IPv6 Addressing Strategies for IoT

Teemu Savolainen, Jonne Soininen, Bilhanan Silverajan

***Abstract*—In this paper we analyze the suitability of different IPv6 addressing strategies for nodes, gateways and various access network deployment scenarios in the Internet of Things. The vast numbers of things being connected to the Internet need IPv6 addresses, as the IPv4 address space was effectively already consumed prior to the introduction of the Internet of Things. We highlight how the heterogeneity of nodes and network technologies, extreme constraint and miniaturisation, renumbering and multihoming, present serious challenges towards IPv6 address allocation. By considering the topologies of various types of IoT networks, their intended uses as well as the types of IPv6 addresses that need to be deployed, we draw attention to allocation solutions as well as potential pitfalls.**

***Index Terms*—IPv6, IoT, addressing, renumbering, low-power, topology.**

I. Introduction

In 2011, nearly 1 billion smart connected devices, comprising of PCs, tablets and smartphones were shipped, with estimates indicating that the number would almost double by 2016 [1]. The total number of Internet connected devices, however, exceeded 8.7 billion in 2012 [2]. Within 7 years, expectations are rife that the present number of connected nodes would be significantly dwarfed, as estimates from standardization bodies, network equipment vendors as well as network operators range from 25 to 50 billion connected devices [2][3][4]. These nodes comprise both smart devices as well as complexity and resource limited nodes such as sensors and actuators. While commonly available connectivity technologies such as cellular, fixed Ethernet and Wi-Fi networks would continue to be used, billions of resource constrained nodes are expected to also utilise low power communication over technologies such as Bluetooth Low Energy (BLE), DASH7, Insteon, 1-Wire, as well as IEEE 802.15.4-based technologies such as ZigBee.

The phrase "The Internet of Things" (IoT) was the title of the seventh report in a series of Internet reports the International Telecommunications Union ITU-T issued to address challenges to the network[5]. This report was published in 2005 and envisioned interconnected Internet-enabled networks providing ubiquitous connectivity which had far reaching implications for machine to machine communications, delivering content to users as well as allowing everyday household objects to be connected to the digital world. Advances in Radio Frequency Identification (RFID), nanotechnology, sensors and smart technologies (such as wearable computing, intelligent homes and vehicles and robotics) were identified as technology enablers for IoT. While the origins of the term "IoT" predate the ITU-T report, the vision became a reality in 2010 when Internet connected devices began outnumbering the world's human population [2].

One of the first steps in allowing such large numbers of nodes to co-exist and communicate in the Internet is the existence of efficient, scalable and federated architectures and schemes for unambiguous naming and addressing. This is particularly so in IoT, where there is an abundance of sleeping nodes, intermittent connectivity, mobility and non-IP devices. In addition to reachability, this provides the ability for unique identification, facilitation of active mechanisms for service discovery as well as passive lookups.

We examine how IPv6 can be effectively deployed for various IoT topologies particularly with emphasis on address allocation approaches. The motivation and contributions of this paper are outlined in the next section. The terminologies used to describe various concepts, topologies and solutions are supplied in Section 3. Section 4 describes various relevant facets of IPv6 for IoT node addressing while Section 5 outlines and explains possible network topologies for realistic deployment as well as upstream connectivity. Mobility implications are then discussed in Section 6 while solutions for address allocation are presented in Section 7. We then arrive at a conclusion of how well current and future addressing needs for IoT devices are met by efforts towards IPv6 adoption for the Internet of Things.

II. Motivation

IPv6 address allocation schemes for constrained nodes have been covered extensively in academic literature, particularly by the wireless sensor networks (WSN) research community. Some of the issues surrounding address allocation in WSN are similar to IoT. The challenges of combining sensor networks with IP access are discussed in [6], particularly with low power networks such as 6LoWPAN. A scheme called MPIPA is presented in [7] that uses three-dimensional location coordinates to assign unique IPv6 addresses to sensor nodes in a smart grid. A lightweight stateless IPv6 address autoconfiguration for 6LoWPAN using color coordinators is discussed in [8]. An IPv6 address allocation scheme applicable to MANETs is outlined in [9] that allows the acquisition of unique IPv6 addresses from neighbouring proxy nodes by mobile nodes. Three ways in which WSNs can be integrated with the Internet are introduced in [10] along with a discussion of the complexities and routing requirements of each approach.

Many of these contributions view IPv6 as a replacement to IPv4 owing to its vast globally unique address space and

Teemu Savolainen (teemu.savolainen@nokia.com) is with the Nokia Research Center.
Jonne Soininen (jonne.soininen@renesasmobile.com) is with the Renesas Mobile.
Bilhanan Silverajan (bilhanan.silverajan@tut.fi) is with the Tampere University of Technology.

the simplicity of network configuration, therefore focusing on parameters for optimal IPv6 address allocations to reduce the chances of address collisions during Duplicate Address Detection (DAD). We do not intend to revisit old ground, but underline how the topology of IoT networks and the types of IoT nodes impose new requirements and limitations on node addressing, address configuration, reachability and naming needs. Consequently this paper's aim is to look at how well current efforts in IPv6 research and standardisation cope with technical challenges in the IoT for various scenarios, bearing in mind the expected properties of IoT nodes and topologies.

