Table Of Contents

Introduction

Online Refrences: Link

YouTube: Link

1. Why Should I Take This Module?

Welcome to IPv4 Addressing!

Currently, there are still plenty of networks using IPv4 addressing, even as the organizations which use them are making the transition to IPv6.

- So it is still very important for network administrators to know everything they can about IPv4 addressing.
- This module covers the fundamental aspects of IPv4 addressing in detail.
- It includes how to segment a network into subnets and how to create a variable-length subnet mask (VLSM) as part of an overall IPv4 addressing scheme.
- Subnetting is like cutting a pie into smaller and smaller pieces.
- Subnetting may seem overwhelming at first, but we show you some tricks to help you along the way.
- This module includes several videos, activities to help you practice subnetting, Packet Tracers and a lab.
- Once you get the hang of it, you'll be on your way to network administration!

2. What Will I Learn To Do In This Module?

2A. Module Title

- IPv4 Addressing

2B. Module Objective

- Calculate an IPv4 subnetting scheme to efficiently segment your network.

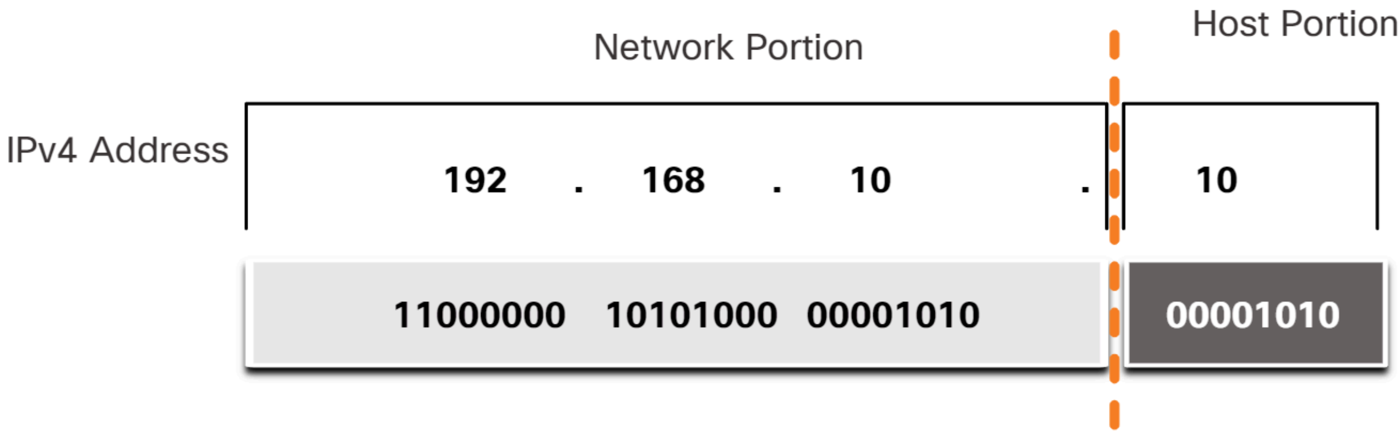
Topic Title	Topic Objective
IPv4 Address Structure	Describe the structure of an IPv4 address including the network portion, the host portion, and the subnet mask.
IPv4 Unicast, Broadcast, and Multicast	Compare the characteristics and uses of the unicast, broadcast and multicast IPv4 addresses.
Types 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.
Subnet a /16 and a /8 Prefix	Calculate IPv4 subnets for a /16 and /8 prefix.
Subnet To Meet Requirements	Given a set of requirements for subnetting, implement an IPv4 addressing scheme.
Variable Length Subnet Masking	Explain how to create a flexible addressing scheme using variable length subnet masking (VLSM).
Structured Design	Implement a VLSM addressing scheme.

IPv4 Address Structure

1. Network and Host Portions

An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion. When determining the network portion versus the host portion, you must look at the 32-bit stream, as shown in the figure.

1A. IPv4 Address



The bits within the network portion of the address must be identical for all devices that reside in the same network. The bits within the host portion of the address must be unique to identify a specific host within a network.

If two hosts have the same bit-pattern in the specified network portion of the 32-bit stream, those two hosts will reside in the same network.

But how do hosts know which portion of the 32-bits identifies the network and which identifies the host? That is the role of the subnet mask.

A subnet mask is used to determine the network and host portions.

1B. How an IPv4 Address Is Divided Into Two Parts: The Network Portion And The Host Portion.

Here's a Breakdown

- **IPv4 Address**
  - An IPv4 address is a 32-bit number. This is typically represented in four octets (or 8-bit sections) separated by dots, like 192.168.10.10 in the image.
  - In binary, the same address would be represented as 11000000.10101000.00001010.00001010.

- **Network Portion vs. Host Portion**
  - **Network Portion:** This part of the address is the same for all devices within the same network. It's used to identify the specific network. Devices in the same network share the same network portion of the address.
  - **Host Portion:** This part is unique to each device within the network, identifying individual hosts (like computers, phones, etc.) within that network. Each device has a unique host portion to differentiate it within that network.

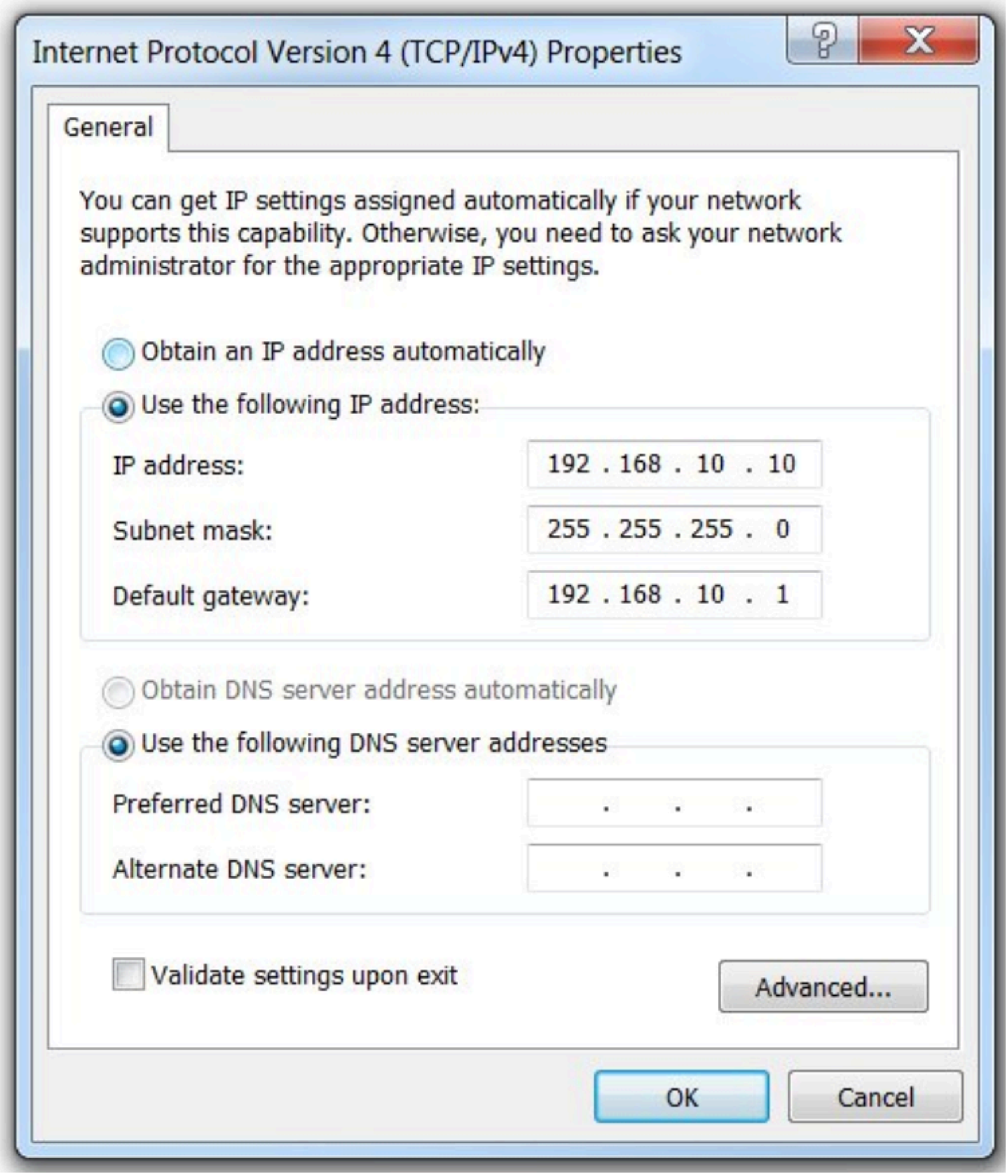
- **Subnet Mask**
  - The subnet mask helps devices figure out which part of the 32-bit address identifies the network and which part identifies the host.
  - In the image, the division between the network and host portions is marked by the dotted line. The bits to the left are the network portion, and the bits to the right are the host portion.

- For example, in the address 192.168.10.10, the network portion might be 192.168.10 (as indicated by the bits 11000000 10101000 00001010), and the host portion might be 10 (as indicated by the bits 00001010).

2. The Subnet Mask

- As shown in the figure, assigning an IPv4 address to a host requires the following:
  - **IPv4 Address** - This is the unique IPv4 address of the host.
  - **Subnet Mask**- This is used to identify the network/host portion of the IPv4 address.

2A. IPv4 Configuration on a Windows Computer



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Screenshot of the TCP/IPv4 properties Windows dialog box showing the device is set to use the following IP addressing information: IP address of 192.168.10.10; subnet mask of 255.255.255.0, and default gateway of 192.168.10.1

Note: A default gateway IPv4 address is required to reach remote networks and DNS server IPv4 addresses are required to translate domain names to IPv4 addresses.

The IPv4 subnet mask is used to differentiate the network portion from the host portion of an IPv4 address. When an IPv4 address is assigned to a device, the subnet mask is used to determine the network address of the device. The network address represents all the devices on the same network.

2B. How To Manually Configure An IPv4 Address For A Device On A Network, Specifically Within The Context Of A Windows Computer. Here's A Breakdown:

1. IPv4 Configuration

- **IP Address**:
  - This is a unique identifier assigned to your device (e.g., computer, smartphone) on a network. In the image, the IP address is set to 192.168.10.10.

- **Subnet Mask**:
  - This is used to determine which portion of the IP address represents the network and which part represents the individual device (host). In this case, the subnet mask is 255.255.255.0, which means that the first three octets (192.168.10) represent the network, and the last octet (10) represents the device on that network.

- **Default Gateway**:
  - This is the IP address of the router or another device that connects the local network to other networks, including the Internet. The default gateway in the image is set to 192.168.10.1.

- **DNS Server**:
  - Domain Name System (DNS) servers translate domain names (like www.example.com) into IP addresses. In the image, the DNS server addresses are not filled in, which means that they would need to be added for the computer to resolve domain names properly.

2. What Does It Mean?

- **Manually Assigned IP Address**:
  - The user is setting up a fixed IP address for the device instead of allowing it to be automatically assigned by a router or DHCP server.

- **Subnet Mask Function**:
  - The subnet mask tells the device how to distinguish the network portion of the IP address from the device portion. This is crucial for the device to communicate correctly within its local network and to other networks.

- **Default Gateway & DNS Servers**:
  - The default gateway allows the device to communicate with devices outside its local network (like accessing the internet), and the DNS servers are needed to resolve domain names to IP addresses so that the device can access websites and other internet services.

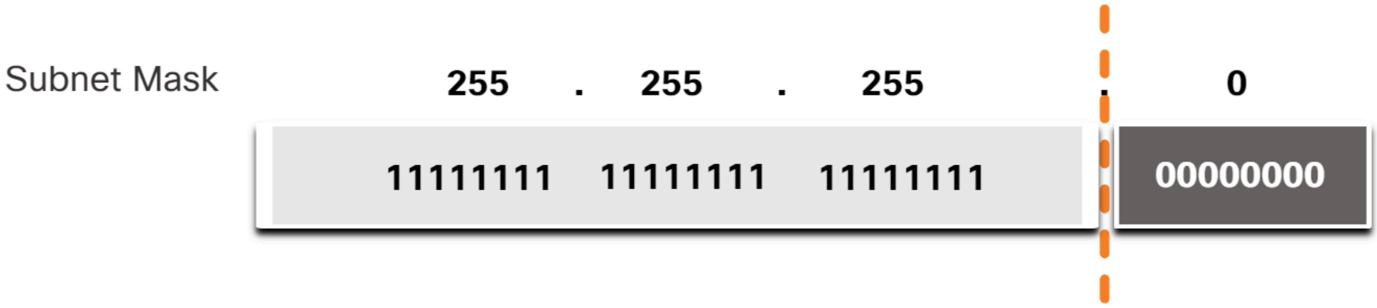
This setup is often used in networks where fixed IP addresses are required, such as in certain business or advanced home network setups.

2C. Subnet Mask 32-Bit

The next figure displays the 32-bit subnet mask in **dotted decimal** and binary formats. The subnet mask is a 32-bit number that helps in identifying which part of an IP address refers to the network and which part refers to the host.

It consists of a sequence of 1s followed by a sequence of 0s. The 1s indicate the network portion and the 0s indicate the host portion.

For example, in the image, the subnet mask 255.255.255.0 is shown in binary as 11111111.11111111.11111111.00000000. The 1s are grouped together on the left, marking the network portion, and the 0s on the right marking the host portion.

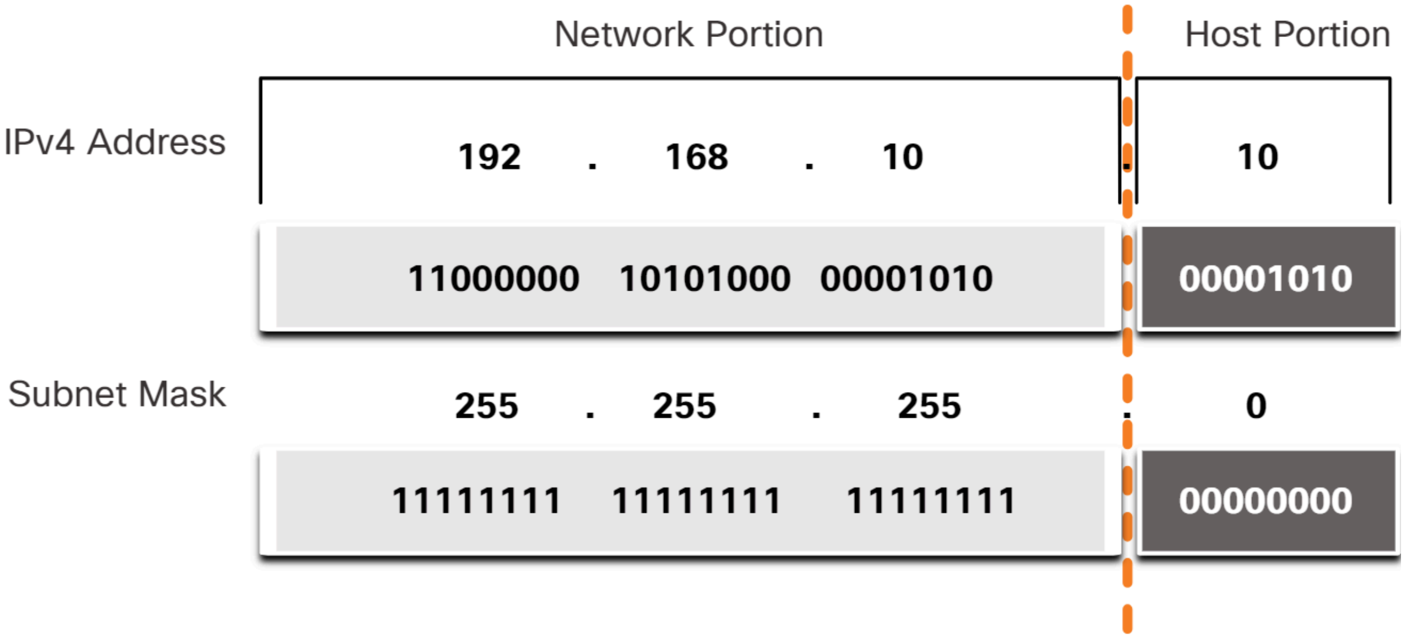


2D. Associating an IPv4 Address with its Subnet Mask

To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right as shown in the figure.

Note that the subnet mask does not actually contain the network or host portion of an IPv4 address, it just tells the computer where to look for the part of the IPv4 address that is the network portion and which part is the host portion.

The actual process used to identify the network portion and host portion is called ANDing.



	Network Portion			Host Portion
IPv4 Address	192	168	10	10
	11000000	10101000	00001010	00001010
Subnet Mask	255	255	255	0
	11111111	11111111	11111111	00000000

3. The Prefix Length

Expressing network addresses and host addresses with the **dotted decimal subnet mask address** can become cumbersome. Fortunately, there is an alternative method of identifying a subnet mask, a method called the **prefix length**.

The prefix length is the number of bits set to 1 in the subnet mask. It is written in "**slash notation**", which is noted by a forward slash (/) followed by the number of bits set to 1. Therefore, count the number of bits in the subnet mask and prepend it with a slash.

Refer to the table for examples. The first column lists various subnet masks that can be used with a host address. The second column displays the converted 32-bit binary address. The last column displays the resulting prefix length.

3A. Comparing the Subnet Mask and Prefix Length

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

Note: A network address is also referred to as a prefix or network prefix. Therefore, the prefix length is the number of 1 bits in the subnet mask.

When representing an IPv4 address using a prefix length, the IPv4 address is written followed by the prefix length with no spaces. For example, **192.168.10.10 255.255.255.0 would be written as 192.168.10.10/24**.

Using various types of prefix lengths will be discussed later. For now, the focus will be on the /24 (i.e. 255.255.255.0) prefix.

This comparison explains how subnet masks and prefix lengths are related in networking, specifically in IPv4 addressing. Here's what it means:

1. Subnet Mask:

- A subnet mask is a 32-bit number that helps define which portion of an IP address identifies the network and which portion identifies the host (a device on the network).
- It is typically written in decimal form, divided into four octets (e.g., 255.255.255.0).

2. Prefix Length:

- The prefix length, also known as CIDR (Classless Inter-Domain Routing) notation, represents the number of consecutive 1 bits in the subnet mask.
- It is written as a slash ("/") followed by the number of 1 bits.
- For example, /24 means the first 24 bits of the subnet mask are 1s.

- The term "**1s**" refers to binary digits that are set to the value of 1 in a binary number.
  - In the context of subnet masks and prefix lengths:
    - A binary number is made up of digits called bits, which can be either 0 or 1.
    - When we talk about "1s" in a subnet mask, we are referring to the bits that are set to 1, which represent the network portion of the IP address.
    - For example, in the subnet mask 255.255.255.0, the binary equivalent is 11111111.11111111.11111111.00000000. The first 24 bits are 1s, meaning those bits are used to identify the network.
    - In summary, "1s" in this context are the bits in the binary representation of a subnet mask that define the network portion of an IP address.

3. Example Breakdown: **255.255.255.0**:

- This subnet mask corresponds to 11111111.11111111.11111111.00000000 in binary.
- The first 24 bits are 1s, so the prefix length is /24.
- An IP address like 192.168.10.10 with this subnet mask would be written as 192.168.10.10/24.

4. Other Prefix Lengths:

- **/8 (255.0.0.0):** The first 8 bits are for the network, allowing a large number of hosts.
- **/16 (255.255.0.0):** The first 16 bits are for the network, offering more networks but fewer hosts per network.
- **/30 (255.255.255.252):** The first 30 bits are for the network, allowing only a few hosts, typically used in point-to-point connections.

5. Key Takeaway:

- The prefix length simplifies the representation of subnet masks by indicating the number of 1s directly. This makes it easier to understand the scope of the network portion of the IP address. For example, a /24 prefix means that the first 24 bits are used for the network, and the remaining 8 bits are used for hosts.

6. Example:

Here are examples of subnet masks and their corresponding binary representations for /25, /26, and /27:

/25 Subnet Mask:

- **Subnet Mask:** 255.255.255.128
- **Binary Representation:** 11111111.11111111.11111111.10000000
- **Explanation:**
  - The first 25 bits are 1s, which represent the network portion of the IP address.
  - The remaining 7 bits are 0s, which represent the host portion of the IP address.
  - This allows for 128 IP addresses, with 126 usable for hosts (2 addresses are reserved for network and broadcast).

/26 Subnet Mask:

- **Subnet Mask:** 255.255.255.192
- **Binary Representation:** 11111111.11111111.11111111.11000000
- **Explanation:**
  - The first 26 bits are 1s, which represent the network portion.
  - The remaining 6 bits are 0s, which represent the host portion.
  - This allows for 64 IP addresses, with 62 usable for hosts.

/27 Subnet Mask:

- **Subnet Mask:** 255.255.255.224
- **Binary Representation:** 11111111.11111111.11111111.11100000
- **Explanation:**
  - The first 27 bits are 1s, which represent the network portion.
  - The remaining 5 bits are 0s, which represent the host portion.
  - This allows for 32 IP addresses, with 30 usable for hosts.

Summary:

- **/25:** 25 bits for the network, 7 bits for hosts.
- **/26:** 26 bits for the network, 6 bits for hosts.
- **/27:** 27 bits for the network, 5 bits for hosts.

Each of these subnet masks further divides a larger network into smaller subnets, with fewer hosts available in each subnet as the prefix length increases.

4. Determining the Network: Logical AND

A logical AND is one of three Boolean operations used in Boolean or digital logic. The other two are OR and NOT. The AND operation is used in determining the network address.

Logical AND is the comparison of two bits that produce the results shown below. Note how only a 1 AND 1 produces a 1. Any other combination results in a 0.

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

Note: In digital logic, **1** represents **True** and **0** represents **False**. When using an AND operation, both input values must be True (1) for the result to be True (1).

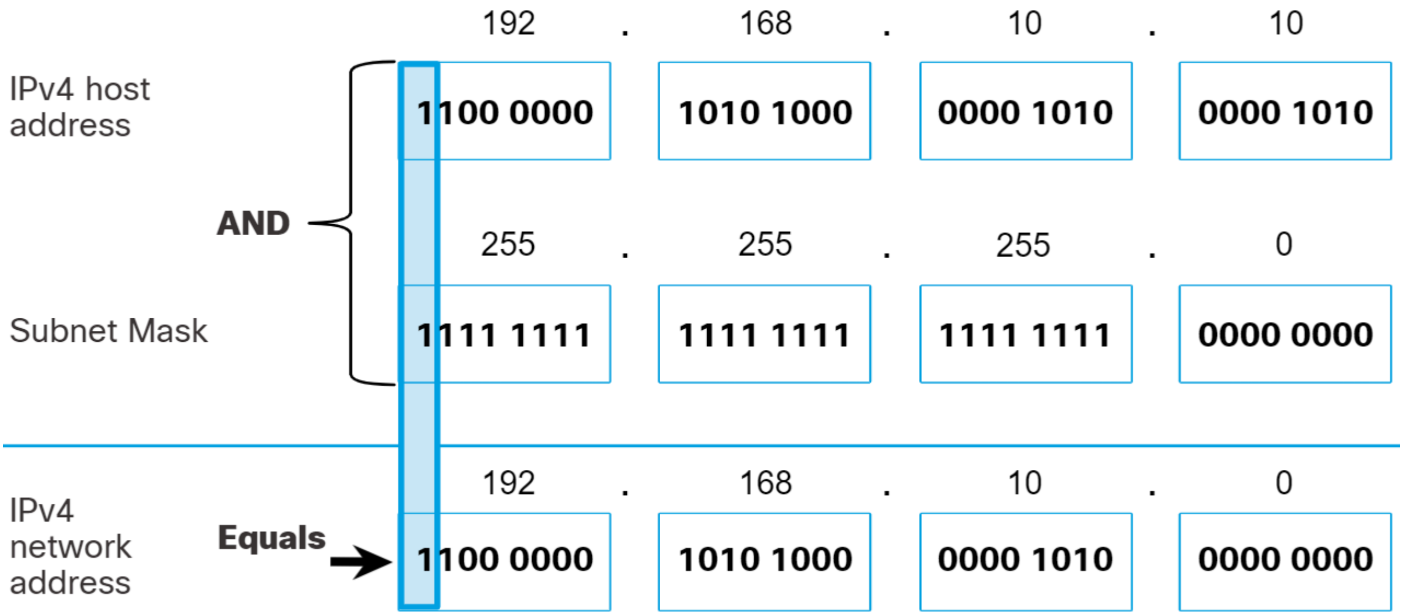
To identify the network address of an IPv4 host, the IPv4 address is logically ANDed, bit by bit, with the subnet mask. ANDing between the address and the subnet mask yields the network address.

