A Standardized and Flexible IPv6 Architecture for Field Area Networks

Smart Grid Last Mile Infrastructure

Rob Kopmeiners, AMI Consultant—Alliander, rob.kopmeiners@alliander.com

Phillip King, Manager, Telecommunications Development—Ausgrid Operational Technology & Innovation, pking@ausgrid.com.au

Jeff Fry, Manager, Technology Innovation—Ausgrid, JFry@ausgrid.com.au

John Lilleyman, Chief technology Architect—BC Hydro, john.lilleyman@bchydro.com

Sol Lancashire, Telecom Architect—BC Hydro, sol.lancashire@bchydro.com

LIU Dong, CEO—BII Group, dliu@biigroup.com

Feng Ming, Network Division Technical department—China Telecom, fengm@chinatelecom.com.cn

Patrick Grossetete, Technical Marketing Engineer—Cisco, pgrosset@cisco.com

Jean-Philippe Vasseur, Cisco Fellow—Cisco, jpv@cisco.com

Matthew K Gillmore, Director of Enterprise Architecture and Standards—Consumer Energy, mkgillmore@cmsenergy.com

Nicolas Déjean, Elster, nicolas.dejean@coronis.com

David Mohler, CTO and SVP—Duke Energy, david.mohler@duke-energy.com

Gary Stuebing, Strategic Product Development—Duke Energy, gary.stuebing@duke-energy.com

Steve Haemelinck, Enterprise Consultant—EANDIS, info@earchitect.be

Michael John, Elster, Michael.John@elster.com

Bernard Tourancheau, Professor University Joseph Fourier of Grenoble—INRIA, Bernard.Tourancheau@INRIA.fr

Daniel Popa, CTO office—Itron, Daniel.Popa@itron.com

Jorjeta Jetcheva, CTO office—Itron, jorjeta.jetcheva@itron.com

Don Shaver, Texas Instruments Inc. Fellow—Texas Instruments Inc., shaver@ti.com

Cedric Chauvenet, Wattecco, c.chauvenet@watteco.com

Last update: December 9th, 2011

This paper is intended to provide a synthetic and holistic view of open standards Internet Protocol version 6 (IPv6) based architecture for Smart Grid Last Mile Infrastructures in support of a number of advanced Smart Grid applications (meter readout, demand-response, telemetry, and grid monitoring and automation) and its benefit as a true Multi-Services platform. In this paper, we show how the various building blocks of IPv6 networking infrastructure can provide an efficient, flexible, secure, and multi-service network based on open standards.

In order to discuss transition paths for electric utilities that deal with such issues as legacy device, network and application integration, and the operation of hybrid network structures during transitional rollouts, a follow-up paper will need to be developed.

1. Introduction

Last mile networks have gained considerable momentum over the past few years due to their prominent role in the Smart Grid infrastructure. These networks—referred as Neighborhood Area Networks (NAN) in this document—support a variety of applications including not only electricity usage measurement and management, but also advanced applications such as Demand-Response (DR), which gives users the opportunity to optimize their energy usage based on real-time electricity pricing information, Distribution Automation (DA), which allows distribution monitoring and control, and automatic fault detection, isolation and management, and serves as a foundation for future Virtual Power Plants, which comprise distributed power generation, residential energy storage (e.g., in combination with Electric Vehicle (EV) charging), and small scale trading communities.

Field Area Networks (FAN)—the combination of NAN and communication device offering the backhaul WAN interface(s)—have emerged as a central component of the Smart Grid network infrastructure. In fact, they can serve as backhaul networks for a variety of other electric grid control devices; multi-tenant services (gas and water meters), and data exchanges to Home Area Network (HAN) devices, all connected through a variety of wireless or wired line technologies. This has created the need for deploying the IP (Internet Protocol) suite of protocols, enabling the use of open-standards that provide the reliability, scalability, security, inter-networking and flexibility required to cope with the fast-growing number of critical applications for the electric grid that distribution power networks need to support. IP also facilitates integration of the Neighborhood Area Networks (NAN) into end-to-end network architecture.

One application being run over Field Area Networks is meter reading, where each meter periodically reports usage data to a utility head-end application server. The majority of meter traffic was thus directed from the meter network to the utility network in a Multipoint-to-Point (MP2P) fashion. With the emergence and proliferation of applications such as Demand Response, distributed energy resource integration and Electrical Vehicle charging, it is expected that the traffic volume across the Field Area Networks would increase substantially and traffic patterns and bi-directional communication requirements would become significantly more complex. In particular, Field Area Networks are expected to support a number of use cases leveraging network services:

- **Communication with an individual meter.** On-demand meter reading, real-time alert reporting, and shutdown of power to a single location require Point-to-Point (P2P) communication between the NMS/Head-end and the electric meter and vice versa.
- **Communication among DA devices.** Subsets of DA devices need to communicate with each other in order to manage and control the operation of the electric grid in a given area, requiring the use of flexible communication with each other, including Peer-to-Peer in some cases.
- **HAN applications.** HAN applications typically require communication between home appliances and the utility head-end server through individual meters acting as application's gateways. For example, a user may activate Direct Load Control (DLC) capabilities, empowering the utility company to turn off or down certain home appliances remotely (e.g. A/C, washer/dryer), when demand and/or the cost of electricity is high.

- **Electric Vehicle Charging.** Users need to have access to their individual vehicle charging account information while away from home in order to be able to charge their vehicles while on the road or while visiting friends. Verifying user and account information would require communication through the meter to the utility head-end servers from potentially a large set of nomadic vehicles being charged simultaneously from dynamic locations.
- **Multi-Tenant Services.** Combining information at the customer side and differentiating information into several services at the other side devises for a complex Multipoint-to-Multipoint network (MP2MP). For example, this could be a converged network connecting devices from multiple utilities as suggested by the UK national multi-utility telecom operator DCC or Germany multi-utility communication box as specified in Open Meter Systems.
- **Security.** Strong authentication mechanisms for validating devices that connect to the Advanced Metering Infrastructure (AMI) network as well as encryption for data privacy and network protection.
- **Network Management.** As the FAN carries increasingly more traffic and is subject to stringent Service Level Objectives (SLOs), managing network-related data becomes critical to monitoring and maintaining network health and performance. This would require the communication of grid status and communications statistics from the meters to the Network Management System (NMS)/Head-end in a MP2P fashion.
- **Multicast Services.** Groups of meters may need to be addressed simultaneously using multicast, e.g., to enable software upgrade or parameters updates sent by a network management system (NMS) to all meters using multicast requests, and multicast queries for meter readings of various subsets of the meters.

2. The Key Advantages of Internet Protocol

An end-to-end IP Smart-Grid architecture can leverage 30 years of Internet Protocol technology development [RFC 6272] guaranteeing open standards and interoperability as largely demonstrated through the daily use of the Internet and its two billion end-users [Stats].

Note—*Using the Internet protocol suite does not mean that an infrastructure running IP has to be an open or publicly accessible network–indeed, many existing mission-critical but private and highly secure networks leverage the IP architecture, such as inter-banking networks, military and defense networks, and public-safety and emergency-response networks, to name a few.*

One of the differences between Information and Communications Technology (ICT) and the more traditional power industry is the lifetime of technologies. Selecting the IP layered stack for AMI infrastructure brings future proofing through smooth evolutionary steps that do not modify the entire industrial workflow. Key benefits of IP for a distribution system operator (DSO) are:

- **Open and Standards-based:** Core components of the network, transport and applications layers standardized by the Internet Engineering Task Force (IETF) while key physical, data link, and applications protocols come from usual industrial organizations, such as, IEC, ANSI, DLMS/COSEM, SAE, IEEE, ITU, etc.
- **Lightweight:** Devices installed in the last mile of an AMI network such as smart meters, sensors, and actuators are not like PC and servers. They have limited resources in terms of power, CPU, memory, and storage. Therefore, an embedded networking stack must work on few kilobits of RAM and a few dozen kilobits of Flash memory. It has been demonstrated over the past years that production IP stacks perform well in such constrained environments. (See [IP-light])

