2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR) | 978-1-6654-4005-9/20/$31.00 ©2021 IEEE | DOI: 10.1109/HPSR52026.2021.9481811

Asymmetric Addressing Structures in Limited Domain Networks

Kiran Makhijani, Lijun Dong
Futurewei Technologies, Santa Clara, CA
{kiranm, ldong}@futurewei.com

***Abstract*—Different industry verticals require their network domains to describe their optimized application control and behavior through custom protocols. Such local protocols are necessary because adapting specific behaviors using current general-purpose network paradigms often leads to constrained design decisions since the IP does not provide necessary customization with its existing format. At the same time, with the growth in Industrial Internet and IoT, there is a need for convergence between the standard Internet and proprietary protocols. In this regard, network addresses are key to representing application semantics or a device's capability, but the current IP address structure does not sufficiently capture these artifacts. We propose the use of New IP shipping specification to accommodate a diverse set of local protocol requirements in a well-structured user-defined address scheme and its effective integration and adaptation to the IP for opaque connectivity over the Internet.**

I. Introduction

Industry verticals, for example, manufacturing, healthcare, transportation, etc. perform specialized operations within their industry sector. All the processes in such verticals are highly customized and designed for a particular outcome. Often the networks serving those verticals are also highly specialized. Firstly, they do not have a homogeneous network of only Internet Protocol (IP) enabled end stations, they also constitute other non-IP-stations (e.g., profinet, CANbus, Modbus, etc). Secondly, even when they use IP-based technologies, it is for local use, since applications are not required to participate in the global Internet, which allows for a high degree of proprietary optimizations. Such specialized networks qualify the RFC8799 definition of Limited Domain Networks (LDN) [1]. As special-purpose networks begin to grow in size and diverse requirements, adapting to existing IP-based stack is not always ideal. Thus, at its core, the LDN concept is expected to enable the evolution network stack without disrupting the Internet. One path to IP evolution is described in New IP [2] framework that provides several packet-level customizations.

In this paper, our proposal concentrates on the Industry Control scenario, where different types of address structures and protocols are common. Often, they lack a well-formed network layer and for devices to communicate in a large-area setting, such a network stack is needed for forwarding and reachability. There are several ways to insert one; the choice of network stack depends on the connecting device's capability and will also impact its addressing. Therefore, we can not default to the IP suite. In our solution, we introduce an 'asymmetric network system' using lightweight 'shipping specification' which takes into consideration that industrial device interfaces are somewhat bound to protocols. We suggest a nimble stack for networks in which one end may be an IP device and the other may be non-traditional.

We are motivated to develop a communication model for supporting asymmetric connectivity patterns. One key aspect is a simplified selective duality of the address space; i.e., the Internet neither sees nor interprets the internal address schemes. It also means that when required, external addresses are compliant with all the protocols of the Internet. Asymmetric mode implies all artifacts of address structure, including flexibility and semantics. Within a limited domain's scope, the semantics are completely managed by the limited domain operator. They can be simple application identifiers or corresponding logical resources or a hint about the protocols they bind to.

Limited-domain concept gives us a confidence that evolution of network stacks is feasible with in a domain since it does not impact Internet protocols. Our asymmetric addressing scheme can be deployed for the interoperability between different types of network technologies.

This paper makes the following contributions: Industry control network study, to emphasize the problems and challenges with new address types in Section II and II-B. Section III provides a discussion on the emerging limited domain networks and their key characteristics w.r.t. addressing, this has not been done yet to the best of our knowledge. We demonstrate different address requirements and types of representations using shipping specification in Section III-D. A brief proposal to routing and forwarding techniques for an asymmetric address system is in Section IV, while Sections V and VI summarize related work and conclusion respectively.

II. Background and Motivation

The Internet at the global scale provides general-purpose, best-effort connectivity using IP protocol. Applications such as web access, video streaming media, newsfeed, e-commerce, social media, and so on are general-purpose, for which the IP suite is a proven and viable network technology.