To illustrate how AND is used to discover a network address, consider a host with IPv4 address 192.168.10.10 and a subnet mask of 255.255.255.0, as shown in the figure:

- **IPv4 host address (192.168.10.10)** - The IPv4 address of the host in dotted decimal and binary formats.

- **Subnet mask (255.255.255.0)** - The subnet mask of the host in dotted decimal and binary formats.

- **Network address (192.168.10.0)** - The logical AND operation between the IPv4 address and subnet mask results in an IPv4 network address shown in dotted decimal and binary formats.



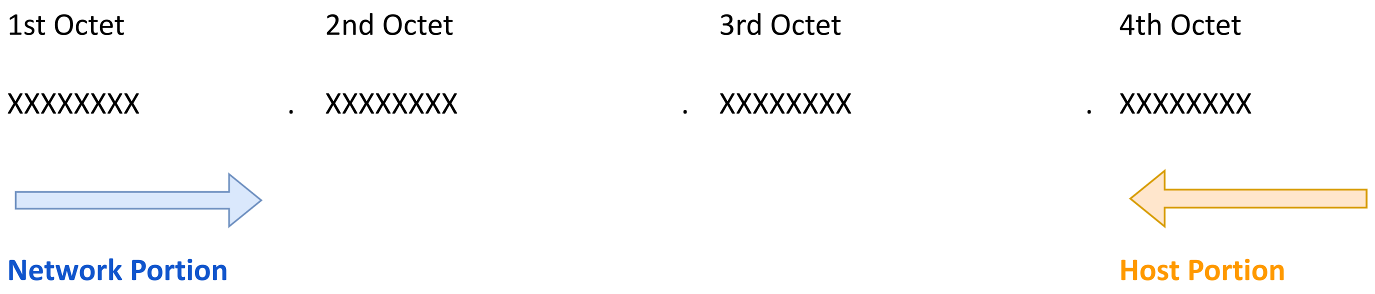
Using the first sequence of bits as an example, notice the AND operation is performed on the 1-bit of the host address with the 1-bit of the subnet mask. This results in a 1-bit for the network address. 1 AND 1 = 1.

The AND operation between an IPv4 host address and a subnet mask results in the IPv4 network address for this host. In this example, the AND operation between the host address of 192.168.10.10 and the subnet mask 255.255.255.0 (/24), results in the IPv4 network address of 192.168.10.0/24. This is an important IPv4 operation, as it tells the host what network it belongs to.

5. Demonstration: Network, Host and Broadcast Addresses

- Demonstration of how the network, host, and broadcast addresses are determined for a given IPv4 address and subnet mask.

5A. Overview of IPv4 Addressing



1st Octet 2nd Octet 3rd Octet 4th Octet

XXXXXXXX . XXXXXXXX . XXXXXXXX . XXXXXXXX

Network Portion

Host Portion

Here's a summary of the key points:

- **IPv4 Addresses**:
  - These are 32-bit logical addresses, represented in a dotted decimal format (e.g., 192.168.1.1).

- **Network and Host Portions**:
  - The IPv4 address consists of two parts:
    - **Network Portion**: Identifies the specific network. The length of this portion varies depending on the size of the network.
    - **Host Portion**: Identifies the specific device (host) within the network.

- **Network ID and Host ID**:
  - All devices on the same network share the same network portion (Network ID).
  - The host portion (Host ID) is unique for each device on the network.

- **Octets**:
  - The 32-bit IPv4 address is divided into four octets (8 bits each).
  - The division between the network portion and the host portion occurs somewhere between these octets, depending on the subnetting.

This is a fundamental concept in networking, helping to identify and distinguish between different devices and networks on the internet or any IP-based network.

5B. Important Addresses To Determine

Some addresses in this range are reserved and have a special name and meaning. For example:

1. Network Address (First Address in the Range)

- A network address is like the name of a street that tells you which part of a city you're in, but not which specific house you're looking for. It identifies a group of IP addresses that are all part of the same network.
- This is the first IP address in the subnet and is **used to identify the network itself** and cannot be assigned to any host.
- For example, in a subnet like 192.168.1.0/24, the network address is 192.168.1.**0** (11000000 10101000 00000001 **00000000**)

2. Broadcast Address (Last Address in the Range)

- The broadcast address is the **last IP address in the subnet** and is used to send data to all hosts on the network and **cannot be assigned to any host**.
- For example, in the same 192.168.1.0/24 subnet, the broadcast address is 192.168.1.255.

3. First Usable Host (Address After the Network Address)

- This is the first IP address that can be assigned to a device on the network.
- For 192.168.1.0/24, the first usable host address is 192.168.1.1.

4. Last Usable Host (Address Before the Broadcast Address)

- This is the last IP address that can be assigned to a device on the network.
- For the 192.168.1.0/24 subnet, the last usable host address is 192.168.1.254.

5C. Using ANDing To Determine The Network

Purpose:

- A device needs to identify its network to forward data correctly.

Process:

- By using its host IP address, subnet mask, and a process called binary ANDing, the device can determine its network.

Binary ANDing:

- The device compares its host IP address and subnet mask bit-by-bit:
    - If both bits are binary 1, the result is binary 1.
    - If one or both bits are 0, the result is 0.

- This process helps the device identify the network portion of its IP address.

Example:

- To find the network address of a host using the IP address and subnet mask, you can perform a bitwise AND operation between the IP address and the subnet mask. This process involves comparing the binary forms of the IP address and the subnet mask. Given:
    - **Host IP Address**: 192.168.2.38
    - **Subnet Mask**: /24, which equals 255.255.255.0

Host IP Address (In Binary)	11000000	10101000	00000010	00100110
Subnet Mask (In Binary)	**11111111**	**11111111**	**11111111**	**00000000**
Using ANDing (&)	1 1 0 0 0 0 0 0 + + + + + + + + 1 1 1 1 1 1 1 1 = = = = = = = = 1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0 + + + + + + + + 1 1 1 1 1 1 1 1 = = = = = = = = 1 0 1 0 1 0 0 0	0 0 0 0 0 0 1 0 + + + + + + + + 1 1 1 1 1 1 1 1 = = = = = = = = 0 0 0 0 0 0 1 0	0 0 1 0 0 1 1 0 + + + + + + + + 1 1 1 1 1 1 1 1 = = = = = = = = 0 0 0 0 0 0 0 0
Network Address (Compare bit for bit)	11000000	10101000	00000010	00000000

Notice that the last octet is all binary zero due to we are using a /24 subnet mask. The first 3 octets represent the network portion, and the last octet is the host portion.

Network Address will always have binary zero in their entire host portion. Now, convert the binary result back to decimal to get the network address:

- 11000000 = 192
- 10101000 = 168
- 00000010 = 2
- 00000000 = 0
- So, the network address is: 192.168.2.0

- This means that the IP address 192.168.2.38 belongs to the network 192.168.2.0/24. The network address 192.168.2.0 represents the entire network, and it's the first address in that range. The /24 indicates that the first 24 bits (192.168.2) are the same for all addresses in this network, leaving 8 bits (the last part) to differentiate individual devices.

/24

Network Portion

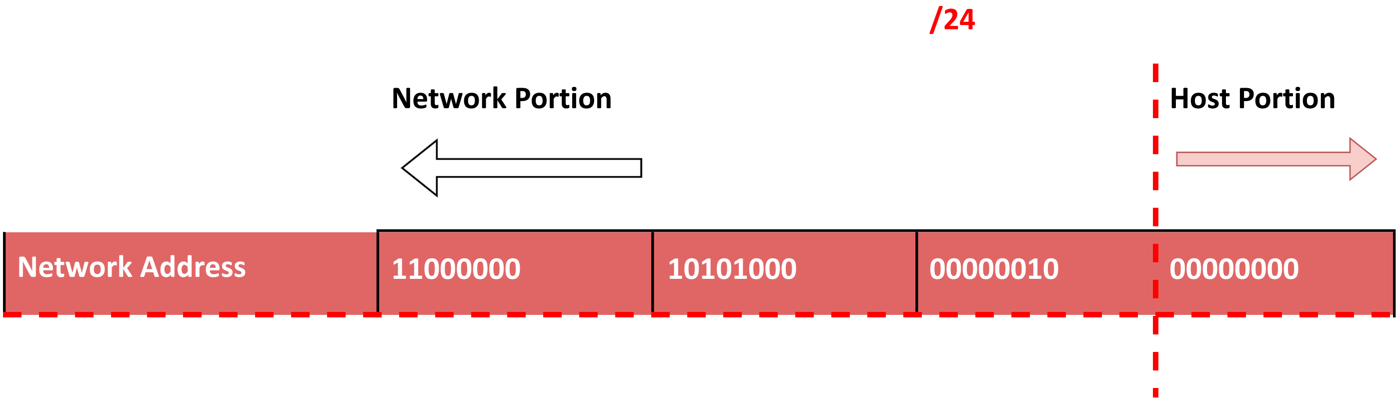
Host Portion

Host IP Address (In Binary)	**11000000**	**10101000**	**00000010**	**00100110**
Subnet Mask	**11111111**	**11111111**	**11111111**	**00000000**
Network Address (Compare bit for bit)	11000000	10101000	00000010	00000000

5D. Determining The Broadcast Address

Determine the Broadcast Address for this Network which is used to send a message to all devices on the network at once.

- Whereas the Network Address had all Binary 0s in the Host Portion.



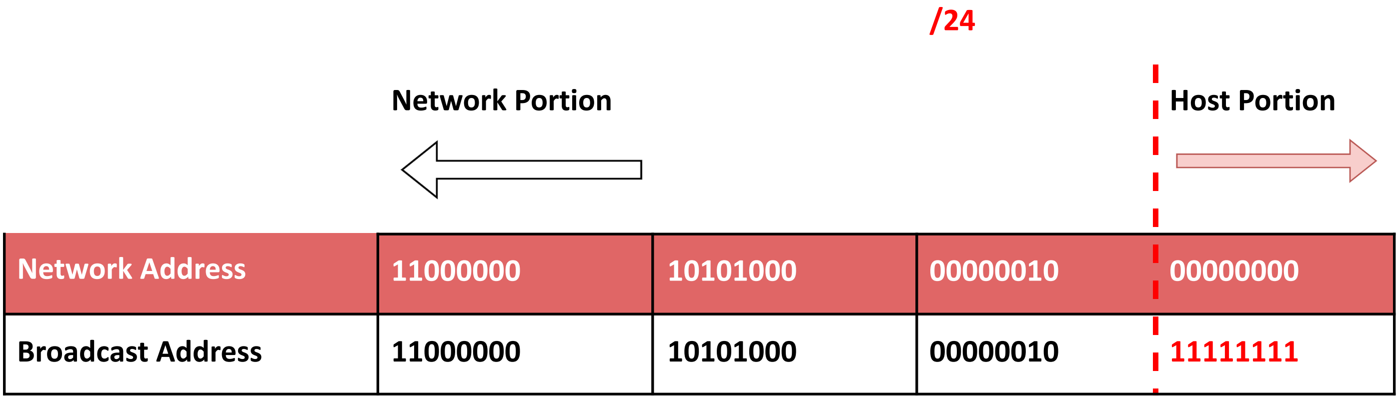
/24

Network Portion

Host Portion

Network Address	**11000000**	**10101000**	**00000010**	**00000000**

The Broadcast Address will have all Binary 1s, since the Host Portion in this example is just the last Octet. To determine the Broadcast Address we keep the Network Portion the same and change the Host Portion to all Binary 1s.



/24

Network Portion

Host Portion

Network Address	**11000000**	**10101000**	**00000010**	**00000000**
Broadcast Address	**11000000**	**10101000**	**00000010**	**11111111**

Convert to dotted-decimal and the Broadcast Address for this Network is 192.168.2.255

/24

Network Portion

Host Portion

Network Address	**11000000**	**10101000**	**00000010**	**00000000**
Broadcast Address	**11000000**	**10101000**	**00000010**	**11111111**
Broadcast Address Dotted-Decimal	**192**	**168**	**2**	**255**

5E. Determining The First Usable Host Address

Determine the Usable Host Addresses which lie between the Network and the Broadcast Addresses.

/24

Network Portion **Host Portion**

Network Address	**11000000**	**10101000**	**00000010**	**00000000**
First Usable Host Address	**11000000**	**10101000**	**00000010**	

The First Usable Host in Binary will be all Binary 0s, with a Binary 1 at the end of the Host Portion.

/24

Network Portion **Host Portion**

Network Address	**11000000**	**10101000**	**00000010**	**00000000**
First Usable Host Address	**11000000**	**10101000**	**00000010**	**00000001**

Convert to dotted-decimal and the First Usable Host for this Network is 192.168.2.1

/24

Network Portion **Host Portion**

Network Address	**11000000**	**10101000**	**00000010**	**00000000**
First Usable Host Address	**11000000**	**10101000**	**00000010**	**00000001**
First Usable Host Dotted-Decimal	**192**	**168**	**2**	**1**

5F. Determining The Last Usable Host Address

Determine the Last Usable Host Addresses which will be all Binary 1s with a Binary 0 at the end of the Host Portion.

/24

Network Portion **Host Portion**

Network Address	11000000	10101000	00000010	00000000
Last Usable Host Address	**11000000**	**10101000**	**00000010**	

This is the opposite bit pattern of the First Usable Host.

/24

Network Portion **Host Portion**

Network Address	11000000	10101000	00000010	00000000
Last Usable Host Address	**11000000**	**10101000**	**00000010**	**11111110**

Convert to dotted-decimal and the Last Usable Host for this Network is 192.168.2.254

/24

Network Portion **Host Portion**

Network Address	11000000	10101000	00000010	00000000
Last Usable Host Address	**11000000**	**10101000**	**00000010**	**11111110**
Last Usable Host Dotted-Decimal	**192**	**168**	**2**	**254**

5G. To Recap Our Calculations

Given the HOst IP Address of 192.168.2.38/24, we determined:

- Using Binary ANDing, we determined that this Host belongs to the Network 192.168.2.0

- Network Address: 192.168.2.0
  - This is the address that identifies the network itself. It's used to define the entire network and cannot be assigned to a host.

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.2.0			

Keeping the Network Portion the same, but placing all Binary 1s in the Host Portion. We determined that the Broadcast Address for this Network is 192.168.2.255

- **Subnet Mask**: 255.255.255.0
  - This subnet mask indicates that the first 24 bits (or the first three octets) are used for the network portion and the last 8 bits (or the last octet) are used for host addresses.

- **In CIDR notation**, this is written as /24.
  - This notation represents a subnet mask where the first 24 bits are set to 1 (255.255.255.0). It allows for 256 IP addresses in total within this subnet.

- **Broadcast Address**: 192.168.2.255
  - This address is used to send data to all devices within the network. It is the highest address in the subnet and is used for broadcasting messages to all hosts in the subnet.

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.2.0			192.168.2.255

Keeping the Network Portion the same, but changing the Host Portion. We determined that the Usable Host range for assigning Addresses to devices on this Network is 192.168.2.1

- Which is one number up from the Network Address.

- First Usable Host: 192.168.2.1
  - This is the first IP address that can be assigned to a device within the network.
  - The address 192.168.2.0 is reserved for the network itself, so the first available IP address is 192.168.2.1.

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.2.0	192.168.2.1		192.168.2.255

192.168.2.254 which is one number down from the broadcast address.

- Last Usable Host: 192.168.2.254
  - This is the last IP address that can be assigned to a device within the network.
  - The address 192.168.2.255 is reserved for the broadcast address, so the last usable IP address is 192.168.2.254.

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.255

To determine whether a specific original host IP address falls within the range of your network, you'll need to check if the IP address falls between the first usable host and the last usable host in the subnet.

- Given the subnet:
  - Network Address: 192.168.2.0
  - First Usable Host: 192.168.2.1
  - Last Usable Host: 192.168.2.254
  - Broadcast Address: 192.168.2.255

- Any IP address in the range from 192.168.2.1 to 192.168.2.254 will be within this subnet.

- If you provide a specific IP address, I can tell you if it falls within this range. For example:
  - 192.168.2.50 is within the range.
  - 192.168.2.300 is not within the range (since it exceeds the maximum address of 192.168.2.255).

5H. Things To Keep In Mind - Understanding IPv4 Addresses

1. Structure of an IPv4 Address

- **Length:** Every IPv4 address is 32 bits long, which is typically represented in a dotted-decimal format like 192.168.1.1.

- **Division:** The address is split into two parts:
  - **Network Portion:** This portion identifies the specific network the device is on. It always starts from the left.
  - **Host Portion:** This identifies the specific device within the network. It takes up the remaining bits on the right.

2. Network vs. Host Portions

- The number of bits dedicated to the network vs. the host portion depends on the subnet mask, which defines how the 32 bits are split.

- **Example:** For an IP address 192.168.1.10 with a subnet mask of 255.255.255.0, the first 24 bits (192.168.1) are for the network, and the last 8 bits (.10) are for the host.

3. Reserved IPv4 Addresses

- **Network Address:**
  - **Definition:** This is the first address in the IP range, where all host bits are set to 0.
  - **Purpose:** It identifies the network itself, rather than any specific host.
  - **Example:** In the 192.168.1.0/24 network, 192.168.1.0 is the network address.

- **Broadcast Address:**
  - **Definition:** This is the last address in the IP range, where all host bits are set to 1.
  - **Purpose:** It's used to send data to all devices on the network simultaneously.
  - **Example:** In the 192.168.1.0/24 network, 192.168.1.255 is the broadcast address.

4. Practical Example

Let's consider a small network:

- **Network Address**: 192.168.1.0/24
  - **Binary Form:** 11000000.10101000.00000001.00000000

- **Subnet Mask**: 255.255.255.0 or /24
  - **Binary Form:** 11111111.11111111.11111111.00000000

- **Range of Usable Host Addresses**: 192.168.1.1 to 192.168.1.254
  - **Usable Hosts:** 254 addresses can be assigned to devices.

- **Broadcast Address**: 192.168.1.255
  - **Binary Form:** 11000000.10101000.00000001.11111111

In this network:

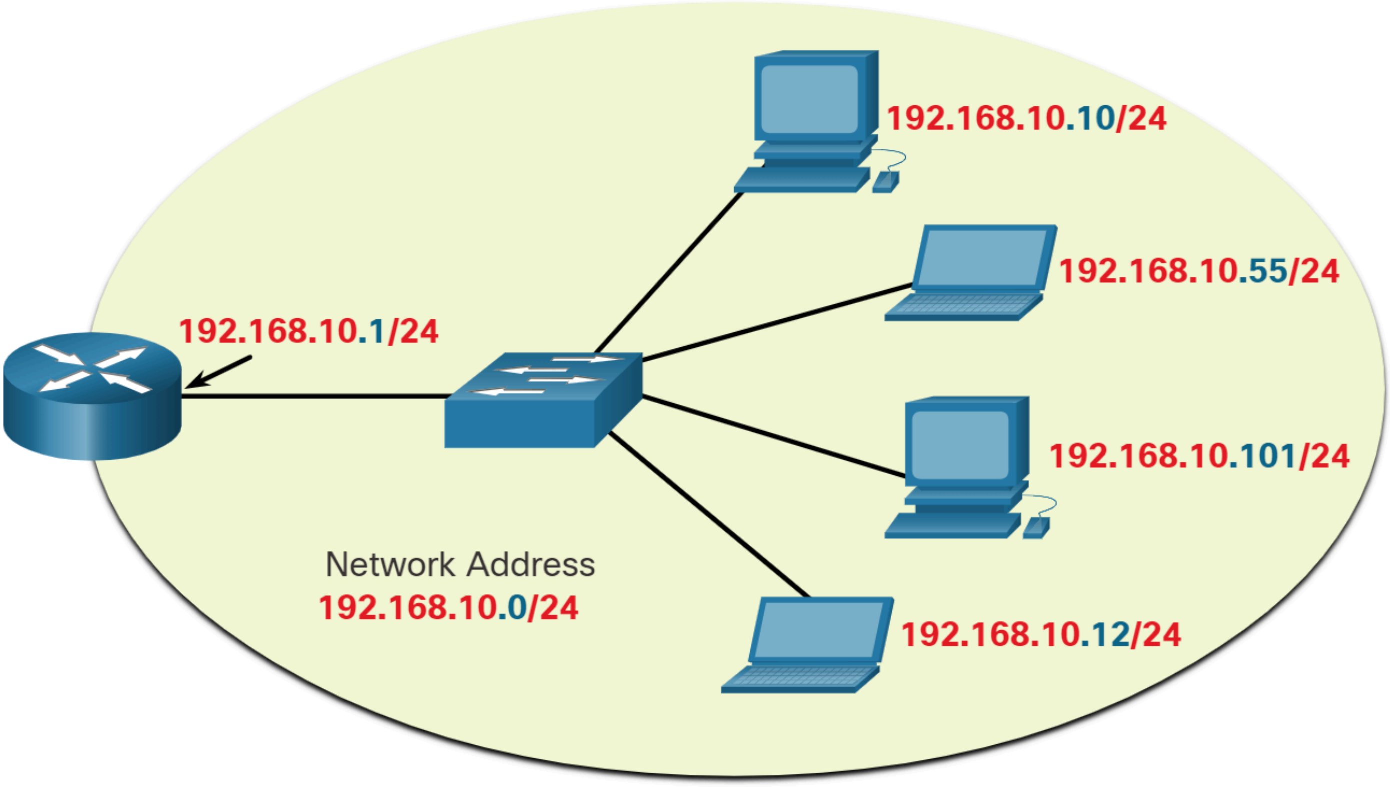
- 192.168.1.0 is the network address and cannot be assigned to any device.
- 192.168.1.255 is the broadcast address, also not assignable to devices.
- Devices on the network can have addresses like 192.168.1.1, 192.168.1.2, etc., up to 192.168.1.254.

6. Network, Host and Broadcast Addresses

Within each network are three types of IP addresses:

- Network Address
- Host Addresses
- Broadcast Address

Using the topology in the figure, these three types of addresses will be examined.



6A. Network Address

A network address is an address that represents a specific network. A device belongs to this network if it meets three criteria:

- It has the same subnet mask as the network address.
- It has the same network bits as the network address, as indicated by the subnet mask.
- It is located on the same broadcast domain as other hosts with the same network address.

A host determines its network address by performing an AND operation between its IPv4 address and its subnet mask.

Definition:

The network address is a unique identifier for a network segment within a larger network. It is the first address in a subnet and is used to identify the entire network in routing processes. This address is not assigned to any specific device; instead, it represents the network itself.

Purpose:

The network address helps routers determine how to route packets between different networks. It's essential for organizing and managing large networks, like those in businesses or internet service providers.

Example:

Imagine a classroom as a network, and each student is a device connected to that network. The network address would be like the room number of the classroom. It identifies the classroom as a whole but doesn't point to any specific student.

If you have an IP address 192.168.1.0/24 (where /24 indicates a subnet mask of 255.255.255.0), the network address would be 192.168.1.0. This address represents the entire network segment that includes all devices from 192.168.1.1 to 192.168.1.254.

6B. Network, Host, and Broadcast Addresses

As shown in the table, the network address has all 0 bits in the host portion, as determined by the subnet mask. In this example, the network address is 192.168.10.0/24. A network address cannot be assigned to a device.

	Network Portion			Host Portion	Host Bits
Subnet mask **255.255.255.**0 or **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Network address **192.168.10.**0 or **/24**	192 11000000	168 10101000	10 00001010	0 00000000	All 0s
First address **192.168.10.**1 or **/24**	192 11000000	168 10101000	10 00001010	1 00000001	All 0s and a 1
Last address **192.168.10.**254 or **/24**	192 11000000	168 10101000	10 00001010	254 11111110	All 1s and a 0
Broadcast address **192.168.10.**255 or **/24**	192 11000000	168 10101000	10 00001010	255 11111111	All 1s

The table shows how different types of IP addresses (Network Address, First Address, Last Address, and Broadcast Address) are derived from a given IP address with a subnet mask of 255.255.255.0 (or /24 in CIDR notation). Let's break down each row and column to understand it in detail.

Understanding the Columns:

- Network Portion: **This part of the IP address corresponds to the network identifier. It is defined by the subnet mask and remains consistent across all devices within the same network**.

- Host Portion: **This part of the IP address is specific to individual devices within the network. It varies from device to device and helps in identifying them uniquely within the network**.

- Host Bits: **These are the bits in the host portion that can vary. They determine the range of available IP addresses within the network**.

Breaking Down the Table Rows:

1. Subnet Mask (255.255.255.0 or /24)

- **Network Portion**: 255.255.255 translates to 11111111.11111111.11111111 in binary, meaning that the first three octets (24 bits) represent the network portion.

- **Host Portion**: 0 in the last octet (00000000 in binary) indicates that the last 8 bits are reserved for hosts.

- **Host Bits**: This row shows the subnet mask in binary format, with all host bits set to 0, which is used to distinguish between the network and host portions.

