Towards the Future Internet: Opportunities with NEW IP

[1]Rushikesh Bhosale, [2] Vaishnavi Aher, [3]Shraddha Maharana, [4] Nikhil Yadhav, [5]Jai Girawale

[1]Student, [2] Student, [3]Student, [4]Student, [5]Faculty
[1]MIT Arts, Commerce & Science College, Pune, India
[1]rushibhosale153@gmail.com, [2]ahervaishnavi28@gmail.com,
[3]shru.maharana0920@gmail.com,[4]yadavnikhil17102004@gmail.com, [5]jaigirawale123@gmail.com

Abstract— **The fast change in the number of internet-connected devices and the inadequacy of existing IP framework necessitates the timely evolution of current packet and information exchange protocols employed in existing networks. This paper dispels New IP, a system developed to address the current encumbrances hindering the growth of traditional IPv4 and IPv6 systems, such as lack of scalability, security, real-time quality-of-service (QoS), and restructuring merit in regard to today are three essential fields: IoT, 5G, and autonomous systems. New IP adds exciting functionalities in terms of variable-length addressing, built-in security, determinism, and energy-efficient processing for state-of-the-art applications. The framework would be design-aware and employ metadata-based configurability, awareness-based routing, and network slicing capabilities toward low latency/high reliability in the support of enhanced QoS. Efficiency in terms of low latency and high-demand bandwidth is illustrated through charming usage cases in industrial IoT and telemedicine. While New IP provides various beneficial perks against existing protocols like flexibility, scalability, and better synergy with tomorrow's technologies, the wide adoption of the said protocol shall once again be the causative agent of change due to overhauling existing infrastructure, compatibility, and centralization-and network neutrality concerns. This paper provides a comparison of New IP with IPv4 and IPv6, specifying its additional merits while also laying bare directions for future work concerning real-world deployment and migration strategies.**

Index Terms— **NEW IP, IPv4, IPv6, AR, VR, Flexible addressing.**

I. INTRODUCTION

As an internet defines as "network of networks", which includes large number of devices and is also challenge to provide these vast range of IP address to each device. Also, traditional IPv4 address have limitation of location. A unique solution new IP emerged to solve all these problems. The concept of New IP presented to international committee like International Telecommunication Union (ITU), Internet Engineering Task Force (IETF), between 2018 and 2020 by Huawei.

The primary goal is replaced or supplement to IPV4 or IPV6 with additional functionality like metadata driven customization, service awareness, additional security. It is more efficient for flexible technologies like 5G, AR (Augmented Reality), VR (Virtual Reality), IOT, Smart Cities and beyond. The New IP framework supports features like variable length addressing, Multi Semantic Addresses, User-defined network (like SDN).

Challenges of current model:

- Addressing Scalabilities: Although IPv6 provide a large range of IP address (2128) but still its deployment is quite slow and inefficient in specific use cases like IOT.
- Lack of built in Security: IPv4 and IPv6 rely on external security protocol likes HTTPS, IPSEC. It is also vulnerable to Spoofing attacks, DDOS attacks and it doesn't provide user authentication.
- Quality of Service (QoS) Issue: Current internet struggle with problems like latency, jitter and packet loss specially in real time applications (AR, VR and autonomous system).
- Mobility support: Modern technologies like autonomous vehicles, drones require continue mobility, which is challenge for current IP system.
- Energy efficiency: The current IP system not optimized for power consuming devices like IOT sensers.
- Network fragment and Centralization risk: The current decentralized model leads to inefficiency and difficulties in large scale device management.
- Difficulties with Emerging technologies: The technologies like homographic communication, 5G, 6G, high precision robotics can have unique requirement of not adequately address by IPv4 or IPv6.

Solution offered by NEW IP over above Challenges:

- Addressing Flexibilities: NEW IP offers variable length addressing which optimized of different device and applications. It also enhances scalabilities for IOT and next generation technologies.
- Built in security: NEW IP provides built in security mechanism into IP protocol itself which reduce external relying on other tools and protocols
- Quality of Service: NEW IP offers deterministic network which is predictable and consistent QOS for real-time application
- Mobility Support: It focuses on native mobility support it enables device to maintain their uninterrupted connectivity across network
- Energy Efficiency: NEW IP claims to enhance energy efficiency through customizable protocol based on specific device need
- Network Fragmentation: It offers centralized manage network that allows better control and lack of openness
- Suitable for Emerging Technology: The main goal or aim to provide unique solution for vertical industries and new emerging technologies.