The motivation of this paper is to highlight IPv6 addressing schemes for nodes and gateways in various topologies with the emphasis on issues such as:

Node Miniaturisation: Extremely severely constrained nodes may not even have the ability to dynamically configure their addresses. There will be nodes which broadcast or communicate only unidirectionally and extremely miniaturized nodes such as nano machines communicating with the Internet (the Internet of NanoThings [11]) need to be considered for the future.

Renumbering Challenges: A smart vehicle and its associated networked sensors and nodes need to be renumbered upon entering specific locations (such as during car servicing and connecting to a service network), or in the absence of Internet connectivity without adverse disruptions to the operation of the intravehicular network, or communication with external nodes

Multihoming Challenges: Smart homes in which multiple stakeholders, which includes home owners as well as 3rd party operators (utility meters, smart grids and device vendors) may wish to access readings and data without being dependent on a single Internet uplink from the home. An electricity meter in the home may be simultaneously accessible from within the firewalled home network by the home owner and from the electricity provider's own Internet uplink and downlink. Multihoming scenarios also consider mobility scenarios with multiple interfaces where vertical handovers occur or when nodes migrate back and forth between IPv6 and non-IPv6 networks.

Proxying and Tracking non-IP nodes: The ability for an IoT node to serve as a bridge or a proxy towards non-IP technologies expected to be prevalent. BLE nodes and objects tracked with RFID provide unique IDs or tag values that can be used to generate IPv6 addresses. However, BLE IDs can be regenerated by the node from time to time, while the points of association for RFID tags change with respect to their readers or writers. Considerations that IPv6 addresses may not be permanent for such node types must be taken into account.

III. IoT Terminology

The architectural elements that form the building blocks for IoT can, and have been classified in many ways. The authors of [12] presented a high level taxonomy of IoT to illustrate the ubiquity of the architecture. They defined three IoT components necessary for seamless ubiquitous computing: *Hardware* such as sensors, actuators and embedded communication systems, *Middleware* such as analytic frameworks for data computation and on-demand storage and *Presentation* which provides a visual perspective with the aid of interpretive, multi-platform tools. Node classifications have also been performed in various ways. The IEEE 802.15.4 low-rate wireless personal area network (LR-WPAN) standard classifies any participating, networked node as either a full-function device (FFD) which can participate in any topology, implement the entire protocol set and act as a PAN co-ordinator, or it can be a reduced-function device (RFD) for more limited nodes that have minimal implementations allowing them to paticipate as leaf nodes in various topologies without the ability to perform any co-ordination activities [13]. In [14] authors discuss nodes constrained by power and memory capacity and classifies them as belonging to *Class 0* for very constrained and simple sensor-style devices, *Class 1* for nodes containing approximately 10 Kilobytes of RAM memory and 100 Kilobytes of Flash memory or *Class 2* for nodes containing approximately 50 Kilobytes of RAM memory and 250 Kilobytes of Flash memory. A different kind of taxonomy is presented when discussing ambient energy harvesting sensors: IoT installations are classified as *Trivial*, *Classic*, and *True IoT* based on the number of nodes and communication technologies, to understand their energy needs [15].

To understand the presented concepts and topologies in this paper, we provide definitions of the various parts of an IoT network and the types of node present in the IoT.

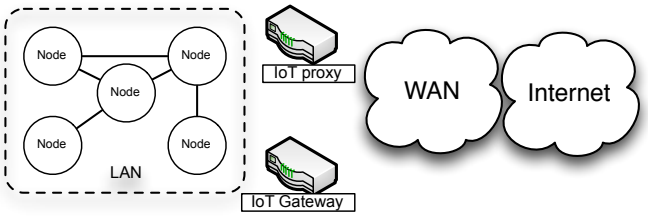

Figure 1: Internet of Things, generalised architecture

Figure 1 shows a high-level layout of the Internet of Things. On the surface, the architecture does not differ from any normal Internet network structure. The explanation of the different building blocks are in the following.

IoT Local Area Network (LAN) is the network connecting IoT nodes in a local - relatively short range - configuration. Different network technologies can be used for connecting the IoT LAN, both wireless, and wireline, and be present in one IoT LAN. However, the technology used is relatively short range, and the administration is under one entity (person, or organization). IoT LAN topologies can differ from low-power, short-range configurations, to building or organization wide configurations. IoT LAN may or might not be connected to the Internet.

IoT Wide Area Network (WAN) is a network that covers geographically, and organizationally a wide area. While IoT LANs may be connected directly to the Internet, the IoT can be perceived also as a network of networks, with LANs connected and aggregated via WANs which are subsequently connected to the Internet. Hence, a WAN is usually a combination of network segments administered by different players reaching

potentially a very large geographical area.

IoT node is a node in the IoT LAN, and through that connected to the other nodes in the IoT LAN. If the IoT LAN is connected to the Internet, the IoT node may also be connected to the Internet directly. However, this is not always the case. In addition, there are cases where the IoT node is connected to the Internet though a WAN connection without an IoT LAN being present.

IoT gateway is a router connecting an IoT LAN with a WAN, and to the Internet. An IoT gateway is a layer 3 device, which forwards IP packets between the IoT LAN and WAN implementing both the network technologies. An IoT gateway can potentially implement several LAN and WAN technologies (wireless or wireline) depending on the configuration. The IoT gateway forwards packets between the IoT LAN and the WAN on the IP layer without performing application layer tasks. In one IoT LAN, there may be zero or more IoT gateways depending on the scenario.

