Smart Grid Priority Action Plan
Guidelines for the Use of IP Protocol Suite for Smart Grid

What:

Develop approaches for developing Guidelines and profiles for use of **IP Protocol** for the smart grid. Examine the applicability and utility of the use of Internet protocol and supporting standards as the network communications infrastructure for proposed Smart Grid applications.

Abstract:

For interoperable networks it is important to study the suitability of Internet networking technologies for smart grid applications. This work area investigates the capabilities of protocols and technologies in the Internet Protocol Suite by working with key SDO committees to determine the characteristics of each protocol for smart grid application areas and types.

Description:

The Internet technologies consist of a set of protocols to network and transport data messages using IP packets, as well as a set of protocols to manage and control the network, such as routing, mapping of IP addresses, device management, etc. This protocol suite enables distributed applications to run over a set of interconnected networks. It also includes session- and transaction-oriented security mechanisms to provide security services.

Objectives:

- Review the communications networks and domains identified in the Smart Grid conceptual model and determine whether they are discussed in fine enough granularity to discuss the application of the Internet protocol suite
- Define the approach for fully defining the network and systems management requirements for Smart Grid networking infrastructures
- Define a set of standards profiles required for Smart Grid networks
- Identify key networking profiles issues including issues surrounding IPv4 vs. IPv6
- Determine the key remaining issues surrounding adoption of standardized networking profiles
- Determine appropriate Smart Grid network architectures and technologies appropriate for basic transport and security requirements (e.g., shared IP networks, virtual private networks, MPLS switching, traffic engineering and resource control mechanisms)
- Determine which transport layer security protocol(s) (e.g., TLS, DTLS, SCTP, and IPsec) are most appropriate for securing Smart Grid applications.
- Identify higher layer security mechanisms (e.g., XML, S/MIME) to secure transactions.
- Develop an action plan for development of necessary usage guides, profiles and remaining work.

Why:

The Smart Grid will need a comprehensive mapping of smart grid application requirements to the capabilities of protocols and technologies in a well define set of Internet Protocol Suite(s) or

Profiles. This should be defined by experts well versed in the applications and protocols including management and security. A set of well-defined networking profiles can be tested for consistency and interoperability to help ensure systems integration as appropriate across the Smart Grid. A set of consistent and testable protocol profiles is also necessary to ensure that the combination of technologies can meet not only today's requirements but meet future application needs as well.

The networking profiles defined by this work will define a significant portion of the interfaces to Smart Grid equipment and systems. Most notably the interfaces that integrate systems over Wide Area Networks and large geographical areas will need to be defined in part by these profiles. The networking profiles will define networking functions such as addressing and the integration of concepts such as multihoming and other key functions necessary for the Smart Grid.

Where:

The Smart Grid will use a variety of different networking environments across smart grid domains and sub-domains as identified in the smart grid applications and conceptual models. The suitability of the proposed protocol suites or profiles in specific application contexts should be analyzed against the requirements emerging for Smart Grid applications and the proposed scale and scope of Smart Grid networks. The analysis should identify which protocols are clearly applicable in specific application contexts (e.g. use of TCP/IP, UDP, TLS/SSL, IPsec , IPV4/IPV6, MPLS) and protocols for network control, management and security, in addition to identifying any existing gaps.

How:

This task will require the development of a combination of networking standards into well defined sets known as profiles. Working from existing and proposed Smart Grid applications and use cases the approach will require the distillation of Smart Grid applications and requirements into sets of networking profiles. These profiles will need to be developed into designs and implementations that can then be tested against the requirements. The communities that need to be involved include those within the Internet Engineering Task Force as well as other research communities that are working on networking technology.

Task Descriptions:

Develop along with project team.

Deliverables:

Develop along with project team.

Who:

Project Team
NIST Lead: David Su, david.su@nist.gov
EPRI Leads: Joe Hughes jhughes@epri.com , Erich Gunther, erich@enernex.com

Project Team
SDO Leads (IETF): Leslie Daigle, ISOC and IETF; Ralph Droms, IETF; Russ Housley, IETF chair; Dave Oran, IETF (Architecture); Henning Schulzrinne, Columbia U. and IETF; Richard Shockey, IETF (ENUM, SIP); Sean Turner, IETF; Geoff Mulligan, IETF (6LOWPAN); Jeff McCullough, IETF.
Other SDOs: ATIS , IEEE, TIA
Users Groups:
Technical Team:

When: [*Timeline for deliverables*.]

Task	Responsible	Date	Notes
Develop a clear set of requirements for specific Smart Grid application areas (include key non-functional requirements with fine enough granularity). Include power engineering applications, as well as the network / communications requirements.	Key group of domain experts (IEEE P2030, Dick DeBlasio; NAESB, ;Zigbee, Bob Heile; UCAiug, Chris Knudsen;…)		Include regulatory and other external sources of requirements. International perspectives included.
Definition of terms (where they need to be understood in context). Define “profile” in terms of applicability.	Key domain experts		Need to define domains and merge/integrate terms, i.e. reliability, security, transport, profile, etc.
Define specific Smart Grid (SG) applications that define distinct networking infrastructures. Define the set of RFC’s /supporting documents that establish an interoperable network.			Design decisions need to be made on defining the core set of RFC’s and supporting documents.
Identify a core set of Internet protocol suite supporting documents.	NAESB, ? ;IETF, Russ Housley; IPSO, ; NIST, David Su; UCAiug Open SG, Chris Knudsen.		Beware of legacy issues.

Application taxonomy to be created. Define well specified environments even within NIST Domains.	IPSO, Doug H., Fred Baker, NAESB		Use cases can be used to describe applications. (Example contributed: CIPs/Real Time, Emergencies, Low Bandwidth/Home, Rest of World)
Develop proposed models for key implementations (e.g. outage management); include Engineering Analysis.	UCAiug, NEMA, Sonoma Innovation (hosting mtgs), others.		Work the design to completion and evaluate. Look to bound the problem space. Get a good interdisciplinary team. Address an architecturally significant set of issues.
Identify lessons learned from networking community that could impact SG. This would include critical infrastructure issues.			Functions such as broadcasting are not done well…other issues need to be identified…multicast.
Identify application use cases that IP protocol suite doesn't do well and hence requires investigating something else.	Outcome of defining use cases…		Be careful of IP vs. something new. The trust domain is an emerging concern.
Testing and Certification for Suites of Standards. Identify plausible approaches, define types of testing needed.	TNIST, UCAiug Open SG		IETF doesn't do. NAESB is involved with testing assurance. Define who defines the tests and who implements testing. Include Quality Assurance.

Metrics:

Issues, Comments, or Observations of Note