Network Working Group
Internet-Draft
Intended status: Informational
Expires: 25 April 2024

L. Iannone, Ed.
Huawei

23 October 2023

# IP Addressing Considerations
## draft-iannone-ip-addressing-considerations-02

Abstract

The Internet Protocol (IP) has been the major technological success in information technology of the last half century. As the Internet becomes pervasive, IP has been replacing communication technology for many domain-specific solutions, but it also has been extended to better fit the specificities of the different use cases. For Internet addressing in particular, as it is defined in RFC 791 for IPv4 and RFC 8200 for IPv6, respectively, there exist many extensions. Those extensions have been developed to evolve the addressing capabilities beyond the basic properties of Internet addressing. This document discusses the properties the IP addressing model, showcasing the continuing need to extend it and the methods used for doing so.

Table of Contents

1. Rationale . . . . . 3
2. Introduction . . . . . 4
3. Current Properties of Internet Protocol Addressing . . . . . 5
3.1. Property 1: Fixed Address Length . . . . . 5
3.2. Property 2: Ambiguous Address Semantic . . . . . 5
3.3. Property 3: Limited Address Semantic Support . . . . . 6
4. Perceived IP Addressing Shortcomings . . . . . 6
5. Existing IP Addressing Extensions . . . . . 10
5.1. Length Extensions . . . . . 10
5.2. Identity Extensions . . . . . 13
5.3. Semantic Extensions . . . . . 17
5.4. IP Addressing Extensions Overall Summary . . . . . 21
6. Concerns Raised by IP Addressing Extensions . . . . . 23
6.1. Limiting Address Semantics . . . . . 23
6.2. Complexity and Efficiency . . . . . 23
6.3. Security . . . . . 26
6.4. Fragility . . . . . 27
6.5. Summary of Concerns . . . . . 28
7. Discussion . . . . . 29
8. Security Considerations . . . . . 31
9. IANA Considerations . . . . . 31
Acknowledgments . . . . . 31
Informative References . . . . . 31
Appendix A. Desirable Networking Features . . . . . 50
Appendix B. IP Addressing Extensions driven by Use Cases . . . . 53
B.1. Communication in Constrained Environments . . . . . 53
B.2. Communication within Dynamically Changing Topologies . . 54
B.3. Communication among Moving Endpoints . . . . . 56
B.4. Communication Across Services . . . . . 59
B.5. Communication Traffic Steering . . . . . 60
B.6. Communication with built-in security . . . . . 61
B.7. Communication protecting user privacy . . . . . 62
B.8. Communication in Alternative Forwarding Architectures . . 62
Appendix C. Examples of Internet Addressing Properties Extensions . . . . . 64
C.1. Length Extensions . . . . . 64
C.2. Identity Extensions . . . . . 66

C.3. Semantic Extensions . . . . . 68
Contributors . . . . . 72
Author's Address . . . . . 74

## 1. Rationale

The IETF community has, at various times, discussed the IP addressing model and its possible evolution, while keeping its structure unchanged, so to accommodate future use cases and existing deployments. This document does (or at least tries to) capture the discussion that the IETF community held about IP addressing model in the early 2020s. The discussion originated from two memos proposing an analysis of the extensions developed to better adapt the IP addressing model to specific use cases [I-D.iannone-internet-addressing-considerations] and a (shorter) companion memo trying to formalize a related problem statement [I-D.iannone-scenarios-problems-addressing]. Further, an informal side meeting was organized during IETF 112 [SIDE112] with a panel of experts, which had a lively discussion. That discussion continued, with a very large volume of messages, on the INTArea mailing list and other mailing lists, like architectural discuss, honing into the related question on what desired features a network should provide in the first place (see Appendix A for a summary of the feature listed in that discussion). The IAB also touched briefly the topic in one of their retreats in 2022. The momentum and the amplitude of the discussion did raise the question whether or not to go for a formal Working Group, however, the community failed to converge on a specific direction that could eventually lead to an evolution of the IP addressing model and at the same time the steam diminished.

This document does not provide a definite answer nor does it propose or promote specific solutions to the issues it portrays. Instead, this document, which includes a large portion of last revision of the aforementioned individual submissions, captures the discussion on the perceived needs for addressing, with the possibility to fundamentally re-think the addressing in the Internet beyond the objectives of IPv6, in order to provide the flexibility to suitably support the many new forms of communication that will emerge.

Although some of the discussions hinted at "something should be done", those same discussions never converged to answer the "what should be done" aspect. However, we assert from experiences in the past that the community may at some point in the future re-open discussions surrounding the IP addressing model and its possible evolution, in which case this document will be useful.

## 2. Introduction

The Internet Protocol (IP), positioned as the unified protocol at the (Internet) network layer, is seen by many as key to the innovation stemming from Internet-based applications and services. Even more so, with the success of the TCP/IP protocol stack, IP has been gradually replacing existing domain-specific protocols, evolving into the core protocol of the ever-growing communication eco-system [CISCO-IOE].

The Internet addressing system [RFC0791], represented in the form of the IP address and its locator-based (topological) semantics, has brought about the notion of a 'common namespace for all communications at the IP layer'. Compared to proprietary technology-specific solutions, such unified namespace ensures end-to-end communication from any device connected to the Internet to another.

As the Internet Protocol adoption has grown towards the global communication system we know today, its characteristics have evolved subtly, with [RFC6250] documenting various aspects of the IP service model and its frequent misconceptions, including Internet addressing. Use cases, associated services, node behaviors, and requirements on packet delivery have since been significantly extended, with suitable Internet technology being developed to accommodate them in the framework of addressing that stood at the aforementioned beginning of the Internet's development.

This continuing evolution includes addressing and, therefore, the address structure, as well as the semantic that is being used for packet forwarding (e.g., service identification, content location, device type). In this, the topological semantic of IP is fundamental when reconciling the often-differing semantics for 'addressing' that can be found in new use cases. Due to this centrality, use cases have to adopt specific solutions, e.g., translating/mapping/converting concepts, semantics, and ultimately, solution-specific addressing, and integrate them into the common IP addressing model.

This per-use-case extension approach has implications that go beyond addressing, nevertheless, in this document the discussion only focuses on the addressing viewpoint, identifying shortcomings perceived from this perspective, in particular with respect to IP addressing properties. The key properties of Internet addressing, outlined in Section 3, are (i) the fixed length of the IP addresses, (ii) the ambiguity of IP addresses semantic, while still (iii) providing limited IP address semantic support. Those properties are derived directly as a consequence of the respective standards that provide the basis for Internet addressing, most notably [RFC0791] for IPv4 and [RFC8200] for IPv6, respectively. The limitations of the IP

addressing properties are discussed in Section 4, including the various use cases and scenarios where such limitations actually show up.

What is interesting to note is that different use cases may actually been handled with the same type of extension. This shows that, based on an architectural approach, evolving the properties discussed in Section 3 is possible and even desirable since it has the advantage to be designed in a coherent fashion, avoiding point-solutions which potentially create contention when deployed. To this end, Section 5 discusses Internet addressing properties extensions, associating the different use cases that take advantage of the property's extensions.

While the various extensions proposed through the years certainly did a fine job in solving the problem at hand, this "patching" approach raises also concerns. Section 6 outlines considerations and concerns that arise with such extension-driven approach, arguing that any requirements for solutions that would revise the basic Internet addressing would require to address those concerns.

## 3. Current Properties of Internet Protocol Addressing

In this section, the three most acknowledged properties related to Internet addressing are detailed. Those are (i) fixed IP address length, (ii) ambiguous IP address semantic, and (iii) limited IP address semantic support.

### 3.1. Property 1: Fixed Address Length

The fixed IP address length is specified as a key property of the design of Internet addressing, with 32 bits for IPv4 [RFC0791], and 128 bits for IPv6 [RFC8200], respectively. Given the capability of the hardware at the time of IPv4 design, a fixed length address was considered as a more appropriate choice for efficient packet forwarding. Although the address length was once considered to be variable during the design of Internet Protocol Next Generation ("IPng", cf., [RFC1752]) in the 1990s, it finally inherited the design of IPv4 and adopted a fixed length address towards the current IPv6. As a consequence, the 128-bit fixed address length of IPv6 is regarded as a balance between fast forwarding (i.e., fixed length) and practically boundless cyberspace (i.e., enabled by using 128-bit addresses).

### 3.2. Property 2: Ambiguous Address Semantic

Initially, the meaning of an IP address has been to identify an interface on a network device, although, when [RFC0791] was written, there were no explicit definitions of the IP address semantic.

With the global expansion of the Internet protocol, the semantic of the IP address is commonly believed to contain at least two notions, i.e., the explicit 'locator', and the implicit 'identifier'. Because of the increasing use of IP addresses to both identify a node and to indicate the physical (or virtual) location of the node, the intertwined address semantics of identifier and locator was then gradually observed and first documented in [RFC2101] as 'locator/ identifier overload' property. With this, the IP address is used as an identification for hosts and servers.

### 3.3. Property 3: Limited Address Semantic Support

Although IPv4 [RFC0791] did not add any semantic to IP addresses beyond interface identification (and location), time has proven that additional semantics are desirable (c.f., the history of 127/8 [HISTORY127] or the introduction of private addresses [RFC1918]). Later on, IPv6 [RFC4291] introduced some form of additional semantics based on specific prefix values, for instance link-local addresses or a more structured multicast addressing. Nevertheless, systematic support for rich address semantics remains limited and basically prefix-based.

## 4. Perceived IP Addressing Shortcomings

What follows is the list of the most relevant perceived shortcomings identified during the various exchanges, which is however not to be considered exhaustive.

1. Limiting Alternative Address Semantics: Several communication scenarios pursue the use of alternative semantics (e.g., for privacy, for service identification, or for content identification) preserving what constitute an 'address' of a packet traversing the Internet, which falls foul of the defined network interface semantic of IP addresses.

2. Hampering Security: Aligning with the semantic and length limitations of IP addressing hampers the security objectives of any new semantic, possibly leading to detrimental effects and possible other workarounds (at the risk of introducing fragility rather than security).

3. Hampering Privacy: The simple use of IP addresses as global stable interface identifiers raises clear privacy concerns. It goes beyond profiling the traffic of end users, since it can even be easily used to obtain the real identity of individuals.

4. Complicating Traffic Engineering: Utilizing a plethora of non-address inputs (e.g., port numbers, segments ID, payload) into the traffic steering decision in real networks complicates traffic engineering in that it makes the development of suitable policies more complex, while also leading to possible contention between methods being used.

5. Hampering Efficiency: Extending IP addressing through point-wise solutions also hampers efficiency, e.g., through needed re-encapsulation (therefore increasing the header processing overhead as well as header-to-payload ratio), through introducing path stretch, or through requiring compression techniques to reduce the header proportion of large addresses when operating in constrained environments.

6. Fragility: The introduction of point solutions, each of which comes with possibly own usages of address or packet fields, together with extension-specific operations, increases the overall fragility of the resulting system, caused, for instance, through contention between feature extensions that were neither foreseen in the design nor tested during the implementation phase.

The above shortcomings are not apparent in every possible use case, rather they appear, in a more or less severe form, in specific use cases. Hereafter, a set of such kind of use cases, for which extensions to the IP addressing model have been already proposed on a case-by-case basis, is listed. Further details about these use cases and related extensions can be found in Appendix B, where for each use case there is an entire section. Here, for each use case, a very short description and the issues they relate to is provided, also summarized inTable 1.

* Communication in Constrained Environments: Resource constrained networks like Internet of Things (IoT), Industrial IoT, avionics. When resources are strongly constrained the use of the single IP addressing space becomes an hindrance. Proposed solutions relay on some form of adaptation that reduces resource consumption but complicates traffic engineering (Issue 4), reduces efficiency (Issue 5), and increases fragility (Issue 6).

* Communication within Dynamically Changing Topologies: Networks that exhibit dynamically changing, e.g. satellite networks, vehicular networks, Flying Ad-hoc NETworks (FANETs). The IP addressing model has been conceived for networks that do not change their topology that often, hence their semantic is not adapted to dynamic networks (Issue 1). This clearly complicates traffic engineering (Issue 4) and reduces efficiency (Issue 5), leading to increased fragility (Issue 6).

* Communication among Moving Endpoints: The huge progress in wireless communications (WiFi, 3G/4G/5G, etc) enables ubiquitous endpoint mobility. The implicit locator semantic (Issue 1) of the addresses does not match the endpoint mobility use case, because of its continuous location change, exposing user location (Issue 3), complicating traffic steering (Issue 4), which reduces efficiency (Issue 5), making end-to-end connectivity more fragile (Issue 6).

* Communication Across Services: Communication among services and resources from various aspects such as remote collaboration, shopping, content production, delivery, education, etc. The IP address has no notion of service (Issue 1), while proposed solutions introduce some form of service identification over the IP layer, which reduces efficiency (Issue 5) and complicates traffic engineering (Issue 4), introducing some fragility in the mapping function between IP addresses and service identifiers (Issue 6) and opening privacy concerns (Issue 3) if the services is accessing are exposed.

* Communication Traffic Steering: The ability to control where the traffic goes through (beyond the simple best-effort shortest-path). The limited semantic of IP addresses translates to limited traffic engineering capabilities (Issue 1), which has been solved by considering other information beside IP addresses, hence using more complex and less efficient solutions (Issues 4 and 5).

* Communication with built-in security: AAA (Authentication, Authorization, Accountability), end-to-end encryption. The limited semantic of IP addresses do not facilitate the implementation of security solutions (Issues 1 and 2), and the introduction of encryptions complicates traffic engineering because some information is now not available anymore (Issue 4), hence reducing efficiency (Issue 5) and adding fragility (Issue 6), because of the workarounds introduced to cope with the lack of security.

* Communication protecting user privacy: Private communication and fingerprinting avoidance is cumbersome in the IP addressing model (Issue 3), while the introduction of additional operations to protect user privacy reduces forwarding efficiency (Issue 5).

* Communication in Alternative Forwarding Architectures: Non-Internet Protocol based networks. Alternative forwarding paradigms do not necessarily leverage on IP addressing, because of its limited semantic (Issue 1), also trying to simplify traffic steering (Issue 4) by leveraging on a reduced set of fields (if not just one). However, while certainly boosting efficiency inside their own deployments, such solutions introduce some fragility (Issue 6) at the boundaries, where translations/ adaptions need to be performed to restore native IP forwarding.

| | Issue 1 | Issue 2 | Issue 3 | Issue 4 | Issue 5 | Issue 6 |
|---|---|---|---|---|---|---|
| Constrained Environments | | | | x | x | x |
| Dynamically Changing Topologies | x | | | x | x | x |
| Moving Endpoints | x | | x | x | x | x |
| Across Services | x | | x | x | x | x |
| Traffic Steering | x | | | x | x | |
| Built-in Security | x | x | | x | x | x |
| User Privacy | | | x | | x | |
| Alternative Forwarding Architectures | x | | | x | | x |

Table 1: Issues Involved in Challenging Use Cases.

## 5. Existing IP Addressing Extensions

As already stated, during the years various technologies have been developed that circumvent some IP addressing shortcomings, basically extending the properties defined in Section 3.

Accommodating new requirements through ever new extensions as an extensibility approach to addressing complicates engineering due to the clearly missing boundaries against which contentions with other extensions could be managed. It complicates standardization since extension-based extensibility requires independent, and often lengthy, standardization processes. And ultimately, deployments are complicated due to backward compatibility testing required for any new extension being integrated into the deployed system.

Hereafter, an overview of existing extensions is provided, grouped by property. For each group, a general description and the methodology used by the various extensions is provided. Details about the cited technologies relates to properties extension can be found in Appendix C.

### 5.1. Length Extensions

Extensions in this section aim at extending the property described in Section 3.1, i.e., the fixed IP address length.

When IPv6 was designed, the main objective was to create an address space that would not lead to the same situation as IPv4, namely to address exhaustion. To this end, while keeping the same addressing model like IPv4, IPv6 adopted a 128-bit address length with the aim of providing a sufficient and future-proof address space. The choice was also founded on the assumption that advances in hardware and Moore's law would still allow to make routing and forwarding faster, and the IPv6 routing table manageable.

