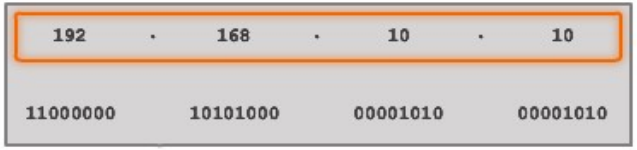


IP addresses

- IPv4: 32 bits, dotted notation, decimal
  - 1.2.3.4
- IPv6: 128 bits, RFC-5952-based notation, hexadecimal
  - 2001:db8::1

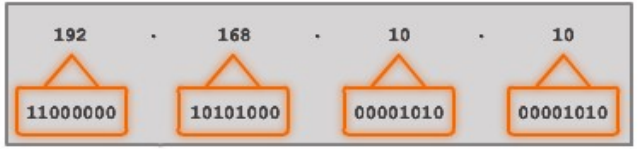
IPv4 Addresses

Dotted Decimal Address



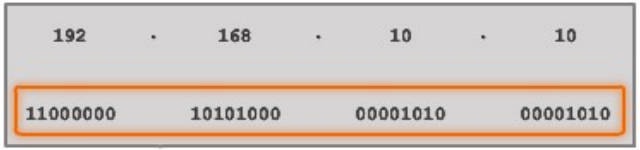
192.168.10.10 is an IP address that is assigned to a computer.

Octets



This address is made up of four different octets.

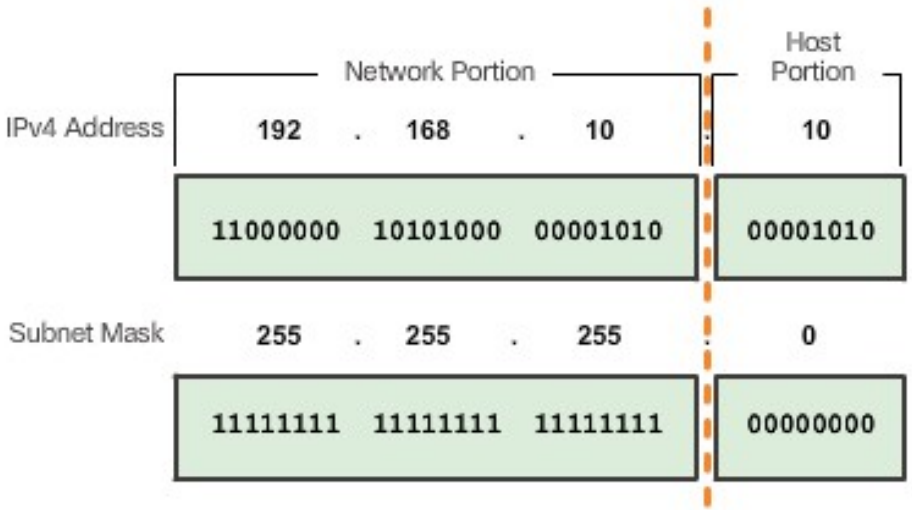
32-Bit Address



The computer stores the address as the entire 32-bit data stream.

Network and Host Portions, The Subnet Mask

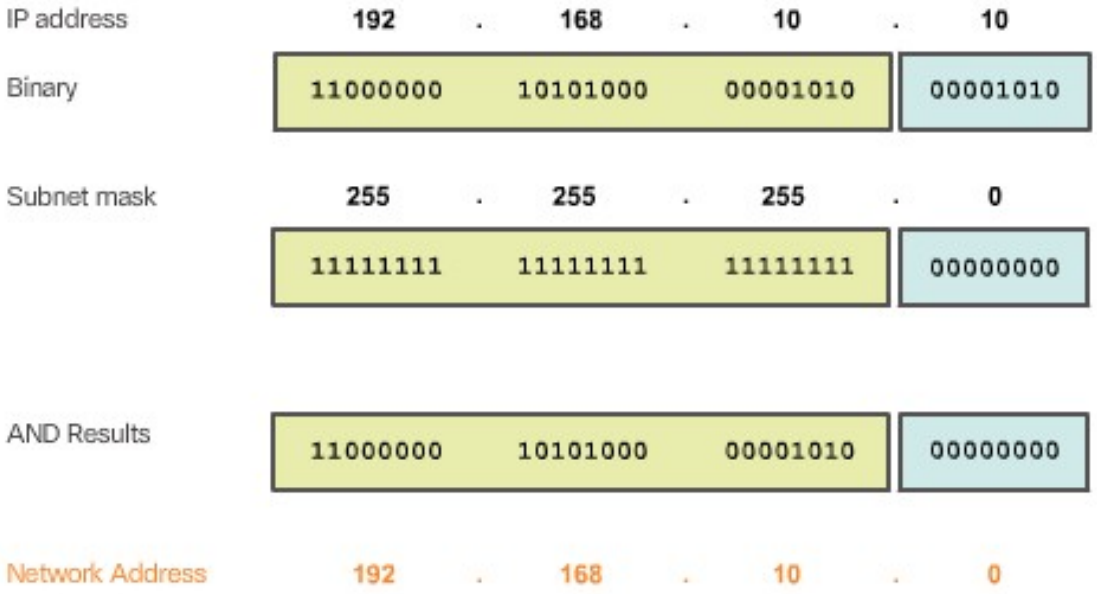
- Comparing the IP Address and the Subnet Mask
- The 1s in the subnet mask identify the network portion while the 0s identify the host portion.



ANDing

- Logical AND is the comparison of two bits.
- ANDing between the IP address and the subnet mask yields the network address.

1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0

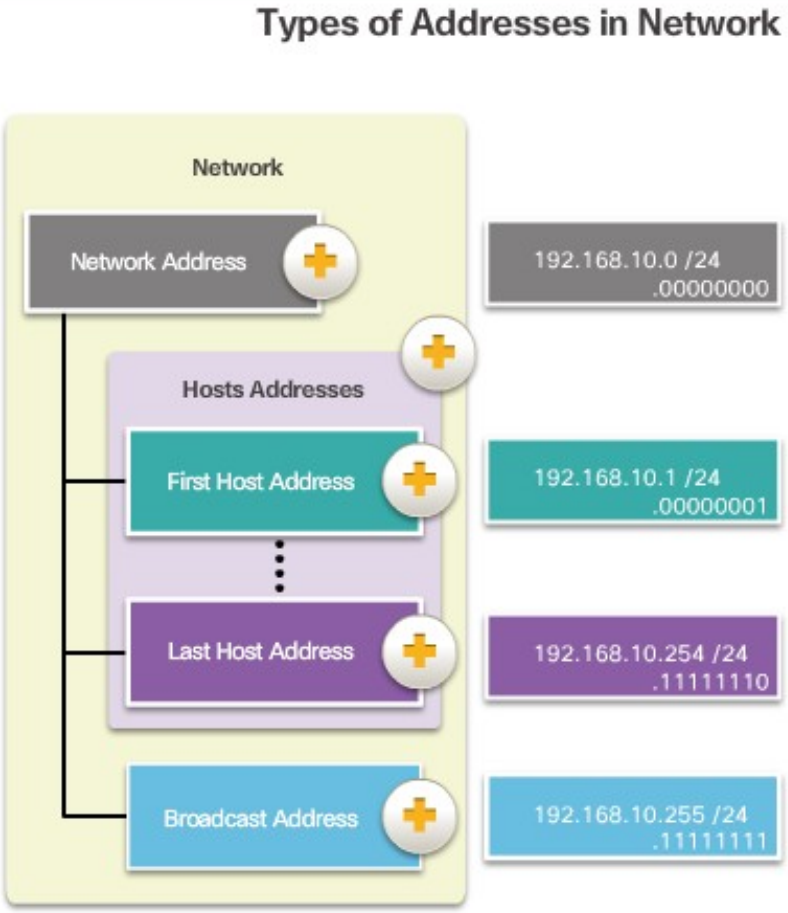


The Prefix Length

- Shorthand method of identifying a subnet mask.
- It is the number of bits set to 1 in the subnet mask.
- Written in “slash notation”, a “/” followed by the number of bits set to 1.

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Network, Host, and Broadcast Addresses



Special Use IPv4 Addresses

- Loopback addresses
  127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254
- Link-Local addresses or Automatic Private IP Addressing (APIPA) addresses
  169.254.0.0 /16 or
  169.254.0.1 to 169.254.255.254
- TEST-NET addresses
  192.0.2.0/24 or 192.0.2.0
  to 192.0.2.255

Legacy Classful Addressing

Class A Specifics	
Address block	0.0.0.0 – 127.0.0.0*
Default Subnet Mask	/8 (255.0.0.0)
Maximum Number of Networks	128
Number of Host per Network	16,777,214
High order bit	0xxxxxxx.___.___.___

* 0.0.0.0 and 127.0.0.0 are reserved and cannot be assigned

Class B Specifics	
Address block	128.0.0.0 – 191.255.0.0
Default Subnet Mask	/16 (255.255.0.0)
Maximum Number of Networks	16,384
Number of Host per Network	65,534
High order bit	10xxxxxx.___.___.___

Class C Specifics	
Address block	192.0.0.0 – 223.255.255.0
Default Subnet Mask	/24 (255.255.255.0)
Maximum Number of Networks	2,097,152
Number of Host per Network	254
High order bit	110xxxxx.___.___.___

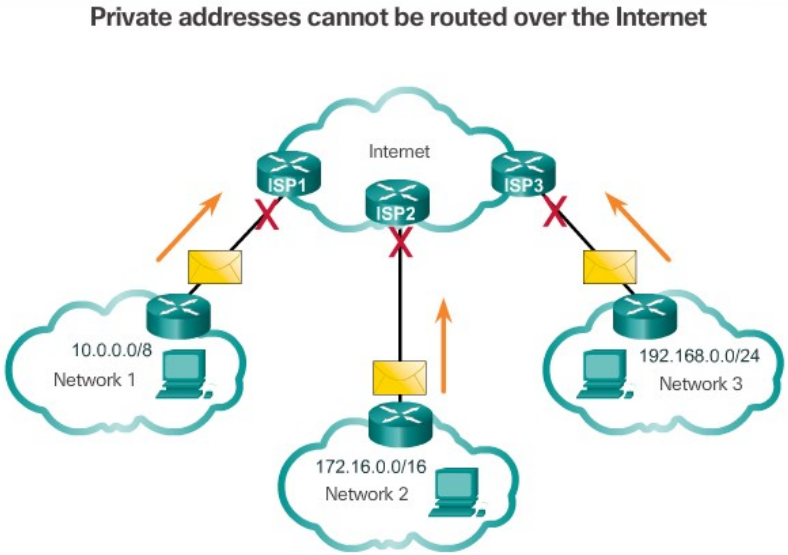
Classless Addressing

- Formal name is Classless Inter-Domain Routing (CIDR, pronounced “cider”).
- Created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address.

Public and Private IPv4 Addresses

Private Addresses:

- 10.0.0.0/8 or 10.0.0.0 to 10.255.255.255
- 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
- 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255



Limitations of IPv4

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

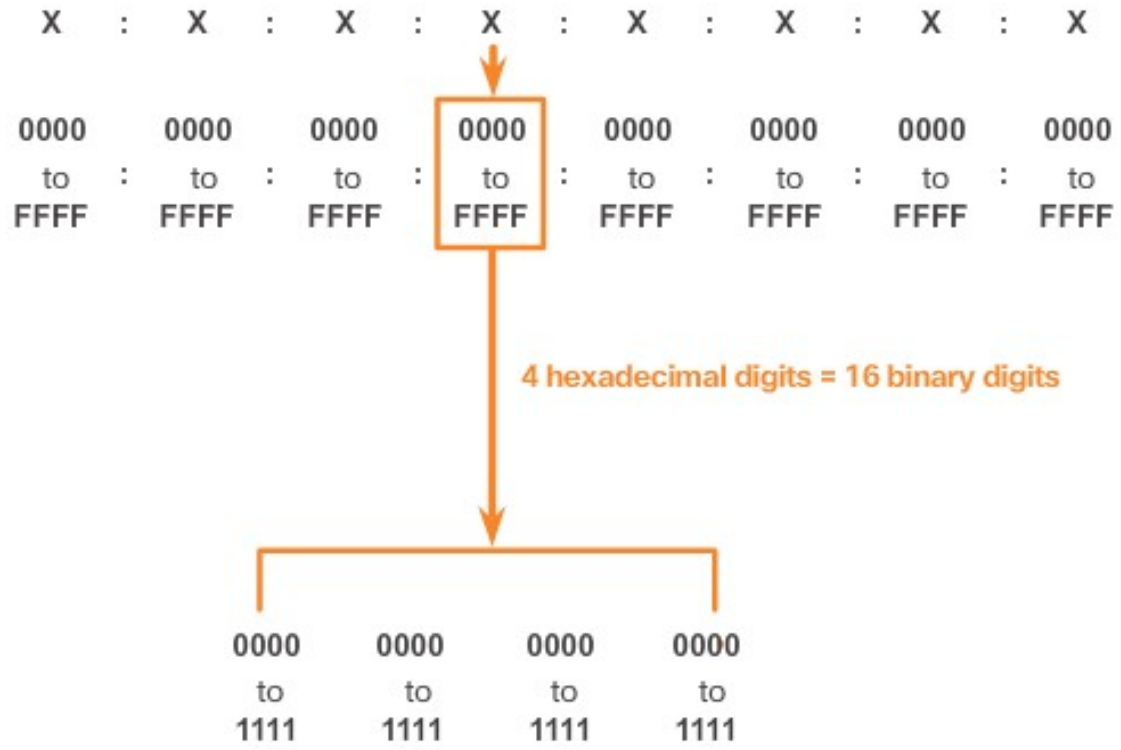
IPv6 Address Representation

Hextets – 4 Hexadecimal digits = 16 binary digits

Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F



IPv6 address canonical representation (RFC 5952)

IPv6 address canonical representation (RFC 5952)

- Full format

2001:0db8:0000:0000:456c:346f:54d6:e931

IPv6 address canonical representation (RFC 5952)

- Full format

2001:0db8:0000:0000:456c:346f:54d6:e931

- Lower case

IPv6 address canonical representation (RFC 5952)

- Full format

2001:0db8:0000:0000:456c:346f:54d6:e931

- Lower case
- Omit leading 0s in 16-bit fields

2001:db8:0:0:456c:346f:54d6:e931

IPv6 address canonical representation (RFC 5952)

