White Paper

A Standardized and Flexible IPv6 Architecture for Field Area Networks:

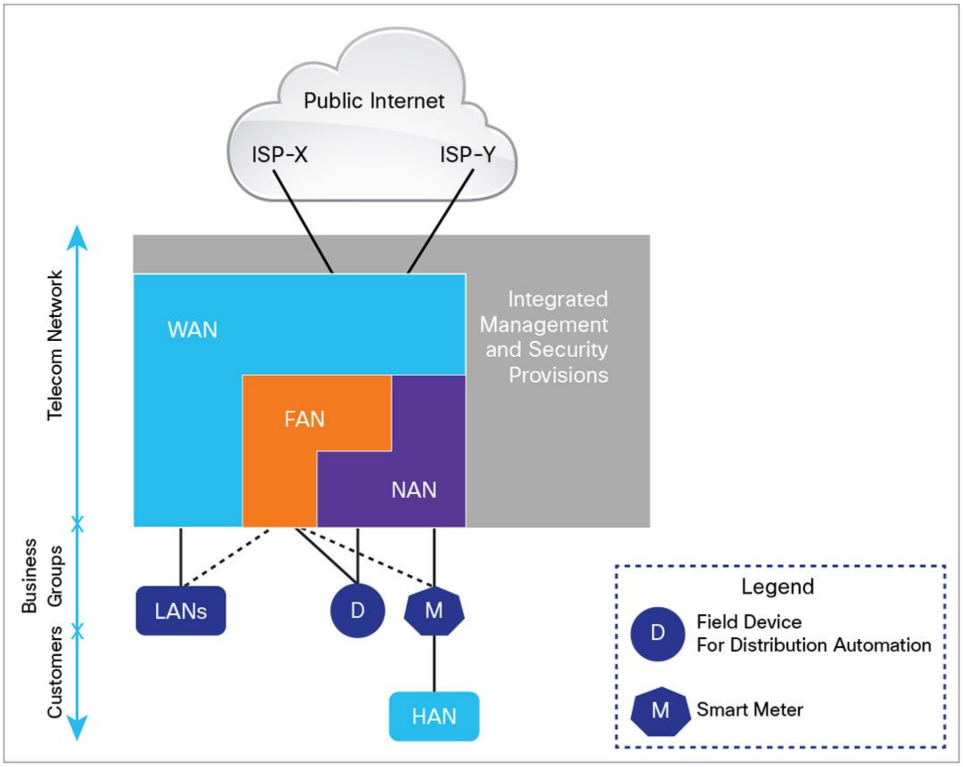
Smart-Grid Last-Mile Infrastructure

Last update: January 2014

This paper is intended to provide a synthetic and holistic view of open-standards-based Internet Protocol Version 6 (IPv6) 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 multiservice platform. In this paper, we show how the various building blocks of IPv6 networking infrastructure can provide an efficient, flexible, highly secure, and multiservice network based on open standards.

This paper does not address transition paths for electric utilities that deal with such issues as legacy devices, network and application integration, and the operation of hybrid network structures during transitional rollouts.

Figure 1. The Telecom Network Architecture Viewed as a Hierarchy of Interrelated Networks



Source: BC Hydro

1. Introduction

Last-mile networks have gained considerable momentum over the past few years because of their prominent role in the smart-grid infrastructure. These networks, referred to as neighborhood-area networks (NANs) 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. NANs also serve as a foundation for future virtual power plants, which comprise distributed power generation, residential energy storage (for example, in combination with electric vehicle (EV) charging), and small-scale trading communities.

Field Area Networks (FANs), which is the combination of NANs and local devices attached to a Field Area Router (FAR) 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, multitenant 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 Internet Protocol (IP) suite of protocols, enabling the use of open standards that provide the reliability, scalability, high security, internetworking, 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 NANs into end-to-end network architecture.

One application being run over FANs is meter reading, where each meter periodically reports usage data to a utility headend 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 DR, distributed energy resource integration and EV charging, it is expected that the traffic volume across FANs would increase substantially and traffic patterns and bidirectional communication requirements would become significantly more complex. In particular, FANs are expected to support a number of use cases that take advantage of 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 network management system (NMS) or headend and the electric meter and conversely.
- **Communication among DA devices:** Subsets of DA devices need to communicate with each other 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 headend server through individual meters acting as application gateways. For example, a user may activate direct load control (DLC) capabilities, empowering the utility company to turn off or turn down certain home appliances remotely when demand and/or the cost of electricity is high.
- **EV 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 headend servers from potentially a large set of nomadic vehicles being charged simultaneously from dynamic locations.

- **Multitenant services:** Combining information at the customer side and differentiating information into several services at the other side creates a complex multipoint-to-multipoint network (MP2MP). For example, this could be a converged network connecting devices from multiple utilities as suggested by the U.K. national multi-utility telecom operator DCC or Germany multi-utility communication box as specified in open meter systems.
- **Security:** Strong authentication mechanisms are needed 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 requires the communication of grid status and communications statistics from the meters to the NMS or Headend in a MP2P fashion.
- **Multicast services:** Groups of meters may need to be addressed simultaneously using multicast, for example to enable software upgrade or parameters updates sent by a 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 take full advantage of 30 years of IP technology development [RFC 6272], facilitating open standards and interoperability as largely demonstrated through the daily use of the Internet and its two billion users [Stats].