There also exist an entirely different category of special-purpose networks for process control and automation in which communication is between the application servers (using IP protocol suite) and the non-IP devices like robots, sensors, actuators that are being used in different industry sectors such

978-1-6654-4005-9/21/$31.00 ©2021 IEEE

as Oil Refineries, Mining, Smart Agriculture, Paper Industry, etc. Their means of connectivity are extremely diverse and these networks have unique characteristics: a) they connect non-traditional (i.e. machine-type) devices, b) their operation is well-defined and purposely built for use in a particular industry vertical, and c) one end of such connections is almost always IP. Because of the specific constraints of battery-life, low memory, short reach, a standard IP-stack is not ideal for these networks and several optimizations are necessary. This becomes readily noticeable in the industrial control scenarios.

A. Control and Automation Network Requirements

We illustrate an industrial network in Fig. 1. There are a high number of protocols in all the interface categories (serial, Ethernet, wireless, radio etc.). In fact, according to one vendor [3], there are more than 100 protocol conversion gateways available in the market. As more sensors or devices are added in a building, or on a factory automation floor, the number of translation protocols could grow even further. Protocol conversions are needed when different types of interfaces need to interact; in Fig. 1, a Profinet controller may act as a server in sub-network Net-E, to get status from the building automation client devices in Net B and Net C.

We observe the absence of a network layer from many IIoT (Industrial IoT) interfaces which is required when crossing the LAN (Local Area Network) boundary. The missing network layer is particularly evident in the bus protocols which are used when time-bound or low latency behavior is desired.

For the most part in industrial networks, the communication is between a controller such as a Programmable Logic Controller (PLC), or a server. The network and transport aspects are embedded in the application data if needed. Packet formats for different protocols are shown in Fig. 1, viz. BACnet MS/TP (Net-A), BACnet/IP [4] (Net B), Modbus [5] (Net-C), and Profibus [6] (Net-D). The corresponding stacks will sometimes show the same protocol adapted for IP, but in reality, it is an encapsulated PDU inside the IP payload from a PLC to higher-layer applications.

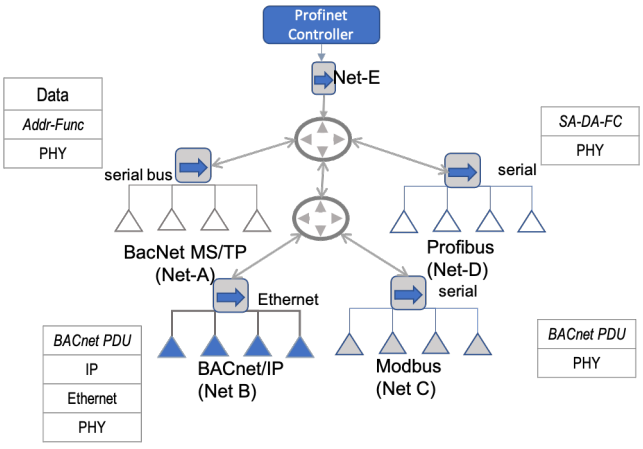

Fig. 1. Reference multi-interface Industry control networks

For devices to communicate over a large area (e.g. campus, zone), a network stack is needed. The choice of the stack should be based on connecting device's capability which directly impacts the network addressing scheme. The industrial control systems have a unique characteristic of client/server relationship between a PLC and sensors/actuators. There is no need for larger addresses beyond the PLCs, which themselves are the nodes with limited capabilities. However, the other end of the PLC connection could be an IT application host with IP stack. This is inherently a case for non-uniform addresses.

We introduce an *Asymmetric Network System of Addressing*, based on earlier work on light-weight 'shipping specification' (Section III-D). It enables industrial devices with different interfaces to inter-work.

B. Problems with Well-known Address

There are scenarios where IP stack is not a natural option and trade-offs should be understood as below:

1) Application Gateway Problem: The communication pattern in IoT devices is primarily *fire and forget* for which even a UDP/IP is an overhead and to overcome this, direct application-level Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) have been designed. They work with the help of IoT gateways between a device and an application server. However, this cannot scale gracefully; Zachariah et al [7] equate the application-gateways approach to each website requiring its browser. The gateways tend to combine connectivity, device state processing, and user interface functions and over time become too big and difficult to manage, provision, upgrade and operate. Thus, stalling the adoption of the new technologies.

2) Reuse of Protocols is not as seamless as anticipated: The choice of integrating with IP networks on industrial devices does not imply that those protocols become readily available from terminal to terminal. Often changes are necessary in the adaptation layer as is evident from mechanisms developed under the 6TiSCH initiative and a new set of protocols are proposed in [8].