We observe, however, that the rise of new use cases but also the number of new devices, e.g., industrial/home or small footprint devices, was possibly unforeseen. Sensor networks and more generally the Internet of Things (IoT) emerged after the core body of work on IPv6, thus different from IPv6 assumptions, 128-bit addresses were costly in certain scenarios. On the other hand, given the investments that IPv6 deployment involved, certain solutions are expected to increase the addressing space of IPv4 in a compatible way, and thus extend the lifespan of the sunk investment on IPv4.

At the same time, it is also possible to use variable and longer address lengths to satisfy current networking demands. For example, in content delivery networks, longer addresses such as URLs are

required to fetch content, an approach that Information-Centric Networking (ICN) applied for any data packet sent in the network, using information-based addressing at the network layer. Furthermore, as an approach to address the routing challenges faced in the Internet, structured addresses are a possible solution in order to avoid the need for routing protocols. Using variable length addresses allow as well to have shorter addresses. So, for requirements for smaller network layer headers, shorter addresses could be used, alleviating the need to compress other fields of the header. Furthermore, transport layer port numbers can be considered short addresses, where the high order bits of the extended address are the public IP of a NAT. Hence, in IoT deployments, the addresses of the devices can be really small and based on the port number, but they all share the global address of the gateway to make each one having a globally unique address.

### 5.1.1. Shorter Address Length

#### 5.1.1.1. Description

In the context of constrained networks [RFC7228], where bandwidth and energy are very scarce resources, the static length of 128-bit for an IP address is more a hindrance than a benefit since 128-bit for an IP address is a lot of space, even to the point of being the dominant part of a packet. In order to use bandwidth more efficiently and use less energy in end-to-end communication, solutions have been proposed that allow for very small network layer headers instead.

#### 5.1.1.2. Methodology

Header Compression/Translation: One of the main approaches to reduce header size is by compressing it. Such technique is based on a stateful approach, utilizing what is usually called a 'context' on the small constrained device and the gateway for communications between an the device and a server placed somewhere in the Internet - from the edge to the cloud.

The role of the 'context' is to provide a way to 'compress' the original IP header into a smaller one, using shorter address information and/or dropping some field(s); the context here serves as a kind of dictionary.

Separate device from locator identifier: Approaches that are able to offer customized address length that is adequate for use in such constrained domains are preferred. Using different namespaces for the 'device identifier' and the 'routing' or 'locator identifier' is one such approach.

### 5.1.2. Longer Address Length

#### 5.1.2.1. Description

Historically, obtaining adequate address space is considered as the primary and raw motivation to invent IPv6. Longer address (more than 32-bit of IPv4 address), which can accommodate almost inexhaustible devices, used to be considered as the surest direction in 1990s. Nevertheless, to protect the sunk cost of IPv4 deployment, certain efforts focus on IPv4 address space depletion question but engineer IPv4 address length in a more practical way. Such effort, i.e., NAT (Network Address Translation), unexpectedly and significantly slows IPv6 deployment because of its high cost-effectiveness in practice.

Another crucial need for longer address lengths comes from "semantic extensions" to IP addresses, where the extensions themselves do not fit within the length limitation of the IP address. This section focuses on address length extensions that aim at reducing the IPv4 addresses depletion, while Section 5.3 discusses when longer address length are suitable to accommodate different address semantic.

#### 5.1.2.2. Methodology

Split address zone by network realm: This methodology first split the network realm into two types: one public realm (i.e., the Internet), and innumerable private realms (i.e., local networks, which may be embedded and/or having different scope). Then, it splits the IP address space into two type of zones: global address zone (i.e., public address) and local address zone (e.g., private address, reserved address). Based on this, it is assumed that in public realm, all devices attached to it should be assigned an address that belongs to the global address zone. While for devices attached to private realms, only addresses belonging to the local address zone will be assigned. In the local realms, addresses can be used for pure identification purpose (e.g. in a single hop WiFi network or a single hop personal area network).

Given that the local address zone is not globally unique, certain mechanisms are designed to express the relationship between the global address zone (in public realm) and the local address zone (in any private realm). In this case, global addresses are used for forwarding when a packet is in the public realm, and local addresses are used for forwarding when a packet is in a private realm.

### 5.1.3. Examples

Table 2 summarizes methodologies and lists examples of IP address length extensions.

| | Methodology | Examples |
|---|---|---|
| Shorter Address Length | Header compression/ translation | 6LoWPAN, ROHC, SCHC |
| | Separate device from locator identifier | EIBP, LISP, ILNP, HIP |
| Longer Address Length | Split address zone by network realm | NAT, EzIP |

Table 2: Length Extensions Summary

## 5.2. Identity Extensions

Extensions in this section attempt extending the property described in Section 3.2, i.e., 'locator/identifier overload' of the ambiguous address semantic.

From the perspective of Internet users, on the one hand, the implicit identifier semantic results in a privacy concern due to network behavior tracking and association. Despite that IP address assignments may be dynamic, they are nowadays considered as 'personal data' and as such undergoes privacy protection regulations. Hence, additional mechanisms are necessary in order to protect end user privacy.

For network regulation of sensitive information, on the other hand, dynamically allocated IP addresses are not sufficient to guarantee device or user identification. As such, different address allocation systems, with stronger identification properties are necessary where security and authentication are at highest priority. Hence, in order to protect information security within a network, additional mechanisms are necessary to identify the users or the devices attached to the network.

### 5.2.1. Anonymous Address Identity

#### 5.2.1.1. Description

As discussed in Section 3.2, IP addresses reveal both 'network locations' as well as implicit 'identifier' information to both traversed network elements and destination nodes alike. This enables recording, correlation, and profiling of user behaviors and historical network traces, possibly down to individual real user identity. The IETF, e.g., in [RFC7258], has taken a clear stand on such pervasive surveillance by classifying it as an attack on end users' right to be left alone (i.e., privacy). Regulations such as the EU's General Data Protection Regulation (GDPR) classifies, for instance, the 'online identifier' as personal data which must be carefully protected; this includes end users' IP addresses [VOIGT17].

Even before pervasive surveillance [RFC7258], IP addresses have been seen as something that some organizational owners of networked system do not want to reveal at the individual level towards any non-member of the organization. Beyond that, if forwarding is based on semantic extensions, like other fields of the header, extension headers, or any other possible extension, if not adequately protected it risks to introduce privacy leakage and/or new attack vectors.

#### 5.2.1.2. Methodology

Traffic Proxy: Since nodes between trusted proxy and destination (including the destination per se) can only observe the source address of the proxy, the 'identification' of the origin source is thereby hidden. To obfuscate information to the nodes between origin and the proxy, the traffic on such route would be encrypted via a key negotiated either in-band or off-band. Considering that all applications' traffic in such route is seen as a unique flow directed to the same trusted proxy, eavesdroppers have to make more efforts to correlate user behavior through statistical analysis even if they are capable of identifying the users via their source addresses. The protection lays in the inability to isolate single application-specific flows. According to the methodology, such approach is IP version independent and works for both IPv4 and IPv6.

Source Address Rollover: Privacy concerns related to address 'identifier' semantic can be mitigated through regular change (beyond the typical 24 hours lease of DHCP). Due to the semantics of 'identifier' that an IP address carries, such approach promotes to change the source IP address at a certain frequency. Under such methodology, the refresh cycling window has to reach a balance between privacy protection and address update cost. Due to the limited space that IPv4 contains, such approach usually works for IPv6 only.

Private Address Spaces: The introduction of private addresses (assigned to specific address spaces by IANA) allowed to communicate purely locally, e.g., within an enterprise, by separating private from public IP addresses ([RFC1597], [RFC1918]). Considering that private addresses are never directly reachable from the Internet, hosts adopting private addresses are invisible and thus 'anonymous' for the Internet. Besides, hosts for purely local communication used the latter while hosts requiring public Internet service access would still use public IP addresses.

Address Translation: The aforementioned original intention for using private IP addresses, namely for purely local communication, resulted in a lack of flexibility in changing from local to public Internet access on the basis of what application would require which type of service.

If eventually every end-system in an organization would require some form of public Internet access in addition to local one, an adequate number of public Internet addresses would be required. Instead, address translation enables to utilize many private IP addresses within an organization, while only relying on one (or few) public IP addresses for the overall organization.

In principle, address translation can be applied recursively. This can be seen in modern broadband access where some Internet providers rely on carrier-grade address translation for all their broadband customers, who in turn employ address translation of their internal home or office addresses to those (private again) IP addresses assigned to them by their network provider.

Two benefits arise from the use of (private to public IP) address translation, namely (i) the hiding of local end systems at the level of the (address) assigned organization (e.g. in [GNATCATCHER]), and (ii) the reduction of public IP addresses necessary for communication across the Internet. While the latter has been seen for long as a driver for address translation, here, we focus on the first one.

Separate device from locator identifier: Solutions that make a clear separation between the routing locator and the identifier, allow a device ID of any size, which in turn can be encrypted by a network element deployed at the border of routing domain (e.g., access/ edge router). Both source and end-domain addresses are encrypted and transported, as in the routing domain, only the routing locator is used.

### 5.2.2. Authenticated Address Identity

#### 5.2.2.1. Description

In some scenarios (e.g., corporate networks or [RFC7039]) it is desirable to being able authenticate IP addresses in order to prevent malicious attackers spoofing IP addresses. This is usually achieved by using a mechanism that allows to prove ownership of the IP address. Another growing use case where identity verification is necessary for security and safety reasons is in the aeronautical context, for both manned and unmanned aerial vehicles ([RFC9153], [I-D.haindl-lisp-gb-atn]).

#### 5.2.2.2. Methodology

Self-certified addresses: This method is usually based on the use of public/private keys. A node creates its own interface ID (IID) by using a cryptographic hash of its public key (with some additional parameters). Messages are then signed using the nodes' private key. The destination of the message will verify the signature through the information in the IP address. Self-certification has the advantage that no third party or additional security infrastructure is needed. Any node can generate its own address locally and then only the address and the public key are needed for verification.

Collision-resistant addresses: When self-certification cannot be used, an alternative approach is to generate addresses in a way that is statistically unique (collision-resistant). Authentication of the address then occurs in an out-of-band protocol, where the unique identifier is resolved to authenticating information.

Third party granted addresses: DHCP (Dynamic Host Configuration Protocol) is widely used to provide IP addresses, however, in its basic form, it does not perform any check and even an unauthorized user without the right to use the network can obtain an IP address. To solve this problem, a trusted third party has to grant access to the network before generating an address (via DHCP or other) that identifies the user. User authentication done securely either based on physical parameters like MAC addresses or based on an explicit login/password mechanism.

### 5.2.3. Examples

Table 3, summarize the methodologies and lists examples of identity extensions.

| | Methodology | Examples |
|---|---|---|
| Anonymous Address Identity | Traffic Proxy | VPN, TOR, ODoH, oHTTP |
| | Source Address Rollover | SLAAC |
| | Private Address Spaces | ULA |
| | Address Translation | NAT |
| | Separate device from locator identifier | EIBP, LISP |
| Authenticated Address Identity | Self-certified Addresses | CGA |
| | Third party granted addresses | DHCP-Option |

Table 3: Identity Extensions Summary

## 5.3. Semantic Extensions

Extensions in this section relate to the property described in Section 3.3, i.e., limited address semantic support.

As explained in Section 3.2, IP addresses carry both locator and identification semantic. Some efforts exist that try to separate these semantics either in different address spaces or through different address formats. Beyond just identification, location, and the fixed address size, other efforts extended the semantic through existing or additional header fields (or header options) outside the Internet address.

How much unique and globally routable an address should be? With the effect of centralization, edges communicate with (rather) local DCs, hence a unique address globally routable is not a requirement anymore. There is no need to use globally unique addresses all the time for communication, however, there is the need of having a unique address as a general way to communicate to any connected entity without caring what transmission networks the packets traverse.

### 5.3.1. Extended Address Semantics

#### 5.3.1.1. Description

Several extensions have been developed to extend beyond the limited IPv6 semantics. Those approaches include the definition of structure to the address, utilize specific prefixes, or entirely utilize the IPv6 address for different semantics, while re-encapsulating the original packet to restore the semantics in another part of the network. For instance, structured addresses have the capability to introduce delimiters to identify semantic information in the header, therefore not constraining any semantic by size limitations of the address fields.

We note here that extensions often start out as being proposed as an extended header semantic, while standardization drives the solution to adopt an approach to accommodate their semantic within the limitations of an IP address. This section does include examples of this kind.

#### 5.3.1.2. Methodology

Semantic prefixes: Semantic prefixes are used to separate the IPv6 address space. Through this, new address families, such as for information-centric networking [CAROFIGLIO19], service routing or other semantically rich addressing, can be defined, albeit limited by the prefix length and structure as well as the overall length limitation of the IPv6 address.

Separate device/resource from locator identifier: The option to use separate namespaces for the device address would offer more freedom for the use of different semantics. For instance, the static binding of IP addresses to servers creates a strong binding between IP addresses and service/resources, which is a limitation for large Content Distribution networks (CDNs) [FAYED21].

As an extreme form of separating resource from locator identifier, recent engineering approaches, described in [FAYED21], decouple web service (semantics) from the routing address assignments by using virtual hosting capabilities, thereby effectively mapping possibly millions of services onto a single IP address.

Structured addressing: One approach to address the routing challenges faced in the Internet is the use of structured addresses, e.g., to void the need for routing protocols. Benefits of this approach are significant, with the structured addresses capturing the relative physical or virtual position of routers in the network as well as being variable in length. Key to the

approach, however, is that the structured addresses capturing the relative physical or virtual position of routers in the network, or networks in an internetwork, may end up not fitting within the fixed and limited IP address length (cf., Section 5.1.2).

Localized forwarding semantics: Layer 2 hardware, such as SDN switches, are limited to the use of specific header fields for forwarding decisions. Hence, devising new localized forwarding mechanisms may be based on re-using differently existing header fields, such as the IPv6 source/destination fields, to achieve the desired forwarding behavior, while encapsulating the original packets in order to be restored at the local forwarding network boundary. Networks in those solutions are limited by the size of the utilized address field, e.g., 256 bits for IPv6, thereby limiting the way such techniques could be used.

### 5.3.2. Existing or Extended Header Semantics

#### 5.3.2.1. Description

While the former section explored extended address semantic, thereby limiting any such extended semantic with that of the existing IPv6 semantic and length, additional semantics are also placed into the header of the packet or the packet itself, utilized for the forwarding decision to the appropriate endpoint according to the extended semantic.

Reasons for embedding such new semantics is related to traffic engineering since it has long been shown that the IP address itself is not enough to steer traffic properly since the IP address itself is not semantically rich enough to adequately describe the forwarding decision to be taken in the network, not only impacting "where" the packet will need to go, but also "how" it will need to be sent.

#### 5.3.2.2. Methodology

In-Header extensions: One way to add additional semantics besides the address fields is to use other fields already present in the header.

Headers option extensions: Another mechanism to add additional semantics is to actually add additional fields, e.g., through Header Options in IPv4 or through Extension Headers in IPv6.

Re-encapsulation extension: A more radical approach for additional semantics is the use of a completely new header that is designed so to carry the desired semantics in an efficient manner (e.g., as a shim header).

Structured addressing: Similar to the methodology that structures addresses within the limitations of the IPv6 address length, outlined in the previous sections, structured addressing can also be applied within existing or extended header semantics, e.g., utilizing a dedicated (extension) header to carry the structured address information.

Localized forwarding semantics: This set of solutions applies capabilities of newer (programmable) forwarding technology, such as [BOSSHART14], to utilize any header information for a localized forwarding decision. This removes any limitation to use existing header or address information for embedding a new address semantic into the transferred packet.