- Full format

2001:0db8:0000:0000:456c:346f:54d6:e931

- Lower case
- Omit leading 0s in 16-bit fields

2001:db8:0:0:456c:346f:54d6:e931

- Shorten subsequent 0 fields ::
  - At least two fields
  - The longest group of subsequent fields
    - Equal? → the left most one

2001:db8::456c:346f:54d6:e931

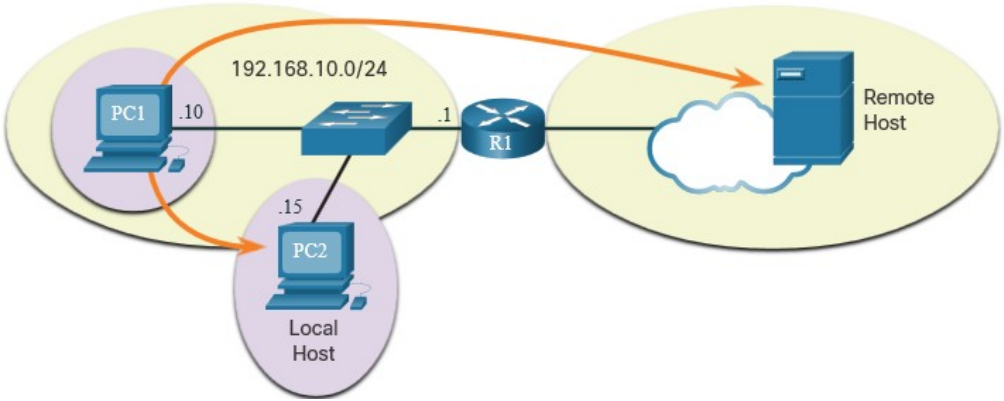
Motivation for canonical representation

- Addresses are writen in configuration files and other files
- Text search
  - Plain string instead of error-prone regex
- Make comparison easier for people without necessary networking knowledge
  - E.g. judges
- Downsides: not all devices support canonical representation
  - Cisco devices included

8.4 How a Host Routes

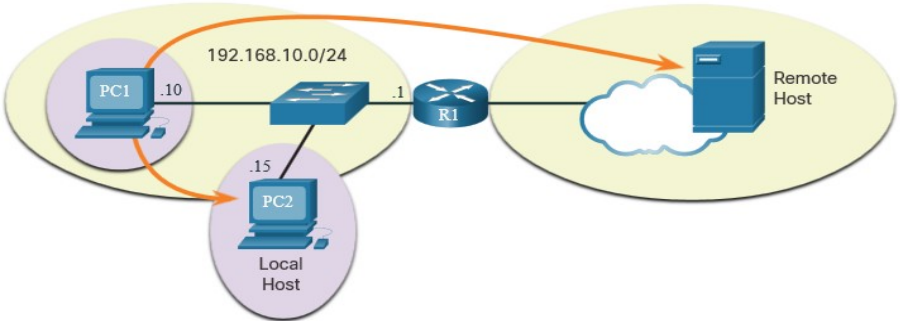
Host Forwarding Decision

- 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.

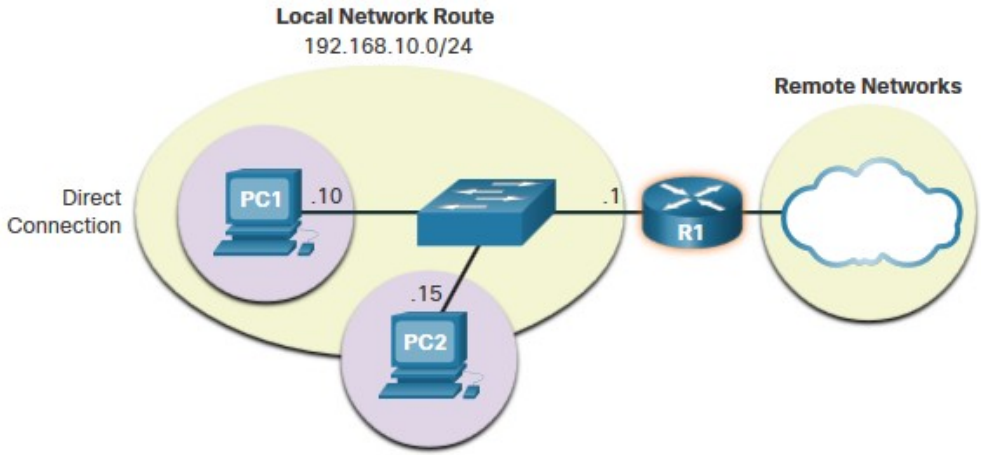
Features of a default gateway (DGW):

- 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

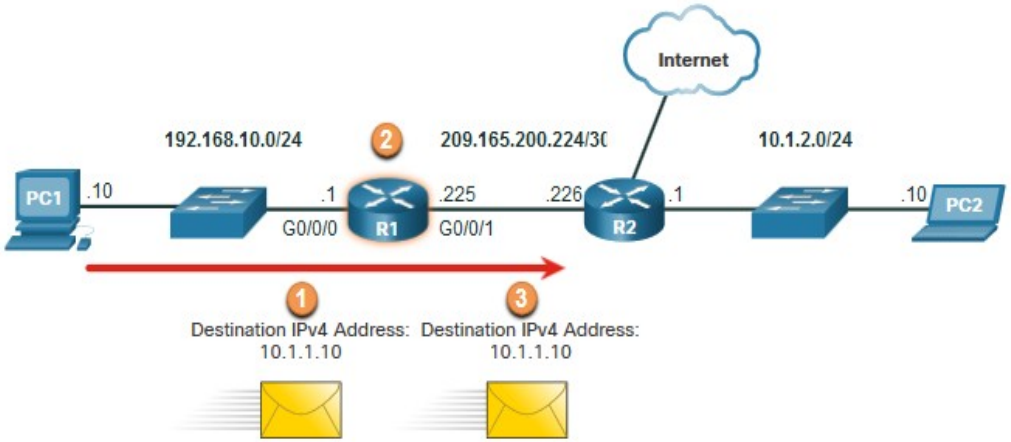
- The host will know the default gateway (DGW) either **statically or through DHCP in IPv4**.
- IPv6 sends the DGW through a **router solicitation (RS)** or can be configured manually.
- A DGW is static route which will be a **last resort route** in the routing table.
- All device on the LAN will need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



8.5 Introduction to Routing

Router Packet Forwarding Decision

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



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.

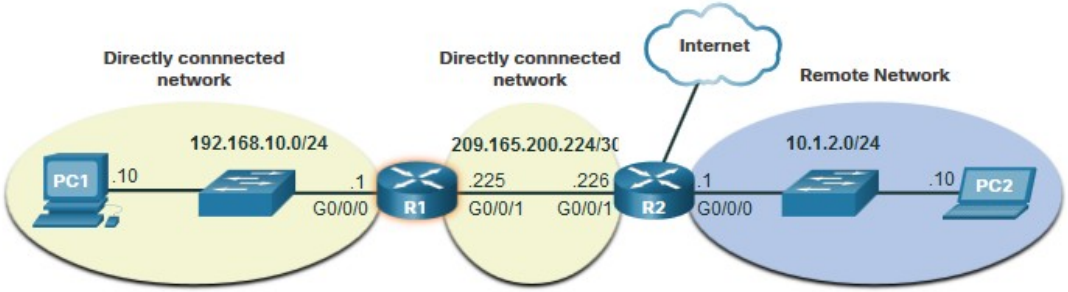
R1 Routing Table

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

IP Router Routing Table

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

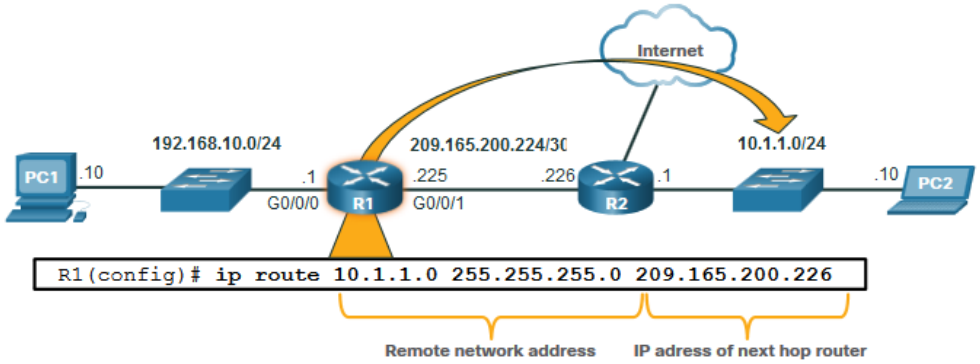
- **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
- **Remote** – These are the routes the router does not have a direct connection and may be learned:
  - Manually – with a static route
  - Dynamically – by using a routing 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



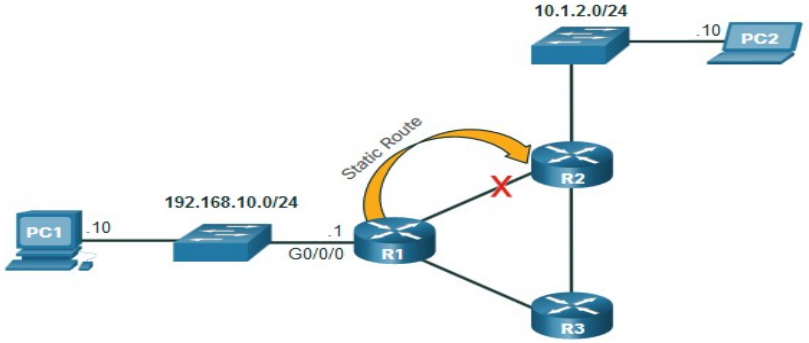
Static Routing

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.



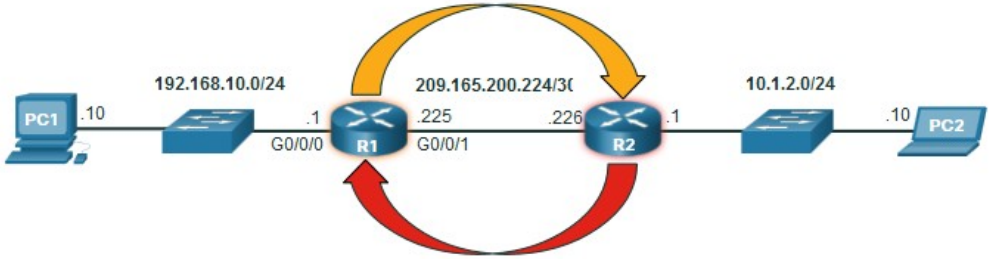
If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

Dynamic Routing

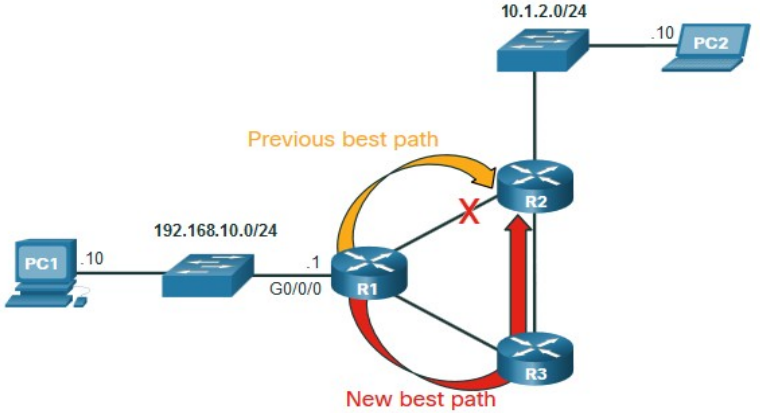
Dynamic Routes Automatically:

- 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.

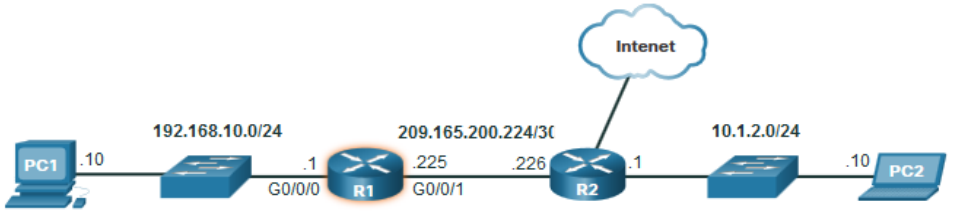
Introduction to an IPv4 Routing Table

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

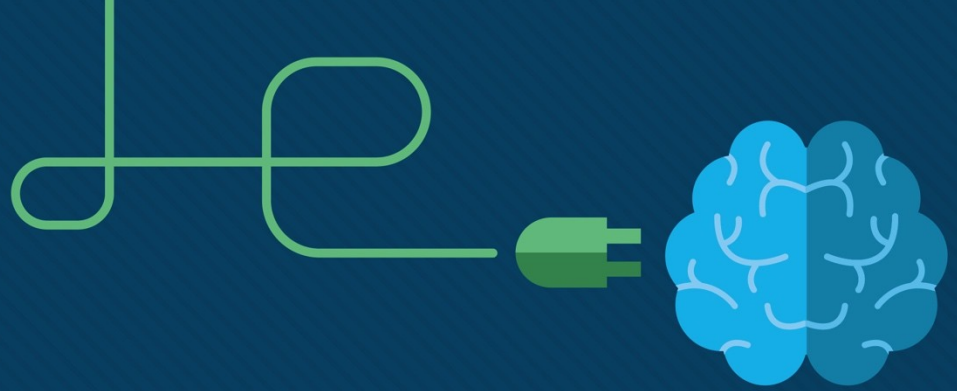
- **L** - Directly connected local interface IP address
- **C** – Directly connected network
- **S** – Static route was manually configured by an administrator
- **O** – OSPF
- **D** – EIGRP