2. Network Address (192.168.10.0 or /24)

- **Network Portion**: The first three octets 192.168.10 correspond to the network portion and remain the same for all devices within the network.

- **Host Portion**: The last octet is 0 (all zeros in binary), indicating the network address itself, not a specific device.

- **Host Bits**: All zeros in the host portion mean this address is reserved as the network identifier.

3. First Address (192.168.10.1 or /24)

- **Network Portion**: Remains the same as 192.168.10.
- **Host Portion**: The last octet is 1 (all zeros and a 1 in binary), indicating the first usable IP address for a device within this network.
- **Host Bits**: The binary shows the transition from the network address (all zeros) to the first address by setting the least significant bit to 1.

4. Last Address (192.168.10.254 or /24)

- **Network Portion**: Again, it remains the same as 192.168.10.
- **Host Portion**: The last octet is 254 (all ones except the least significant bit in binary), indicating the last usable IP address for a device within this network.
- **Host Bits**: The host bits show all ones except for the last bit being 0, indicating the last device before the broadcast address.

5. Broadcast Address (192.168.10.255 or /24)

- **Network Portion**: Consistent with 192.168.10.
- **Host Portion**: The last octet is 255 (all ones in binary), which is reserved for broadcasting to all devices within the network.
- **Host Bits**: All ones in the host portion indicate this address is used to send messages to every device in the network.

Further Example:

Consider a company network using 192.168.20.0/24:

- **Subnet Mask**: 255.255.255.0
  - **Binary**: 11111111.11111111.11111111.00000000
  - This indicates the first 24 bits are for the network, and the last 8 bits are for hosts.

- **Network Address**: 192.168.20.0
  - **Binary**: 11000000.10101000.00010100.00000000
  - This is the identifier for the network.

- **First Address**: 192.168.20.1
  - **Binary**: 11000000.10101000.00010100.00000001
  - This would be the IP address of the first device on this network.

- **Last Address**: 192.168.20.254
  - **Binary**: 11000000.10101000.00010100.11111110
  - This would be the IP address of the last device before the broadcast.

- **Broadcast Address**: 192.168.20.255
  - **Binary**: 11000000.10101000.00010100.11111111
  - This address is used to send data to all devices within the 192.168.20.0/24 network.

Conclusion:

- **Network Address**: Identifies the network itself.
- **First Address**: The first available IP for a device on that network.
- **Last Address**: The last available IP for a device on that network.
- **Broadcast Address**: Used to communicate with all devices on that network.

Understanding these concepts is essential for network configuration, management, and ensuring that IP addresses are properly allocated without conflicts.

6C. Host Addresses

Host addresses are addresses that can be assigned to a device such as a host computer, laptop, smartphone, web camera, printer, router, etc. The host portion of the address is the bits indicated by 0 bits in the subnet mask. Host addresses can have any combination of bits in the host portion except for all 0 bits (this would be a network address) or all 1 bits (this would be a broadcast address).

All devices within the same network must have the same subnet mask and the same network bits. Only the host bits will differ and must be unique.

Notice that in the table, there is a first and last host address:

- **First Host Address** - This first host within a network has all 0 bits with the last (right-most) bit as a 1 bit. In this example, it is 192.168.10.1/24.
- **Last Host Address** - This last host within a network has all 1 bits with the last (right-most) bit as a 0 bit. In this example, it is 192.168.10.254/24.

Any addresses between and including, 192.168.10.1/24 through 192.168.10.254/24 can be assigned to a device on the network.

Definition:

Host addresses are the specific IP addresses assigned to individual devices (hosts) within a network. Each device on a network **must have a unique host address to communicate within and outside the network**.

Purpose:

Host addresses allow devices to communicate with each other and access network resources. Each device (like a computer, smartphone, printer) needs a unique host address to send and receive data.

Example:

Continuing with the classroom analogy, if the classroom is the network, each student represents a host. Each student has a unique name (host address) within the classroom. For instance, in the network 192.168.1.0/24, the host addresses would range from 192.168.1.1 to 192.168.1.254. Each device in this range can send and receive data packets.

6D. Broadcast Address

A broadcast address is an address that is used when it is required to reach all devices on the IPv4 network. As shown in the table, the network broadcast address has all 1 bits in the host portion, as determined by the subnet mask. In this example, the network address is 192.168.10.255/24. **A broadcast address cannot be assigned to a device**.

Definition:

The broadcast address is the last address in a network range and is used to send data to all devices within that network simultaneously. When a packet is sent to the broadcast address, it is delivered to every device on the network.

Purpose:

Broadcast addresses are used for sending information that needs to be received by every device in the network, such as network announcements, or when devices need to discover each other.

Example:

In the classroom analogy, the broadcast address would be like making an announcement over the classroom's loudspeaker. Every student (device) in the classroom (network) hears the message. For the network 192.168.1.0/24, the broadcast address would be 192.168.1.255. Sending a packet to this address means every device in the network segment receives the packet.

6E. Putting It All Together with an Example

Let's consider a network with the following details:

- **IP Address**: 192.168.1.0
- **Subnet Mask**: 255.255.255.0 (which is /24 in CIDR notation)

Network Address:

- **192.168.1.0**
  - **This identifies the entire network. No device can have this address; it's used by routers to know where to send data destined for the network**.

Host Addresses:

- **192.168.1.1** to **192.168.1.254**
  - Each address within this range can be assigned to a device (e.g., 192.168.1.5 could be a laptop, 192.168.1.10 could be a printer).

Broadcast Address:

- **192.168.1.255**
  - This address is used to communicate with all devices in the 192.168.1.0/24 network. For example, if the network administrator wants to alert all devices to an update, they would send a message to 192.168.1.255.

6F. Analogous Explanation

Imagine a large building with multiple offices:

- **Network Address:** This is like the address of the building itself, which identifies the entire building (e.g., "123 Main Street").

- **Host Addresses:** These are like the suite numbers within the building, each representing an individual office (e.g., "Suite 101," "Suite 102," etc.).

- **Broadcast Address:** This would be akin to the public announcement system in the building. An announcement made over the system reaches every suite in the building.

In essence:

- The **network address** identifies the network.
- The **host addresses** identify individual devices within the network.
- The **broadcast address** allows communication to all devices within that network.

Understanding these addresses is crucial for managing and routing data efficiently within and between networks.

7. Activity - ANDing to Determine the Network Address

Use the ANDing process to determine the network address (in binary and decimal formats). Identify the Network Address in binary & decimal.

Question 1:

Host Address	10	224	42	232
Subnet Mask	255	255	0	0
Host Address in binary	00001010	11100000	00101010	11101000
Subnet Mask in binary	11111111	11111111	00000000	00000000
Network Address in binary				
Network Address in decimal				

Answer:

Network Address In Binary: 00001010 11100000 00000000 00000000

Network Address In Decimal: 10 224 0 0

Question 2:

Host Address	172	20	145	109
Subnet Mask	255	255	225	192
Host Address in binary	10101100	00010100	10010001	01101101
Subnet Mask in binary	11111111	11111111	11111111	11000000
Network Address in binary				
Network Address in decimal				

Answer:

Network Address In Binary: 10101100 00010100 10010001 01000000

Network Address In Decimal: 172 20 145 64

Question 3:

Host Address	10	202	64	140
Subnet Mask	255	255	224	0
Host Address in binary	00001010	11001010	01000000	10001100
Subnet Mask in binary	11111111	11111111	11100000	00000000
Network Address in binary				
Network Address in decimal				

Answer:

Network Address In Binary: 00001010 11001010 01000000 00000000

Network Address In Decimal: 10 202 64 0

Question 4:

Host Address	10	94	179	147
Subnet Mask	255	255	255	240
Host Address in binary	00001010	01011110	10110011	10010011
Subnet Mask in binary	11111111	11111111	11111111	11110000
Network Address in binary				
Network Address in decimal				

Answer:

Network Address In Binary: 00001010 01011110 10110011 10010000

Network Address In Decimal: 10 94 179 144

Question 5:

Host Address	172	19	7	124
Subnet Mask	255	255	254	0
Host Address in binary	10101100	00010011	00000111	01111100
Subnet Mask in binary	11111111	11111111	11111110	00000000
Network Address in binary				
Network Address in decimal				

Answer:

Network Address In Binary: 10101100 00010011 00000110 00000000

Network Address In Decimal: 172 19 6 0

Question 6:

Host Address	10	210	227	39
Subnet Mask	255	255	255	248
Host Address in binary	00001010	11010010	11100011	00100111
Subnet Mask in binary	11111111	11111111	11111111	11111000
Network Address in binary				
Network Address in decimal				

Answer:

Network Address In Binary: 00001010 11010010 11100011 00100000

Network Address In Decimal: 10 210 227 32

8. Check Your Understanding - IPv4 Address Structure

Check your understanding of IPv4 address structure by choosing the correct answer to the following questions.

Question 1**:** Host-A has the IPv4 address and subnet mask 10.5.4.100 255.255.255.0. What is the network address of Host-A?

(a) 10.0.0.0

(b) 10.5.0.0

(c) 10.5.4.0

(d) 10.5.4.100

Answer: **(c) 10.5.4.0 - The network address for 10.5.4.100 with a subnet mask of 255.255.255.0 is 10.5.4.0.**

Question 2**:** Host-A has the IPv4 address and subnet mask 172.16.4.100 255.255.0.0. What is the network address of Host-A?

(a) 172.0.0.0

(b) 172.16.0.0

(c) 172.16.4.0

(d) 172.16.4.100

Answer: **(b) 172.16.0.0 - The network address for 172.16.4.100 with a subnet mask of 255.255.0.0 is 172.16.0.0.**

Question 3**:** Host-A has the IPv4 address and subnet mask 10.5.4.100 255.255.255.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

(a) 10.5.4.1

(b) 10.5.0.1

(c) 10.5.4.99

(d) 10.0.0.98

(e) 10.5.100.4

Answer: **(a) 10.5.4.1 & (c) 10.5.4.99 - Host A is on network 10.5.4.0. Therefore, devices with the IPv4 addresses 10.5.4.1 and 10.5.4.99 are on the same network.**

Question 4: Host-A has the IPv4 address and subnet mask 172.16.4.100 255.255.0.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

(a) 172.16.4.99

(b) 172.16.0.1

(c) 172.17.4.99

(d) 172.17.4.1

(e) 172.18.4.1

Answer: **(a) 172.16.4.99 & (b) 172.16.0.1 - Host A is on network 172.16.0.0; 255.255.0.0. Therefore, devices with the IPv4 addresses 172.16.4.99 and 172.16.0.1 are on the same network.**

Question 5: Host-A has the IPv4 address and subnet mask 192.168.1.50 255.255.255.0. Which of the following IPv4 addresses would be on the same network as Host-A? (Choose all that apply)

(a) 192.168.0.1

(b) 192.168.0.100

(c) 192.168.1.1

(d) 192.168.1.100

(e) 192.168.2.1

Answer: **(c) 192.168.1.1 & (d) 192.168.1.100 - Host A is on network 192.168.1.0. Therefore, devices with the IPv4 addresses 192.168.1.1 and 192.168.1.100 are on the same network.**

IPv4 Unicast, Broadcast, and Multicast

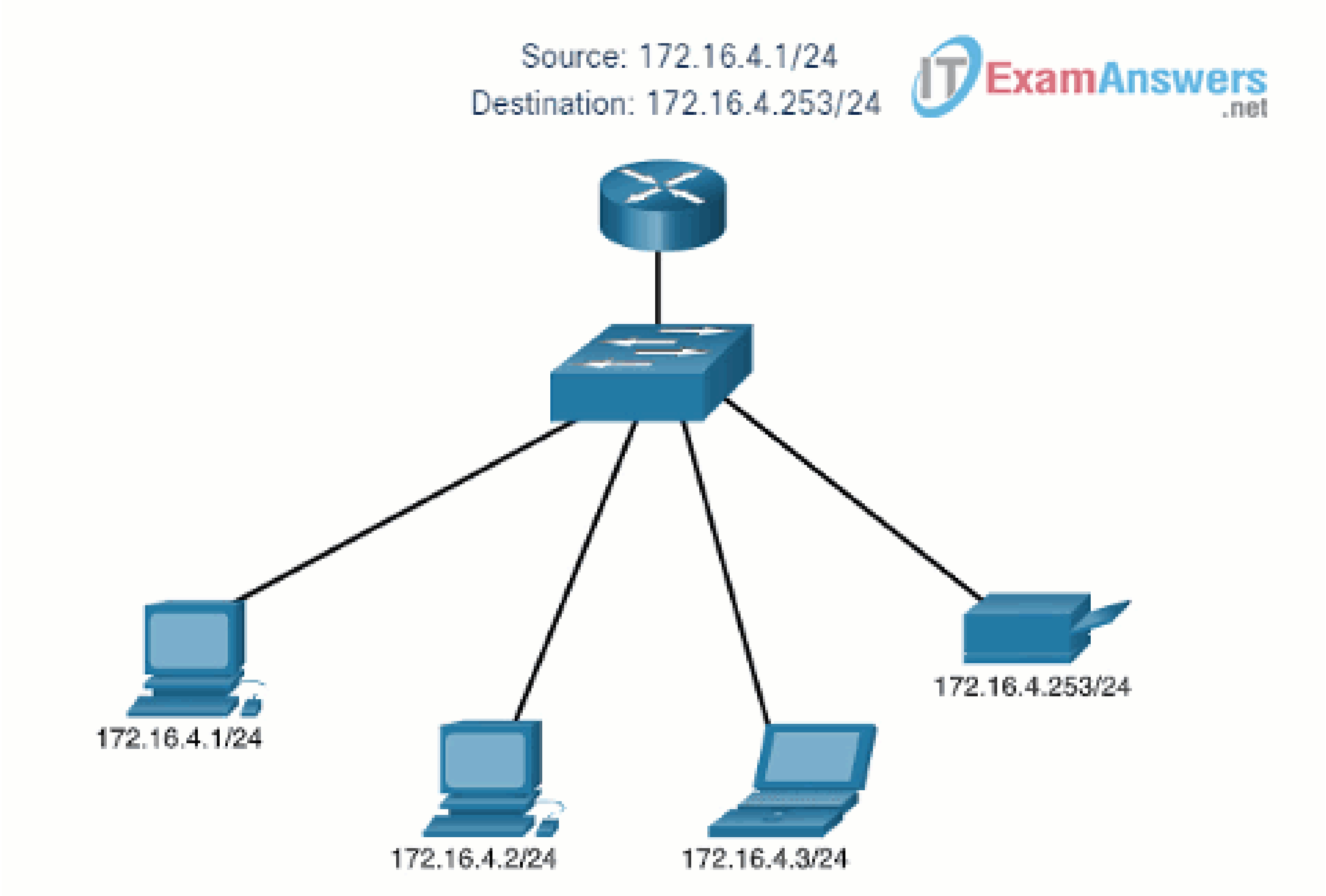
1. Unicast (One To One Communication)

In the previous topic, you learned about the structure of an IPv4 address; each has a network portion and a host portion. There are different ways to send a packet from a source device, and these different transmissions affect the destination IPv4 addresses.

Unicast transmission refers to one device sending a message to one other device in one-to-one communications.

A unicast packet has a destination IP address that is a unicast address which goes to a single recipient. A source IP address can only be a unicast address because the packet can only originate from a single source. This is regardless of whether the destination IP address is a unicast, broadcast or multicast.

Example Of Unicast Transmission.



Note: In this course, all communication between devices is unicast unless otherwise noted.

IPv4 unicast host addresses are in the address range of 1.0.0.1 to 223.255.255.255. However, within this range are many addresses that are reserved for special purposes. These special purpose addresses will be discussed later in this module.

2. Broadcast (One To Many Communication within same Network Address)

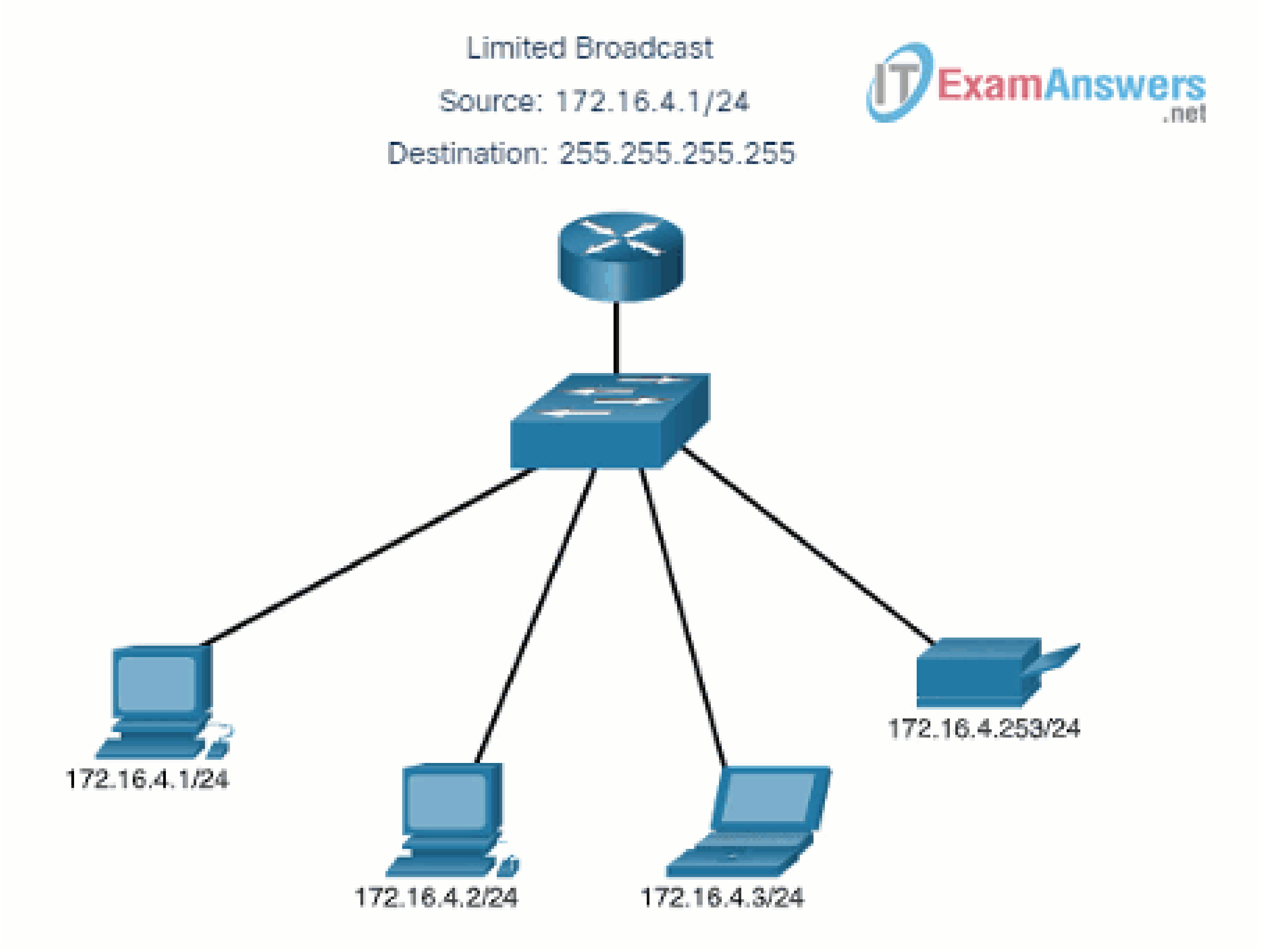
Broadcast transmission refers to a device sending a message to all the devices on a network in one-to-all communications.

A broadcast packet has a destination IP address with all ones (1s) in the host portion, or 32 one (1) bits.

Note: IPv4 uses broadcast packets. However, there are no broadcast packets with IPv6.

A broadcast packet must be processed by all devices in the same broadcast domain. A broadcast domain identifies all hosts on the same network segment. A broadcast may be directed or limited. A directed broadcast is sent to all hosts on a specific network. For example, a host on the 172.16.4.0/24 network sends a packet to 172.16.4.255. A limited broadcast is sent to 255.255.255.255. By default, routers do not forward broadcasts.

Example Of A Limited Broadcast Transmission.



Broadcast packets use resources on the network and make every receiving host on the network process the packet. Therefore, broadcast traffic should be limited so that it does not adversely affect the performance of the network or devices. Because routers separate broadcast domains, subdividing networks can improve network performance by eliminating excessive broadcast traffic.

IP Directed Broadcasts

In addition to the 255.255.255.255 broadcast address, there is a broadcast IPv4 address for each network. Called a directed broadcast, this address uses the highest address in the network, which is the address where all the host bits are 1s. For example, the directed broadcast address for 192.168.1.0/24 is 192.168.1.255. This address allows communication to all the hosts in that network. To send data to all the hosts in a network, a host can send a single packet that is addressed to the broadcast address of the network.

A device that is not directly connected to the destination network forwards an IP directed broadcast in the same way it would forward unicast IP packets destined to a host on that network. When a directed broadcast packet reaches a router that is directly connected to the destination network, that packet is broadcast on the destination network.

Note: Because of security concerns and prior abuse from malicious users, directed broadcasts are turned off by default starting with Cisco IOS Release 12.0 with the global configuration command **no IP directed-broadcasts**.

3. Multicast (One To All particular Network)

Multicast transmission reduces traffic by allowing a host to send a single packet to a selected set of hosts that subscribe to a multicast group.

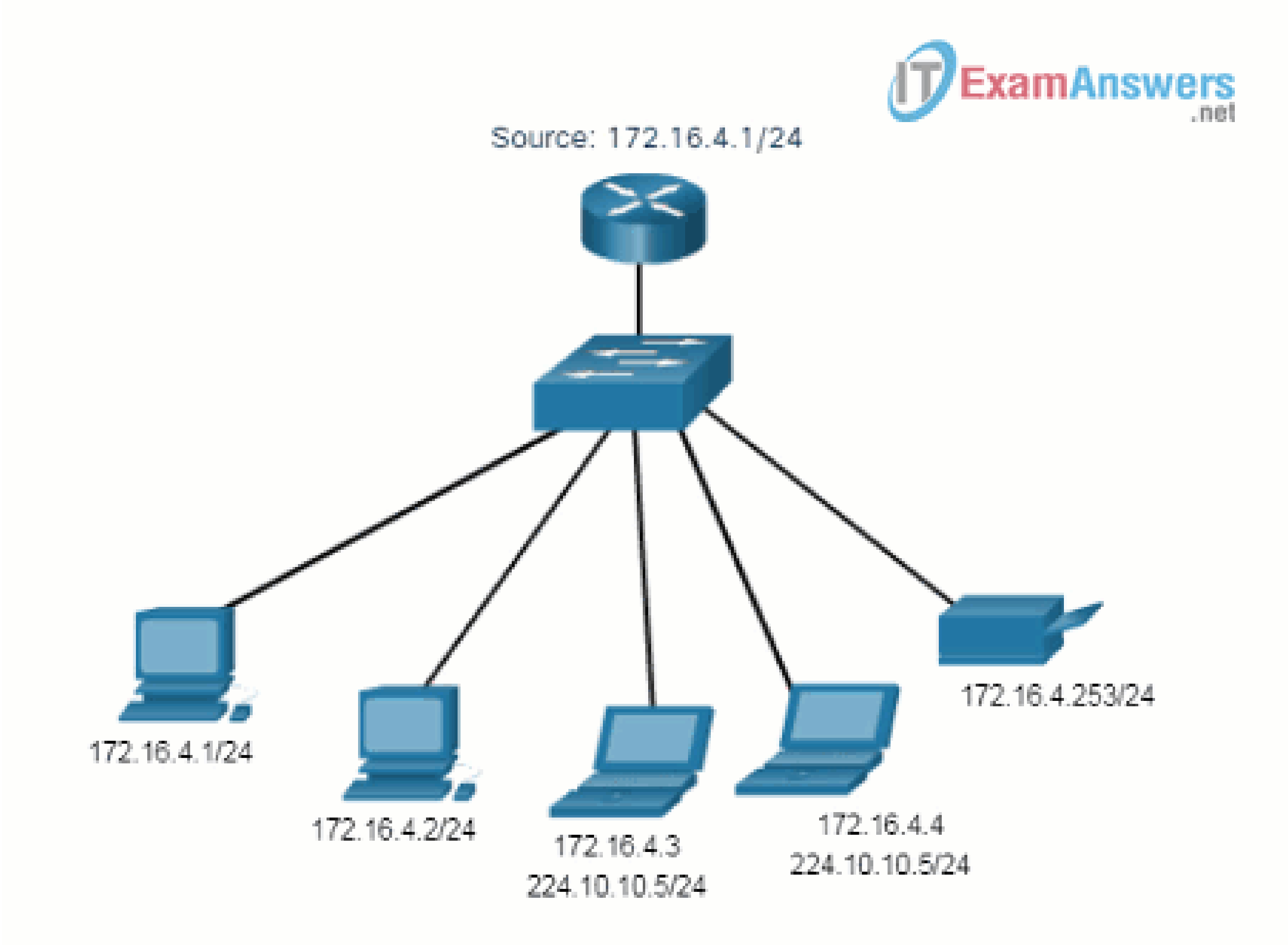
A multicast packet is a packet with a destination IP address that is a multicast address. **IPv4 has reserved the 224.0.0.0 to 239.255.255.255 addresses as a multicast range**.