- **Versatile:** Last mile infrastructure in Smart Grid has to deal with two key challenges. First, one given technology (wireless or wired) may not fit all field deployment's criteria. Second, communication technologies evolve at a pace faster than the expected 15 to 20 years lifetime of a smart meter. The layered IP architecture is well equipped to cope with any type of physical and data link layers, making it future proof as various media can be used in a deployment and, over time, without changing the whole solution architecture and data flow.
- **Ubiquitous:** All recent operating systems releases from general-purpose computers and servers to lightweight embedded systems (TinyOS, Contiki, etc.) have an integrated dual (IPv4 and IPv6) IP stack that gets enhanced over time. This makes a new networking feature set easier to adapt over time.
- **Scalable:** As the common protocol of the Internet, IP has been massively deployed and tested for robust scalability. Millions of private or public IP infrastructure nodes, managed under a single entity (similarly to what is expected for FAN deployments) have been operational for years, offering strong foundations for newcomers not familiar with IP network management.
- **Manageable and Secure:** Communication infrastructure requires appropriate management and security capabilities for proper operations. One of the benefits of 30 years of operational IP networks is its set of well-understood network management and security protocols, mechanisms, and toolsets that are widely available. Adopting IP network management also helps utility operational business application by leveraging network-management tools to improve their services, for example when identifying power outage coverage through the help of the Network Management System (NMS).
- **Stable and resilient:** With more than 30 years of existence, it is no longer a question that IP is a workable solution considering its large and well-established knowledge base. More important for Field Area Networks is how we can leverage the years of experience accumulated by critical infrastructures, such as financial and defense networks as well as critical services such as Voice and Video that have already transitioned from closed environments to open IP standards. It also benefits from a large ecosystem of IT professionals that can help designing, deploying and operating the system solution.
- **End-to-end:** The adoption of IP provides end-to-end and bi-directional communication capabilities between any devices in the network. Centralized or distributed architecture for data manipulations are implemented according to business requirements. The removal of intermediate protocol translation gateways facilitates the introduction of new services.

3. An IPv6 Distribution Network Architecture

The networking requirements for Neighborhood Area Networks have been extensively documented: cost efficiency, scalability (millions of nodes in a network is common), security, reliability and flexibility are absolute musts, and technologies based on open standards and the future proofing of 15 to 20 years lifetime are minimum expectations from utilities. This explains why the IPv6 suite was the initial protocol of choice, although new IPv6 protocols have been designed to address the unique requirements of such networks, as discussed in the next chapter.

The adoption of IPv6 facilitates a successful transformation to connected energy network in the last mile. However, before describing in greater detail IPv6 networking components such as IP addressing, security, Quality of Service (QoS), and routing and network management, it is worth asking why should we use end-to-end IPv6? After all, IPv6 as any other technologies requires appropriate education to the whole workforce, from technicians to the executives evaluating vendors, subcontractors and contractors.

One of the major steps in favor of building the momentum around using IP end-to-end in the last mile of Smart Grid networks was to demonstrate that IP could be light enough to be used on constrained devices with limited resources in terms of energy, memory, and processing power. Thus FANs were seen as single application, stub

networks with end nodes such as meters not running IP that could be reached through IP through protocol-translation gateways, with each gateway being tied to a dedicated service and/or solution's vendor.

The past two decades, with the transition of protocols such as SNA (through DLSw), Appletalk, DECnet, IPX, and X25, showed us that such gateways were viable options only during transition periods with smaller, single application, networks. But proprietary protocol and translation gateways suffer from well-known severe issues, such as high CapEx and OpEx[1], along with significant technical limitations[2], including lack of end-to-end capabilities in terms of QoS, fast recovery consistency, single point of failures (unless implementing complex stateful failover mechanisms), limiting factors in terms of innovation (forcing to least common denominator), lack of scalability, vulnerability to security attacks, and more. Therefore, using IPv6 end-to-end (IP running on each and every device in the network) will be, in many ways, a much superior approach for multi-services Field Area Networks as shown on Figure 1.

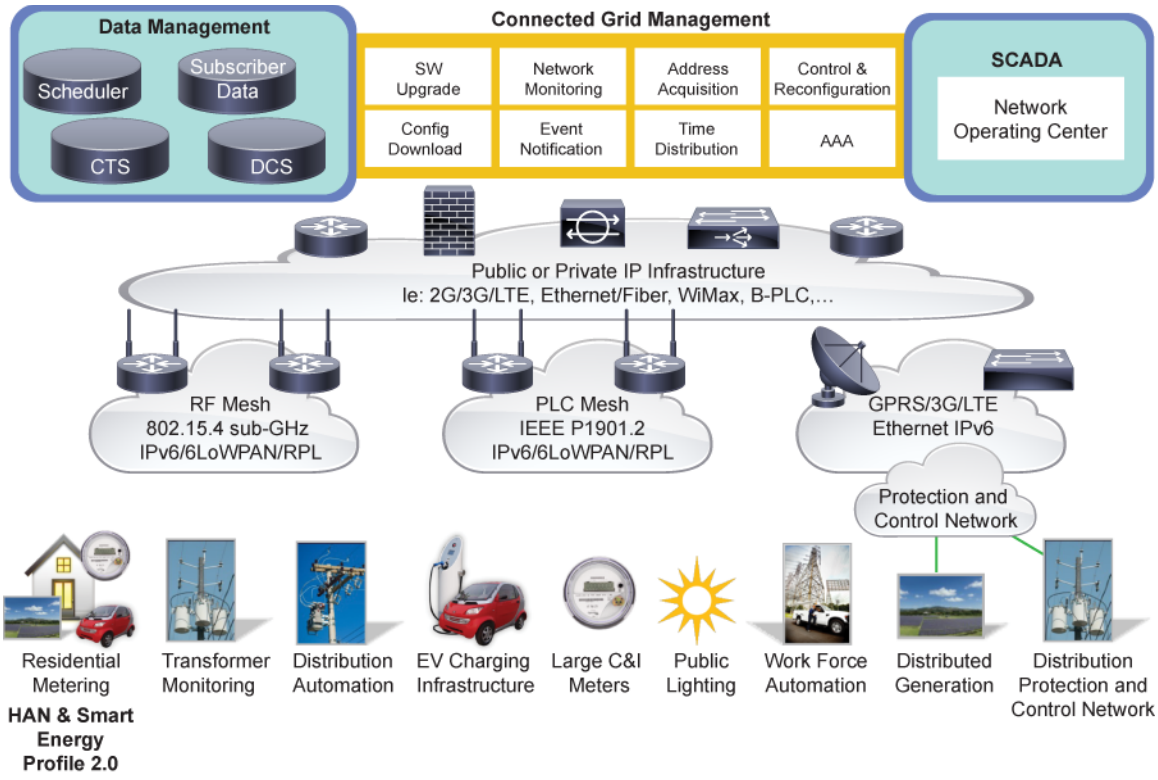

Figure 1. Multi-Services Infrastructure for Last Mile Smart Grid Transformation (*Source: Cisco*)

[1] In the 1990's, fueled by a Gartner Group report stating that "users with SNA as their primary protocol will spend a total of 20% more than IP users on training staff, hardware and software purchases, and administration", organizations began to migrate to Internet Protocol based networks.

Read more: http://www.articlesnatch.com/Article/Reducing-Costs-By-Migrating-From-Sna-Applications-To-Ip/531425#ixzz1ZHZEmWkH
Under Creative Commons License: Attribution No Derivatives

[2] See RFC 3027 as an example of protocol complications with translation gateways

4. The Unique Network Requirements of Constrained Networks

Devices deployed in the context of NANs are often constrained in terms of resources and often named IP Smart Object. Smart-Object networks are also referred to as Low power and Lossy Networks (LLN) considering their unique characteristics and requirements. By contrast with typical IP networks, in which powerful routers are interconnected by highly stable and fast links, LLNs are usually interconnected by low-power, low-bandwidth links (wireless and wired) operating between a few kbps and a few-hundreds kbps and forming a meshed network for guaranteeing proper operations. In addition to providing limited bandwidth, it is not unusual to see on such links the Packet Delivery Rate (PDR) oscillating between 60 percent and 90 percent, with large bursts of unpredictable errors and even loss of connectivity at intervals. Those behaviors can be observed on both wireless (such as IEEE 802.15.4g) and Power Line Communication (PLC) (such as IEEE P1901.2) links, where packet delivery variation may happen during the course of one day!