Note: Using the IP 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, such as interbanking networks, military and defense networks, and public-safety and emergency-response networks, use the IP architecture.

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 can support future applications 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 have been standardized by the Internet Engineering Task Force (IETF) while key physical, data link, and application protocols come from the usual industrial organizations, such as the International Electrochemical Commission (IEC), American National Standards Institute (ANSI), Device Language Message Specification (DLMS)/Companion Specification for Energy Metering (COSEM), SAE International, Institute of Electrical and Electronic Engineers (IEEE), and the International Telecommunication Union (ITU).
- **Lightweight:** Devices, such as smart meters, sensors, and actuators, which are installed in the last mile of an AMI network, are not like personal computers (PCs) 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 networks has to deal with two key challenges. First, one given technology (wireless or wired) may not fit all field deployment criteria. Second, communication technologies evolve at a pace faster than the expected lifetime of a smart meter, or 15 to 20 years. The layered IP architecture is well-equipped to cope with any type of physical and data link layers, making it ideal as a long-term investment because various media can be used in a deployment now and over time, without changing the whole solution architecture and data flow.
- **Ubiquitous:** All recent operating system 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 highly secure:** Communications 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, which are widely available. Adopting IP network management also brings an operational business application to the utility. Utilities can use network-management tools to improve their services, for example, when identifying power outage coverage through the help of the 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 FANs is how we can take full advantage of the years of experience accumulated by critical infrastructures, such as financial and defense networks, as well as critical services, such as voice and video, which have already transitioned from closed environments to open IP standards. It also benefits from a large ecosystem of IT professionals who can help design, deploy, and operate the system solution.
- **End to end:** The adoption of IP provides end-to-end and bidirectional communication capabilities between any devices in the network. Centralized or distributed architectures 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

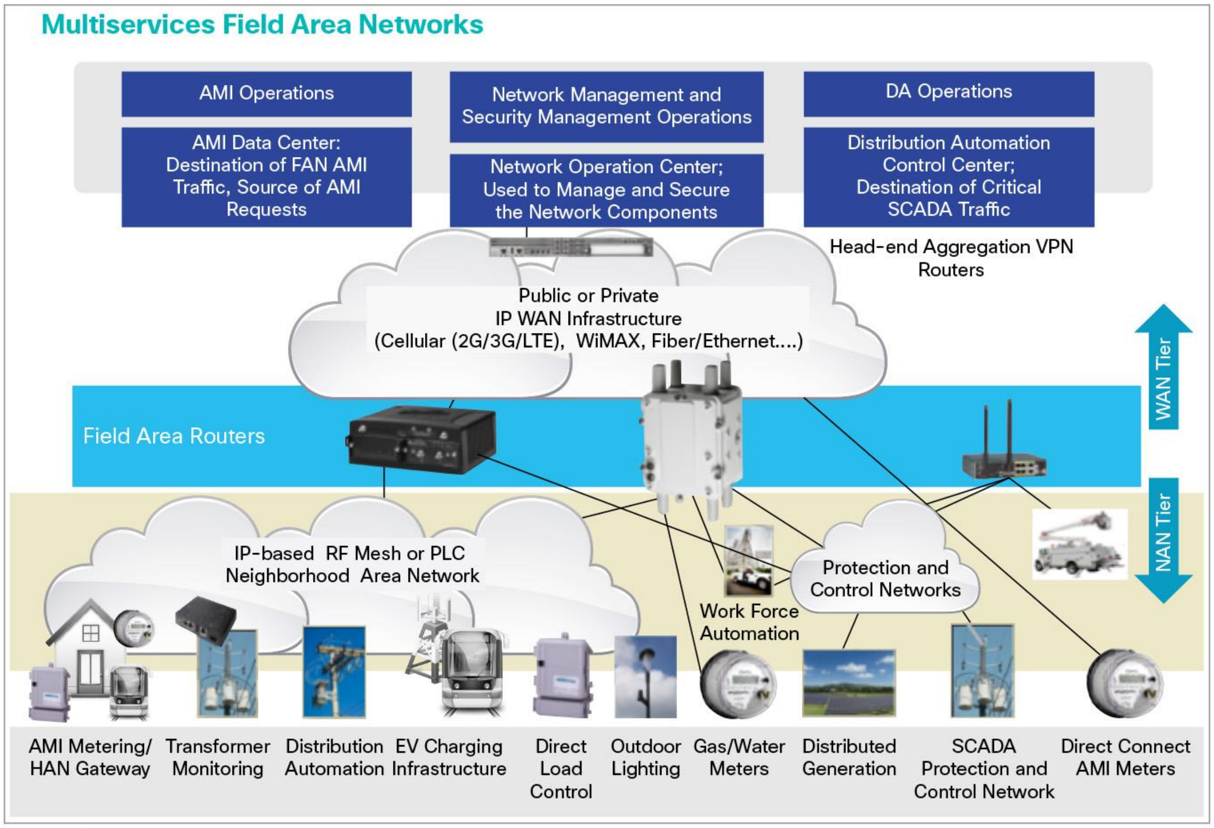
The networking requirements for NANs have been extensively documented: cost efficiency, scalability (millions of nodes in a network is common), robust security, reliability, and flexibility are absolute musts. Technologies based on open standards and with the flexibility to be relevant for 15 to 20 years 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 networks in the last mile. However, before describing in greater detail IPv6 networking components such as IP addressing, security, quality of service (QoS), routing, and network management, it is worth asking why we should use end-to-end IPv6. After all, IPv6, as with any other technology, 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 Systems Network Architecture (SNA) (through data-link switching [DLSw]), Appletalk, DECnet, Internetwork Packet Exchange (IPX), and X.25, 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 capital expenditures (CapEx) and operating expenses (OpEx) [SNA-IP], along with significant technical limitations[1], including lack of end-to-end capabilities in terms of QoS, fast recovery consistency, single points of failure (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 (that is, IP running on each and every device in the network) will be, in many ways, a much superior approach for multiservice FANs as shown in Figure 2.