Hosts that receive particular multicast packets are called multicast clients. The multicast clients use services requested by a client program to subscribe to the multicast group.

Each multicast group is represented by a single IPv4 multicast destination address. When an IPv4 host subscribes to a multicast group, the host processes packets addressed to this multicast address, and packets addressed to its uniquely allocated unicast address.

Routing protocols such as OSPF use multicast transmissions. For example, routers enabled with OSPF communicate with each other using the reserved OSPF multicast address 224.0.0.5. Only devices enabled with OSPF will process these packets with 224.0.0.5 as the destination IPv4 address. All other devices will ignore these packets.

An Example Of Demonstrates Clients Accepting Multicast Packets.



Types of IPv4 Addresses

1. Public and Private IPv4 Addresses

Just as there are different ways to transmit an IPv4 packet, there are also different types of IPv4 addresses. Some IPv4 addresses cannot be used to go out to the Internet, and others are specifically allocated for routing to the Internet. Some are used to verify a connection and others are self-assigned. As a network administrator, you will eventually become very familiar with the types of IPv4 addresses, but for now, you should at least know what they are and when to use them.

Public IPv4 addresses are addresses which are globally routed between internet service provider (ISP) routers. However, not all available IPv4 addresses can be used on the internet. There are blocks of addresses called private addresses that are used by most organizations to assign IPv4 addresses to internal hosts.

In the mid-1990s, with the introduction of the World Wide Web (WWW), private IPv4 addresses were introduced because of the depletion of IPv4 address space. **Private IPv4 addresses are not unique** and can be used internally within any network.

Note: The long-term solution to IPv4 address depletion was IPv6.

1A. The Private Address Blocks

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Note: Private addresses are defined in RFC 1918 and sometimes referred to as RFC 1918 address space.

1B. Public IPv4 Address

Definition:

A Public IPv4 address is an IP address that is assigned to devices that need to communicate with other devices over the internet. These addresses are **globally unique**, meaning no two devices can have the same public IP address at the same time. Public IP addresses are assigned by the **Internet Assigned Numbers Authority (IANA)** and distributed through **regional internet registries (RIRs)**.

Example:

Imagine your home network as a house, and each device inside your home (computer, smartphone, tablet) is a room in that house. The public IP address is like the house's street address. When someone sends a letter (data) to your house (network), the post office (internet) uses your street address (public IP address) to ensure it arrives at the right location.

Usage:

- A public IP address allows devices to be identified and accessed directly from the internet.
- Websites, email servers, and other internet-facing services use public IP addresses to communicate with users worldwide.

1C. Private IPv4 Address

Definition:

A Private IPv4 address is an IP address **used within a private network**, such as a home, office, or enterprise network. These addresses are not routable on the internet and are reserved for use within local networks. Private IP addresses are defined by specific ranges according to the **Internet Engineering Task Force (IETF)** in RFC 1918.

Example:

Continuing with the house analogy, private IP addresses are like the room numbers inside your house. Each room (device) has a unique number within the house (network), but this number is only meaningful within that context.

If you send a letter within your house (from one device to another within the same network), you only need the room number (private IP address) to identify where it should go.

Private IP Address Ranges:

- **10.0.0.0 to 10.255.255.255**: Commonly used in large corporate networks.
- **172.16.0.0 to 172.31.255.255**: Sometimes used in medium-sized networks.
- **192.168.0.0 to 192.168.255.255**: Widely used in home and small office networks.

Usage:

- Private IP addresses are used to communicate between devices within the same local network.
- Devices with private IP addresses need to use a Network Address Translation (NAT) service to communicate with devices on the internet.

1D. How to Differentiate Public and Private IPv4 Addresses

1. By Range:

- **Private IP Addresses**: Fall within the specific ranges mentioned above.
- **Public IP Addresses**: Any IP address that does not fall within the private ranges is considered a public IP address.

2. By Usage:

- **Private IP Addresses**: Used within local networks and cannot be accessed directly from the internet.
- **Public IP Addresses**: Used for devices that need to be accessible over the internet.

3. By Accessibility:

- **Private IP Addresses**: Cannot be routed on the internet, only within the local network.
- **Public IP Addresses**: Can be routed over the internet, allowing devices to communicate globally.

4. Example of Differentiation:

- **Home Network Example**:
  - Your router might have a public IP address like 203.0.113.5 provided by your Internet Service Provider (ISP). This is the address visible to the outside world.
  - Inside your home network, your devices might have private IP addresses like 192.168.1.2, 192.168.1.3, and so on. These are only visible within your local network.

- **Office Network Example**:
  - A company's web server might have a public IP address like 198.51.100.8, which customers use to access the company's website.
  - Employees' computers within the office network might have private IP addresses like 10.0.0.101, 10.0.0.102, etc., used for internal communication.

By understanding the differences in range, usage, and accessibility, you can easily differentiate between public and private IPv4 addresses.

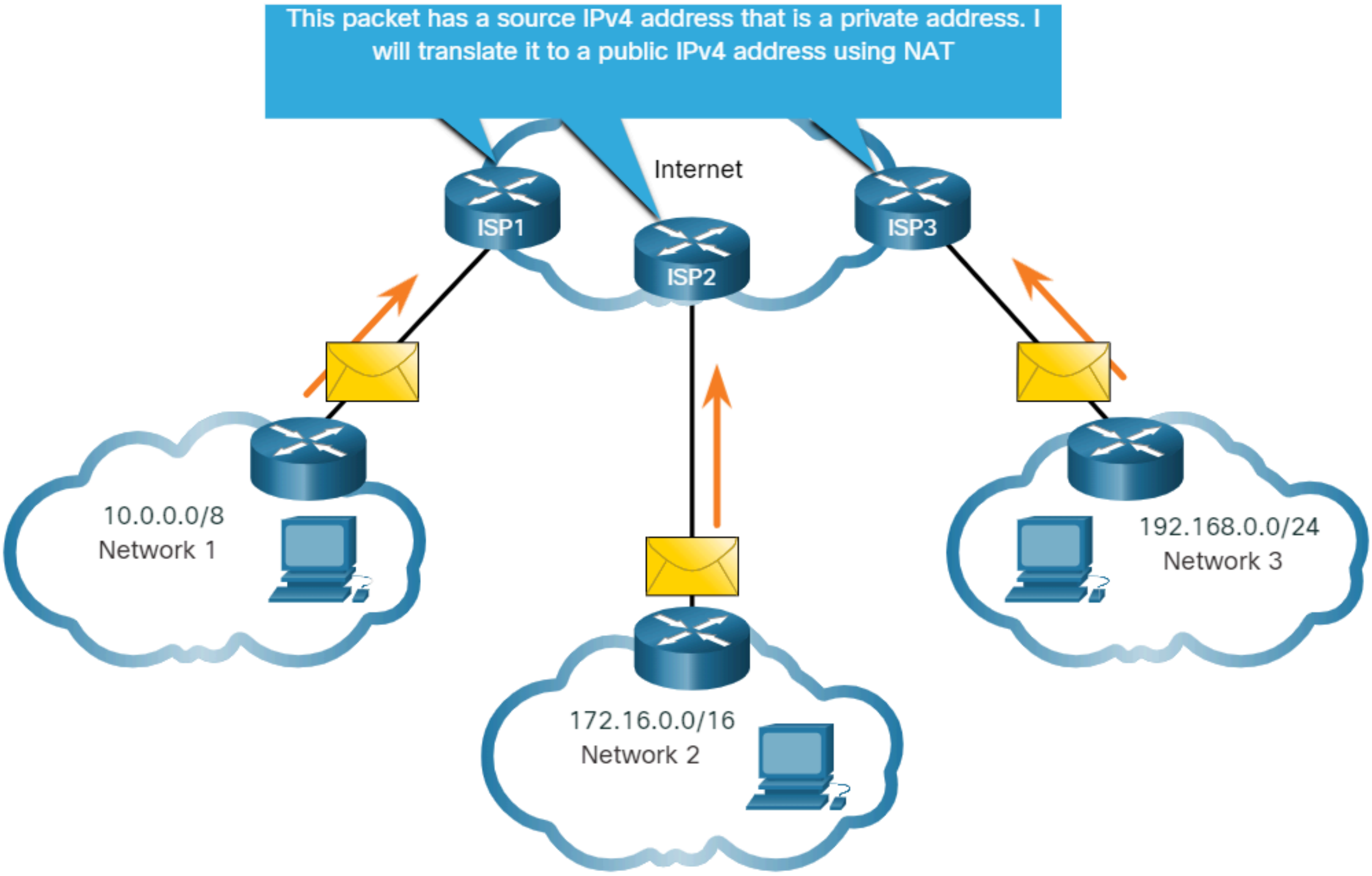
2. Routing to the Internet

Most internal networks, from large enterprises to home networks, use private IPv4 addresses for addressing all internal devices (intranet) including hosts and routers. However, private addresses are not globally routable.

In the figure, customer networks 1, 2, and 3 are sending packets outside their internal networks. These packets have a source IPv4 address that is a private address and a destination IPv4 address that is public (globally routable). Packets with a private address must be filtered (discarded) or translated to a public address before forwarding the packet to an ISP.

2A. Private IPv4 Addresses and Network Address Translation (NAT)

The diagram is a network topology with three networks, each connected to a different ISP router. The ISP routers are performing NAT between each network and the Internet.

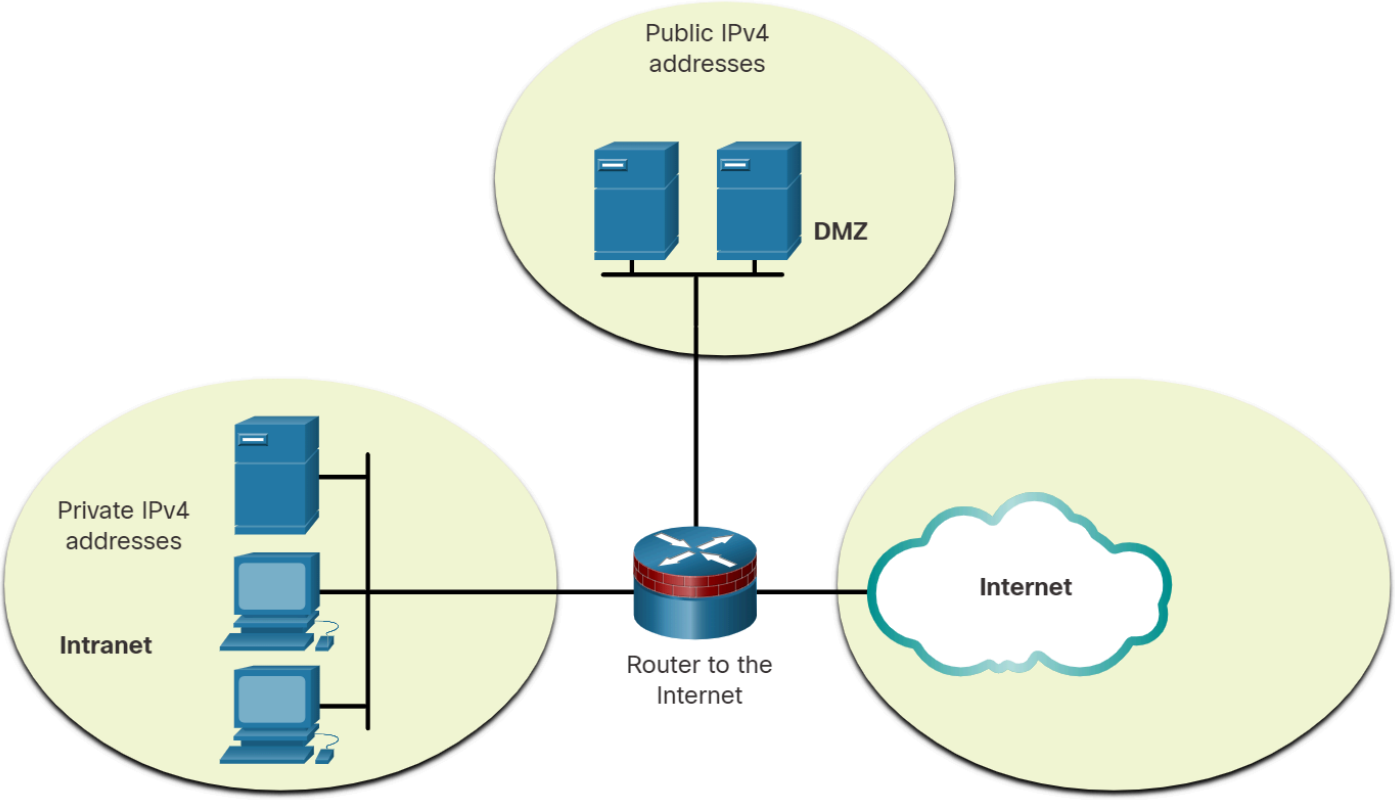

This packet has a source IPv4 address that is a private address. I will translate it to a public IPv4 address using NAT

Before the ISP can forward this packet, it must translate the source IPv4 address, which is a private address, to a public IPv4 address using Network Address Translation (NAT). NAT is used to translate between private IPv4 and public IPv4 addresses. This is usually done on the router that connects the internal network to the ISP network. Private IPv4 addresses in the organization’s intranet will be translated to public IPv4 addresses before routing to the internet.

Note: Although a device with a private IPv4 address is not directly accessible from another device across the internet, the IETF does not consider private IPv4 addresses or NAT as effective security measures.

Organizations that have resources available to the internet, such as a web server, will also have devices that have public IPv4 addresses. As shown in the figure, this part of the network is known as the DMZ (demilitarized zone). The router in the figure not only performs routing, it also performs NAT and acts as a firewall for security.

The diagram is a network topology showing a router in the center with three connections; one to the company Intranet, one to a DMZ, and one to the Internet. On the left is the Intranet with devices using private IPv4 addresses. At the top, is the DMZ with two servers using public IPv4 addresses. On the right is the Internet cloud. The router acts as a firewall and performs NAT.



Note: Private IPv4 addresses are commonly used for educational purposes instead of using a public IPv4 address that most likely belongs to an organization.

3. Special Use IPv4 Addresses

There are certain addresses, such as the network address and broadcast address, that cannot be assigned to hosts. There are also special addresses that can be assigned to hosts, but with restrictions on how those hosts can interact within the network.

3A. Loopback addresses

Loopback addresses (127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254) are more commonly identified as only 127.0.0.1, these are special addresses used by a host to direct traffic to itself. For example, it can be used on a host to test if the TCP/IP configuration is operational, as shown in the figure.

Notice how the 127.0.0.1 loopback address replies to the **ping** command. Also note how any address within this block will loop back to the local host, which is shown with the second **ping** in the figure.