Another characteristic of IP smart objects is that various types of nodes could get mixed in the communication's infrastructure. It implies that the routing protocol needs to have the capability managing traffic paths based on node's capabilities—ie: powered electric meters able to forward traffic and co-existing with battery powered water meters, or battery powered faulted circuit indicators, acting as leaves in a LLN routing domain. Node failures may also be significantly more frequent than in traditional IP networks where nodes have as much as power they require and are highly redundant (multiprocessors, supporting non-stop forwarding (NSF), In-Service Software Upgrade (ISSU), etc).

Another necessary characteristic for LLNs is scalability. Some LLNs are made up of dozens of nodes; others comprise millions of nodes, as is the case of AMI networks, however they are usually made up of subnets (or smaller networks) of a few thousand nodes. This explains why specifying protocols for very large-scale, constrained, and unstable environments brings its own challenges. For example, one of the golden rules in an LLN is to "under-react to failure," by contrast to routing protocols such as OSPF or ISIS, where the network needs to re-converge within a few dozens of milliseconds. Meeting this challenge required a real paradigm shift, since over-reaction would lead, very rapidly, to network collapse. Furthermore, control-plane overhead should be minimized, while supporting dynamic link/node metrics, Multi-Topology Routing (MTR), and so forth.

That explains why several techniques that were developed for traditional IP networks had been redesigned resulting in various protocols especially for Mesh routing (RPL) as discussed later in this paper. In addition, the IETF Light-Weight Implementation Guidance WG [LWIG] is developing implementation guidelines for constraint devices.

Last but not least is the strong requirement for deploying highly secure networks, using years of IP protocols and algorithms, as discussed later in this paper.

5. The Technical Components of IPv6 Smart Grid Last Mile Infrastructure

Today, the Internet runs mostly over IP version 4 (IPv4), with exceptions in academic and research networks, leading Internet Service Providers or Enterprises, and government networks (where IPv6 is increasingly being deployed). See Figure 3 for an IPv4-IPv6 comparison. However, the Internet faces a major transition [OECD] due to the exhaustion of address pool managed by IANA since February 2011. With little existing IPv4 networking legacy in the areas of AMI and Distribution Automation, there is an opportunity to start deploying IPv6 as the de facto IP version from Day One. The industry has been working on IPv6 for nearly 15 years, and the adoption of IPv6 —which provides the same IP services as IPv4 (see figure 5)—would be fully aligned with numerous recommendations (U.S. OMB and FAR, European Commission IPv6 recommendations, Regional Internet Registry recommendations, and IPv4 address depletion countdown) and latest 3G cellular evolution known as LTE (Long Term Evolution).

Moreover, all new developments in relation to IP for Smart Objects and LLNs as discussed above, make use of or are built on IPv6 technology. Therefore, the use of IPv6 for Smart Grid FANs deployment benefits from several features, some being extensively reviewed in the next sections:

- A huge address space accommodating any expected multi-millions meter's deployment (AMI), thousands of sensors (DA) over the hundred thousands of secondary substations and additionally all standalone meters. It includes additional flexibility of address configuration that helps adapting with the size of deployments as well as the need to lower field workers tasks when installing small devices. The structure of the IPv6 address is also flexible enough to manage a large number of sub-networks that may be created by futures services such as e-vehicle charging stations or distributed renewable energy
- IPv6 is the de facto IP version for meter communication over open RF Mesh wireless (IEEE 802.15.4g, DECT Ultra Low Energy) and Power Line Communications infrastructures (IEEE P1901.2) using the 6LoWPAN adaptation layer that only defines IPv6 as its protocol version.
- IPv6 is the de facto IP version for the standardized IETF Routing Protocol for Low Power and Lossy Networks (RPL)—IETF RoLL WG—RPL is an IPv6-only protocol.

This goes without forgetting all well-known IP features set that enables design variations for the deployment of highly available and secured communications infrastructure tying a Network Operations Center(s) and all Neighborhood Area Networks (NAN) through public and/or private Wide Area Networks (WAN) links such as shown on Figure 2.

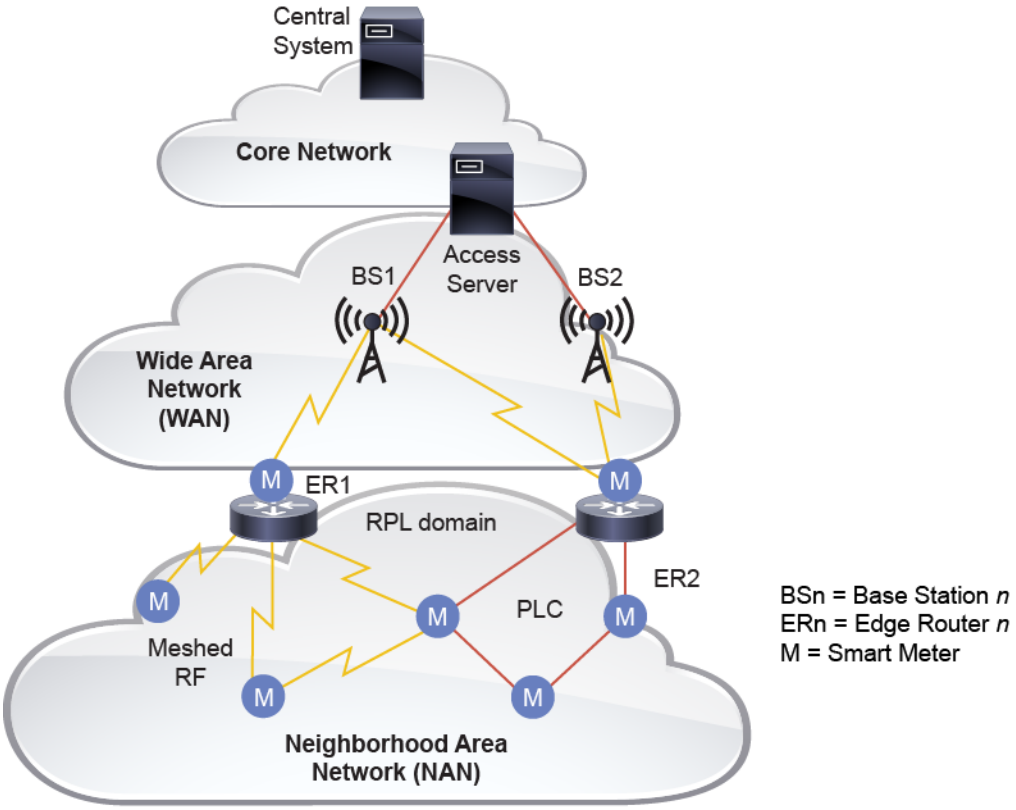

Figure 2. Example of basic Last Mile Smart Grid Infrastructure with several levels of redundancy (*Source: Alliander*)

The Head-end System of a basic FAN as shown in Figure 2 collects the meter readings, maintains meter configurations and monitors network operation. It has end-to-end connections to the meter nodes, provided by wide area networks (WANs) and neighborhood area networks (NANs). So, while the physical connections to the meter nodes change from WAN to NAN technologies, the principle of logical end-to-end IPv6 connections is maintained. This is achieved by introducing one or more routers at the borders of the NAN, also called IP Edge Routers that connect to the WAN, enabling bi-directional data streams between WAN and NAN. In case of multi-services infrastructures, it may be expected that IP Edge Routers have to be configured as dual-stack—IPv6 and IPv4 and will be capable of tunneling IPv6 over IPv4 or vice-versa. This may be required when connecting over its serial or Ethernet interfaces legacy Distribution Automation devices that only run IPv4 or providing remote workforce connectivity to an IPv4 Intranet or when using WAN infrastructure that are IPv4-only (ie: GPRS). The IP Edge Router will have to be properly configured to accommodate scenario such as running both IPv6 and IPv4 over the WAN or tunneling one protocol version over the other, mechanisms that have been well defined and tested by the Internet industry.