Figure 2. Multiservice Infrastructure for Last-Mile Smart-Grid Transformation


Multiservices Field Area Networks
AMI Operations
AMI Data Center: Destination of FAN AMI Traffic, Source of AMI Requests
Network Management and Security Management Operations
Network Operation Center; Used to Manage and Secure the Network Components
DA Operations
Distribution Automation Control Center; Destination of Critical SCADA Traffic
Head-end Aggregation VPN Routers
Public or Private IP WAN Infrastructure (Cellular (2G/3G/LTE), WiMAX, Fiber/Ethernet....)
Field Area Routers
WAN Tier
NAN Tier
IP-based RF Mesh or PLC Neighborhood Area Network
Protection and Control Networks
Work Force Automation
AMI Metering/ HAN Gateway
Transformer Monitoring
Distribution Automation
EV Charging Infrastructure
Direct Load Control
Outdoor Lighting
Gas/Water Meters
Distributed Generation
SCADA Protection and Control Network
Direct Connect AMI Meters

Source: Cisco

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

4. The Unique Requirements of Constrained Networks

Devices deployed in the context of NANs are often constrained in terms of resources and often named IP smart objects. Smart-object networks are also referred to as low-power and lossy networks (LLNs) considering their unique characteristics and requirements. As a 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 hundred kbps and forming a meshed network for helping to ensure 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 1901.2) 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 to manage traffic paths based on node capabilities, for example, powered electric meters able to forward traffic and coexisting 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 power as they require and are highly redundant (multiprocessors, supporting Nonstop 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 can create challenges. For example, one of the golden rules in an LLN is to "underreact to failure." Contrast this with routing protocols, such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (ISIS), where the network needs to reconverge within a few dozen milliseconds. Meeting this challenge required a real paradigm shift, since overreaction would lead, very rapidly, to network collapse. Furthermore, control-plane overhead should be minimized, while supporting dynamic link and 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 as discussed later in this paper. In addition, the IETF Light-Weight Implementation Guidance [LWIG] Working Group (WG) is developing implementation guidelines for constrained 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

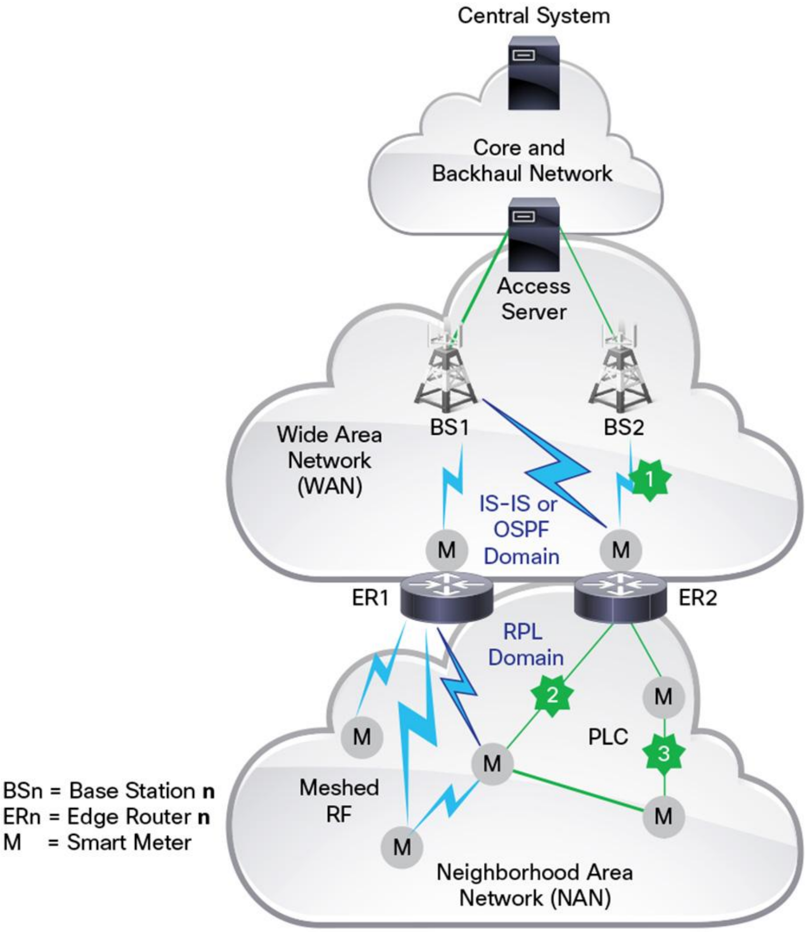
Today, the Internet runs mostly over IP version 4 (IPv4), with exceptions in academic and research networks, leading Internet service providers or enterprises, and government networks (where IPv6 is increasingly being deployed). However, the Internet faces a major transition [OECD] due to the exhaustion of address pools managed by the Internet Assigned Numbers Authority (IANA) since February 2011. With little existing IPv4 networking legacy in the areas of AMI and DA, there is an opportunity to start deploying IPv6 as the de facto IP version for new network implementations. The industry has been working on IPv6 for nearly 15 years, and the adoption of IPv6, which provides the same IP services as IPv4 (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 the latest 3G cellular evolution known as Long-Term Evolution (LTE).