IoT proxy is an entity that performs an active application layer function between IoT nodes, and other entities. The application layer functionality can range from relatively simple application protocol conversion to more active application functions. The IoT proxy can be collocated with the IoT gateway.

IV. Background to IPv6

Recent development of IoT technologies, including the transport of IP over low-power radio technologies, have concentrated almost solely on IPv6. For example, only IPv6 support for 802.15.4 has been defined. An IPv6 address is a 128-bit fixed length numerical address consisting of a *subnet prefix* and an *Interface Identifier* (IID) portions. The length of the prefix and the IID can vary based on link type, but typically a 64-bit prefix, and hence also 64-bit IID, is used for address configuration. The split at 64-bit boundary has become the industry standard in the most common IPv6 implementations. Thus, most if not all of the current implementations have been designed with the assumption of 64-bit IID length.

The bits for the IID can be selected in several different ways depending on the use-case and deployment scenario, as described below. Additionally, the relatively large size of 64-bit IID has fostered innovations where meaningful information is encoded within IIDs.

- **Modified EUI-64-based IIDs**: A globally unique IID generated from network interface's globally unique identifier, such as IEEE 802 48-bit MAC address.
- **Privacy Addresses**: An IID generated using pseudo-random algorithms, if a globally unique identifier is not available, or if a host wishes to improve privacy by making IID-based tracking impossible.
- **Cryptographically Generated Addresses**: For securing IPv6 Neighbor Discovery procedures, IIDs may be derived from public keys and signed using private keys. These are seldom used.

A. IPv6 Addressing Architecture

The IPv6 address architecture defines two *scopes* for unicast addresses: link-local and global. *Link-local addresses* are used for auto-discovery and auto-configuration, and at least one is always configured for each interface of a node. IPv6 packets using link-local addresses will not be forwarded by routers to other links, as the link-local addresses are not guaranteed to be unique over a larger network. The global scope addresses, on the other hand, are expected to be globally unique and can be used in the scope of the whole Internet. A node needs a global IP address to be able to communicate over the Internet.

Unique Local Addresses (ULA) [18] are designed to be used in local networks larger than a single link, but not for communications through the Internet. However, ULA are designed to provide adequate uniqueness in order to have extremely small risk of address collision. These addresses are intended to allow routing over a network that expands over multiple links and routing hops, and even can expand over multiple networks. The address independence from the Internet's global routing system, and address administration, is a desired characteristic in some deployments. ULA may provide address stability and independence from an outside provider such as the operator, but come with the cost of limiting the communications' scope.

Globally Unique Addresses (GUA) are globally administratively guaranteed to be unique and routable in the Internet. The administration is done by the Internet Assigned Number Authority (IANA), which administers the global pool of addresses, and by the Regional Internet Registries (RIRs) who administer address space received from IANA regionally. The RIRs provide address space to the Local Internet Registries (LIRs) - operators, companies, and other organizations, who require address space for themselves, and possibly for further allocation to their customers.

B. Host Address Configuration

The IPv6 protocol suite defines a set of well-known mechanisms for address autoconfiguration on an attached link. These are Stateless Address Autoconfiguration (SLAAC) and Stateful Address Autoconfiguration, the latter being nowadays synonymous with the Dynamic Host Configuration Protocol version 6 (DHCPv6). In addition, in the case of Virtual Private Networks (VPN), Internet Key Exchange version 2 (IKEv2) can be used for address configuration.

SLAAC has been designed to provide simplest possible, yet dynamic, way for nodes to configure IPv6 addresses for themselves. With SLAAC, hosts must configure *link-local addresses* for all interfaces they use IPv6 on. The link-local address can be configured even in absence of routers. The routers on networks transmit ICMPv6 Router Advertisement (RA) messages that may include IPv6 prefixes, which nodes can use to configure one or more ULA or GUA addresses. Once a node receives RA, it will parse it and select one or more 64-bit IPv6 prefixes for combination with selected 64-bit IIDs in order to create one or more 128-bit IPv6 addresses. SLAAC is the most scalable of the mechanisms, as it does not require the network to know which nodes exist and which addresses they have configured.

DHCPv6 can be used to explicitly configure IPv6 addresses to nodes, thereby providing network administrators with added

control over the nodes on their networks. Hence DHCPv6 is popular in environments where stricter control is required, such as in enterprise networks. In addition, DHCPv6 can be used for prefix delegation[16]. In prefix delegation, a router is given the responsibility over a shorter prefix from which it can advertise longer prefixes to the network segments under its responsibility. DHCPv6 requires the DHCP server to keep state on the allocated addresses. Hence, it provides more control on the addresses, but less scalability than SLAAC.

Obviously IPv6 protocol suite supports manual configuration of addresses, and this can include provisioning of addresses with mechanisms other than SLAAC or DHCPv6, including proprietary out-of-band tools. Provisioning or manual configuration is the least scalable of these approaches.

C. Remote Address Anchor Points

IPv6 hosts will always configure addresses from the point of network attachment, but additionally hosts may have addresses configured from remote anchor points. These addresses belong topologically to locations other than the hosts' direct points of network attachment. In order for the hosts to be able to use these addresses, tunneling of sorts is is required. These tunneling solutions include client-based Mobile IPv6 (MIPv6), Network Mobility (NEMO)[17], or Dual-Stack Mobile IPv6 (DS-MIPv6)[20], but also gateway-based solutions exist, such as Proxy Mobile IPv6 (PMIPv6)[19].