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#
```



Module 13: ICMP

Introduction of Networks v7.0
(ITN)

Module Objectives

Module Title: ICMP

Module Objective: Use various tools to test network connectivity.

Topic Title	Topic Objective
ICMP Messages	Explain how ICMP is used to test network connectivity.
Ping and Traceroute Testing	Use ping and traceroute utilities to test network connectivity.

13.1 ICMP Messages

ICMPv4 and ICMPv6 Messages

- Internet Control Message Protocol (ICMP) provides feedback about issues related to the processing of IP packets under certain conditions.
- ICMPv4 is the messaging protocol for IPv4. ICMPv6 is the messaging protocol for IPv6 and includes additional functionality.
- The ICMP messages common to both ICMPv4 and ICMPv6 include:
  - **Host reachability**
  - Destination or Service **Unreachable**
  - **Time exceeded**

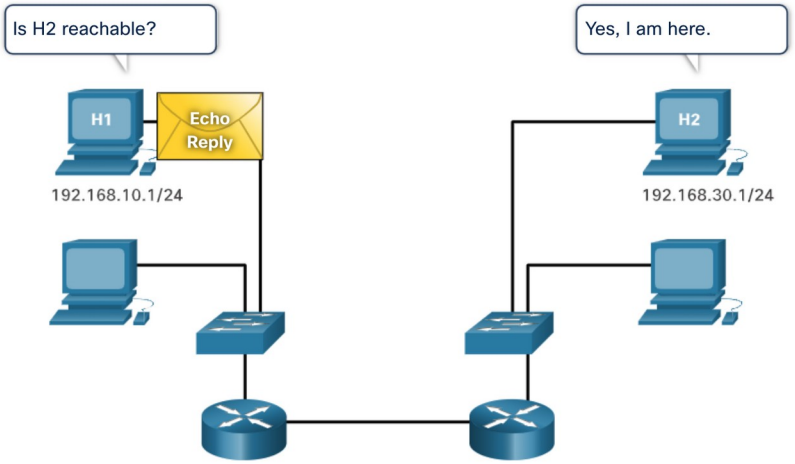
Note: ICMPv4 messages are not required and are often not allowed within a network for security reasons.

Host Reachability

ICMP Echo Message can be used to test the reachability of a host on an IP network.

In the example:

- The local host sends an ICMP Echo Request to a host.
- If the host is available, the destination host responds with an Echo Reply.



13.2 Ping and Traceroute Tests

Ping – Test Connectivity

- The **ping** command is an IPv4 and IPv6 testing utility that uses ICMP echo request and echo reply messages to test connectivity between hosts and provides a summary that includes the success rate and average round-trip time to the destination.
- If a reply is not received within the timeout, ping provides a message indicating that a response was not received.
- It is common for the first ping to timeout if address resolution (ARP or ND) needs to be performed before sending the ICMP Echo Request.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

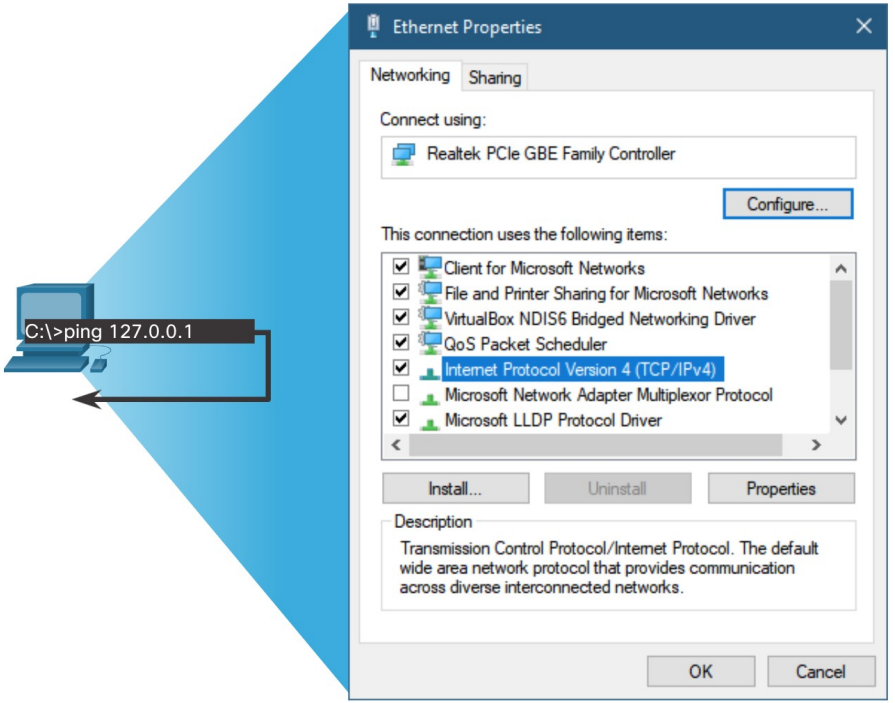
```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Ping the Loopback

Ping can be used to test the internal configuration of IPv4 or IPv6 on the local host. To do this, **ping** the local loopback address of 127.0.0.1 for IPv4 (::1 for IPv6).

- A response from 127.0.0.1 for IPv4, or ::1 for IPv6, indicates that IP is properly installed on the host.
- An error message indicates that TCP/IP is not operational on the host.

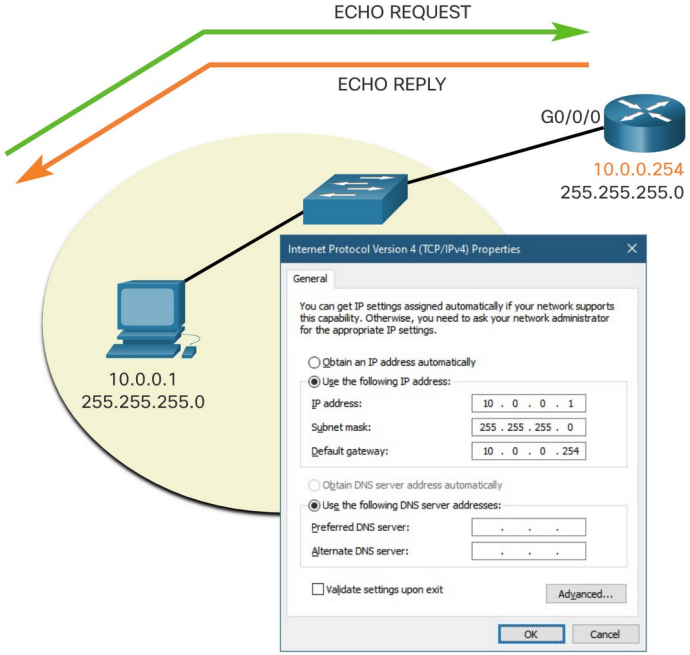


Ping the Default Gateway

The **ping** command can be used to test the ability of a host to communicate on the local network.

The default gateway address is most often used because the router is normally always operational.

- A successful **ping** to the default gateway indicates that the host and the router interface serving as the default gateway are both operational on the local network.
- If the default gateway address does not respond, a **ping** can be sent to the IP address of another host on the local network that is known to be operational.

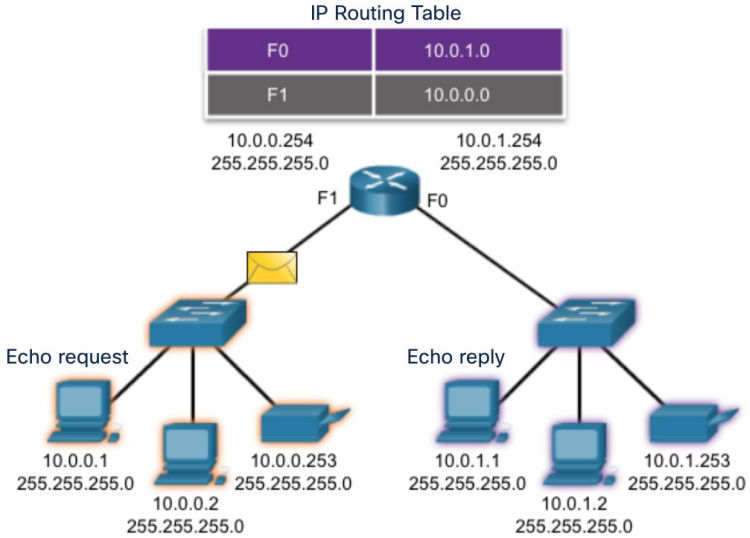


Ping a Remote Host

Ping can also be used to test the ability of a local host to communicate across an internetwork.

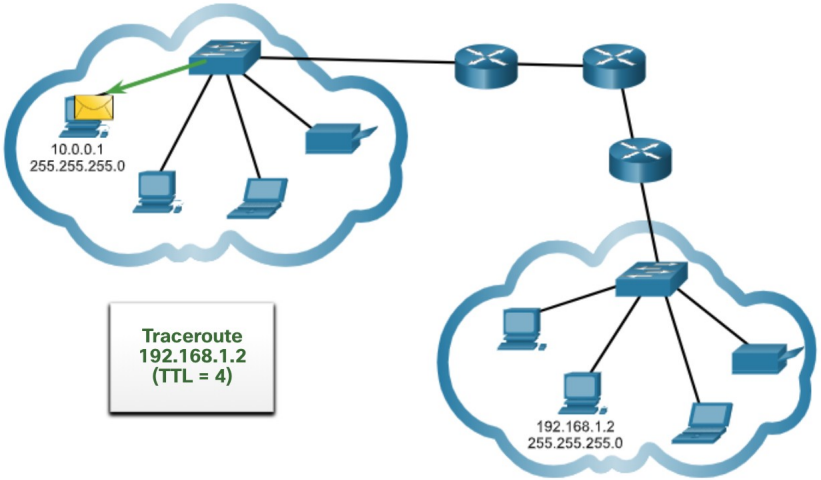
A local host can ping a host on a remote network. A successful **ping** across the internetwork confirms communication on the local network.

Note: Many network administrators limit or prohibit the entry of ICMP messages therefore, the lack of a **ping** response could be due to security restrictions.



Traceroute – Test the Path

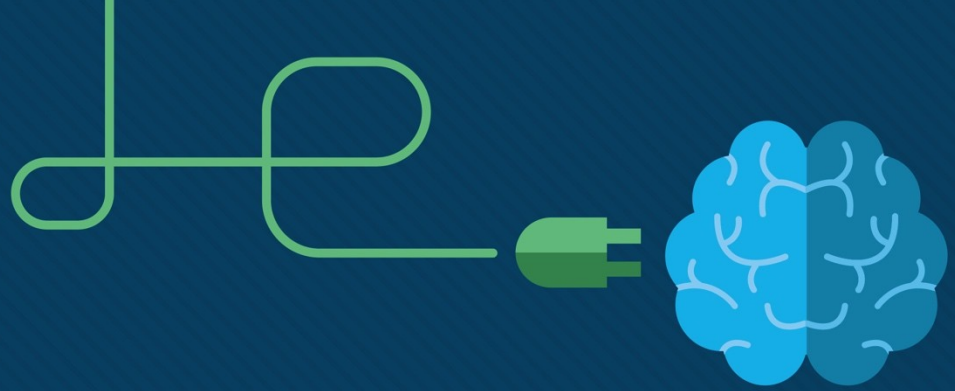
- Traceroute (**tracert**) is a utility that is used to test the path between two hosts and provide a list of hops that were successfully reached along that path.




```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2     1 msec     0 msec     0 msec
  2   192.168.20.2     2 msec     1 msec     0 msec
  3   192.168.30.2     1 msec     0 msec     0 msec
  4   192.168.40.2     0 msec     0 msec     0 msec
```

Note: Traceroute makes use of a function of the TTL field in IPv4 and the Hop Limit field in IPv6 in the Layer 3 headers, along with the ICMP Time Exceeded message.



Module 11: IPv4 Addressing

Introduction to Networks v7.0
(ITN)

Module Objectives

Module Title: IPv4 Addressing

Module Objective: Calculate an IPv4 subnetting scheme to efficiently segment your network.

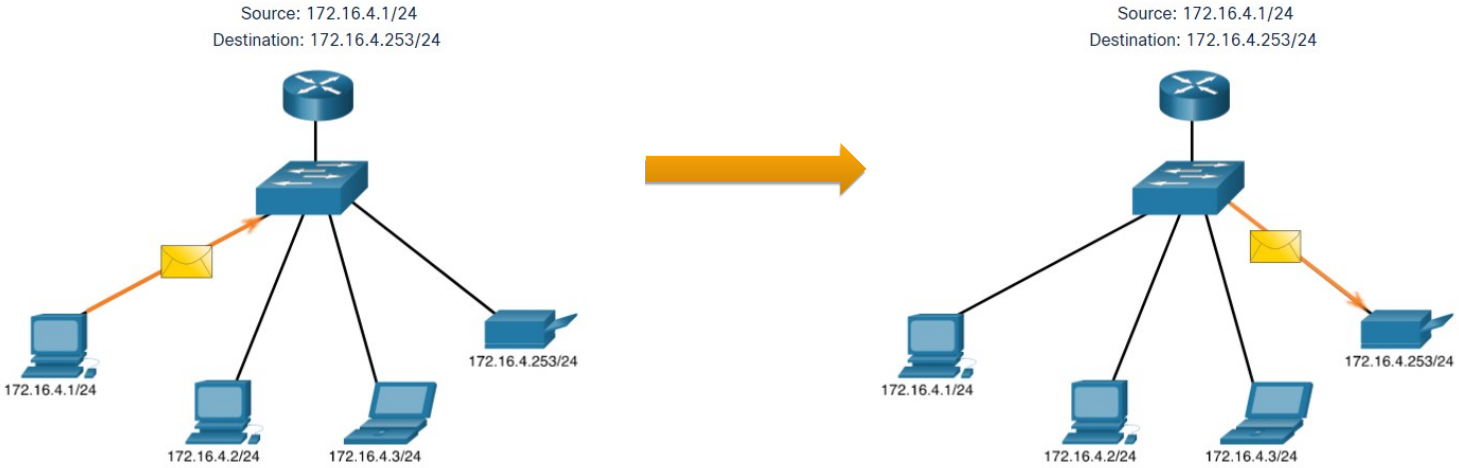
Topic Title	Topic Objective
IPv4 Address Structure ✓	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
Types of IPv4 Addresses ✓	Explain public, private, and reserved IPv4 addresses.
Network Segmentation	Explain how subnetting segments a network to enable better communication.
Subnet an IPv4 Network	Calculate IPv4 subnets for a /24 prefix.