3) Adaptation Layer for Compression: To minimize transmission cost over a constrained medium, RObust Header Compression (ROHC) [9] is used. It classifies header fields and identifies their variation pattern and omits static fields during the data transmission. We can assume that the terminal performing the compression is not a constrained device. For those types of devices, the adaptation layer Static Context Header Compression (SCHC) [10] is an option. Even with SCHC, the burden of optimization stays with the constrained node, since it performs network layer functions. Such approaches require more work on the constrained (in power, memory, and processing capabilities) devices than on general-purpose well-resourced servers. Although the memory footprint for SCHC is small, we argue that maintaining and programming the context in devices affects their battery life-time whenever it is required to update the context.

4) Application Semantics: At the apex of Industry 4.0 vision, the role of Digital Twins (DT) [11] is undeniable.

They use both recent and past data to predict different future scenarios in simulations. There is no match between the power of a digital entity and its physical counterpart. DT-enabled systems can become very complex at large-scale, But semantic knowledge about this type of relationship (virtual to physical) can be embedded in the addresses. For example, an address to say "is-a-twin-of" can help design access policies and enhance security through path control mechanisms.

5) Fixed Addressing is not Ideal: While the structure of an address is important, its fixed format is too rigid. There is no intelligence encoded about the device being addressed. Especially, in industry control, the number of applications as well as small devices is growing. We view this as a problem of not only a smaller address space but as an unbalanced space, in which one end is well resourced, and the other is not.

The current available optimizations or gateways are at best short-term solutions. They are not suited for a long-term automation roadmap.

C. Challenges in Adoption of New Address Formats

Due to the omnipresence of IP (v4 or v6), it has been the only network protocol solution considered from terminal to terminal. Obviously, it has several important advantages highlighted by Slywczak, in [12]. Firstly, it facilitates seamless integration between different kinds of infrastructures, for example, radio and wired networks. Potentially, terminal to terminal IP eliminates a total number of translations needed to retrieve the data. Finally, its pervasiveness and maturity makes it the most suitable method in terms of development cost and time because using an already existing set of protocols is a well- understood problem.

The repelling forces between problems $vs.$ challenges highlighted above make it difficult to integrate different technologies necessary for industry automation.

Observe that (a) fixed addressing is necessary for global Internet access but this type of access is not a requirement for industry networks. Instead, they only need a global reachability service, (b) Special-purpose networks are administratively autonomous and control in their business domain. Leveraging these two properties, such networks are characterized as limited domains and, we develop a novel scheme that supports address duality of 'global-reach' and 'locally-controlled' addresses through an Asymmetric address system. But first, we briefly discuss limited domains in the following section.

III. Emerging Structure of Limited Domains

The networks of organizations are growing consistently, which requires them to develop and maintain home-grown features specific to their business goals. Sometimes it is not possible to use Internet technology directly and organizations overcome such limitations with proprietary approaches limited to their networks. They are described as LDNs in [1].

A. Conceptual Structure of the Networks

The generic structure of connectivity is evolving along with the following three categories which led to the identification of limited domains.

i. Private large-scale (all-IP) network: Internally use IP-based hosts and protocols. See Fig. 2-A) and B).
ii. IoT domain networks (IP-adapted IP): in which internal end-stations are largely non-IP but use adaptation layer. Such as Fig. 2-C).
iii. The Controlled domain or Operations Technology (OT) networks (IP-non IP) in which many end stations are non-IP based but they connect to IP enabled applications. See Fig. 2-D).

Fig 2-A) is the most common scenario observed in the generic, end-user type of applications. Here, a host is on the Internet and accesses services from the large-scale distributed networks. Whereas Fig. 2-B) is an enterprise or campus network setting, still enabled by IP terminal to terminal but require additional service or application specific orchestration semantics which should be captured in packet headers (e.g., SR, SFC, VXLAN, VPN, etc.).