Distribution System Operators (DSOs) require redundancy as a means to improve communication reliability in the LLNs, as well as measure against vendor lock-in and technology lock-in due to incompatibility in lifetime between communication and metering technologies. Redundancy can be achieved at several levels through mesh capabilities in the WAN and NAN or by using multiple technologies simultaneously. Routing shall be transparent from end to end and independent from the technology. For example, the WAN connection of the IP Edge Router is established by a private reliable fiber connection or by public flexible cellular communication technology like GPRS/3G/LTE. An IP Edge Router can be co-located with a metering node or located as separated entity in a substation while the majority of the metering nodes communicate over a meshed NAN through 6LoWPAN/IPv6/RPL over RF or PLC technologies or both. The possibility of multiple IP Edge Routers enabled by dynamic IP routing protocols is important to prevent single point of failure, typically introduced by concentrators as used today for proprietary PLC and RF Mesh. Dynamic routing would allow for transportable NAN nodes, such as electric vehicles, field tools, or pagers. IP Edge Routers capable of routing traffic over different NAN technologies and cooperating with other IP Edge Routers over the backbone for global connectivity are key elements to prevent vendor lock-in and technology lock-in, since alternative WAN and NAN communication technologies can easily be adapted. This is in contrast with IP (non-IP) gateway connecting the NAN with the rest of the network where the failure of one equipment handling states and protocol translation unavoidably leads to communication failure.

This allows DSOs also to optimize on capital investments (CAPEX) and operational costs (OPEX), both in time and place. Take for example the situation with GSM/GPRS in some countries. While this mature technology is readily available for rollout and has low cost, it might be at the end of its life cycle and a risk to deploy. However, using it for WAN access only easily mitigates this risk and placing more advanced 3G/LTE modems in (some of) the IP Edge Routers from the start or exchanging them gradually when coverage and prices are right.

Another concern for DSOs on optimizing costs is dispersed rollout. NAN technologies (RF or PLC Mesh) typically need sufficiently dense grouping of nodes to achieve mesh capabilities (to see its neighbor). When starting a rollout in a location, an IP Edge router has to be installed first, close enough from a first meter, ensuring the WAN communications. Later it will serve as foundation for a larger NAN that will grow as soon as more neighbor nodes are deployed as well.

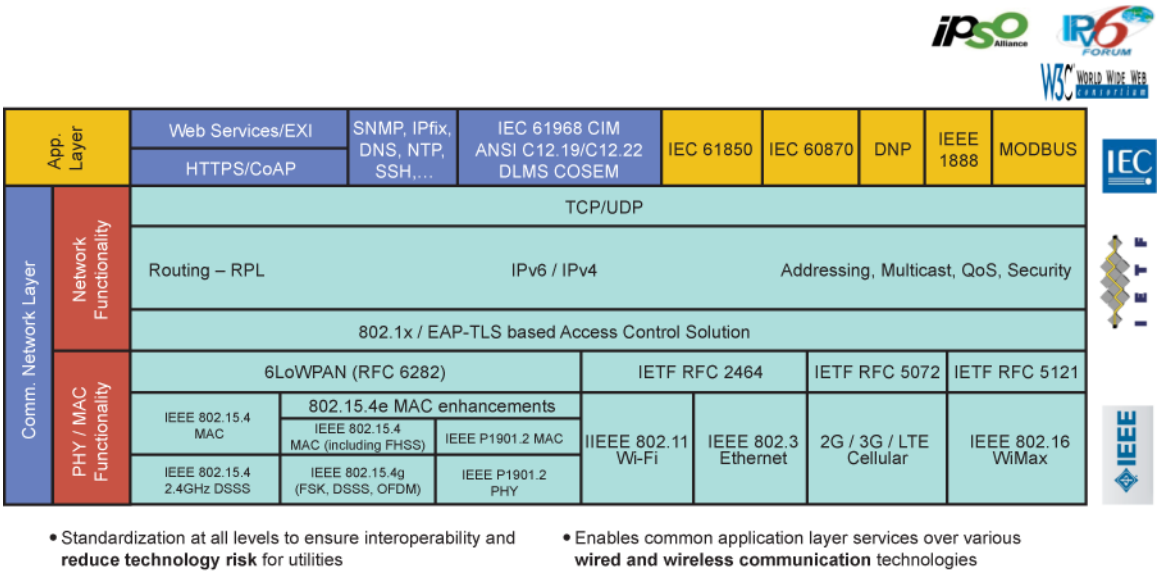

Figure 3. An IPv6 networking stack for Smart Grid Field Area Networks (*Source: Cisco*)

Figure 3 summarizes the whole proposed IPv6 end-to-end architecture for Field Area Networks and clearly shows the power and flexibility provided by a layered architecture. First the layers are independent from each other, still allowing cross-layer optimizations made possible by the Application Programming Interface (API) between the layers. For example, new link types can be added without having to revisit the network-addressing scheme, or new applications can be supported without impacting the rest of the stack. And yet another example, the routing functionality taking place on Layer 3, enables new link layers to be added without impacting the routing architecture. In the rest of this chapter, we describe, in greater detail, technical aspects related to the networking stack for FAN, knowing that a plethora of existing IP protocols are re-used without requiring any change.

5.1. Diversity of Physical and Data Link Layers

As mentioned, one main difference between energy distribution networks and ICT is the pace of changes in technologies. Every three to five years, physical and data link layers evolve offering greater bandwidth, enhanced robustness, longer reach, lower cost, etc.—all contributing to the success of the IP architecture which allows smooth evolution and future proofing without reconsidering the whole architecture. Such evolutions on the time scales above are familiar to anyone observing the evolution of Ethernet, Wi-Fi, or Cellular technologies, to name just a few technologies with very high visibility.

Considering the lifetime of meters or other devices that will get deployed in the last mile, the use of the IP suite guarantees new technologies and services being added without jeopardizing the stability of an overall deployment that is expected to serve a useful life of several decades. Deploying modular devices acting as “IP Edge routers” at the NAN level allows the addition of new interfaces in addition to the support of new protocol and feature set via software/firmware upgrades and the co-existence of different generations of meters, and physical and data link layers while improving last-mile capabilities without greatly modifying existing infrastructures. This statement is not only true for the last mile—toward the meters—but also on the backhaul links over wide-area networks—that connect the Information System.

Looking at existing AMI projects around the world, it is obvious that several physical and data link layers technologies will be selected for the last mile of Smart Grid FAN infrastructure and/or to connect the last mile to the NMS/Head-End systems.

Considering the backhaul connectivity of substations, there is no real difference of choice between technologies selected by an Internet Service Provider (ISP) or by utilities; whatever the technology—Wired (Fiber, Ethernet, xDSL, broadband PLC) or wireless (WiMax, GPRS, 3G, LTE, satellite)—they all support IP. The real challenge of introducing IP in the last mile of an AMI network is more related to selecting open standards for RF Mesh or narrowband PLC (such as IEEE 802.15.4g and IEEE P1901.2) as current deployments include non-IP, closed or proprietary solutions.

The physical and data-link layer standardization is outside the scope of the Internet Engineering Task Force (IETF). IETF only defines how IP and upper layers run on top of the MAC and PHY layers standardized by the Institute of Electrical and Electronics Engineers (IEEE) or other standards bodies. Therefore, let's have a quick overview of standards-based PHY and MAC layers for IEEE 802.15.4g (and some of 15.4.e) RF Mesh and IEEE P1901.2 narrowband PLC as they are fully aligned with the IP layered architecture and very well suited to AMI networks.

IEEE 802.15.4g–Smart Utility Networks (SUN)

In an effort to promote open standards for the Smart Grid environment and to meet specific regional and national regulations, the IEEE 802.15.4g Task Group, also known as the Smart Utility Networks (SUN) Task Group, reviewed the IEEE 802.15.4-2006 standards and proposed amendments, principally for outdoor, low-data rate, wireless, smart metering utility networks. Initially, IEEE 802.15.4 was designed as low-power wireless PHY and MAC layers of choice for smart object networks by offering low power consumption with acceptable link speeds (up to 250 Kbits/s) in the 2.4GHz ISM frequency band.