### 5.3.3. Examples

Table 4, summarize the methodologies and lists examples of semantic extensions.

| | Methodology | Examples |
|---|---|---|
| Utilizing Extended Address Semantics | Semantic prefixes | HICN |
| | Separate device from locator identifier | EIBP, ILNP, LISP, HIP |
| | Structured addressing | EIBP, ILNP |
| | Localized forwarding semantics | REED |
| Utilizing Existing or Extended Header Semantics | In-Header extensions | DetNet |
| | Headers option extensions | SHIM6, SRv6, HIP |
| | Re-encapsulation extension | VxLAN, ICNIP |
| | Structured addressing | EIBP |
| | Localized forwarding semantics | REED |

Table 4: Semantic Extensions Summary

## 5.4. IP Addressing Extensions Overall Summary

The following Table 5 describes the objectives of the extensions discussed in this memo with respect to the properties of Internet addressing (Section 3). As summarized, extensions aim to extend one property of the Internet addressing, or extend other properties at the same time.

| | Length Extension | Identity Extension | Semantic Extension |
|---|---|---|---|
| 6LoWPAN ([RFC6282], [RFC7400], [BADENHOP15], [RFC8376], [RFC8724]) | x | | |

| | | | | |
|---|---|---|---|---|
| ROHC [RFC5795] | x | | | |
| EzIP [EZIP] | x | | | |
| TOR [TOR] | | x | | |
| ODoH [RFC9230], oHTTP [I-D.ietf-ohai-ohttp] | | x | | |
| SLAAC [RFC8981] | | x | | |
| CGA [RFC3972] | | x | x | |
| NAT [RFC3083] | x | x | | |
| HICN [CAROFIGLIO19] | | x | x | |
| ICNIP [ICNIP] | x | x | x | |
| CCNx names | x | x | x | |
| EIBP [SHENOY21] | x | x | x | |
| Geo addressing | x | | x | |
| REED [REED16] | x (with P4 [BOSSHART14]) | | x | |
| DetNet [DETNETWG] | | x | | |
| Mobile IP [RFC6275] | | | x | |
| SHIM6 [RFC5533] | | | x | |
| SRv6 [RFC8402] | | | x | |
| HIP [RFC7401] | | x | x | |
| VxLAN [RFC7348] | | x | x | |
| LISP ([RFC9300], [RFC8060]) | | x | x | |
| SFC [RFC7665] | | x | x | |

Table 5: Relationship between Extensions and Internet Addressing

Properties

## 6. Concerns Raised by IP Addressing Extensions

While the extensions to the original Internet properties, discussed in Section 5, demonstrate that flexibility in the addressing model is desirable in certain circumstances, they also raise a number of concerns, which are discussed in the following sections. To this end, the problems outlined hereafter link to the approaches to extensions summarized in Section 5.4. These considerations are not present all the time and everywhere, since extensions are developed and deployed in different part of the Internet, which may worsen things.

### 6.1. Limiting Address Semantics

Many approaches changing the semantics of communication, e.g., through separating host identification from network node identification [RFC7401], separating the device identifier from the routing locator ([SHENOY21], [RFC9299]), or through identifying content and services directly [CAROFIGLIO19], are limited by the existing packet size and semantic constraints of IPv6, e.g., in the form of its source and destination network addresses.

While approaches such as ICNIP [I-D.trossen-icnrg-internet-icn-5glan] overrides the addressing semantics, e.g., by replacing IPv6 source and destination information with path identification, a possible unawareness of endpoints still requires the carrying of other address information as part of the payload, through a procedure that always provides the addressing information in the address fields to those non-participants.

Other approaches, like for instance [CAROFIGLIO19] and [REED16], use an hybrid approach preserving the existing addressing fields, while using them in a different way, but the limited number of available bits limits the benefits introduced by these proposals.

### 6.2. Complexity and Efficiency

Realizing the additional addressing semantics introduces additional complexity. This is particularly a concern since those additional semantics are observed particularly at the edge of the Internet, utilizing the existing addressing semantic of the Internet to interconnect the domains that require those additional semantics.

Furthermore, any additional complexity comes with an efficiency and/or cost penalty, particularly at the edge of the network, where resource constraints play a significant role. Compression processes,

taking [FITZEK05] as an example, require additional resources both for the sender generating the compressed header but also the gateway linking to the general Internet by re-establishing the full IP header.

Conversely, the performance requirements of core networks, in terms of packet processing speed, makes the accommodation of extensions to addressing not possible. This is not only due to the necessary extra processing that is specific to the extension, but also due to the complexity that will need to be managed in doing so at significantly higher speeds than at the edge of the network. The observations on the dropping of packets with IPv6 extension headers in the real world is (partially) due to such an implementation complexity [RFC7872].

Another example for lowering the efficiency of packet forwarding is the routing in systems like Tor [TOR]. Traffic in Tor, for anonymity purposes, should be handed over by at least three intermediates before reaching the destination. Frequent relaying enhances the privacy [CHAUM81], however, because such kind of solutions are implemented at application level, they come at the cost of lower communication efficiency. A different privacy enhanced address semantic enables efficient implementation of Tor-like solutions at network layer.

Repetitive Encapsulation: Repetitive encapsulation is a concern since it bloats the packets size due to additional encapsulation headers. Addressing proposals such as those in [I-D.trossen-icnrg-internet-icn-5glan] utilize path identification within an alternative forwarding architecture that acts upon the provided path identification. However, due to the limitation of existing flow-based architectures with respect to the supported header structures (in the form of IPv4 or IPv6 headers), the new routing semantics are being inserted into the existing header structure, while repeating the original, sender-generated header structure, in the payload of the packet as it traverses the local domain, effectively doubling the per-packet header overhead.

The problem is also present in a number of solutions tackling different use cases, e.g., mobility [I-D.ietf-lisp-mn], data center networking ([RFC8926], [RFC7348], [I-D.ietf-intarea-gue]), traffic engineering [RFC8986], and privacy ([TOR], [DANEZIS09]). Certainly, these solutions are able to avoid issues like path lengthening or privacy concerns, as described before, but they come at the price of multiple encapsulations that reduce the effective payload. This, not only hampers efficiency in terms of header-to-payload ratio, but also introduces 'encapsulation points', which in turn add complexity to the (edge) network as well as fragility due to the addition of possible failure points; this aspect is discussed in further details in Section 6.4.

Compounding Concerns with Header Compression: IP header overhead requires header compression in constrained environments, such as wireless sensor networks and IoT in general. Together with fragmentation, both tasks constitute significant energy consumption, as shown in [MESRINEJAD11], negatively impacting resource limited devices, especially those that rely on battery for operation. Further, the reliance on the compression/ decompression points creates a dependence on such gateways, which is a problem for intermittent scenarios.

According to [AYERS20] the implementation of the 6LowPAN protocol stack requires, once compiled, between 6.2 and 26.6 Kilobytes (Kb), depending on the implementation and supported features. On extremely constrained devices, contiki-ng [CONTIKI], is the best choice because of its very small size (only 6.2 Kb), however, it offers less features.

Introducing Path Stretch: Mobile IP [RFC6275], which was designed for connection continuity in the face of moving endpoints, is a typical case for path stretch. Since traffic must follow a triangular route before arriving at the destination, such detour routing inevitably impacts transmission efficiency as well as latency. Mobile IP is not the only technology introducing path stretch. Privacy preserving protocols like Tor, but also more classic VPNs introduce path stretch.

Complicating Traffic Engineering: While many extensions to the original IP address semantic target to enrich the decisions that can be taken to steer traffic, according to requirements like QoS, mobility, chaining, compute/network metrics, flow treatment, path usage, etc., the realization of the mechanisms as individual solutions complicates the original goal of traffic engineering when individual solutions are being used in combination. Ultimately, this may even prevent the combined use of more than one mechanism and/or policy with a need to identify and prevent

incompatibilities of mechanisms. Key here is not the concerns arising from using conflicting traffic engineering policies, rather conflicting realizations of policies that should generally work well alongside ([CANINI15], [CURIC18]).

This not only increases fragility, as discussed separately in Section 6.4, but also requires careful planning of which mechanisms to use and in which combination, needing human-in-the-loop approaches alongside possible automation approaches for the individual solutions.

## 6.3. Security

The properties described in Section 5 have, obviously, also consequences in terms of security and privacy related concerns, as already mentioned in other parts of this document.

For instance, in the effort of being somehow backward compatible, HIP [RFC7401] uses a 128-bit Host Identity, which will be not sufficiently cryptographically strong in the future, because of the limited size (future computational power will erode 128-bit security). Similarly, CGA [RFC3972] also aligns to the 128-bit limit, but uses only 59 bits of them, hence, the packet signature is not sufficiently robust to attacks [I-D.rafiee-6man-cga-attack].

IP addresses, even temporary ones meant to protect privacy, have been long recognized as a 'Personal Identification Information' that allows even to geolocate the communicating endpoints [RFC8280]. Depending on the renewal rate, some issues arise, like the large overhead due to the Duplicate Address Detection, the impact on the Neighbor Discovery mechanism, in particular the cache, potentially leading to communication disruption. With such drawbacks, the extensions defeat their target, actually lowering security rather than increasing it.

The introduction of alternative addressing semantics has also been used to help in (D)DoS attacks mitigation. This leverages on changing the service identification model so to avoid topological information exposure, making the potential disruptions remain limited [HAO21]. However, this increased robustness for ongoing communications to DDoS on the servers comes at the price of important communication setup latency and fragility, as discussed next.

### 6.4. Fragility

From the extensions discussed in Section 5, it is evident that having alternative or additional address semantic and formats available for making routing as well as forwarding decisions dependent on these, is common place in the Internet. This, however, adds many extension-specific translation/adaptation points, mapping the semantic and format in one context into what is meaningful in another context, but also, more importantly, creating a dependency towards an additional component without explicit exposure to the endpoints that originally intended to communicate.

For instance, the re-writing of IP addresses to facilitate the use of private address spaces throughout the public Internet, realized through network address translators (NATs), conflicts with the end-to-end nature of communication between two endpoints. Additional (flow) state is required at the NAT middle-box to smoothly allow communication, which in turn creates a dependency between the NAT and the end-to-end communication between those endpoints, thus increasing the fragility of the communication relation.

A similar situation arises when supporting constrained environments through a header compression mechanism, adding the need for, e.g., a ROHC [RFC5795] element in the communication path, with communication-related compression state being held outside the communicating endpoints. Failure will introduce some inefficiencies due to context regeneration, which will affect the communicating endpoints, increasing fragility of the system overall.

Such translation/adaptation between semantic extensions to the original 'semantic' of an IP address is generally not avoidable when accommodating more than a single universal semantic. However, the solution-specific nature of every single extension risk to noticeably increase the fragility of the overall system, since individual extensions will need to interact with other extensions that are deployed in parallel, but were not designed taking into account such deployment scenario (cf., [I-D.ietf-intarea-tunnels]). Considering that extensions to traditional per-hop-behavior (based on IP addresses) can essentially be realized over almost 'any' packet field, the possible number of conflicting behaviors or diverging interpretation of the semantic and/or content of such fields, among different extensions, will at some point become an issue, requiring careful testing and delineation at the boundaries of the network within which the specific extension has been realized.

## 6.5. Summary of Concerns

Table 6, derived from the previous sections, summarizes the concerns discussed in this section related to each extension listed in Section 5.4. While each extension involves at least one concern, some others, like ICNIP [I-D.trossen-icnrg-internet-icn-5glan], create several at the same time.

| | Limiting Address Semantics | Complexity and Efficiency | Security | Fragility |
|---|---|---|---|---|
| 6LoWPAN | | x | | x |
| ROHC | | x | | x |
| EzIP | | x | | |
| TOR | | x | | x |
| ODoH | | x | | |
| oHTTP | | x | | |
| SLAAC | | x | | |
| CGA | x | | x | |
| NAT | | x | | x |
| HICN | x | | | |
| ICNIP | x | x | | |
| CCNx name | x | | | |
| EIBP | | | | x |
| Geo addressing | x | | | x |
| REED | x | | | |
| DetNet | | x | | |
| Mobile IP | | x | | x |

| | | | | | |
|---|---|---|---|---|---|
| SRv6 | | x | | | x |
| HIP | | | x | | x |
| VxLAN | | x | | | |
| LISP | | x | | | x |
| SFC | | x | | | x |

Table 6: Concerns in Extensions to Internet Addressing

## 7. Discussion

The examples of extensions discussed in Section 5 to the original Internet addressing scheme show that extensibility beyond the original model (and its underlying per-hop behavior) is a desired capability for networking technologies and has been so for a long time. Generally, we can observe that those extensions are driven by the requirements of stakeholders, derived from the aforementioned problems and communication scenarios, thus, expecting a desirable extended functionality from the introduction of the specific extension. If interoperability is required, those extensions require standardization of possibly new fields, new semantics as well as (network and/or end system) operations alike.

This points to the conclusion that the existence of the many extensions to the original Internet addressing is clear evidence for wanting to develop evolution paths over time by the wider Internet community, each of which come with a raft of issues that we need to deal with daily. This makes it desirable to develop an architectural and, more importantly, a sustainable approach to make Internet addressing extensible in order to capture the many new use cases that will still be identified for the Internet to come.

This is not to 'second guess' the market and its possible evolution, but to outline clear features from which to derive clear principles for a design. Any such design must not skew the technical capabilities of addressing to the current economic situation of the Internet and its technical realization, e.g., being a mere ephemeral token for accessing PoP-based services, since this bears the danger of locking down innovation capabilities as an outcome of those technical limitations introduced. Instead, addressing must be aligned with enabling the model of permissionless innovation that the IETF has been promoting, ultimately enabling the serendipity of new applications that has led to many of those applications currently deployed in the Internet.

Having a more systematic approach, rather than point extensions, would allow the Internet community to identify an overall evolutionary path able to accommodate existing and future use cases, without disruptive solutions breaking existing deployments, rather with a well-thought out set of incremental steps.

An architectural evolution of the IP addressing model allows bring clear benefits in various scenarios. Examples of such benefits are provided hereafter, for a short sample of use cases. An extensive discussion about these use cases can be found in Appendix B.

* Communication in Constrained Environments Potential Benefits: Avoid complex and energy hungry operations, like header compression and fragmentation, necessary to translate protocol headers from one limited domain to another, while enabling semantics different from locator-based addressing allows to better support the communication that occurs in those environments.

* Communication within Dynamically Changing Topologies Potential Benefits: Allow for accommodating such geographic address semantics into the overall Internet addressing, while also enabling name/content-based addressing, utilizing the redundancy of many network locations providing the possible data.

* Communication among Moving Endpoints Potential Benefits: Enable better mobility, e.g., through an augmented semantic that fulfils the mobility requirements [RFC7429] in a more efficient way or through moving from a locator- to a content or service-centric semantic for addressing.

* Communication Across Services Potential Benefits: Allow for incorporating different information, e.g., service as well as chaining semantics, into the overall Internet addressing.

* Communication Traffic Steering Potential Benefits: More semantic rich encoding schemes help in steering traffic at hardware level and speed, without complex mechanisms usually resulting in handling packets in the slow path of routers.

* Communication with built-in security Potential Benefits: Security-related key, certificate, or identifier could be included in a suitable address structure without any information loss, which weakens security and trust.

* Communication protecting user privacy Potential Benefits: Enable easy mechanism to obfuscate IP addresses to entities not involved in the communication.

* Communication in Alternative Forwarding Architectures Potential Benefits: Reduce the wastage by accommodating Internet addressing in the light of alternative forwarding architectures, instead enabling the direct use of the alternative forwarding information.

Finally, it is important to remark that any change in the addressing, hence at the data plane level, leads to changes and challenges at the control plane level, i.e., routing. The latter is an even harder problem than just addressing and might need more research efforts that are beyond what is discussed in this document, which focuses solely on the data plane.

## 8. Security Considerations

The present memo does not introduce any new technology and/or mechanism and as such does not introduce any new security threat to the TCP/IP protocol suite.

As an additional note, and as discussed in this document, security and privacy aspects were not considered as part of the key properties for Internet addressing, which led to the introduction of a number of extensions intending to fix those gaps. The analysis presented in this memo (non-exhaustively) shows those concerns are either solved in an ad-hoc manner at application level, or at transport layer, while at network level only few extensions tackling specific aspects exist, albeit with limitations due to the adherence to the Internet addressing model and its properties.