i. Pinging the Loopback Interface

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad> ping 127.1.1.1
Pinging 127.1.1.1 with 32 bytes of data:
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Reply from 127.1.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.1.1.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\NetAcad>
```

3B. Link-Local addresses

Link-local addresses (169.254.0.0 /16 or 169.254.0.1 to 169.254.255.254) are more commonly known as Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses.

They are used by a Windows DHCP client to self-configure in the event that there are no DHCP servers available. Link-local addresses can be used in a peer-to-peer connection but are not commonly used for this purpose.

4. Legacy Classful Addressing

In 1981, IPv4 addresses were assigned using classful addressing as defined in RFC 790 (https://tools.ietf.org/html/rfc790), Assigned Numbers. Customers were allocated a network address based on one of three classes, A, B, or C. The RFC divided the unicast ranges into specific classes as follows:\

- **Class A (0.0.0.0/8 to 127.0.0.0/8)** - Designed to support extremely large networks with more than 16 million host addresses. Class A used a fixed /8 prefix with the first octet to indicate the network address and the remaining three octets for host addresses (more than 16 million host addresses per network).

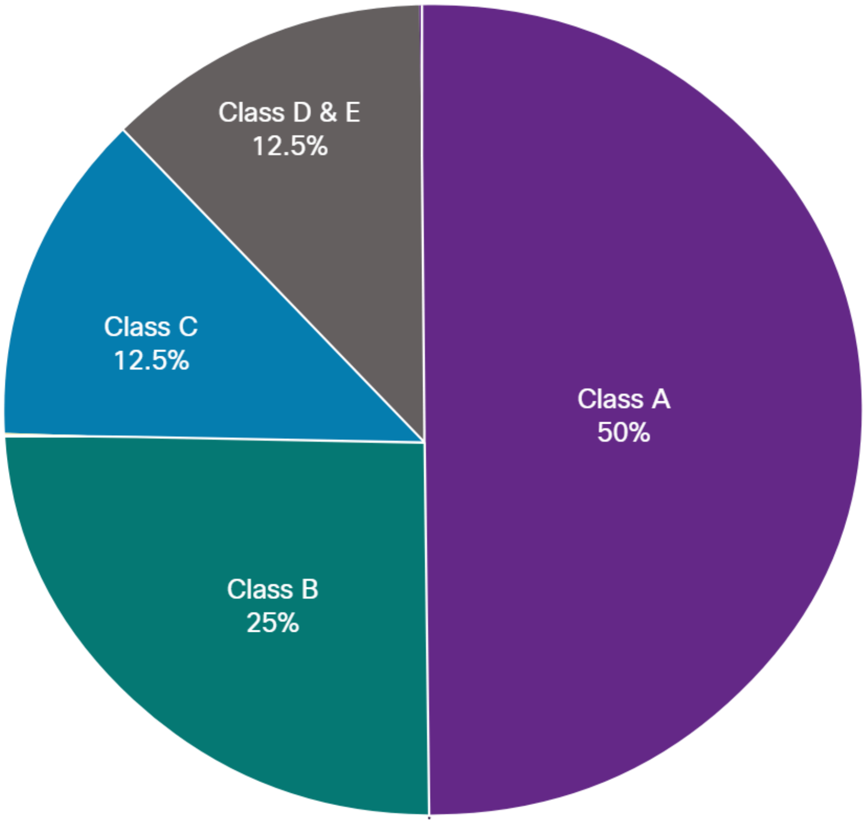
- **Class B (128.0.0.0 /16 - 191.255.0.0 /16)** - Designed to support the needs of moderate to large size networks with up to approximately 65,000 host addresses. Class B used a fixed /16 prefix with the two high-order octets to indicate the network address and the remaining two octets for host addresses (more than 65,000 host addresses per network).

- **Class C (192.0.0.0 /24 - 223.255.255.0 /24)** - Designed to support small networks with a maximum of 254 hosts. Class C used a fixed /24 prefix with the first three octets to indicate the network and the remaining one octet for the host addresses (only 254 host addresses per network).

Note: There is also a **Class D** multicast block consisting of **224.0.0.0 to 239.0.0.0** and a **Class E** experimental address block consisting of **240.0.0.0 - 255.0.0.0**.

At the time, with a limited number of computers using the internet, classful addressing was an effective means to allocate addresses. As shown in the figure, Class A and B networks have a very large number of host addresses and Class C has very few. Class A networks accounted for 50% of the IPv4 networks. This caused most of the available IPv4 addresses to go unused.

The diagram is a pie chart showing the percentage of Class A, B, C, D, & E IPv4 addressing with the total number of networks and hosts per Class A, B, and C networks. Percentages are: class A = 50%, class B = 25%, class C = 12.5%, and class D and E = 12.5%. For the total number of networks and the total number of hosts per network: class A = 128 networks with 16,777,214 total hosts per network; class B = 16,384 networks with 65,534 total hosts per network; and class C = 2,097,152 networks with 254 total hosts per network.



Class A

Total Networks: 128
Total Hosts/Net: 16,777,214

Class B

Total Networks: 16,384
Total Hosts/Net: 65,534

Class C

Total Networks: 2,097,152
Total Hosts/Net: 254

In the mid-1990s, with the introduction of the World Wide Web (WWW), classful addressing was deprecated to more efficiently allocate the limited IPv4 address space. Classful address allocation was replaced with classless addressing, which is used today. Classless addressing ignores the rules of classes (A, B, C). Public IPv4 network addresses (network addresses and subnet masks) are allocated based on the number of addresses that can be justified.

5. Assignment of IP Addresses

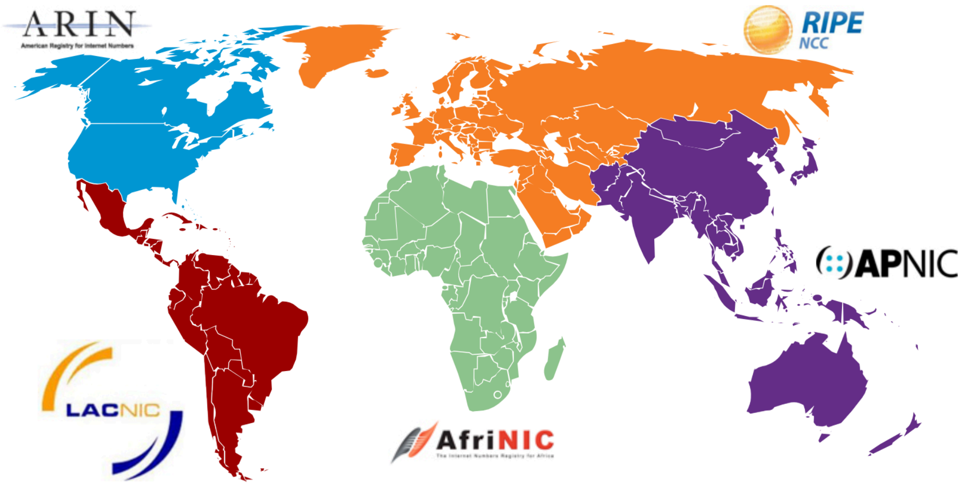
Public IPv4 addresses are addresses which are globally routed over the internet. Public IPv4 addresses must be unique.

Both IPv4 and IPv6 addresses are managed by the Internet Assigned Numbers Authority (IANA). The IANA manages and allocates blocks of IP addresses to the Regional Internet Registries (RIRs). The five RIRs are shown in the figure.

RIRs are responsible for allocating IP addresses to ISPs that provide IPv4 address blocks to organizations and smaller ISPs. Organizations can also get their addresses directly from an RIR (subject to the policies of that RIR).

5A. Regional Internet Registries

This figure shows the geographic locations of the Reginal Internet Registries (RIR). The regions governed by each RIR are as follows: AfriNIC (African Network Information Center) – serving the African region, APNIC (Asia Pacific Network Information Centre) – serving the Asia/Pacific Region, ARIN (American Registry for Internet Numbers) – serving the North America Region, LACNIC (Regional Latin-American and Caribbean IP Address Registry) – serving Latin America and some Caribbean Islands, and RIPE NCC (Reseaux IP Europeens Network Coordination Centre) – serving Europe, the Middle East, and Central Asia.



- **AfriNIC** (African Network Information Centre) - Africa Region
- **APNIC** (Asia Pacific Network Information Centre) - Asia/Pacific Region
- **ARIN** (American Registry for Internet Numbers) - North America Region
- **LACNIC** (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands
- **RIPE NCC** (Réseaux IP Européens Network Coordination Centre) - Europe, the Middle East, and Central Asia

5. Activity - Public or Private IPv4 Address

Instructions: Select Public or Private below each address to choose the correct network type.

Question 1: 172.16.35.2

(a) Public

(b) Private

Answer: **(b) Private**

Question 2: 192.168.3.5

(a) Public

(b) Private

Answer: **(b) Private**

Question 3: 192.0.3.15

(a) Public

(b) Private

Answer: **(a) Public**

Question 4: 64.104.0.22

(a) Public

(b) Private

Answer: **(a) Public**

Question 5: 209.165.201.30

(a) Public

(b) Private

Answer: **(a) Public**

Question 6: 192.168.11.5

(a) Public

(b) Private

Answer: **(b) Private**

Question 7: 172.16.30.30

(a) Public

(b) Private

Answer: **(b) Private**

Question 8: 10.55.3.168

(a) Public

(b) Private

Answer: **(b) Private**

6. Check Your Understanding - Types of IPv4 Addresses

Check your understanding of the types of IPv4 addresses by choosing the BEST answer to the following questions.

Question 1**: Which two statements are correct about private IPv4 addresses? (Choose two.)**

(a) Private IPv4 addresses are assigned to devices within an organization's intranet (internal network)

(b) Internet routers will typically forward any packet with a destination address that is a private IPv4 address

(c) 172.99.1.1 is a private IPv4 address.

(d) Any organization (home, school, office, company) can use the 10.0.0.0/8 address.

Answer: **(a) & (d) - Private IPv4 addresses are assigned to devices within an organization's intranet (internal network) and any organization (home, school, office, company) can use the 10.0.0.0/8 address.**

Question 2**: Which two statements are correct about public IPv4 addresses? (Choose two.)**

(a) Public IPv4 addresses are allowed to be assigned to devices within an organization's intranet (internal network).

(b) To access a device over the internet, the destination IPv4 address must be a public address.

(c) 192.168.1.10 is a public IPv4 address.

(d) Public IPv4 address exhaustion is a reason why there are private IPv4 addresses and why organizations are transitioning to IPv6.

Answer: **(b) & (d) - To access a device over the internet, the destination IPv4 address must be a public address. Public IPv4 address exhaustion is a reason why there are private IPv4 address and why organizations are transitioning to IPv6.**

Question 3**:** Which organization or group of organizations receives IP addresses from IANA and is responsible for allocating these addresses to ISPs and some organizations?

(a) IETF

(b) IEEE

(c) RIRs

(d) Tier 1 ISPs

Answer: **(c) RIRs - RIRs receive IP addresses from IANA and are responsible for allocating these addresses to ISPs and some other organizations.**

Network Segmentation

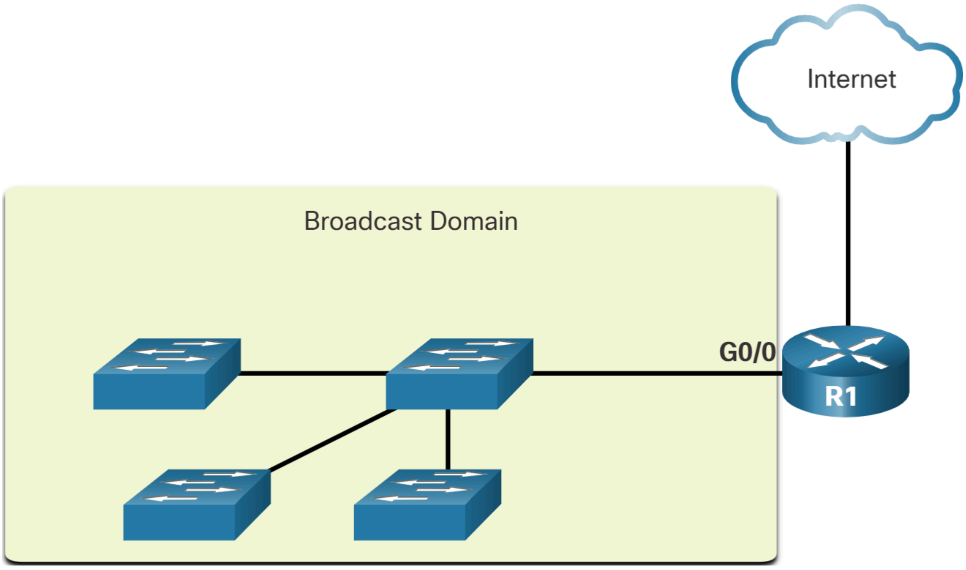
1. Broadcast Domains and Segmentation

Have you ever received an email that was addressed to every person at your work or school? This was a broadcast email. Hopefully, it contained information that each of you needed to know. But often a broadcast is not really pertinent to everyone in the mailing list. Sometimes, only a segment of the population needs to read that information.

In an Ethernet LAN, devices use broadcasts and the Address Resolution Protocol (ARP) to locate other devices.. ARP sends Layer 2 broadcasts to a known IPv4 address on the local network to discover the associated MAC address. Devices on Ethernet LANs also locate other devices using services. A host typically acquires its IPv4 address configuration using the Dynamic Host Configuration Protocol (DHCP) which sends broadcasts on the local network to locate a DHCP server.

Switches propagate broadcasts out all interfaces except the interface on which it was received. For example, if a switch in the figure were to receive a broadcast, it would forward it to the other switches and other users connected to the network.

1A. Routers Segment Broadcast Domains



Routers do not propagate broadcasts. When a router receives a broadcast, it does not forward it out to other interfaces. For instance, when R1 receives a broadcast on its Gigabit Ethernet 0/0 interface, it does not forward out another interface.

Therefore, each router interface connects to a broadcast domain and broadcasts are only propagated within that specific broadcast domain.

2. Problems with Large Broadcast Domains

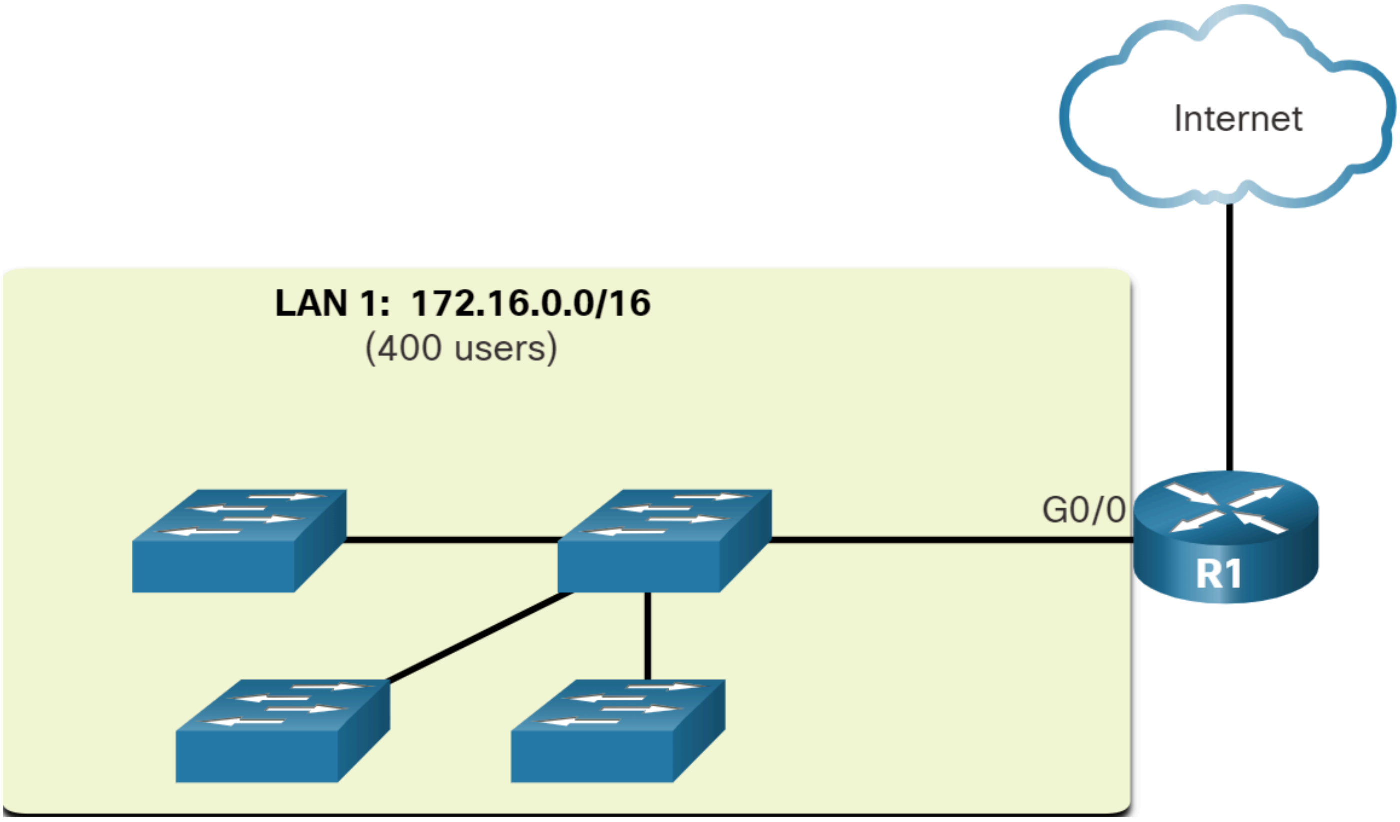
A large broadcast domain is a network that connects many hosts. A problem with a large broadcast domain is that these hosts can generate excessive broadcasts and negatively affect the network. In the figure, LAN 1 connects 400 users that could generate an excess amount of broadcast traffic. This results in slow network operations due to the significant amount of traffic it can cause, and slow device operations because a device must accept and process each broadcast packet.

2A. A Large Broadcast Domain

A router, R1, is connected to a switch via interface G0/0. The switch has connections to three other switches. The broadcast domain consists of the four switches and the router interface to which they are connected. This is identified as LAN1 with an address of 172.16.0.0/16. A connection from the router to the Internet is not within the broadcast domain.

The solution is to reduce the size of the network to create smaller broadcast domains in a process called subnetting. These smaller network spaces are called subnets.

In the figure, the 400 users in LAN 1 with network address 172.16.0.0 /16 have been divided 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. Therefore, a broadcast in LAN 1 would not propagate to LAN 2.

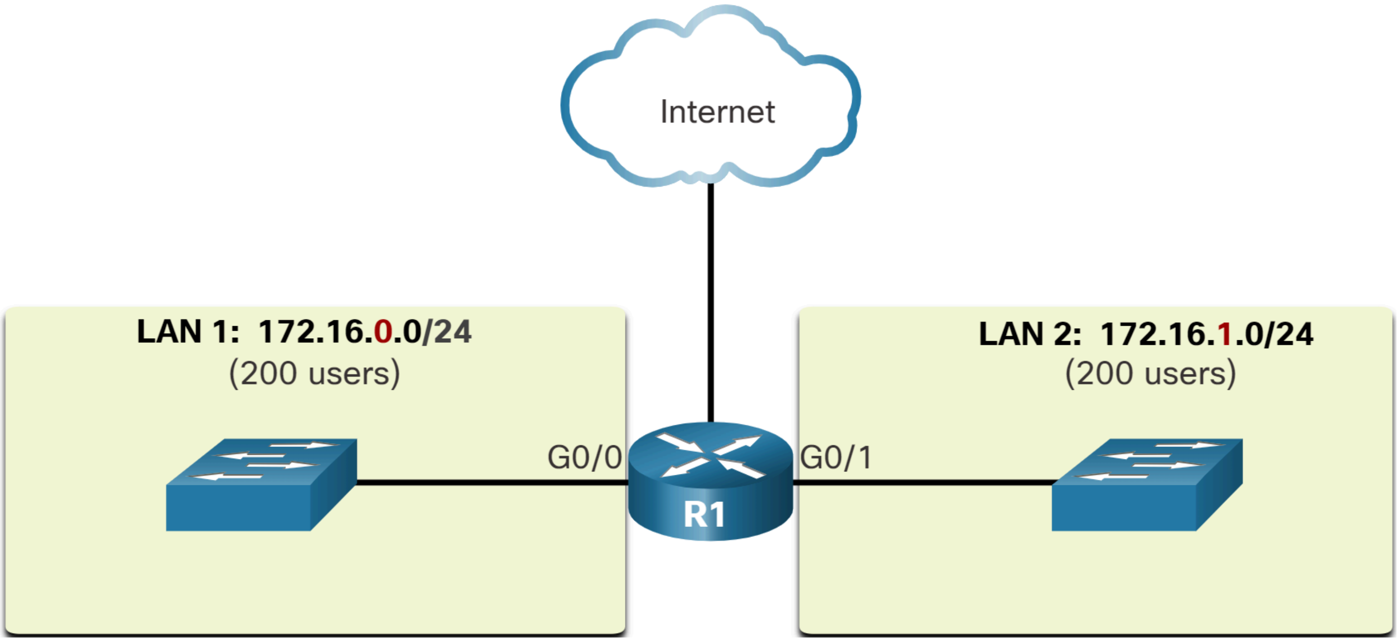


2B. Communicating Between Networks

A router, R1, is connected to two LANs which represent two different broadcast domains. Connected on the left via G0/0 is a switch supporting 200 users in LAN 1 with a network address of 172.16.0.0/24. Connected on the right via G0/1 is a switch supporting 200 users in LAN 2 with a network address of 172.16.1.0/24.

Notice how the prefix length has changed from a single /16 network to two /24 networks. This is the basis of subnetting: using host bits to create additional subnets.

Note: The terms subnet and network are often used interchangeably. Most networks are a subnet of some larger address block.



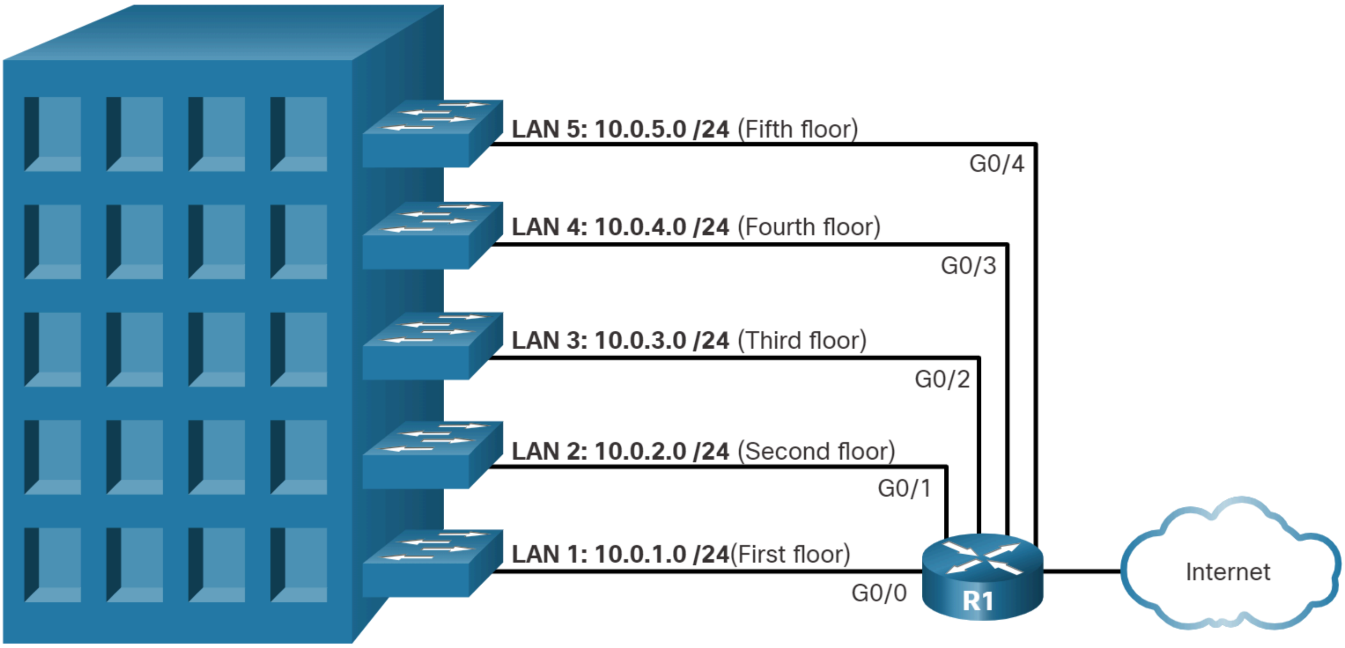
3. Reasons for Segmenting Networks

Subnetting reduces overall network traffic and improves network performance. It also enables an administrator to implement security policies such as which subnets are allowed or not allowed to communicate together. Another reason is that it reduces the number of devices affected by abnormal broadcast traffic due to misconfigurations, hardware/software problems, or malicious intent.

There are various ways of using subnets to help manage network devices.

3A. Location

Subnetting by Location


LAN 5: 10.0.5.0 /24 (Fifth floor)
G0/4
LAN 4: 10.0.4.0 /24 (Fourth floor)
G0/3
LAN 3: 10.0.3.0 /24 (Third floor)
G0/2
LAN 2: 10.0.2.0 /24 (Second floor)
G0/1
LAN 1: 10.0.1.0 /24(First floor)
G0/0
R1
Internet

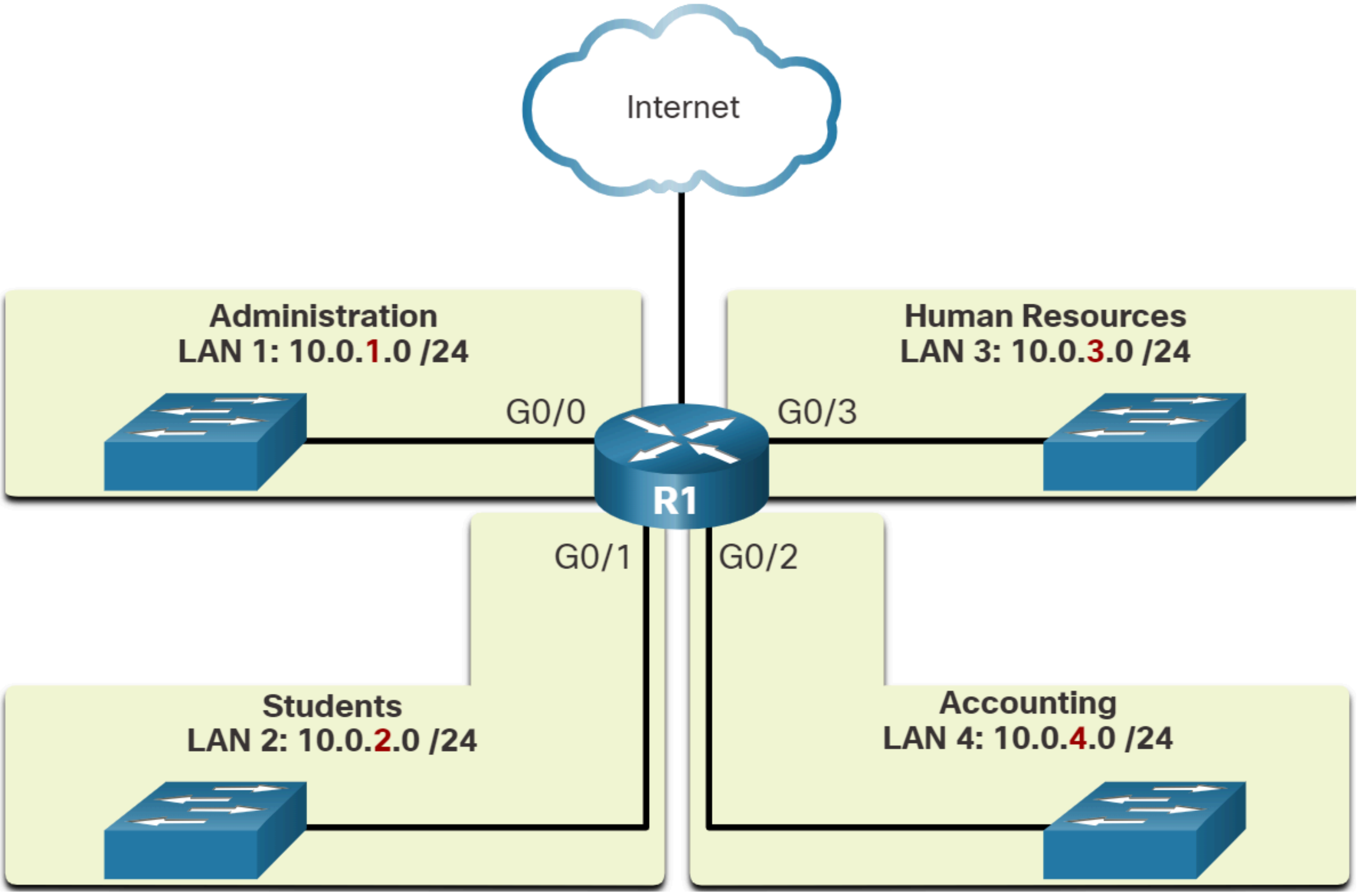
The diagram shows a five floor building with a switch on each floor. Each switch is on a different LAN/subnet with a different network address, all connected to the same router, R1, via a different gigabit Ethernet interface. The following subnets are shown from the first to the fifth floor: LAN 1 has a network address of 10.0.1.0/24 and is connected to G0/0; LAN 2 has a network address of 10.0.2.0/24 and is connected to G0/1; LAN 3 has a network address of 10.0.3.0/24 and is connected to G0/2; LAN 4 has a network address of 10.0.4.0/24 and is connected to G0/3; and LAN 5 has a network address of 10.0.5.0/24 and is connected to G0/4. R1 also has a connection to the Internet.

Network administrators can create subnets using any other division that makes sense for the network. Notice in each figure, the subnets use longer prefix lengths to identify networks.

Understanding how to subnet networks is a fundamental skill that all network administrators must develop. Various methods have been created to help understand this process. Although a little overwhelming at first, pay close attention to the detail and, with practice, subnetting will become easier.

3B. Group or Function

Subnetting by Group or Function



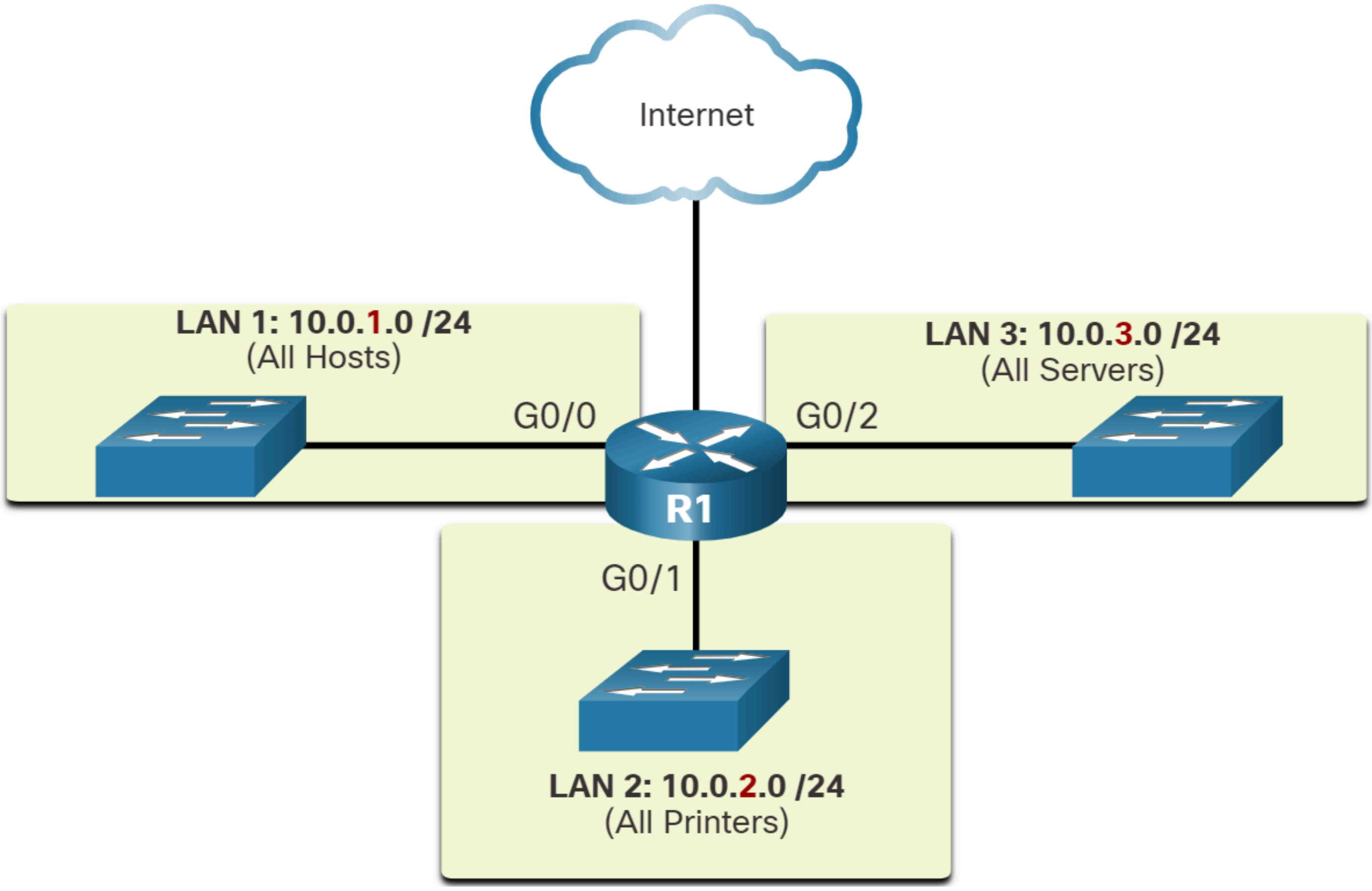
The diagram shows a router, R1, connecting four LANs/subnets together that have been assigned according to employee group. The administration subnet, LAN 1 at address 10.0.1.0/24, is connected to G0/0. The student subnet, LAN 2 at address 10.0.2.0/24, is connected to G0/1. The human resources subnet, LAN 3 at address 10.0.3.0/24, is connected to G0/3. The accounting subnet, LAN 4 at address 10.0.4.0/24, is connected to G0/2. R1 also has a connection to the Internet.

Network administrators can create subnets using any other division that makes sense for the network. Notice in each figure, the subnets use longer prefix lengths to identify networks.

Understanding how to subnet networks is a fundamental skill that all network administrators must develop. Various methods have been created to help understand this process. Although a little overwhelming at first, pay close attention to the detail and, with practice, subnetting will become easier.

3C. Device Type

Subnetting by Device Type



The diagram shows a router, R1, connecting three LANs/subnets together that have been assigned according to device type. LAN 1 at address 10.0.1.0/24 is connected to G0/0 and includes all hosts. LAN 2 at address 10.0.2.0/24 is connected to G0/1 and includes all printers. LAN 3 at address 10.0.3.0/24 is connected to G0/2 and includes all servers. R1 also has a connection to the Internet.

Network administrators can create subnets using any other division that makes sense for the network. Notice in each figure, the subnets use longer prefix lengths to identify networks.

Understanding how to subnet networks is a fundamental skill that all network administrators must develop. Various methods have been created to help understand this process. Although a little overwhelming at first, pay close attention to the detail and, with practice, subnetting will become easier.

4. Check Your Understanding - Network Segmentation

Check your understanding of the network segmentation by choosing the BEST answer to the following questions.

Question 1: Which devices will not forward an IPv4 broadcast packet by default?

(a) Ethernet switch

(b) router

(c) Windows PC

(d) None of the above. All devices forward IPv4 broadcast packets by default.

Answer: **(b) router - Routers will not forward an IPv4 broadcast packet by default.**

Question 2: Which two situations are the result of excessive broadcast traffic? (Choose two)

(a) slow network operations

(b) slow device operations

(c) when devices on all adjacent networks are affected

(d) when the router has to forward an excessive number of packets

Answer: **(a) slow network operations & (b) slow device operations - Slow network operations and slow device operations are the result of excessive broadcast traffic.**

Subnet an IPv4 Network

1. Subnet on an Octet Boundary

In the previous topic you learned several good reasons for segmenting a network. You also learned that segmenting a network is called subnetting. Subnetting is a critical skill to have when administering an IPv4 network. It is a bit daunting at first, but it gets much easier with practice.

IPv4 subnets are created by using one or more of the host bits as network bits. This is done by extending the subnet mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits that are borrowed, the more subnets that can be defined. The more bits that are borrowed to increase the number of subnets reduces the number of hosts per subnet.

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

1A. Subnet Masks on Octet Boundaries

To understand how subnetting on the octet boundary can be useful, consider the following example. Assume an enterprise has chosen the private address 10.0.0.0/8 as its internal network address. That network address can connect 16,777,214 hosts in one broadcast domain. Obviously, having more than 16 million hosts on a single subnet is not ideal.

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

1B. Subnetting Network 10.0.0.0/8 using a /16

The enterprise could further subnet the 10.0.0.0/8 address at the octet boundary of /16 as shown in the table. This would provide the enterprise the ability to define up to 256 subnets (i.e., 10.0.0.0/16 - 10.255.0.0/16) with each subnet capable of connecting 65,534 hosts. Notice how the first two octets identify the network portion of the address whereas the last two octets are for host IP addresses.

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

1C. Subnetting Network 10.0.0.0/8 using a /24 Prefix

Alternatively, the enterprise could choose to subnet the 10.0.0.0/8 network at the /24 octet boundary, as shown in the table. This would enable the enterprise to define 65,536 subnets each capable of connecting 254 hosts. The /24 boundary is very popular in subnetting because it accommodates a reasonable number of hosts and conveniently subnets at the octet boundary.

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 - 10.255.255.25**	**10.255.255.255**

2. Subnet within an Octet Boundary

The examples shown thus far borrowed host bits from the common /8, /16, and /24 network prefixes. However, subnets can borrow bits from any host bit position to create other masks.

For instance, a /24 network address is commonly subnetted using longer prefix lengths by borrowing bits from the fourth octet. This provides the administrator with additional flexibility when assigning network addresses to a smaller number of end devices. Refer to the table to see six ways to subnet a /24 network.

2A. 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

For each bit borrowed in the fourth octet, the number of subnetworks available is doubled, while reducing the number of host addresses per subnet:

- **/25 row** - Borrowing 1 bit from the fourth octet creates 2 subnets supporting 126 hosts each.
- **/26 row** - Borrowing 2 bits creates 4 subnets supporting 62 hosts each.
