# 1 Discovering an example network

## 1.1 IP addressing

文本

描述已自动生成

### Question : how many network interfaces can you see, excluding lo ?

From the ip address show output provided, there is one network interface excluding the loopback interface (lo). The output shows the Ethernet interface (eth0) with the IP address of 192.168.138.58/24. Therefore, the answer to your question is one.

### Question : What is the external IP address of the host and the netmask and the format of these netmask ?

ip address show 命令的输出结果中没有包含主机的外部 IP 地址，因此无法从这些信息中确定主机的外部 IP 地址。

但是，以太网接口 (eth0) 的网络掩码在 ip address show 的输出结果中显示为 /24，这表示它的网络掩码为 255.255.255.0。网络掩码的格式为点分十进制表示法，其中每个八位组由八个 1 后面跟足够的 0 组成，如 255.255.255.0 所示。此网络掩码用于确定网络的大小以及该网络中可用的 IP 地址范围。

/24。

### Question : Calculate the mask in its binary and canonical form

以太网接口(eth0)的网络掩码在ip address show命令的输出结果中显示为/24，这表示该网络掩码是255.255.255.0（点分十进制表示法）。为将这个网络掩码转换为二进制形式，我们可以将每个十进制八位组表示为一个8位二进制数，并将所得的24位拼接在一起。

因此，255的二进制表示是11111111，0的二进制表示是00000000。因此，该网络掩码的二进制表示为11111111 11111111 11111111 00000000。

要将网络掩码转换为其规范形式，我们可以计算二进制表示中连续1的数量，并将其表示为前缀长度。在这种情况下，有24个连续的1，因此前缀长度是/24。网络掩码的规范形式也称为CIDR表示法。

因此，该网络掩码的二进制形式是11111111 11111111 11111111 00000000，其规范形式是/24。

### Question : Calculate the network address of this host

根据提供的ip address show输出，该主机在eth0接口上的网络地址是该主机IP地址和网络掩码进行逻辑与运算的结果。

eth0接口的IP地址显示为192.168.138.58，其网络掩码为255.255.255.0（或/24）。我们可以将IP地址和网络掩码转换为二进制形式，并执行位与运算以获得网络地址。

192.168.138.58的二进制表示形式为11000000.10101000.10001010.00111010

255.255.255.0的二进制表示形式为11111111.11111111.11111111.00000000

对这两个二进制数进行按位与运算，我们得到：

11000000.10101000.10001010.00000000

因此，该主机的网络地址是192.168.138.0，其点分十进制表示法。

### Question : What should be and what is the broadcast address in this network ?

根据提供的ip address show输出，该主机的网络地址是192.168.138.0，网络掩码为255.255.255.0（或/24）。要计算网络的广播地址，我们可以对主机IP地址和网络掩码按位取反后进行按位或运算。

以二进制形式表示，主机IP地址为11000000.10101000.10001010.00111010，网络掩码为11111111.11111111.11111111.00000000。网络掩码的按位取反形式为00000000.00000000.00000000.11111111。对主机IP地址和网络掩码按位取反的结果进行按位或运算，我们得到：

11000000.10101000.10001010.00111010 (主机IP地址)

00000000.00000000.00000000.11111111 (网络掩码的按位取反形式)

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

11000000.10101000.10001010.11111111 (广播地址)

因此，该网络的广播地址是192.168.138.255。

广播地址是用于将数据包发送到网络上的所有主机的地址。它始终是网络上可用地址范围内的最后一个地址。

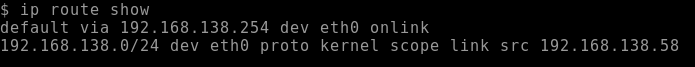
### Question : What are the address that we can use for hosts in this network ?