11.2 IPv4 Unicast, Broadcast, and Multicast

Unicast

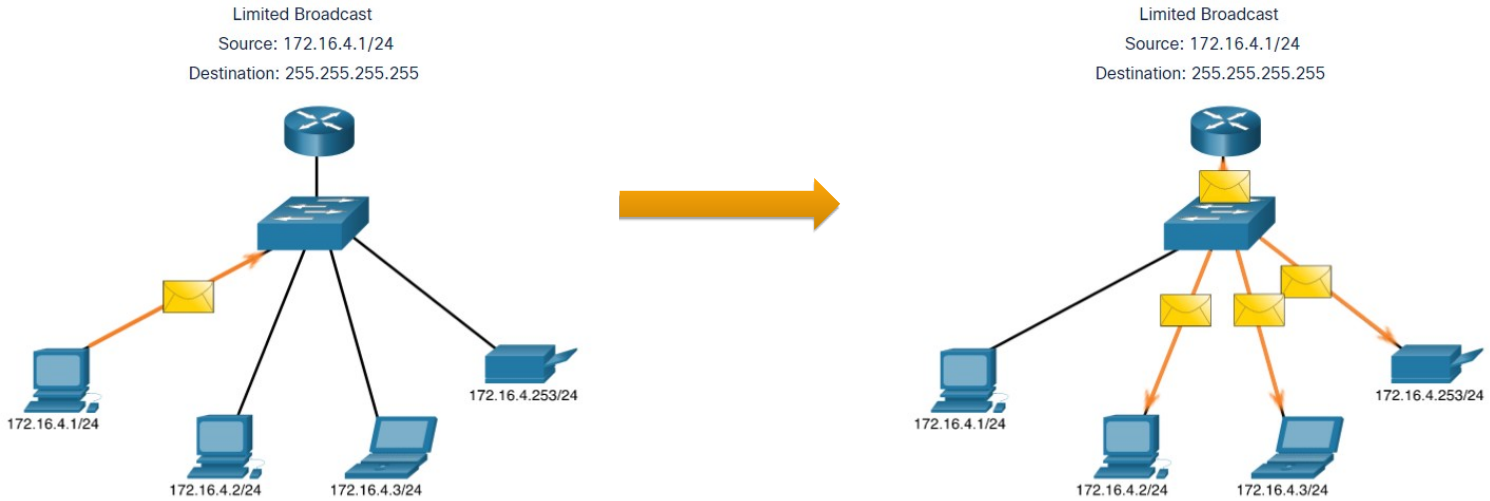
- Unicast transmission is sending a packet to one destination IP address.

- For example, the PC at 172.16.4.1 sends a unicast packet to the printer at 172.16.4.253.



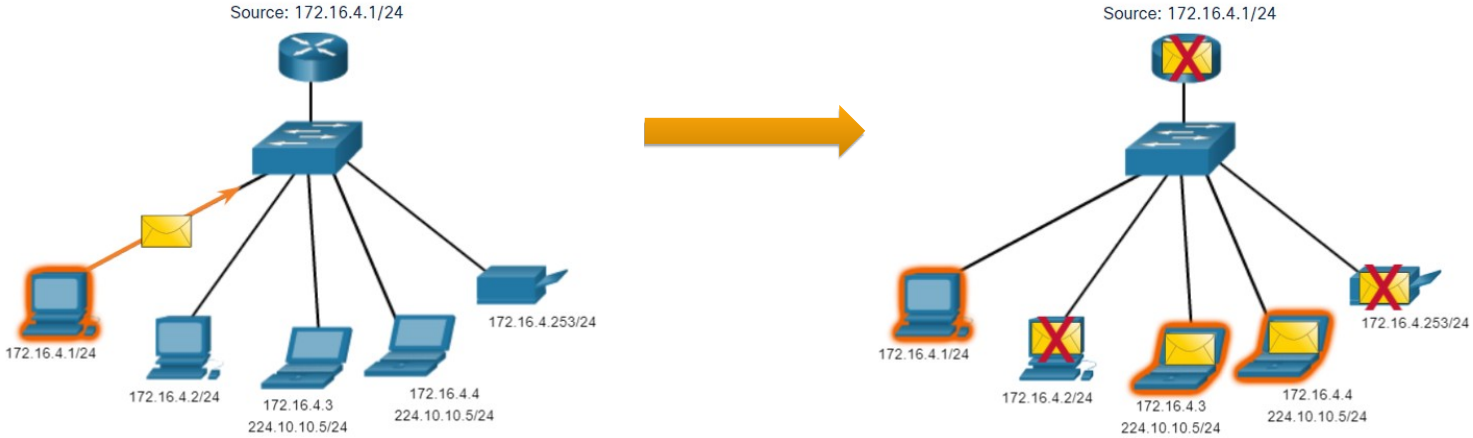
Broadcast

- Broadcast transmission is sending a packet to all other destination IP addresses.
- For example, the PC at 172.16.4.1 sends a broadcast packet to all IPv4 hosts.



Multicast

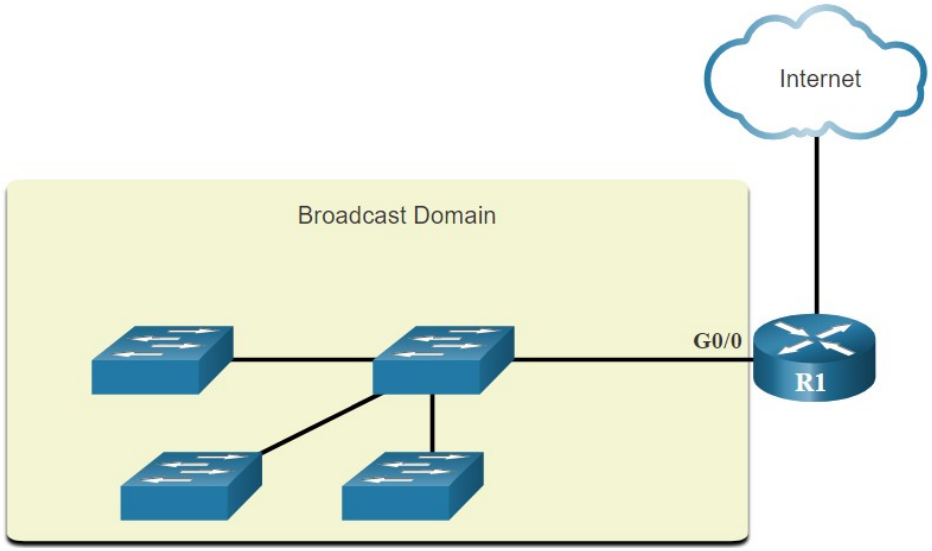
- Multicast transmission is sending a packet to a multicast address group.
- For example, the PC at 172.16.4.1 sends a multicast packet to the multicast group address 224.10.10.5.



11.4 Network Segmentation

Broadcast Domains and Segmentation

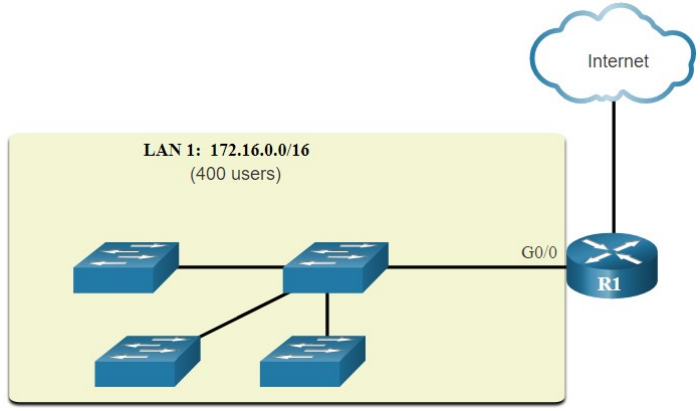
- Many protocols use broadcasts or multicasts (e.g., ARP use broadcasts to locate other devices, hosts send DHCP discover broadcasts to locate a DHCP server.)
- Switches propagate broadcasts out all interfaces except the interface on which it was received.

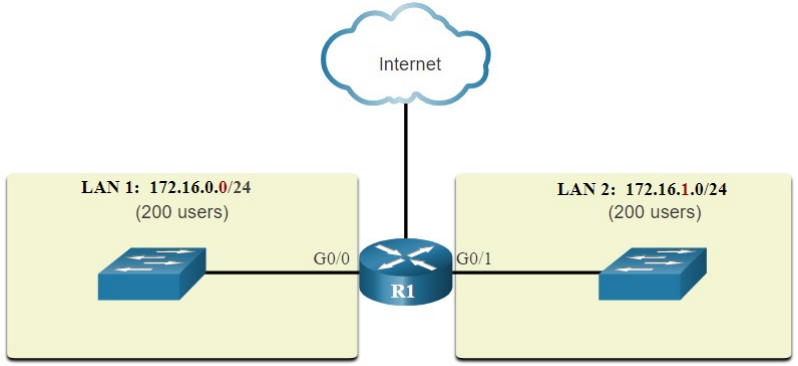


- The only device that stops broadcasts is a router.
- Routers do not propagate broadcasts.
- Each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

Problems with Large Broadcast Domains

- A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network.
- The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting.
- Dividing the network address 172.16.0.0 /16 into two subnets of 200 users each: 172.16.0.0 /24 and 172.16.1.0 /24.
- Broadcasts are only propagated within the smaller broadcast domains.



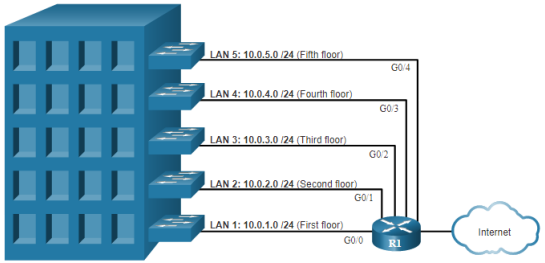


Reasons for Segmenting Networks

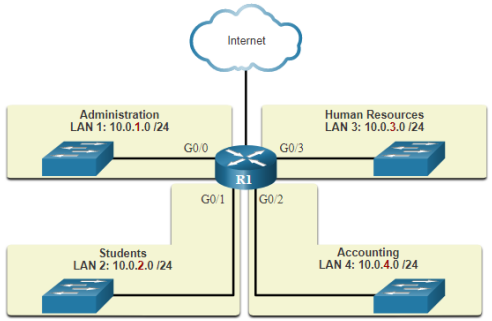
- Subnetting reduces overall network traffic and improves network performance.
- It can be used to implement security policies between subnets.
- Subnetting reduces the number of devices affected by abnormal broadcast traffic.

- Subnets are used for a variety of reasons including by:

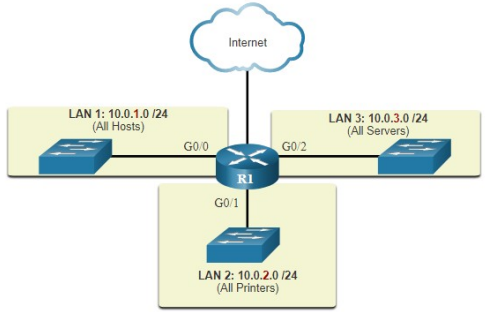
Location



Group or Function



Device Type



11.5 Subnet an IPv4 Network

Subnet on an Octet Boundary

- Networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Notice that using longer prefix lengths decreases the number of hosts per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	**255**.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16,777,214
/16	**255.255**.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65,534
/24	**255.255.255**.0	**nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh **11111111.11111111.11111111**.00000000	254

Subnet on an Octet Boundary (Cont.)

- In the first table 10.0.0.0/8 is subnetted using /16 and in the second table, a /24 mask.

Subnet Address (256 Possible Subnets)	**Host Range** (65,534 possible hosts per subnet)	**Broadcast**
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
…	…	…
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Subnet Address (65,536 Possible Subnets)	**Host Range** (254 possible hosts per subnet)	**Broadcast**
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
…	…	…
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

Subnet within an Octet Boundary

- Refer to the table to see six ways to subnet a /24 network.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

11.7 Subnet to Meet Requirements

Subnet to Meet Requirements
Minimize Unused Host IPv4 Addresses and Maximize Subnets

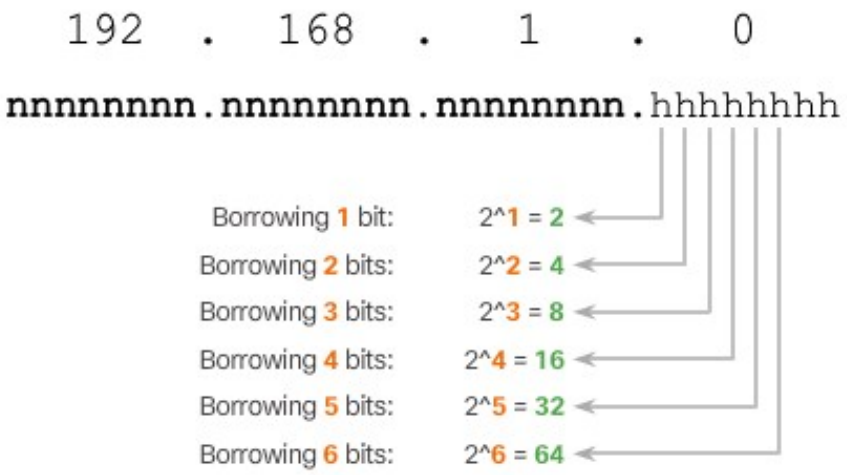
There are two considerations when planning subnets:

- The number of host addresses required for each network
- The number of individual subnets needed

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

Subnetting Formulas

To calculate the number of subnets.



2^b

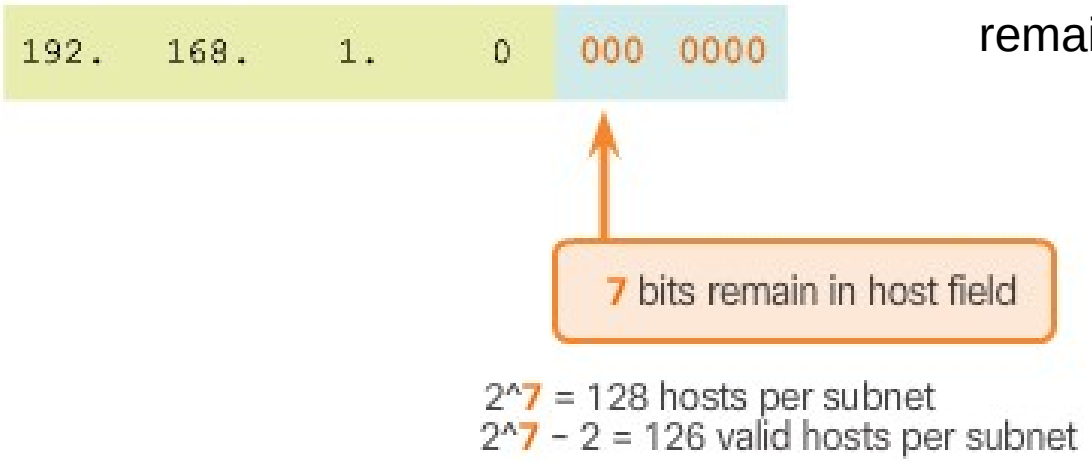
b ~ bits borrowed

Subnetting Formulas (cont.)