IEEE 802.15.4g adds new PHY support for Smart Utility Networks (SUN) to IEEE 802.15.4-2011 that will help develop and deploy standards-based RF-Mesh solutions around the world. In addition to the new PHY, the amendment also defines MAC modifications (may require 15.4e add-on features) needed to support their implementation.

The SUN PHY supports multiple data rates in bands ranging from 450MHz to 2450 MHz and working in one of these 3 modes:

- Orthogonal frequency division multiplexing (MR-OFDM) PHY–Provides higher data rates at higher spectral efficiency
- Multi-rate and multi-regional offset quadrature phase-shift keying (MR-O-QPSK) PHY—Shares the characteristics of the IEEE 802.15.4-2006 O-QPSK PHY, making multi-mode systems more cost effective and easier to design
- Multi-rate and multi-regional frequency shift keying (MR-FSK) PHY—Good transmit power efficiency due to the constant envelope of the transmit signal

IEEE 802.15.4g addresses regional regulations (North America, Europe, Japan, Korea and China) by adding support for new frequencies including sub-GHz frequency bands. The IEEE 802.15.4 radio can now operate in one of the dedicated-use or unlicensed bands. A table summarizing the various operating frequencies can be found at http://developer.cisco.com/web/cegd/blogroll.

IEEE P1901.2 Power Line Communication

Power Line Communications (PLC) system provides ability to transmit data over power lines.

Also known as a no new-wire technology, it simply reuses the electrical wire of mains-powered devices. Carrying data over existing wires reduce significantly installation costs. In the context of AMI, PLC makes use of the most widely existing wired network: the electrical grid. PLC is not sensitive to the same disturbers as wireless links and come with its own challenges:

- Time-varying channel characteristics and parameters varying with frequency, location, and the type of equipment connected to it
- Low bandwidth, calling for optimizations at all layers of the communication's stack
- Possible high propagation losses
- Frequency-dependent attenuation
- Changing characteristic impedance caused by cable transition and devices connected
- Noise/interference generated by devices connected or the electrical network itself

Some of these characteristics are common with wireless links characteristics such as IEEE 802.15.4. In particular, PLC links characteristics are continually varying, and could benefit from principles developed for wireless or mobile networks. Though, no standard was designed to address such challenges over PLC. This is why the IEEE 1901 working group started to specify such standards for PLC. While IEEE 1901 has been published covering In-Home and Broadband PLC, there is an on-going effort by the IEEE P1901.2 Task Group to standardize the narrowband PLC, which is used by utilities, also for the last-mile AMI infrastructure.

The expected benefits of IEEE P1901.2 standard for Narrowband PLC are:

- Open PHY (OFDM-based) and MAC layers definition allows chipset vendors to develop their offering and users to look at interoperability
- Data rate is expected to be scalable to 500 kbps, depending on the application requirements
- Covers the full low-frequency (below 500 KHz) PLC communication spectrum, while complying with regional regulations such as CENELEC A band dedicated to utilities in Europe.
- Expands the use-cases for IEEE P1901.2 PLC beyond AMI—Electric Vehicle (EV) to charging station, street lighting, power plugs, solar panels/inverters, and Home Area Networking (HAN).
- Enable Medium Voltage/Low Voltage crossing for grid to utility meter communication and helping to lower the deployment cost with reducing the number of concentrators.
- Assure coexistence with other existing Narrowband and Broadband Power Line (BPL) technologies with a dedicated bandwidth
- Address the necessary security requirements that assure communication privacy and allow use for security sensitive services
- MAC layer aligned with IEEE 802.15.4 MAC and leveraging the work done by IETF 6LoWPAN WG in particular for header compression. Therefore, it enables straight IPv6 support and simplifying the learning curve when running both IEEE 802.15.4 and PLC

The resulting IEEE P1901.2 standard can naturally fit with the IP layering architecture and make P1901.2 links part of the overall IPv6 network.

We presented a very short overview of two link layer technologies, but other technologies will undoubtedly be developed in the coming years. The adoption of an IP architecture permits, from day one, a diversity of physical and data link layer technologies appropriate to the density, cost and operational requirements of the FAN deployment. Supporting IP and its layered architecture over PHY and MAC layers guarantees that the FAN infrastructure can benefit of new link layer's technologies when, and where, they are needed.

5.2. The 6LoWPAN Adaptation Layer

When sending IP packets over PHY and MAC layers, an adaptation layer is always defined as an open standard generally published by the IETF. For example, RFC 2464 described how an IPv6 packet must get encapsulated over an Ethernet frame, and is also used for IEEE 802.11 WiFi. Similarly, the IETF 6LoWPAN working group specified how IP packets are encapsulated over IEEE 802.15.4.

The main focus of the 6LoWPAN WG was to optimize the transmission of IPv6 packets over Low Power and Lossy networks such as 15.4. 6LoWPAN WG led to the publication of RFCs specifying:

- Header compression (RFC 6282), which reduces the impact of sending IPv6 40-bytes headers and UDP 8-bytes headers. The way an IPv6 header can get compressed is one of the elements that led to a specific IPv6-only adaptation layer.

Note: *While nothing precludes running TCP over IPv6/6LoWPAN, no TCP header compression was defined as the congestion avoidance algorithms could overreact to LLN's packet drops and/or round-trip delay variance would make TCP operate very slowly.*

- Fragmentation and reassembly of IPv6 packets, as the IEEE 802.15.4 127 bytes data link layer did not match the requirement of an IPv6 1280-byte Maximum Transmission Unit (MTU). It is worth noting that IEEE 802.15.4g has no such short MTU limitations
- Other functions such as 6LoWPAN for Duplicate Address Detection (DAD) over broadcast link layers.

Although these features were initially developed for IEEE 802.15.4 links, they are now re-used by other link layers as long as they adhere to the IEEE 802.15.4 MAC and addressing scheme. For example, this is the case for the IEEE P1901.2 narrowband PLC link layer and DECT Ultra Low Energy (ULE) or Bluetooth Low Energy (LE).

5.3. IPv6 Addressing

The adoption of IPv6 in the FAN infrastructure requires an Energy Provider to consider all steps required by an IP network design and particularly an understanding of IPv6 addressing and how internal policies may help the operations.

Global, public, and private address space have been defined for IPv6, therefore a decision must be made regarding which type of IPv6 addressing scheme should be used in utility networks. Global addressing means the utility must follow the Regional Internet Registries (RIR) policies (such as ARIN https://www.arin.net/policy/nrpm.html) to register an IPv6 prefix that is large enough for the expected deployment and its expansion over the coming years. This does not mean the address space allocated to the infrastructure must be advertised over the Internet allowing any Internet users to reach a given device. The public prefix can be advertised if representing the entire utility corporation–or not–and proper filtering mechanisms are in place to block all access to the Field Area Networks and devices. On the other end, using a private address space means the prefix not be advertised over the Internet, but, in case there is a need for B2B services and connectivity, a private address would lead to the deployment of additional networking devices known as IPv6-IPv6 NPT (Network Prefix Translation, RFC 6296) gateways.

Once the IPv6 addressing structure (see RFC 4291, 4193) and policies are well understood and a prefix is allocated to the infrastructure, it is necessary to structure the addresses according to the number of sites and end-points that would connect to it. This is no different to what an ISP or a large Enterprise has to perform. (See 6NET)

Internal policies may be defined by the way an IPv6 address is assigned to an end-device, by using a global or private prefix.

Three methods to set an IPv6 address on an end-point are available:

- **Manual configuration**–This is appropriate for Head-End and NMS servers that never change their address, but is inappropriate to millions of end-points, such as meters, in regards to the associated operational cost and complexity
- **Stateless auto-configuration**–A mechanism similar to Appletalk, IPX and OSI, meaning an IPv6 prefix gets configured on a router interface (interface of any routing device such as a meter in a mesh or PLC AMI network), which is then advertised to nodes attached to the interface. When receiving the prefix at boot time, the node can automatically set-up its IPv6 address
- **Stateful auto-configuration**–Through the use of DHCPv6 Individual Address Assignment, this method requires DHCPv6 Server and Relay to be configured in the network but benefits of a strong security as the DHCPv6 process can be coupled with AAA authentication, population of Naming Services (DNS) available for Head-End and NMS applications.