- **/27 row** - Borrowing 3 bits creates 8 subnets supporting 30 hosts each.
- **/28 row** - Borrowing 4 bits creates 16 subnets supporting 14 hosts each.
- **/29 row** - Borrowing 5 bits creates 32 subnets supporting 6 hosts each.
- **/30 row** - Borrowing 6 bits creates 64 subnets supporting 2 hosts each.

2B. Explanation

1. Understanding Subnets and Hosts

When you have a /24 network, it means the first 24 bits are used for the network, and the remaining 8 bits are for hosts. The subnet mask for /24 is 255.255.255.0.

2. Subnetting Concepts

Subnetting:

This is the process of dividing a network into smaller sub-networks (subnets). When you subnet, you're borrowing bits from the host portion to create more subnets.

Number of Subnets:

The number of subnets you can create depends on how many bits you borrow. For each bit you borrow, the number of subnets doubles.

Number of Hosts per Subnet:

The number of hosts in each subnet is determined by the remaining bits after borrowing. You **subtract 2** from the total number of hosts because the first address is used as the **network address**, and the last address is the **broadcast address**.

3. Calculating the Number of Subnets and Hosts

Original Network: /24

A /24 subnet is often represented as 255.255.255.0, which means the first 24 bits of the IP address are used for the network portion, and the remaining 8 bits are for the host portion.

Borrowing Bits: 1 Bit to Create /25 Subnets

When you borrow 1 bit from the host portion of the /24 subnet, you create a /25 subnet. The subnet mask for a /25 network would be 255.255.255.128, which uses 25 bits for the network portion and leaves 7 bits for the host portion.

Number of Subnets

Original Network (/24):

- In a /24 subnet, you have 8 bits available for hosts. All 8 bits can be used as part of the same network, allowing for a single large subnet.

Borrowed Bits:

- By borrowing 1 bit from the 8 bits available for hosts, you divide the original /24 network into 2 smaller subnets.

Calculation:

- The number of subnets is calculated using the formula: **Number of Subnets =** $2^{number\ of\ borrowed\ bits}$
- You **borrowed 1 bit**, so the number of subnets is 2^1 = **2**.
- This means you can create 2 subnets.

Example:

- Original /24 network: 192.168.1.0/24
- **Subnet 1**: 192.168.1.0/25 (Network address 192.168.1.0, subnet mask 255.255.255.128)
- **Subnet 2**: 192.168.1.128/25 (Network address 192.168.1.128, subnet mask 255.255.255.128)

Number of Hosts per Subnet

Original Network (/24):

- In a /24 network, 8 bits are available for hosts, which allows for 2^8 **- 2 = 256 - 2 = 254** hosts per subnet. The subtraction of 2 accounts for the network address (all host bits set to 0) and the broadcast address (all host bits set to 1).

New Subnets (/25):

- After borrowing 1 bit, 7 bits remain for hosts in each of the /25 subnets.

Calculation:

- The number of hosts per subnet is calculated using the **formula**:

  Number of Hosts per Subnet = $2^{Remaining\ Host\ Bits} - 2 = 2^7 - 2 = 128 - 2 = 126$

The "**- 2**" represents the **two IP addresses** in each subnet that are reserved and cannot be assigned to individual devices (hosts).

Here's what these two addresses are:

- **Network Address**: The first IP address in a subnet. It is used to identify the subnet itself. For example, in the subnet 192.168.1.0/25, 192.168.1.0 is the network address.

- **Broadcast Address**: The last IP address in a subnet. It is used to send data to all devices within that subnet. For example, in the subnet 192.168.1.0/25, 192.168.1.127 is the broadcast address.

These two addresses are subtracted from the total number of possible IP addresses in the subnet, which is why you see the formula for the number of usable hosts as 2^n - 2, where n is the number of bits allocated for the host portion. So, the "**- 2**" in 126 = 128 - 2 accounts for these two reserved addresses. The number **126** represents the total **usable host addresses** within each subnet.

Here's how it works:

- In any subnet, the first IP address is reserved as the **network address**, which identifies the subnet itself.
- The last IP address is reserved as the **broadcast address**, used to communicate with all devices within that subnet.

For a /25 subnet, which has 128 possible IP addresses, 2 are reserved (network and broadcast addresses). This leaves **126 usable IP addresses** that can be assigned to devices (hosts) within that subnet. So, the **126** is the number of devices (like computers, printers, or other networked devices) that can have unique IP addresses in each /25 subnet.

2C. Demonstration

To subnet a /24 network into smaller subnets, we'll need to understand how subnetting works and then apply that knowledge to calculate the subnet masks, number of subnets, and number of hosts per subnet for different prefix lengths.

Understanding the Basics of Subnetting

- **Prefix Length**: This specifies the number of bits used for the network portion of the IP address. In a /24 network, the prefix length is 24, meaning the first 24 bits are used for the network portion and the remaining bits are used for hosts.

- **Subnet Mask**: This is a 32-bit number that divides an IP address into network and host portions. For a /24 network, the subnet mask is 255.255.255.0.

- **Binary Representation**: This shows the subnet mask in binary form, where '1's represent the network portion and '0's represent the host portion.

- **Number of Subnets and Hosts**: The number of subnets and hosts depends on how many bits are borrowed from the host portion to create more network bits.

Subnetting Calculations

Let's break down each subnet size:

/25 Subnet

- **Subnet Mask**: 255.255.255.128

- **Binary Representation**: 11111111.11111111.11111111.10000000

- **Prefix Length**: /25 (The first 25 bits are network bits)

- **Number of Subnets**: To calculate the number of subnets, we use the formula 2^N, where n is the number of bits borrowed. Here, n=1 (since /25 is one bit more than /24).
  - **Number of Subnets = 2^1 = 2**

- **Number of Hosts**: The number of hosts per subnet is $2^{(32-prefix\ length)}$ **− 2**. Subtracting 2 accounts for the network and broadcast addresses.
  - **Number of Hosts = $2^{(32-25)}$ − 2 = 2^7 − 2 = 126**

/26 Subnet

- **Subnet Mask**: 255.255.255.192
- **Binary Representation**: 11111111.11111111.11111111.11000000
- **Prefix Length**: /26 (The first 26 bits are network bits)
- **Number of Subnets**: n = 2 (since /26 is two bits more than /24).
  - **Number of Subnets =** 2^{2} **= 4**
- **Number of Hosts**:
  - **Number of Hosts =** $2^{(32-26)}$ **− 2 =** 2^{6} **− 2 = 62**

/27 Subnet

- **Subnet Mask**: 255.255.255.224
- **Binary Representation**: 11111111.11111111.11111111.**111**00000
- **Prefix Length**: /27 (The first 27 bits are network bits)
- **Number of Subnets**: n = **3** (since /27 is three bits more than /24).
  - **Number of Subnets =** 2^{3} **= 8**
- **Number of Hosts**:
  - **Number of Hosts =** $2^{(32-27)}$ **− 2 =** 2^{5} **− 2 = 30**

/28 Subnet

- **Subnet Mask**: 255.255.255.240
- **Binary Representation**: 11111111.11111111.11111111.11110000
- **Prefix Length**: /28 (The first 28 bits are network bits)
- **Number of Subnets**: n=4 (since /28 is four bits more than /24).
    - **Number of Subnets =** 2^4 **= 16**
- **Number of Hosts**:
    - **Number of Hosts =** $2^{(32-28)}$ **− 2 =** 2^4 **− 2 = 14**

/29 Subnet

- **Subnet Mask**: 255.255.255.248
- **Binary Representation**: 11111111.11111111.11111111.11111000
- **Prefix Length**: /29 (The first 29 bits are network bits)
- **Number of Subnets**: n = 5 (since /29 is five bits more than /24)
    - **Number of Subnets =** 2^5 **= 32**
- **Number of Hosts**:
    - **Number of Hosts =** $2^{(32-29)}$ **− 2 =** 2^3 **− 2 = 6**

/30 Subnet

- **Subnet Mask**: 255.255.255.252

- **Binary Representation**: 11111111.11111111.11111111.11111100

- **Prefix Length**: /30 (The first 30 bits are network bits)

- **Number of Subnets**: n=6 (since /30 is six bits more than /24).
  - **Number of Subnets =** 2^{6} **= 64**

- **Number of Hosts**:
  - **Number of Hosts =** $2^{(32-30)}$ **− 2 =** 2^{2} **− 2 = 2**

3. The Subnet Mask

3A. The Purpose Of The Subnet Mask

The subnet mask plays a crucial role in IPv4 addressing, particularly in the process of subnetting. To understand its purpose, let's break down the concept with detailed explanations and examples, focusing on how the subnet mask works in conjunction with an IP address to determine the network address.

1. What is a Subnet Mask?

A subnet mask is a 32-bit number that masks an IP address and divides it into two parts:

- **Network Portion**: Identifies the specific network on which the device resides.
- **Host Portion**: Identifies the specific device (or host) within that network.

The subnet mask works by defining which part of the IP address is the network portion and which part is the host portion. This is done by representing the network portion with binary 1s and the host portion with binary 0s in the subnet mask.

2. The Role of ANDing in Determining the Network Address

When a computer or router receives an IP address and its corresponding subnet mask, it performs a process called **logical ANDing** to find the network address. The ANDing process compares each bit of the IP address with the corresponding bit of the subnet mask.

ANDing Process:

- **True AND True = True (1 AND 1 = 1)**
- **True AND False = False (1 AND 0 = 0)**
- **False AND False = False (0 AND 0 = 0)**

	Network Portion	Network Portion	Network Portion	Host Portion
IP Address	192	168	1	10
IP Address (Binary)	1100 0000	1010 1000	0000 0001	0000 1010
Subnet Mask	255	255	255	0
Subnet Mask (Binary)	1111 1111	1111 1111	1111 1111	0000 0000
Network Address (ANDing)	1100 0000	1010 1000	0000 0001	0000 0000
Network Address (Binary)	192	168	1	0

3B. Understanding Non-Classful Subnet Masks (Classless Inter-Domain Routing - CIDR)

Classful Subnet Masks:

Traditionally, IP addresses were divided into classes based on the first few bits of the address, with default subnet masks:

- **Class A:** 255.0.0.0 (/8)
- **Class B:** 255.255.0.0 (/16)
- **Class C:** 255.255.255.0 (/24)

These masks determined how much of the IP address was used for the network portion and how much was left for host addresses within that network.

Classless Subnet Masks:

Classless Inter-Domain Routing (CIDR) allows for more flexible subnetting. Instead of being restricted to the default subnet masks, you can use any subnet mask, which allows for more precise allocation of IP addresses. This is crucial in conserving IP address space, especially with the exhaustion of IPv4 addresses.

How Classless Subnetting Works

Example 1: /25 Subnet Mask (255.255.255.128)

- **IP Address**: 192.168.1.0
- **Subnet Mask**: 255.255.255.128 (/25)

A /25 subnet mask means that the first 25 bits of the IP address are used for the network portion, and the remaining 7 bits are used for host addresses.

- **Binary Representation**:
  - **Network Portion (25 bits):** 11000000.10101000.00000001.0 (from 192.168.1.x)
  - **Host Portion (7 bits):** 00000000 to 01111111 (0 to 127 in decimal)

This allows for 2^7 = 128 possible IP addresses. However, one address is reserved for the network (192.168.1.0), and one for the broadcast (192.168.1.127), leaving 126 usable IP addresses.

- **Subnets Created**:
  - 192.168.1.0/25 (network address: 192.168.1.0, broadcast address: 192.168.1.127)
  - **Usable Range:** 192.168.1.1 - 192.168.1.126

This splits the original /24 network (which could support 256 IP addresses) into two smaller /25 networks, each supporting 128 addresses.

Example 2: /18 Subnet Mask (255.255.192.0)

- **IP Address**: 172.16.0.0
- **Subnet Mask**: 255.255.192.0 (/18)

A /18 subnet mask means that the first 18 bits of the IP address are used for the network portion, and the remaining 14 bits are used for host addresses.

- **Binary Representation**:
  - **Network Portion (18 bits):** 10101100.00010000.00 (from 172.16.x.x)
  - **Host Portion (14 bits):** 00000000000000 to 00111111111111 (0 to 16,383 in decimal)

This allows for 2^{14} = 16,384 possible IP addresses. Subtracting the network and broadcast addresses gives 16,382 usable addresses.

- **Subnets Created**:
  - 172.16.0.0/18 (network address: 172.16.0.0, broadcast address: 172.16.63.255)
  - **Usable Range:** 172.16.0.1 - 172.16.63.254

This splits the original /16 network (which could support 65,536 IP addresses) into smaller /18 networks, each supporting 16,384 addresses.

Example 3: /12 Subnet Mask (255.240.0.0)

- **IP Address**: 10.0.0.0
- **Subnet Mask**: 255.240.0.0 (/12)

A /12 subnet mask means that the first 12 bits of the IP address are used for the network portion, and the remaining 20 bits are used for host addresses.

- **Binary Representation**:
  - **Network Portion (12 bits):** 00001010.0000 (from 10.x.x.x)
  - **Host Portion (20 bits):** 00000000000000000000 to 11111111111111111111 (0 to 1,048,575 in decimal)

This allows for 2^{20} = 1,048,576 possible IP addresses. Subtracting the network and broadcast addresses gives 1,048,574 usable addresses.

- **Subnets Created**:
  - 10.0.0.0/12 (network address: 10.0.0.0, broadcast address: 10.15.255.255)
  - **Usable Range:** 10.0.0.1 - 10.15.255.254

This splits the original /8 network (which could support 16,777,216 IP addresses) into smaller /12 networks, each supporting 1,048,576 addresses.

3C. Example: Subnetting a /24 Network

Starting Network: 192.168.1.0/24

Initial Setup:

- **Network Address**: 192.168.1.0
- **Subnet Mask**: /24 or 255.255.255.0
- **Binary Representation of Subnet Mask**: 11111111.11111111.11111111.00000000

Objective:

We want to create smaller subnets by borrowing bits from the host portion of the address. For this example, we'll borrow 1 bit to create a /25 subnet mask.

Subnetting Process:

- **New Subnet Mask**: /25
  - **Binary Representation of New Subnet Mask:** 11111111.11111111.11111111.10000000
  - **Decimal Representation:** 255.255.255.128

- **Number of Subnets**:
  - Borrowed Bits: 1
  - Number of Subnets = 2^1 = 2

- **Number of Host Bits**:
  - Remaining Bits for Hosts: 7
  - Number of Hosts per Subnet = 2^7 - 2 = 128 - 2 = 126 (subtracting 2 for network and broadcast addresses)

- **Subnetworks**:
  - **First Subnetwork:** 192.168.1.0/25
  - **Second Subnetwork:** 192.168.1.128/25

Understanding the Number of Hosts in a Subnet

In IP subnetting, the total number of IP addresses in a subnet includes both usable IP addresses and special addresses (network and broadcast addresses). Here's how it works:

Total Number of Addresses:

- Each subnet has a total number of IP addresses calculated by $2^{number\ of\ host\ bits}$. For a /25 subnet mask:
  - The subnet mask of /25 leaves 7 bits for hosts (32 - 25 = 7).
  - The total number of IP addresses in this subnet is 2^{7} = 128.

Special Addresses:

- **Network Address:** The first IP address in the subnet, used to identify the subnet itself.
- **Broadcast Address:** The last IP address in the subnet, used to send messages to all hosts in the subnet.

Usable Addresses:

- To get the number of usable IP addresses, you subtract the network address and the broadcast address from the total number of addresses.
- So, for a /25 subnet:
  - Total Addresses = 128
  - Network Address = 1 address
  - Broadcast Address = 1 address
  - Usable Addresses = 128 - 2 = 126

Why is 128 Not Usable?

- **Network Address (e.g., 192.168.1.0 in a /25 subnet):** This address represents the subnet itself. It cannot be assigned to a host.
- **Broadcast Address (e.g., 192.168.1.127 in a /25 subnet):** This address is used to broadcast messages to all hosts in the subnet. It also cannot be assigned to a host.

Example in Context

For the subnet 192.168.1.0/25:

- **Total Number of Addresses:** 128
- **Network Address:** 192.168.1.0
- **Broadcast Address:** 192.168.1.127
- **Usable IP Addresses:** 192.168.1.1 to 192.168.1.126 (126 addresses)

So, the 128 addresses include the network address and the broadcast address, which are not available for hosts. Thus, there are 126 usable addresses for devices in the subnet.

Steps to Calculate the Broadcast Address

Identify the Network Address and Subnet Mask:

- Network Address: 192.168.1.128
- Subnet Mask: 255.255.255.128 (or /25)

Convert the Subnet Mask to Binary:

- Subnet Mask (255.255.255.128) in binary: 11111111.11111111.11111111.10000000

Determine the Number of Host Bits:

- The subnet mask /25 means that 25 bits are used for the network portion and 7 bits are left for the host portion (32 - 25 = 7).

Calculate the Broadcast Address:

To find the broadcast address, you set all the host bits to 1 in the subnet's address range.

Detailed Calculation:

- **Network Address in Binary:**
  - 192.168.1.128 in binary: 11000000.10101000.00000001.10000000
- **Subnet Mask in Binary:**
  - 255.255.255.128: 11111111.11111111.11111111.10000000
- **Broadcast Address Calculation:**
  - In the subnet mask, the host bits are the bits after the 25th bit.
  - Set all these host bits to 1.

Example:

- **Network Address Binary:** 11000000.10101000.00000001.10000000
- **Broadcast Address Binary:** 11000000.10101000.00000001.11111111
- **Convert the Broadcast Address Binary to Decimal:**
  - **First Octet:** 11000000 = 192
  - **Second Octet:** 10101000 = 168
  - **Third Octet:** 00000001 = 1
  - **Fourth Octet:** 11111111 = 255
- **Resulting Broadcast Address:** 192.168.1.255

Steps to Calculate the Broadcast Address

Verification

To verify, you can check that all possible IP addresses in the subnet are correctly calculated:

- **Range Calculation for Subnet 192.168.1.128/25:**
  - **Network Address:** 192.168.1.128
  - **Broadcast Address:** 192.168.1.255
  - **Usable IP Range:** 192.168.1.129 to 192.168.1.254

Summary:

To find the broadcast address, convert the subnet mask to binary, determine which bits are used for the host portion, set all those bits to 1, and then convert the result back to decimal. For the subnet 192.168.1.128/25, the broadcast address is 192.168.1.255.

Details of Each Subnetwork:

Subnet 1: 192.168.1.0/25

- **Network Address:** 192.168.1.0
- **Broadcast Address:** 192.168.1.127
- **Usable IP Range:** 192.168.1.1 to 192.168.1.126

Subnet 2: 192.168.1.128/25

- **Network Address:** 192.168.1.128
- **Broadcast Address:** 192.168.1.255
- **Usable IP Range:** 192.168.1.129 to 192.168.1.254

Verification with Example IP Addresses:

Example IP Address 192.168.1.68:

- **Subnet Mask:** 255.255.255.128 (/25)
- **Network Address Calculation:**
    - Convert IP Address and Subnet Mask to Binary:
        - IP Address: 11000000.10101000.00000001.01000100
        - Subnet Mask: 11111111.11111111.11111111.10000000

    - Perform a Logical AND Operation:
        - Network Address = 11000000.10101000.00000001.00000000
        - Resulting Network Address = 192.168.1.0

- **Conclusion:** 192.168.1.68 is in the 192.168.1.0/25 subnet.

Verification with Example IP Addresses:

Example IP Address 192.168.1.138:

- **Subnet Mask:** 255.255.255.128 (/25)
- **Network Address Calculation:**
  - Convert IP Address and Subnet Mask to Binary:
    - IP Address: 11000000.10101000.00000001.10001010
    - Subnet Mask: 11111111.11111111.11111111.10000000
  - Perform a Logical AND Operation:
    - Network Address = 11000000.10101000.00000001.10000000
    - Resulting Network Address = 192.168.1.128
- **Conclusion:** 192.168.1.138 is in the 192.168.1.128/25 subnet.

Summary

By borrowing 1 bit from the host portion of the 192.168.1.0/24 network, we created two subnets with a /25 mask. Each subnet accommodates up to 126 hosts and has a distinct network and broadcast address. The subnetting process helps to efficiently utilize IP addresses and manage network traffic by creating smaller, manageable subnetworks.