To calculate the number of hosts.

$$2^{h'}-2$$

h' ~ number of bits remaining in the host field

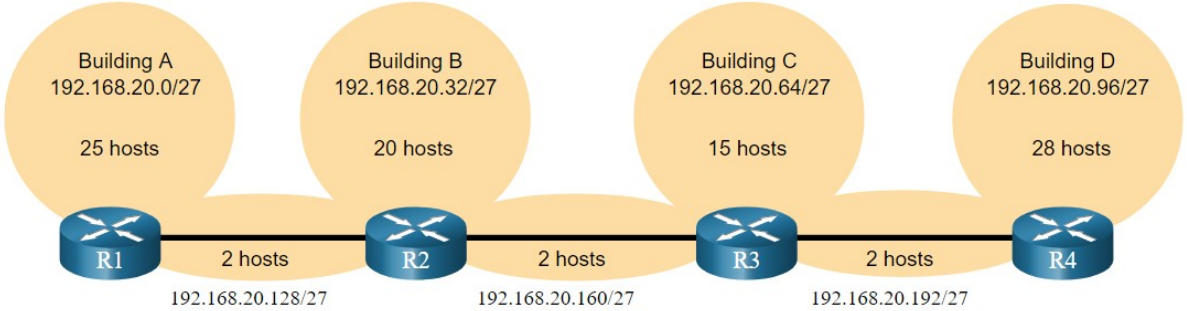


11.8 VLSM

IPv4 Address Conservation

Given the topology, 7 subnets are required (i.e, four LANs and three WAN links) and the largest number of host is in Building D with 28 hosts.

- A /27 mask would provide 8 subnets of 30 host IP addresses and therefore support this topology.



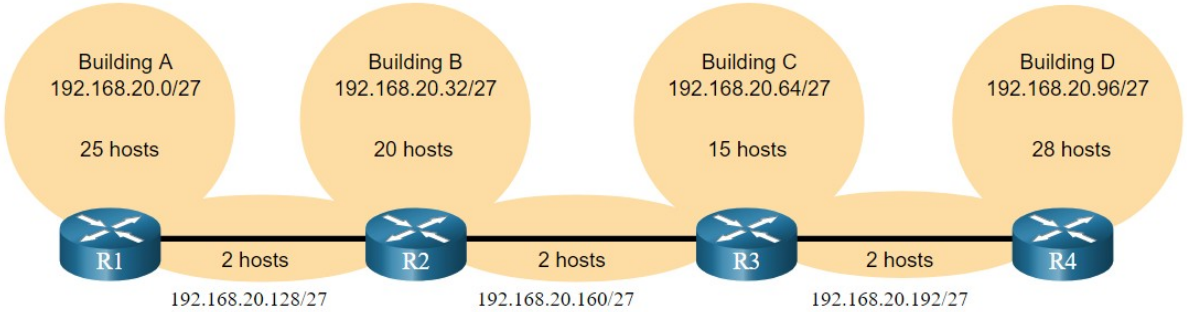
IPv4 Address Conservation (Cont.)

However, the point-to-point WAN links only require two addresses and therefore waste 28 addresses each for a total of 84 unused addresses.

Host portion
2^5 – 2 = 30 host IP addresses per subnet

30 – 2 = 28
Each WAN subnet wastes 28 addresses

28 x 3 = 84
84 addresses are unused



- Applying a traditional subnetting scheme to this scenario is not very efficient and is wasteful.

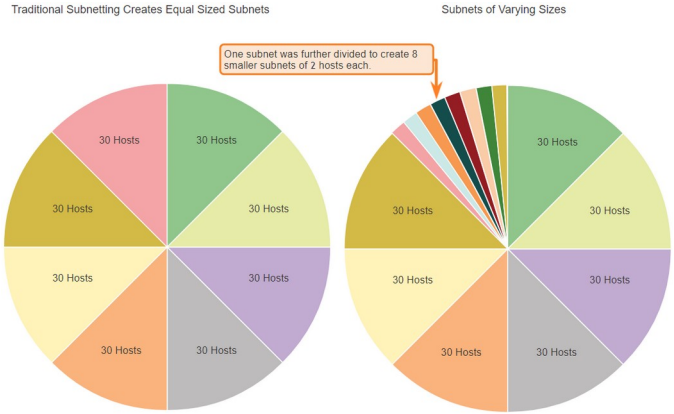
- VLSM was developed to avoid wasting addresses by enabling us to subnet a subnet.

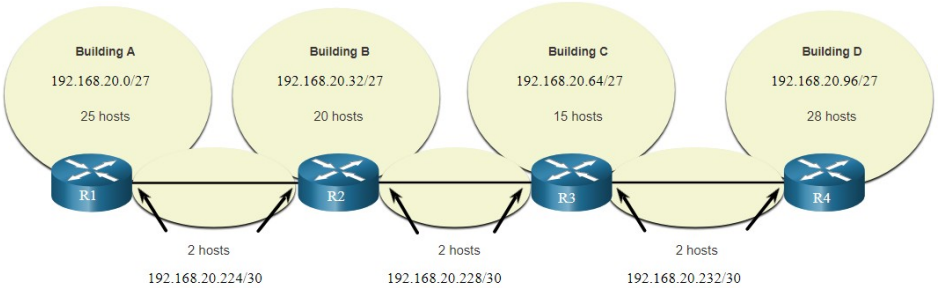
VLSM

- The left side displays the traditional subnetting scheme (i.e., the same subnet mask) while the right side illustrates how VLSM can be used to subnet a subnet and divided the last subnet into eight /30 subnets.

- When using VLSM, always begin by satisfying the host requirements of the largest subnet and continue subnetting until the host requirements of the smallest subnet are satisfied.

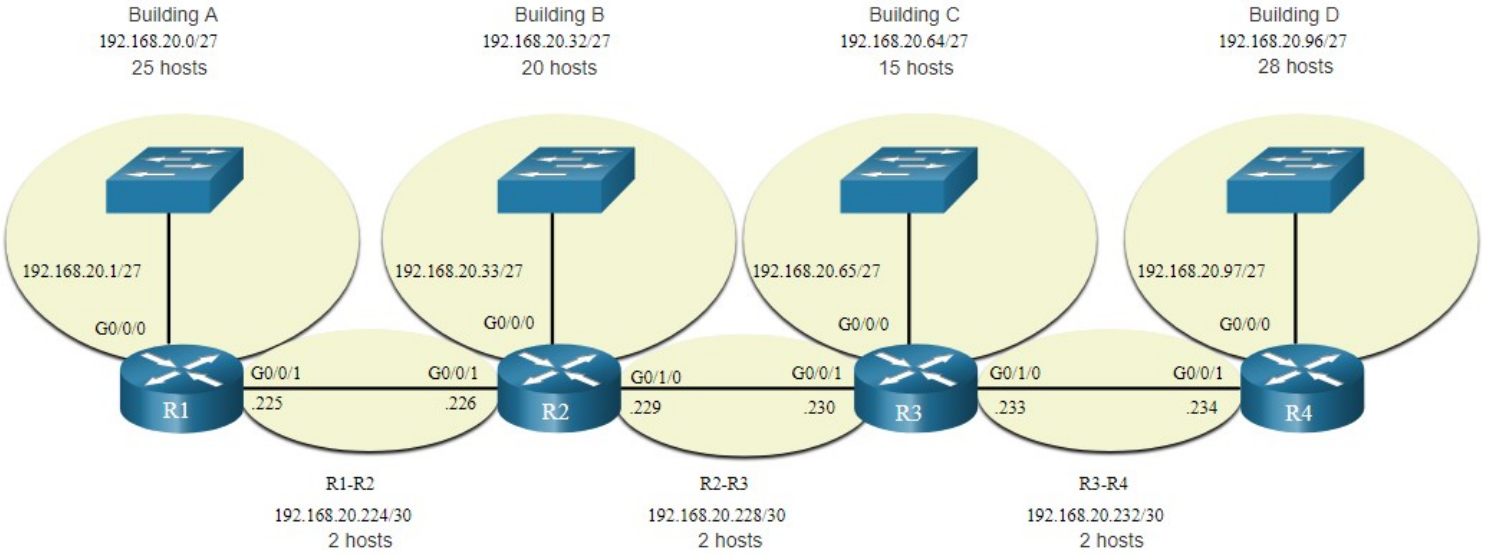
- The resulting topology with VLSM applied.





VLSM Topology Address Assignment

- Using VLSM subnets, the LAN and inter-router networks can be addressed without unnecessary waste as shown in the logical topology diagram.



IP Addressing and Subnetting IP networks examples

Libor Polčák
Vysoké učení technické v Brně, Fakulta informačních technologií
Božetěchova 1/2, 612 66 Brno
ipolcak@fit.vutbr.cz

Cvičebnice v souborech předmětu

- Příklady (examples)
  - Ip_Addressing_and_Subnetting_Workbook_-_Student_Version_v2_0.pdf
  - VLSM_Workbook__Student_Edition_-_v2_0.pdf

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1

229 = 128 + 64 + 32 + 4 + 1

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1

229 = 128 + 64 + 32 + 4 + 1

176 = 128 + 32 + 16

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1
229 = 128 + 64 + 32 + 4 + 1
176 = 128 + 32 + 16
19 = 16 + 2 + 1

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1	10010011
229 = 128 + 64 + 32 + 4 + 1	11100101
176 = 128 + 32 + 16	10110000
19 = 16 + 2 + 1	00010011

Převod IP adresy do binární soustavy

- Převeďte adresu serveru merlin do binární soustavy (147.229.176.19):

147 = 128 + 16 + 2 + 1	10010011
229 = 128 + 64 + 32 + 4 + 1	11100101
176 = 128 + 32 + 16	10110000
19 = 16 + 2 + 1	00010011

10010011.11100101.10110000.00010011

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
...
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
    inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
       valid_lft forever preferred_lft forever
```

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
...
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
    inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
       valid_lft forever preferred_lft forever
```

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
...
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
    inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
       valid_lft forever preferred_lft forever
```

- Délka prefixu: /23

  → 23 jedniček, zbytek 0

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
...
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
    inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
       valid_lft forever preferred_lft forever
```

- Délka prefixu: /23

  → 23 jedniček, zbytek 0

- 11111111.11111111.11111110.00000000

Maska sítě

- Zapište hodnotu masky serveru merlin binárně a dekadicky

```
$ ip addr show
...
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:25:90:c8:3f:1b brd ff:ff:ff:ff:ff:ff
    inet 147.229.176.19/23 brd 147.229.177.255 scope global eth2
       valid_lft forever preferred_lft forever
```

- Délka prefixu: /23

  → 23 jedniček, zbytek 0

- 11111111.11111111.11111110.00000000
- 255.255.254.0

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----------------------------------
```

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----------------------------------
10010011.11100101.10110000.00000000
```

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
--------------------------------------
10010011.11100101.10110000.00000000
```

Adresa sítě: 147.229.176.0

Vyhrazené adresy

- Jaká je adresa sítě a všesměrová adresa serveru merlin (147.229.176.19/23)

