**IP CALCULATOR**

**Developed by: Alvarez, Benjamin**

**Date: 14/05/2023**

**Language: English**

**Programming language: Python**

**Introduction:**

The main purpose of this document is to try to explain what an IP calculator consists of, what it is for and the code to use in the python language to be able to develop it.

**How important is understanding IP addresses and netmasks in network management?**

Understanding IP addresses and netmasks is critical in network management. These concepts are the basis of how the Internet works and are used to identify and connect devices on a network.

**What is an IP address?**

IP addresses are unique numbers assigned to each device connected to a network, whether local or on the Internet. They allow devices to communicate with each other and know where to send and receive data. Without an IP address, devices cannot connect or exchange information.

**What are netmasks?**

Netmasks are used in conjunction with IP addresses to define the number of bits representing the network and the number of bits representing devices on that network. These masks determine which part of an IP address refers to the network and which part refers to the device.

**Understanding IP addresses and netmasks is essential for performing network management tasks, such as:**

1. IP Address Assignment: Network administrators should understand how to assign unique IP addresses to devices on the network, either manually or through automatic assignment protocols such as DHCP.

2. Network troubleshooting: When diagnosing and troubleshooting network issues, it is important to understand IP addresses and netmasks to identify address conflicts, misconfigurations, or connectivity issues.

3. Configuring routers and switches: Routers use IP addresses and netmasks to route traffic and establish communication rules. Understanding these concepts is essential to properly configure these devices.

4. Network segmentation: Netmasks allow you to divide a network into smaller subnets, which is useful for managing traffic and improving security. Understanding network masks is crucial to designing an efficient and secure network structure.

**In short, understanding IP addresses and netmasks is essential in network management. These concepts are critical to connectivity, troubleshooting, and configuring network devices.**

**Let's look at some basic fundamentals:**

**Internet Protocol (IP)**

An Internet Protocol (IP) address is a unique identifier assigned to each device connected to a network. It allows devices to communicate and be located on the network in a unique way.

An IP address is represented in decimal notation of four octets (bytes) separated by periods. Each octet is composed of 8 bits and can have a value between 0 and 255. For example, a typical IP address would look like this: "192.168.0.1".

In this notation, each octet represents a portion of the IP address. The IP address is divided into two main parts: the network part and the host part. The number of bits used for the network part and the host part is determined by the netmask.

For example, in the IP address "192.168.0.1", the first three octets (192.168.0) represent the network portion, while the last octet (1) represents the host portion.

Four-octet decimal notation is widely used in IPv4, which is the most commonly used version of the IP protocol today. However, with the increasing demand for IP addresses due to the growth of the Internet, IPv6 has been gradually adopted, which uses an eight-group hexadecimal notation of four characters to represent IP addresses. This allows for a greater number of available IP addresses compared to IPv4.

**What is ipv4?**

IPv4 (Internet Protocol version 4) is the fourth version of the Internet Protocol and is widely used today for network communication. It was the first protocol to be widely implemented on the Internet and is still the most widely used on most networks.

IPv4 uses 32-bit IP addresses, represented in four-octet decimal notation separated by periods, as mentioned above. This means that there are approximately 4.3 billion unique IP addresses available in IPv4. However, due to the exponential growth of the Internet and the increasing demand for IP addresses, the supply of IPv4 addresses has reached its limit and many addresses have already been assigned.

Every device connected to an IPv4 network, whether it's a computer, smartphone, or router, must have a unique IP address in order to communicate with other devices on the Internet. IPv4 addresses are used to uniquely identify each device and establish connections between them.

Although IPv4 has been very successful and widely used, its limited number of available IP addresses has led to the gradual adoption of IPv6. IPv6 uses 128-bit addresses and provides a much larger number of available IP addresses, enabling future growth of the Internet and connectivity for a greater number of devices. However, due to the wide implementation of IPv4 and the need for compatibility with existing devices and systems, IPv4 is still used today.

**Subnet Masks:**

A subnet mask is a numerical value used in conjunction with an IP address to determine which part of the IP address corresponds to the network and which part corresponds to the host within that network. Essentially, the subnet mask is used to divide an IP address into two parts: the network portion and the host portion.

The subnet mask consists of a sequence of bits, usually represented in decimal dotted quad notation (like an IP address). Each bit in the subnet mask can be 0 or 1, where 1 indicates the network portion and 0 indicates the host portion.

