http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

D2-02_04

Building an Interoperable Grid with Industry-Standard IPv6 Architecture

Paulo Pereira

Cisco Systems

(PT)

SUMMARY

The broad adoption of open standards is vital to smart grid success. It is generally accepted that open standards enable interoperability, reduce costs of ownership, and encourage innovation. However, today's electric grids are far from interoperable, with systems comprising a combination of proprietary and open standards and designed to support application like advanced metering in silo deployments. To arrive at a truly smart grid, the best-practices approach is to run multiple applications over a common, secure, enterprise-class network infrastructure that remains agnostic to the growing number of applications and devices running on it. This vision guides a joint development effort to develop a native IPv6 reference architecture for smart grid networking that will be made available to the entire industry. This session will review the progress of this effort, key architectural and design attributes, and an overview of early utility deployments.

KEYWORDS

Interoperability, Standards, Multi-services, Secure, Scalable, Architecture, Management

* Lagoas Park, Ed 12, Porto Salvo
Fax: + 351 21 454 1000 e-mail: pauloper@cisco.com

Industry Drivers and Challenges

Last mile networks have gained considerable relevance for power utilities over the past few years. These networks - referred as Neighborhood Area Networks (NAN) in this document – can support a variety of applications including not only meter reading, but also advanced applications such as demand-response (DR), distribution automation (DA), which allows distribution monitoring and control, automatic fault detection, isolation and management, distributed energy resources (DER), electrical vehicle charging (EV), etc.

Field Area Networks (FAN) is the combination of NAN and communication device offering the backhaul WAN interface(s). The FAN can serve as backhaul network 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.

With the emergence and proliferation of these advanced applications it is expected that the traffic volume across the Field Area Networks (FAN) 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 IP networks and 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 (P2P) in some cases and point-to-multipoint (P2MP) in some other cases.

● **HAN applications -** HAN applications typically require communication between home appliances and the utility head-end server through individual meters or concentrators acting as application's gateways.

● **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. Verifying user and account information would require communication 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).

- **Network Management -** As the FAN, 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.

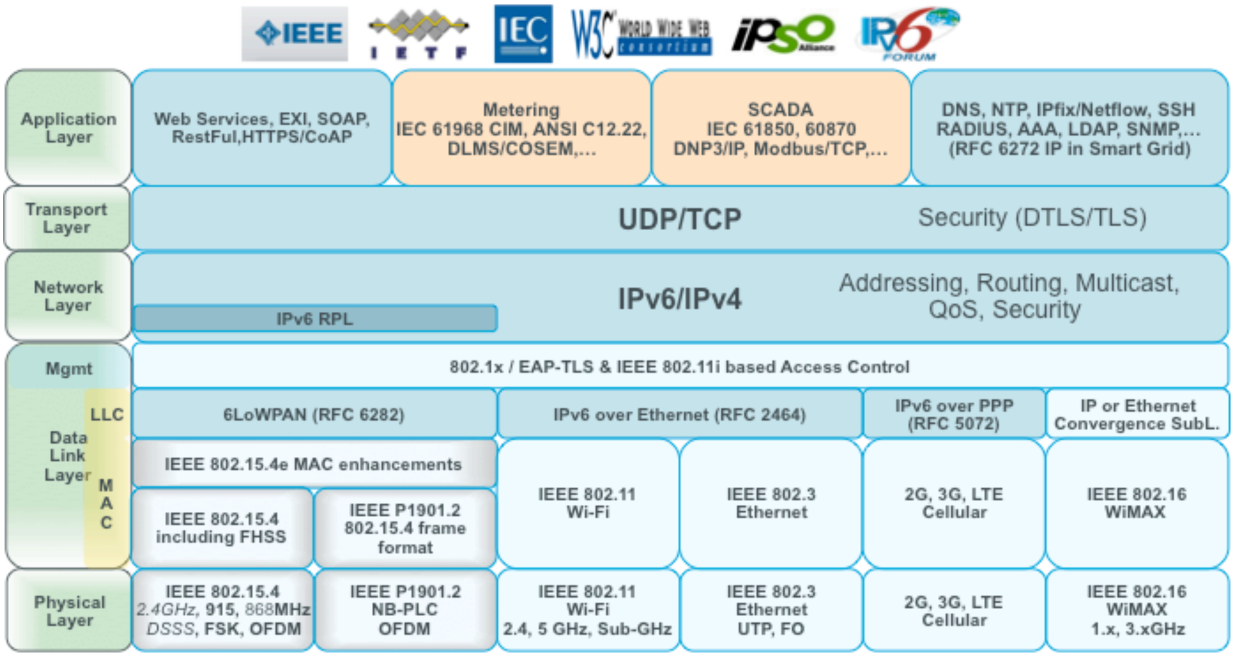
- **Multicast Services -** Groups of meters may need to be addressed simultaneously using multicast, e.g., to enable software upgrade or parameters updates sent by a network management system (NMS) to all meters using multicast.