The list above is the minimum set of tasks to be performed, but as already indicated; you must also establish internal policies and operational design rules. This is particularly true when considering security and management tasks such as registering IPv6 addresses and names in DNS (Domain Name System) and in NMS (network management station(s) or setting-up filtering and firewalling across the infrastructure.

5.4. Routing

Proprietary systems originally developed for application-specific sensor networks usually neglect the architectural aspect of a scalable networking architecture. In most of these systems, it is not rare to find non-layered architecture, despite the lack of flexibility and scalability, with a layer violation. Routing is no exception.

Where should routing take place?

Several closed systems place the routing function at the data link layer (Layer 2). The consequence is that the network is limiting itself to a single data link layer technology. It therefore becomes impossible to mix or add data link layers technologies, which is a fundamental requirement of Field Area Networks (as previously discussed, mixing low-power RF, PLC, or even Cellular is a use-case requirement). In Layer 2 routing networks, the support of multiple types of links, would require to superpose two routing protocols (both at the IP layer and the link layer—this is for example the case when the NAN becomes a multi-service network, a transit network to other networks (e.g gas, water or home), etc), which is an architecture that has proven to be extremely complex, expensive and difficult to manage even in a non-constrained classic network (IP over ATM (PNNI) is one of the notorious examples). Needless to say that adding this level of complexity to AMI networks hurts the requirements for scalability, ease of operations and future proofing.

Therefore, performing routing at the network layer, as fundamentally adopted in the layered IP architecture is an appropriate choice. To that end, the IETF formed in 2008 the Routing over Low Power and Lossy Networks Working Group (RoLL WG) chartered to specify an IPv6 Routing protocol for constrained large-scale networks such as FAN [RPL-AMI]. Tasked with designing a routing solution for IP smart-objects, the RoLL WG initially specified four standard documents, spelling out in detail the technical routing Use-Case requirements for urban networks, including Smart Grid, industrial, and home and building automation networks. A protocol survey made to determine whether an existing routing protocol (OSPF, OLSRv2, TBRPF, RIP, AODV, DSDV, DYMO[Low], and DSR) could be used for IP smart objects, given the characteristics and requirements of these networks (including table scalability, loss response, cost control, support of cost routing for links and nodes) led to the consensus that a new routing protocol had to be specified. Being re-chartered, and after almost two years of intensive work done by a number of industry routing experts, RoLL WG published a new distance-vector routing protocol, called IPv6 Routing Protocol for Low Power and Lossy Networks, or RPL ([RPL]).

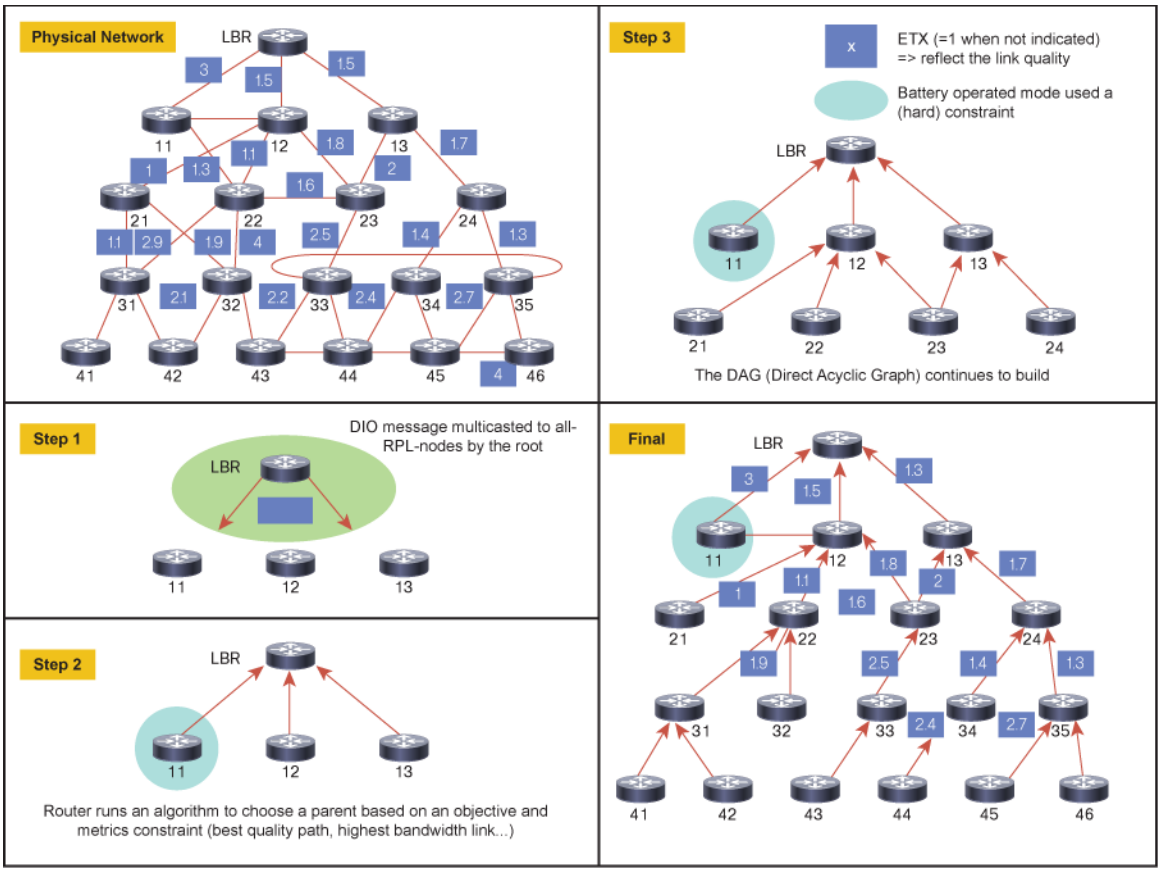

Figure 4. RPL—basic network RPL initialization steps (*Source: Cisco*)

RPL provides support for a large number of technologies and features (as documented in [RPL-WP]) that matches all services requirements reviewed in the introduction. One of the key characteristics of RPL is that the protocol is highly flexible and dynamic; it has fundamentally been designed to operate in harsh environments with low-speed links potentially experiencing high error rates, while generating very low control plane traffic. RPL offers number of advanced features, such as trickle timers limiting the chattiness of control plane, dynamic link (Hop count, Throughput, Latency, Link / path Reliability, Link Colors) and node (Node state/attribute, node power levels) routing metrics for constraint-based routing useful for combined AMI and DA deployment, multi-topology routing, and loop detection or ability to avoid oscillations in case of transient failures (local repair mode and Global repair mode)

Today, RPL is an approved international standard with various implementations, extensive simulations and testing being carried out. This led several alliances such as Zigbee/IP (and more explicitly as part of Smart Energy Profile (SEP) 2.0), ZWave, and others to adopt routing at the network layer, and particularly RPL, into their evolution to the IP architecture. While offering a fairly sophisticated set of functionalities, RPL has been tailored to fit in few kilobytes of memory footprint and should become the IPv6 routing protocol of choice for Field Area Networks as documented in the applicability statement [RPL-AMI]. In combination with more traditional IP routing technics, such as route redistribution, load balancing through multiple IP edge routers, dynamic re-routing in case of hardware or WAN failures, RPL deployment has all capabilities required by large and scalable FAN infrastructure. It worth stressing the fact that the use of multiple routing protocols all operating at the IP layer is not an issue in contrast with the co-existence of multiple routing protocols at different layers (link layer and IP), as pointed out at the beginning of this section.