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 FAN deployments benefits from several features:

- A huge address space to accommodate any expected millions of meter deployments (AMI), thousands of sensors (DA) in the hundred-thousands of secondary substations, and, additionally, all standalone meters. Its address configuration flexibility helps it adapt to the size of deployments as well as the time-consuming process of installing small devices. The structure of the IPv6 address is also flexible enough to manage a large number of subnetworks that may be created by future services such as EV 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 PLC infrastructures (IEEE 1901.2) using the IPv6 over low-power wireless personal-area network (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). RPL is an IPv6-only protocol.

This goes without forgetting all well-known IP feature sets, which help enable design variations for the deployment of highly available and highly secure communications infrastructure tying a network operations center (NOC) and all NANs through public and/or private WAN links such as shown in Figure 3.

Figure 3. Example of Basic Last-Mile Smart-Grid Infrastructure with Several Levels of Redundancy



Source: Alliander

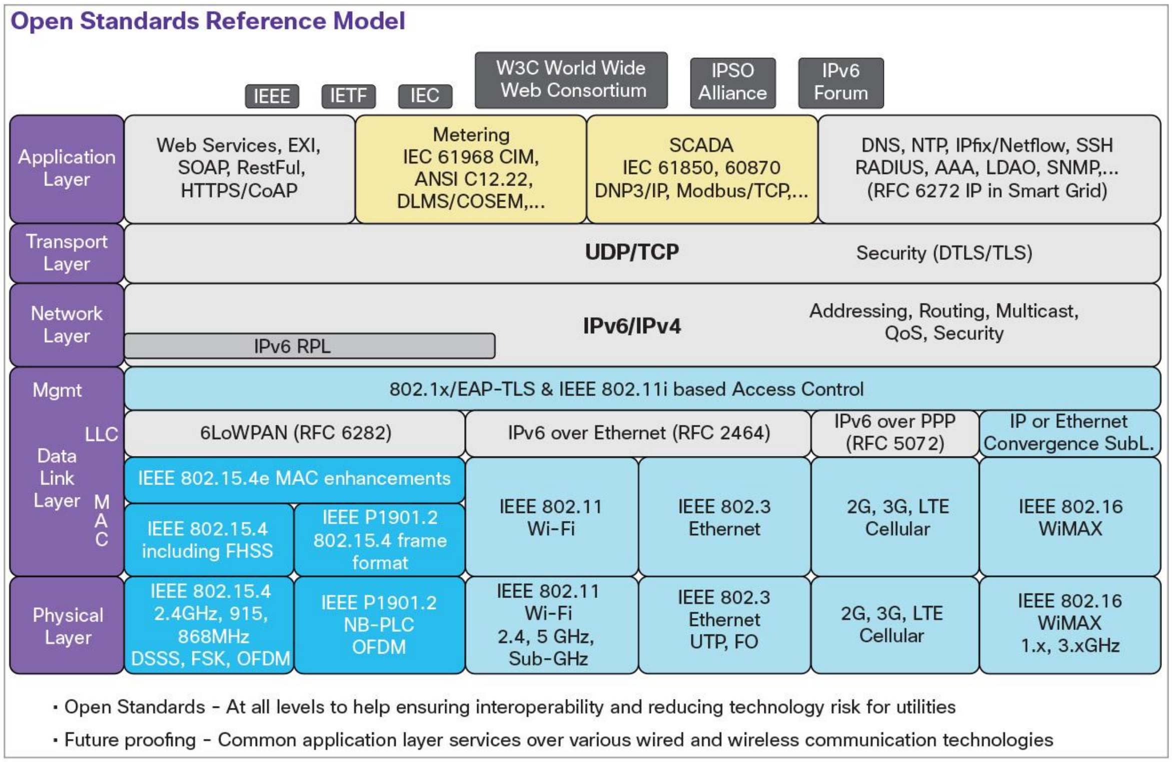
The headend system of a basic FAN, as shown in Figure 3, collects the meter readings, maintains meter configurations, and monitors network operations. It has end-to-end connections to the meter nodes, provided by WANs and NANs. So, while the physical connections to the meter nodes change from WAN to 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, these routers connect to the WAN, enabling bidirectional data streams between WAN and NAN. In case of multiservice infrastructures, it may be expected that IP edge routers have to be configured as dual-stack (that is, IPv6 and IPv4) and will be capable of tunneling IPv6 over IPv4 or the converse. This may be required when connecting legacy DA devices that only run IPv4 over serial or Ethernet interfaces, or when providing remote workforce connectivity to an IPv4 intranet, or when using IPv4-only WAN infrastructure, such as General Packet Radio Service (GPRS). The IP edge router has to be properly configured to accommodate scenarios 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.

DSOs require redundancy as a means to improve communication reliability in the LLNs, as well as to measure against vendor lock-in and technology lock-in because of incompatibility in lifetime expectancies 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, highly reliable, fiber connection or by public, flexible, cellular communication technology, such as GPRS, 3G, or LTE. An IP edge router can be colocated with a metering node or located as a separate entity in a substation, while the majority of the metering nodes communicate over a meshed NAN through 6LoWPAN, IPv6, or 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 points 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 piece of equipment that handles states and translates protocol unavoidably leads to communication failure.