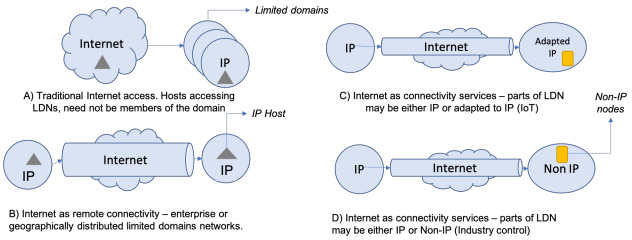

Fig. 2. Conceptual structure of Limited Domain Networks connecting to Internet

Fig. 2-C) and D) are representative scenarios of our interest in this paper. They necessitate the need for non-IP to IP based connectivity within a domain (e.g., factory floor or a mining site). They also need remote site connectivity to IT systems that run applications such as supply chain, inventory management, sales, quality control, etc. These types of networks are naturally asymmetric. They are also carefully engineered to support only small set of scenarios. In other words, they only need a limited set of IP features. For example, TCP transport is not ideal for sensor networks. These devices send or receive short commands to/from the server. They do not require long persistent connections but have real-time and low latency constraints. Moreover, standardization and development procedures in Industry control are different from the protocols developed for Internet technologies. Overall, the process of integrating with IP based stack is non-trivial.

B. Inheriting Limited Domain Characteristics

The adoption of non-traditional addresses can take place in a limited domain. It should not depend on the corresponding changes in the global Internet, since the Internet architecture favors a slow to change network and transport layers [13]. Often changes are so slow that organizations end up building their custom protocols. Ammar [14] observes this as a ManyNets phenomenon, in which when networks need new features, they bypass the global Internet and develop those features for their use. Because, within a limited domain, the

administrative control and management are localized, it gives a lot more flexibility to evolve different types of network layers.

The LDNs capture three characteristics - at the core of LDNs is their ability to evolve independently on its own (via inside protocols) without impacting the global Internet, it's requirement for global reach when necessary (via outside Internet protocols), remaining inert to the effects of the changes that happen outside its domain (via isolation boundaries).

Thus, to bring a new address format for the industry control networks we embrace LDN model. Our design first identifies the address structure inside the LDN; then suggests a method on the boundaries of the LDNs to allow transiting over the Internet.

C. Asymmetric Address Structure

A network packet header is a concise description of the payload and at minimum tells where the packet is destined to, additionally how it may be treated in the network. The IP network protocol works over different layer 2 technologies (wifi, LTE, Ethernet, etc.) yet, it is not always ideal to assign an IPv6 network address for all types of networks. The notion of asymmetric address at the basic level indicates that the source-address and destination-address formats can be different. By doing so it can support several other features such as hierarchical, compressed, or semantic structure. LDN-operators based on their business objectives and network technology requirements can utilize several encoding features in the asymmetric address structure. Some of the examples are:

i. Hierarchical: The address structure can carry information hierarchically. For example, an address contains only its subnet and device identifier. Which is sufficient for routing within the LDN.
ii. Layered: The addresses can also be layered. This allows variable length addresses to incorporate topological requirements. i.e., the extent to which a device is reachable. The layered subnets can help isolate the scope of an address.
iii. Compact: To conserve header length address bits may be packed instead of using the canonical format. For example, a device with $1 - byte$ serial bus address has canonical representation as $device = 2 \rightarrow 0.0.0.2$. When it communicates with another device in the LAN then the prefix part is not necessary to be on the wire.
iv. Semantic: To express application specific routing, application-type can be part of the address.

All of the above concepts can be incorporated using shipping specification. in particular, with compact addresses, it will be possible to devise a network layer suitable for constrained IoT and IIoT devices.

D. Shipping Specification - Representation of Asymmetric Addresses

The ability to capture different address formats requires a programmable and flexible approach for which we lean on our prior work: New IP. Shipping specification was first introduced as a free-choice addressing component of New IP [2]. The overarching motivation for New IP is to enable new network capabilities that meet the diverse needs of different market verticals through a common framework. It requires an extensible and programmable packet structure, allowing network operators to select and encode their service-level objectives, path constraints, and domain-specific reachability aspects such as choice of an address structure for their domain. When integrated with the limited domain paradigm, shipping specification can embody any addressing scheme desired by the network operators for the inside domains. As shown in Fig. 3 the spec has a format that allows a separate definition of source and destination. In the following sections, a few address-format examples are presented to demonstrate that shipping spec can be a generalized packet structure in the LDNs.

