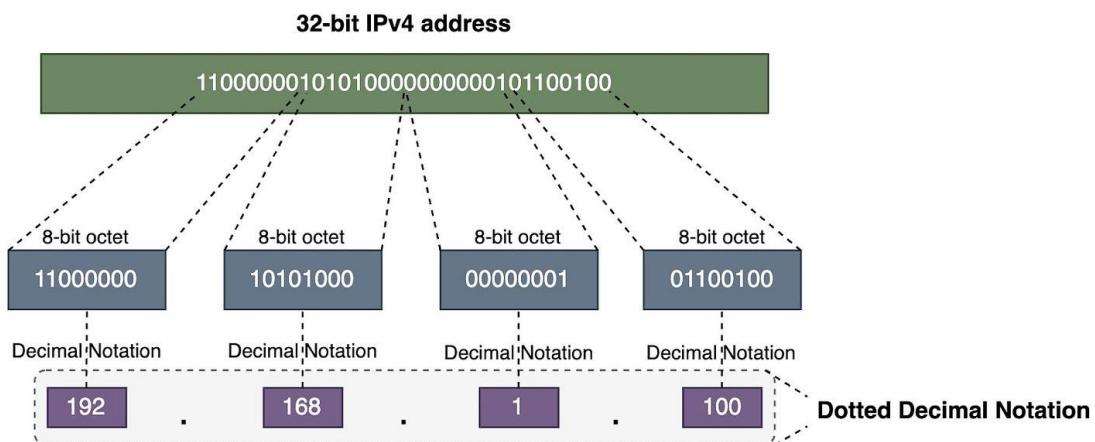


IPv4 地址速成课程

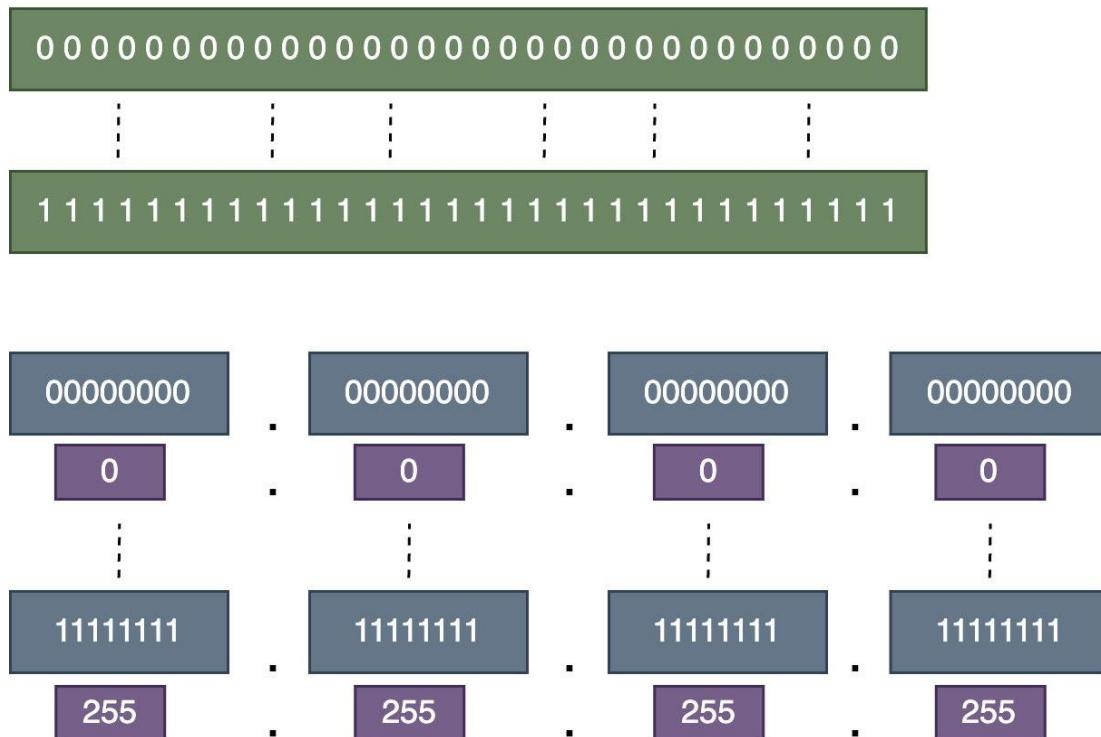
IPv4 地址结构

IPv4 地址用点分十进制表示，但实际上它是一个 32 位地址。这使我们总共有大约 42.9 亿个可能的地址。我们将 32 位地址分为四个 8 位的部分，称为八位组（octet）。然后把每个八位组转换成十进制值。这就是所谓的点分十进制表示法，这也是我们书写 IPv4 地址的方式。