When the subnet mask is applied to an IP address, a bitwise logical AND operation is performed between the IP address and the subnet mask. The result of this operation produces the network portion of the IP address.

For example, let's assume we have the IP address "192.168.1.100" and the subnet mask "255.255.255.0". In binary, the IP address would be "11000000.10101000.00000001.01100100" and the subnet mask would be "11111111.11111111.11111111.00000000".

By applying the AND operation between the IP address and the subnet mask, we get:

**11000000.10101000.00000001.01100100 (IP address)**

**11111111.11111111.11111111.00000000 (subnet mask)**

-----------------------------------

11000000.10101000.00000001.00000000

The result, "192.168.1.0", is the network portion of the IP address. The remaining bits in the IP address ("100") represent the host portion.

In summary, the subnet mask is used to divide an IP address into the network portion and the host portion. By applying an AND operation between the IP address and the subnet mask, the network portion is obtained. The remaining bits in the IP address correspond to the host portion. This division allows for identifying the network to which a device belongs and distinguishing it from other devices on that network.

**Let's do some basic calculations:**

An IP calculator provides a series of essential calculations related to IP addresses and subnet masks. Some of the most common calculations you can perform with an IP calculator include:

1. Network Address: Using the IP address and the subnet mask, you can calculate the network address, which represents the first valid address in the network. This is achieved by performing a bitwise AND operation between the IP address and the subnet mask.

Example:

The AND operation between an IP address and a subnet mask involves comparing each corresponding bit in both addresses and applying the logical AND rule to each pair of bits. The result will be a new IP address that represents the network portion of the original address.

**IP Address: 192.168.1.100 (binary: 11000000.10101000.00000001.01100100)**

**Subnet Mask: 255.255.255.0 (binary: 11111111.11111111.11111111.00000000)**

Applying the bitwise AND operation:

**11000000.10101000.00000001.01100100 (IP address)**

**11111111.11111111.11111111.00000000 (subnet mask)**

11000000.10101000.00000001.00000000

The result of the AND operation is: 192.168.1.0. This is the network address corresponding to the original IP address. Each bit in the resulting network address is determined by applying the logical AND rule to the corresponding bits in the IP address and the subnet mask. If both bits are 1, the result will be 1. If one or both bits are 0, the result will be 0.

The AND operation between an IP address and a subnet mask is essential to determine the network address and divide the IP address into the network portion and the host portion.

2. Broadcast Address: The broadcast address is the highest address in a network and is used to send messages to all devices on that network. It can be calculated by performing a bitwise OR operation between the network address and the bitwise negation (one's complement) of the subnet mask.

Example:

**Network Address: 192.168.1.0 (binary: 11000000.10101000.00000001.00000000)**

**Subnet Mask: 255.255.255.0 (binary: 11111111.11111111.11111111.00000000)**

First, we need to find the bitwise negation of the subnet mask, which involves flipping each bit. In this case, the negation of 255.255.255.0 will be 0.0.0.255.

Negation of the subnet mask: 0.0.0.255 (binary: 00000000.00000000.00000000.11111111)

Then, we apply the bitwise OR operation between the network address and the bitwise negation of the subnet mask:

**11000000.10101000.00000001.00000000 (network address)**

**00000000.00000000.00000000.11111111 (negation of the subnet mask)**

11000000.10101000.00000001.11111111

The result of the OR operation is: 192.168.1.255. This is the broadcast address for the network corresponding to the original network address.

In each pair of bits, if at least one of them is 1, the result will be 1. If both bits are 0, the result will be 0. The bitwise OR operation is used to set all corresponding bits to 1 in the broadcast address, indicating that the broadcast address encompasses all devices on the network.

The bitwise OR operation between the network address and the bitwise negation of the subnet mask is used to calculate the broadcast address and allow for message broadcasting to all devices on a specific network.

3. IP Address Range: With the network address and the broadcast address, you can determine the range of available IP addresses in a network. This includes all IP addresses between the network address and the broadcast address, excluding these two addresses.

4. Number of Hosts: The number of hosts is the count of devices that can be connected to a specific network. You can calculate the number of hosts by subtracting 2 (for the network address and the broadcast address) from the total number of available IP addresses in the range.

5. Subnet Mask: If you want to divide a network into smaller subnets, you can calculate the appropriate subnet mask. This is done by determining the number of bits needed to represent the number of subnets and the number of hosts required in each subnet.