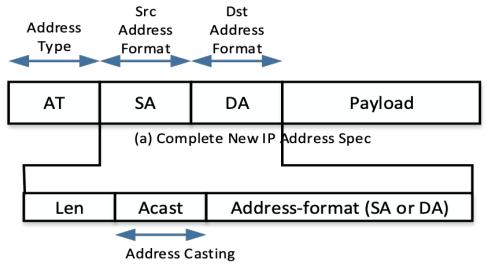

Fig. 3. Shipping Specification Format

1) Semantically Structured Representation: The `address-type` and `address-cast` fields are explicit semantic representations that tell what type of address follows. Besides the `address-format` itself can be formed based on the semantics assigned by an operator. By adopting this type of addressing, the work done by gateways is minimized. They only need to perform state-less translations between the multiple interfaces (for example from Serial to Ethernet or Modbus to Profinet, etc.). A typical Industry control network layered packet is shown in Fig. 4.

As discussed earlier, gateways can easily add to the complexity of an application design and real time requirements. In contrast, embedded semantics in the address structure can directly provide clues to the forwarding nodes about real-time packet constraints.

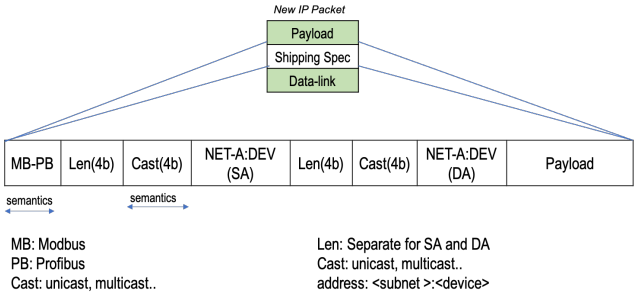

Fig. 4. Asymmetric Network Packet

2) Natural Compact Representation: We have argued in previous sections that the IP address encoding need not to be fixed. A canonical representation of IP address format (specifically IPv6) is too large for LPWAN (Low-Power Wide-Area Network) applications even larger than the payload sent on the wire in OT or IoT scenarios. Alternately, in a closed control network, certain situations may not need to know the source address and such overheads can be further removed (Fig. 5(a)). In fact, a small device can not often verify the source address. Integration with newer protocols such as SCHC is also possible with shipping spec as shown in Fig. 5 (b).

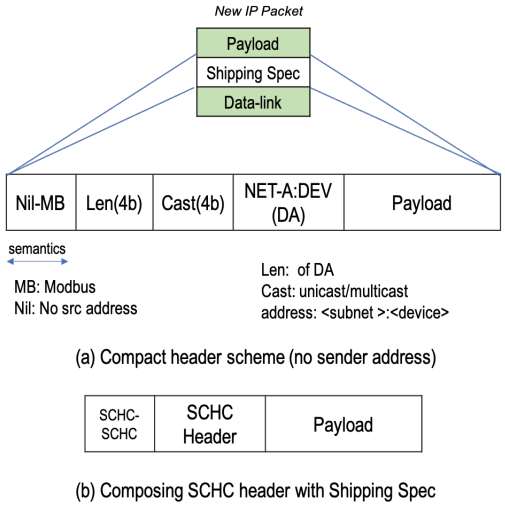

Fig. 5. Compact Addressing Using Shipping Specification

3) Constrained Device Network Layer Representation: To support a network layer for tiny devices, the device needs a simple capability of keeping a network address (which may or may not be the same as its PHY address) and means to insert a shipping-spec structure. For example, the current format of a frame "$addr|function|data$" changes to include the shipping spec - "$addr|shipping-spec|function|data$". This can be easily done with programmable serial devices, otherwise, for the legacy devices, attached PLC acts as their network interface.

IV. Asymmetric Addressing System in Limited Domains

An Asymmetric Address System (AAS) is the one that supports any operator-defined suitable addressing scheme within an LDN supporting shipping specification in the data plane for interconnection of end-points with the same or different protocol. Such a system is required to maintain the scope of addresses within its limited domains. AAS is a combination of several functions such as address- discovery, allocations, management, scope, and distribution. In this section, we briefly consider concepts related to the distribution of asymmetric addresses in the inside, outside, and at the border network nodes.