***Note**—IPv6 communications as defined by SEP 2.0 for Home Area Networks (HAN) communications requires additional discussion in term of addressing, routing and security policies that are outside the scope of this document. For example, a smart meter may get an IPv6 prefix belonging to the Utility on its NAN interface as well as a private IPv6 prefix locally managed or a public one assigned by a broadband ISP to its HAN SEP 2.0 interface. Traffic flows between interfaces has to be strictly controlled. The new IETF HomeNet WG [In-Home] may provide guidelines in future.*

5.5. Quality of Service (QoS)

Over the past years, several Industries have leveraged the scalable IETF Differentiated Services (DiffServ) architecture for IP Quality of Services (QoS) when integrating critical classes of traffic over their IP networks. Therefore, the mix of traffic—metering, distribution automation, remote workforce management, etc.—flowing over the last mile of the Smart Grid network can be controlled and prioritized accordingly to defined Service Level Agreement (SLA) policies in terms of delays, jitter, packet loss, and scheduling, etc. This implies considering the variety of QoS mechanisms and their adaptation to the constrained AMI environment, for example:

- **Compression**–Control of packet size sent over low-bandwidth links helps to scale the AMI infrastructure. As discussed in the 6LoWPAN section, this adaptation layer deals with IP and UDP headers. In addition, other compression and optimization techniques such as those discussed in the Network Management section can be applied to other layers, validating once again the benefits of the IPv6 layered architecture.
- **Traffic marking**–When packets get transmitted, they can be marked (colored) by the end-node application or by a router performing packet inspection by setting-up the specific fields on the IPv6 header (traffic-class field) used to specify their CoS (Class of Service). This allows appropriate prioritization of the packets through other forwarding nodes.
- **Scheduling and congestion avoidance techniques**–To give priority to traffic according to their CoS. For example, when a device in a RF or PLC mesh network implements several queues enabling real-time traffic from Distribution Automation sensors to pass through an interface with high priority.
- **Call Admission Control (CAC) techniques**–To reserve bandwidth for high-priority traffic, for example on an edge router connecting the last mile to the Head-end system through low-speed cellular networks.
- **Multiple RPL DAG**–As discussed in the RPL section, the routing metrics could get leverage to build different DAG differentiating the routing path for a certain class of traffic. For more details on RPL, please refer to [RPL-WP]

While the QoS model is not fundamentally different between IPv4 and IPv6 version, the appropriate definition of Differentiated Services Code Points (DSCP) will help fine-tuning the last-mile infrastructure traffic.

5.6. Security

Coupling data communications capabilities with the power transmission, distribution, and consumption infrastructures increases the efficiency of the power grid, but also creates a long list of operational challenges—Security tops that list. Thus, security represents a key challenge for enabling a successful rollout of Smart Grids and AMIs. It needs to be addressed in a holistic, end-to-end fashion, leveraging the concept of “Security by Design”.

In the past it was sometimes claimed that the use of open standards and protocols may itself represent a security issue, but this is overcome by the largest possible community effort, knowledge database and solutions available for monitoring, analyzing and fixing flaws and threats—something a proprietary system could never achieve.

Said otherwise, a private network, IP-based architecture based on open standards has the best understood and remedied set of threat models and attack types that have taken place and have been remedied against, on the open Internet. This is the strongest negation of the now deprecated concept of “security by obscurity” that argues that the use of non-standard networking protocols increases security and which is unanimously rejected by the network security expert community. Security per se is not a new topic to utilities as they are already operating and maintaining large-scale data communication networks. Using IP as a common technology in the core of Smart Grids and AMIs will help to ensure security knowledge is available within the involved organizations.

It is important to note that IPv6 security has at least the same strengths as IPv4, but both IPv4 and IPv6 are certainly not worse than proprietary networking protocols. We recommend people focusing on FAN security to review documents such as NISTIR 7628, Guidelines for Smart Grid Cyber Security or UCAIUG, AMI System Security Requirements. In Europe, Smart Grid Information Security requirements are currently under definition by the standardization organizations, several guidelines and requirements have been issued or are under definition by the Member States. All are asking for open standards. With Security being a multi-layer challenge, it is important to review some additional features that provide nodes authentication and data integrity and privacy on a FAN deployment.

Strong authentication of nodes can be achieved by leveraging a set of open standards mechanisms. For example, after a node discovered a RF or PLC Mesh network leveraging IEEE 802.15e enhanced Beacon frames, it can get properly authenticated through IEEE 802.1x, PKI, certificate and AAA/Radius mechanisms before beginning to communicate using a Link-local IPv6 address. From there, the node can join its RPL domain before getting a global IPv6 address through DHCPv6 as well as other information (DNS server, NMS, etc).

Data integrity and privacy leverages the encryption mechanisms available at various layers of the communication stack. For example, an IPv6 node on a last mile subnet has options to encrypt data at layer 2 (AES-128 on IEEE 802.15.4g or IEEE P1901.2), layer 3 (IPsec), layer 4 (DTLS) or per application at layer 7, ie: encryption of ANSI C12.22 or DLMS/COSEM for the metering traffic. While multiple levels of encryption may be implemented on a constraint node, the processing resources (processor speed and memory, energy consumption) requirements must be evaluated in regards of the additional hardware cost this could generate. With multiple options available it can be assured that nodes can be integrated into existing security architectures, relying on Link, Transport and/or Application Layer encryption. Furthermore, this will ease the integration and enhancement of existing Application Layer protocols (i.e. ANSI C12.22 or DLMS/COSEM) where certain security functions could convert at a lower layer, e.g. by providing a secured end-to-end path, and where other functionalities (i.e. message integrity / proof of origin) can remain at the Application Layer.

The choice of a given layer for data encryption and devices performing the encryption also impact the network services, performances and scalability of a deployment. For example, when software upgrade, demand/response or dynamic pricing should use Multicasting, the choice of encrypting data at transport layer (L4 DTLS) precludes leveraging the replication capabilities of IP Multicast routers on the infrastructure.

Whatever the encryption layer selected on the NAN devices, an IP Edge router can also perform layer 3 encryption (IPsec) for all traffic forwarded over the backhaul links. Therefore, hardware cost and resources may limit to layer 2 authentication and encryption and potentially encryption at layer 3 or 7 on constrained devices while layer 3 encryption on the IP Edge router takes care of all traffic sent over the WAN without loosing network services capabilities.

Combined with more traditional security features such as digital signatures for firmware images or data objects on devices (ie. for meter reads or critical commands), traffic filtering, firewalling and intrusion prevention on the IP Edge routers, the last mile of a Smart Grid deployment can get strong security reinforcement whatever the traffic patterns.

With IP offering the possibility of end-to-end communication down to the last mile, also, in case this is required, end-to-end encryption can be established in an efficient manner. Moreover, Application Layer protocol translation would not be required within the communication network. Multiple protocols do not have to be maintained, this would represent a clear advantage for the efficiency and security of the network.

In addition, IP, as well known technology, offers already available, tested, certified software stacks, implementing proven security algorithms and Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Team (CERT)). Thus, the Security of Smart Grids and AMIs can directly benefit from security findings within the Internet Community, now and in the future.

5.7. Network Management for Smart Meters

Today, use cases solution, such as AMI or DA handles most, if not all, services at the application layer. By adopting IPv6 for the last mile (and therefore enabling bi-directional IP end-to-end communications) there is the opportunity of leveraging well-known services from the open-standards IP architecture, decreasing complexity, and enabling required services of Smart Grid applications which could stay focused on utility data and application requirements, helping on achieving modularity and scalability and dealing with security at all levels. However, to be able to leverage all services, we acknowledge that some features would not only require proper configuration on the last mile, but may also need an evolution of the Information System which is due in any case as IPv6 adoption for the last mile requires changes on the head-end system and Meter Data Management System (MDMS) to deal with IPv6 address of meters. For example, the use of DNS may allow devices to automatically register their names and the services they offer which can simplify add/move/change operations on the last mile infrastructure.

When focusing on the particular use case of AMI, with millions of end-points with constrained resources and low-bandwidth built subnets, it is important to stress that gathering network statistics for network management can be achieved through a pull model (for example, SNMP), as well as a push model (for example, CoAP or IPfix). The push model represents a key feature to scale network management to millions of nodes that have scarce CPU resources. Therefore, although not restricted to IPv6, the overview of network services as shown in figure-5 is an opportunity to introduce a new protocol called Constrained Application Protocol (CoAP) designed by the IETF Constrained Restful Environments (CoRE) working group. CoAP is a new lightweight application protocol for constrained devices such as those deployed in IPv6/6LoWPAN FAN infrastructures. Although CoAP can be used end-to-end, the architecture also supports proxies performing a mapping function between CoAP and HTTP Rest API, independent of the application. CoAP supports various modes of caching and traffic flow (UDP binding with optional reliability supporting unicast and multicast requests, Asynchronous message exchanges, etc), which can be useful in AMI. Although CoAP is not yet fully mature and widely deployed as a protocol, its progress is significant with about a dozen companies having implemented CoAP with several successful interoperability tests. It will definitively be a key protocol of an IPv6-based FAN deployment.