As we will see in the next two sections, an IPv6 standards-based architecture for the FAN will address these complex communication challenges with many benefits for the power utility. This communications architecture however is not self-contained in the FAN. It extends to the Wide Area Networks (WAN), Data Centres and can even extend to the Primary Substations with the increasing trend for distributed control but also for communications optimization.

IPv6 Technology for Power Utilities

Cisco and other companies are determined to deliver a definitive Internet Protocol (IP)-based communications and control platform for the power utilities market, and help advance consistent and reliable delivery of energy across the electric distribution system. These developments creates the first IPv6-based enterprise-class utility networking solution by combining grid applications, such as advanced metering, with the Cisco connected grid architecture, cyber security technology, and communications expertise.

Cisco and world leaders in smart metering and distribution automation are delivering a standards-based, highly secure and scalable communications platform that is simple to deploy and manage and extensible to multiple utility applications.


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, LDAP, SNMP,... (RFC 6272 IP in Smart Grid)
Transport Layer
UDP/TCP
Security (DTLS/TLS)
Network Layer
IPv6/IPv4
Addressing, Routing, Multicast, QoS, Security
IPv6 RPL
Mgmt
802.1x / EAP-TLS & IEEE 802.11i based Access Control
Data Link Layer
LLC
MAC
6LoWPAN (RFC 6282)
IPv6 over Ethernet (RFC 2464)
IPv6 over PPP (RFC 5072)
IP or Ethernet Convergence SubL.
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

Benefits of IPv6 standards based architecture

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.

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 connected grid infrastructure brings future proofing through smooth evolutionary steps that do not modify the entire industrial workflow. Key benefits of IP for a power utility are:

• **Open and Standards-based:** The core components of the network, transport, and applications layers are 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, IEEE, and ITU.

• **Versatile:** Last-mile infrastructure in the connected 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. Various media can be used in a deployment and, over time, without changing the whole solution architecture and data flow.

• **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. The benefits of 30 years of operational IP networks are sets of well-understood network management and security protocols, mechanisms, and toolsets.

• **Stable and Resilient:** With more than 30 years existence, IP has established itself as a workable solution considering its large and well-established knowledge base. More important is how we can leverage these 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 design, deploy, and operate 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.

Multi-service Communications Network

Several hardware and software capabilities are necessary to deploy a true multiservice network: Quality of Service (QoS); IPv4 and IPv6 dual stack network; traffic segmentation and security; proactive monitoring and performance management; hardware modularity; application installation; etc. This section will focus on QoS only.

Quality of Service (QoS) refer to the ability of the network to provide priority service to selected network traffic, providing improved and more predictable network service by:

- Supporting dedicated bandwidth
- Reducing loss characteristics, DA real-time traffic prioritization
- Avoiding and managing network congestion, multiservice traffic
- Shaping network traffic, for example, remote workforce traffic
- Setting traffic priorities across the network, multiservice capabilities

QoS is a key feature when designing multiservice FANs, because there is a need to differentiate and prioritize between traffic from AMI, DA, Remote workforce, and network management use cases.

Estimated transport losses, delay, and jitter introduced by networking devices must be understood when forwarding sensitive data, particularly when a WAN backhaul link offers a limited amount of bandwidth.

On a multiservice FAN, QoS DiffServ and CoS can apply to traffic categorized as:

- IPv4 traffic: DA, Remote workforce, protocol translation, and network management
- IPv6 traffic: AMI, Remote workforce management, and network management
- Layer-2 traffic: IP QoS mapped to WiMAX CoS over WiMAX WAN backhaul

While some AMI traffic (for example, power outage notifications) might require true real-time capabilities, DA has different requirements that require understanding of the latency and jitter across networking devices.

This specification can occur in different ways, for example, using the IP Precedence bit settings in IP packets or source and destination addresses. Use QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queuing.