## 9. IANA Considerations

This document does not include any IANA request.

## Acknowledgments

Thanks to all the people that shared insightful comments both privately to the authors as well as on various mailing list, especially on the INTArea Mailing List. Thanks as well, for the interesting discussions, to Carsten Borman, Brian E. Carpenter, and Eric Vyncke. Thanks to Eliot Lear for his thorough review of this document.

## Informative References

[ABDALLAH16]
Abdallah, A., Abdallah, E., Bsoul, M., and A. Otoom, "Randomized geographic-based routing with nearly guaranteed delivery for three-dimensional ad hoc network", International Journal of Distributed Sensor Networks vol.

12, no. 10, pp. 155014771667125,
DOI 10.1177/1550147716671255, October 2016,
<https://doi.org/10.1177/1550147716671255>.

[ADACORSA] "Airborne data collection on resilient system architectures", n.d.,
<https://www.kdt-ju.europa.eu/projects/adacorsa>.

[ALMADANI20]
AL-Madani, B., Elkhider, S., and S. El-Ferik, "DDS-Based Containment Control of Multiple UAV Systems", Applied Sciences vol. 10, no. 13, pp. 4572,
DOI 10.3390/app10134572, July 2020,
<https://doi.org/10.3390/app10134572>.

[APPLEPRIV]
"Apple iCloud Private Relay", n.d.,
<https://www.apple.com/icloud/docs/iCloud_Private_Relay_Overview_Dec2021.pdf>.

[AYERS20] Ayers, H., Crews, P., Teo, H., McAvity, C., Levy, A., and P. Levis, "Design Considerations for Low Power Internet Protocols", 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS),
DOI 10.1109/dcoss49796.2020.00027, May 2020,
<https://doi.org/10.1109/dcoss49796.2020.00027>.

[BADENHOP15]
Badenhop, C., Fuller, J., Hall, J., Ramsey, B., and M. Rice, "Evaluating ITU-T G.9959 Based Wireless Systems Used in Critical Infrastructure Assets", IFIP Advances in Information and Communication Technology pp. 209-227,
DOI 10.1007/978-3-319-26567-4_13, 2015,
<https://doi.org/10.1007/978-3-319-26567-4_13>.

[BOSSHART14]
Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., and D. Walker, "P4: programming protocol-independent packet processors", ACM SIGCOMM Computer Communication Review vol. 44, no. 3, pp. 87-95,
DOI 10.1145/2656877.2656890, July 2014,
<https://doi.org/10.1145/2656877.2656890>.

[BUJLOW17] Bujlow, T., Carela-Espanol, V., Lee, B., and P. Barlet-Ros, "A Survey on Web Tracking: Mechanisms, Implications, and Defenses", Proceedings of the IEEE vol. 105, no. 8, pp. 1476-1510, DOI 10.1109/jproc.2016.2637878, August 2017, <https://doi.org/10.1109/jproc.2016.2637878>.

[CANINI15] Canini, M., Kuznetsov, P., Levin, D., and S. Schmid, "A distributed and robust SDN control plane for transactional network updates", 2015 IEEE Conference on Computer Communications (INFOCOM), DOI 10.1109/infocom.2015.7218382, April 2015, <https://doi.org/10.1109/infocom.2015.7218382>.

[CAROFIGLIO19] Carofiglio, G., Muscariello, L., Auge, J., Papalini, M., Sardara, M., and A. Compagno, "Enabling ICN in the Internet Protocol: Analysis and Evaluation of the Hybrid-ICN Architecture", Proceedings of the 6th ACM Conference on Information-Centric Networking, DOI 10.1145/3357150.3357394, September 2019, <https://doi.org/10.1145/3357150.3357394>.

[CCSDS-702.1-B-1] CCSDS - Consultative Committee for Space Data Systems, "IP over CCSDS Space Links", SIS Space Internetworking Services Area, n.d., <https://public.ccsds.org/Pubs/702x1b1c1.pdf>.

[CHAUM81] Chaum, D., "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM vol. 24, no. 2, pp. 84-90, DOI 10.1145/358549.358563, February 1981, <https://doi.org/10.1145/358549.358563>.

[CHEN21] Chen, Y., Li, H., Liu, J., Wu, Q., and Z. Lai, "GAMS: An IP Address Management Mechanism in Satellite Mega-constellation Networks", 2021 International Wireless Communications and Mobile Computing (IWCMC), DOI 10.1109/iwcmc51323.2021.9498722, June 2021, <https://doi.org/10.1109/iwcmc51323.2021.9498722>.

[CHERITON00] Cheriton, D. R. and M. Gritter, "TRIAD - A Scalable Deployable NAT-based Internet Architecture", Technical Report , 2000, <https://www.scss.tcd.ie/hitesh.tewari/papers/triad.pdf>.

[CHRIKI19] Chriki, A., Touati, H., Snoussi, H., and F. Kamoun, "FANET: Communication, mobility models and security issues", Computer Networks vol. 163, pp. 106877, DOI 10.1016/j.comnet.2019.106877, November 2019, <https://doi.org/10.1016/j.comnet.2019.106877>.

[CISCO-IOE] Cisco, "The Internet of Everything", 2012, <https://www.cisco.com/c/dam/global/en_my/assets/ciscoinnovate/pdfs/IoE.pdf>.

[COMP4DRONES] "COMP4DRONES", n.d., <https://www.kdt-ju.europa.eu/projects/comp4drones>.

[CONTIKI] "Contiki-NG: The OS for Next Generation IoT Devices", n.d., <https://github.com/contiki-ng/contiki-ng>.

[CURIC18] Curic, M., Despotovic, Z., Hecker, A., and G. Carle, "Transactional Network Updates in SDN", 2018 European Conference on Networks and Communications (EuCNC), DOI 10.1109/eucnc.2018.8442793, June 2018, <https://doi.org/10.1109/eucnc.2018.8442793>.

[DANEZIS09] Danezis, G. and I. Goldberg, "Sphinx: A Compact and Provably Secure Mix Format", 2009 30th IEEE Symposium on Security and Privacy, DOI 10.1109/sp.2009.15, May 2009, <https://doi.org/10.1109/sp.2009.15>.

[DETNETWG] "Deterministic Networking (DetNet) Working Group", n.d., <https://datatracker.ietf.org/wg/detnet/about/>.

[DINRG] "Decentralized Internet Infrastructure - DINRG", n.d., <https://datatracker.ietf.org/rg/dinrg/about/>.

[DONENFELD17] Donenfeld, J., "WireGuard: Next Generation Kernel Network Tunnel", Proceedings 2017 Network and Distributed System Security Symposium, DOI 10.14722/ndss.2017.23160, 2017, <https://doi.org/10.14722/ndss.2017.23160>.

[ETSI-NIN] ETSI - European Telecommunication Standards Institute, "Non-IP Networking - NIN", n.d., <https://www.etsi.org/technologies/non-ip-networking>.

[EZIP] Chen, A., Ati, R. R., Karandikar, A., and D. Crowe, "Adaptive IPv4 Address Space", Work in Progress, Internet-Draft, draft-chen-ati-adaptive-ipv4-address-space-13, 13 June 2023, <https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space-13>.

[FAYED21] Fayed, M., Bauer, L., Giotsas, V., Kerola, S., Majkowski, M., Odintsov, P., Sitnicki, J., Chung, T., Levin, D., Mislove, A., Wood, C., and N. Sullivan, "The ties that un-bind: decoupling IP from web services and sockets for robust addressing agility at CDN-scale", Proceedings of the 2021 ACM SIGCOMM 2021 Conference, DOI 10.1145/3452296.3472922, August 2021, <https://doi.org/10.1145/3452296.3472922>.

[FINKHAUSER21] Finkhauser, J. and M. Larsen, "Reliable Command, Control and Communication Links for Unmanned Aircraft Systems: Towards compliance of commercial drones", Proceedings of the 2021 Drone Systems Engineering and Rapid Simulation and Performance Evaluation: Methods and Tools Proceedings, DOI 10.1145/3444950.3444954, January 2021, <https://doi.org/10.1145/3444950.3444954>.

[FITZEK05] Fitzek, F., Rein, S., Seeling, P., and M. Reisslein, "RObust Header Compression (ROHC) Performance for Multimedia Transmission over 3G/4G Wireless Networks", Wireless Personal Communications vol. 32, no. 1, pp. 23-41, DOI 10.1007/s11277-005-7733-2, January 2005, <https://doi.org/10.1007/s11277-005-7733-2>.

[GNATCATCHER] "Global Network Address Translation Combined with Audited and Trusted CDN or HTTP-Proxy Eliminating Reidentification", n.d., <https://github.com/bslassey/ip-blindness>.

[GOLDSCHLAG99] Goldschlag, D., Reed, M., and P. Syverson, "Onion routing", Communications of the ACM vol. 42, no. 2, pp. 39-41, DOI 10.1145/293411.293443, February 1999, <https://doi.org/10.1145/293411.293443>.

[HANDLEY18] Handley, M., "Delay is Not an Option: Low Latency Routing in Space", Proceedings of the 17th ACM Workshop on Hot Topics in Networks, DOI 10.1145/3286062.3286075, November 2018, <https://doi.org/10.1145/3286062.3286075>.

[HAO21] Hao, S., Liu, R., Weng, Z., Chang, D., Bao, C., and X. Li, "Addressless: A new internet server model to prevent network scanning", PLOS ONE vol. 16, no. 2, pp. e0246293, DOI 10.1371/journal.pone.0246293, February 2021, <https://doi.org/10.1371/journal.pone.0246293>.

[HISTORY127] "History of 127/8 as localhost/loopback addresses", n.d., <https://elists.isoc.org/pipermail/internet-history/2021-January/006920.html>.

[HUGHES03] Hughes, L., Shumon, K., and Y. Zhang, "Cartesian Ad Hoc Routing Protocols", Ad-Hoc, Mobile, and Wireless Networks pp. 287-292, DOI 10.1007/978-3-540-39611-6_27, 2003, <https://doi.org/10.1007/978-3-540-39611-6_27>.

[I-D.chen-ati-adaptive-ipv4-address-space] Chen, A., Ati, R. R., Karandikar, A., and D. Crowe, "Adaptive IPv4 Address Space", Work in Progress, Internet-Draft, draft-chen-ati-adaptive-ipv4-address-space-13, 13 June 2023, <https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-ipv4-address-space-13>.

[I-D.gont-v6ops-ipv6-addressing-considerations] Gont, F. and G. Gont, "IPv6 Addressing Considerations", Work in Progress, Internet-Draft, draft-gont-v6ops-ipv6-addressing-considerations-02, 1 June 2022, <https://datatracker.ietf.org/doc/html/draft-gont-v6ops-ipv6-addressing-considerations-02>.

[I-D.haindl-lisp-gb-atn] Haindl, B., Lindner, M., Moreno, V., Portoles-Comeras, M., Maino, F., and B. Venkatachalapathy, "Ground-Based LISP for the Aeronautical Telecommunications Network", Work in Progress, Internet-Draft, draft-haindl-lisp-gb-atn-09, 27 March 2023, <https://datatracker.ietf.org/doc/html/draft-haindl-lisp-gb-atn-09>.

[I-D.iannone-internet-addressing-considerations] Iannone, L., Trossen, D., Mendes, P., Shenoy, N., Toutain, L., Chen, A., Farinacci, D., Finkhauser, J., and Y. Jia, "Internet Addressing Considerations", Work in Progress, Internet-Draft, draft-iannone-internet-addressing-considerations-01, 5 September 2022, <https://datatracker.ietf.org/doc/html/draft-iannone-internet-addressing-considerations-01>.

[I-D.iannone-scenarios-problems-addressing]
Iannone, L., Trossen, D., Shenoy, N., Mendes, P., Eastlake, D. E., Liu, P., Farinacci, D., Finkhauser, J., and Y. Jia, "Challenging Scenarios and Problems in Internet Addressing", Work in Progress, Internet-Draft, draft-iannone-scenarios-problems-addressing-00, 5 September 2022, <https://datatracker.ietf.org/doc/html/draft-iannone-scenarios-problems-addressing-00>.

[I-D.ietf-bier-multicast-http-response]
Trossen, D., Rahman, A., Wang, C., and T. T. Eckert, "Applicability of BIER Multicast Overlay for Adaptive Streaming Services", Work in Progress, Internet-Draft, draft-ietf-bier-multicast-http-response-06, 10 July 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-multicast-http-response-06>.

[I-D.ietf-intarea-gue]
Herbert, T., Yong, L., and O. Zia, "Generic UDP Encapsulation", Work in Progress, Internet-Draft, draft-ietf-intarea-gue-09, 26 October 2019, <https://datatracker.ietf.org/doc/html/draft-ietf-intarea-gue-09>.

[I-D.ietf-intarea-tunnels]
Touch, J. D. and M. Townsley, "IP Tunnels in the Internet Architecture", Work in Progress, Internet-Draft, draft-ietf-intarea-tunnels-13, 26 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-intarea-tunnels-13>.

[I-D.ietf-lisp-mn]
Farinacci, D., Lewis, D., Meyer, D., and C. White, "LISP Mobile Node", Work in Progress, Internet-Draft, draft-ietf-lisp-mn-14, 23 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-mn-14>.

[I-D.ietf-lisp-nexagon]
Barkai, S., Fernandez-Ruiz, B., Tamir, R., Rodriguez-Natal, A., Maino, F., Cabellos-Aparicio, A., Paillisse, J., and D. Farinacci, "Network-Hexagons:Geolocation Mapping Network Based On H3 and LISP", Work in Progress, Internet-Draft, draft-ietf-lisp-nexagon-51, 5 August 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-lisp-nexagon-51>.

[I-D.ietf-ohai-ohttp]
Thomson, M. and C. A. Wood, "Oblivious HTTP", Work in Progress, Internet-Draft, draft-ietf-ohai-ohttp-10, 25 August 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-10>.

[I-D.irtf-icnrg-5gc-icn]
Ravindran, R., Suthar, P., Trossen, D., Wang, C., and G. White, "Enabling ICN in 3GPP's 5G NextGen Core Architecture", Work in Progress, Internet-Draft, draft-irtf-icnrg-5gc-icn-04, 10 January 2021, <https://datatracker.ietf.org/doc/html/draft-irtf-icnrg-5gc-icn-04>.

[I-D.irtf-pearg-ip-address-privacy-considerations-01]
Finkel, M., Lassey, B., Iannone, L., and B. Chen, "IP Address Privacy Considerations", Work in Progress, Internet-Draft, draft-irtf-pearg-ip-address-privacy-considerations-01, 23 October 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-pearg-ip-address-privacy-considerations-01>.

[I-D.rafiee-6man-cga-attack]
Rafiee and C. Meinel, "Possible Attack on Cryptographically Generated Addresses (CGA)", Work in Progress, Internet-Draft, draft-rafiee-6man-cga-attack-03, 8 May 2015, <https://datatracker.ietf.org/doc/html/draft-rafiee-6man-cga-attack-03>.

[I-D.templin-6man-aero]
Templin, F., "Automatic Extended Route Optimization (AERO)", Work in Progress, Internet-Draft, draft-templin-6man-aero-63, 12 October 2022, <https://datatracker.ietf.org/doc/html/draft-templin-6man-aero-63>.

[I-D.trossen-icnrg-internet-icn-5glan]
Trossen, D., Robitzsch, S., Essex, U., AL-Naday, M., and J. Riihijarvi, "Internet Services over ICN in 5G LAN Environments", Work in Progress, Internet-Draft, draft-trossen-icnrg-internet-icn-5glan-04, 1 October 2020, <https://datatracker.ietf.org/doc/html/draft-trossen-icnrg-internet-icn-5glan-04>.

[I-D.trossen-rtgwg-impact-of-dlts]
Trossen, D., Guzman, D., McBride, M., and X. Fan, "Impact of DLTs on Provider Networks", Work in Progress, Internet-Draft, draft-trossen-rtgwg-impact-of-dlts-02, 30 August 2022, <https://datatracker.ietf.org/doc/html/draft-trossen-rtgwg-impact-of-dlts-02>.