```
10010011.11100101.10110000.00010011
11111111.11111111.11111110.00000000
-----------------------------------
10010011.11100101.10110000.00000000
```

Adresa sítě: 147.229.176.0

Všesměrová adresa: 147.229.177.255

Počet podsítí

- Víte, že VUT má k dispozici IP adresy 147.229.0.0/16 a server merlin používá rozsah /23, kolik podsítí v rozsahu /23 může na VUT maximálně existovat?

Počet podsítí

- Víte, že VUT má k dispozici IP adresy 147.229.0.0/16 a server merlin používá rozsah /23, kolik podsítí v rozsahu /23 může na VUT maximálně existovat?

$$2^{23-16}=2^{7}=128$$

Počet zařízení v síti

- Kolik zařízení může být nejvýše v síti 147.229.176.0/23?

Počet zařízení v síti

- Kolik zařízení může být nejvýše v síti 147.229.176.0/23?

32-23=9

Počet zařízení v síti

- Kolik zařízení může být nejvýše v síti 147.229.176.0/23?

32-23=9

2^9-2=510 zařízení

Podsíťování

- Máte k dispozici rozsah IP adres 10.15.80.0/22. Máte za úkol vytvořit podsítě pro A) nejméně 40 zařízení, B) nejméně 60 zařízení, C) nejméně 16 zařízení, D) nejméně 14 zařízení, E) nejméně 8 point-to-point propojů. Navrhněte podsíťování, kolik volných adres vám zbyde v rezervě?

Podsíťování

Podsíťování

- 10.15.80.0/22

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$

Podsíťování

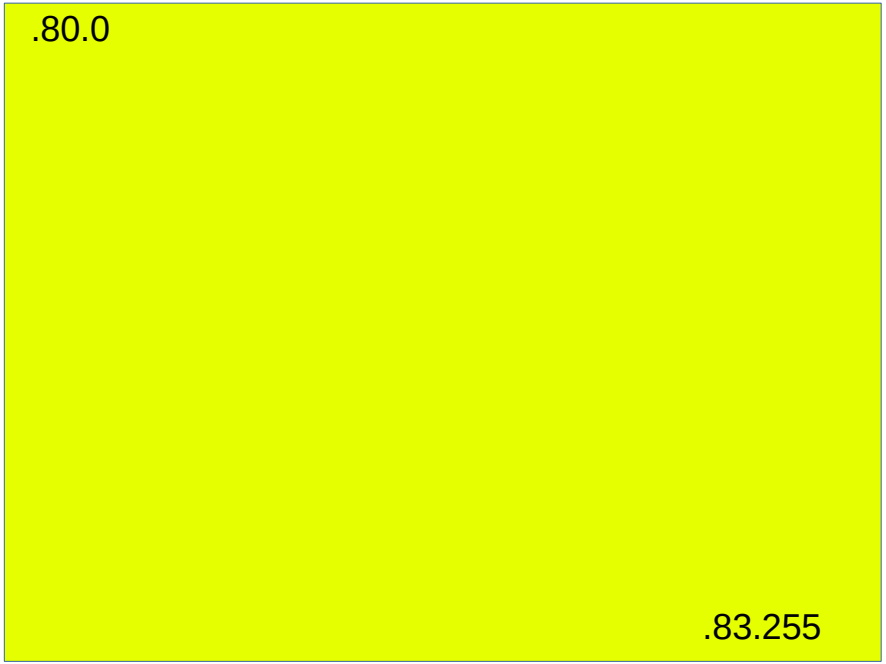
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů

Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)

Podsíťování

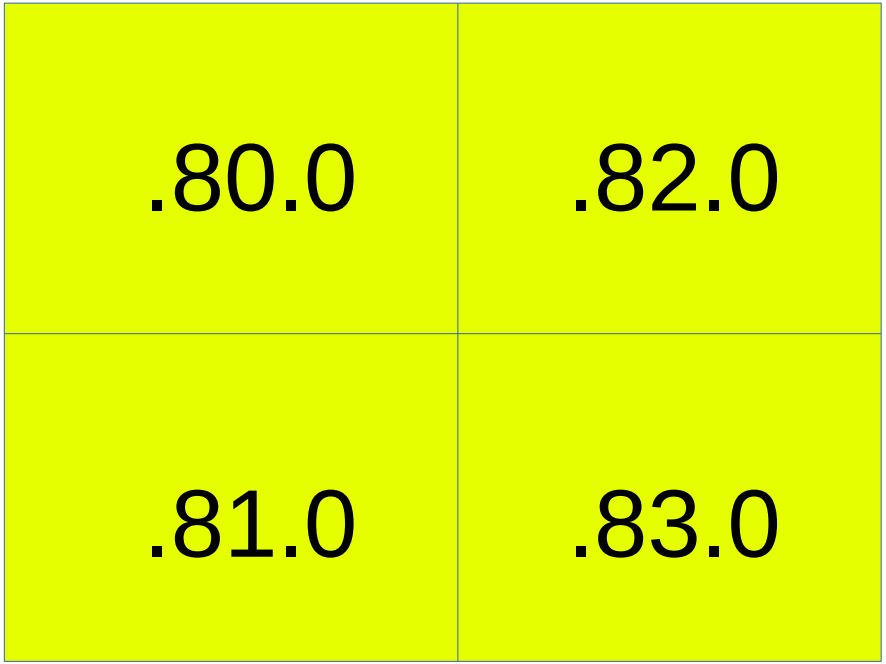
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



nes.at.fit

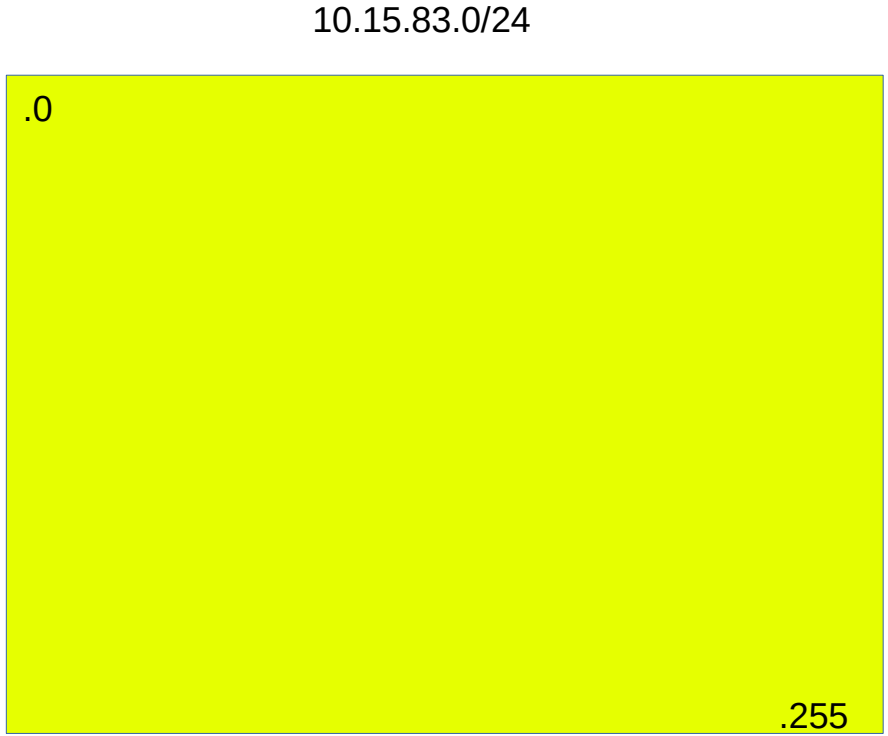
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



Podsíťování

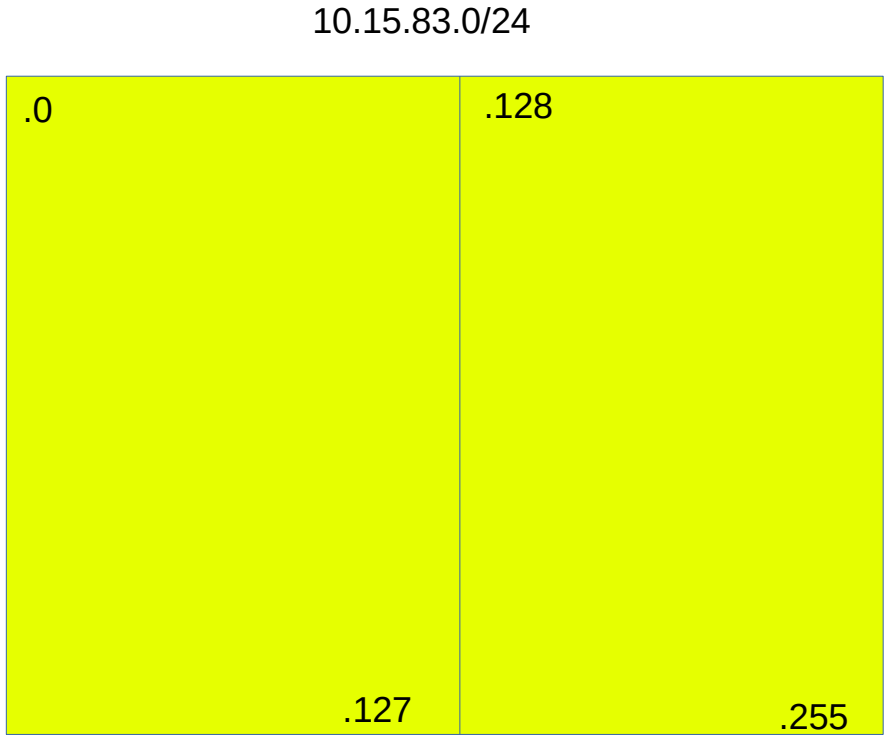
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



nes.at.fit

Podsíťování

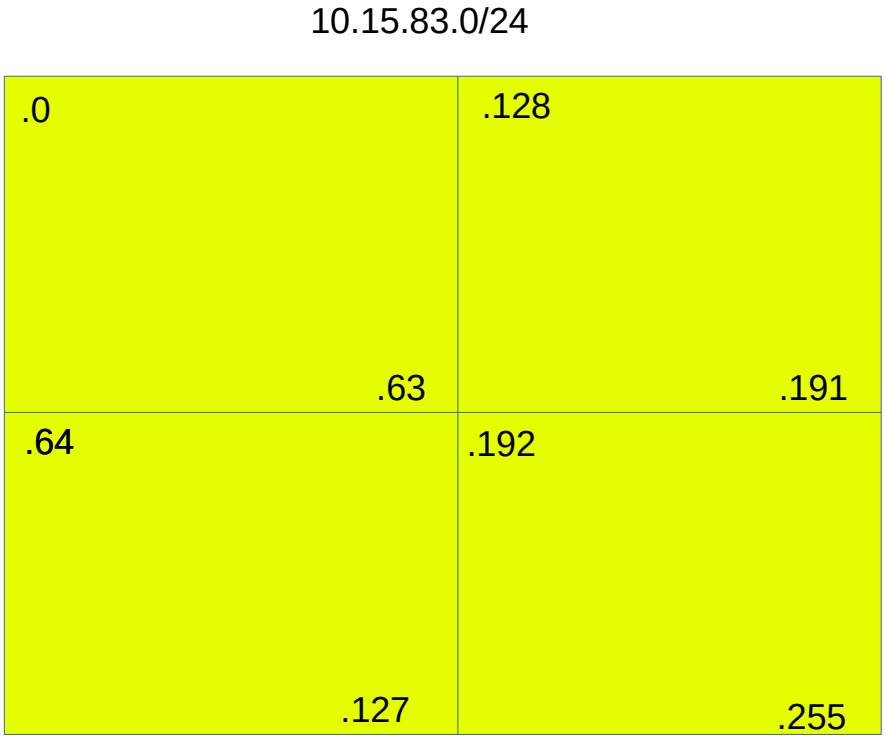