D. Network Prefix Translation

If hosts do not require direct visibility for global addresses, it might be feasible to number a network with ULA and utilize experimental IPv6-to-IPv6 Network Prefix Translation (NPTv6)[21] at the gateway. NPTv6 differs from traditional port and address translating NAT in that it translates in checksum neutral way and only the prefix part and not the transport layer protocol port number. If reachability from Internet to nodes numbered in such a setup is needed, the nodes need to register their public IPv6 address, the address on the Internet side of the gateway, to the used rendezvous system. Other forms of IPv6 address translation, namely NAT66, have also been discussed and speculated, but not adopted into use even in an experimental manner.

V. Topologies for IoT Deployments

The network topologies for which addressing needs are considered in this paper and that are explained in this section are illustrated in Figures 2 and 3. These topologies can be extended to more complex topologies with variations, as we will discuss in the end of the section.

A. Case A: Disconnected IoT Network Without a Central Node

A disconnected IoT LAN may have no Internet connectivity, but only connectivity within a link itself. The underlying medium may provide mesh, star, or shared connectivity, but nevertheless IPv6-wise nodes are in a single link without any router. Hence, there is no entity in the network providing numbering services - ULA or GUA prefixes. In this kind of topology, the main requirement for addressing is that IoT nodes must be able to automatically number themselves. As the automatic numbering has to be in very simple in some cases, the IPv6 addresses may be statically configured. To be clear, routable addresses are not needed, as the network is not connected to other networks, such as to the Internet. The absence of routers restricts the nodes to be on the same link in this scenario. Therefore, the most suitable address type is IPv6 link-local addresses.

B. Case B: Network With an IoT proxy

In the case B, the IoT LAN has been enhanced with an IoT proxy, which is able to provide addresses and possibly connectivity services for the IoT nodes in the IoT LAN. The IoT proxy can have permanent or intermittent connectivity to the external network, or in some cases without connectivity. When the IoT proxy has uplink connectivity, it proxies communication between the local IoT nodes and nodes in the external network. In this scenario, where all communications go through a proxy, the IoT LAN does not need global addressing, but can manage with link-local or ULA addresses, depending on the type of proxy.

C. Case C: Connected IoT network

This is a typical setup for providing IoT nodes with Internet connectivity. An Internet connected IoT gateway provides Internet connectivity to the IoT LAN. The IoT gateway receives a globally routable IPv6 prefix from the Internet service provider, and uses that prefix to number the nodes in the IoT LAN. The different mechanisms for obtaining the IPv6 prefixes are further described in Section VII. This scenario allows the IoT nodes in the LAN to be provided with a globally routable address. In addition, the IoT nodes, which communicate only within their own link, may use link-local addresses, and the IoT gateway may also provide ULA addresses to the IoT nodes.

D. Case D: An IoT Network with Bridging Star Topology

In some scenarios a gateway is a center of a network utilizing star topology. In such a network the same IPv6 prefix can be shared by nodes connected via point-to-point links to a gateway, and the gateway may implement a bridge. This approach is used for ongoing IETF work on IPv6 transmission over Bluetooth Low-Energy[23]. Also IoT deployment scenarios exist that emulate a bridging star topology, but having only the gateway maintain IPv6 representational states for extremely simple IoT nodes which do not implement IPv6 at all. For example, sensors connect and communicate to an IPv6 gateway with 1-wire or a similar solution without being IPv6-aware. The gateway however allocates IPv6 addresses and internally maintains a 1:1 IPv6 to a proprietary ID mapping for each node.

E. Case E: A Point-to-Point Network with an Internet Gateway

The scenario E is very similar to scenario D, except that the IoT nodes are not on a same link. Instead, they are connected to the IoT Gateway via their own links. Hence communication using link-local addresses is not possible between IoT nodes.

