Why IP Is the Right Foundation for the Smart Grid

The energy community is starting to combine information and communications technology (ICT) with the electric power grid. This "smart grid" is a data communications network integrated with the power grid that collects and analyzes data captured in near real-time about power transmission, distribution, and consumption. Based on this data, smart grid technology then provides predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power delivery and consumption. Having near real-time information and recommendations allows utilities to manage the entire electricity system as an integrated framework, actively sensing and responding to changes in power demand, supply, costs, quality, and emissions across various locations and devices. Similarly, better information enables consumers to manage energy use to meet their needs.

The smart grid will enable optimization of energy generation, transmission, distribution, and consumption. It provides an opportunity for energy companies to make power delivery more efficient, whether by minimizing personnel visits to transmission and distribution locations or by enabling better decisions through more timely information. It will enable millions of distribution field devices, thousands of transmission substation devices, millions of customer premises devices (for example, smart meters, home energy controllers, and electric vehicles), data center applications, and customer service and support apparatuses to interoperate and communicate to empower energy supplies and consumers to manage energy more effectively, increasing efficiency and service levels while lowering overall expenditures.

At the same time, the smart grid must address the following critical issues:

- **Transmitting data over multiple media:** Smart grid data must be able to travel rapidly and reliably over a variety of different network media, from copper cables to fiber infrastructure to wireless networks.
- **Changing and growing with the industry:** The smart grid must be able to evolve as technological advances yield new hardware, applications, and devices. At the same time, it must incorporate such advances into the network with minimal cost and difficulty.
- **Connecting large numbers of devices:** The smart grid architecture must enable communication and correlation of data from approximately 61,000 substations and 180 million transformers and meters, with the number of devices connected to the smart grid growing annually.
- **Maintaining reliability:** High network availability is absolutely critical. Network outages are costly and debilitating—and currently all too frequent. In fact, 41 percent more outages affected 50,000 or more consumers in the second half of the 1990s than in the first half of the decade[1]. Ensuring uninterrupted electrical service to ratepayers is a prime challenge for the smart grid. Therefore, ensuring that the smart grid data network is reliable, so that it in turn can ensure uninterrupted electrical service to ratepayers, is crucial.
- **Connecting multiple types of systems:** The smart grid must connect and exchange data freely with many different types of hardware, ranging from smart sensors in home appliances to home energy meters to transformers and beyond.
- **Ensuring security:** The unfortunate reality is that because of the critical nature of the technology and the services it provides, the grid becomes a prime target for acts of terrorism and cyberattacks. The transformation of traditional energy networks to smart grids requires an intrinsic security strategy and specific security mechanisms to safeguard this critical infrastructure.

[1] The Smart Grid: An Introduction," 2009, U.S. Department of Energy.

- **Providing smooth migration:** Utilities must be able to migrate from their current disjointed data communications networks to converged networks in a phased approach with minimal service effect.

Underlying each of these goals is the challenge of exchanging data freely and securely among all components of the power grid. However, the existing electrical grid consists by and large of isolated “islands” of transmission and distribution capability with limited data communications among them.

The Grid Today

At the highest level, today’s grid is operationally and functionally divided into two large systems, the transmission system and the distribution system, each of which has multiple subsystems. In general, each of these subsystems has its own specialized rules for exchanging data within the subsystem. These data exchange rules are known as communications protocols or simply protocols. Because these different devices “speak” using different communications protocols that are not designed to communicate with each other, they essentially function as information “islands,” and thus it is very difficult to integrate communications across systems or to correlate data from different systems and devices.

Smart grid technology must connect disparate networks and information “islands” described above. The smart grid depends upon fast and free exchange of data among all components of the smart grid from generation plants to substations home and business meters. Connecting data from all these systems mandates adoption of a common communication protocol so that all systems speak the same “language.” Using the same protocol end to end in the smart grid to ensure that all systems can communicate freely is undoubtedly the most scalable and flexible approach to building the foundation of the smart grid. The Internet Protocol, or IP, has been the protocol of choice in businesses and the home for decades and is the ideal data communications protocol for the smart grid.

Why IP for the Smart Grid

IP is a communications foundation that was developed for helping data networks talk to each other, and it helps to answer some of the issues faced by the smart grid. It has been proven in some of the largest networks in the world and provides practically unlimited scalability. Its original purpose was to help unrelated network systems communicate, so it was designed with flexibility in terms of protocols as well as the underlying physical connections, whether wired or wireless. IP has the greatest number of tools to fine-tune performance, security, and reliability.

Today IP is the glue that allows multiple types of physical equipment to operate transparently from end to end over a wide variety of media without adding the burden of conversion of protocols. Smart grid deployments need the kind of transparent interconnection that IP provides to connect the various types of equipment and sensors that will be deployed to make the grid smart.