A. AAS Network Model

A conceptual model for our proposal is shown in Fig. 6 below. In this model, an LDN core network is shown using different address schemes marked as $AF1$, $AF2$ and $AF3$ in their respective subnets. A border node is used to communicate with remote LDN sites. Inside the LDN, subnet AF_n specific routing is enabled, and distributed for forwarding of packets between the subnet in this LDN. The end-hosts packetize according to asymmetric addresses. Finally, for transit over the IP network, we insert a numeric value of non-IP $AF1$ address into IP format. This step can be done using a stateless function support.

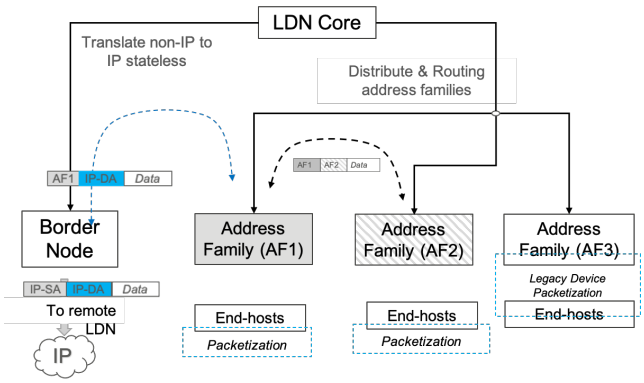

Fig. 6. LDN based AAS Network Model

B. Routing Characteristics

AAS supports extensions to dynamic routing protocols for learning and distribution of a) topology, b) path information, c) backup path, d) traffic engineering, e) semantic-based routing, etc. Our AAS supports non-Internet address structures to distribute the origin of address prefixes from a router for a particular address scheme and its numbering plan. The intermediate routers learn these prefixes, compute the Forwarding Information Base (FIB), and populate per AFI FIB look-up tables with next-hop information. Obviously, AFIs need to be globally allocated by central authority Internet Assigned Numbers Authority (IANA) for interoperability.

Local-Domain Address Family Identifier: In AAS, we introduce Local-Domain Address Family Identifier (LDAFI). These are functionally equivalent to the AFIs but do not require Internet Assigned Numbers Authority (IANA) approval. The address structures are defined by the network management layer of the LDN. This way our New IP routers can host per LDAFI FIBs. Since forwarding is based on destination address, the format of the source address does not influence the FIBs.

AAS Packet setup: The AAS end-hosts will form the packets according to the LDAFIs supported in the LDN and are expected to have a thin network layer (Section III-D3) and are forwarded seamlessly; otherwise the edge network device will need to do the AAS packetization, as is required for legacy devices in the subnet $AF3$ in Fig. 6. Industry control networks

use client server interface and configuring this server address information is straight forward. However, generating packets in a AAS format should be done efficiently. Host side address management is an independent topic and has not been covered here.

C. Inside Domain Forwarding

LDAFI is designed to use traditional routing protocols (OSPF, IS-IS, BGP-LS, etc.). Proven algorithms for path-computation and other features can be deployed in LDNs with LDAFI extensions. Thus, the forwarding rules for limited domains are governed by the inside address structures. In some cases, even simple rules such as push, pop,or swap can be supplied to the LD-FIB, where end-to-end shipping spec apply. For example, the industry control, OT protocols have historically relied on protocol gateways. Now, these gateways can be made stateless and act as routers using New IP shipping spec functions. A controller in $AF1$ in Fig. 6, originates a New IP packet with asymmetric address toward a device in subnet $AF2$.

D. Outside Domain Forwarding

Outside of a limited-domain is a pure IP-based network that neither understands LD-AFI nor asymmetric addresses. Outside domain forwarding is required to connect with remote LDN sites. Internet is used as a connectivity service, therefore, only IP forwarding protocols are available between the border nodes of the LDN sites. This means a translation from internal address scheme to IPv6 is needed. Conventional tunneling interconnects are possible (VPNs, overlays, NATs, etc.). However, they are often used with known (IP, MAC) address families and address-formats. Thus any overlay approach will require exposing LD-AFIs to be IANA approved or at the very least an assumption that intermediate hops will neither interpret nor drop those AAS packets.

