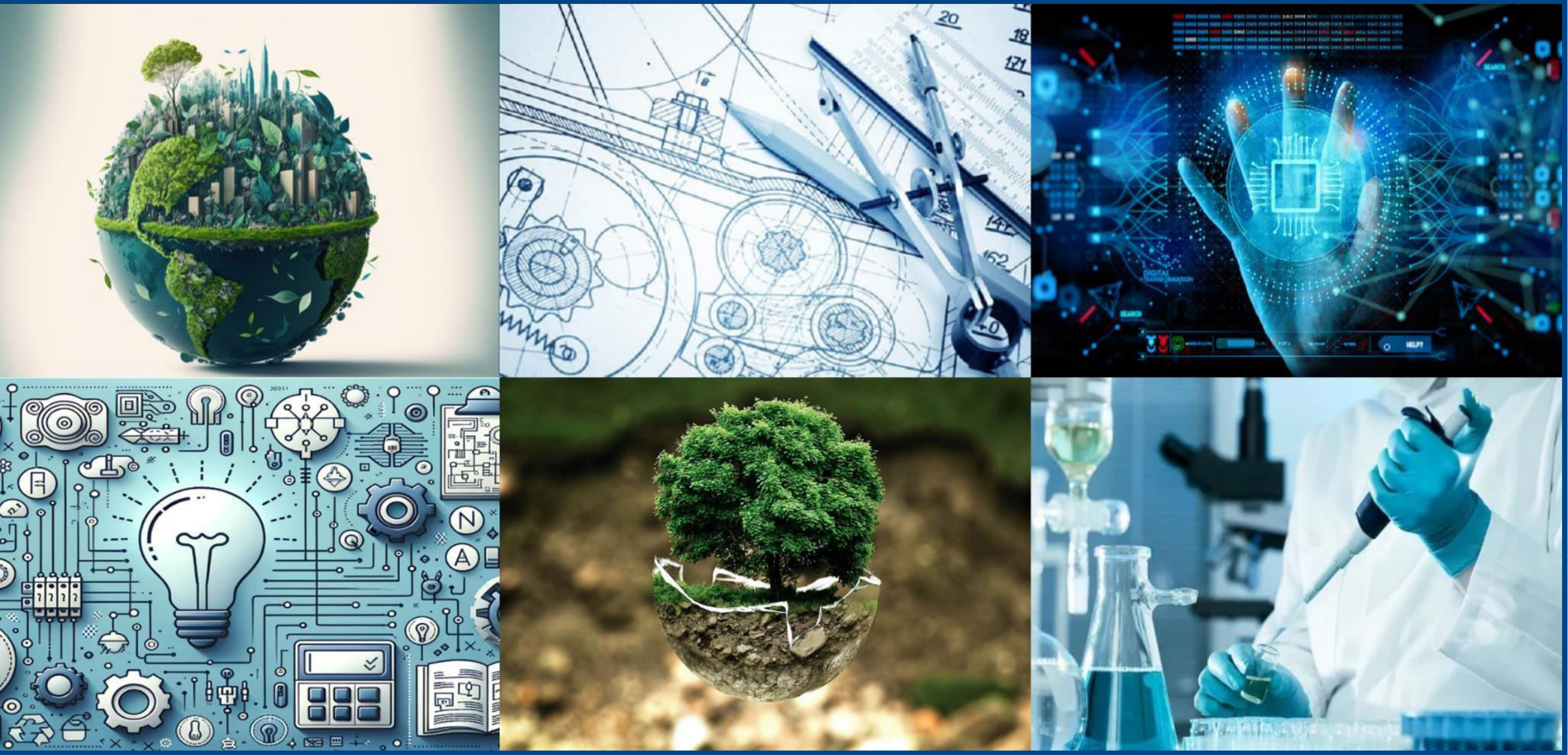
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 7, July 2025

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

How to Connect to Edge Device Without using IP: Techniques and Applications in Modern Networks

Vibha Negi[1], Pramod Negi[1], Srihari Kumar Pendyala[2]

Independent Researcher, USA[1]

T-Mobile, USA[2]

ABSTRACT: IP addresses have always been the primary method for identifying and communicating with devices across networks. However, as computing shifts closer to the edge—where devices such as smart sensors, home appliances, and embedded systems operate in changing and often disconnected environments—this model begins to show its cracks. In many edge settings, devices may not have stable IP addresses, or any IP at all. This makes traditional, IP-based communication and discovery difficult, if not impossible.

This paper explores how devices can connect and communicate without depending on IP. Instead of the conventional approach, we explore alternatives such as Bluetooth, hardware-based identifiers (like MAC addresses), and name-resolution techniques like Multicast DNS (mDNS) and Link-Local Multicast Name Resolution (LLMNR). These methods enable devices to communicate with each other, even in areas with low internet availability and where IP assignment is not possible.

