SKYDATA-IoT

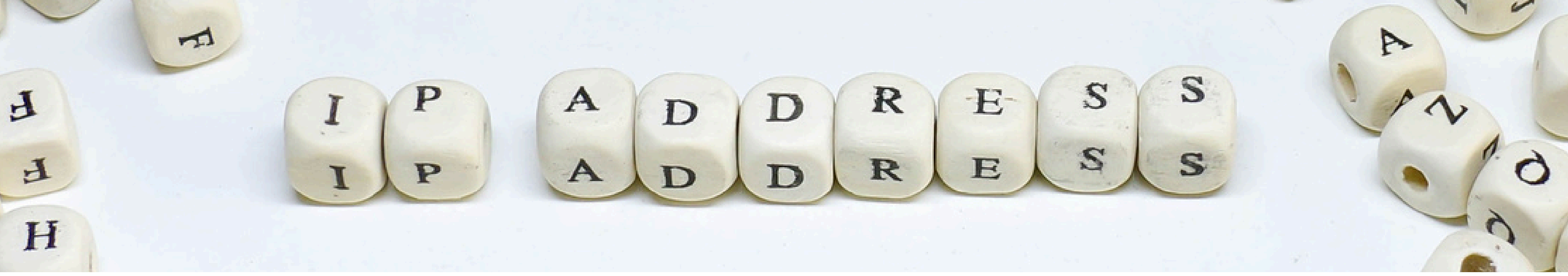
Choosing the Suitable IP Type for Your Application: Comparing Public and Private IPs

IP (Internet Protocol) addresses are crucial for cellular connectivity in IoT applications because they enable devices to communicate with each other and with other systems on the Internet. Because the Internet must differentiate between different devices, IP addresses provide a unique identifier that ensures information is transmitted to the right device. This allows an IoT ecosystem's various applications and hardware and software components to communicate securely and allow for remote control and management.

Understanding the differences and selecting the right type of IP address is not just important, it's crucial. It's the key to ensuring secure and reliable communication between devices and networks within your IoT application. This knowledge empowers you to make informed decisions and ensures the smooth operation of your IoT application.

While our goal, as your partner, is to help you make informed decisions about your IoT application, having comprehensive discussions with your team is vital in establishing your risk appetite and mitigation strategy.

> IT'S ALWAYS FUN TO PICK ON THE NERD.....UNTIL THEY HAVE YOUR IP ADDRESS



To understand which type of IP address is suitable for your use case, you must first understand the difference between each.

Dynamic vs. Static IP Addresses

Dynamic IP: Are are assigned by routers or servers to devices upon connection to the network. This type of address is suitable for IoT devices like smartphones or smart home gadgets that do not need a constant network connection. Dynamic IP addresses are temporary and may change each time the device reconnects to the network, making them perfect for devices with intermittent network usage that do not necessitate a permanent IP address.

Static or Fixed IP: Remains constant, even when the device is not connected to the network. This guarantees that the device will always retain the same IP address, irrespective of its power status. Static IP addresses are perfect for IoT devices that necessitate a continuous network connection, like servers or routers. These devices must be reachable at all times, and a static IP address guarantees accessibility even when they are disconnected and reconnected to the network.

Using a static IP address simplifies device management and configuration, aids network integration, and enhances security by being less vulnerable to hacking compared to dynamic IP addresses.

Public vs. Private IP Address Profiles

Fixed Private IP Address: This type of address will always retain the same IP address, but it will have a private profile that's not hosted in the public domain. This means that the IP address is visible within your own network, but it can't be seen over the internet. This is great for devices that need to communicate with each other across an internal network, but to be able to remotely access connected devices over the web, a secure VPN would need to be in place.

Fixed Public IP Address: This type of IP address stays the same but it's hosted in the public domain so it can be accessed over the Internet. This type of IP address needs to be provisioned by your supplier and, due a national shortage of available public IP addresses, they are chargeable. However, the cost is outweighed by the benefits of gaining full access to your connected devices from other devices or terminals, particularly for applications where remote access is critical, such as CCTV and digital signage.

Making the Right Choice

Factors to Consider When Choosing Between Public and Private IP Addresses

When choosing IP addresses for IoT devices, consider factors like use cases, security, accessibility, costs, and network size. Public IPs may be needed for remote access, while private IPs are suitable for internal communication.

Consideration	Public IP Address	Private IP Address
Use Case	Ideal for devices needing remote access or internet services (e.g., surveillance cameras or remote sensors).	Best suited for devices within a controlled environment (e.g., smart home systems or internal office networks).
Security Concerns	Higher exposure to cyber threats requires stronger security measures.	Naturally safer for data-sensitive operations due to reduced exposure.
Accessability	Enables easier remote access and control, crucial for many IoT applications.	Offers more control over network traffic and user access within the network.
Cost and Resources	More expensive and resource-intensive due to global uniqueness and security needs.	Generally more cost-effective and simpler to manage locally.
Network Scale	Suitable for large-scale networks needing external communication.	Preferable for smaller or more contained networks focused on internal communication.

Selecting the right partnerships is crucial for tailored solutions that meet unique business needs. You'll want to look for a flexible, adaptable provider that offers customized solutions to fit your needs.

SKYDATA-IoT offers global cellular connectivity that supports public and private IP protocols. Contact our experts to learn more.