Because of the inherent design of the Internet Protocol, the Internet architecture addresses each of the goals set for the smart grid:

- **Transmitting data over multiple media:** IP can run over any link layer network, including Ethernet, wireless radio networks, and serial lines, providing a common and flexible way to use and manage a network composed of disparate parts.
- **Changing and growing with the industry:** One of the principal benefits of IP is its ability to add a capability such as a new application without having to change IP itself. A good analogy is a highway and cars: car designs change constantly in response to emerging consumer demands, but nonetheless can still use the same roads and traffic management. That is why IP can run applications it was not originally designed to support, such as secure Internet commerce, voice, collaboration, and Web 2.0 applications. And just as highways are designed to support traffic for the next 100 years, IP will be able to support new applications as they are developed for decades to come.

- **Connecting large numbers of devices:** One of the main challenges with connecting large numbers of devices is providing a unique identifier, or address, for each device. Unlike the many architectures that went before it, IPv6 offers straightforward addressing and routing for a huge network such as the smart grid.
- **Maintaining reliability:** IP already has more tools and applications to help manage the network and maintain reliability than any other communication protocol.
- **Connecting multiple types of systems:** IP is device independent. This means that it can identify any type of system to which data is addressed and deliver it to its destination. IP can also identify the system from which the data came, so it enables the receiving device to respond back to the sending device to let it know the data has arrived.
- **Ensuring security:** IP is secure as you want to make it. Although IP was designed to be open and flexible, over the years more and more tools have been built to provide security in the communications that travel over an IP network. In fact, of all communications protocols, IP has the most tools for securing and managing the transport of data. Therefore, while all the communications systems in the smart grid will be able to utilize IP as a communications pipeline, IP has state-of-the-art tools to ensure the information travels as privately as needed, sending the information to the right destination while ensuring that it is not intercepted or accessed by unauthorized users. IP is able to provide security on both public and private networks, and today many industries transmit their communications over both these types of networks. For example, some parts of financial networks are public as well as very secure, such as the retail banking section, while at the same time, many other areas of financial networks are completely private. All of these networks utilize IP as their foundation.

  Many industries with exacting security standards have embraced IP, despite initial reservations. For example, governments, militaries, service providers for both voice and cable services, telecommunications providers, and mainframe compute utilities were at first concerned about using IP for their operations, fearing security risks. Now all of these industries use IP as their communications foundation. IP has adapted to meet the stringent requirements of their networks, especially in the area of security.
- **Providing smooth migration:** IP provides a way to migrate in phases from multiple monitoring and control networks to a single converged network without disrupting service. This enables utilities to receive all the benefits of IP without having to undergo a massive “forklift” implementation. The steps to the convergence are:
  - **Encapsulation:** Legacy nonroutable data communications protocols are encapsulated in an IP “wrapper,” which can then be routed over an IP network. To accomplish this, Cisco uses bisync serial tunneling, or BSTUN, a protocol originally designed to facilitate migration from mainframe System Network Architecture (SNA) networks to IP. Not only is this method an effective first step in IP migration, it also emphasizes IP’s proven track record of flexibility and reliability. However, encapsulation does not offer the kind of end-to-end manageability and high performance afforded by native IP, but it is a relatively straightforward and easy to implement first step.
  - **Gateways:** Protocol translation devices, called gateways, are installed between legacy networks and the IP network. The gateway maps the legacy protocol functions to IP functions. Protocol translation not a format conversion operation. Rather, it is similar to translating between two human languages—not every word or phrase in one language has an equivalent in the other. Some words and phrases cannot be translated at all, so the translator simply does its best to supply as close a translation as possible. Therefore, like encapsulation, gateways are a useful but temporary migration step.
  - **Native IP:** The ultimate goal of migration is a native IP network. A native IP network provides the end-to-end robust security and outstanding manageability discussed above, along with quality of service, redundancy, scalability, and adaptability. A native IP network also delivers benefits of lower operational expense due to easier implementation and streamlined management.

Conclusion

IP is the proven, scalable, secure, cost-effective, and interoperable foundation for the communications, information, and commercial networks around the world. Cisco believes that the Internet architecture should similarly serve as the foundation for the smart grid. The IP protocol suite includes a number of protocols and mechanisms to ensure high quality of service that meets the requirements of the most stringent applications, high availability, and a very strong and secure architecture. The flexibility of the layered architecture also ensures mkes sure of investment protection for utilities for decades to come. IP has also demonstrated its ability to scale with billions of connected devices, and smart grid networks require similar scalability requirements.

Solution providers and innovators have developed application systems, used across many global utilities for mission-critical and life-critical systems, to meet the rugged demands of the energy industry. To meet the energy demands of the 21st century, utilities must invest in new, secure, and scalable solutions that can deliver energy efficiently and reliably for future generations. IP has proven over the past 30 years to meet those principles.

Cisco is committed to collaborating with industry, standards bodies, and government to develop a migration path for utilities and government that optimizes existing assets and, over time, migrates new investments into an IP-based smart grid that delivers the reliability, scalability, interoperability, manageability, security, and cost-effectiveness necessary to meet tomorrow's energy needs.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-581079-00 01/10