(1) What are the current and future communications needs of utilities, including for the deployment of new Smart Grid applications, and how are these needs being met?

Utilities' current communications needs are diverse, with considerable variation from utility to utility. Current communications needs that are related to, but generally pre-date, smart grid include:

- System control and data acquisition (SCADA)
- Drive-by meter reading
- One-way direct load control
- Mobile workforce management
- Demand response, dynamic pricing for commercial/industrial customers

In the smart grid-enabled future, utility smart grid applications will require advanced communications technologies that are characterized at the neighborhood area network-level by:

- Ubiquitous coverage (>99% of all customers for a given utility)
- High bandwidth (but not necessarily broadband to every meter)
- Low latency (<1s for alarms/alerts, <100ms peer-to-peer)
- Open standards (e.g., Internet Protocol, AES encryption)
- Low cost (as measured by *total lifecycle cost*, not just by capital cost)

Utilities deploying smart grid solutions today are converging upon a network-first approach that addresses the prioritizes network connectivity at the neighborhood level by deploying robust radio frequency mesh communications that utilize Internet Protocol to leverage the unrivaled ecosystem of IP-based technology innovation for interoperability and cybersecurity.

(2) What are the basic requirements, such as security, bandwidth, reliability, coverage, latency, and backup, for smart grid communications and electric utility communications systems in general - today and tomorrow? How do these requirements impact the utilities' communication needs?

Security

- Smart grid communications systems should be designed with at least a 20-year threat model in mind.
- Retail attacks (e.g., compromise of individual endpoints) must be categorically prevented from escalating into wholesale attacks (e.g., compromise of entire categories of devices or the network itself).
- Over-the-air firmware upgrades must receive top-tier protections, such as

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

proven encryption technologies, digital authentication measures, and sophisticated role-based authorization techniques.

- Critical and sensitive smart grid functions, such as remote disconnects, should be additionally hardened with advanced technological and physical security measures.

Bandwidth

- Initial network capacity should exceed current requirements by at least 5 times (e.g., 15 minute intervals pulled every 4 hours requires ~15kbps, so starting point for smart grid networks initially designed for smart metering should be at least 75kbps).
- Bandwidth should be designed to be scalable to enable a cost-effective pathway to add network capacity in the future (e.g., the deployment of additional wide-area-network backhaul points accelerates the collection of data generated by radio (RF) frequency mesh neighborhood-area-networks).

Reliability

- Smart grid networks should be capable of providing reliability of at least 99.5%, backed by service level agreements. Such high reliability requirements reflect the mission-critical, just-in-time nature of the electric grid.

Coverage

- Smart grid networks should reach no less than 99% of all customers in any given utility service territory, preferably using a unified network platform, rather than separate siloed networks for urban and rural areas.
- To provide anything less than 99% coverage raises difficult questions of fairness and equity, since the costs of smart grid technologies are generally spread out among all utility customers.
- Arguments suggesting that 99% coverage is impractical due to the disproportionate costs of networking the last 10% of hard-to-reach customers have been proven to be invalid based upon performance demonstrated in modern RF mesh smart grid network deployments.

Latency

- Smart grid networks should be designed to accommodate the least latency-tolerant application foreseeable for broad deployment over the planned operating life of the network infrastructure. Normally, these applications require timely human interaction.
    - We note that some applications, such as substation Goose Messaging, may require extremely low latency, but represent too small a share of the total number of smart grid-networked devices in a fully implemented system to qualify as being broadly deployed. Accordingly, these extreme applications should not set the standard for

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

overall network latency.

- In most, if not all, cases, distribution automation represents the least latency-tolerant smart grid application available today, with requirements for less than 1 second of latency for alarms and alert communications and sub-100 milliseconds for messaging between peer-to-peer nodes inside RF mesh configurations.
- Due to their network architecture, RF mesh systems will exhibit a "bell curve" histogram for latency, largely driven by the number of hops required for endpoints to communicate with backhaul access points. We recommend that no less than 90% of endpoints be within a 5 second roundtrip for connectivity.

Backup

- Redundancy is an essential characteristic to ensure resiliency of smart grid network communications. There should be multiple, pre-defined, and flexible options for any smart grid endpoint to send and receive information to and from the smart grid network to which it is connected.
- Batteries and capacitors should be widely utilized across both network endpoints and network backhaul devices to ensure that critical smart grid functions, such as outage detection and management, are decoupled from the availability of the electricity grid itself.

(3) What are other additional considerations (*e.g.* terrain, foliage, customer density and size of service territory)?

Considerations such as terrain, foliage, customer density, and size of service territory should not reduce the performance standards described in response to Question #2 above.

(4) What are the use cases for various smart grid applications and other communications needs?

A comprehensive response to this question could fill many volumes, and organizations such as the Electric Power Research Institute are developing highly detailed repositories toward this end (http://www.smartgrid.epri.com/Repository/Repository.aspx).