[ICNIP] Trossen, D., Robitzsch, S., Essex, U., AL-Naday, M., and J. Riihijarvi, "Internet Services over ICN in 5G LAN Environments", Work in Progress, Internet-Draft, draft-trossen-icnrg-internet-icn-5glan-04, 1 October 2020, <https://datatracker.ietf.org/doc/html/draft-trossen-icnrg-internet-icn-5glan-04>.

[IPv4pool] "IANA IPv4 Address Space Registry", n.d., <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>.

[JACOBSON09]
Jacobson, V., Smetters, D., Thornton, J., Plass, M., Briggs, N., and R. Braynard, "Networking named content", Proceedings of the 5th international conference on Emerging networking experiments and technologies, DOI 10.1145/1658939.1658941, December 2009, <https://doi.org/10.1145/1658939.1658941>.

[KHANVILKAR04]
Khanvilkar, S. and A. Khokhar, "Virtual private networks: an overview with performance evaluation", IEEE Communications Magazine vol. 42, no. 10, pp. 146-154, DOI 10.1109/mcom.2004.1341273, October 2004, <https://doi.org/10.1109/mcom.2004.1341273>.

[KOMORI02] Komori, T. and T. Saito, "The secure DHCP system with user authentication", 27th Annual IEEE Conference on Local Computer Networks, 2002. Proceedings. LCN 2002., DOI 10.1109/lcn.2002.1181774, August 2003, <https://doi.org/10.1109/lcn.2002.1181774>.

[KRAHENBUHL21]
Krahenbuhl, C., Legner, M., Bitterli, S., and A. Perrig, "Pervasive Internet-Wide Low-Latency Authentication", 2021 International Conference on Computer Communications and Networks (ICCCN), DOI 10.1109/icccn52240.2021.9522235, July 2021, <https://doi.org/10.1109/icccn52240.2021.9522235>.

[KUO95] Kuo, F., "The ALOHA System", ACM SIGCOMM Computer Communication Review vol. 25, no. 1, pp. 41-44, DOI 10.1145/205447.205451, January 1995, <https://doi.org/10.1145/205447.205451>.

[MAROJEVIC20] Marojevic, V., Guvenc, I., Dutta, R., Sichitiu, M., and B. Floyd, "Advanced Wireless for Unmanned Aerial Systems: 5G Standardization, Research Challenges, and AERPAW Architecture", IEEE Vehicular Technology Magazine vol. 15, no. 2, pp. 22-30, DOI 10.1109/mvt.2020.2979494, June 2020, <https://doi.org/10.1109/mvt.2020.2979494>.

[MESRINEJAD11] Mesrinejad, F., Hashim, F., Noordin, N., Rasid, M., and R. Abdullah, "The effect of fragmentation and header compression on IP-based sensor networks (6LoWPAN)", The 17th Asia Pacific Conference on Communications, DOI 10.1109/apcc.2011.6152926, October 2011, <https://doi.org/10.1109/apcc.2011.6152926>.

[MISHRA20] Mishra, V., Laperdrix, P., Vastel, A., Rudametkin, W., Rouvoy, R., and M. Lopatka, "Don't Count Me Out: On the Relevance of IP Address in the Tracking Ecosystem", Proceedings of The Web Conference 2020, DOI 10.1145/3366423.3380161, April 2020, <https://doi.org/10.1145/3366423.3380161>.

[OCADO] "Ocado Technology's robot warehouse a Hive of IoT innovation", n.d., <https://techmonitor.ai/tech-leaders/ocado-technology-robot-hive-innovation>.

[PANRG] "Path Aware Networking Research Group - PANRG", n.d., <https://datatracker.ietf.org/rg/panrg/about/>.

[REED16] Reed, M., Al-Naday, M., Thomos, N., Trossen, D., Petropoulos, G., and S. Spirou, "Stateless multicast switching in software defined networks", 2016 IEEE International Conference on Communications (ICC), DOI 10.1109/icc.2016.7511036, May 2016, <https://doi.org/10.1109/icc.2016.7511036>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/rfc/rfc791>.

[RFC1597] Rekhter, Y., Moskowitz, B., Karrenberg, D., and G. de Groot, "Address Allocation for Private Internets", RFC 1597, DOI 10.17487/RFC1597, March 1994, <https://www.rfc-editor.org/rfc/rfc1597>.

[RFC1621] Francis, P., "Pip Near-term Architecture", RFC 1621, DOI 10.17487/RFC1621, May 1994, <https://www.rfc-editor.org/rfc/rfc1621>.

[RFC1752] Bradner, S. and A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC 1752, DOI 10.17487/RFC1752, January 1995, <https://www.rfc-editor.org/rfc/rfc1752>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/rfc/rfc1918>.

[RFC2009] Imielinski, T. and J. Navas, "GPS-Based Addressing and Routing", RFC 2009, DOI 10.17487/RFC2009, November 1996, <https://www.rfc-editor.org/rfc/rfc2009>.

[RFC2101] Carpenter, B., Crowcroft, J., and Y. Rekhter, "IPv4 Address Behaviour Today", RFC 2101, DOI 10.17487/RFC2101, February 1997, <https://www.rfc-editor.org/rfc/rfc2101>.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/rfc/rfc2474>.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, DOI 10.17487/RFC2663, August 1999, <https://www.rfc-editor.org/rfc/rfc2663>.

[RFC2775] Carpenter, B., "Internet Transparency", RFC 2775, DOI 10.17487/RFC2775, February 2000, <https://www.rfc-editor.org/rfc/rfc2775>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/rfc/rfc2865>.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, DOI 10.17487/RFC3031, January 2001, <https://www.rfc-editor.org/rfc/rfc3031>.

[RFC3083] Woundy, R., "Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems", RFC 3083, DOI 10.17487/RFC3083, March 2001, <https://www.rfc-editor.org/rfc/rfc3083>.

[RFC3118] Droms, R., Ed. and W. Arbaugh, Ed., "Authentication for DHCP Messages", RFC 3118, DOI 10.17487/RFC3118, June 2001, <https://www.rfc-editor.org/rfc/rfc3118>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/rfc/rfc3972>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/rfc/rfc3986>.

[RFC4014] Droms, R. and J. Schnizlein, "Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option", RFC 4014, DOI 10.17487/RFC4014, February 2005, <https://www.rfc-editor.org/rfc/rfc4014>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/rfc/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/rfc/rfc4291>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/rfc/rfc4301>.

[RFC4581] Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format", RFC 4581, DOI 10.17487/RFC4581, October 2006, <https://www.rfc-editor.org/rfc/rfc4581>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <https://www.rfc-editor.org/rfc/rfc4919>.

[RFC4982] Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, DOI 10.17487/RFC4982, July 2007, <https://www.rfc-editor.org/rfc/rfc4982>.

[RFC5061] Stewart, R., Xie, Q., Tuexen, M., Maruyama, S., and M. Kozuka, "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, DOI 10.17487/RFC5061, September 2007, <https://www.rfc-editor.org/rfc/rfc5061>.

[RFC5177] Leung, K., Dommety, G., Narayanan, V., and A. Petrescu, "Network Mobility (NEMO) Extensions for Mobile IPv4", RFC 5177, DOI 10.17487/RFC5177, April 2008, <https://www.rfc-editor.org/rfc/rfc5177>.

[RFC5275] Turner, S., "CMS Symmetric Key Management and Distribution", RFC 5275, DOI 10.17487/RFC5275, June 2008, <https://www.rfc-editor.org/rfc/rfc5275>.

[RFC5517] HomChaudhuri, S. and M. Foschiano, "Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment", RFC 5517, DOI 10.17487/RFC5517, February 2010, <https://www.rfc-editor.org/rfc/rfc5517>.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, DOI 10.17487/RFC5533, June 2009, <https://www.rfc-editor.org/rfc/rfc5533>.

[RFC5795] Sandlund, K., Pelletier, G., and L. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, DOI 10.17487/RFC5795, March 2010, <https://www.rfc-editor.org/rfc/rfc5795>.

[RFC5944] Perkins, C., Ed., "IP Mobility Support for IPv4, Revised", RFC 5944, DOI 10.17487/RFC5944, November 2010, <https://www.rfc-editor.org/rfc/rfc5944>.

[RFC6158] DeKok, A., Ed. and G. Weber, "RADIUS Design Guidelines", BCP 158, RFC 6158, DOI 10.17487/RFC6158, March 2011, <https://www.rfc-editor.org/rfc/rfc6158>.

[RFC6182] Ford, A., Raiciu, C., Handley, M., Barre, S., and J. Iyengar, "Architectural Guidelines for Multipath TCP Development", RFC 6182, DOI 10.17487/RFC6182, March 2011, <https://www.rfc-editor.org/rfc/rfc6182>.

[RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, DOI 10.17487/RFC6250, May 2011, <https://www.rfc-editor.org/rfc/rfc6250>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/rfc/rfc6275>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/rfc/rfc6282>.

[RFC6626] Tsirtsis, G., Park, V., Narayanan, V., and K. Leung, "Dynamic Prefix Allocation for Network Mobility for Mobile IPv4 (NEMOv4)", RFC 6626, DOI 10.17487/RFC6626, May 2012, <https://www.rfc-editor.org/rfc/rfc6626>.

[RFC6740] Atkinson, RJ. and SN. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description", RFC 6740, DOI 10.17487/RFC6740, November 2012, <https://www.rfc-editor.org/rfc/rfc6740>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/rfc/rfc6973>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <https://www.rfc-editor.org/rfc/rfc7039>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/rfc/rfc7228>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/rfc/rfc7258>.

[RFC7343] Laganier, J. and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2)", RFC 7343, DOI 10.17487/RFC7343, September 2014, <https://www.rfc-editor.org/rfc/rfc7343>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/rfc/rfc7348>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/rfc/rfc7400>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/rfc/rfc7401>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <https://www.rfc-editor.org/rfc/rfc7426>.

[RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <https://www.rfc-editor.org/rfc/rfc7429>.

[RFC7476] Pentikousis, K., Ed., Ohlman, B., Corujo, D., Boggia, G., Tyson, G., Davies, E., Molinaro, A., and S. Eum, "Information-Centric Networking: Baseline Scenarios", RFC 7476, DOI 10.17487/RFC7476, March 2015, <https://www.rfc-editor.org/rfc/rfc7476>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/rfc/rfc7665>.

[RFC7687] Farrell, S., Wenning, R., Bos, B., Blanchet, M., and H. Tschofenig, "Report from the Strengthening the Internet (STRINT) Workshop", RFC 7687, DOI 10.17487/RFC7687, December 2015, <https://www.rfc-editor.org/rfc/rfc7687>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/rfc/rfc7872>.

[RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", RFC 8060, DOI 10.17487/RFC8060, February 2017, <https://www.rfc-editor.org/rfc/rfc8060>.

[RFC8061] Farinacci, D. and B. Weis, "Locator/ID Separation Protocol (LISP) Data-Plane Confidentiality", RFC 8061, DOI 10.17487/RFC8061, February 2017, <https://www.rfc-editor.org/rfc/rfc8061>.

[RFC8105] Mariager, P., Petersen, J., Ed., Shelby, Z., Van de Logt, M., and D. Barthel, "Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)", RFC 8105, DOI 10.17487/RFC8105, May 2017, <https://www.rfc-editor.org/rfc/rfc8105>.

[RFC8163] Lynn, K., Ed., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks", RFC 8163, DOI 10.17487/RFC8163, May 2017, <https://www.rfc-editor.org/rfc/rfc8163>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/rfc/rfc8200>.

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/rfc/rfc8280>.

[RFC8376] Farrell, S., Ed., "Low-Power Wide Area Network (LPWAN) Overview", RFC 8376, DOI 10.17487/RFC8376, May 2018, <https://www.rfc-editor.org/rfc/rfc8376>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/rfc/rfc8402>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/rfc/rfc8484>.

[RFC8595] Farrel, A., Bryant, S., and J. Drake, "An MPLS-Based Forwarding Plane for Service Function Chaining", RFC 8595, DOI 10.17487/RFC8595, June 2019, <https://www.rfc-editor.org/rfc/rfc8595>.

[RFC8609] Mosko, M., Solis, I., and C. Wood, "Content-Centric Networking (CCNx) Messages in TLV Format", RFC 8609, DOI 10.17487/RFC8609, July 2019, <https://www.rfc-editor.org/rfc/rfc8609>.

[RFC8677] Trossen, D., Purkayastha, D., and A. Rahman, "Name-Based Service Function Forwarder (nSFF) Component within a Service Function Chaining (SFC) Framework", RFC 8677, DOI 10.17487/RFC8677, November 2019, <https://www.rfc-editor.org/rfc/rfc8677>.

[RFC8724] Minaburo, A., Toutain, L., Gomez, C., Barthel, D., and JC. Zuniga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation", RFC 8724, DOI 10.17487/RFC8724, April 2020, <https://www.rfc-editor.org/rfc/rfc8724>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/rfc/rfc8754>.

[RFC8763] Rahman, A., Trossen, D., Kutscher, D., and R. Ravindran, "Deployment Considerations for Information-Centric Networking (ICN)", RFC 8763, DOI 10.17487/RFC8763, April 2020, <https://www.rfc-editor.org/rfc/rfc8763>.

[RFC8926] Gross, J., Ed., Ganga, I., Ed., and T. Sridhar, Ed., "Geneve: Generic Network Virtualization Encapsulation", RFC 8926, DOI 10.17487/RFC8926, November 2020, <https://www.rfc-editor.org/rfc/rfc8926>.

[RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <https://www.rfc-editor.org/rfc/rfc8928>.

[RFC8939] Varga, B., Ed., Farkas, J., Berger, L., Fedyk, D., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP", RFC 8939, DOI 10.17487/RFC8939, November 2020, <https://www.rfc-editor.org/rfc/rfc8939>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/rfc/rfc8981>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/rfc/rfc8986>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/rfc/rfc9000>.

[RFC9153] Card, S., Ed., Wiethuechter, A., Moskowitz, R., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Requirements and Terminology", RFC 9153, DOI 10.17487/RFC9153, February 2022, <https://www.rfc-editor.org/rfc/rfc9153>.

[RFC9230] Kinnear, E., McManus, P., Pauly, T., Verma, T., and C.A. Wood, "Oblivious DNS over HTTPS", RFC 9230, DOI 10.17487/RFC9230, June 2022, <https://www.rfc-editor.org/rfc/rfc9230>.

[RFC9268] Hinden, R. and G. Fairhurst, "IPv6 Minimum Path MTU Hop-by-Hop Option", RFC 9268, DOI 10.17487/RFC9268, August 2022, <https://www.rfc-editor.org/rfc/rfc9268>.

[RFC9299] Cabellos, A. and D. Saucez, Ed., "An Architectural Introduction to the Locator/ID Separation Protocol (LISP)", RFC 9299, DOI 10.17487/RFC9299, October 2022, <https://www.rfc-editor.org/rfc/rfc9299>.

[RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <https://www.rfc-editor.org/rfc/rfc9300>.

[RFC9301] Farinacci, D., Maino, F., Fuller, V., and A. Cabellos, Ed., "Locator/ID Separation Protocol (LISP) Control Plane", RFC 9301, DOI 10.17487/RFC9301, October 2022, <https://www.rfc-editor.org/rfc/rfc9301>.

[RFC9354] Hou, J., Liu, B., Hong, Y., Tang, X., and C. Perkins, "Transmission of IPv6 Packets over Power Line Communication (PLC) Networks", RFC 9354, DOI 10.17487/RFC9354, January 2023, <https://www.rfc-editor.org/rfc/rfc9354>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/rfc/rfc9374>.

[RFC9414] Gont, F. and I. Arce, "Unfortunate History of Transient Numeric Identifiers", RFC 9414, DOI 10.17487/RFC9414, July 2023, <https://www.rfc-editor.org/rfc/rfc9414>.

[RFC9428] Choi, Y., Ed., Hong, Y., and J. Youn, "Transmission of IPv6 Packets over Near Field Communication", RFC 9428, DOI 10.17487/RFC9428, July 2023, <https://www.rfc-editor.org/rfc/rfc9428>.