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



nes.at.fit

Podsíťování

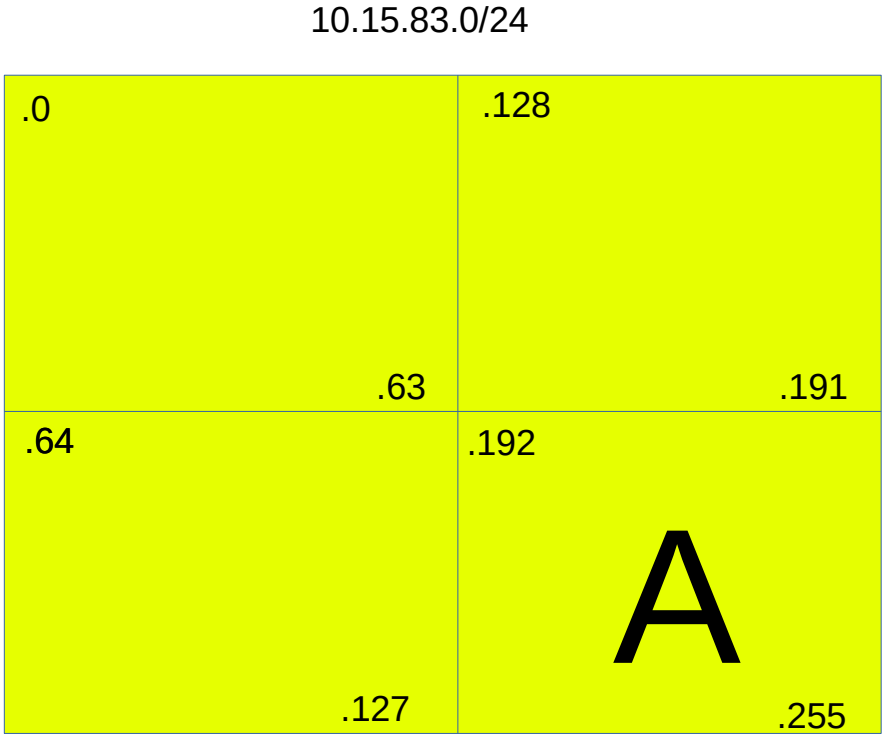
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



nes.at.fit

Podsíťování

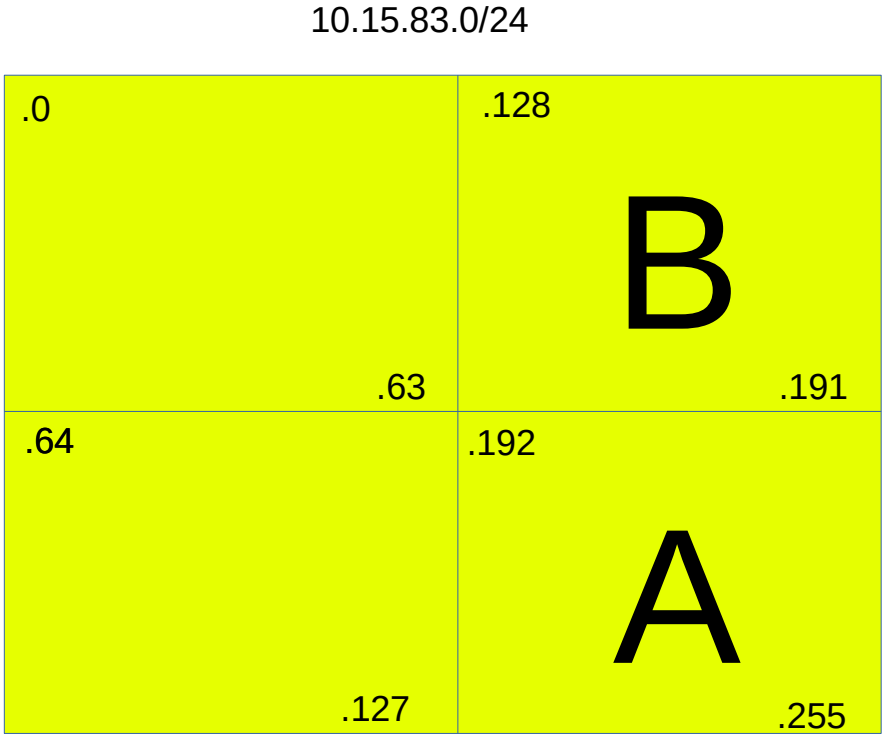
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



nes.at.fit

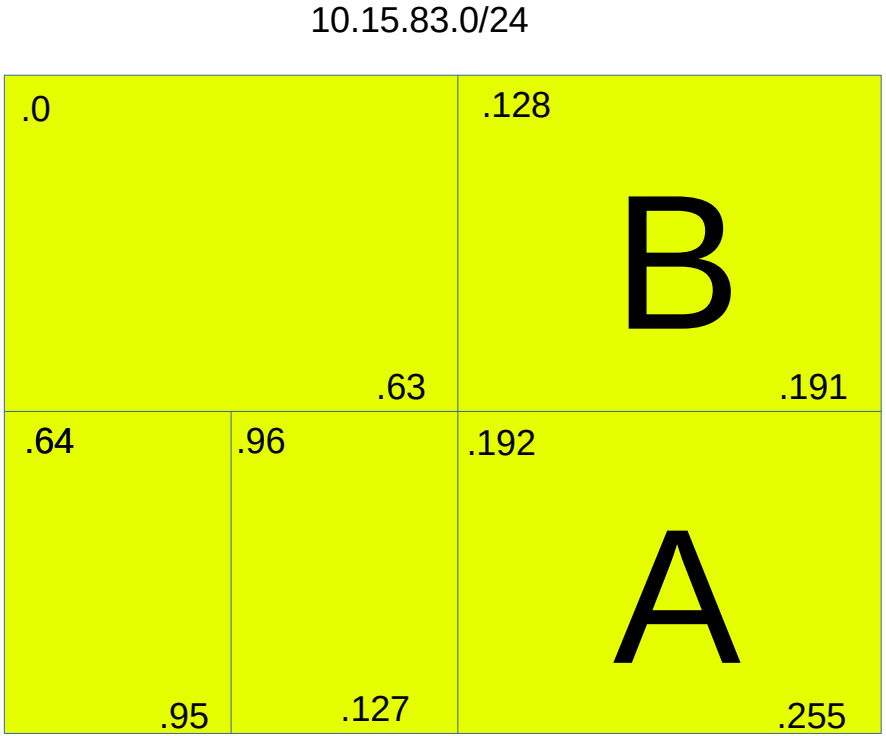
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



Podsíťování

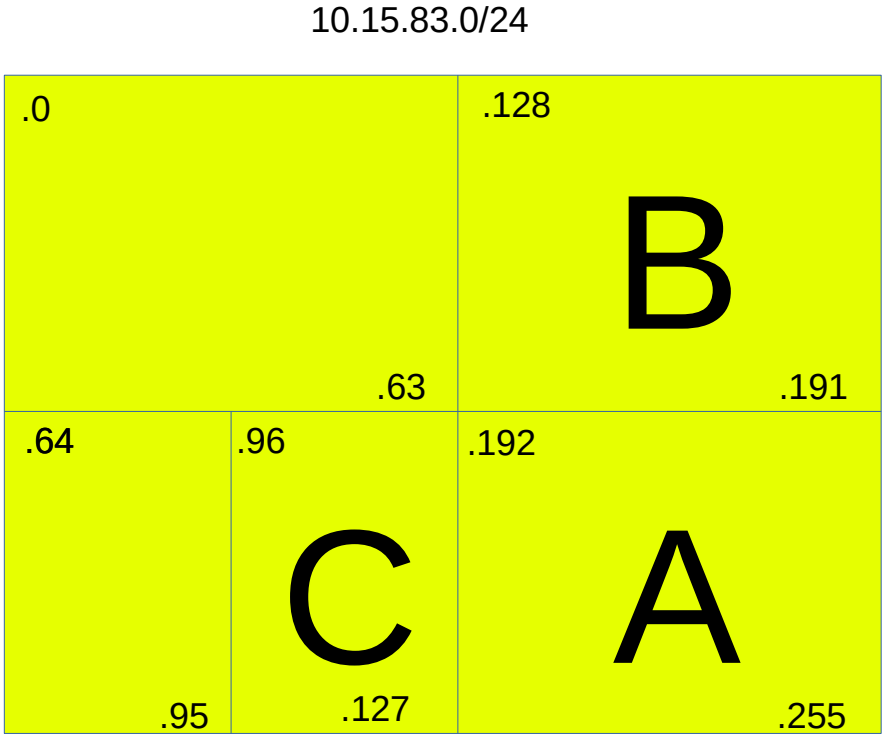
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



nes.at.fit

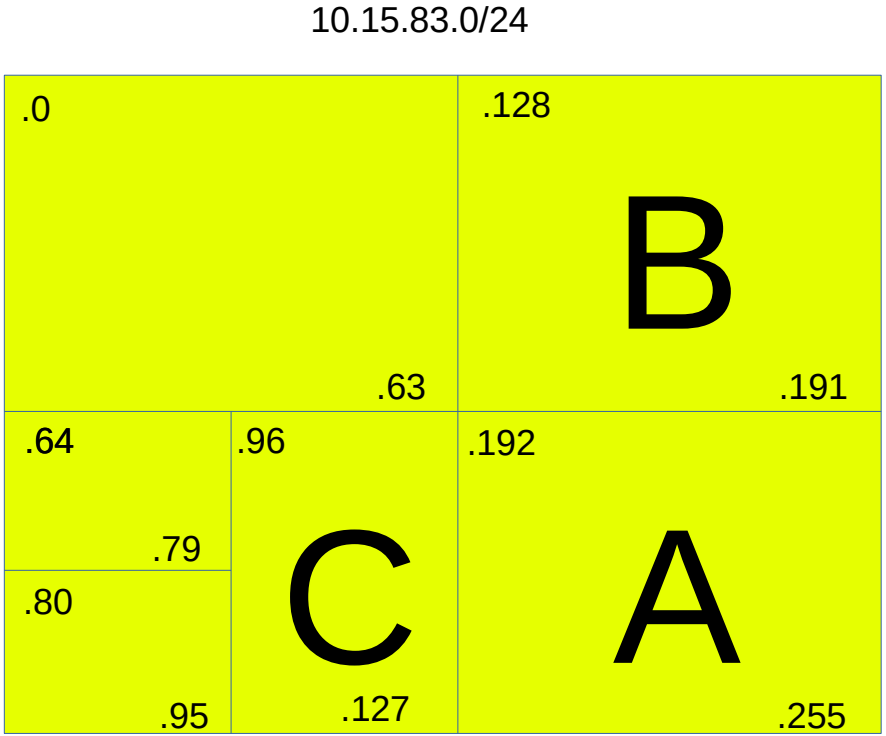
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



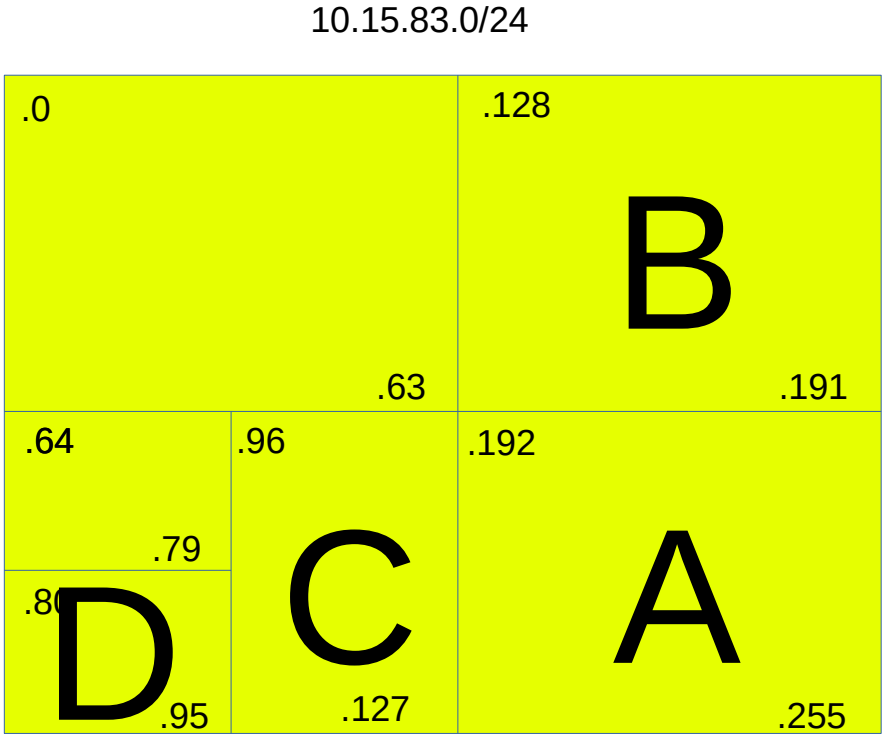
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



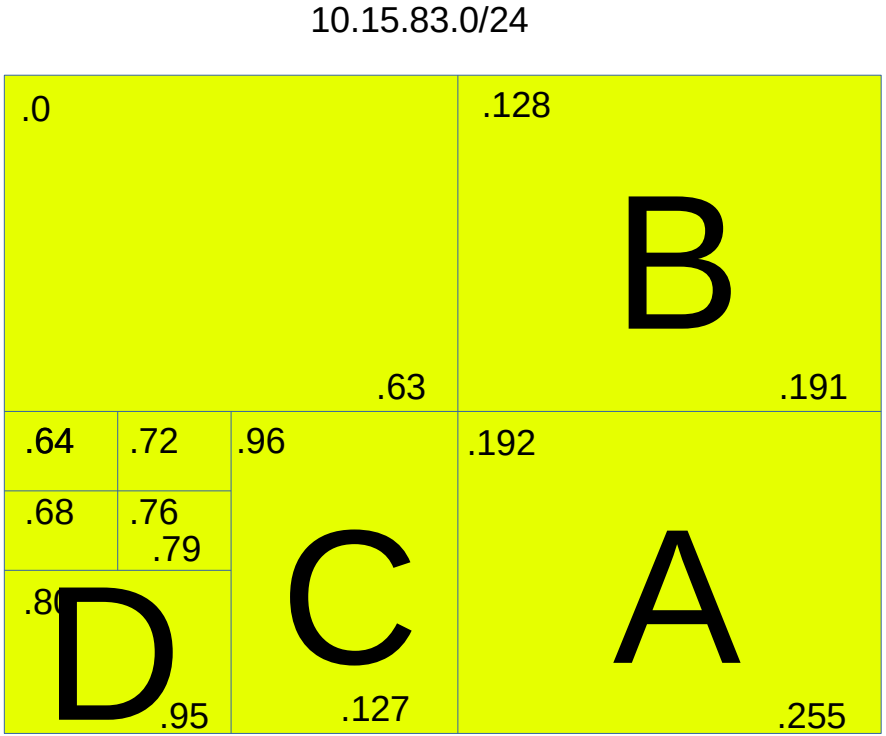
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



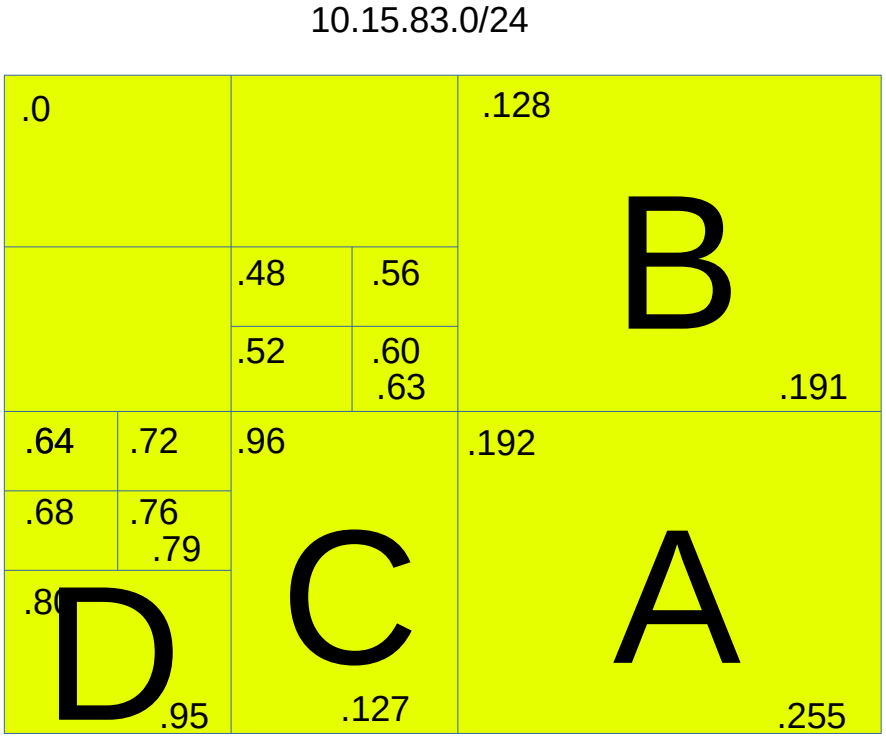
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



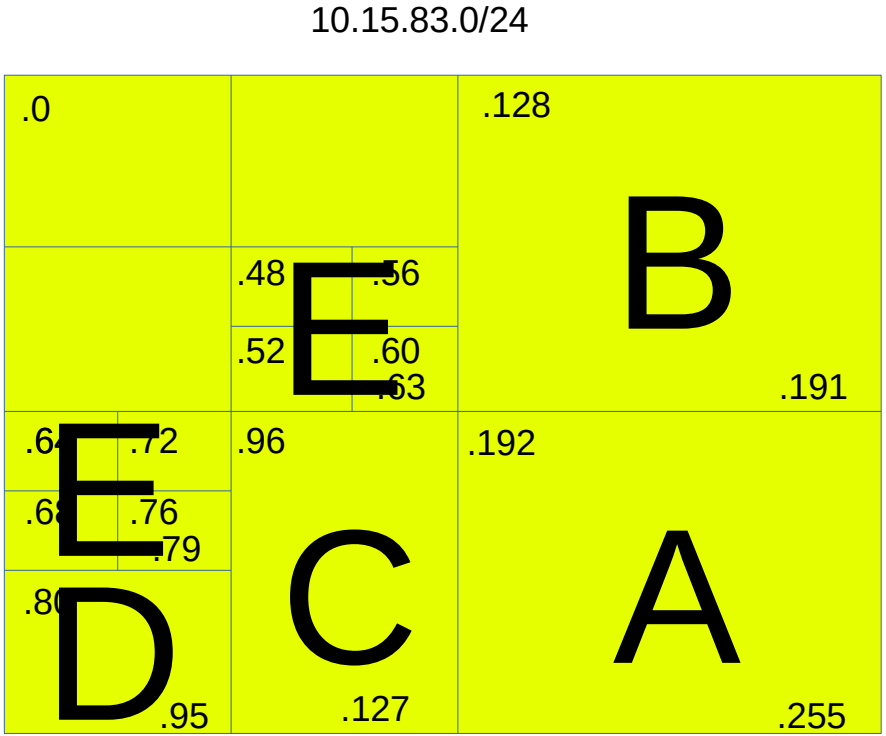
Podsíťování

- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



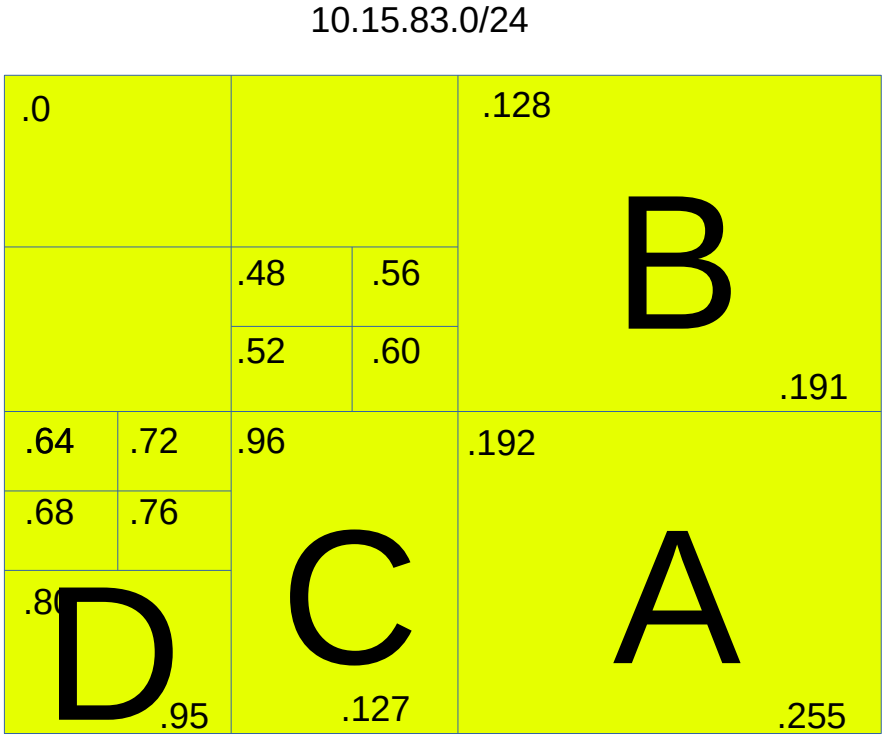
Podsíťování

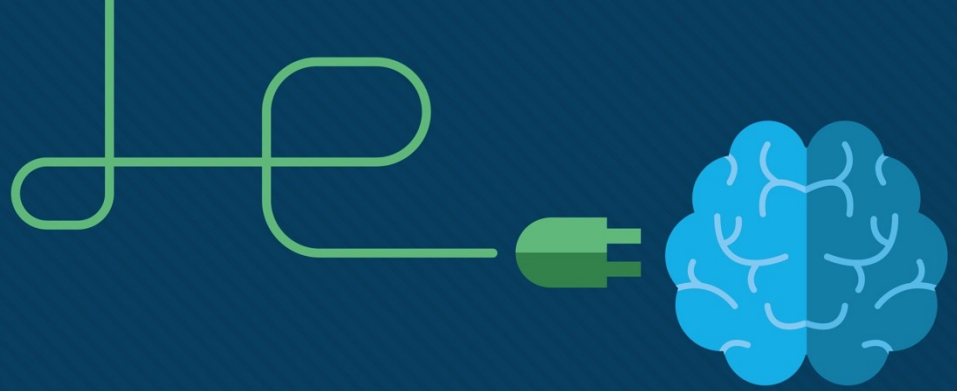
- 10.15.80.0/22
- A) 40 zařízení
  - $2^6 \rightarrow /26$
- B) 60 zařízení
  - $2^6 \rightarrow /26$
- C) 16 zařízení
  - $2^5 \rightarrow /27$
- D) 14 zařízení
  - $2^4 \rightarrow /28$
- E) 8 point-to-point propojů
  - $2^2 \rightarrow /30$ (8-krát)



Podsíťování

- 10.15.80.0/22
- A) 10.15.83.192/26
- B) 10.15.83.128/26
- C) 10.15.83.96/27
- D) 10.15.83.80/28
- E) 8 point-to-point propojů
  - 10.15.83.48/30
  - 10.15.83.52/30
  - 10.15.83.56/30
  - 10.15.83.60/30
  - 10.15.83.64/30
  - 10.15.83.68/30
  - 10.15.83.72/30
  - 10.15.83.76/30





Module 9: Address Resolution

Introduction to Networks v7.0
(ITN)

Module Objectives

Module Title: Address Resolution