This allows DSOs also to optimize on CapEx and 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 lifecycle and a risk to deploy. However, using it for WAN access only easily mitigates this risk and supports 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 node groupings to achieve mesh capabilities (that is, 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, to help ensure the WAN communications. Later, it will serve as a foundation for a larger NAN that will grow as soon as more neighbor nodes are deployed.

Figure 4. An IPv6 Networking Stack for Smart-Grid FANs



Open Standards Reference Model

IEEE | IETF | IEC | W3C World Wide Web Consortium | IPSO Alliance | IPv6 Forum

Application Layer: Web Services, EXI, SOAP, RestFul, HTTPS/CoAP | Metering IEC 61968 CIM, ANSI C12.22, DLMS/COSEM,... | SCADA IEC 61850, 60870 DNP3/IP, Modbus/TCP,... | DNS, NTP, IPfix/Netflow, SSH RADIUS, AAA, LDAO, SNMP,... (RFC 6272 IP in Smart Grid)

Transport Layer: UDP/TCP | Security (DTLS/TLS)

Network Layer: IPv6/IPv4 | IPv6 RPL | Addressing, Routing, Multicast, QoS, Security

Mgmt: 802.1x/EAP-TLS & IEEE 802.11i based Access Control

Data Link Layer, LLC: 6LoWPAN (RFC 6282) | IPv6 over Ethernet (RFC 2464) | IPv6 over PPP (RFC 5072) | IP or Ethernet Convergence SubL.

Data Link Layer, MAC: IEEE 802.15.4e MAC enhancements | IEEE 802.15.4 including FHSS | IEEE P1901.2 802.15.4 frame format | IEEE 802.11 Wi-Fi | IEEE 802.3 Ethernet | 2G, 3G, LTE Cellular | IEEE 802.16 WiMAX

Physical Layer: IEEE 802.15.4 2.4GHz, 915, 868MHz DSSS, FSK, OFDM | IEEE P1901.2 NB-PLC OFDM | IEEE 802.11 Wi-Fi 2.4, 5 GHz, Sub-GHz | IEEE 802.3 Ethernet UTP, FO | 2G, 3G, LTE Cellular | IEEE 802.16 WiMAX 1.x, 3.xGHz

- Open Standards - At all levels to help ensuring interoperability and reducing technology risk for utilities
- Future proofing - Common application layer services over various wired and wireless communication technologies

Source: Cisco

Figure 4 summarizes the whole proposed IPv6 end-to-end architecture for FANs 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 affecting the rest of the stack. As another example, the routing function taking place on Layer 3 helps enable new link layers to be added without affecting 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 reused 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 change in technologies. Every three to five years, physical and data link layers evolve, offering greater bandwidth, enhanced robustness, longer reach, lower cost, etc. This evolution contributes to the success of the IP architecture, which supports smooth evolution and upgrades 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 means new technologies and services can be 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 plus the addition of new protocol and feature sets via software or firmware upgrades, plus the coexistence of different generations of meters and physical and data link layers to improve 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 WANs that connect the information system.

Looking at existing AMI projects around the world, it is obvious that several physical and data link layer technologies will be selected for the last mile of smart-grid FAN infrastructure and/or to connect the last mile to the NMS/headend 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 1901.2) because current deployments include non-IP, closed, or proprietary solutions.

The physical and data-link layer standardization is outside the scope of the IETF. IETF only defines how IP and upper layers run on top of the MAC and PHY layers standardized by the 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 1901.2 narrowband PLC because they are fully aligned with the IP layered architecture and well-suited to AMI networks.

IEEE 802.15.4g Smart Utility Networks (SUN)

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 kbps) in the 2.4GHz ISM frequency band.

IEEE 802.15.4g-2012 adds new PHY support for 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 450 MHz to 2450 MHz and working in one of these three modes:

- Orthogonal frequency division multiplexing (MR-OFDM) PHY: Provides higher data rates at higher spectral efficiency
- Multirate and multiregional offset quadrature phase-shift keying (MR-O-QPSK) PHY: Shares the characteristics of the IEEE 802.15.4-2006 O-QPSK PHY, making multimode systems more cost-effective and easier to design
- Multirate and multiregional frequency shift keying (MR-FSK) PHY: Good transmit power efficiency because of 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 1901.2 Power Line Communication

Power Line Communications (PLC) systems provide the ability to transmit data over power lines.

Also known as a "no new-wire technology," PLC simply reuses the electrical wire of mains-powered devices. Carrying data over existing wires significantly reduces 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 comes 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 stack
- Possible high-propagation losses
- Frequency-dependent attenuation
- Changing characteristic impedance caused by cable transition and devices connected
- Noise and interference generated by connected devices 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 WG started to specify such standards for PLC. While IEEE 1901 has been published covering in-home and broadband PLC, the IEEE 1901.2 Task Group has standardized the narrowband PLC, which is used by utilities, also for the last-mile AMI infrastructure.