Each of these technologies has its own series of trade-offs. Some are optimized for short-range connections, while others are optimized for local networks. Some are platform-independent; others are more specialized. By comparing these methods side by side, we aim to offer a practical guide for engineers and researchers building edge systems. The goal is to design communication frameworks that are flexible, resilient, and better suited for the increasingly decentralized world of edge computing.

KEYWORDS: Edge computing, device discovery, non-IP communication, mDNS, Bluetooth, MAC address, LLMNR, peer-to-peer connectivity

I. INTRODUCTION

Today, with the growing use of edge devices such as smart sensors, home appliances, wearables, and industrial controllers, there are many situations where IP-based communication just doesn’t fit. In some cases, assigning an IP address may be too complex. In others, the network may lack the necessary hardware, such as a router, a DHCP server, or an internet connection, to support conventional IP networking. Instead, those devices will often have to connect directly to each other, especially in local, short-distance, or temporary arrangements.

Consider the following examples:

1. Setting up a new smart device from your phone before it connects to Wi-Fi
2. Wearables syncing data in a moving vehicle or a remote area
3. IoT devices in a smart factory are talking locally to keep operations running, even if the internet is down
4. Environmental sensors deployed in areas with no connectivity at all

In these cases, requiring an IP address can add unnecessary complexity or simply won’t work. That’s where alternative, non-IP communication methods come in.

This paper examines how devices can connect in these types of environments without relying on traditional IP addresses. We focus on practical solutions that enable devices to discover and communicate directly with each other, and evaluate each option to determine its suitability depending on the use case and constraints.

II. WHY IP IS PROBLEMATIC FOR EDGE ENVIRONMENTS

IP addressing is particularly useful when working with traditional networks, such as office Wi-Fi, home internet, or large cloud systems. However, when we move to the edge, where devices are smaller, mobile, deployed in unusual locations, or operate without constant internet connectivity, IP-based communication begins to fall short.

- Dynamic Environments: In edge settings, devices often move around or connect to different networks. This causes their IP addresses to change frequently, especially when DHCP (Dynamic Host Configuration Protocol) or NAT (Network Address Translation) is involved. If a device's address keeps changing, it becomes difficult for others to reliably connect to it.
- No Infrastructure: Many edge deployments lack the standard network building blocks we take for granted, such as DNS servers to resolve names to IP addresses, routers to handle traffic, or gateways to connect to the internet. For instance, a group of sensors in a forest or a wearable network at a sporting event might have no infrastructure at all. Without those core services, IP-based networking struggles to even get started.
- Security Concerns: IP addresses can introduce their own security challenges. Devices with static IP addresses can become easy targets for attackers; once the address is known, it can be spoofed or attacked. On the other hand, when IP addresses are assigned dynamically, it becomes harder to establish trusted identities or maintain consistent authentication between devices.
- Resource Constraints: Many edge devices are built to be small, inexpensive, and energy-efficient. Consider a temperature sensor that operates on a coin battery or utilizes a microcontroller in a wearable device. Such devices often lack the processing power or memory to run a full TCP/IP stack, which is necessary for traditional IP networking. So using IP adds unnecessary overhead.
- Initial Discovery: Devices must first discover each other before they can utilize IP, but IP itself doesn't facilitate discovery unless the addresses are already known or assigned.

In short, while IP is still a vital part of modern networking, it isn't always the right tool for the job at the edge. That's why alternative, more flexible methods are gaining traction that let devices connect in a lightweight, direct, and resilient way.

III. NON-IP-BASED COMMUNICATION TECHNIQUES

We examine four primary techniques that enable connectivity or discovery without requiring an IP address.

3.1 Bluetooth

Overview: Bluetooth is a short-range wireless technology that you've likely used to connect devices such as headphones, fitness trackers, or smartwatches. It allows devices to "see" each other nearby and exchange information securely; no internet or IP address required.

Devices use Bluetooth to scan for nearby peers, exchange device names or services (such as battery level or temperature), and establish encrypted connections using predefined profiles, like GATT (used in BLE).

PROSCONS

- ➢ Works great without internet or a traditional network
- ➢ Offers built-in encryption and secure pairing
- ➢ Supported on nearly all smartphones, laptops, and wearables
- ➢ Ideal for offline-first or one-time setup scenarios
- ➢ Works best when devices are physically close (usually within 10 to 100 meters)
- ➢ Requires manual pairing in most cases
- ➢ Can be slow during initial discovery or reconnection

Best suited for: Smartphones, wearables, medical devices, smart appliances, or any setup where users interact closely with a device.