(5) What are the technology options for smart grid and other utility communications?

Physical

Wired

- Power Line Carrier (PLC) modulates data over existing electricity delivery wires. It is appealing for its low cost and would seem to offer broad coverage

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

(e.g., electricity wires reach all utility customers), but is limited by its low bandwidth (often well below 20kbps for neighborhood area networking) and the high cost associated with hopping the PLC signal around transformers by converting it to a wireless signal and back again. PLC perhaps holds its greatest promise within buildings for home area networking (e.g., HomePlug).
- Broadband over Power Line (BPL) offers higher bandwidth and performance over a wired connection, but is widely considered too costly to deploy ubiquitously as a network foundation for smart grid communications.

Wireless
- Radio frequency mesh (RF mesh) is becoming the technology upon which much of the smart grid networking world is converging. By giving every endpoint the ability to also function as a router, RF mesh systems provide high reliability, robust performance, and unparalleled coverage for smart grid networking.
- Radio frequency networking built around "fixed" topologies (Fixed RF, a.k.a. "star", "radial", or "spoke" networks) is widely utilized today for mobile (e.g, cellular) communications, public safety systems, and other commercial applications, but face challenges in both delivering utility-grade network reliability (e.g., the "dropped calls" effect) and in connecting customers in hard-to-hear locations (e.g., small or sparse populations in valleys and around hills) for smart grid purposes. Fixed RF over commercial wireless networks is widely utilized for smart grid network backhaul.
- Wireless broadband systems (e.g., WiMAX, LTE) are a noteworthy subset of Fixed RF technologies, in that they deliver very high bandwidth and performance, making them highly attractive for data-intensive applications, such as video monitoring of substations; for mobile applications, such as workforce management; and also for backhaul to and from neighborhood area networks.

Networking

As noted above, there is a wide range of carrier technologies that might be appropriate for specific functions, and indeed most SG implementations use a variety of physical transports at different points in the smart grid communications architecture. We strongly encourage an ordered approach to harmonize between these different technologies, using Internet Protocol (IP) as the unifying networking language to bring consistency and interoperability to the wide range of potential physical transports.

(6) What are the recommendations for meeting current and future utility requirements, based on each use case, the technology options that are available, and other considerations?

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

We recommend a combination of RF mesh for neighborhood area networks (a.k.a, field area networks; e.g., 900 MHz 802.15.4g); fixed RF for wide area networks (a.k.a., backhaul; e.g., commercial 3G or 4G) where Ethernet at the substation is not readily available; and a diversity of wired and wireless communications options (e.g., ZigBee over 802.15.4, WiFi, or HomePlug) for home area networks.

In all cases, we strongly advocate for use of widely-utilized open standards - such as Internet Protocol (IP) for addressing and routing - over proprietary protocols that are inherently-limited and vendor-specific.

(7) To what extent can existing commercial networks satisfy the utilities' communications needs?

Existing commercial networks provide an important infrastructure for backhaul of smart grid information through wide area networks, which serve as gateways to connect utility backoffice systems to neighborhood area network devices, such as smart meters.

However, existing commercial networks are limited, at best, in their ability to provide smart grid connectivity to neighborhood area network devices, such as smart meters. For comparison, private, purpose-built RF mesh neighborhood area networks can cost nearly 100x less than the OpEx of existing commercial networks, while providing superior coverage and reliability, as well as arguably more robust security.

(8) What, if any, improvements to the commercial networks can be made to satisfy the utilities' communications needs?

Coverage of commercial networks could be expanded to improve the availability of wireless backhaul for utility smart grid networks, especially in rural and remote locations.

(9) As the Smart Grid grows and expands, how do the electric utilities foresee their communications requirements as growing and adapting along with the expansion of Smart Grid applications?

The proliferation of smart grid devices and the accelerating pace of the deployment of smart grid applications will place increased demands on utility smart grid networks. For example, consider network performance: smart meters today might generate a read every 15 minutes, and this data might be collected every 4 hours. But future requirements might ramp this up to, say, 5 minute

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com

intervals collected hourly – a twelve-fold increase in data that must be matched by a comparable boost in network capacity.

As another example, consider interoperability: a utility that begins its smart grid journey by starting with smart metering may soon find that it wishes to deploy new categories of smart devices. If the utility initially invested in an interoperable network based on open standards, such as Internet Protocol (IP), to meet its communications needs for smart metering, then it will be in a much stronger position to use that same infrastructure to support new devices. In contrast, a smart metering system built upon proprietary protocols is far less likely to accommodate additional categories of smart grid devices from different vendors, thus leading to the costly implementation of redundant, application-specific networking infrastructure.

Michael Jung // Policy Director // Silver Spring Networks
888.406.1882 // mjung@silverspringnet.com