[RFC9434] Card, S., Wiethuechter, A., Moskowitz, R., Zhao, S., Ed., and A. Gurtov, "Drone Remote Identification Protocol (DRIP) Architecture", RFC 9434, DOI 10.17487/RFC9434, July 2023, <https://www.rfc-editor.org/rfc/rfc9434>.

[RFC9453] Hong, Y., Gomez, C., Choi, Y., Sangi, A., and S. Chakrabarti, "Applicability and Use Cases for IPv6 over Networks of Resource-constrained Nodes (6lo)", RFC 9453, DOI 10.17487/RFC9453, September 2023, <https://www.rfc-editor.org/rfc/rfc9453>.

[SHENOY21] Shenoy, N., Chandraiah, S., and P. Willis, "A Structured Approach to Routing in the Internet", 2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), DOI 10.1109/hpsr52026.2021.9481818, June 2021, <https://doi.org/10.1109/hpsr52026.2021.9481818>.

[SIDE112] IETF 112 Side Meetings, "Internet Addressing: problems and gap analysis", 2021, <https://trac.ietf.org/trac/ietf/meeting/wiki/112sidemeetings>.

[TERASTREAM]
"Deutsche Telekom tests TeraStream, the network of the future, in Croatia", n.d., <https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-tests-terastream-the-network-of-the-future-in-croatia-358444>.

[TOR] "The Tor Project", n.d., <https://www.torproject.org/>.

[TROSSEN10]
Trossen, D., Sarela, M., and K. Sollins, "Arguments for an information-centric internetworking architecture", ACM SIGCOMM Computer Communication Review vol. 40, no. 2, pp. 26-33, DOI 10.1145/1764873.1764878, April 2010, <https://doi.org/10.1145/1764873.1764878>.

[VOIGT17] Voigt, P. and A. von dem Bussche, "The EU General Data Protection Regulation (GDPR)", Springer International Publishing book, DOI 10.1007/978-3-319-57959-7, 2017, <https://doi.org/10.1007/978-3-319-57959-7>.

[WANG19] Wang, P., Zhang, J., Zhang, X., Yan, Z., Evans, B., and W. Wang, "Convergence of Satellite and Terrestrial Networks: A Comprehensive Survey", IEEE Access vol. 8, pp. 5550-5588, DOI 10.1109/access.2019.2963223, 2020, <https://doi.org/10.1109/access.2019.2963223>.

[WION19] Wion, A., Bouet, M., Iannone, L., and V. Conan, "Distributed Function Chaining with Anycast Routing", Proceedings of the 2019 ACM Symposium on SDN Research, DOI 10.1145/3314148.3314355, April 2019, <https://doi.org/10.1145/3314148.3314355>.

[YU22] Yu, Q., Liu, H., Xu, P., Li, J., Zhang, L., and H. Chen, "Next Generation Wireless Avionics Intra-Communications: Challenges and Research Topics", IEEE Wireless Communications pp. 1-21, DOI 10.1109/mwc.003.2200087, 2022, <https://doi.org/10.1109/mwc.003.2200087>.

## Appendix A. Desirable Networking Features

The present section outlines the general features that are desirable in a networked system at large, i.e., not specific to any application/usage. Such list is a "by-product" of the addressing discussion.

1. Always-On: The world is getting more and more connected, leading to being connected to the Internet, anywhere, by any technology (e.g., cable, fiber, or radio), even simultaneously, "all the time", and, most importantly, automatically (without any switch turning). However, when defining "all the time" there is a clear and important difference to be made between availability and reliability vs "desired usage". From an end user perspective, clearly the former is of importance, not necessarily leading to an "always on" system notion but instead "always-app-available", merely requiring the needed availability and reliability to realize the perception of being "always on" (e.g., for earthquake alerts), possibly complemented by app-specific methods to realize the "always on" perception (e.g., using local caching rather than communication over the network).

2. Transparency: Being agnostic with respect to local domains network protocols (Bluetooth, ZigBee, Thread, Airdrop, Airplay, or any others) is key to provide an easy and straightforward method for contacting people and devices without any knowledge of network issues, particularly those related to network-specific solutions. While having a flexible addressing model that accommodates a wide range of use cases is important, the centrality of the IP protocol remains key as a mean to provide global connectivity.

3. Multi-homing: Seamless multi-homing capability for the host is key to best use the connectivity options that is available to an end user, e.g., for increasing resilience in cases of failures of one available option. Protocols like LISP, SHIM6, QUIC, MPTCP, SCTP (to cite a few) have been successful at providing this capability in an incremental way, but too much of that capability is realized within the specific use case, making it hard to leverage across all applications. While today each transport protocol has its own way to perform multi-address discovery, the network layer should provide the multi-homing feature (e.g., SHIM6 can be used to discover all addresses on both ends), and then leave the address selection to the transport. With that, multi-address discovery remains a network feature exposed to the upper layers. This also means to update the Socket API (which may be actually the first thing to do), which does not necessarily mean to expose more network details to the applications, rather to be more address agnostic, yet, more expressive.

4. Mobility: A lot of work has been put in MobileIP ([RFC5944], [RFC6275]) to provide seamless and lossless communications for moving nodes (vehicle, satellites). However, it has never been widely deployed for several reasons, like complexity of the

protocol and the fact that the problem has also been tackled at higher layers, with applications resilient to address changes. However, similar to multi-homing, solving the problem at higher layers means that each and every transport protocol and application have their own way to deal with mobility, leading to similar observations as those for the previous multi-homing aspect.

5. Security and Privacy: The COVID-19 pandemic has boosted end users' desire to be protected and protect their privacy. The balance among privacy, security, and accountability is not simple to achieve. There exist different views on what those properties should be, however the network should provide the means to provide what is felt as the best trade-off for the specific use case.

6. Performance: While certainly desirable, "performance" is hard to define since it depends on the objectives of those building for but also paying for performance. Examples are (i) speed (shorter paths/direct communications), (ii) bandwidth (10petabit/s for a link), (iii) efficiency (less overlays/encapsulations), (iv) high efficacy or sustainability (avoid waste). From an addressing perspective, length/format/semantics that adapt to the specific use case (e.g. use short addresses for low power IoT, or, where needed, longer for addresses embedding certificates for strong authentication, authorization and accountability) contribute to the performance aspects that end users desire, such as reducing waste through not needed encapsulation or needed conversion at network boundaries.

7. Availability, Reliability, Predictability: These three properties are important to enable wide-range of services and applications according to the desired usage (cf. point 1).

8. Do not do harm: Access to the Internet is considered a human right [RFC8280]. Access to and expression through it should align with this core principle. This issue transcends through a variety of previously discussed 'features' that are desired, such as privacy, security but also availability and reliability. However, lifting the feature of network access onto a basic rights level also brings in the aspect of "do not do harm" through the use of the Internet with respect to wider societal objectives. Similar to other industries, such as electricity or cars, preventing harm usually requires an interplay of commercial, technological, and regulatory efforts, such as the enforcement of seat belt wearing to reduce accident mortality. As a first step, the potential harmfulness of a novel method must be recognized and weighted against the benefits of its

introduction and use. One increasingly important consideration in the technology domain is "sustainability" of resource usage for an end user's "consumption of" and "participation in" Internet services. As an example, Distributed Ledger Technologies (DLT) are seen as an important tool for a variety of applications, including Internet decentralization [DINRG]. However, the non-linear increase in energy consumption means that extending proof-of-work systems to the entire population of the planet would not only be impractical but also possibly highly wasteful, not just at the level of computation but also communication resource usage [I-D.trossen-rtgwg-impact-of-dlts]. This poses the question on how novel methods for addressing may improve on sustainability of such technologies, particularly if adopted more widely.

9. Maximum Transmission Unit (MTU): One long standing issue in the Internet is related to the MTU and how to discover the path MTU in order to avoid fragmentation ([RFC9268], [I-D.templin-6man-aero]). While it makes sense to always leverage as much performance from local systems as possible, this should come without sacrificing the ability to communicate with all systems. Having a solid solution to solve the issue would make the overall interconnection of systems more robust.

## Appendix B. IP Addressing Extensions driven by Use Cases

Over the years, a plethora of extensions has been proposed in order to move beyond the native properties of IP addresses. The development of those extensions are, in a certain way, attempts, in a limited scope, to go beyond the original properties of Internet addressing and desired new capabilities that those developing the extensions identified as being missing and yet needed and desirable.

The following sections provide a detailed and in-depth analysis of the use cases listed in Section 4 and how they relates to the shortcomings listed in that very same section.

### B.1. Communication in Constrained Environments

In the Internet of Things (IoT) scenario, a simple, communication network demanding minimal resources is required, allowing for a group of IoT network devices to form a network of constrained nodes, with the participating network and end nodes requiring as little computational power as possible and having small memory requirements. Furthermore, in the context of industrial IoT, real-time requirements and scalability make IP technology not naturally suitable as communication technology [OCADO].

The end-to-end principle [RFC2775] requires IP addresses to be used on such constrained nodes, allowing IoT devices to talk on the Internet. Given the constraints imposed on the computational and possibly also lower layer communication technology, the usage of a single addressing semantic in the form of a 128-bit endpoint identifier, i.e., IPv6 address, poses a challenge when operating such networks, e.g. because of limited Maximum Transmission Unit or to reduce power consumtion. As a consequence, devices located at the edge of constrained networks act as gateway performing header compression [RFC4919] or other forms of protocol adaptation ([RFC9453], [RFC8928], [RFC8724]).

Another type of (differently) constrained environment is an aircraft, which encompasses not only passenger communication but also the integration of real-time data exchange to ensure that processes and functions in the cabin are automatically monitored or actuated. The proposal for having an Wireless Avionics Intra-Communications (WAIC [YU22]) system promises reduction in the complexity of electrical wiring harness design and fabrication, reduction in wiring weight, increased configuration, and potential monitoring of otherwise inaccessible moving or rotating aircraft parts. Similar to the IoT concept, WAIC systems consist of short-range communications and are a potential candidate for passenger entertainment systems, smoke detectors, engine health monitors, tire pressure monitoring systems, and other kinds of aircraft maintenance systems. Most of the aircraft applications and services are focused on the data (e.g. temperature of gas tank on left wing) and not on the topological location of the data source. This means that the current topological location semantic of IP addresses is not beneficial for aircraft applications and services.

### B.2. Communication within Dynamically Changing Topologies

Communication may occur over networks that exhibit dynamically changing
topologies. One such example is that of satellite networks, providing global Internet connections through a combination of inter-satellite and ground station communication. With the convergence of space-based and terrestrial networks, users experience seamless broadband access, e.g., on cruise ships, flights, and within cars, seamlessly switching between Wi-Fi, cellular, or satellite based networks at any time [WANG19]. With large scale LEO (Low Earth Orbit) satellites, the involved topologies of the satellite network will be changing constantly while observing a regular flight pattern in relation to other satellites and predictable overflight patterns to ground users [CHEN21].

Although satellite bearer services are capable of transporting IPv4 and IPv6 [CCSDS-702.1-B-1], as well as associated protocols such as IP Multicast, DNS services, and routing information; no IP functionality is implemented on-board of the spacecraft, limiting the capability of leveraging for instance on large scale satellite constellations.

Moreover, due to the current IP addressing scheme and its focus on IP unicast addressing with extended deployment of IP multicast and some IP anycast, current deployments do not take advantage of the broadcast nature of satellite networks.

As a result of these constraints, the Consultative Committee for Space Data Systems (CCSDS) has produced its own communication standards distinct from those of the IETF. The conceptual model shares many similarities with the Open Systems Interconnection model, and individual CCSDS protocols address comparable concerns to those standardized by the IETF, but always under the distinct concerns that connectivity is intermittent, and while throughput rates is high, so is latency.

Concerning the vehicular networks use case, the communication includes Road Side Units (RSU) with the possibility to create ephemeral connections to those RSUs for the purpose of workload offloading, joint computation over multiple (vehicular) inputs, and other purposes [I-D.ietf-lisp-nexagon]. Communication here exhibits a multi-hop nature, not just involving the vehicle and the RSU over a direct link.

Those topologies are naturally changing constantly due to the dynamic nature of the involved communication nodes.

The advent of Flying Ad-hoc NETworks (FANETs) has opened up an opportunity to create new added-value services [CHRIKI19]. Due to high mobility of FANET nodes, the network topology changes more frequently than in a typical vehicular ad hoc network. From a routing point of view, although ad-hoc reactive and proactive routing approaches can be used, there are other type of routing protocols that have been developed for FANETS, such as hybrid routing protocols and position based routing protocols, aiming to increase efficiency in large scale networks with dynamic topologies.

Both type of protocols challenge the current Internet addressing semantic: in the case of hybrid protocols, two different routing strategies are used inside and outside a network zone. While inside a zone packets are routed to a specific destination IP address, between zones, query packets are routed to a subset of neighbors as determined by a broadcast algorithm. In the case of position based

routing protocol, the IP addressing scheme is not used at all, since packets are routed to a different identifier, corresponding to the geographic location of the destination and not its topological location. Hence, what is needed is to consolidate the geo-spatial addressing with that of a locator-based addressing in order to optimize routing policies across the zones.

In the aforementioned network technologies, there is a significant difference between the high dynamics of the underlying network topologies, compared to the relative static nature of terrestrial network topology, as reported in [HANDLEY18]. As a consequence, the notion of a topological network location becomes restrictive in the sense that not only the relation between network nodes and user endpoint may change, but also the relation between the nodes that form the network itself. This leads to the challenge of maintaining and updating the topological addresses in this constantly changing network topology.

In attempts to utilize entirely different semantics for the addressing itself, geographic-based routing, such as in [HUGHES03], has been proposed for MANETs (Mobile Ad-hoc NETworks) through providing geographic coordinates based addresses to achieve better routing performance, lower overhead, and lower latency [ABDALLAH16].

### B.3. Communication among Moving Endpoints

When packet switching was first introduced, back in the 60s/70s, it was intended to replace the rigid circuit switching with a communication infrastructure that was more resilient to failures. As such, the design never really considered communication endpoints as mobile. Even in the pioneering ALOHA [KUO95] system, despite considering wireless and satellite links, the network was considered static (with the exception of failures and satellites, which fall in what is discussed in Appendix B.2). Ever since, a lot of efforts have been devoted to overcome such limitations once it became clear that endpoint mobility will become a main (if not THE main) characteristic of ubiquitous communication systems.

The IETF has for a long time worked on solutions that would allow extending the IP layer with mobility support. Because of the topological semantic of IP addresses, endpoints need to change addresses each time they visit a different network. However, because routing and endpoint identification is also IP address based, this leads to communication disruption.

The lack of an efficient mobility management solution at network layer enabled the involvement of the transport layer in mobility solutions, either by introducing explicit in-band signaling to allow

for communicating IP address changes (e.g., in SCTP [RFC5061] and MPTCP [RFC6182]), or by introducing some form of connection ID that allows for identifying a communication independently from IP addresses (e.g., the connection ID used in QUIC [RFC9000]).

Concerning network layer only solutions, anchor-based Mobile IP mechanisms have been introduced in the past ([RFC5177], [RFC6626] [RFC5944], [RFC5275]). Mobile IP is based on a relatively complex and heavy mechanism that makes it hard to deploy and it is not very efficient. Furthermore, it is even less suitable than native IP in constrained environments like the ones discussed in Appendix B.1.

Some of the alternative approaches to Mobile IP leverage the introduction of some form of overlay. LISP [RFC9299], by separating the topological semantic from the identification semantic of IP addresses, is able to cope with endpoint mobility by dynamically mapping endpoint identifiers with routing locators [I-D.ietf-lisp-mn]. This comes at the price of an overlay that needs its own additional control plane [RFC9301].

Similarly, the NVO3 (Network Virtualization Overlays) Working Group, while focusing on Data Center environments, also explored an overlay-based solution for multi-tenancy purposes, but also resilient to mobility since relocating Virtual Machines (VMs) is common practice. NVO3 considered for a long time several data planes that implement slightly different flavors of overlays ([RFC8926], [RFC7348], [I-D.ietf-intarea-gue]), but lacks an efficient control plane specifically tailored for DCs.