Example:

Let's assume you have a network with the IP address 192.168.0.0 and you want to divide it into 4 subnets, each with a sufficient number of hosts.

What do you need to do?

1. Determine the number of bits needed to represent the number of subnets: In this case, we need 2 bits to represent 4 subnets (2^2 = 4).
2. Determine the number of bits needed to represent the number of hosts per subnet: To ensure that each subnet has enough IP addresses for hosts, you need to calculate how many bits are required to represent the maximum number of hosts in each subnet. Let's say we want to have a maximum of 50 hosts per subnet. In this case, we will need 6 bits to represent 64 IP addresses (2^6 = 64), as some of these bits are used for the network address and the broadcast address.
3. Calculate the subnet mask: The subnet mask is calculated by setting the bits corresponding to the network part to 1 and the bits corresponding to the host part to 0. Taking into account the previous results, the appropriate subnet mask would be 255.255.255.192 (in binary: 11111111.11111111.11111111.11000000).

By applying this subnet mask to each subnet, you would obtain the following configurations:

1. Subnet 1:

Network Address: 192.168.0.0

Broadcast Address: 192.168.0.63

Available IP Address Range: 192.168.0.1 - 192.168.0.62

Maximum Number of Hosts: 62

1. Subnet 2:

Network Address: 192.168.0.64

Broadcast Address: 192.168.0.127

Available IP Address Range: 192.168.0.65 - 192.168.0.126

Maximum Number of Hosts: 62

1. Subnet 3:

Network Address: 192.168.0.128

Broadcast Address: 192.168.0.191

Available IP Address Range: 192.168.0.129 - 192.168.0.190

Maximum Number of Hosts: 62

1. Subnet 4:

Network Address: 192.168.0.192

Broadcast Address: 192.168.0.255

Available IP Address Range: 192.168.0.193 - 192.168.0.254

Maximum Number of Hosts: 62

Please note that when dividing a network into smaller subnets, you need to consider that some IP addresses are reserved for the network address and the broadcast address, so the maximum number of hosts in each subnet will be slightly less than the total number of available IP addresses.

**These calculations are essential for network management and configuration as they allow you to understand and work with IP addresses, network masks, subnets, and address distribution within a network. An IP calculator facilitates these calculations, eliminating the need for manual calculations and helping you optimize your network configuration.**

**So why do I want an ip calculator?**

An IP calculator is a useful tool for network administrators and IT professionals who need to perform tasks related to network management and configuration.

***Here are some reasons why it is a great tool:***

1. Network Subnetting: If you need to divide a network into smaller subnets, an IP calculator allows you to determine the appropriate IP addresses and network masks for each subnet.

2. Router and Switch Configuration: When configuring network devices such as routers and switches, you can use an IP calculator to calculate routing configurations, routes, and IP-based Access Control Lists (ACLs).

3. Network Troubleshooting: In situations where there are IP address conflicts or connectivity issues, an IP calculator allows you to verify network configurations and diagnose problems by identifying errors in IP addresses, network masks, or routing configurations.

4. Traffic Analysis: When examining network traffic logs, an IP calculator can help you identify the source and destination of IP addresses and subnets involved in communication.

5. Network Security Configuration: If you are implementing security policies in your network, an IP calculator can assist you in determining the necessary IP addresses and network masks to apply firewall filters, Network Address Translation (NAT) rules, and Virtual Private Network (VPN) configurations.

**In general, an IP calculator gives you tools and functions to perform accurate calculations and configurations related to IP addresses and netmasks. It facilitates the network management process and solves specific tasks that require detailed knowledge of IP addresses.**

**Here are some tips on how to properly use an IP calculator:**

**Validate Inputs:** Make sure to enter IP addresses and network masks correctly into the calculator. Verify that they are in the correct format and that there are no spelling errors. A small error in input can lead to incorrect results.

**Understand Different Types of Network Masks:** Familiarize yourself with different types of network masks, such as Variable Length Subnet Masks (VLSM) and Fixed Length Subnet Masks (FLSM). Understand how network masks are represented in binary and decimal form and how they affect the division of IP addresses into subnets.

**Proper Documentation:** It is important to document all calculations and results obtained with the IP calculator. Note down network addresses, broadcast addresses, IP address ranges, and any other relevant information. This will help you maintain an accurate record and facilitate future configuration or troubleshooting tasks.