在点分十进制表示法中，IPv4 地址的取值范围从四个 0 (0.0.0.0) 到四个 255 (

Theoretical Range of IPv4 Addresses

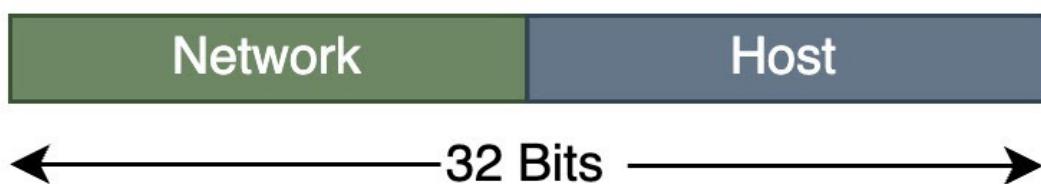


IPv4 地址与子网掩码

IPv4 地址有两个主要部分：

- 网络部分
- 主机部分

IPv4 Address



子网掩码（也称为前缀长度）用于将 IPv4 地址的网络部分与主机部分区分开。

子网掩码为 32 位长。它由一组 1 紧跟一组 0 组成。1 表示 IP 地址的网络部分，0 表

如何书写子网掩码

书写子网掩码有两种方式：

点分十进制表示法

我们可以使用点分十进制表示法，就像表示 IPv4 地址一样。

示例：255.255.0.0

斜线表示法或前缀长度

我们也可以使用斜线记法，该记法表示掩码中为1的比特位数量。

示例：

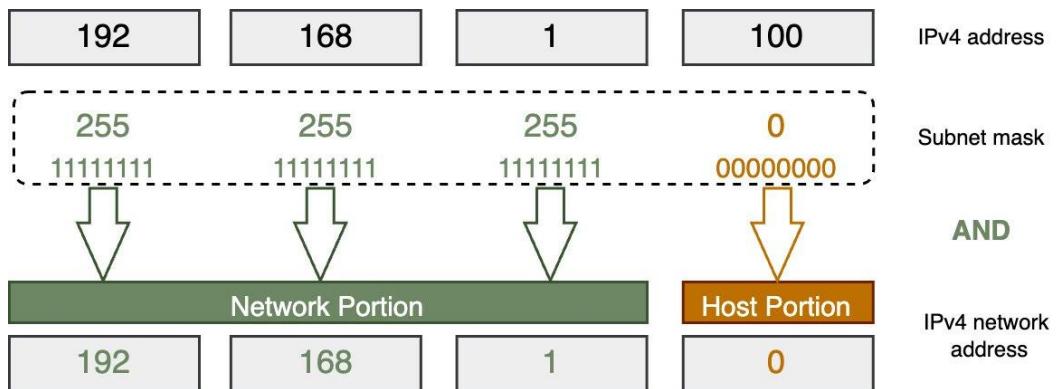
- /16（表示16个一比特）
- 172.18.0.0/16

现在更常用的是斜线记法。

使用子网掩码查找 IPv4 网络地址

假设我们有一个主机 IPv4 地址 (192.168.1.100) 和一个子网掩码 (255.255.255.0)。如何使用子网掩码从主机地址中计算出网络地址？

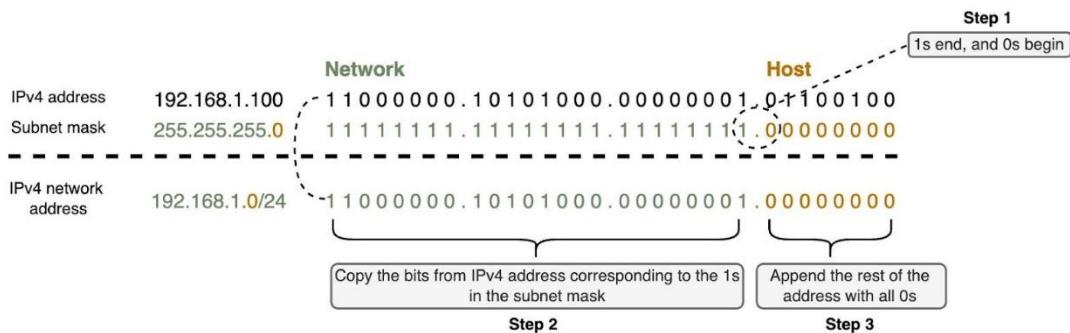
在二进制表示中，我们对主机地址和子网掩码执行按位与 (AND) 运算。对于每一位，如果地址位和掩码位都为1，则结果为1；否则结果为0。该结果就是网络地址。



让它更简单

有一种使用子网掩码来快速找出网络地址的方法，而无需逐位进行按位与运算。假设我们有一个主机 IPv4 地址（192.168.1.100）和子网掩码（255.255.255.0）。有三个

1. 在子网掩码中，找出 1 结束和 0 开始的位置。
2. 从 IPv4 地址中复制与子网掩码中 1 对应的比特。
3. 在末尾补 0 以形成完整的 32 位 IPv4 网络地址。下图显示了这些步骤。



我们需要子网掩码来确定主机属于哪个网络。那就是为什么任何 IPv4 设备都有一个

有效或无效的子网掩码

当子网掩码在八位字节边界结束，如 /8 /16 或 /24 时，查找网络和主机部分很容易。但子网掩码并不总是落在八位字节边界。要理解这一点，我们需要知道什么使子网掩

请记住，子网掩码必须是先一串 1 再一串 0。图像显示了子网掩码在十进制下唯一

| Valid Subnet Mask Values | | | | | | | | |
|--------------------------|----|----|----|---|---|---|---|---------------|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Decimal Value |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 128 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 192 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 224 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 240 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 248 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 252 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 254 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 255 |

下表显示了一些有效和无效的子网掩码：

| Subnet Mask | Valid / Non-valid | Reason |
|-----------------|-------------------|---|
| 255.255.255.0 | Valid | Valid decimal numbers, contiguous 1s and 0s |
| 255.255.0.255 | Non-valid | Valid decimal numbers, but 0s between 1s |
| 255.255.240.254 | Non-valid | Valid decimal numbers, but 0s between 1s |
| 255.255.240.0 | Valid | Valid decimal numbers, contiguous 1s and 0s |
| 255.255.255.223 | Non-valid | Invalid decimal numbers |