Module Objective: Explain how ARP and ND enable communication on a network.

Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Describe the purpose of ARP.
Neighbor Discovery	Describe the operation of IPv6 neighbor discovery.

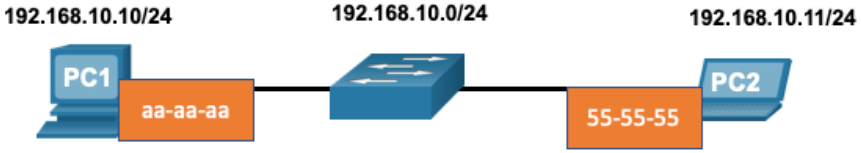
9.1 MAC and IP

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.

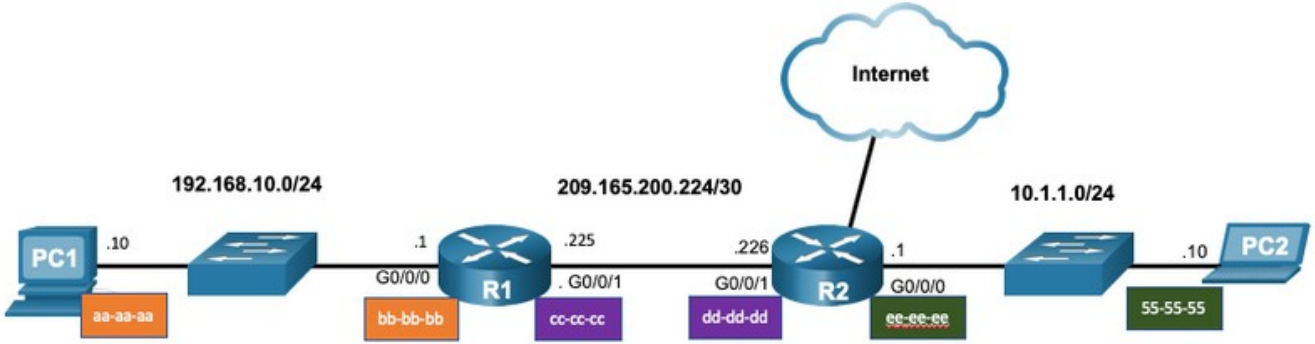


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

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

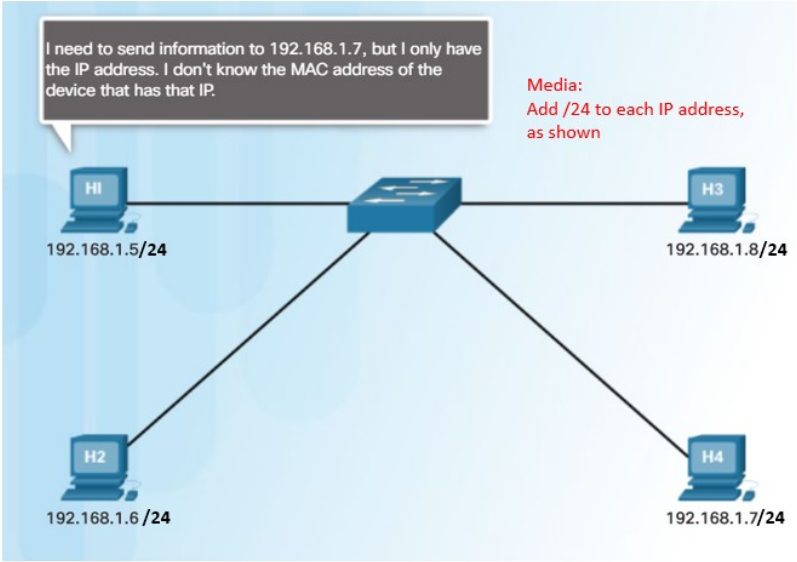
9.2 ARP (IPv4)

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



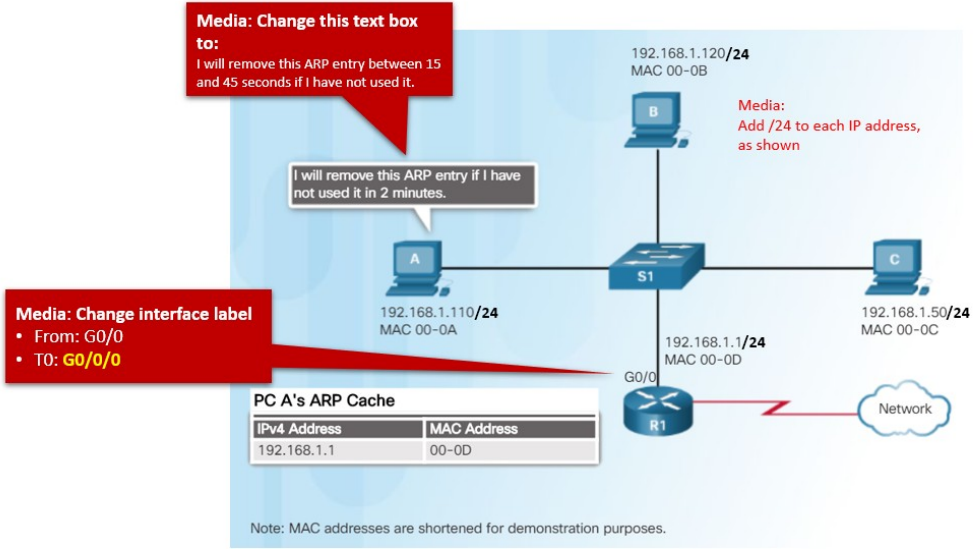
ARP Functions

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**.

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.

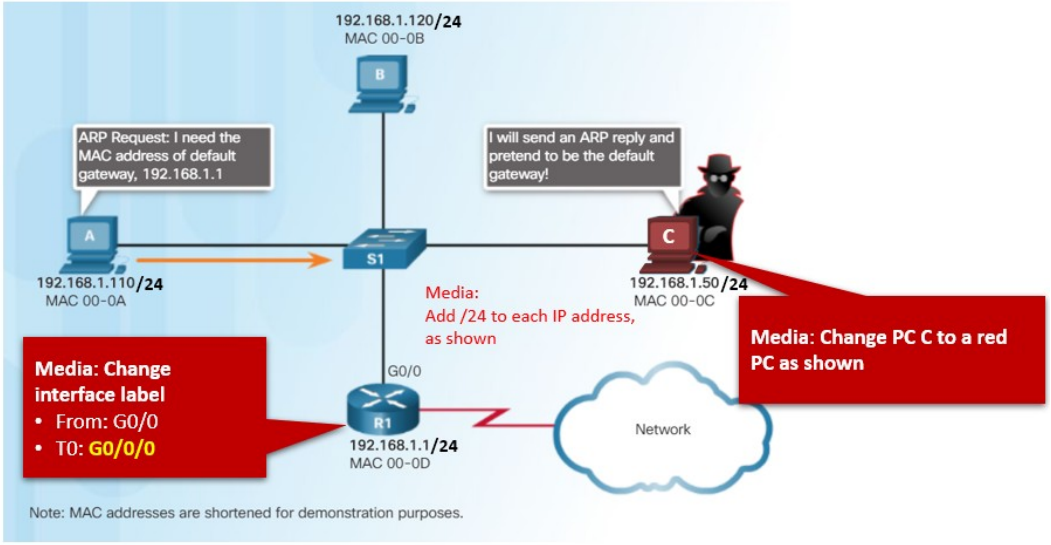
```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1            -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

```
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.



9.3 Neighbor Discovery (IPv6)

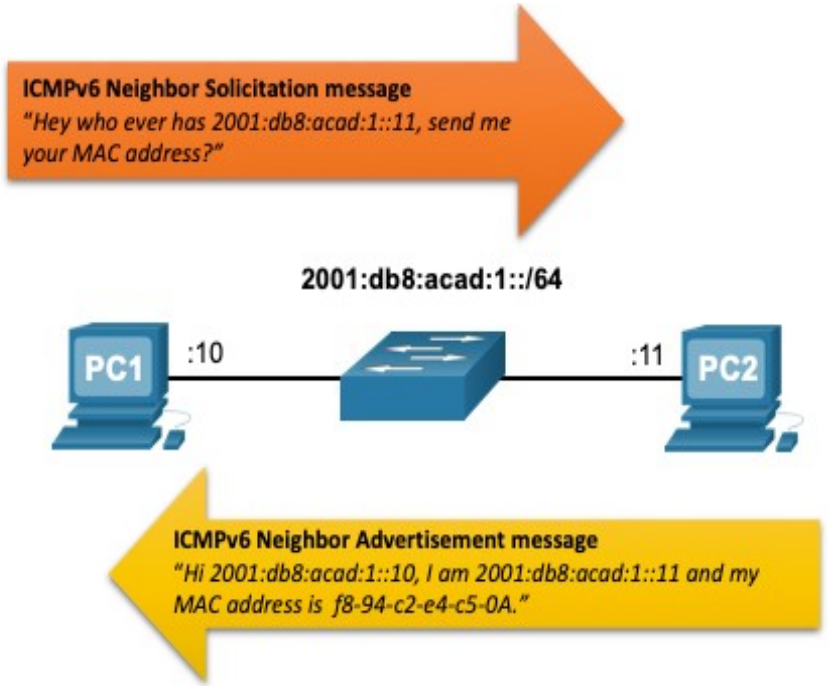
IPv6 Neighbor Discovery Messages

IPv6 Neighbor Discovery (ND) protocol provides:

- Address resolution
- Router discovery
- Redirection services

- ICMPv6 Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages are used for device-to-device messaging such as address resolution.
- ICMTPv6 Router Solicitation (RS) and Router Advertisement (RA) messages are used for messaging between devices and routers for router discovery.
- ICMPv6 redirect messages are used by routers for better next-hop selection.

IPv6 Neighbor Discovery – Address Resolution



- IPv6 devices use ND to resolve the MAC address of a known IPv6 address.
- ICMPv6 Neighbor Solicitation messages are sent using special Ethernet and IPv6 multicast addresses.


CISCO