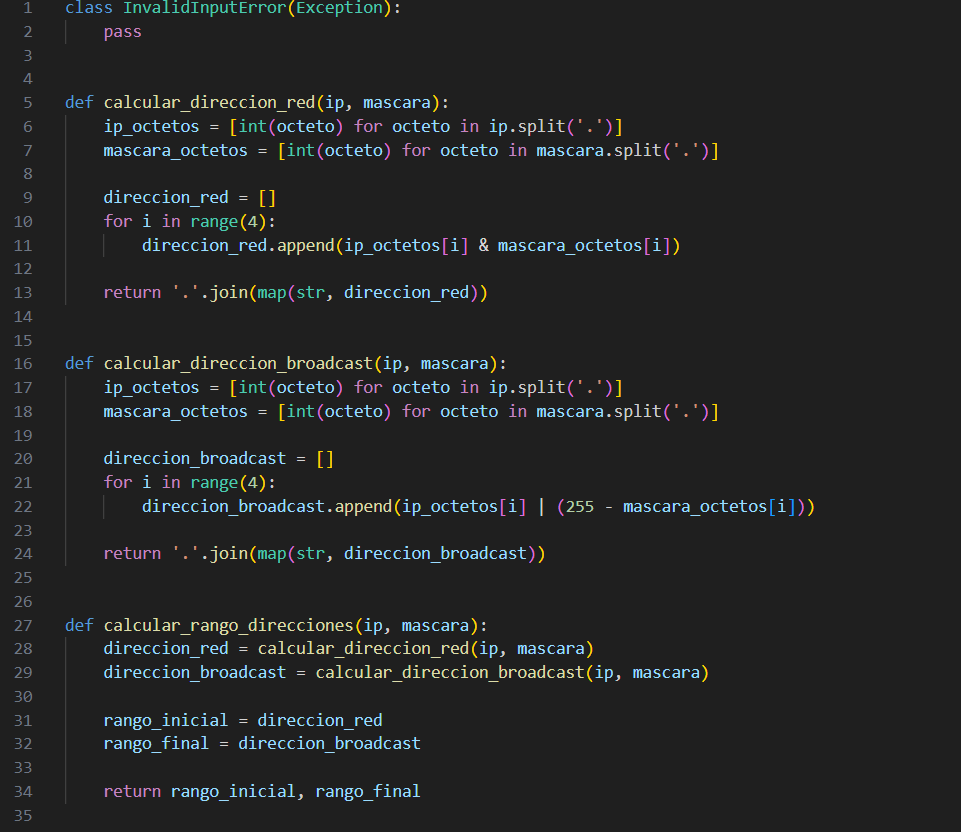
**Verify the Results:** After performing calculations with the IP calculator, verify the obtained results. Ensure that network addresses, broadcast addresses, and IP address ranges are consistent and meet your expectations. If something appears incorrect, review the inputs and calculation steps.

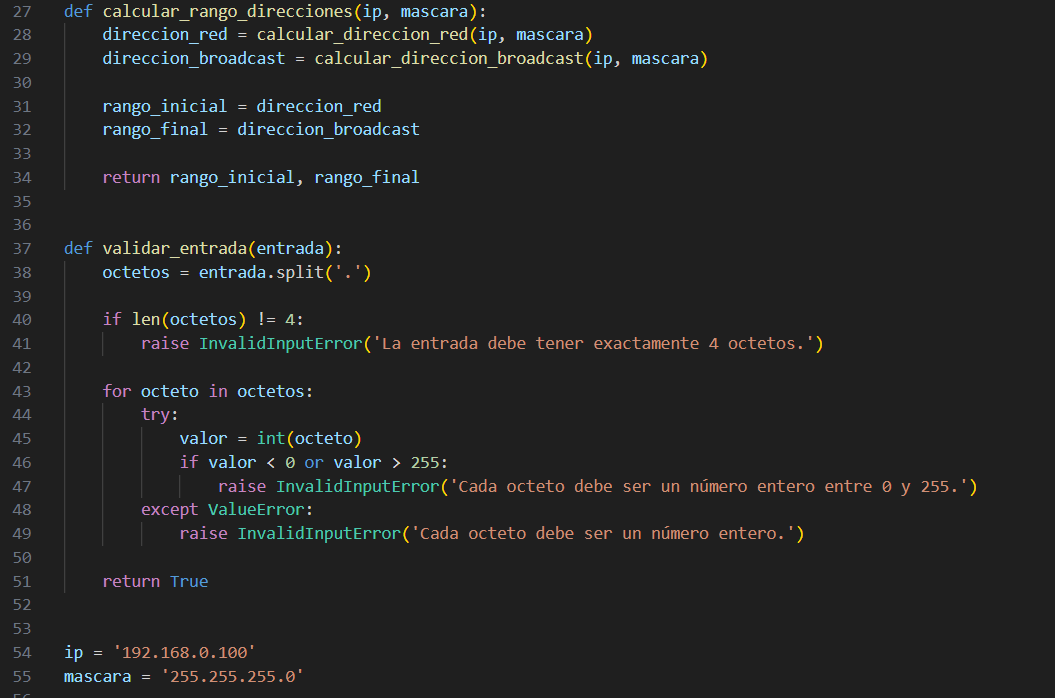
**Update Network Documentation:** Once you have obtained the desired results, be sure to update the network documentation with the relevant information. This includes IP address assignments, network masks, created subnets, and any other related configurations. Keeping updated documentation is essential for efficient network management.