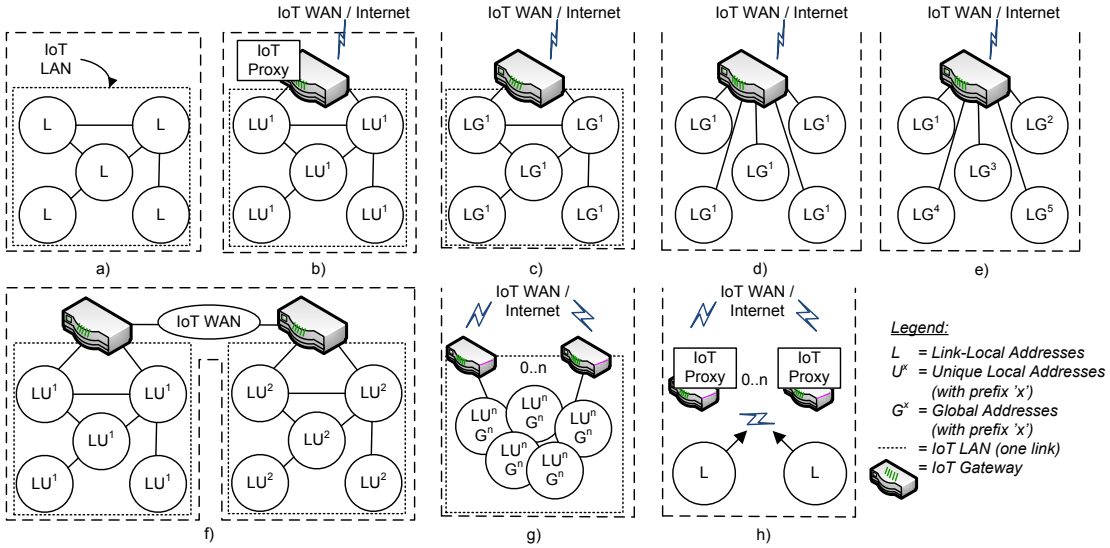

Figure 2: Set of IoT LAN Network Setups

F. Case F: Interconnected IoT Networks

When it comes to more advanced scenarios, two or more IoT LANs can be connected to each other via a shared link or through an IoT WAN. In this kind of case, the IoT nodes of different LANs are obviously not on a shared link with each other. Hence, the communication between them is not possible with link-local addresses. If the IoT nodes need to communicate with nodes on different network segments, used addresses have to be either ULA or GUA, depending on the network that is between the gateways. If the network is the Internet, globally routable IPv6 addresses have to be used within the network. Otherwise, the ULA will suffice. In addition, in cases where, for instance, the Internet connectivity is not always available, both address scopes can be used.

G. Case G: Multiple Gateways

The topologies described earlier represent the different basic topologies. There are, however, variations to these basic topologies that introduce additional addressing requirements. For instance, there can be multiple gateways connecting an IoT LAN to the Internet, or to the Internet and a private wide area network - such as a corporate network - therefore, making the IoT LAN multihomed. If the IoT nodes need to be reachable from both networks, the IoT nodes need to have addresses from the both networks. Consequently, the IoT nodes may need to have multiple addresses of global scope.

H. Case H: Unidirectional IoT Nodes

A significantly different approach for using IPv6 with IoT nodes is to run IPv6 over unidirectional links, or put otherwise: have send-only IoT nodes. The unidirectional approach is not fully compatible with existing IPv6 addressing solutions, as all of those assume bidirectional communications channel for Duplicate Address Detection, and for other signaling. However, in some cases it might be an attractive use case to utilize IPv6 even in such situations. For example, sensors could be reporting readings using IP multicast. One way to address nodes in such deployment is to trust link-local addresses to be unique, hard-code them, and use link-local multicast as destination address[22].

I. Variations of the Basic Topologies

In addition to the topology variations, the topologies can also be combined. For instance, in the same IoT LAN some nodes may be connected directly to Internet using global addresses, and some nodes may utilize ULA or link-local addresses for local communications or communicatios via a proxy. In these cases, even if the addressing requirements may vary between IoT nodes within the same network, it is important to remember that nodes which communicate between each other need to have an address of the same scope.

VI. Mobility Implications to Addressing

Movement in IP networks is related to the topological location of the network. Hence, virtually any event where the IPv6 prefix changes is considered movement. The IoT networks may either be stationary, or mobile. Thus, due to an event that causes renumbering of an IoT network, such as the loss and regain of Internet access with a prefix change, even a stationary network may move in the IP network topology. This generates challenges to the addressing of an IoT network. Figure 3 illustrates network movement and its implications to addresses. In the following, we will briefly describe mobility scenarios relevant to IoT networks.

1) The IoT network initially uses IPv6 global prefix 'A'. Due to movement or a renumbering event, the network is renumbered with global prefix 'B'. The IoT LAN is capable of renumbering, and hence resilient to movement.
2) As above, the IoT Gateway's WAN-side addressing changes. However, in the IoT LAN addressing is expected to stay stable. For instance, IoT nodes may be

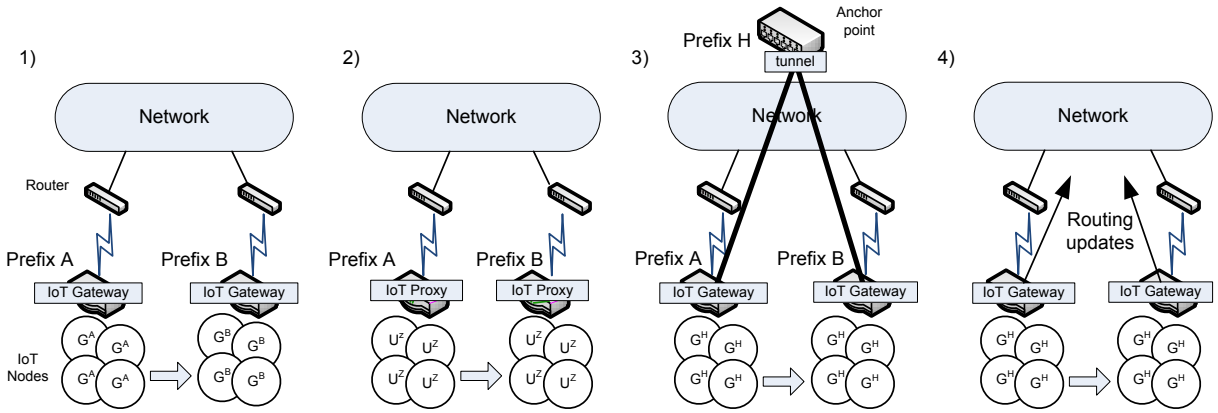

Figure 3: Mobility for IoT Networks

sleeping for extended periods and propagation of the new prefix would take long. Hence, the IoT network utilizes an addressing scheme independent from the addressing used to connect to the Internet - for instance, a ULA prefix ('U^Z' in Figure 3). The IoT gateway must isolate the IoT LAN's internal addressing from the global addressing with a mediation function such as a proxy.