II. LITERATURE REVIEW

This research paper proposes a new internet protocol framework called NEW IP to address the limitations of current IP. NEW IP's key features are variable-length and multi-semantic addresses, allowing flexible identification of both physical and virtual objects. It also enables user-definable networking, letting users customize packet processing. The paper details NEW IP's architecture and illustrates its benefits through use cases focusing on smart home applications and service-aware routing. It compares NEW IP to existing solutions like 6LoWPAN and ICN architectures, highlighting NEW IP's advantages in efficiency and flexibility. The authors conclude by outlining future work, including real-world implementation and a migration strategy for legacy systems. The current internet works on IPv4 and IPv6 which is introduced by Postell in 1981. Current IP uses 32 bits for IPv4 and 128 for IPv6 address. It provides a strong foundation of internet connectivity, but nowadays it struggled as many evolutions takes place in the field as per explanation of Peering and Hidden in 1998.

IPv6 introduced for vastly larger address space. It also enhances routing capabilities but still the adoption of IPv6 is slow. We faced issues like mobility, energy, efficiency and real time communication remains unaddressed

TO overcome above challenge, Huawei (2019-2020) introduces concept of NEW IP Framework with features deterministic network, native mobility supports and built in security features. It enables variable length addressing to optimized network for IOT and ultra-low latency application, however it is a theoretical groundwork which highlights NEW IPs potential to meet future demand. But still, it remains conceptual.

The Future Internet Architecture (FIA) and named data networking (NDN) takes efforts to shorten the length of current IP Address. Jacobson et al (2009) discover NDN as central approach which focus on securing data rather than medium of communication similarly Koponen et al (2007) proposed data-oriented architecture for flexible and efficient networking while both of these offers innovative and unique solution but they lack comprehensive scope of NEW IP in security addressing and scalability.

The draft of NEW IP has been opposed for division of worldwide internet imposition of centralized governance. ISOC claims that centralization in NEW IP architecture allows pervasive surveillance and restrict network neutral (ISOC 2020) additionally ICANN added that NEW IP transaction would significantly poses compatibility financial burden to existing infrastructure.

This all-feasibility studies have described importance of deterministic networking for applications like autonomous system and telemedicine. IEEE research (2021) gives us variable length addressing system which promises the efficiency and optimization of these industries

III. BRIEF EXPLANATION OF NEW IP FRAMEWORK

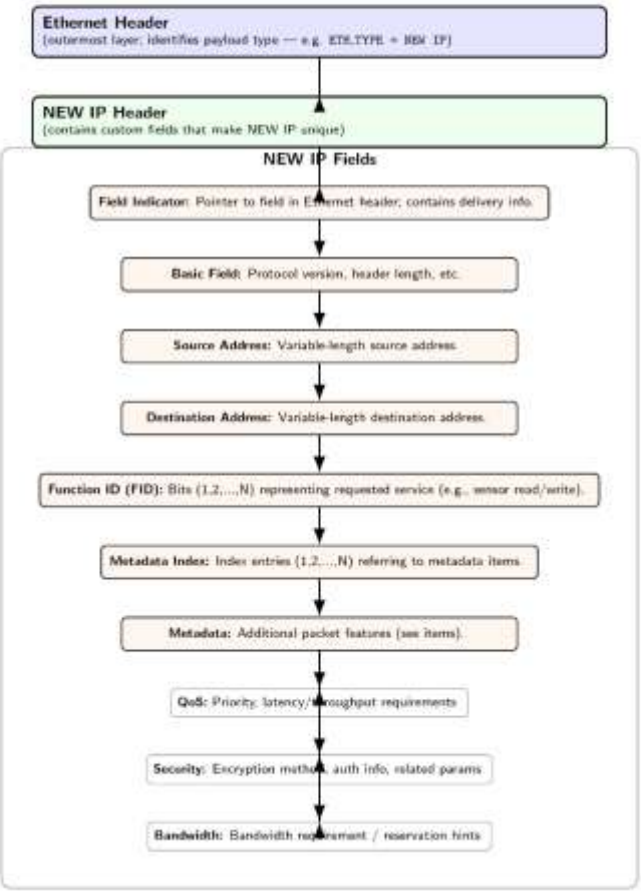
Ethernet Header
(outermost layer; identifies payload type — e.g. ETH.TYPE = NEW IP)
NEW IP Header
(contains custom fields that make NEW IP unique)
NEW IP Fields
Field Indicator: Pointer to field in Ethernet header; contains delivery info.
Basic Field: Protocol version, header length, etc.
Source Address: Variable-length source address.
Destination Address: Variable-length destination address.
Function ID (FID): Bits (1,2,...,N) representing requested service (e.g., sensor read/write).
Metadata Index: Index entries (1,2,...,N) referring to metadata items.
Metadata: Additional packet features (see items).
QoS: Priority, latency/throughput requirements
Security: Encryption method, auth info, related params
Bandwidth: Bandwidth requirement / reservation hints