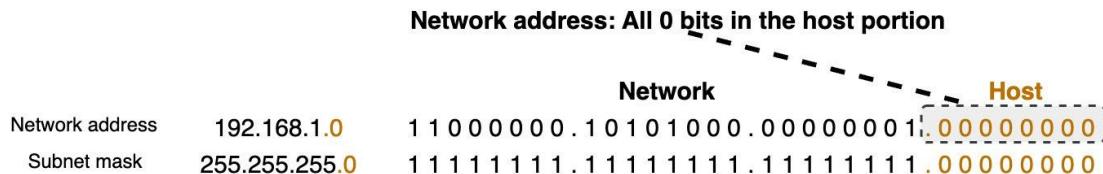
因此，有时我们必须将子网掩码转换为二进制以查看它属于哪个网络，因为它并不以八

总之，我们需要子网掩码（或前缀长度），因为仅凭 IPv4 地址无法告诉设备它所属的网络。子网掩码提供了该信息。

IPv4 网络、广播和主机地址

网络地址

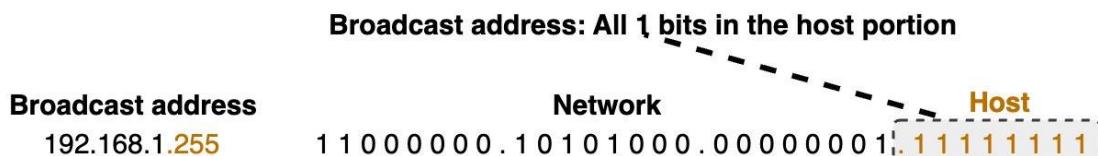
网络地址在 IP 地址的主机部分总是全为 0。**网络上的任何设备都不能使用该网络地址。**这就是设备需要子网掩码以识别地址的网络和主机部分的原因。



广播地址

广播地址是一种用于向网络上所有设备发送消息的特殊 IPv4 地址。**它在主机部分全为 1。**

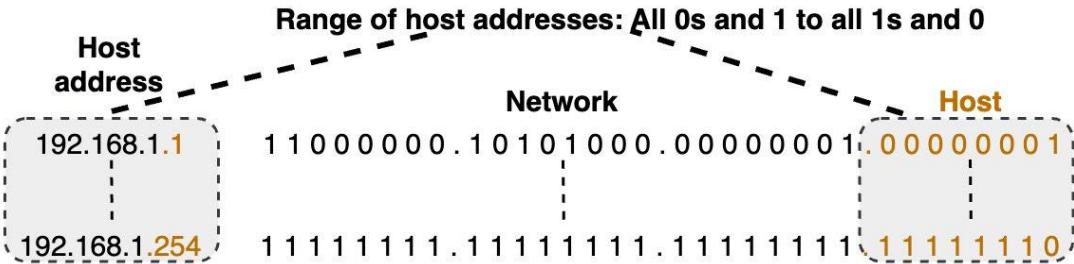
我们来看一个广播地址的示例。



和网络地址一样，任何设备都不允许被分配为广播地址。

主机地址

有效的主机地址是任何不是网络地址或广播地址的 IPv4 地址。**主机部分必须至少包含一个 0 位和一个 1 位—不能全为 0 或全为 1。**主机地址是在网络地址与广播地址之间可供该网络设备使用的地址。



回到我们的 [192.168.1.0/24](#) 示例，网络地址是 192.168.1.0，广播地址是 192.168.1.255。第一个主机地址是 192.168.1.1（主机部分为 00000001），最后一个主机是 192.168.1.254（主机部分为 11111110）。该范围内的地址可分配给主机。