3) In certain use cases it is expected that the IoT nodes' global addresses stay stable regardless of the address stability of the access network. An example is when the IoT nodes are expected to be reachable from the Internet, and their addresses are stored in some semi-permanent database such as the Domain Name System (DNS). In this case, IoT network must be numbered with a prefix topologically anchored to a different location ('H' in Figure 3) than where the gateway is actually attached. In this case, there is a tunnel to a remote anchor point. As the IoT gateway's uplink prefix changes from 'A' to 'B', no renumbering of IoT nodes takes place as the nodes' communications are using global prefix 'G^H' and always routed via the remote anchor.
4) In some deployments the gateway might have ability to make dynamic routing updates to the network, and hence the prefix used in the IoT LAN can remain functional even during movements. Essentially, the IoT LAN would move within the network topology. Applicability of this approach is limited to networks and IoT WANs, that allow such routing updates from IoT gateways, that do not leak updates to the Internet, that can handle the numbers of routing updates, and that contain IoT nodes tolerating delays caused by routing information propagation through the network.

As with the topology scenarios, the mobility scenarios can be combined in one network. An IoT LAN can be comprised of multiple different types of nodes that have different requirements for the connectivity. For instance, some of the nodes can be renumbered, some use either link-local or ULA for address stability, and there may be even nodes that require stable global addresses. This is dependent on the use case of specific nodes.

VII. Address Allocation Solutions

In the previous two sections, we discussed the different addressing requirements related to topology, mobility and resilience. In this section, we discuss solutions fulfilling the identified requirements. As the IoT gateway (possibly with proxy functionalities) is the element that provides the IoT LAN with Internet connectivity, it also has a central role in the IoT LAN address management. Thus, many of the following solutions place functional requirements on the IoT Gateway.

A. Allocating Addresses for IoT Nodes

The same mechanisms are used for address allocation of IoT nodes as other nodes in the Internet - Stateless Address Autoconfiguration (SLAAC), and Dynamic Host Configuration Protocol for IPv6 (DHCPv6). These mechanisms were described in Section IV-B in detail. Additionally, the nodes can be statically configured in different ways, an address can be configured over a management interface, or a node may use IPv6 address based on a hardcoded hardware identifier. A static IID may be helpful in scenarios where node identification based on IPv6 address is a requirement.

Considering the requirements of Section V, the most relevant mechanism for IoT node addressing is SLAAC with ULA or GUA addresses depending on the deployment scenario. A hardware-based or dynamically selected IID can be used for creating link-local address, ULA or GUA. However, link-local addresses based on hardware identifiers are practically the only choice of addressing in setups where IoT nodes do not have receive capabilities, and hence cannot perform Duplicate Address Detection procedure.

Static configuration through a management interface could be used, but the high operational maintenance cost, due to reconfiguration effort in the case of network address renumbering, makes it an impractical approach for IoT.

Hardcoding addresses, during manufacturing or by reflashing of IoT node firmware, of any other scope than link-local is not advisable. The network topology, and environment cannot be sufficiently known during manufacturing, and the network topology can significantly outlive the lifetime of an IoT node making this approach too restrictive. An IoT node with a topologically incorrect address would be unreachable,

and transmissions of packets with improper addresses would likely fail due to routers' source address validation filters.

B. IoT Gateway/Proxy

IoT Gateway and IoT Proxy play central nodes in allocating addresses to the IoT nodes, because they are the routers in the IoT LAN and responsible for both the Internet connectivity and possibly connectivity between IoT LANs. In the scenarios C, D, E, and G, illustrated in Figure 2, the gateway advertises globally routable prefixes, which are used by IoT nodes to configure addresses with SLAAC. The IoT Gateway must obtain prefixes from the upstream network with mechanisms such as DHCPv6 Prefix Delegation. In addition to globally routable prefixes, and regardless of the presence of Internet connectivity, an IoT Gateway or IoT Proxy may also generate an ULA prefix, as illustrated in scenarios B, F, and G, and advertise it to the IoT LAN. As ULA addresses can be generated and maintained independently from global addresses or Internet connectivity, ULA is a good choice for IoT LAN addressing in use cases where internal address stability is important or connectivity to other IoT LANs is required.

The simplest of IoT nodes might only deliver data to the closest IoT Proxy, as illustrated in scenario H in Figure 2, which could furthermore aggregate data from multiple nodes. In these cases, having ULA or GUA in use might be either computationally exhaustive, or simply unnecessary. The simplest nodes could manage with link-local addresses, and utilize link-local multicast address as the destination address of their packets. The IoT Proxy would gather packets sent to the link-local multicast group, and proxy them forward.

When ULAs are used for providing address stability, but IoT Nodes need to communicate to the Internet, the IoT Proxy may need to implement application layer proxy, or possibly the IoT Gateway may need to support the experimental NPTv6. An application layer proxy could also perform other processing as well, in addition to just passing data between the Internet and the IoT Nodes. For example, the proxy could enrich the information sent by IoT Nodes. Use of NPTv6 cannot be recommended at this point of time, as the technology is experimental and more research is needed generally, and in particular in case of IoT, to assess its usability.

Until the Internet has fully transitioned to IPv6, the IoT gateway may only have an IPv4-only uplink. Despite significant efforts by the community to design a perfect IPv6 transition solution, no universal solution has been found despite the availability of a toolbox of various tricks. Due to the challenges in transition, forthcoming IoT deployments should be designed to have native IPv6 connectivity. Otherwise, suboptimal alternatives have to be chosen belonging to three categories: protocol translation from IPv6 to IPv4 (e.g. NAT64), tunneling IPv6 packets over the IPv4 (e.g. 6to4), and data relaying (e.g. application layer proxies).