To summarize, the adoption of IP based networking for all Smart Grid services allows all devices involved in the delivery of these services to be managed through a single network view. All devices and the relationships between them at the IP level can be defined in the network management application and the impact of a failure of communication to any given device can be instantly evaluated and displayed.

IP Services	IPv6	Benefits
Addressing	**128 bits, multiple scopes (global, private, link-local,…)**	Large address space, public or private infrastructure
Address Auto-configuration	**Stateless,** DHCP**v6, renumbering, DHCPv6 Prefix Delegation**	Zero-touch configuration
Data Link Adaptation layers	Ethernet, WiFi, ATM, FR, PPP, Sonet/SDH, **6LoWPAN (802.15.4g, 1901.2),…**	Media Diversity
Routing	RIP, OSPF, IS-IS, E-IGRP, MP-BGP, **RPL**	Reachability
IP Network & transport layer Security	IPsec, TLS/DTLS, Filtering (firewall)	Security, Data Integrity
Multicast	**MLD**/PIM/Multicast MP-BGP, **Scope Identifier**	Software upgrade, Demand/Response, Dynamic pricing
QoS	IPv6 QoS Differentiated Service	Multi-Services network, SLA
Time Distribution	NTP version 4	Secured Time Synchronization
Management	DNS, IPfix/PSAMP, SNMP, CoAP…	Push/Pull Mgmt model, scalable end-points mgmt

Figure 5. Leveraging IPv6 Network Services (**IPv6 specific features**) (*Source: Cisco*)

6. Conclusion

The IP protocol suites have been deployed in a number of private and public networks (Internet) during the past three decades interconnecting billions of IP devices. The architecture has proven to be highly flexible (thus protecting investments) in many ways: new link types have been adapted, new routing and transport protocols have been specified and deployed; the number of supported applications has exceeded all expectations by an order of magnitude! Once again, this is not just because all of these protocols were well designed but due to the layered nature of the architecture, which provides a very high degree of flexibility.

Field Area Networks are a key component of Smart Grid infrastructures and the number of applications that these networks support keeps growing at a fast pace. Their networking requirements are no different: flexibility, reliability, QoS, security, manageability and scalability, which are absolute requirements that explain why IPv6 was evaluated as the most appropriate networking architecture for Field Area Networks. Additionally, FAN imposed constraints: links are not only low-speed (which is no different than in the early days of the Internet), but lossy and unstable with a large number of constrained devices, and they must provide high reliability without requiring heavy and costly management.

The vast majority of the IP protocols and technologies could be re-used “as-is” (addressing, address provisioning, QoS, transport, reliability, etc.) and several new IPv6 protocols have been specified to meet the unique requirements of the Last Mile in Smart Grid networks (RPL, 6LoWPAN, and CoAP) in addition to several low-power, low-speed links such as IEEE 802.15.4 or IEEE P1901.2.

We are at the beginning of an exciting journey that will extend the use of IPv6 to billions of devices of a new type such as meters and sensors deployed in Field Area Networks. The IPv6 protocols supporting these networks have been specified and standardized and a number of large-scale IPv6 networks are being deployed, once again showing the impressive ability of meeting new networking requirements.

To summarize, the IP adoption for the last mile enables:

- **Media diversity:** Physical and data link technology evolution, driven by innovation in communication technology at its own pace, independently from the Information System (driven by its own innovation pace and decoupled from the above)
- **Future proofing:** Adoption of new standards when available and required. No major architecture change in the sense of any necessary “cut-over day” but instead an evolutionary and piecemeal evolutionary path
- **Industry transformation:** Ease the infrastructure convergence for multi-services such as metering, Distribution Automation, workforce communications, etc.
- **Cost control:** Localized or global CAPEX and OPEX optimization
- **Reliability:** from ruggedized hardware to dynamic routing and multiple routers connecting a NAN, a FAN infrastructure can be designed for high-availability.
- **Management:** open standards based tools can contribute to improve the operations and customer support.
- **Security:** Strong security through IP solutions, also leveraging associated industry processes and IT professional ecosystem
- **Interoperability** between IP devices in a multi-service network sharing a common physical infrastructure with no need for complex and hard to manage multiprotocol gateways.

Glossary

- **6LoWPAN:** IPv6 over Low power Wireless Personal Area Networks
- **AMI:** Advanced Metering Infrastructure
- **ANSI:** American National Standards Institute
- **CERT:** Computer Emergency Response Team
- **CoAP:** Constrained Applications
- **CoRE:** Constrained Restful Environments
- **COSEM:** COmpanion Specification for Energy Metering
- **CSIRT:** Computer Security Incident Response Teams
- **DA:** Distribution Automation
- **DAG:** Directed Acyclic Graph
- **DLMS:** Device Language Message specification
- **DR:** Demand/Response
- **DTLS:** Datagram Transport Layer Security
- **EV:** Electrical Vehicle
- **FAN:** Field Area Network
- **HAN:** Home Area Network
- **IEC:** International Electrotechnical Commission
- **IEEE:** Institute of Electrical and Electronics Engineers
- **IETF:** Internet Engineering Task Force
- **IPv6:** Internet Protocol version 6
- **LLN:** Low-power and Lossy Networks
- **LTE:** Long Term Evolution
- **NAN:** Neighborhood Area Network
- **NERC CIP:** North American Electric Reliability Corporation—Critical Infrastructure Protection
- **OFDM:** Orthogonal frequency-division multiplexing
- **PAN:** Personal Area Network
- **PLC:** Power Line Communication
- **QoS:** Quality of Service
- **RFC:** Request For Comment
- **RIR:** Regional Internet Registry
- **RPL:** IPv6 Routing Protocol for Low Power and Lossy Networks
- **UCAIUG:** Utility Communications Architecture International Users Group
- **WAN:** Wide Area Network

References

[6LoWPAN] IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)
http://datatracker.ietf.org/wg/6lowpan/

[IEEE 1888] IEEE Standard for Ubiquitous Green Community Control Network Protocol (UGCCNet)
http://standards.ieee.org/findstds/standard/1888-2011.html

[In-Home] IETF HomeNet WG http://datatracker.ietf.org/wg/homenet/charter/

[IP-Light] "Internet Protocol for Smart Objects (IPSO) Alliance"
http://ipso-alliance.org/wp-content/uploads/why_ip.pdf

[IP-Smart-Objects] Interconnecting Smart Objects with IP, JP Vasseur and Adam Dunkels, Morgann Kauman, July 2010.

[LP-Links] "A survey of several low power Link layers for IP Smart Objects "—
http://ipso-alliance.org/wp-content/uploads/low_power_link_layer.pdf

[LWIG] IETF Light-Weight Implementation Guidance WG http://datatracker.ietf.org/wg/lwig/charter/

[OECD] "Economic Considerations in the Management of IPv4 and in the Deployment of IPv6", June 2008
http://www.oecd.org/sti/ict/ipv6

[RFC 6272] Internet Protocols for the Smart Grid ftp://ftp.ietf.org/rfc/rfc6272.txt

[RPL] "RPL: IPv6 Routing Protocol for Low power and Lossy Networks"—
http://datatracker.ietf.org/doc/draft-ietf-roll-rpl/

[RPL-AMI] Applicability Statement for the Routing Protocol for Low Power and Lossy Networks (RPL) in AMI Networks http://datatracker.ietf.org/doc/draft-ietf-roll-applicability-ami/

[RPL-WP] "RPL: The IP routing protocol designed for low power and lossy networks "—
http://ipso-alliance.org/wp-content/uploads/RPL.pdf

[Stats] Worldwide Internet statistics—http://www.internetworldstats.com/stats.htm