Instead, we suggest to convert numeric value of non-IP LDN address to a 64-bit host part of the IPv6 address. In our proposal, limited domain identifier (LDN-ID) is needed for remote site connections and is not necessary for inside the LDN forwarding. Therefore, a 64-bit IPv6 global routing prefix as a unique identifier is most suitable id for an LDN and requires no translation. Remaining 64 bits of host address space is obtained for translating internal address semantics as below in Fig. 7. The role of border routers is to perform these translations.

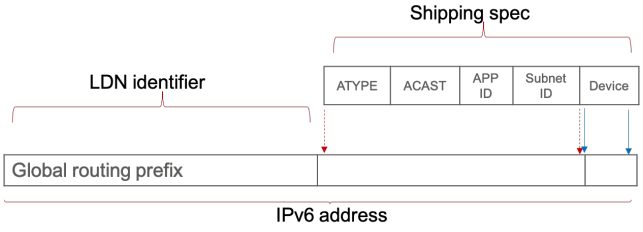

Fig. 7. Outside IPv6 representation of limited domains

In addition, the following forwarding considerations apply:

Shipping Spec to IP forwarding: It is possible that a remote site under the same administrative control supports pure IP. For example, in Industry networks, often application software and middleware reside in the IT network at a different location. When connecting to such an IP network, only the border router on non-IP site needs to maintain a mapping between internal semantics and IP. while IT applications continue to connect as originally. In our example, let's assume (Fig. 7) this is a non-IP address of a source device. The destination address (not-shown) will be a well-known IP and needs no translation. It carries $ATYPE$ and $ACAST$ fields which as mandatory part of the shipping spec. In our example, $ACAST$ is not important, but $ATYPE$ is required by remote application to derive entire semantics of the address. $ATYPE$ tells an application, about the device-type (such as Modbus, IP, Profibus, etc.). This is the key to inter-operation of heterogeneous protocols between applications and industry control devices.

Shipping Spec to Shipping Spec forwarding: When all connecting remote sites of a limited-domain under the same administrative control support shipping spec (e.g, two or more remote mining sites), then the free-choice addressing still applies and the outside protocol is also opaque. The amount of translation work at the border router is minimized and possibly stateless.

Border Router Strategies and Domain Semantics: The role of border routers is to enforce policies and security boundaries. We believe due to semantic addressing (e.g. self-describing scope), the language and structure of those rules can be simplified.This topic need a thorough discussion and we defer them as part of our follow-up work.

E. Analysis of AAS

The asymmetric addresses facilitate communication between two devices with different address schemes over the same network without any protocol translations. This is achieved without increasing the number of protocols or bifurcating the network. By associating with LDN, the scope is confined from the external Internet providing boundary protection from the design itself. The number of stateful gateways is reduced as the need to normalize everything encapsulated in IP packets is eliminated. We especially like the idea of native (no overlay) connectivity between the two heterogeneous networks. Shipping spec does not lose any information about the host interface, it abstracts those hints at a higher layer.

A comprehensive solution requires end-host participation which may not be possible for several legacy devices. The biggest challenge is to have devices form the AAS packets with shipping spec. We believe this hurdle can be overcome at least on devices that have some memory and compute support, only a few instructions will be needed. Arguably, policy language used within a network needs to be refined to accommodate rules that match different LDN AFIs. Finally, operators of AAS networks are responsible for managing address-families choices. We have been working on a proof-of-

concept with the shipping spec on this type of network model and will be able to share more when the software is ready.

V. Related Work

The evolution of network addresses has been covered from different perspectives such as Francis and Govindan proposed SIPP [15] for larger addresses at the network layer with two key features of a global hierarchy of addresses and a loose source routing with a fixed 64-bit structure. Lately, Moskowitz et al. in FAS [16] suggest a variable length addressing mechanism at the global scale. Their proposals are similar to our work since they are based on evolution to the IP stack. But these evolutionary approaches demand global IP changes. In contrast, we exploit LDNs characteristics and provide an evolution that is opaque to the internet.

In the context of IP, compression techniques [10] covered earlier are relevant, but are limited to shorter headers and miss out on other address-specific properties such as asymmetric, source-less, or semantic addresses, therefore, represent a very small feature set. In industry control networks, Kulik, et al. proposed a semantic [17] gateway appliance but they do not solve the interface conversions, say from serial to Ethernet. Their intended to enable a gateway that understands different communication interfaces. Moreover, such an approach is overly centralized where the semantic gateway could become overloaded and a single point of failure.