C. Global Address Stability

As stated above, ULAs can provide address stability within the IoT LAN but with a cost. However, in certain scenarios the IoT network, be it physically mobile or not, may require globally routable addresses. IoT nodes or gateways have to implement ways to inform upstream network about IoT LAN, or node, movement. The solutions include tunneling based approaches discussed herein, or use of routing protocols discussed in Section VII-E.

Host-based mobility, such as DS-MIPv6, can be supported by computationally capable IoT nodes, but is unlikely to be supported by constrained nodes of any form. If the number of IoT nodes in an IoT LAN is large, the signalling load to the DS-MIPv6 tunneling end-point (Home Agent) - would become an issue. In addition to host mobility, DS-MIPv6 supports network mobility. Therefore, a more suitable place to terminate DS-MIPv6 is the IoT Gateway.

As explained earlier, other mobility management technologies in addition to DS-MIPv6 do exist for IPv6 including MIPv6, NEMO and PMIPv6. However, these technologies have limitations that make them inferior in the IoT context. MIPv6, and NEMO are constrained to work only on IPv6 which is a serious restriction in the beginning of IoT deployments, as currently, many networks are still IPv4 only capable. DS-MIPv6 supports tunneling to the Home Agent (HA) even over IPv4, and it works also in IPv6 only environments. Thus, it is both a good solution now when IPv6 is not ubiquitously available, and it is future proof. PMIPv6, on the other hand, is made for network based mobility management. It means that the access network has to provide the mobility management. Therefore, it is only available as a solution as an operator provided service.

D. Upstream Bridging

In some cases, address delegation mechanisms such as DHCPv6 Prefix Delegation may not be available. The IoT Gateway may be provided a single /64 prefix, from which it obviously cannot delegate prefixes to the IoT LAN. This scenario is present today, for instance, in 3GPP networks where a mobile device is allocated a single /64 prefix. In this case, the IoT Gateway has to somehow "bridge" between the upstream provider and the IoT LAN. This problem is topical in the IETF, as all proposals for this problem, this far, have all had some issues.

E. Routing

In cases where the IoT LAN is considerably big and independently operated, dynamic address allocation via DHCPv6 may not provide enough address stability and be sufficiently scalable. As with any relatively big networks, the interface between the IoT LAN, and its upstream network or networks can be done with routing. When the IoT LAN is served by one operator, and the IoT LAN has its address space from that operator, interior routing protocols such as OSPF and IS-IS may be feasible. In topologies where there are multiple segments and routers within the IoT WAN, IoT LANs may also use routing protocols for location updates. The IETF is working on such scenarios in the Homenet Working Group, which has been concentrating on the use of OSPF protocol.

F. Multihoming

Both networks, and nodes can be multihomed. We described use cases where multihoming may be needed in Section II. As small networks, such as home IoT LANs, cannot afford to have their own address space, a multihomed IoT LAN would have different prefixes from different Internet connections. Different approaches to this problem exist. The two main approaches are described in the following.

Proxy based approach: Either one proxy manages multiple upstream connections with their relative IP addresses, or there are separate IoT Proxies per upstream connection. In addition to the different proxies, an IoT Gateway providing a prefix from an upstream link can be provided.

Separate IoT Gateways: Multiple IoT Gateways provide their own address space to the IoT LAN, and the IoT Nodes are multihomed.

The first scenario above is relatively straightforward as the nodes would not be aware of multihoming. However, there may be cases where that approach is too restrictive. The communication between the node, and the upstream network is isolated by the proxy, which may not be desirable.

The challenge of multihoming is the multihomed node has to know, which source address to use in communication depending on the destination, and the IoT LAN originated packets have to be routed over the correct IoT Gateway. For upstream IoT Gateway selection, routing protocols can be used between the Gateways. However, the IPv6 source address selection rules may provide suboptimal results if the destination address and source address are not derived from the same prefix. Otherwise, the multihomed node has to use policy information to select the correct source address. However, currently no defined solution exists to convey such information. The IETF has worked on multihoming solutions, such as in the Multiple Interfaces (MIF) Working Group, but currently there is no consensus on the solution.

VIII. Conclusion

Device heterogeneity, IP networks interoperating with non-IP networks, and the amount of connected, unique entities are defining features of the IoT. The configuration schemes used to number IoT nodes are largely similar to current practices for numbering standard nodes. The bigger question is more often what address scopes to use and when, as we've demonstrated herein. However, the more constrained the IoT device, the more challenges emerge and areas for improvement appear. For constrained IoT nodes, mobility, multihoming, and generally renumbering events are resource consuming due to an increased need to monitor movement and refresh addresses. Mobility with help of remote anchor points requires more infrastructure, routing-based mobility poses scalability issues, and if these mobility events are hidden with the use of ULA, IoT gateways are required to implement non-transparent mediation functions. Similar requirements also arise from IoT nodes that operate in unidirectional mode, and are unable to configure global scoped addresses for themselves. These mediation functions can, for example, take the shape of application layer proxies or perhaps even perform translation via NPTv6. It is also entirely possible we may encounter situations where even the most constrained nodes can use IPv6, but are not addressable with, or may completely disregard obtaining IPv6 addresses. This may even be desirable in certain scenarios. If not, however, it might be wise to define lightweight, IPv6-friendly, and generic mediation functions. We anticipate further research by both the academy and the industry for discovering how, and if even the most constrained nodes could somehow be efficiently addressed with global scoped IPv6 addresses.