3.2 MAC Address-Based Discovery

Overview: Every network-enabled device has a unique MAC (Media Access Control) address. On a local network, devices can be detected by monitoring their MAC addresses, much like recognizing someone by their fingerprints rather than their name.

Some devices send out broadcasts or respond to queries (like ARP requests), which can be picked up by others on the same network. This enables them to detect nearby devices without relying on IP addresses.

PROSCONS

- Operates below the IP layer (Layer 2), so no IP addresses are needed
- Quick detection in wired or Wi-Fi LANs
- Handy for simple inventory tasks or device monitoring
- Not secure; MAC addresses can be faked (spoofed)
- Doesn’t support advanced features like service discovery or encryption
- Limited to very local communication; won’t work across subnets or wide networks

Best suited for: Local diagnostics, hardware inventory, or basic discovery in stable, secure LANs.

3.3 Multicast DNS (mDNS)

Overview: Multicast DNS enables devices to communicate with each other using hostnames (such as hostname.local) instead of IP addresses, eliminating the need for a dedicated DNS server. It’s the backbone of zero-configuration networking, used in tools like Apple Bonjour and Linux’s Avahi.

When a device wants to find another, it sends out a multicast query on the local network asking, “Who is hostname.local?” The device that owns that name replies with its details.

PROSCONS

- Doesn’t need any manual setup—devices just find each other automatically
- Lets devices advertise services (e.g., a webcam saying “I’m available!”)
- Supported across Linux, macOS, and many smart home systems
- Multicast traffic might be blocked or filtered by some networks (especially corporate ones)
- Not natively supported on older versions of Windows
- No built-in encryption—suitable only for trusted local networks

Best suited for: Smart homes, IoT hubs, shared devices (such as speakers or printers), or any device designed for plug-and-play operation.

3.4 Link-Local Multicast Name Resolution (LLMNR)

Overview: LLMNR is Microsoft’s take on zero-configuration discovery, meant for Windows devices. It lets Windows machines resolve each other’s names when no DNS server is available.
Like mDNS, it uses multicast to ask “Who is DeviceName?” and gets responses directly from other devices on the local link.
PROS
CONS

- Built into all recent versions of Windows
- Works out of the box—no need for additional software
- Helps in Windows labs or enterprise setups where central DNS may not be configured
- Only works reliably in all-Windows environments
- Vulnerable to spoofing and other security risks

Best suited for: Small Windows-only environments or isolated enterprise test networks.

IV. COMPARATIVE OVERVIEW

Method	Platform Support	Security	Range/Scope	Discovery Type	Use Case Fit
Bluetooth	Cross-platform	Secure pairing	~10–100 meters	Proximity based	Wearables, mobile
MAC Discovery	Universal (Layer 2)	Weak	LAN only	Passive/ARP-based	Diagnostics, static
mDNS	Linux/macOS/IoT	Unencrypted	LAN Multicast	Name and service	Smart home, printers
LLMNR	Windows only	Weak	LAN Multicast	Name only	Windows discovery

V. CHALLENGES AND CONSIDERATIONS

While non-IP-based communication techniques can address many problems at the edge, they also come with their own set of challenges. These approaches are often designed for simplicity, but this also means they can encounter issues when applied in real-world networks—especially at scale or in more complex environments.
Below are some of the things to consider:

➢Security: Most non-IP discovery methods were designed for local and trusted environments, not hostile ones. As a result, they often lack strong security features. For example:
○No encryption means that any data exchanged can be read by anyone listening on the network.
○No authentication makes it easy for a malicious device to impersonate something it's not (such as a printer, sensor, or trusted node).
This is especially concerning in environments where sensitive data is exchanged or where critical systems depend on device communication.

➢Interoperability: Not all non-IP techniques play nicely with each other. For instance:
○mDNS is commonly used on Apple and Linux devices.
○LLMNR is mostly limited to Windows environments.
○MAC-based methods focus on low-level hardware detection and don't support service discovery.
This means that in mixed environments, like a smart home with Android, Apple, and Windows devices, you might run into compatibility issues where some devices can't "see" or communicate with others.

➢Network Policy: Many non-IP techniques rely on multicast, where a device sends a message to all others on the local network. This can be a problem because:
○Some routers and firewalls block multicast traffic by default to reduce noise or potential abuse.
○In enterprise or managed networks, multicast may be restricted for security or performance reasons.
This can result in devices not being able to find each other, even if they're technically on the same network.

➢Scalability: These methods generally work best in small, local networks, such as a home or a small office, where only a handful of devices need to connect. But as the number of devices grows, things can quickly get messy:
○More devices mean more broadcast or multicast traffic, which can slow down the discovery process.
○There's no built-in way to organize or group devices beyond very basic naming.
○Managing updates, identity, and trust at scale becomes difficult without centralized tools.