所有主机地址的网络部分都与网络地址相同。每个地址仅主机部分不同。

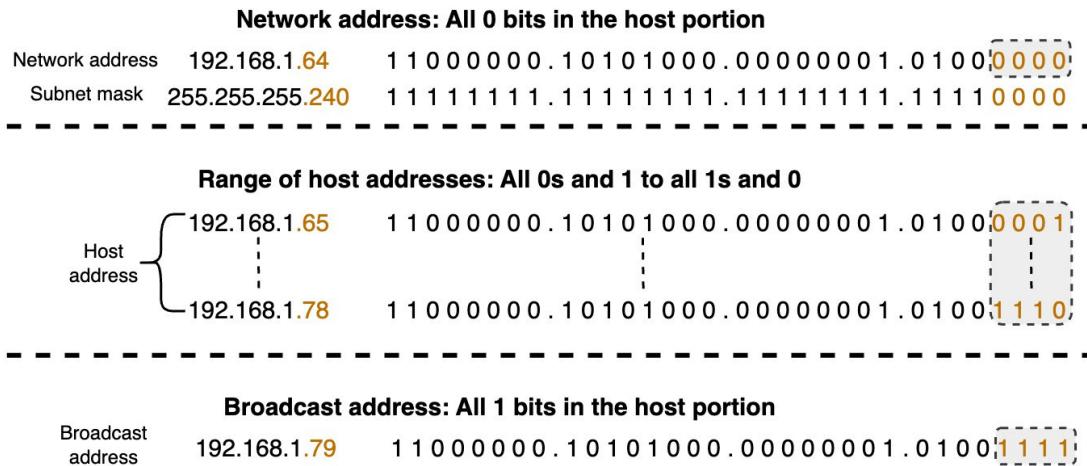


第1个主机地址：通常第一个主机地址（例如 192.168.1.1）会被用作该网络的路由器

常见误解

关于网络地址和广播地址存在一些常见的误解：

- 网络地址并不总是以 .0 结尾
 - 例如，使用 /28 子网掩码时，网络地址以 .64 结尾（[192.168.1.64/28](#)）
- 广播地址并不总是以 .255 结尾
 - 对于[192.168.1.64/28](#)网络，广播地址是 192.168.1.79。网络部分既有0又有1，所以广播地址并不以 .255 结尾



仅仅查看十进制表示很难直观地看清这些地址范围。将所有地址转换为二进制后，更容易分辨出在给定子网掩码下网络地址、广播地址和主机地址范围的位置。

目标 IPv4 地址：单播、多播和广播

让我们来讨论不同类型的目标 IPv4 地址：单播、多播和广播。



注意：这里我们关注的是目标地址，但了解源 IP 地址始终是单播地址也很重要。这意味着数据包的源只能来自一个特定设备。

单播地址

单播地址是分配给单个网络接口的网络地址，表示网络上的唯一端点。当数据发送到单播地址时，目标是由该地址标识的特定设备。单播通信是点对点的，即单个发送方与单个接收方进行通信。

组播地址

组播地址表示网络上一组设备。与表示单个设备的单播地址不同，组播地址用于一对多通信。这意味着发送到组播地址的数据会被属于该特定组的多个设备接收。

希望接收组播流量的设备可以使用专用的组地址加入组播组。当数据发送到组播地址时，数据会被传送到所有已加入相应组播组的设备。这允许同时高效地将信息分发给多个接收者。

组播通信通常用于多媒体流、视频会议和协同通信等应用场景，在这些场景中多个设备需要同时接收相同的数据。它通过仅向注册到组播组的设备传送数据而不是向整个网络广播，从而减少了网络流量。

虽然组播具有优势并在特定领域得到广泛部署，但在更广泛的互联网部署方面仍面临挑战。路由器需要维护的大量组播路由状态信息会导致使用许多组播组的应用无法正常工作。尽管组播通常在受控环境和特定应用中使用，但其在公共互联网的部署仍然有限。

