Deploying AMI Solutions

A Best Practices Approach

This paper is authored by Salim Patel, Richard Scafuto, Warren Westrup and Don Troxell.

Executive Summary

This white paper is intended to help Utility customers plan their AMI deployment by adopting best practices. The paper outlines best practices around the design, deployment and operation of wirelessly enabled smart meters. These best practices will help avoid common deployment, testing and management problems.

at&t

Smart Grid is a framework to modernize the power generation, transmission and distribution systems via the use of latest information technologies. The Department of Energy defines a Smart Grid as the transformation from a centralized, producer-controlled network to one that is less centralized and more consumer-interactive. Efficiency, reliability, flexibility, remote monitoring and grid visibility are some of the key attributes used to define a Smart Grid.

Fundamental enabling technologies for Smart Grid are sensing and measurement technologies with data from the sensing and measurement devices integrated with the utility's integrated system communications. These technologies provide real-time information and control to support faster and more accurate response such as remote monitoring, time-of-use pricing and demand-side management.

Within the Smart Grid framework, technologies like Advanced Metering Infrastructure (AMI) leverages 'smart' devices deployed at homes and other end-points to not only measure and analyze usage but also offer pricing based on time of use and device types. This is achieved via the use of two-way data transmission with the smart meter.

Wireless enabled devices like smart meters are being adopted in AMI solutions utilizing the AT&T wireless data network. A comprehensive approach in the planning, design and deployment of wireless AMI solutions can help avoid some of the common pitfalls. A robust wireless AMI solution must account for factors like wireless coverage variability and end-point manageability.

This white paper describes several best practices identified by AT&T that can help utilities avoid common deployment, testing and management problems associated with their wireless AMI deployment.

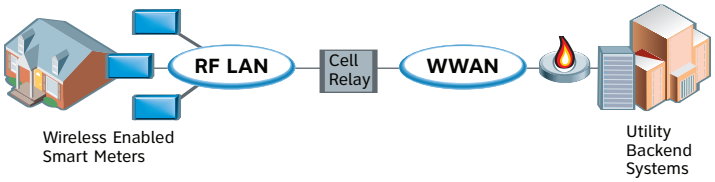
AMI Solution Reference Architecture

Wireless AMI solutions come in two basic flavors: mesh and point-to-point. In a point-to-point solution, each wireless end-point connects directly to the backend systems over a cellular/WWAN link. In a mesh solution, multiple end-points are aggregated locally over a WLAN; each aggregation point connects to the backend systems over a cellular link.

Mesh networks can be comprised of a Home Area Network (HAN), commonly based on Zigbee standard and a Local Area Network (LAN) that can operate in both licensed and unlicensed spectrum. The aggregation point, often called a Cell Relay (CR), is equipped with a cellular modem. The radios in the device (e.g. meter) end points transmit to the CR over a private RF network, primarily over unlicensed spectrum. It has the capability to aggregate multiple end-points and transport the information over the WWAN to the backend systems. The CR can be under-glass or pole mounted types. In the under-glass type the cellular modem and antenna is within the meter housing with no external antenna port. Pole mounted types have external antenna for improved wireless reception.

The CR connects to the backend systems, hosted by the Utility customer, over private links. AT&T offers a comprehensive solution for data center connectivity, which leverages custom Access Point Name (APN) defined in the GSM/UMTS standard.

Figure 1: Mesh AMI Solution Architecture



AT&T Mobility Commercial Connectivity Services

AT&T Mobility Commercial Connectivity Services (CCS) enables a customer to extend its private network into AT&T Mobility's cellular network CCS enables cellular connected devices to appear 'on the customer network' using the customer's IP addressing scheme and security policies.

There are three parts to the CCS design architecture: (a) cellular end-point configuration, (b) network connectivity and (c) customer network configuration. Each one has associated best practices that can stand alone, but following best practices on all three component parts can result in a more comprehensive solution.

Cellular End-Point Configuration

In both point-to-point and mesh architectures, each cellular end-point (or CR) should have a static IP address. A static IP address can better facilitate a correlation between IP address, phone number and wireless device serial number. Once entered into customer's databases and management systems, the IP address will be constant for the life of the device.

Dynamic IP addressing should be used only if the device has the ability to update the customer-owned server each time the IP addresses changes on the device. The customer must have a backend server that will log the current IP address of each device (dynamic DNS) and provide the ability for management systems to acquire the updated IP address when needed.

Each IP address should also be in the private IP address range. Utility customers may find it useful to refer to Internet Engineering Task Force (IETF) Request for Comment RFC 1918 – Address Allocation for Private Internets for private IP addressing standards. Unlike IP addresses in the public IP address range, these private IP addresses are not globally assigned and are not routable on the public Internet.

In addition to IP address considerations, wireless device functionality should be analyzed before deploying a wireless AMI solution. Specifically, some cellular devices have SMS capability. SMS can be used for device wake up or device management functions. For device wake up, after receiving an SMS message, the device issues a packet data protocol (PDP) connection request message to the wireless network. This limited connection request is relatively benign from a security perspective. For device management, the device is able to accept commands from users, execute the command and generate a reply to the SMS message. It is possible for unauthorized users to exploit the SMS device management functionality to gain access to the

device information and control device behavior by issuing commands. Accordingly, it is a good idea to disable the SMS command functionality or turn off SMS altogether via SIM provisioning. It is also recommended to disable voice call capability via SIM provisioning.

AT&T Network Connectivity

CCS provides multiple options for network-to-network connectivity. These options include Frame Relay, Network VPN and IP-enabled PVC. The Network VPN option can be used as the back up option for Frame Relay or IP-enabled PVC. CCS offers a number of customizations tailored to the customer needs.