➢Dynamic Topologies: Edge devices often move, go offline, or change roles. In these dynamic setups, devices must frequently rediscover each other. But many non-IP protocols:
○Don't handle mobility well (e.g., if a device changes networks or reboots, it may disappear from others' view).
○Require full rediscovery every time something changes, which can add delays or create inconsistent behavior.
Without reliable mechanisms for tracking devices as they move or reconnect, networks can become unstable or unpredictable.

VI. RECOMMENDATIONS

When working in edge environments, there's no single "best" method for device communication without IP; each option has its strengths depending on the situation. Here's how to decide what to use, based on your environment and goals:
➢Use mDNS for Cross-Platform Smart Environments: If you're building a smart home, a local IoT setup, or any other system where devices from different platforms (such as Apple, Android, and Linux) need to communicate with each other, Multicast DNS (mDNS) is often the best choice. It works well in local networks, requires no configuration, and supports service advertisement, so devices can both discover and describe what they offer (e.g., "I'm a smart speaker").

➢Use Bluetooth for Mobile and Wearable Devices: For scenarios where devices are close together, such as a smartwatch syncing with a phone or a fitness tracker communicating with a tablet, Bluetooth is an ideal choice. It doesn't rely on Wi-Fi or IP, works offline, and offers built-in encryption and secure pairing.

➢Use LLMNR for Windows-Only Environments: If your setup is Windows-specific, such as a small office lab, classroom, or enterprise environment where all devices are running Windows, LLMNR can be a simple way to enable device name resolution without additional configuration.

➢Use MAC-Based Discovery for Diagnostics in Tightly Controlled Networks: MAC address-based methods are effective when you need to identify devices physically present on a local network, such as during network diagnostics, hardware inventory checks, or low-level monitoring in static environments. However, because these methods lack security and can be easily spoofed, they should only be used in trusted, controlled networks, such as a laboratory environment or within a secure facility.

➢When Security Matters: Add a Second Layer: Most of these non-IP methods offer convenience, not ironclad security. So, if you're working in a context where security is critical, such as healthcare, finance, or industrial control, you don't rely solely on discovery. Here's what can be done:

○Add application-level authentication: Ensure devices verify their identity after discovery using credentials or tokens.
○Use device certificates: Public key infrastructure (PKI) can help validate device identity and prevent impersonation.
○Secure the data: Even after discovery, use protocols like TLS or DTLS to encrypt communication and protect against eavesdropping or tampering.

VII. CONCLUSION

As technology moves closer to where data is created, in homes, factories, vehicles, and remote environments, edge computing is becoming the new frontier. However, in these decentralized and often disconnected spaces, relying on traditional IP networking is simply insufficient.

Non-IP-based communication methods are becoming essential. Whether you're trying to pair a wearable device, set up smart home equipment, or run a sensor network in a field, these methods offer the kind of flexibility, simplicity, and offline capability that IP-based systems struggle to deliver.

The future lies in combining these techniques rather than just choosing one. Systems that can adapt to their surroundings (e.g., switching from Bluetooth to mDNS when Wi-Fi becomes available) will be more resilient and user-friendly. And when security is layered on top, through authentication, encryption, and smart device management, these edge networks can operate safely even without a central internet connection.

Ultimately, to support the growing number of edge devices in our world, we need hybrid frameworks —systems that utilize the right tool for the job based on the environment, the device, and the level of trust required. This kind of adaptability will enable "zero-touch" deployments, where devices can find each other, connect securely, and start working together right out of the box.

Edge networking doesn't have to be complex. But it does have to be smarter, and that starts with rethinking how devices connect when IP isn't an option.

REFERENCES

1. Cheshire, S., & Krochmal, M. (2013). Multicast DNS (RFC 6762). IETF. Retrieved from https://datatracker.ietf.org/doc/html/rfc6762
2. Aboba, B., & Thaler, D. (2007). Link-Local Multicast Name Resolution (LLMNR) (RFC 4795). IETF. Retrieved from https://datatracker.ietf.org/doc/html/rfc4795
3. Apple Inc. (n.d.). Bonjour Overview. Apple Developer. Retrieved from https://developer.apple.com/bonjour/
4. Avahi Project. (n.d.). Avahi Daemon Documentation. Retrieved from https://www.avahi.org/
5. Microsoft Corporation. (n.d.). LLMNR Whitepaper. Microsoft Learn. Retrieved from https://learn.microsoft.com/
6. BlueZ Project. (n.d.). The Official Linux Bluetooth Protocol Stack. Retrieved from http://www.bluez.org/
7. IEEE. (2022–2024). Edge Computing: A Comprehensive Survey Series. IEEE Xplore. [Surveys published across 2022–2024].

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com