广播地址

广播地址是一种特殊的网络地址类型，用于向特定网络上的所有设备发送数据。在广播通信中，数据面向该指定网络内的每一台设备，实现一对多的通信。



注意：在 IPv6 中，广播已被多播和任播通信取代。

IPv4 子网掩码与数据包转发

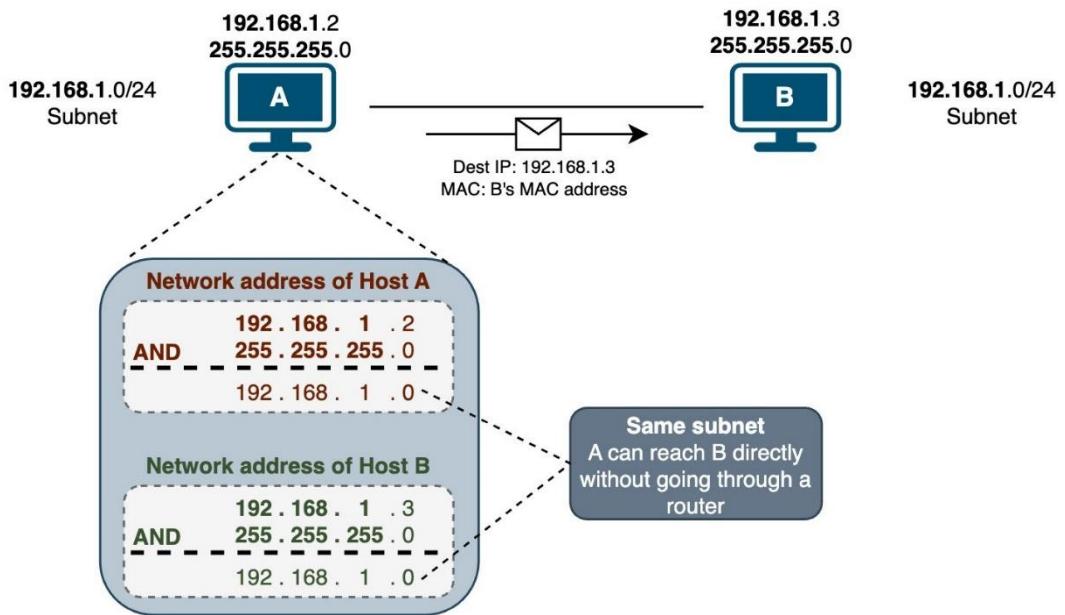
让我们来谈谈 IPv4 地址和子网掩码如何帮助设备在网络上通信。每台设备都有一个 IPv4 地址和子网掩码。这些信息告诉设备它属于哪个网络。网络上的每台设备还有一个默认网关地址。**如果设备需要将数据发送到其自身网络外的其他设备，它就会先将数据发送到默认网关。**

向同一网络上的设备发送数据

IPv4 设备只能与同一子网内的其他设备直接通信。下面通过一个例子来更好地理解这一点。假设主机 A (192.168.1.2) 需要将数据发送到地址为 192.168.1.3 的主机 B。A 如何判断 B 是否在它的网络内？主机 A 按照以下步骤进行：

- 主机 A 知道自己位于 **192.168.1.0/24** 子网（通过对 IP 地址和子网掩码执
- 主机 A 知道主机 B (192.168.1.3) 也在与其相同的子网内（通过对主机

由于主机 A 和主机 B 具有相同的网络地址，它们位于同一网络。主机 A 现在可以直接将数据发送到主机 B 的 MAC 地址。如果主机 A 还不知道主机 B 的 MAC 地址，它会发送一个 ARP 请求以从主机 B 获取 MAC 地址。一旦主机 A 拥有主机 B 的 MAC 地址，就可以