Alternative mobility architectures have also been proposed in order to cope with endpoint mobility outside the IP layer itself. The Host Identity Protocol (HIP) [RFC7401] introduced a new namespace in order to identify endpoints, namely the Host Identity (HI), while leveraging the IP layer for topological location. On the one hand, such an approach needs to revise the way applications interact with the network layer, by modifying the DNS (now returning an HI instead of an IP address) and applications to use the HIP socket extension. On the other hand, early adopters do not necessarily gain any benefit unless all communicating endpoints upgrade to use HIP.

Another alternative approach is adopted by Information-Centric Networking (ICN) [RFC7476]. By making content a first class citizen of the communication architecture, the "what" rather than the "where" becomes the real focus of the communication. However, as explained in the next section, ICN can run either over the IP layer or completely replace it, which in turn can be seen as running the Internet and ICN as logically separated limited domains.

Unmanned Aircraft Systems (UAS) are another example of moving devices that require a stable mobility management scheme since they consist of a number of Unmanned Aerial Vehicles (UAV; or drones) subordinated to a Ground Control Station (GCS) [MAROJEVIC20]. There exist a variety of specialized UAVs that, although having redundant links to maintain communications in long-range missions (e.g., satellite), perform most of the communications with the GCS over wireless data links, e.g., based on a radio line-of-sight technology such as Wi-Fi or 3G/4G/5G. In particular, in Beyond Visual Line of Sight (BVLOS) operations, legal requirements include the use of multiple redundant radio links (even employing different radio bands), but still require unique identification of the vehicle. This implies that some resolution mechanism is required that securely resolves drone identifiers to link locators.

To this end, Drone Remote Identification Protocol [RFC9434] uses hierarchical DRIP Entity Tags, which are hierarchical versions of Host Identity Tags, and thus compatible with HIP [RFC7401]. DRIP does not mandate the use of HIP, but suggests its use in several places. Using the mobility extensions of HIP provides for one way to ensure secure identifier resolution.

In addition to such connectivity considerations, data-centric communication plays an increasing role, where information is named and decoupled from its location, and applications/services operate over these named data rather than on host-to-host communications.

In this context, the Data Distribution Service [ALMADANI20] has emerged as an industry-oriented open standard. The space and time decoupling allowed by DDS is very relevant in any dynamic and distributed system, since interacting entities are not forced to know each other and are not forced to be simultaneously present to exchange data. Time decoupling significantly simplifies the management of intermittent data-links, in particular for wireless connectivity between UAS. This model of communication, in turn, questions the locator-based addressing used in IP using instead a data-centric naming.

When it comes to link reliability, this translates into an end-point selection problem, as multiple underlying links are available, but the determination of the "best" link depends on specific radio characteristics [FINKHAUSER21] or even the vehicle's spatial location.

Scenarios from research projects such as [COMP4DRONES] and [ADACORSA] regarding connectivity assume worse conditions. Consider an emergency scenario in which 3GPP towers are inoperable. Emergency services need to deploy a mobile ground control station that issues

emergency landing overrides to all UAV in the area. UAV must be able to authenticate this mobile GCS to prevent malicious interference with their opreations, but must be able to do so without access to internet-connected authentication databases. HIP provides a means to secure communications to this mobile GCS, with no means for establishing its authority. While such considerations are not directly part of the mechanism by which identifiers are mapped to locators, they illustrate the need for carrying authenticating and authorizing information within identifiers.

Mobility management solutions increase the complexity of the deployment impacting the performance of data distribution, both in terms of signaling/data overhead and communication path delay. Considering the specific case of multicast data streams, mobility of content producers and consumers is inherently handled by multicast routing protocols, which are able to react to changes of location of mobile nodes by reconstructing the corresponding multicast delivery trees. Nevertheless, this comes with a cost in terms of signaling and data overhead (data may still flow through branches of a multicast delivery tree where there are no receivers while the routing protocol is still converging).

Another alternative is to perform the mobility management of producers and consumers not at the application layer based on IP multicast trees, but on the network layer based on an Information Centric Network approach, which was already mentioned in this section.

### B.4. Communication Across Services

As a communication infrastructure spanning many facets of life, the Internet integrates services and resources from various aspects such as remote collaboration, shopping, content production as well as delivery, education, and many more. Accessing those services and resources directly through URIs has been proposed by methods such as those defined in ICN [RFC7476]. Users access required services and resources by virtue of using the URI-based identification, with an ephemeral relationship built between user and provider, while the building of such relationship may be constrained with user- as well as service-specific requirements, such as proximity (finding nearest provider), load (finding fastest provider), and others.

While systems like ICN [JACOBSON09] provide an alternative to the topological addressing of IP, its deployment requires an overlay (over IP) or native deployment (alongside IP), the latter with dedicated gateways needed for translation. Underlay deployments are also envisioned in [RFC8763], where ICN solutions are being used to facilitate communication between IP addressed network endpoints or

URI-based service endpoints, still requiring gateway solutions for interconnection with ICN-based networks as well as IP routing based networks (cf., [I-D.irtf-icnrg-5gc-icn][I-D.trossen-icnrg-internet-icn-5glan]).

Another aspect of communication across services is that of chaining individual services to a larger service. Here, an identifier would be used that serves as a link to next hop destination within the chain of single services, as done in the work on Service Function Chaining (SFC). With this, services are identified at the level of Layer 2/3 ([RFC7665], [RFC8754], [RFC8595]) or at the level of name-based service identifiers like URLs [RFC8677] although the service chain identification is carried as a Network Service header (NSH) [RFC7665], separate to the packet identifiers. The forwarding with the chain of services utilizes individual locator-based IP addressing (for L3 chaining) to communicate the chained operations from one Service Function Forwarder [RFC7665] to another, leading to concerns regarding overhead incurred through the stacking of those chained identifiers in terms of packet overhead and therefore efficiency in handling in the intermediary nodes.

### B.5. Communication Traffic Steering

Steering traffic within a communication scenario involves at least two aspects, namely (i) limiting certain traffic towards a certain set of communication nodes and (ii) restraining the sending of packets towards a given destination (or a chain of destinations) with metrics that would allow the selection among one or more possible destinations.

One possibility for limiting traffic inside limited domains, towards specific objects, e.g., devices, users, or group of them, is subnet partition with techniques such as VLAN [RFC5517], VxLAN [RFC7348], or more evolved solution like TeraStream [TERASTREAM] realizing such partitioning. Such mechanisms usually involve significant configuration, and even small changes in network and user nodes could result in a repartition and possibly additional configuration efforts. Another key aspect is the complete lack of correlation of the topological address and any more semantic-rich identification that could be used to make policy decisions regarding traffic steering. Suitably enriching the semantics of the packet address, either that of the sender or receiver, so that such decision could be made while minimizing the involvement of higher layer mechanisms, is a crucial challenge for improving on network operations and speed of such limited domain traffic.

When making decisions to select one out of a set of possible destinations for a packet, IP anycast semantics is applied albeit being limited to the locator semantic of the IP address itself. Recent work in [WION19] suggests utilizing the notion of IP anycast address to encode a "service identifier", which is dynamically mapped onto network locations where service instances fulfilling the service request are located. Scenarios where this capability is utilized are provided in [WION19] and include, but are not limited to, scenarios such as edge-assisted VR/AR, transportation, smart cities, smart homes, smart wearables, and digital twins.

The challenge here lies in the possible encoding of not only the service information itself, but the constraint information that helps the selection of the "best" service instance, which is a service-specific constraint in relation to the particular scenario. The notion of an address here is a conditional (on those constraints) one where this conditional part is an essential aspect of the forwarding action to be taken. It needs therefore consideration in the definition of what an address is, what is its semantic, and how the address structure ought to look like.

As outlined in the previous section, chaining services are another aspect of steering traffic along a chain of constituent services, where the chain is identified through either a stack of individual identifiers, such as in Segment Routing [RFC8402], or as an identifier that serves as a link to next hop destination within the chain, such as in Service Function Chaining (SFC). The latter can be applied to services identified at the level of Layer 2/3 ([RFC7665], [RFC8754], [RFC8595]) or at the level of name-based service identifiers like URLs [RFC8677]. However, the overhead incurred through the stacking of those chained identifiers is a concern in terms of packet overhead and therefore efficiency in handling in the intermediary nodes.

### B.6. Communication with built-in security

Today, strong security in the Internet is usually implemented as a general network service ([KRAHENBUHL21], [RFC6158]). Among the various reasons for such approach is the limited semantic of current IP addresses, which do not allow to natively express security features or trust relationships. In specific contexts strong identification and tracking is necessary for safety and security purposes, like for instance for UAS [RFC9153] or aeronautical telecommunications networks [I-D.haindl-lisp-gb-atn]. This becomes very cumbersome when communication goes beyond limited domains and in the public Internet, where security and trust associated to those identifier is lost or just impossible to verify.

Efforts like Cryptographically Generated Addresses (CGA) [RFC3972], provide some security features by embedding a truncated public key in the last 57-bit of IPv6 address, thereby greatly enhancing authentication and security within an IP network via asymmetric cryptography (known to be not as efficient as symmetric ecryptography) and IPsec [RFC4301]. The development of the Host Identity Protocol (HIP) [RFC7401] saw the introduction of cryptographic identifiers for the newly introduced Host Identity (HI) to allow for enhanced accountability, and therefore trust. The use of those HIs, however, is limited by the size of IPv6 128bit addresses.

### B.7. Communication protecting user privacy

The last decade has witnessed increasing concerns for user privacy ([RFC7258], [RFC6973]). IP Addresses are particularly exposed because they can easily be associated to end users, allowing fingerprinting and cross-site linking ([BUJLOW17], [MISHRA20], [I-D.irtf-pearg-ip-address-privacy-considerations-01]). Indeed, while encryption is widely used to conceal the traffic payload, the IP header remain, and particularly IP addresses, must be transmitted in clear in order to forward packets. Like mobility, privacy solutions have been developped with the help of higher layers, like for instance [I-D.ietf-ohai-ohttp] or [APPLEPRIV].

Specific to the network layer, one widely used approach to obfuscate the mapping between end users and IP addresses is the use of temporary addresses [RFC8981]. The idea here is to reduce the time window during which eavesdroppers and information collectors can correlate network activity based on the simple IP address. Ephemeral IP addresses have been in the working for more than 30 years [RFC9414], showing that having a temporal semantic in IP addresses can provide improved privacy protection.

A more radical approch leverages on recursively encrypt packets on a per segment basis, so that source and destination is not directly accessible[GOLDSCHLAG99]. Such kind of solution offers strong privacy properties, but comes at the price of reduced forwarding performance due to cryptographic operations involved.

### B.8. Communication in Alternative Forwarding Architectures

The performance of communication networks has long been a focus for optimization, due to the immediate impact on cost of ownership for communication service providers. For instance, technologies like MPLS [RFC3031] have been introduced to optimize lower layer communication, e.g., by mapping L3 traffic into aggregated labels of forwarding traffic for the purposes of, e.g., traffic engineering.

Even further, other works have emerged in recent years that have replaced the notion of packets with other concepts for the same purpose of improved traffic engineering and therefore efficiency gains. One such area is that of Software Defined Networks (SDN) [RFC7426], which has highlighted how a majority of Internet traffic is better identified by flows, rather than packets. Based on such observation, alternate forwarding architectures have been devised that are flow-based or path-based. With this approach, all data belonging to the same traffic stream is delivered over the same path, and traffic flows are identified by some connection or path identifier rather than by complete routing information, possibly enabling fast hardware based switching (e.g. [DETNETWG], [PANRG]).

On the one hand, such a communication model may be more suitable for real-time traffic like in the context of Deterministic Networks [DETNETWG], where indeed a lot of work has focused on how to "identify" packets belonging to the same DETNET flow in order to jointly manage the forwarding within the desired deterministic boundaries.

On the other hand, it may improve the communication efficiency in constrained wireless environments (cf., Appendix B.1), by reducing the overhead, hence increasing the number of useful bits per second per Hertz.

Another opportunity to improve communication efficiency is being pursued in ongoing IETF/IRTF work to deliver IP- or HTTP-level packets directly over path-based or flow-based transport network solutions, such as in [I-D.ietf-bier-multicast-http-response], [TROSSEN10], [I-D.trossen-icnrg-internet-icn-5glan], and [I-D.irtf-icnrg-5gc-icn], with the capability to bundle unicast forward communication streams flexibly together in return path multipoint relations. Such capability is particularly opportune in scenarios such as chunk-based video retrieval or distributed data storage. However, those solutions currently require gateways to "translate" the flow communication into the packet-level addressing semantic in the peering IP networks. Furthermore, the use of those alternative forwarding mechanisms often require the encapsulation of Internet addressing information, leading to wastage of bandwidth as well as processing resources.

Providing an alternative way of forwarding data has also been the motivation for the efforts created in the European Telecommunication Standards Institute (ETSI), which formed an Industry Specification Group (ISG) named Non-IP Networking (NIN) [ETSI-NIN]. This group sets out to develop and standardize a set of protocols leveraging an alternative forwarding architecture, such as provided by a flow-based switching paradigm. The deployment of such protocols may be seen to

form limited domains, still leaving the need to interoperate with the (packet-based forwarding) Internet; a situation possibly enabled through a greater flexibility of the addressing used across Internet-based and alternative limited domains alike.

As an alternative to IP routing, EIBP (Extended Internet Bypass Protocol) [SHENOY21] offers a communications model that works with IP in parallel and entirely transparent and independent to any operation at network layer. For this, EIBP proposes the use of physical and/or virtual structures in networks and among networks to auto assign routable addresses that capture the relative position of routers in a network or networks in a connected set of networks, which is used to route packets between end domains. EIBP operates at Layer 2.5 and provides encapsulation (at source domain), routing, and de-encapsulation (at destination domain). A resolver to map the domain ID to EIBP's edge router addresses is required. When queried for a specific domain, the resolver will return the corresponding edge router structured address.

EIBP decouples routing operations from end domain operations, offering to serve any domain, without point solutions to specific domains. EIBP also decouples routing IDs or addresses from end device/domain addresses. This allows for accommodation of new and upcoming domains. A domain can extend EIBP's structured addresses into the domain, by joining as a nested domain under one or more edge routers, or by extending the edge router's structure addresses to its devices.

## Appendix C. Examples of Internet Addressing Properties Extensions

### C.1. Length Extensions

#### C.1.1. Shorter Address Length Examples

* Header Compression/Translation: Considering one base station is supposed to serve hundreds of user devices, maximizing the effectiveness for specific spectrum directly improves user quality of experience. To achieve the optimal utilization of the spectrum resource in the wireless area, the RObust Header Compression (ROHC) [RFC5795] mechanism, which has been widely adopted in cellular networks like WCDMA, LTE, and 5G, utilizes header compression to shrink existing IPv6 headers onto shorter ones.

  Similarly, header compression techniques for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) have been around for several years now, constituting a main example of using the notion of a 'shared context' in order to reduce the size of the network layer header ([RFC6282], [RFC7400], [BADENHOP15]). More recently,

other compression solutions have been proposed for Low Power Wide Area Networks (LPWAN - [RFC8376]). Among them, the Static Context Header Compression (SCHC - [RFC8724]) generalized the compression mechanism developed by 6lo. Instead of a standard compression behavior implemented in all 6lo nodes, SCHC introduces the notion of rules shared by two nodes. The SCHC compression technique is generic and can be applied to IPv6 and layers above. Regarding the nature of the traffic, IPv6 addresses (source and destination) can be elided, partially sent, or replaced by a small index. Instead of the versatile IP packet, SCHC defines new packet formats dedicated to specific applications. SCHC rules are equivalence functions mapping this format to standard IP packets.

Also, constraints coming from either devices or carrier links would lead to mixed scenarios and compound requirements for extraordinary header compression. For native IPv6 communications on DECT ULE and MS/TP Networks [RFC6282], dedicated compression mechanisms are specified in [RFC8105] and [RFC8163], while the transmission of IPv6 packets over NFC and PLC, specifications are being developed in [RFC9428] and [RFC9354].