4. Video - Subnet with the Magic Number Technique

The "magic number" in subnetting doesn't have a complex formula; instead, it's derived from the subnet mask. Here's how you determine the magic number:

Formula to Find the Magic Number:

- **Identify the Subnet Mask**: Convert the subnet mask into decimal form if it's given in CIDR notation (e.g., /24).
- **Locate the Last Non-Zero Octet in the Subnet Mask**: This is where the last 1 bit in the subnet mask resides.
- **Calculate the Magic Number**: The magic number is simply the place value of the last 1 bit in the binary representation of that octet.

Steps to Calculate the Magic Number:

- **Convert the Subnet Mask to Binary**: For example, let's say you have a subnet mask of /26, which in decimal is 255.255.255.192.
    - The binary form of 192 is 11000000.
- **Identify the Last 1 Bit**: In 11000000, the last 1 is in the 64 position (from the right). [Hint: Base 2 → 128 64 32 16 88 4 2 1]
- **Determine the Magic Number**: The magic number is 64.

Example:

Let's calculate the magic number for a /27 subnet mask:

- **Subnet Mask**: /27 in decimal is 255.255.255.224.
    - Convert 224 to binary: 11100000.
- **Last 1 Bit**: The last 1 bit is in the 32 position.
- **Magic Number**: The magic number is 32.

Magic Number Application:

This magic number tells you the increment between subnets. For example, if your base network is 192.168.1.0/27:

- Subnets will be 192.168.1.0, 192.168.1.32, 192.168.1.64, etc.

Summary of Magic Number Formula:

- **Magic Number** = Place value of the last 1 bit in the subnet mask binary representation.
    - This method simplifies finding the subnet boundaries, making it quicker to determine valid subnets in a network.

Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks, called subnets. The primary goal is to optimize the use of IP addresses and improve network efficiency.

One efficient way to determine these subnets is by using the "Magic Number" technique. This technique allows you to quickly and accurately identify the subnet boundaries without needing to perform complex calculations manually.

Let's break down the concept with an example and further details:

Example Scenario: Subnetting a /24 Network

Step 1: Understanding the Basics

- **IP Address**: 192.168.1.0/24
- **Subnet Mask**: 255.255.255.0

A /24 subnet mask means that the first 24 bits are used for the network portion, leaving the remaining 8 bits for hosts. This means the network is divided as follows:

- **Network Portion**: 192.168.1 (24 bits)
- **Host Portion**: 0-255 (8 bits)

With a /24 network, we have one large network with 256 addresses (0 to 255). However, we want to create smaller subnets within this network.

Step 2: Borrowing Bits

Borrowing bits from the host portion allows us to create subnets. The more bits we borrow, the more subnets we can create, but it reduces the number of available hosts per subnet.

Let’s start by borrowing 1 bit from the host portion:

- **New Subnet Mask**: /25 (255.255.255.128)
- **Subnetting**: 2^1 = 2 subnets
- **Host Addresses per Subnet**: 2^7 = 128 total addresses (126 usable)

Step 3: Introducing the Magic Number

The "Magic Number" is a quick way to identify subnet boundaries. It’s derived from the value of the least significant bit (the rightmost 1) in the subnet mask. This value tells us the size of each subnet and how to calculate the next subnet.

For a /25 subnet:

- **Subnet Mask:** 255.255.255.128 (Binary: 11111111.11111111.11111111.10000000)
- **Magic Number:** 128 (The last 1 in the binary subnet mask is in the 128's place)

This means the subnets will increment by 128. Starting at 192.168.1.0:

- **First Subnet:** 192.168.1.0/25
- **Second Subnet:** 192.168.1.128/25

Step 4: Borrowing More Bits & Applying the Magic Number to Different Subnet Masks

Let’s explore what happens if we borrow more bits:

i. Borrowing 2 Bits:

- **New Subnet Mask:** /26 (255.255.255.192)
- **Subnets:** 2^2 = 4 subnets
- **Host Addresses per Subnet:** 2^6 = 64 total addresses (62 usable)
- **Magic Number:** 64 (Subnet boundaries will increment by 64)

The subnets will be:

- **First Subnet:**
  - **Starting IP:** 192.168.1.0
  - **Range:** 192.168.1.0 - 192.168.1.63
  - **Broadcast Address:** 192.168.1.63

- **Second Subnet:**
  - **Starting IP:** 192.168.1.64 (192.168.1.0 + 64)
  - **Range:** 192.168.1.64 - 192.168.1.127
  - **Broadcast Address:** 192.168.1.127

- **Third Subnet:**
  - **Starting IP:** 192.168.1.128 (192.168.1.0 + 64 + 64)
  - **Range:** 192.168.1.128 - 192.168.1.191
  - **Broadcast Address:** 192.168.1.191

- **Fourth Subnet:**
  - **Starting IP:** 192.168.1.192 (192.168.1.0 + 64 + 64 + 64)
  - **Range:** 192.168.1.192 - 192.168.1.255
  - **Broadcast Address:** 192.168.1.255

Final Subnets

- **192.168.1.0/26:** Range 192.168.1.0 - 192.168.1.63
- **192.168.1.64/26:** Range 192.168.1.64 - 192.168.1.127
- **192.168.1.128/26:** Range 192.168.1.128 - 192.168.1.191
- **192.168.1.192/26:** Range 192.168.1.192 - 192.168.1.255

Each subnet has 64 addresses, with 62 usable for hosts (subtracting the network address and broadcast address).

ii. Borrowing 3 Bits:

- **New Subnet Mask:** /27 (255.255.255.224)
- **Subnets:** 2^3 = 8 subnets
- **Host Addresses per Subnet:** 2^5 = 32 total addresses (30 usable)
- **Magic Number:** 32 (Subnet boundaries will increment by 32)

The subnets will be:

- **192.168.1.0/27**
- **192.168.1.32/27**
- **192.168.1.64/27**
- **192.168.1.96/27**
- **192.168.1.128/27**
- **192.168.1.160/27**
- **192.168.1.192/27**
- **192.168.1.224/27**

Borrowing 4 Bits:

- **New Subnet Mask:** /28 (255.255.255.240)
- **Magic Number:** 16 (Subnet boundaries will increment by 16)

The subnets will be:

- **192.168.1.0/28**
- **192.168.1.16/28**
- **192.168.1.32/28**
- **192.168.1.48/28**
- **...**
- **192.168.1.240/28**

Borrowing 5 Bits:

- **New Subnet Mask:** /29 (255.255.255.248)
- **Magic Number:** 8 (Subnet boundaries will increment by 8)

The subnets will be:

- **192.168.1.0/29**
- **192.168.1.8/29**
- **192.168.1.16/29**
- **192.168.1.24/29**
- **…**
- **192.168.1.248/29**

Step 6: Larger Networks (Class A/B)

The magic number technique works similarly for larger networks. If you start with a Class B network like 172.16.0.0/16 and borrow bits, the magic number will help you determine subnets in larger octets.

For example:

- **Starting Network**: 172.16.0.0/16
- **Subnet Mask (Original)**: /16 (which is 255.255.0.0 in decimal)
- **Subnet Mask after Borrowing 7 Bits**: /23 (255.255.254.0)
- **Magic Number**: 2 (Subnet boundaries will increment by 2 in the third octet)

The subnets will be:

- **172.16.0.0/23 ------- 172.16.1.255/23**
- **172.16.2.0/23**
- **172.16.4.0/23**
- **...**

Summary

The Magic Number technique simplifies the process of subnetting by providing a straightforward way to calculate subnet boundaries.

By identifying the last 1 in the subnet mask and converting its position to a decimal value, you can quickly determine the increment size for each subnet.

This method is both efficient and practical, especially when working with different classes of IP networks.

5. Packet Tracer - Subnet an IPv4 Network

5A. Background / Scenario

In this activity, starting from a single network address and network mask, you will subnet the Customer network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

After you have created a subnetting scheme and completed the table by filling in the missing host and interface IP addresses, you will configure the host PCs, switches and router interfaces.

After the network devices and host PCs have been configured, you will use the **ping** command to test for network connectivity.

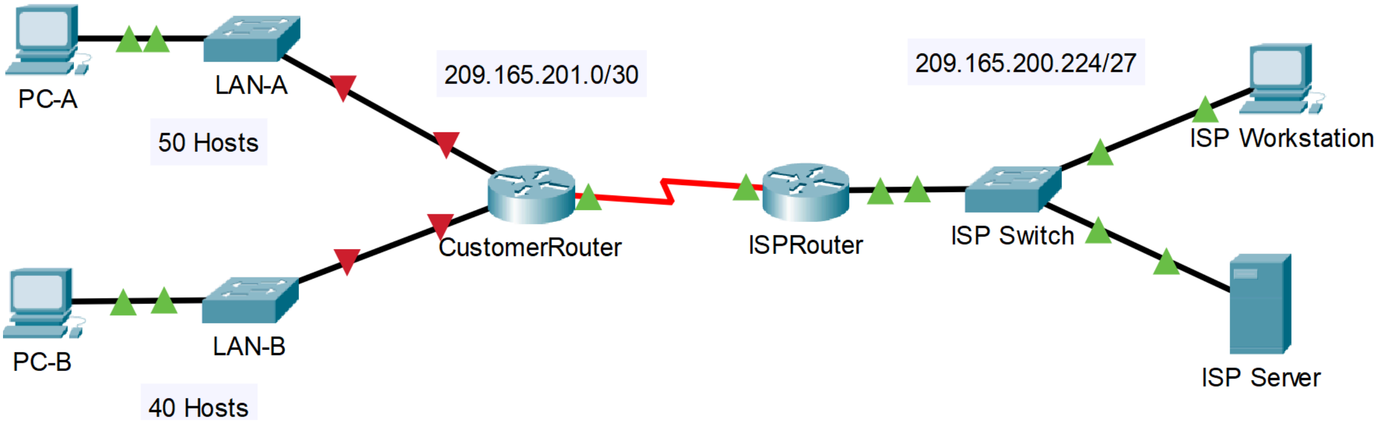
Download Packet Tracer (.pka) file

5B. Objectives

Part 1: Design an IPv4 Network Subnetting Scheme

Part 2: Configure the Devices

Part 3: Test and Troubleshoot the Network



5C. Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
CustomerRouter	G0/0			N/A
	G0/1			N/A
	S0/1/0	209.165.201.2	255.255.255.252	N/A
LAN-A Switch	VLAN1			
LAN-B Switch	VLAN1			
PC-A	NIC			
PC-B	NIC			
ISPRouter	G0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NIC	209.165.200.235	255.255.255.224	209.165.200.225
ISP Server	NIC	209.165.200.240	255.255.255.224	209.165.200.225

5D. Part 1: Subnet the Assigned Network

Step 1: Create a subnetting scheme that meets the required number of subnets and required number of host addresses.

In this scenario, you are a network technician assigned to install a new network for a customer.

You must create multiple subnets out of the 192.168.0.0/24 network address space to meet the following requirements:

a. The **first subnet** is the LAN-A network. You need a minimum of 50 host IP addresses.

b. The **second subnet** is the LAN-B network. You need a minimum of 40 host IP addresses.

c. You also need at least two additional **unused subnets** for future network expansion.

Note: Variable length subnet masks will not be used. All of the device subnet masks should be the same length.

d. Answer the following questions to help create a subnetting scheme that meets the stated network requirements:

Questions:

- How many host addresses are needed in the largest required subnet?
  - 50 Host

- What is the minimum number of subnets required?
  - The requirements stated above specify two company networks plus two additional networks for future expansion.

- The network that you are tasked to subnet is 192.168.0.0/24. What is the /24 subnet mask in binary?
  - 1111111.11111111.11111111.00000000

- Number of subnets? Number of hosts?

  Number of subnets: (2^0 = 1)

  128 hosts (2^8) – 2 = 254 hosts per subnet

e. The subnet mask is made up of two portions, the network portion, and the host portion. This is represented in the binary by the ones and the zeros in the subnet mask.

Questions:

- In the network mask, what do the ones represent?
  - The ones represent the network portion.

- In the network mask, what do the zeros represent?
  - The zeroes represent the host portion.

f. To subnet a network, bits from the host portion of the original network mask are changed into subnet bits. The number of subnet bits defines the number of subnets.

Questions:

Given each of the possible subnet masks depicted in the following binary format, how many subnets and how many hosts are created in each example?

Hint: Remember that the number of host bits (to the power of 2) defines the number of hosts per subnet (minus 2), and the number of subnet bits (to the power of two) defines the number of subnets. The subnet bits (shown in bold) are the bits that have been borrowed beyond the original network mask of /24. The /24 is the prefix notation and corresponds to a dotted decimal mask of 255.255.255.0.

1) (/25) 11111111.11111111.11111111.**1**0000000

- Dotted decimal subnet mask equivalent:
  255.255.255.128

- Number of subnets? Number of hosts?

  Number of subnets: 2 subnets (2^1)

  128 hosts (2^7) – 2 = 126 hosts per subnet

2) (/26) 11111111.11111111.11111111.**11**000000

- Dotted decimal subnet mask equivalent:
  255.255.255.192

- Number of subnets? Number of hosts?

  Number of subnets: 4 subnets (2^2)

  64 hosts (2^6) – 2 = 62 hosts per subnet

3) (/27) 11111111.11111111.11111111.**111**00000

- Dotted decimal subnet mask equivalent:

  255.255.255.224

- Number of subnets? Number of hosts?

  Number of subnets: 8 subnets (2^3)

  32 hosts (2^5) – 2 = 30 hosts per subnet

4) (/28) 11111111.11111111.11111111.**1111**0000

- Dotted decimal subnet mask equivalent:

  255.255.255.240

- Number of subnets? Number of hosts?

  Number of subnets: 16 subnets (2^4)

  16 hosts (2^4) – 2 = 14 hosts per subnet

5) (/29) 11111111.11111111.11111111.**11111**000

- Dotted decimal subnet mask equivalent:

  255.255.255.248

- Number of subnets? Number of hosts?

  Number of subnets: 32 subnets (2^5)

  8 hosts (2^3) – 2 = 6 hosts per subnet

6) (/30) 11111111.11111111.11111111.**111111**00

- Dotted decimal subnet mask equivalent:

  255.255.255.252

- Number of subnets? Number of hosts?

  Number of subnets: 64 subnets (2^6)

  4 hosts (2^2) – 2 = 2 hosts per subnet

- Considering your answers above, which subnet masks meet the required number of minimum host addresses?

  /25, /26 due to number of hosts per subnet is more than 50.

- Considering your answers above, which subnet masks meets the minimum number of subnets required?

  /26, /27, /28, /29, /30 will give the required number of subnets due to LAN-A, LAN-B Network & 2 Additional Unused Subnets = 4 Subnet required for minimum.

- Considering your answers above, which subnet mask meets both the required minimum number of hosts and the minimum number of subnets required?

  /26 will give you the four subnets that are required, and 62 hosts per subnet, which is greater than the 50 hosts required for the first subnet.

Prefix	Subnet Mask	Binary	Number of Subnets	Number of Host Per Subnet
/24	**255.255.255.0**	**11111111.11111111.11111111.00000000**	2^0 **= 1**	2^{88} **- 2 = 254**
/25	**255.255.255.128**	**11111111.11111111.11111111.10000000**	2^1 **= 2**	2^7 **- 2 = 126**
/26	**255.255.255.192**	**11111111.11111111.11111111.11000000**	2^2 **= 4**	2^6 **- 2 = 62**
/27	**255.255.255.224**	**11111111.11111111.11111111.11100000**	2^3 **= 8**	2^5 **- 2 = 30**
/28	**255.255.255.240**	**11111111.11111111.11111111.11110000**	2^4 **= 16**	2^4 **- 2 = 14**
/29	**255.255.255.248**	**11111111.11111111.11111111.11111000**	2^5 **= 32**	2^3 **- 2 = 6**
/30	**255.255.255.252**	**11111111.11111111.11111111.11111100**	2^6 **= 64**	2^2**- 2 = 2**

- When you have determined which subnet mask meets all of the stated network requirements, derive each of the subnets. List the subnets from first to last in the table. Remember that the first subnet is 192.168.0.0 with the chosen subnet mask.

Answer:

We have 64 Address and 62 usable IP Address.

Subnet Address (Network Address)	Prefix	Subnet Mask	Number of Host Per Subnet	First Usable IP Address
192.168.0.0	/26	255.255.255.192	64 (1st Subnet - LAN A)	192.168.0.1
192.168.0.64	/26	255.255.255.192	64 (2nd Subnet - LAN B)	192.168.0.65
192.168.0.128	/26	255.255.255.192	64 (3rd Subnet)	192.168.0.129
192.168.0.192	/26	255.255.255.192	64 (4th Subnet)	192.168.0.193

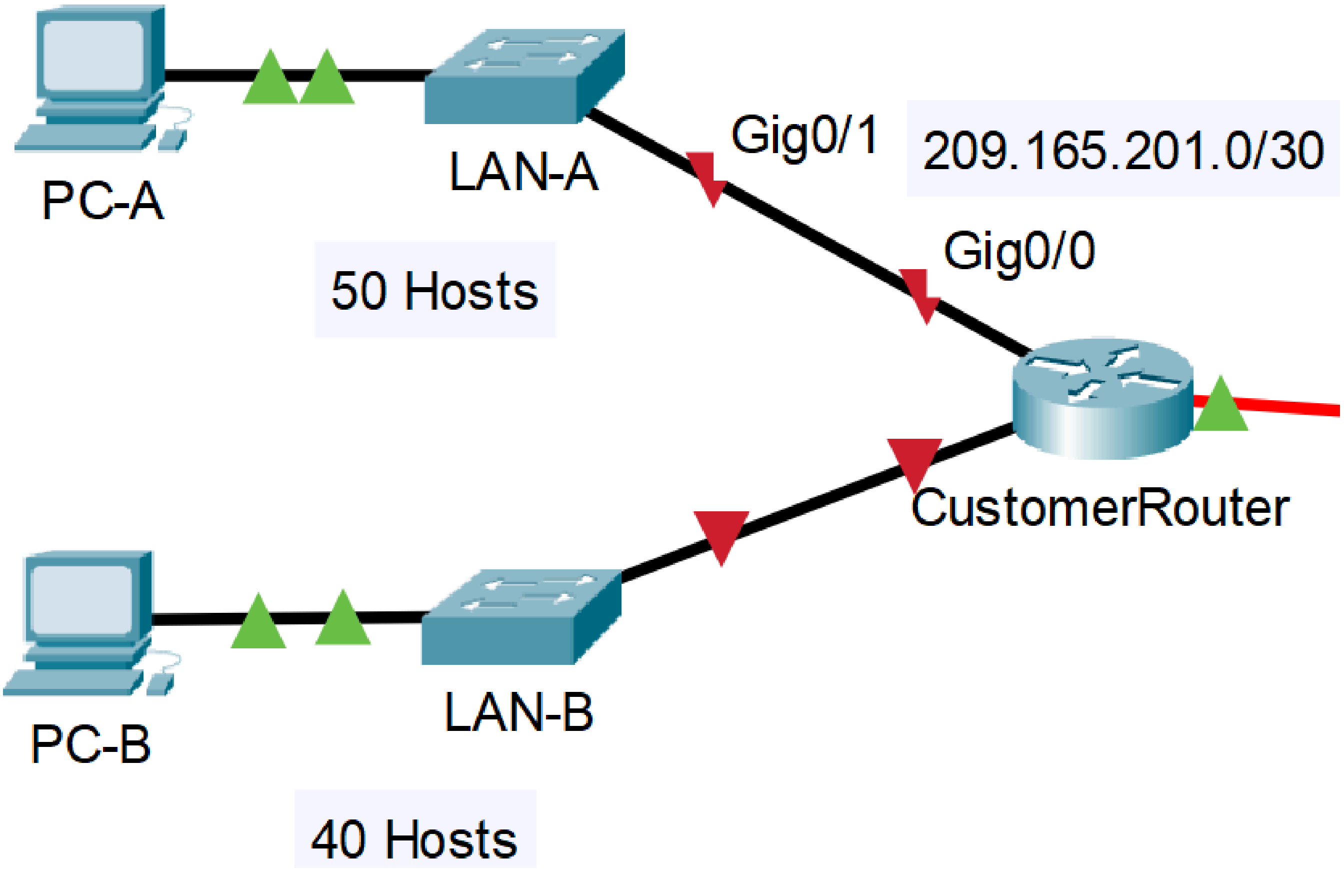
Last Usable IP Address	Broadcast Address
192.168.0.62	192.168.0.63
192.168.0.126	192.168.0.127
192.168.0.190	192.168.0.191
192.168.0.254	192.168.0.255

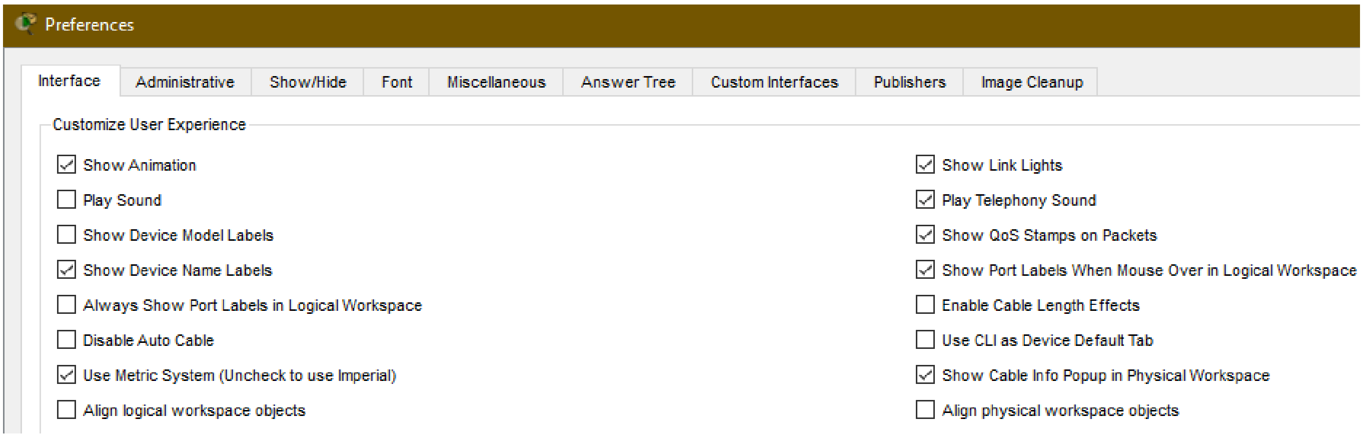
Step 2: Fill in the missing IP addresses in the Addressing Table

Assign IP addresses based on the following criteria: Use the ISP Network settings as an example.

a. Assign the **first subnet** to LAN-A.

- Use the **first host address** for the CustomerRouter interface connected to LAN-A switch.
  - First Host Address = **192.168.0.1**
  - In Cisco Packet Tracer → Click Options → Preferences → Show Port Labels When Mouse Over in Logical Workspace
  - You can see CustomerRouter to LAN-A is Giga 0/0
  - Fill Up G0/0 IP Address as **192.168.0.1** and Subnet Mask **255.255.255.192**




Preferences

Interface | Administrative | Show/Hide | Font | Miscellaneous | Answer Tree | Custom Interfaces | Publishers | Image Cleanup

Customize User Experience

☑ Show Animation
□ Play Sound
□ Show Device Model Labels
☑ Show Device Name Labels
□ Always Show Port Labels in Logical Workspace
□ Disable Auto Cable
☑ Use Metric System (Uncheck to use Imperial)
□ Align logical workspace objects

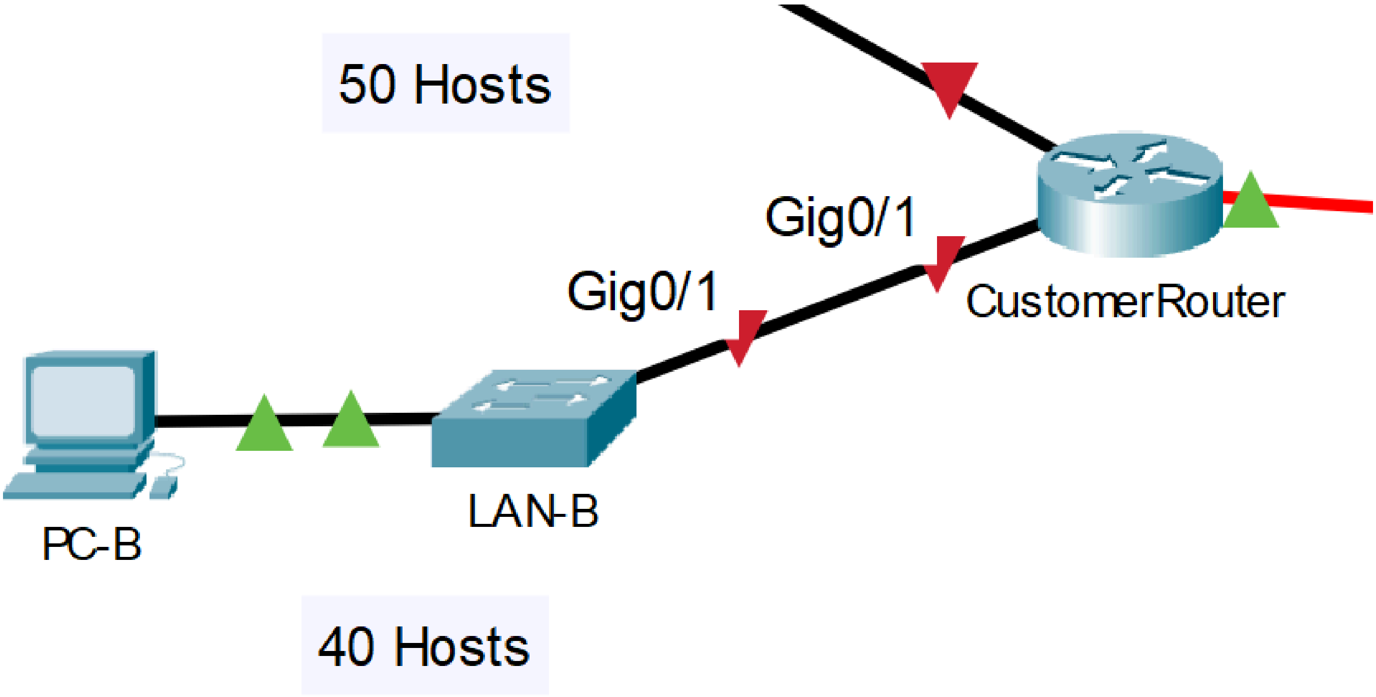
☑ Show Link Lights
☑ Play Telephony Sound
☑ Show QoS Stamps on Packets
☑ Show Port Labels When Mouse Over in Logical Workspace
□ Enable Cable Length Effects
□ Use CLI as Device Default Tab
☑ Show Cable Info Popup in Physical Workspace
□ Align physical workspace objects

- Use the second host address for the LAN-A switch. Make sure to assign a default gateway address for the switch.
    - We use First Usable IP Address for G0/0, We use Second Usable IP Address for LAN-A Switch IP Address: **192.168.0.2**.
    - Same subnet mask due to it is place it on the same subnet.
    - The default gateway is **192.168.0.1** because the IP Address of Gig0/0 is the default gateway for all the subnets (LAN-A).

- Use the last host address for PC-A. Make sure to assign a default gateway address for the PC.
    - Last Host Address: **192.168.0.62**.
    - Same subnet mask due to it is place it on the same subnet.
    - The default gateway is **192.168.0.1** because the IP Address of Gig0/0 is the default gateway for all the subnets (PC-A).

b. Assign the **second subnet to LAN-B**.

- Use the first host address for the CustomerRouter interface connected to LAN-B switch.
  - First Host Address = **192.168.0.65**
  - PC-B & LAN-B Switch are place it on Gig0/1 on the Customer Router.
  - The First Host Address for interface G0/1 Router: **192.168.0.65**.



- Use the second host address for the LAN-B switch. Make sure to assign a default gateway address for the switch.
  - If The First Host Address for interface G0/1 Router: **192.168.0.65**. **65** is the first then 66 will be the second in LAN-B Switch IP Address.
  - The default gateway is **192.168.0.65**. (IP Address G0/1 from CustomerRouter)

- Use the last host address for PC-B. Make sure to assign a default gateway address for the PC.
  - Last Host Address: **192.168.0.126**.

c. Full Answer

Device	Interface	IP Address	Subnet Mask	Default Gateway
CustomerRouter	G0/0	**192.168.0.1**	**255.255.255.192**	N/A
	G0/1	**192.168.0.65**	**255.255.255.192**	N/A
	S0/1/0	209.165.201.2	255.255.255.252	N/A
LAN-A Switch	VLAN1	**192.168.0.2**	**255.255.255.192**	**192.168.0.1**
LAN-B Switch	VLAN1	**192.168.0.66**	**255.255.255.192**	**192.168.0.65**
PC-A	NIC	**192.168.0.62**	**255.255.255.192**	**192.168.0.1**
PC-B	NIC	**192.168.0.126**	**255.255.255.192**	**192.168.0.65**
ISPRouter	G0/0	209.165.200.225	255.255.255.224	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A
ISPSwitch	VLAN1	209.165.200.226	255.255.255.224	209.165.200.225
ISP Workstation	NIC	209.165.200.235	255.255.255.224	209.165.200.225
ISP Server	NIC	209.165.200.240	255.255.255.224	209.165.200.225

5E. Part 2: Configure the Devices

Configure basic settings on the PCs, switches, and router. Refer to the Addressing Table for device names and address information.

Step 1: Configure CustomerRouter.

a. Set the enable secret password on CustomerRouter to **Class123**

b. Set the console login password to **Cisco123.**

c. Configure **CustomerRouter** as the hostname for the router.

d. Configure the G0/0 and G0/1 interfaces with IP addresses and subnet masks, and then enable them.

e. Save the running configuration to the startup configuration file.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CustomerRouter
CustomerRouter(config)#enable secret Class123
CustomerRouter(config)#line console 0
CustomerRouter(config-line)#password Cisco123
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#interface g0/0
CustomerRouter(config-if)#ip address 192.168.0.1 255.255.255.192
CustomerRouter(config-if)#no shutdown

CustomerRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

CustomerRouter(config-if)#interface g0/1
CustomerRouter(config-if)#ip address 192.168.0.65 255.255.255.192
CustomerRouter(config-if)#no shutdown

CustomerRouter(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

CustomerRouter(config-if)#end
CustomerRouter#
%SYS-5-CONFIG_I: Configured from console by console
CustomerRouter#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CustomerRouter#
```