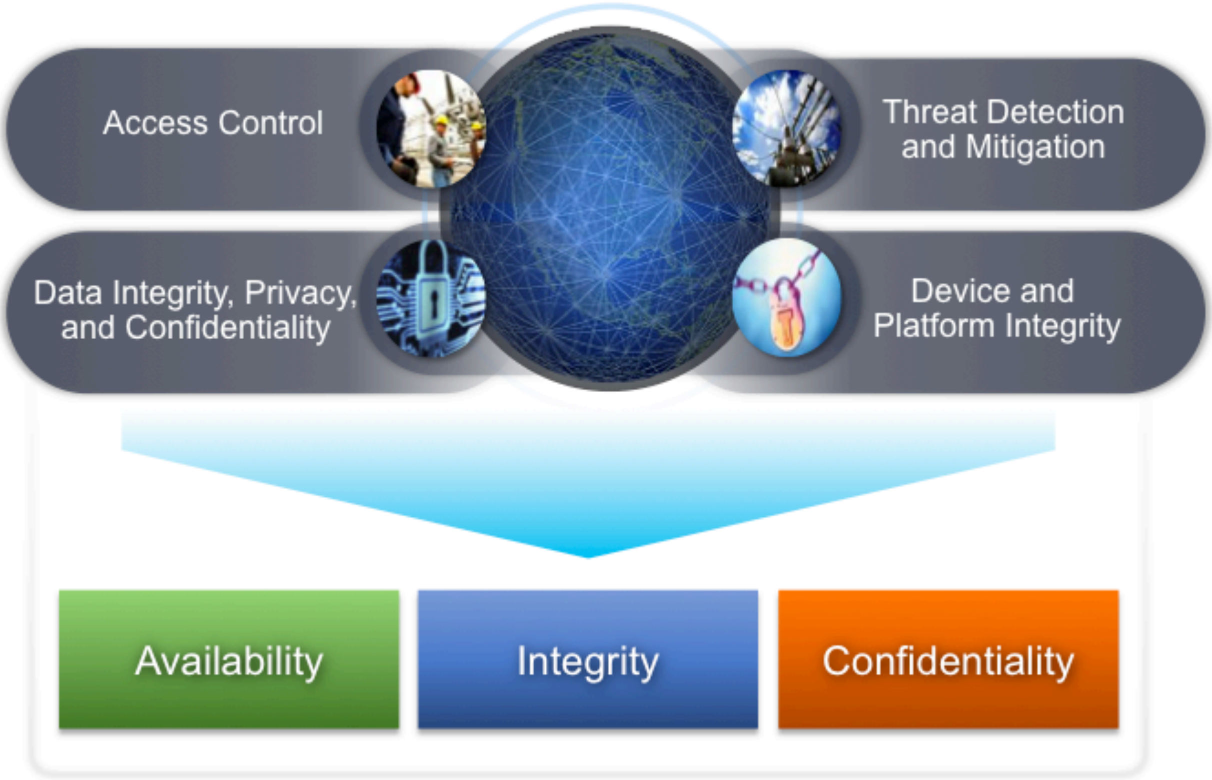
QoS for the grid-mesh architecture is designed considering multiservices FAN scenarios, where traffic from NAN, Ethernet, and Serial interfaces are mixed over the WAN backhaul.

Security

Today's utilities main security challenge is to move away from security by obscurity and include security as a fundamental building block of any network architecture. The main security concerns with the grid modernization are:

- Protection of critical infrastructure
- Uptime and availability
- Meeting regulatory requirements (ex. NERC CIP)
- Network device access control
- Role-based user access control
- Vulnerability management and securing legacy devices
- Ensuring privacy of customer data throughout the system

The following connected grid security principles address the concerns mentioned before, when considered inside an architectural approach:


Access Control
Threat Detection and Mitigation
Data Integrity, Privacy, and Confidentiality
Device and Platform Integrity
Availability
Integrity
Confidentiality

Access Control Tools: RBAC, Port Security, Certificates, Authentication, Authorization and Accounting (AAA) for user and devices, Network Admission Control (NAC)

Data Confidentiality and Privacy Tools: X.509 Certificates, IPSec based on flexible VPN-Architectures, Scalable Key-Management, DMVPN or GETVPN

Threat Detection and Mitigation Tools: Zones, Segmentation, Access Lists, Firewalls and IPS, Logging