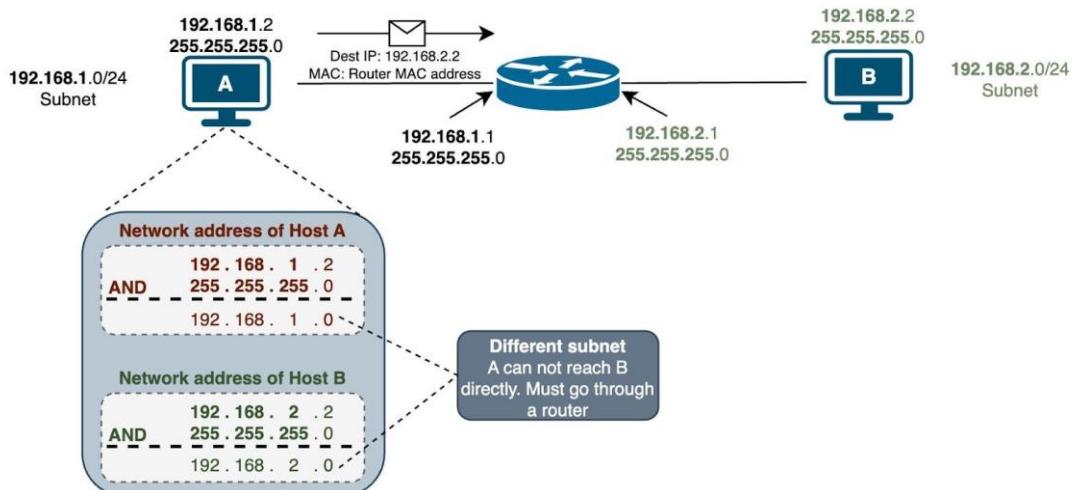


向不同网络上的设备发送数据

现在让我们看另一个示例，主机 A 需要将数据发送到位于不同网络的

- 主机 A 知道它位于 192.168.10.0/24 子网
- 主机 A 知道主机 C (192.168.20.12) 在不同的子网（其网络地址不同于 C

由于主机 C 位于不同的网络，主机 A 无法直接向主机 C 发送数据。主机 A 需要将数据发送到其默认网关，然后路由器会将数据转发到主机 C 所在的网络。



私有和公网 IPv4 地址

我们的 IPv4 地址快要用尽了（只有 42.9 亿个）。我们需要一些快速解决办法和一个

- NAT（网络地址转换）
- 私有地址空间
- CIDR（无类域间路由）

IPv6 是长期的解决方案，并且已经在推进。

私有 IP 地址

私有地址和 NAT 让 IPv4 比预期使用得更久。RFC 1918 定义了私有 IPv4 地址空间。

- 这些地址仅用于私有网络，不用于互联网。
- 它们用于家庭或企业网络内的内部通信。
- 私有 IP 地址范围为：
 - 10.0.0.0 到 10.255.255.255
 - 172.16.0.0 到 172.31.255.255
 - 192.168.0.0 到 192.168.255.255
- 私有网络内的设备可以使用这些地址而不会发生冲突。

公网 IP 地址

公共 IP 地址在互联网上使用，并且在全球范围内是唯一的。IANA（互联网号码分配局）负责分配这些公共 IP 地址。它们用于互联网上设备之间的通信。

IP 地址分配

谁分配 IP 地址（IPv4 和 IPv6）？互联网号码分配局（IANA）负责将 IP 地址空间分配给称为 区域互联网注册管理机构（RIR） 的组织。世界上不同地区存在五个 RIR：

- AfriNIC（非洲网络信息中心）——非洲地区
- APNIC（亚太网络信息中心）——亚太地区
- ARIN（美国互联网号码注册局）——北美地区
- LACNIC（拉丁美洲和加勒比地区 IP 地址注册处）——拉丁美洲及部分
- RIPE NCC（欧洲 IP 网络组织）——欧洲、中东和中亚。大型公司和大学可以直接从其区域互联网注册管理机构（RIR）获得 IP 地址空间。这也称为独立于服务提供商的地址空间，因为他们不是通过互联网服务提供商（ISP）来获取地址空间。大多数其他组织则会通过其 ISP 获取地址空间。

摘要

今天，我们使用无类域间路由（CIDR）。与传统的基于类的系统相比，CIDR 在 IP 地址分配上提供了更灵活的方式。在 CIDR 表示法中，IP 地址后跟斜杠和一个数字，例如 [192.168.1.0/24](#)。斜杠后的数字表示用于地址网络部分的位数。

例如，[192.168.1.0/24](#)。“/24” 表示前 24 位代表网络，剩余的 8 位代表该网络内的主机地址。



注意：CIDR 通过将 IP 地址聚合成块并将这些块作为单条路由进行通告，从

减少了互联网骨干路由器上路由表的规模。随着互联网不断增长且可用地址池愈发紧张，它提高了 IP 地址分配的效率。

参考

<https://bytebytego.com/>