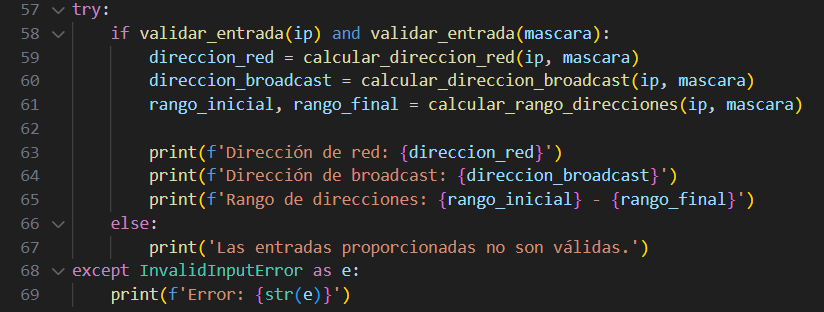
**Learn to Interpret the Results**: Don't just stop at obtaining the results; try to understand what they mean. Learn to interpret network addresses, broadcast addresses, IP address ranges, and the number of available hosts in each subnet. This will help you make informed decisions about the configuration and administration of your network.

**Remember that an IP calculator is a useful tool, but it's important to understand the underlying concepts and have basic knowledge about networks. This will allow you to use it effectively and avoid errors in configuring IP addresses and network masks.**

**THE FINAL CODE WOULD LOOK LIKE THIS:**

****

****

****

**Below is its operation:**

1. A custom exception called Invalid Input Error is defined, which is used to indicate errors in the provided inputs.
2. The function calculates network address(ip, mask) , takes an IP address and a network mask as parameters and calculates the resulting network address. To do this, it divides each octet of the IP address and the mask into a list, performs a bitwise AND operation between them, and then concatenates them back into a string.
3. The function calculates broadcast address(ip, mask) , takes an IP address and a network mask as parameters and calculates the resulting broadcast address. Similar to the previous function, it divides each octet of the IP address and the mask into a list, performs a bitwise OR operation between them, and then concatenates them into a string.
4. The function calculate address range(ip, mask) uses the two previous functions to calculate both the network address and the broadcast address. It then returns the address range as a tuple containing the starting address and the ending address.
5. The function validates input(input) checks whether an input (either an IP address or a network mask) meets certain requirements. Firstly, it verifies if there are exactly 4 octets in the input. Then, it performs validation on each octet, checking if it is an integer within the valid range (0 to 255). If any validation fails, the Invalid Input Error exception is raised with a descriptive error message.

The variables "ip" and "mask" are defined with examples of IP addresses and network masks.

A try-except block is used to handle exceptions that may occur during validation and calculations. Within the try block, the inputs are checked for validity using the validate\_input() function. If they are valid, the calculations for the network address, broadcast address, and address range are performed using the corresponding functions. Finally, the results are printed. If the inputs are not valid, an appropriate error message is displayed.

**If an exception of the Invalid Input Error type occurs, it is caught in the except block and the corresponding error message is printed.**

**In summary, this code provides an IP address calculator that performs thorough validations of entries and handles errors by using custom exceptions. This helps ensure that the entries are correct and provides descriptive error messages in case any problems are detected.**