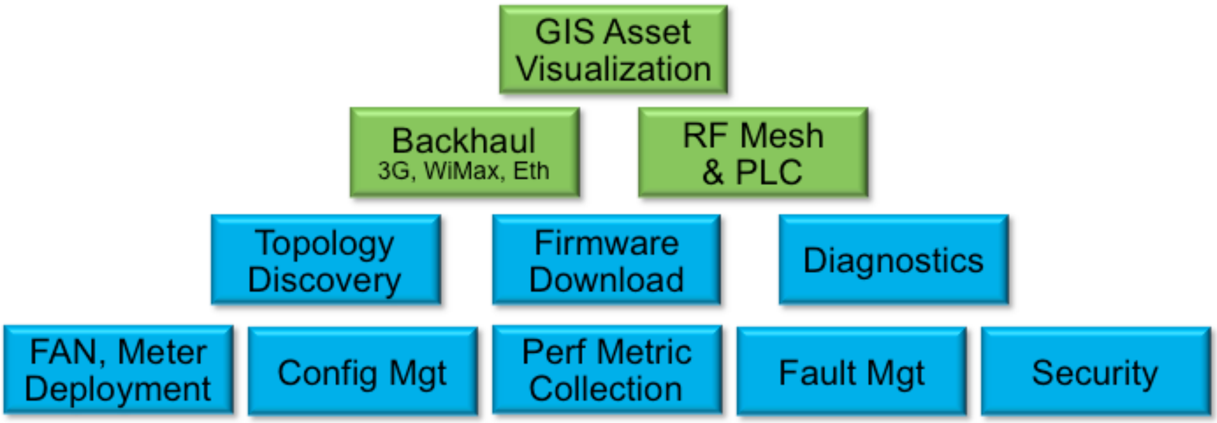
Integrity of Platforms and Devices Tools: Tamper-resistant design, authenticity and integrity of hardware and software

Management

Smart Grid FAN deployments approximate the scale of an Internet Service Provider (ISP) with tens or hundreds of thousands of sites in total, containing several million endpoints such as smart meters, sensors, actuators, and so on. Network management is performed by selecting protocols that are the most relevant to cope with the scale of the deployment as well as the device location and role. For high scale statistics collection, Connected Grid Endpoints use a push model (CoAP based), where the less numerous Field Area Routers or Head End Routers use either SNMP (pull model) or possibly Netflow/IPfix (push model).

CoAP: The push model represents a key feature to scale network management to millions of nodes that have scarce CPU resources. It is an opportunity to leverage a new Internet Engineering Task Force (IETF) protocol called Constrained Application Protocol (CoAP) designed by the 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.

CSMP: In addition to CoAP, the Cisco-designed CSMP (Cisco CoAP Simple Management Protocol) defines how network management objects are carried over CoAP. CoAP and CSMP are implemented on endpoints and NMS.



Secure zero-touch commissioning of devices by field worker, GIS context-view of field devices and their status, and visibility of business critical communications reduces need for truck rolls, reduces times for problem resolution and decreases commissioning costs of field communications equipment.

Cyber-security management and policy compliance for critical infrastructure network operations (NERC-CIP, Enterprise security policies, or other) should also be part of the management solutions, including features like robust access security for clear separation of responsibilities across different operational groups (AMI, DA etc).

Efficiently manage a large-scale business critical network where communication problems impact grid operations and utility business metrics by proactively monitor and address network faults before they impact business operations and optimize network operations based on historical, trending data.

Conclusions

The IP protocol suites have been deployed in a number of 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; the number of supported applications has exceeded all expectations by an order of magnitude. 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 power utilities infrastructures and the number of applications that these networks support keeps growing at a fast pace. Their networking requirements are similar to others and that explain why IPv6 was evaluated as the most appropriate networking architecture for Field Area Networks. Although the introduction of IPv6 is driven by the FAN modernization and new applications, we need to consider it inside an end-to-end architectural design that includes the WAN, the Data Center, the Primary Substations and other places in the network.

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.

To summarize, the IP adoption for the last mile enables: Interoperability; Scalability; Reliability; Future proofing (media and application diversity); Security; Advanced management; and Cost control.

BIBLIOGRAPHY

A Standardized and Flexible IPv6 Architecture for Field Area Networks, White Paper

http://www.cisco.com/web/strategy/docs/energy/ip_arch_sg_wp.pdf

Cisco Smart Grid Multi-services Field Area Network (FAN) Design Implementation Guide

Cisco Connected Grid Security for Field Area Network

http://www.cisco.com/web/strategy/docs/energy/C11-696279-00_cgs_fan_white_paper.pdf