Fig. 1 Header of NEW IP

NEW IP Header Architecture and Routing Mechanisms

The NEW IP protocol introduces a redefined packet header structure designed to address the limitations of conventional Internet Protocols and to support the needs of future communication systems. Its architecture integrates flexibility, extensibility, and application-awareness directly into the header fields, enabling advanced routing and service customization.

Header Structure

Ethernet Header: The Ethernet Header represents the outermost encapsulation of the NEW IP packet. Its primary role is to identify the payload type; for example, the field ETH_TYPE is used to indicate that the encapsulated payload belongs to the NEW IP protocol.

NEW IP Header

- The NEW IP Header is the innovation core of this protocol. It introduces custom-defined fields that extend beyond the capabilities of IPv4 and IPv6.
- Field Indicator: Acts as a pointer to the Ethernet header fields and carries essential delivery information.
- Basic Field: Encodes fundamental information such as the protocol version and header length.
- Source Address: A variable-length field that flexibly accommodates diverse addressing schemes.
- Destination Address: Similarly variable in length, supporting heterogeneous addressing environments.
- Function ID (FID): Represents service-specific identifiers using bit patterns (1,2,…,N). In IoT systems, for instance, FIDs may directly correspond to sensor operations such as data read or write requests.
- Metadata Index: Serves as a reference system (1,2,…,N) pointing to associated metadata records.
- Metadata: Enhances packet intelligence by embedding:
- Quality of Service (QoS) parameters: latency and priority requirements.
- Security parameters: details of encryption mechanisms and authentication methods.
- Bandwidth specifications: allocation needs for reliable data transmission.
- This modular design ensures that the header can evolve with emerging requirements while maintaining backward compatibility with traditional networking layers.

Routing Mechanisms in NEW IP

In addition to its flexible header fields, NEW IP incorporates advanced routing strategies tailored to application-level requirements:

Application-Aware Routing

- Packet headers are actively inspected to align routing paths with application needs. Critical requirements such as latency tolerance, bandwidth guarantees, and security constraints directly influence route selection.

Deterministic Path Selection

- For use cases that demand strict reliability (e.g., industrial automation or mission-critical IoT), the protocol supports predefined routing paths to ensure deterministic delivery.

Quality of Service (QoS) Integration

- Packets are dynamically prioritized based on QoS metadata. High-priority traffic such as real-time control signals is routed preferentially, ensuring minimal delay.

Network Slicing

- The protocol enables logical partitioning of the physical infrastructure into multiple virtual networks. Each slice can be optimized for a specific use case, such as low-latency applications, high-throughput video streaming, or secure IoT communications.

IV. GENERAL OVERVIEW OF ALL IP ADDRESS:

Table 1

Feature	IPv4	IPv6	NEW IP
Address Length	32 bits	128 bits	Variable length
Header size	20-60 bytes	40 bytes	Variable length
Header Field	12 field	8 field	Variable fields based on customization
Protocol version	4	6	NEW IP

V. *HEADER STRUCTURE OF ALL IP ADDRESS*

Table 2

Field	IPv4	IPv6	NEW IP
Version	4	6	Defined in Basic Field
Header Length	Fixed length (20-40 bytes)	Not required as they use flexible length header	Not required as they use flexible length header
Source Address	32 bits	128 bits	Variable length
Destination Address	32 bits	128 bits	Variable length
QoS Parameters	Present in the Type of Service (ToS) field.	Supported via Flow Label and Traffic Class	Explicit field with customization.
Payload Length	Total length (header + data)	Total length (header + data)	Support variable payload length for various application.
Fragmentation	Supported (fields: ID, Flags, Offset).	Not supported; handled at the source node.	support metadata-based fragmentation.
Security	IPSEC as add-on	IPSEC as built in security	Built-in security with encryption and signature options.
Routing Instructions	Limited.	Simplistic hop-by-hop routing.	Application-aware and deterministic routing.
Metadata Support	Not present	Limited	More Metadata for QoS support

VI. *COMPARISON OF ROUTING MECHANISM*

Table 3

Features	IPv4	IPv6	NEW IP
Routing Method	Hop-by-hop based on destination address.	Hop-by-hop based on destination address.	Application-aware and deterministic routing.
Deterministic Routing	Not supported.	Not supported.	Fully supported for time-sensitive applications.
Network slicing	Not supported.	Not supported.	supported with independent virtual network slices.
Quality of Service (QoS)	Basic (ToS field).	Enhanced (Traffic Class and Flow Label).	Detailed QoS parameters embedded in the header.