Step 2: Configure the two customer LAN switches.

Configure the IP addresses on interface VLAN 1 on the two customer LAN switches. Make sure to configure the correct default gateway on each switch.

- LAN-A Switch → CLI

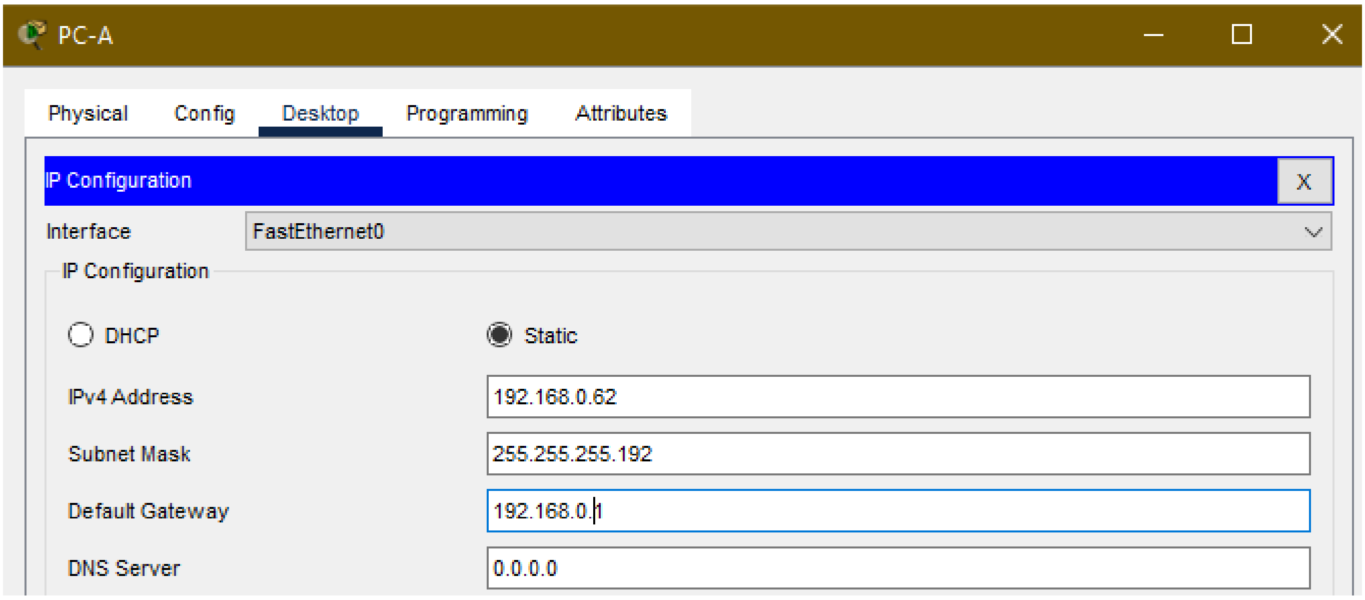
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.0.2 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.0.1
Switch(config)#hostname LAN-A
LAN-A(config)#
```

- LAN-B Switch → CLI

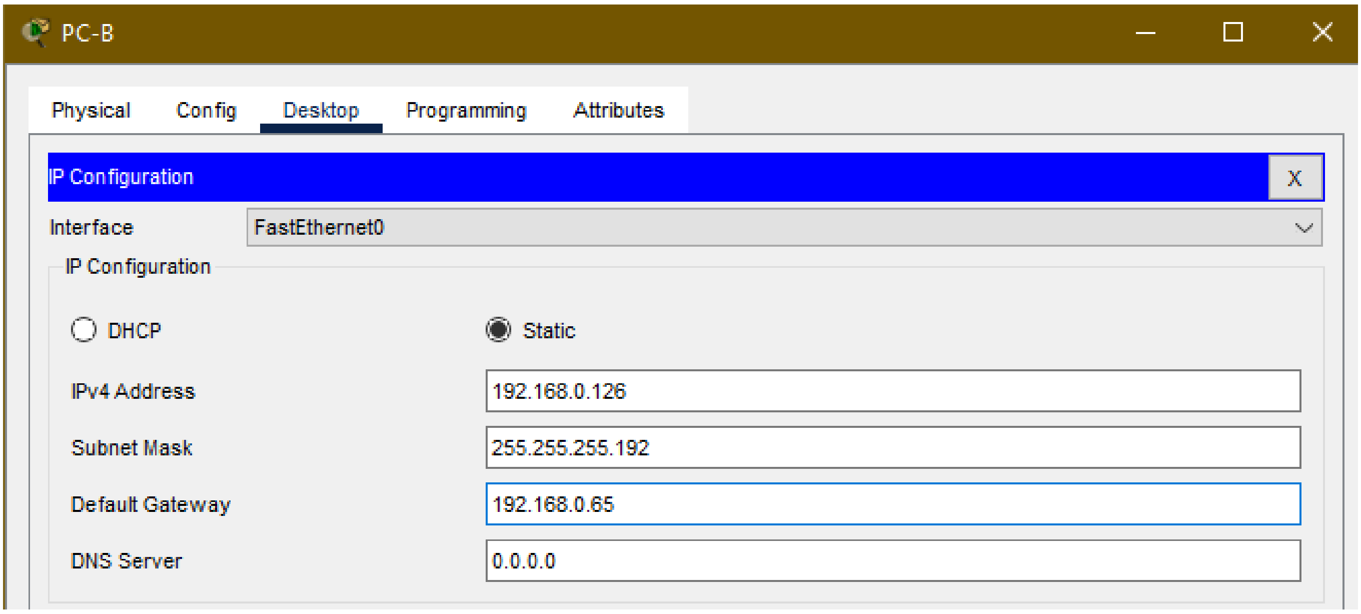
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname LAN-B
LAN-B(config)#int vlan 1
LAN-B(config-if)#ip address 192.168.0.66 255.255.255.192
LAN-B(config-if)#no shutdown
LAN-B(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
LAN-B(config-if)#exit
LAN-B(config)#ip default-gateway 192.168.0.65
LAN-B(config)#
```

Step 3: Configure the PC interfaces.

Configure the IP address, subnet mask, and default gateway settings on **PC-A** and **PC-B.**



Interface	FastEthernet0
○ DHCP	● Static
IPv4 Address	192.168.0.62
Subnet Mask	255.255.255.192
Default Gateway	192.168.0.1
DNS Server	0.0.0.0



Interface	FastEthernet0
○ DHCP	● Static
IPv4 Address	192.168.0.126
Subnet Mask	255.255.255.192
Default Gateway	192.168.0.65
DNS Server	0.0.0.0

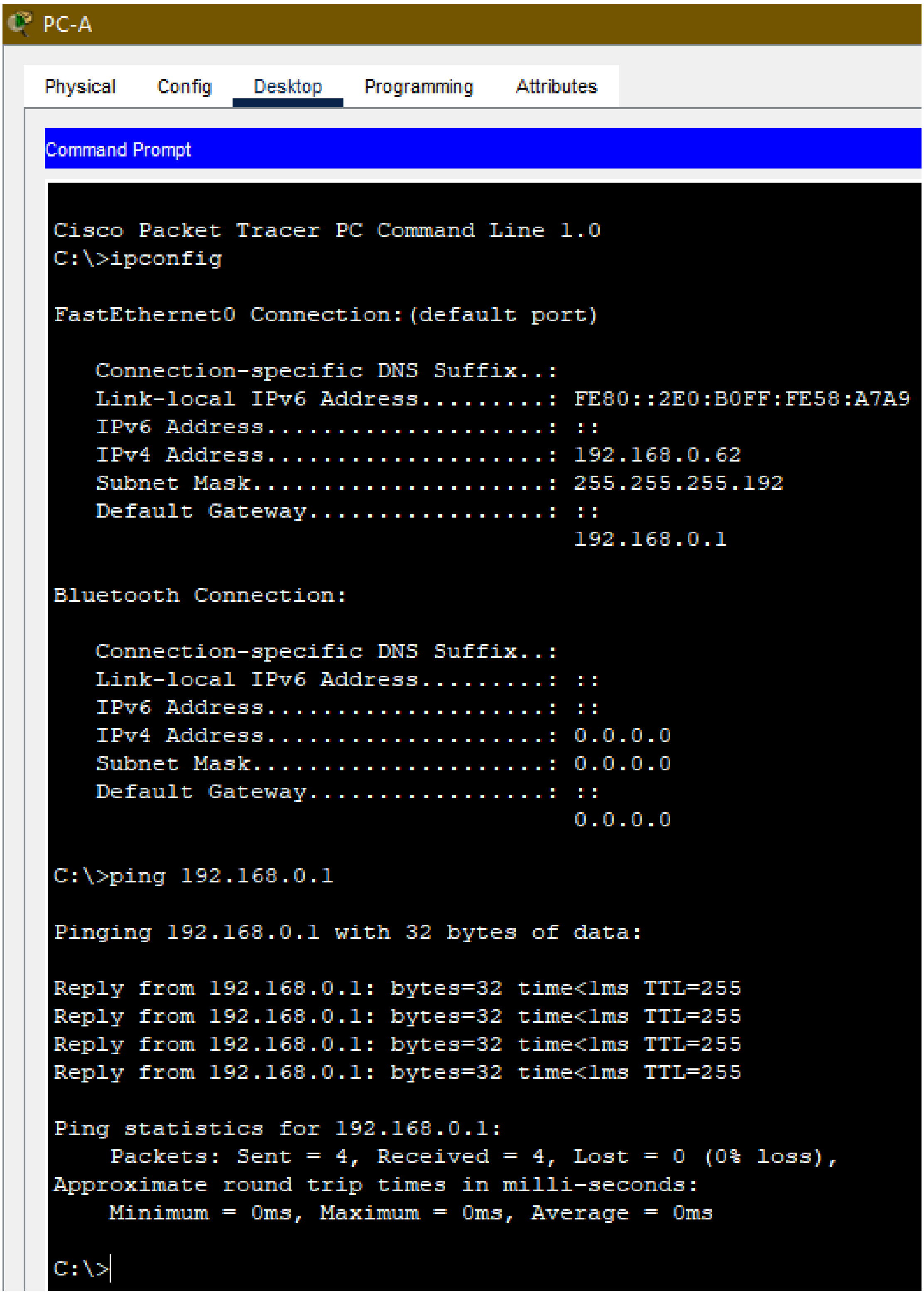
5F. Part 3: Test and Troubleshoot the Network

In Part 3, you will use the ping command to test network connectivity.

a. Determine if PC-A can communicate with its default gateway. Do you get a reply?

- Yes

PC-A → Command Prompt

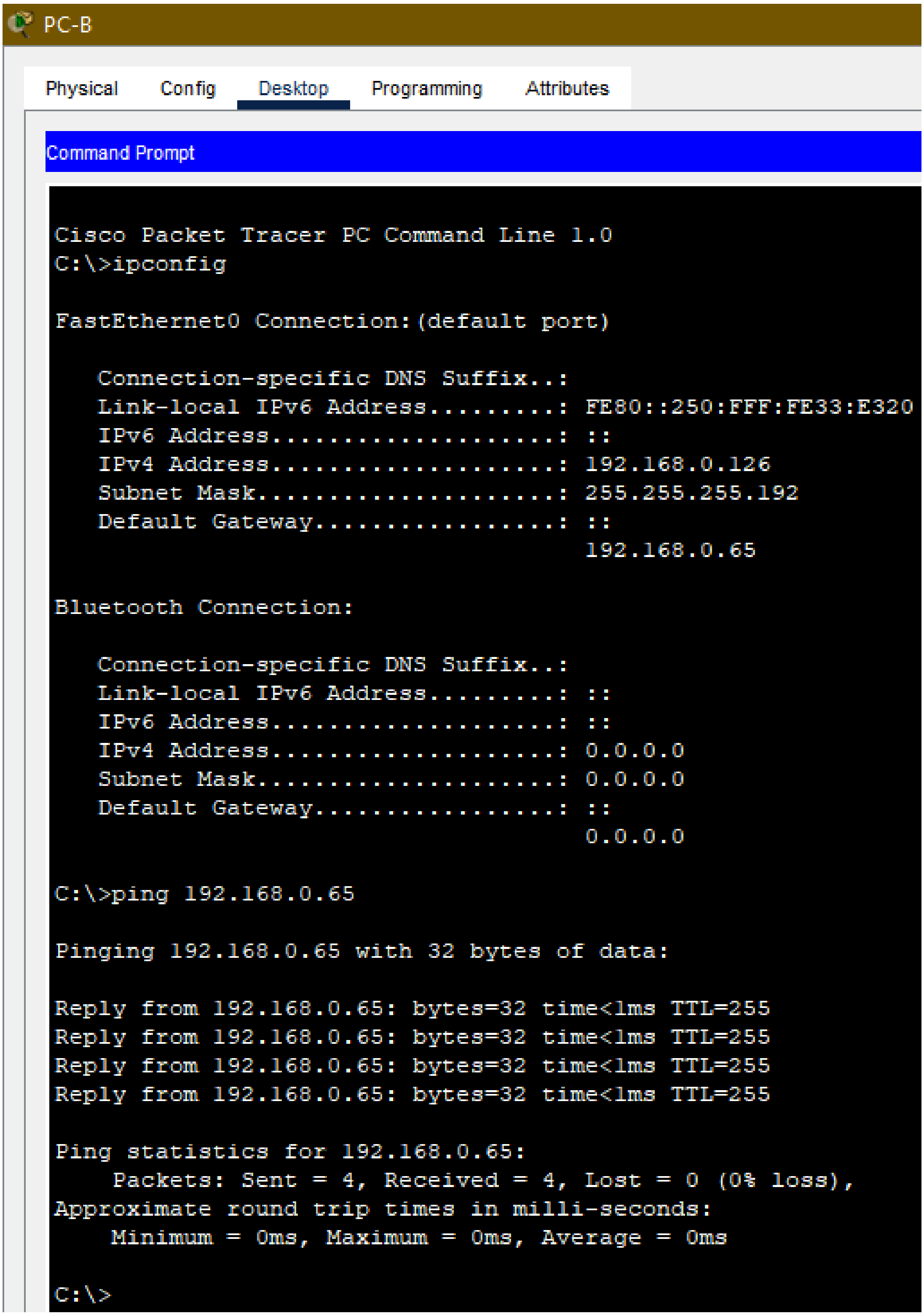


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2E0:B0FF:FE58:A7A9
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.62
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: ::
                                     192.168.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

b. Determine if PC-B can communicate with its default gateway. Do you get a reply?

- Yes

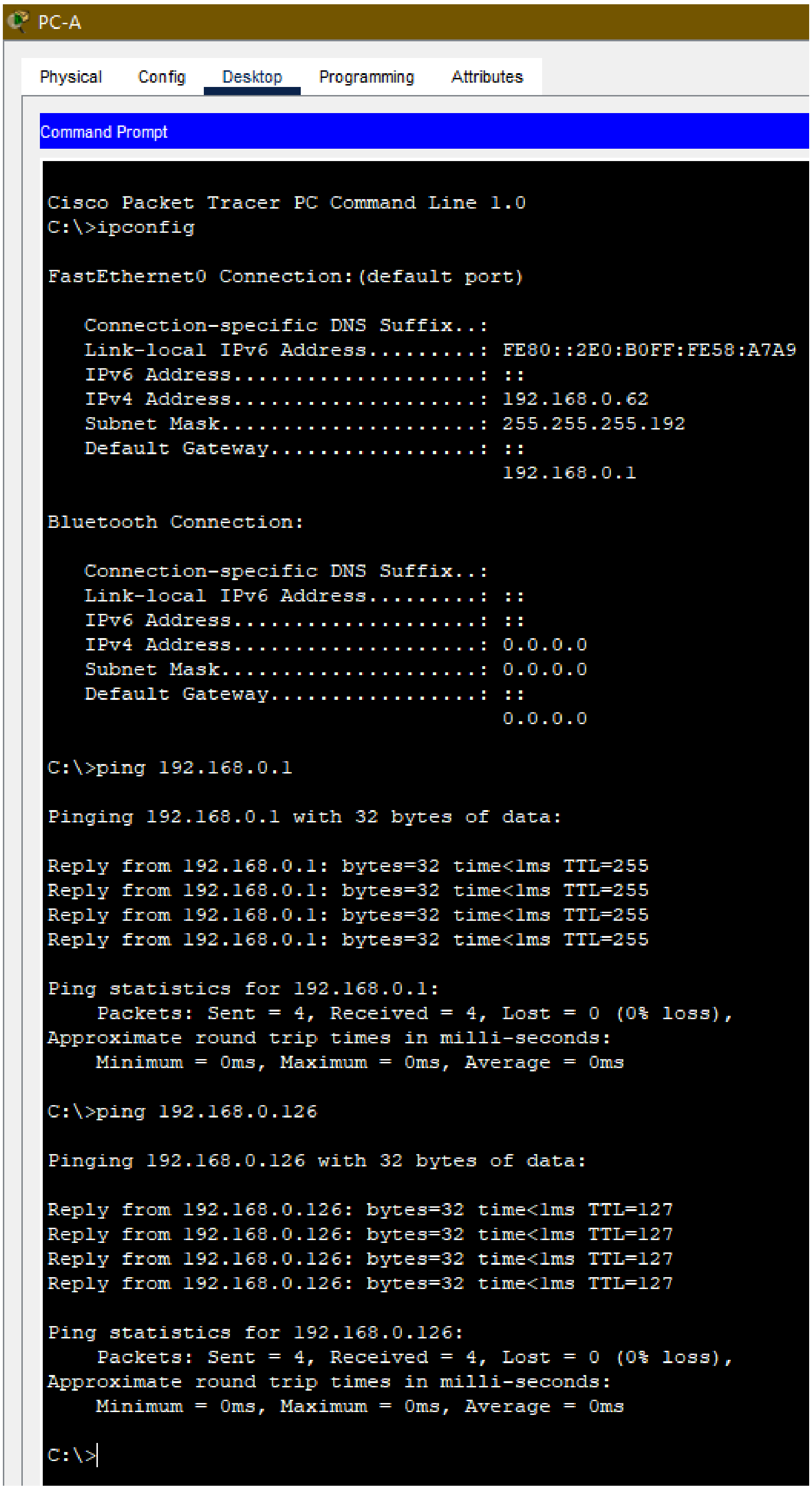
PC-B → Command Prompt



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::250:FFF:FE33:E320
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.126
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: ::
                                     192.168.0.65

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.0.65

Pinging 192.168.0.65 with 32 bytes of data:

Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255
Reply from 192.168.0.65: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

c. Determine if PC-A can communicate with PC-B. Do you get a reply?

- Yes
  - If you answered “no” to any of the preceding questions, then you should go back and check your IP address and subnet mask configurations, and ensure that the default gateways have been correctly configured on PCA and PC-B.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2E0:B0FF:FE58:A7A9
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.62
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: ::
                                     192.168.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.0.126

Pinging 192.168.0.126 with 32 bytes of data:

Reply from 192.168.0.126: bytes=32 time<1ms TTL=127
Reply from 192.168.0.126: bytes=32 time<1ms TTL=127
Reply from 192.168.0.126: bytes=32 time<1ms TTL=127
Reply from 192.168.0.126: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```