IX. Acknowledgements

This work was supported by authors' employers and in part by TIVIT's Internet of Things research program, Finland.

References

[1] International Data Corporation (IDC), "Nearly 1 Billion Smart Connected Devices Shipped in 2011 with Shipments Expected to Double by 2016", IDC Press Release, http://www.idc.com/getdoc.jsp?containerId=prUS23398412, 2012.

[2] Cisco Systems, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything", White Paper, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, 2011.

[3] ITU Broadband Commission, "The State of Broadband 2012: Achieving Digital Inclusion for All", ITU Broadband Commission Report, http://www.broadbandcommission.org/Documents/bb-annualreport2012.pdf, 2012.

[4] Ericsson, "More than 50 Billion Connected Devices", White Paper, http://www.ericsson.com/res/docs/whitepapers/wp50billions.pdf, 2011.

[5] ITU, "The Internet of Things", International Telecommunication Union Internet Reports, 2005.

[6] P. Neves and J. Rodrigues, "Internet Protocol over Wireless Sensor Networks, from Myth to Reality", Journal of Communications, Vol 5, No 3 (2010), 189-196, 2010.

[7] C. Cheng, C. Chuang and R. Chang, "Three-Dimensional Location-Based IPv6 Addressing for Wireless Sensor Networks in Smart Grid," Proc. IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), pp. 824-831 2012.

[8] S. Hyojeong, E. Talipov and C. Hojung, "IPv6 lightweight stateless address autoconfiguration for 6LoWPAN using color coordinators," Proc. IEEE International Conference on Pervasive Computing and Communications(PerCom) 2009, pp. 1-9 2009.

[9] X. Wang and Y. Mu, "A secure IPv6 address configuration scheme for a MANET", Security and Communcations Networks, 2012 :Wiley

[10] K. Zhang, D. Han and H. Feng, "Research on the complexity in Internet of Things," Proc. 2010 International Conference on Advanced Intelligence and Awareness Internet (AIAI 2010), pp.395-398, 2010.

[11] I.F. Akyildiz and J.M Jornet, "The Internet of nano-things," IEEE Wireless Communications, vol.17, no.6, pp.58-63, 2010.

[12] G. Jayavardhana, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." arXiv preprint arXiv:1207.0203 2012.

[13] IEEE-TG15.4, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE standard for Information Technology, 2003.

[14] C. Bormann, M. Ersue and A. Keranen "Terminology for Constrained Node Networks", IETF Internet Draft draft-ietf-lwig-terminology-03 (work in progress), 2013.

[15] M. Lamppi, "Ambient Energy Harvesting", Proc. Aalto University T-106.5840 Seminar on embedded systems, https://wiki.aalto.fi/display/esgsem/2011S-iot, 2011.

[16] O. Troan and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", IETF RFC 3633, 2003.

[17] V. Deverapalli, R. Wikikawa, A. Petresku and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", IETF RFC3963, 2005.

[18] R. Hinden and B. Haberman, "Unique Local IPv6 Unicast Addresses", IETF, RFC 4193, 2005.

[19] S. Gundavelli (Ed.), "Proxy Mobile IPv6", IETF RFC 5213, 2008.

[20] H. Soliman H (Ed.), "Mobile IPv6 Support for Dual Stack Hosts and Routers", IETF RFC 5555, 2009.
[21] M. Wasserman and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", IETF RFC 6296, 2011.
[22] J. Arkko, H. Rissanen, S. Loreto, Z. Turanyi and O. Novo, "Implementing Tiny COAP Sensors", draft-arkko-core-sleepy-sensors-01 (work-in-progress), 2011.
[23] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby and C. Gomez, "Transmission of IPv6 Packets over BLUETOOTH Low Energy", draft-ietf-6lowpan-btle-12 (work-in-progress), 2013.

BIOGRAPHIES

Teemu Savolainen received his M.Sc of Information Technology in 2011 from Tampere University of Technology, Finland. He is Principal Researcher and inventor at Nokia and has worked on wireless networking with emphasis on IPv6 enabled mobile handsets since 1999. Teemu has been actively contributing to the IPv6 related standards at IETF, 3GPP, and lately at Bluetooth SIG for standardization of IPv6 over Bluetooth Low-Energy. He is co-authoring a book with Jonne Soininen about "Deploying IPv6 in 3GPP Networks".

Jonne Soininen, M.Sc from University of Helsinki, is Head of Standardization Strategy at Renesas Mobile. He has been working on IPv6 support for IETF and 3GPP standards and networks since late 90s. Jonne has been active in different standards organizations contributing to the evolution of IPv6 and mobile cellular networks both from technical and regulatory angle. He has co-authored "Deploying IPv6 in 3GPP Networks" with Teemu Savolainen.

Bilhanan Silverajan received his M.Sc in Engineering from Lappeenranta University of Technology, Finland in 1998 and his B.Sc in Computer Engineering from Nanyang Technological University, Singapore in 1993. He is currently pursuing his PhD in Tampere University of Technology. His research interests include pervasive networking, service discovery, communications middleware and constrained protocols for the Internet of Things.