Our foundational work in the New IP packet format [2] is well suited for asymmetric, flexible and semantic properties of addresses. They can be utilized for different industry verticals. Moreover, we also utilize LDN framework to isolate non-IP addresses from the global Internet. By introducing the LD-AFI, we provide mechanisms for using existing routing protocols for custom addresses.

VI. Conclusions and Next Steps

We recognize that changing addresses at Internet scale is extremely slow process (if not impossible). Therefore, we blended IP and non-IP addresses using two concepts - shipping spec and limited domains. We propose an asymmetric addressing approach which offers a great amount of flexibility to the operators of the limited domain networks. We leveraged New IP's shipping specification for expressing different types of address structure. We demonstrated industrial network scenarios and applied asymmetric addresses to such networks, in doing so we identified a lack of network stack and network address in small devices.

Our solution includes a routing and forwarding strategy which does not impact the global Internet and therefore, it is a promising technology for the evolution of the network layer. We hope to continue exploring distribution, routing, and forwarding aspects of our work.

VII. Acknowledgments

The authors would like to thank Lin Han, Stewart Bryant, and Wael William Diab for insightful discussions on the topic of addressing and Industrial Networks.

References

[1] B. E. Carpenter and B. Liu, "Limited Domains and Internet Protocols," *RFC*, vol. 8799, pp. 1–23, 2020.

[2] R. Li, K. Makhijani, and L. Dong, "New IP: A Data Packet Framework to Evolve the Internet : Invited paper," in *21st IEEE International Conference on High Performance Switching and Routing, HPSR 2020, Newark, NJ, USA, May 11-14, 2020*, pp. 1–8, IEEE, 2020.

[3] "Chipkin Automation Systems - case studies." https://store.chipkin.com/about-us/case-studies.

[4] "BACNet: Data Communication Protocol for Building Automation and Control Networks." http://www.bacnet.org/index.html.

[5] "MODBUS Protocol." https://modbus.org/.

[6] "Profibus profinet international (pi) industrial communication interest group.." https://www.profibus.com/.

[7] T. Zachariah, N. Klugman, B. Campbell, J. Adkins, N. Jackson, and P. Dutta, "The internet of things has a gateway problem," in *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, HotMobile '15, (New York, NY, USA), p. 27–32, Association for Computing Machinery, 2015.

[8] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, and P. Thubert, "Ietf 6tisch: A tutorial," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 595–615, 2020.

[9] E. e. a. Bormann, C., "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed." RFC 3095 (Proposed Standard), 2001.

[10] A. C. Minaburo, L. Toutain, C. Gomez, D. Barthel, and J. C. Zúñiga, "SCHC: Generic Framework for Static Context Header Compression and Fragmentation," *RFC*, vol. 8724, pp. 1–71, 2020.

[11] "GLOSSARY OF DIGITAL TWINS - Digital Twin consortium." https://www.digitaltwinconsortium.org/glossary/index.htm.

[12] R. A. Slywczak, "NASA/TM—2004-212299: Low-Earth-Orbit Satellite Internet Protocol Communications Concept and Design."

[13] J. Rexford and C. Dovrolis, "Future internet architecture: Clean-slate versus evolutionary research," *Commun. ACM*, vol. 53, no. 9, p. 36–40, 2010.

[14] M. Ammar, "Ex uno pluria: The service-infrastructure cycle, ossification, and the fragmentation of the internet," vol. 48, p. 56–63, Apr. 2018.

[15] P. Francis and R. Govindan, "Flexible routing and addressing for a next generation ip," *SIGCOMM Comput. Commun. Rev.*, vol. 24, p. 116–125, Oct. 1994.

[16] S. Ren, D. Yu, G. Li, S. Hu, Y. Tian, X. Gong, and R. Moskowitz, "Routing and addressing with length variable ip address," in *Proceedings of the ACM SIGCOMM 2019 Workshop on Networking for Emerging Applications and Technologies*, NEAT'19, p. 43–48, 2019.

[17] V. Kulik and R. Kirichek, "The Heterogeneous Gateways in the Industrial Internet of Things," in *2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 1–5, 2018.