VII. *CASE STUDY*

1. Industrial IoT with Deterministic Networking:

- Scenario: A modern smart factory has machines, sensors, and robots that network over communication to coordinate manufacturing processes. Some of these tasks include the assembling process by robotic arms, sensors performing surveillance on production lines, and quality assurance cameras, where their communication must be in real-time with minimum delay.

- Problems with IP Models Currently Used:
    - Latency: IPv4 and IPv6 utilize best-effort delivery, which results in delays. In real-time systems, any delayed action can completely cause disarray.
    - Quality of Service (QoS): Current protocols lack precise mechanisms to ensure consistent network performance for critical operations.
    - QoS Integration: QoS parameters like the tolerance to latency and bandwidth demands are explicitly present in the header as metadata. Critical packets such as robotic arm controls have high priority, whereas a system log file would have much lower priority.
    - Variable-Length Addressing: The addressing of the IoT devices tends to be uniquely different. New IP applies variable-length addressing for efficiently incorporating all these differing device types and minimizes overhead.
    - Real-Time Feedback: The metadata fields allow devices to share real-time status updates and diagnostics

- Example Workflow:
  A sensor detects a problem on the production line and transmits a packet with:
    - Source Address: Sensor ID.
    - Destination Address: Factory control system.
    - Function ID: Emergency signal.
    - QoS Metadata: High priority, low latency.
    - Routers route this packet according to its metadata and along deterministic paths to the destination.
    - The factory control system receives the packet within milliseconds and shuts down the production line before any damage can occur.
- Advantages
    - Guaranteed low latency.
    - Exact QoS for critical processes.
    - Enhanced scalability for diverse IoT devices.

2. Telemedicine and Remote Surgery:

- Scenario: A surgeon performs remote robotic surgery by using a high-speed network to command the surgical robots in real time. The network must support Real-time control signals (commands from the surgeon to the robot). High-definition video streams (feedback from cameras on the robot). Sensor data (e.g., force applied by surgical instruments).

- Challenges with Current IP Models:
    - Latency Sensitivity: Even the slightest delay in control signals may be dangerous enough to cost a life.
    - Bandwidth: High-definition video streams require significant bandwidth and priority over less critical traffic.
    - Security: Medical data must remain secure to protect patient privacy.

- How New IP Works in This Use Case:
    - Multi-Path Transmission: New IP supports multi-path routing, where different types of data (e.g., control signals, video streams) are transmitted along separate optimized paths. Control signals take low-latency paths, while video streams take high-bandwidth routes.
    - QoS and Application Metadata: The New IP header includes QoS metadata for each type of data.
    - Control signals: Ultra-low latency and high reliability.
    - Video streams: High bandwidth and loss tolerance.
    - This ensures that critical data is prioritized over non-critical data.
    - Security and Encryption: Metadata fields include encryption parameters and security metadata to ensure the data cannot be intercepted or altered during transmission.
    - Network Slicing: Using network slicing, the New IP infrastructure creates dedicated virtual networks for different types of data. For instance,
        - Slice 1: Ultra-low latency control signals
        - Slice 2: High-bandwidth video streams
        - Slice 3: Sensor data for monitoring

- Example Flow: The surgeon sends control signals to a robotic arm. The New IP header contains a Function ID that defines the type of control signal. The header also carries QoS requirements for ultra-low latency The robot sends back real-time HD video and force feedback Metadata in the video packets gives a priority to bandwidth. Sensor packets include security metadata to ensure the integrity of the feedback. Routers along the path process the metadata and. Route control signals through low-latency paths. Route video streams through high-bandwidth paths.
- Benefits:
    - Minimal latency ensures precise robotic movements.
    - High-quality video and sensor data improve surgical accuracy.
    - Enhanced security protects patient data.