The expected benefits of the IEEE 1901.2-2013 standard for narrowband PLC are:

- Open PHY (OFDM-based) and MAC layers definition allows chipset vendors to develop their offerings 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 1901.2 PLC beyond AMI; for example, EV charging station, street lighting, power plugs, solar panels and inverters, and HANs
- Helps enable medium voltage and low voltage crossing for grid-to-utility meter communication and helps to lower deployment costs with reducing the number of concentrators
- Facilitates coexistence with other existing narrowband and broadband power line (BPL) technologies with dedicated bandwidth

- Addresses the necessary security requirements that help ensure communication privacy and allow use for security-sensitive services
- By aligning the MAC layer with IEEE 802.15.4 MAC and taking advantage of the work done by IETF 6LoWPAN WG, in particular for header compression, it helps enable straight IPv6 support and simplifies the "learning curve" when running both IEEE 802.15.4 and PLC

The resulting IEEE 1901.2-2013 standard can naturally fit with the IP layering architecture and make 1901.2 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 helps to ensure that the FAN infrastructure can benefit from new link layer 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 describes how an IPv6 packet must get encapsulated over an Ethernet frame, and is also used for IEEE 802.11 Wi-Fi. Similarly, the IETF 6LoWPAN WG 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 LLNs such as IEEE 802.15.4. 6LoWPAN WG led to the publication of RFCs specifying:

- Header compression (RFC 6282), which reduces the effects of sending IPv6 40-byte headers and User Datagram Protocol (UDP) 8-byte 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 because 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, other link layers now reuse them as long as they adhere to the IEEE 802.15.4 MAC and addressing scheme. For example, this is the case for the IEEE 1901.2 narrowband PLC link layer and DECT Ultra Low Energy (ULE) or Bluetooth Low Energy (LE) or other technologies as now discussed in IETF 6LO WG.

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 FANs 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 business-to-business (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 endpoints 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 endpoint are available:

- **Manual configuration:** This method is appropriate for headend and NMS servers that never change their address, but is inappropriate for millions of end-points, such as meters, because of the associated operational cost and complexity.
- **Stateless autoconfiguration:** This mechanism is 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 autoconfiguration:** Through the use of Dynamic Host Control Protocol for IPv6 (DHCPv6) Individual Address Assignment, this method requires DHCPv6 server and relay to be configured in the network. It benefits from strong security because the DHCPv6 process can be coupled with authentication, authorization, and accounting (AAA), plus population of Domain Name System (DNS) available for headend 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 and in NMSs or establishing filtering and firewalling across the infrastructure.

5.4. Routing

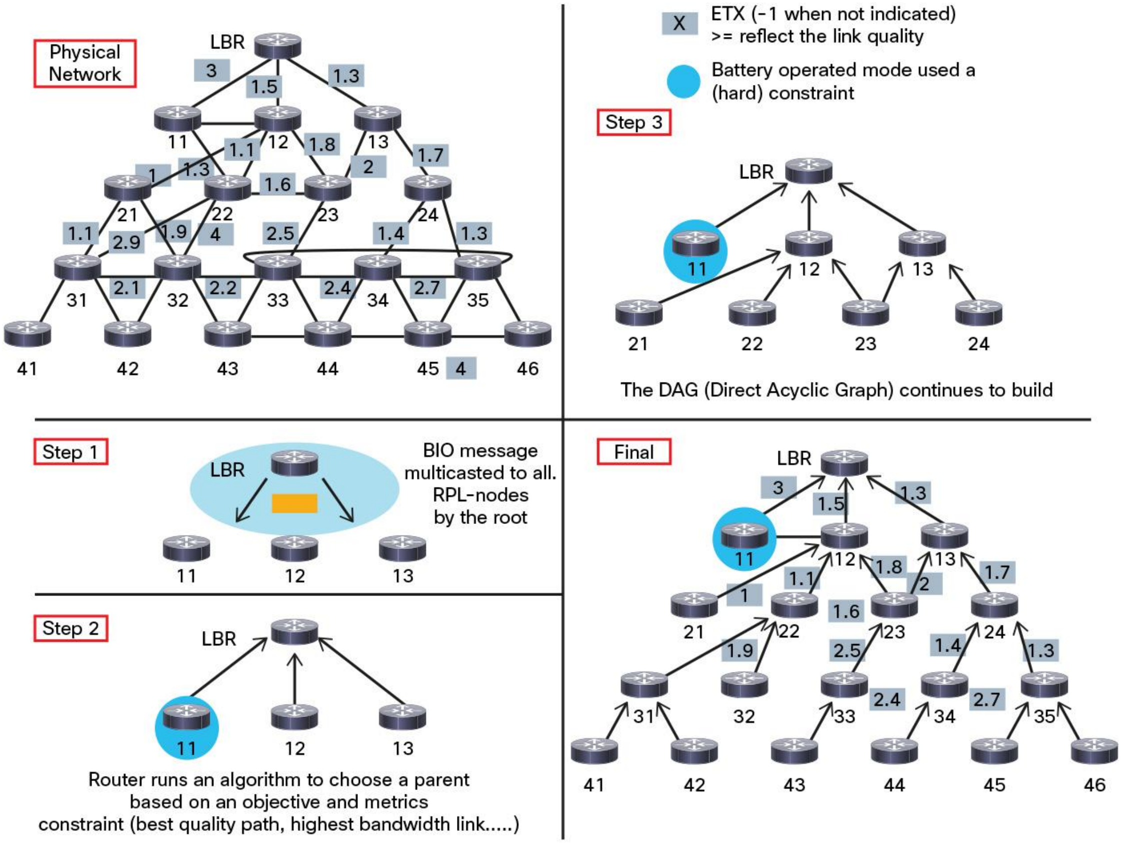
Proprietary systems originally developed for application-specific sensor networks usually neglect the architectural aspect of a scalable networking architecture. In most of these systems, it is not rare to find nonlayered architecture, despite the lack of flexibility and scalability, with a layer violation. 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 limits itself to a single data link layer technology. It therefore becomes impossible to mix or add data link layer technologies, which is a fundamental requirement of FANs (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 superposing two routing protocols (both at the IP layer and the link layer; this is for example the case when the NAN becomes a multiservice network, a transit network to other networks), which is an architecture that has proven to be extremely complex, expensive, and difficult to manage even in an unconstrained classic network (IP over ATM (Private Network-to-Network Interface [PNNI]) is one of the notorious examples). Adding this level of complexity to AMI networks hurts the requirements for scalability, ease of operations, and support for long device lifecycles.