根据提供的 ip address show 输出，该主机的网络地址是 192.168.138.0，网络掩码是 255.255.255.0（或者 /24），这意味着该网络上可用于主机的 IP 地址范围是从 192.168.138.1 到 192.168.138.254。

网络地址（即 192.168.138.0）和广播地址（即 192.168.138.255）是保留地址，不能分配给该网络上的主机。因此，在该网络中，可用于主机的 IP 地址是从 192.168.138.1 到 192.168.138.254。

值得注意的是，该范围内的某些 IP 地址也可能被保留用于特殊目的，例如私有网络地址、组播地址或回环地址。

## IP routing



### Question : What does the first row represent in the result above and what it is used for ?

ip route show 命令的输出中，第一行表示主机的默认路由，用于确定发送到本地子网外的网络的数据包的下一跳。

在输出中，第一行显示主机的默认路由是通过 IP 地址为 192.168.138.254 的网关，并且出站接口是 eth0。这意味着，如果主机收到一个目标地址不在 eth0 接口所连接的子网内的数据包，它将把数据包转发给默认网关 192.168.138.254，然后由该网关负责将数据包发送到互联网上的目标主机。

第一行中的 onlink 关键字表示网关在同一链路上可直接到达，因此主机无需使用额外的路由表将数据包发送到默认网关。

### Question : What does the second row represent in the result above and what it is used for ?

ip route show 命令输出的第二行表示直接连接到主机的网络，也称为本地子网。该路由条目是由内核自动生成的，并且通常不需要手动配置。

在输出中，第二行显示主机连接到网络 192.168.138.0/24，出站接口为 eth0，并且源地址为 192.168.138.58。这意味着如果主机要与本地子网内的其他主机通信，它将使用该路由条目来直接发送数据包而不需要经过任何网关。

该路由条目也用于实现反向路径过滤和其他网络安全功能。如果从其他子网中收到的数据包源地址不是本地子网地址，该条目将用于检查数据包是否来自正确的来源，并拒绝不合法的数据包。

### Question : What should be and what is the default gateway router address ?

默认网关路由器的地址应该是 192.168.138.254，就如同 ip route show 命令的输出结果所显示的一样：

default via 192.168.138.254 dev eth0 onlink

这意味着任何不是本地子网的流量都会被发送到默认网关路由器 192.168.138.254 进行进一步的处理。

实际的默认网关地址取决于网络管理员的配置，并且可能因具体的网络设置而异。

### Question : Is the host 8.8.8.8 belonging to our network ?

不，主机 8.8.8.8 并不属于本地网络 192.168.138.0/24，因为它有一个不同的 IP 地址范围。8.8.8.8 实际上是谷歌公司拥有的公共 IP 地址，通常用作 DNS 解析器。换句话说，它位于本地网络之外，只能通过连接本地网络与更广泛的互联网的路由器或网关访问。

# Discovering your network

## IP addressing

文本

描述已自动生成

整个2跟1是一模一样的。

# Discovering the rest of the internet

To analyze the networks traversed between our host and a destination host, we will use the tool traceroute. It is based on RFC 791 and RFC 792 relating to IP routing process.

## The rules of the game

### To do : Have a look at the RFC 791

You can find the document at https://datatracker.ietf.org/doc/html/rfc791. Read carefully the section 2.4 about gateways.

### To do : Read the RFC 792

You can find the document at https://datatracker.ietf.org/doc/html/rfc792. Read carefully the section about TIME EXCEEDED MESSAGE and mainly the description of the message.

### Question : what happens when a message go thought a gateway ?

当一条消息通过网关时，它将离开当前子网并进入另一个子网。此时，网关的作用就是将消息从一个子网转发到另一个子网，使得不同子网上的设备可以互相通信。通常情况下，消息首先到达本地网络中的发送设备，然后发送设备通过本地网络的路由器或网关将其发送到外部网络。消息首先进入路由器或网关，然后再由路由器或网关进行下一步处理。具体来说，路由器或网关将检查消息的目标地址，并根据该地址查找路由表，以确定消息的下一步转发位置。然后，路由器或网关将消息转发到下一个目标设备或路由器，直到消息到达目标设备为止。

文本

描述已自动生成

### Question : How traceroute uses RFC 792 rules ?

Il lit le ip header pour savoir ou il va aller.

## Map the Internet

### Todo : Use traceroute ?

Use traceroute to show the path from your host to :

• Your default gateway (identified using ip route show) ;

文本

描述已自动生成

• www.epf.fr using it IP address 136.243.104.86 ;

文本

描述已自动生成

• www.montpellier.fr using its IP address 31.193.50.86 ;

文本

描述已自动生成

• Google DNS server 8.8.8.8

文本

描述已自动生成

### Todo : Draw a network map

Try to draw à network tree map using the information you get above.