VIII. *CONCLUSION:*

In this paper, we review a NEW IP Framework and expressed its application in future, also give comparative study of NEW IP, IPv4, IPv6. from our review we conclude following things:

Table 4 Protocol Comparison

Protocols	Advantages	Disadvantages
IPv4	- Simple design.	- Address exhaustion. - Limited QoS and security support. - High overhead due to fragmentation
IPv6	- Larger address space. - Better QoS and security (IPSec).	- Fixed header size increases packet size even for minimal use cases. - Slow adoption worldwide.
NEW IP	- Flexible addressing and headers. - Built-in QoS and security. - Ideal for real-time, IoT, and AI applications.	- Not yet adopted. - Complex implementation requiring infrastructure overhaul. - Centralization concerns.

As NEW IP provides KPI guarantee, latency, customization field. It is a very useful for next generation technologies.

REFERENCES

[1] Stephen E. Deering, Robert M. Hinden (1998), "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460 [https://www.rfc-editor.org/rfc/rfc2460]

[2] Jon Postel (1981), "Internet Protocol - DARPA Internet Program Protocol Specification", RFC 791.

[3] C. Gomez, J. Paradells, C. Bormann, and J. Crowcroft, “From 6LoWPAN to 6Lo: Expanding the Universe of IPv6-Supported Technologies for the Internet of Things”, IEEE Communications Magazine, vol. 55, no. 12, pp. 148-155, 2017

4] R. Li, A. Clemm, U. Chunduri, L. Dong, and K. Makhijani, “A New Framework and Protocol for Future Networking Applications”, ACM SIGCOMM 2018 Workshop on Networking for Emerging Applications and Technologies (NEAT 2018), August 2018.

[5] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, “A Survey of Information-Centric Networking”, IEEE Communications Magazine, vol. 50, no. 7, pp. 26-36, 2012.

[6] S. Ren, D. Yu, Y. Tian, X. Gong, and R. Moskowitz, “Routing and Addressing with Length Variable IP Address”, ACM SIGCOMM 2019 Workshop on Networking for Emerging Applications and Technologies (NEAT 2019), pp. 21-26, 2018.

[7] A. Afanasyev, J. Burke, T. Refaei, L. Wang, B. Zhang, and L. Zhang, “A Brief Introduction to Named Data Networking”, 2018 IEEE Military Communications Conference (MILCOM), pp. 605-611, 2018.

[8] S. S. Adhatarao, J. Chen, M. Aurmaithurai, X. Fu, and K. K. Ramakrishnan, “Comparison of Naming Schema in ICN”, 2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), June 2016.

[9] D. Raychaudhuri, K. Nagaraja, and A. Venkataramani, “MobilityFirst: A Robust and Trustworthy Mobility-Centric Architecture for the Future Internet”, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 16, no. 3, pp. 2-13, 2012.

[10] C. Bormann, and P. Hoffman, “Concise Binary Object Representation (CBOR)”, IETF RFC, vol. 7049, October 2013.

[11] X. Li, B. Liu, Y. Chen, Y. Xiao, J. Tang, and X. Wang, “Artemis: A Practical Low-Latency Naming and Routing System”, in 48th International Conference on Parallel Processing (ICPP 2019), August 2019.

[12] P. Bosshart, D. Daly, G. Gibb, M. Martin and et al., “P4: Programming Protocol-Independent Packet Processors”, ACM SIGCOMM Computer Communication Review, July 2014.

[13] H. Song, “Protocol-oblivious Forwarding: Unleash the Power of SDN through a Future-Proof Forwarding Plane”, ACM SIGCOMM 2013 Workshop on Hot Topics in Software Defined Networking (HotSDN ’13), August 2013.

[14] C. Hickman, and F. Wang, “A Variable Length Address Assignment Scheme for 6LoWPAN”, 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), August 2019

. [15] M. R. Sabir, M. S. Mian, K. Sattar, and M. A. Fahiem, “IP Address Space Management using Aggregated Fixed Length Subnet Masking”, 2007 International Conference on Electrical Engineering, August 2007.

[16] K. Ryu, and B. Choe, “A novel address pointer switch architecture for variable length packets”, 2008 10th International Conference on Advanced Communication Technologym, April 2008.

[17] G. Bouabene, C. Jelger, C. Tschudin, S. Schmid, A. Keller, and M. May, “The autonomic network architecture (ANA)”, IEEE Journal on Selected Areas in Communications, vol. 28, no. 1, pp. 4-14, 2010.

[18] Y. Kang, B. Jung, “IPv6 Anycast Routing aware of a Service Flow”, 2007 IEEE International Symposium on Consumer Electronics, June 2007.

[19] A. Galis, S. Denazis, C. Brou, and C. Klein, “Programmable Networks for IP Service Deployment”, Artech House, 2004.