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 conducted to determine whether an existing routing protocol (OSPF, etc.) 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 rechartered, and after almost two years of intensive work performed by numerous industry routing experts, RoLL WG published a new distance-vector routing protocol, called IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL).

Figure 5. Basic Network RPL Initialization Steps


Physical Network
LBR
3
1.5
1.3
11
12
13
1.1
1.8
1.7
1
1.3
2
1.6
21
22
23
24
1.1
2.9
1.9
4
2.5
1.4
1.3
31
32
33
34
35
2.1
2.2
2.4
2.7
41
42
43
44
45
4
46
X
ETX (-1 when not indicated)
>= reflect the link quality
Battery operated mode used a (hard) constraint
Step 3
LBR
11
12
13
21
22
23
24
The DAG (Direct Acyclic Graph) continues to build
Step 1
LBR
BIO message multicasted to all. RPL-nodes by the root
11
12
13
Step 2
LBR
11
12
13
Router runs an algorithm to choose a parent based on an objective and metrics constraint (best quality path, highest bandwidth link.....)
Final
LBR
3
1.5
1.3
11
12
13
1.1
1.8
2
1.7
1
1.6
21
22
23
24
1.9
2.5
1.4
1.3
31
32
33
34
35
2.4
2.7
41
42
43
44
45
46

Source: Cisco

RPL provides support for a large number of technologies and features (as documented in [RPL-WP]) that matches all service requirements reviewed in the introduction. One of the key characteristics of RPL is that the protocol is highly flexible and dynamic; it has 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 numerous advanced features, such as trickle timers limiting the chattiness of control plane, dynamic link (hop count, throughput, latency, link and path reliability, link colors) and node (node state or 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 underway. 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 FANs as documented in the applicability statement [RPL-AMI]. In combination with more traditional IP routing techniques, such as route redistribution, load balancing through multiple IP edge routers, and dynamic rerouting in case of hardware or WAN failures, RPL deployment meets all the capabilities required by large and scalable FAN infrastructure.

It is 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 coexistence 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 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 taken advantage of the scalable IETF Differentiated Services (DiffServ) architecture for IP quality of service (QoS) when integrating critical classes of traffic over their IP networks. Therefore, the mix of traffic, including metering, DA, and remote workforce management, flowing over the last mile of the smart-grid network can be controlled and prioritized according to defined service-level agreement (SLA) policies in terms of delays, jitter, packet loss, and scheduling. Thus, it’s important to consider the variety of QoS mechanisms and their adaptation to the constrained AMI environment:

- **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 class of service (CoS). This allows appropriate prioritization of the packets through other forwarding nodes.
- **Scheduling and congestion avoidance techniques:** These techniques give priority to traffic according to their CoS. For example, a device in a RF or PLC mesh network can implement several queues, enabling real-time traffic from DA sensors to pass through an interface with high priority.
- **Call Admission Control (CAC) techniques:** These methods reserve bandwidth for high-priority traffic, for example on an edge router connecting the last mile to the headend system through low-speed cellular networks.
- **Multiple RPL directed acyclic graph (DAG):** As discussed in the RPL section, the routing metrics could build different DAGs, 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, the appropriate definition of Differentiated Services Code Points (DSCP) will help fine-tune 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. Network security tops that list. Thus, security represents a key challenge for helping to enable a successful rollout of smart grids and AMIs. It needs to be addressed in a holistic, end-to-end fashion, taking advantage of 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 nonstandard networking protocols increases security and which is unanimously rejected by the network security expert community. Security is not a new topic to utilities because 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, and 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 multilayer challenge, it is important to review some additional features that provide node authentication and data integrity and privacy on a FAN deployment.

Strong authentication of nodes can be achieved by applying a set of open-standards mechanisms. For example, after a node discovered a RF or PLC mesh network using 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 takes advantage of 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 1901.2), Layer 3 (IP Security [IPsec]), Layer 4 (Datagram Transport Layer Security [DTLS]), or per application at Layer 7 (that is, 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, memory, and energy consumption) requirements must be evaluated in regard to the additional hardware cost this could generate. With multiple options available, nodes can be integrated into existing network 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, for example, by providing a highly secured end-to-end path, and where other functions (such as message integrity and proof of origin) can remain at the application layer.

The choice of a given layer for data encryption, as well as devices performing the encryption, also affects the network services, performance, and scalability of a deployment. For example, for a software upgrade, DR or dynamic pricing should use multicasting, the choice of encrypting data at the transport layer (Layer 4 DTLS) precludes using 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 be limited 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 losing network service capabilities.