* Separate device from locator identifier: Solutions such as proposed in Expedited Internet Bypass Protocol [SHENOY21] and [RFC9300] use a separation of device from locator, where only the latter is used for routing between the different domains using the same technology, therefore enabling the use of shorter addresses in the (possibly constrained) local environment. Device IDs used within such domains are carried as part of the payload by EIBP and hence it is possible to use addresses of shorter size, suited to the domain. In LISP a flexible address encoding [RFC8060] allows shorter addresses to be supported in the LISP control plane [RFC9301].

### C.1.2. Longer Address Length Examples

* Split address zone by network realm: Network Address Translation (NAT), which was first laid out in [RFC2663], using private address and a stateful address binding to translate between the realms. As outlined in [RFC2663], basic address translation is usually extended to include port number information in the translation process, supporting bidirectional or simple outbound traffic only. Because the 16-bits port number is used in the address translation, NAT theoretically increase IPv4 address length from 32-bit to 48-bit, i.e., 281 trillion address space. [CHERITON00] also proposed to revise the Internet architecture so to make NAT natively part of it.

Similarly, EzIP [I-D.chen-ati-adaptive-ipv4-address-space] expects to utilize a reserved address block, i.e., 240/4, and an IPv4 header option to include it. Based on this, EzIP is carrying a hierarchical address with two parts, where each part is a partial 32-bit IPv4 address. The first part is a public address residing in the "address field" of the header from globally routable IPv4 pool [IPv4pool], i.e., ca. 3.84 billion address space. The second part is the reserved address residing in "option field" and belongs to the 240/4 prefix, i.e., ca. 2^28=268 million. Based on that, each EzIP deployment is tethered on the existing Internet via one single IPv4 address, and EzIP then have 3.84B * 268M address, ca. 1,000,000 trillion. Collectively, the 240/4 can also be used as end point identifier and form an overlay network providing services parallel to the current Internet, yet independent of the latter in other aspects.

Compared to NAT, EzIP is able to establish a communication session from either side of it, hence being completely transparent, and facilitating a full end-to-end networking configuration.

## C.2. Identity Extensions

### C.2.1. Anonymous Address Identity Examples

* Traffic Proxy: Although not initially designed as a traffic proxy approach, a Virtual Private Network (VPN [KHANVILKAR04]) is widely utilized for packets origin hiding as a traffic detouring methodology. As it evolved, VPN derivatives like WireGuard [DONENFELD17] have become a mainstream instance for user privacy and security enhancement.

  With such methodology in mind, onion routing [GOLDSCHLAG99], instantiated in the Tor Project [TOR], achieves high anonymity through traffic hand over via intermediates, before reaching the destination. Since the architecture of Tor requires at least three proxies, none of them is aware of the entire route. Given that the proxies themselves can be deployed all over the cyberspace, trust is not the prerequisite if proxies are randomly selected.

  In addition, dedicated protocols are also expected to be customized for privacy improvement via traffic proxy, as originally discussed during the the Strengthening the Internet (STRINT) IAB Workshop [RFC7687]. For example, Oblivious DNS over HTTPS (ODoH [RFC9230]) uses a third-party proxy to obscure identifications of user source addresses during DNS over HTTPS (DoH [RFC8484]) resolution. Similarly, Oblivious HTTP (oHTTP [I-D.ietf-ohai-ohttp]) involves proxy in the HTTP environment.

* Source Address Rollover: As for source address rollover, it has been standardized that IP addresses for Internet users should be dynamic and temporary every time they are being generated [RFC8981]. This benefits from the available address space in the case of IPv6, through which address generation or assignment should be unpredictable and stochastic for outside observers.

  More radically, [I-D.gont-v6ops-ipv6-addressing-considerations] advocates an 'ephemeral address', changing over time, for each process. Through this, correlating user behaviors conducted by different identifiers (i.e., source address) becomes much harder, if not impossible, if based on the IP packet header alone.

* Private Addresses: The use and assignment of private addresses for IPv4 is laid out in [RFC1918], while Unique Local Addresses (ULAs) in IPv6 [RFC4193] take over the role of private address spaces.

* Network Address Translation: NATs exist as part of existing customer premise equipment (CPE), such as a cable or an Ethernet router, with private wired/wireless connectivity, or it can be provided in a carrier environment to further translate ISP-internal private addresses to a pool of (assigned) public IP addresses.

* Separate device from locator identifier: EIBP [SHENOY21] separates the routing ID from the device ID, where only the former is used for routing. As such, it is possible to encrypt the device IDs, protecting the end device identity. Similarly, LISP uses separate namespaces for routing and identification allowing to 'hide' identifiers in encrypted LISP packets that expose only known routing information [RFC8061].

### C.2.2. Authenticated Address Identity Examples

* Self-certified Addresses: As an example of this methodology, [RFC3972] defines IPv6 cryptographically Generated Addresses (CGA). A Cryptographically Generated Address is formed by replacing the least-significant 64 bits of an IPv6 address with the cryptographic hash of the public key of the address owner. Packets are then signed with the private key of the sender. The receiveer authehticates packets by using the public key and address of the sender. The original specifications have been already amended (cf., [RFC4581] and [RFC4982]) in order to support multiple (stronger) cryptographic algorithms.

* Collision-resistant addresses: In order to provide a mechanism for IP mobility considerations, [RFC7343] defines Overlay Routable Cryptographic Hash Identifiers (ORCHIDv2). ORCHIDs use a

determinstic scheme for generating statistically unique addresses by concatenating a designated IPv6 prefix, a hash function identifier, and a truncated hash. The hash input is a unique, statically assigned context identifier concatenated with random data. A variation of this scheme is proposed to solve requirements of [RFC9153] in identification of unmanned aerial vehicles using Drone Remote Identification Protocol Entity Tags (DRIP Entity Tag - DET) [RFC9374]. This variation proposes a distinct IPv6 prefix and new hash functions, but the major change is to further truncate the hash, and use the freed bits for a two-level registration authority hierarchy.

* Third party granted addresses: [RFC3118] defines a DHCP option through which authorization tickets are generated and newly attached hosts with proper authorization can be automatically configured from an authenticated DHCP server. Solutions exist where separate servers are used for user authentication like [KOMORI02] and [RFC4014]. The former proposing to enhance the DHCP system using registered user login and password before actually providing an IP address lease and recording the MAC address of the device the user used to sign-in. The latter, couples the RADIUS authentication protocol [RFC2865] with DHCP, basically piggybacking RADIUS attributes in a DHCP option, with the DHCP server contacting the RADIUS server to authenticate the user.

## C.3. Semantic Extensions

### C.3.1. Extended Address Semantics Examples

* Semantic prefixes: Newer approaches to IP anycast suggest the use of service identification in combination with a binding IP address model [WION19] as a way to allow for metric-based traffic steering decisions; approaches for Service Function Chaining (SFC) [RFC7665] utilize the Network Service Header (NSH) information and packet classification to determine the destination of the next service.

  Another example of the usage of different packet header extensions based on IP addressing is Segment Routing. In this case, the source chooses a path and encodes it in the packet header as an ordered list of segments. Segments are encoded using new Routing Extensions Header type, the Segment Routing Header (SRH), which contains the Segment List, similar to what is already specified in [RFC8200], i.e., a list of segment ID (SID) that dictate the path to follow in the network. Such segment IDs are coded as 128 bit IPv6 addresses [RFC8986].

Approaches such as [CAROFIGLIO19] utilize semantic prefixing to allow for ICN forwarding behavior within an IPv6 network. In this case, an HICN name is the hierarchical concatenation of a name prefix and a name suffix, in which the name prefix is encoded as an IPv6 128 bits word and carried in IPv6 header fields, while the name suffix is encoded in transport headers fields such as TCP. However, it is a challenge to determine which IPv6 prefixes should be used as name prefixes. In order to know which IPv6 packets should be interpreted based on an ICN semantic, it is desirable to be able to recognize that an IPv6 prefix is a name prefix, e.g. to define a specific address family (AF_HICN, b0001::/16). This establishment of a specific address family allows the management and control plane to locally configure HICN prefixes and announce them to neighbors for interconnection.

* Separate device from locator identifier: Separating the identity from routing is an idea that goes back to PIP [RFC1621], which defined "PIP addresses" for routing and "PIP ID" for end device identification. More recently, EIBP [SHENOY21] separates the routing locator from the device identifier, relaxing therefore any semantic constraints on the device identifier. Similarly, LISP uses a flexible encoding named LISP Canonical Address Format (LCAF [RFC8061]), which allows to associate to routing locators any possible form (and length) of identifier. ILNP [RFC6740] introduces as well a different semantic of IP addresses, while aligning to the IPv6 address format (128 bits). Basically, ILNP introduces a sharper logical separation between the 64 most significant bits and the 64 least significant bits of an IPv6 address. The former being a global locator, while the latter being an identifier that can have different semantics (rather than just being an interface identifier).

* Structured addressing: Network topology captures the physical connectivity among devices in the network. There is a structure associated with the topology. Examples are the core-distribution-access router structure commonly used in enterprise networks and clos topologies that are used to provide multiple connections between Top of Rack (ToR) devices and multiple layers of spine devices. Internet service providers use a tier structure that defines their business relationships. A clear structure of connected networks can be noticed in the Internet. EIBP [SHENOY21] proposes to leverage the physical structure (or a virtual structure overlaid on the physical structure) to auto assign addresses to routers in a network or networks in an internetwork to capture their relative position in the physical/virtual topology. EIBP proposes to administratively identify routers/networks with a tier value based on the structure.

* Localized forwarding semantics: Approaches such as those outlined in [REED16] suggest using a novel forwarding semantic based on path information carried in the packet itself, said path information consists in a fixed size bit-field (see [REED16] for more information on how to represent the path information in said bit-field). In order to utilize existing, e.g., SDN-based, forwarding switches, the direct use of the IPv6 source/destination address is suggested for building appropriate match-action rules (over the suitable binary information representing the local output ports), while preserving the original IPv6 information in the encapsulated packet. As mentioned above, such use of the existing IPv6 address fields limits the size of the network to a maximum of 256 bits (therefore paths in the network over which such packets can be forwarded). [I-D.trossen-icnrg-internet-icn-5glan], however, goes a step further by suggesting to use the local forwarding as direct network layer mechanism, removing the IP packet and only leaving the transport/application layer, with the path identifier constituting the network-level identifier albeit limited by using the existing IP header for backward compatibility reasons (the next section outlines the removal of this limitation).

### C.3.2. Existing or Extended Header Semantics Examples

* In-Header extensions: In order to allow additional semantic with respect to the pure Internet addressing, the original design of IPv4 included the field 'Type of Service' [RFC2474], while IPv6 introduced the 'Flow label' and the 'Traffic Class' [RFC8200] fields. In a certain way, those fields can be considered 'semantic extensions' of IP addresses, and they are 'in-header' because natively present in the IP header (differently from options and extension headers). However, they proved not to be sufficient. Indeed, a variety of network operations are performed on the well-known 5-tuple (source and destination addresses; source and destination port number; and protocol number). In some contexts all of the above-mentioned fields are used in order to have a very fine grained solution [RFC8939].

* Headers option extensions: Header options have been largely under-exploited in IPv4. However, the introduction of the more efficient extension header model in IPv6 along with technology progress made the use of header extensions more widespread in IPv6. Segment Routing re-introduced the possibility to add path semantic to the packet by encoding a loosely defined source routing [RFC8402]. Similarly, in the aim to overcome the inherent shortcoming of the multi-homing in the IP context, SHIM6 [RFC5533] also proposed the use of an extension header able to carry multi-homing information which cannot be accommodated natively in the IPv6 header.

  To serve a moving endpoint, mechanisms like Mobile IPv6 [RFC6275] are used for maintaining connection continuity by a dedicated IPv6 extension header. In such case, the IP address of the home agent in Mobile IPv6 is basically an identification of the on-going communication. In order to go beyond the interface identification model of IP, the Host Identity Protocol (HIP) tries to introduce an identification layer to provide (as the name says) host identification. The architecture here relies on the use of another type of extension header [RFC7401].

* Re-encapsulation extension: Differently from the previous approach, re-encapsulation prepends complete new IP headers to the original packet introducing a completely custom shim header between the outer and inner header. This is the case for LISP, adding a LISP specific header right after an IP+UDP header [RFC9300]. A similar design is used by VxLAN [RFC7348] and GENEVE [RFC8926], even if they are designed for a data center context. IP packets can also be wrapped with headers using more generic and semantically rich names, for instance with ICN [I-D.trossen-icnrg-internet-icn-5glan].

* Structured addressing: Solutions such as those described in the previous section, e.g., EIBP [SHENOY21], provide structured addresses that are not limited to the IPv6 address length but instead carry the information in an extension header to remove such limitation.

  Also, Information-Centric Networking (ICN) naming approaches usually introduce structures in the (information) names without limiting themselves to the IP address length; more so, ICN proposes its own header format and therefore radically breaks with not only IP addressing semantic but the format of the packet header overall. For this, approaches such as those described in [RFC8609] define a TLV-based binary application component structure that is carried as a 'name' part of the CCN messages. Such a name is a hierarchical structure for identifying and

locating a data object, which contains a sequence of name components. For textual representation, URIs are normally used to represent names, as defined in [RFC3986].

In geographic addressing, position based routing protocols use the geographic location of nodes as their addresses, and packets are forwarded when possible in a greedy manner towards the destination. For this purpose, the packet header includes a field coding the geographic coordinates (x, y, z) of the destination node, as defined in [RFC2009]. Some proposals also rely on extra fields in the packet header to code the distance towards the destination, in which case only the geographic coordinates of neighbors are exchanged. This way the location of the destination is protected even if routing packets are eavesdropped.

* Localized forwarding semantics: Unlike the original suggestion in [REED16] to use existing SDN switches, the proliferation of P4 [BOSSHART14] opens up the possibility to utilize a locally limited address semantic, e.g., expressed through the path identifier, as an entirely new header (including its new address) with an encapsulation of the IP packet for E2E delivery (including further delivery outside the localized forwarding network) or positioning the limited address semantic directly as the network address semantic for the packet, i.e., removing any IP packet encapsulation from the forwarded packet, as done in [I-D.trossen-icnrg-internet-icn-5glan]. Removing the IPv6 address size limitation by not utilizing the existing IP header for the forwarding decision also allows for extensible length approaches for building the path identifier with the potential for increasing the supported network size. On the downside, this approach requires to encapsulate the original IP packet header for communication beyond the local domain in which the new header is being used, such as discussed in the previous point above on 're-encapsulation extension'.

## Contributors

Dirk Trossen
Huawei Technologies Duesseldorf GmbH
Riesstr. 25C
80992 Munich
Germany
Email: dirk.trossen@huawei.com

Paulo Mendes
Airbus
Willy-Messerschmitt Strasse 1
81663 Munich
Germany
Email: paulo.mendes@airbus.com

Nirmala Shenoy
Rochester Institute of Technology
New-York, 14623
United States of America
Email: nxsvks@rit.edu

Laurent Toutain
IMT-Atlantique
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France
Email: laurent.toutain@imt-atlantique.fr

Abraham Y. Chen
Avinta Communications, Inc.
142 N. Milpitas Blvd.
Milpitas, CA, 95035-4401
United States of America
Email: AYChen@Avinta.com

Dino Farinacci
lispers.net
United States of America
Email: farinacci@gmail.com

Jens Finkhaeuser
Interpeer gUG
Feldgereuth 8
86926 Greifenberg
Germany
Email: ietf@interpeer.io

Peng Liu
China Mobile
32 Xuanwumen West Ave
Xicheng, Beijing
100053
P.R. China
Email: liupengyjy@chinamobile.com

Yihao Jia
Email: yhjia03@gmail.com

Donald E. Eastlake 3rd
Futurewei Technologies
2386 Panoramic Circle
Apopka, FL, 32703
United States of America
Email: d3e3e3@gmail.com

## Author's Address

Luigi Iannone (editor)
Huawei Technologies France S.A.S.U.
18, Quai du Point du Jour
92100 Boulogne-Billancourt
France
Email: luigi.iannone@huawei.com