Combined with more traditional security features such as digital signatures for firmware images or data objects on devices (for example, 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 a well-known technology, offers already available, tested, and 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-case solutions, such as AMI or DA, handle most, if not all, services at the application layer. By adopting IPv6 for the last mile (and therefore enabling bidirectional IP end-to-end communications) there is the opportunity of using well-known services from the open-standards IP architecture, decreasing complexity, and supporting many required services of smart-grid applications, which could stay focused on utility data and application requirements, help to achieve modularity and scalability, and deal with security at all levels. However, to be able to use 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 because IPv6 adoption for the last mile requires changes on the headend 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 endpoints with constrained resources and subnets built with low bandwidth, it is important to stress that gathering network statistics for network management can be achieved through a pull model (for example, Simple Network Management Protocol [SNMP]), as well as a push model (for example, 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 Table 6 is an opportunity to introduce a new protocol called Constrained Application Protocol (CoAP) designed by the IETF Constrained Restful Environments (CoRE) WG. 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 representational state transfer (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.

Table 1. Taking Advantage of IP Network Services

Network Services	Layers and Services	Benefits
Unique device's addressing (Network Layer)	From IPv4 (32-bit address space, now deprecated at IANA) to IPv6 (128-bit address space), including multiple scopes (global, private, link)	Large address space able to cope with the IOT evolution. Private or public infrastructure
Address auto-configuration (Network Layer)	Manual (IPv4/IPv6), stateless (IPv6) and stateful (DHCP for IPv4 and IPv6), Prefix Delegation (DHCPv6 PD)	Centralized or distributed address management. Additional DHCP options Zero Touch Provisioning
Media independency (PHY & MAC layers)	IEEE 802.3 Ethernet, IEEE 802.11 Wi-Fi, IEEE 802.16 WiMAX, IEEE 802.15.4g/e RF 6LoWPAN, IEEE 1901.2 NB-PLC 6LoWPAN Serial, ATM, FR, SONET/SDH	Media diversity for local and backhaul communications Smooth evolution over long lifetime period **Note:** IPv6/6LoWPAN is the only IP protocol version defined for IEEE 802.15.4g/e and 1901.2.
Routing (Network Layer)	Static, RIP, OSPF, E-IGRP, IS-IS, MP-BGP, RPL (IPv6 only)	Dynamic reactivity to communication and network device failures. Scalability of deployment
Data Integrity and Confidentiality, Privacy (all layers)	Layer-2 (MAC specific), Layer-3 (IPSec IPv4/IPv6), Layer-4 (TCP/TLS, UDP/DTLS) and Layer-7 (application dependent authentication & Encryption) Packet filtering, Deep packet inspection (DPI), Intrusion Detection Service (IDS), Flow monitoring	Multi layered secure networking
Multicast (Network layer)	IPv4/IPv6 multicast protocols: IGMP/MLD, PIM, MP-BGP	Scalable software upgrade, group commands
Quality of Services (QoS)	Specific MAC layers Class of Services (CoS), i.e. Ethernet, WiMAX IPv4/IPv6 QoS Differentiated Services architecture	Multi services field area networks Prioritization of data traffic Service Level Agreement
Network Segmentation and isolation	Virtual Private Networks (Layer-3), i.e. IPSec VPN, VRF-Lite	Shared infrastructures but dedicated and isolated traffic paths for critical applications
Time Distribution	Layer-3, i.e. Network Time Protocol version 4 (NTPv4)	Secure NTP4 for both IPv4 and IPv6
Management	DNS, IPFix, SNMP, CoAP, SSH, Telnet, XML/Netconf, etc.	Push and Pull management models Scalable end-point management

Source: Cisco

6. Conclusion

The IP protocol suites have been deployed in private and public networks 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; and 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 because the layered nature of the architecture provides a very high degree of flexibility.

Field Area Networks (FANs) 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, which include flexibility, reliability, QoS, security, manageability, and scalability, are absolute requirements that explain why IPv6 was evaluated as the most appropriate networking architecture for FANs. Additionally, FANs impose constraints.

For example, links are not only low-speed (which is no different than in the early days of the Internet), but also 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, including addressing, address provisioning, QoS, transport, reliability, etc., could be reused "as is," plus several new IPv6 protocols have been specified to meet the unique requirements of the last mile in smart-grid networks.

We are at the beginning of an exciting journey that will extend the use of IPv6 to billions of a new type of devices, such as meters and sensors deployed in FANs. 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, led by innovation in communication technology at its own pace, independent from the information system
- **Longevity:** Adoption of new standards when available and required; no major architecture changes in the sense of any necessary "cut-over day" but instead an evolutionary path
- **Industry transformation:** Ease the infrastructure convergence for multiservices such as metering, distribution automation, and workforce communications
- **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 operations and customer support
- **Security:** Strong security through IP solutions, also taking advantage of associated industry processes and an IT professional ecosystem
- **Interoperability:** IP devices work together in a multiservice network sharing a common physical infrastructure with no need for complex and hard-to-manage multiprotocol gateways

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

[SNA-IP] In the 1990s, 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 IP-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)**

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

Contributors

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, 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 at EANDIS, info@earchitect.be

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

Bernard Tourancheau, Professor INP, 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 Fellow, Texas Instruments, shaver@ti.com

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