To help ensure the highest level of CCS service availability, CCS is deployed with Geo-Diversity features as a standard practice. Redundant connections are deployed between the CCS customers' private Enterprise Network and 2 different Geo-Diverse AT&T Data Centers to help ensure that CCS service is not impacted in the event of a single CCS Network-to-Network connection outage.

AT&T has multiple Geo-Diverse Data Centers in the U.S. In the unlikely event of a catastrophic failure of a data center, the redundant data center can provide backup connectivity. Within data centers, each system has built-in redundancy and utilizes carrier grade appliances. Carrier grade systems are tested and engineered to high availability standards, and provide fast fault recovery.

Customer Network Configuration

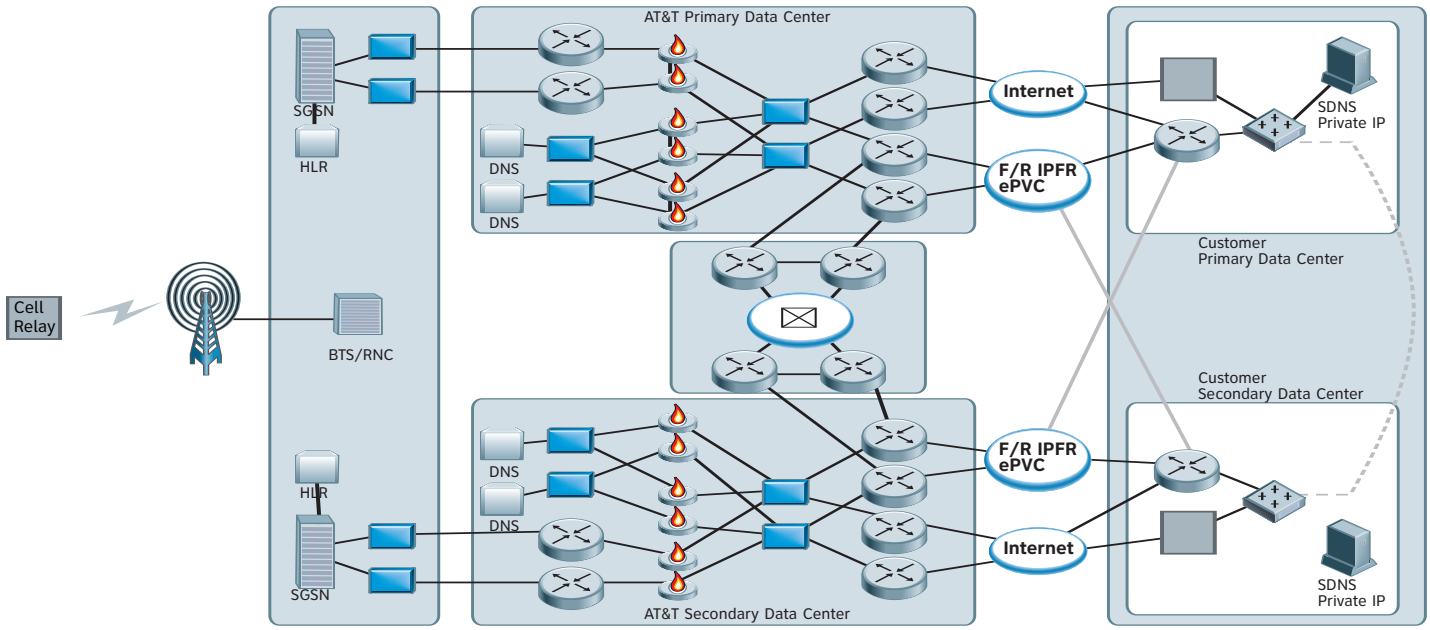
Utility customers desiring to connect their corporate data centers to AT&T's wireless network using one of the CCS offers should also build their network with full geo-redundancy. A primary/secondary data center concept should be employed where the customer's data centers are geographically separated. Each customer data center should not share a carrier's point of presence (POP) for connectivity. For example, two geographically diverse circuits traversing through the same fiber bundle can negate the geo-diverse redundancy. In addition, all IP addressing such as servers, NTP, DNS, etc. should use private static IP addressing as discussed earlier.

The customer's primary and secondary data centers should also be connected. If the AT&T primary data center fails, all traffic will be routed to the AT&T secondary data center and then to the customer's secondary data center. Two options are available if the customer would like the traffic to be routed to their primary data center. The first option is for the customer to provide a back-end network allowing traffic to flow through the customer's secondary data center to the customer's primary data center (red dotted line in figure 2). The second option is for the customer to add PVCs or IP-enabled PVCs on the front-end network (red solid line in figure 2). When building data links, the customer must calculate the maximum bandwidth required and provide adequate availability and performance.

All connectivity should employ BGP as the routing protocol. BGP is a standard protocol document in Internet Engineering Task Force (IETF) Request for Comment RFC 4271 providing a robust mechanism for network reach-ability. When choosing the BGP Autonomous Systems (AS) number, the customer can use their registered number (1-64511) or can use a number set aside for private use (64512-65535, excluding 64601). Within BGP the customer should provide a default route to AT&T. The customer can then manipulate how traffic is routed from the AT&T network to the customer's network without the need to contact AT&T.

The customers should provide their own Domain Name Servers (DNS). This allows easy IP address additions and changes to servers within their network. Mobile devices can make requests to names rather than IP addresses. If the customer wishes to change the IP address of that server, they can simply make a change to the DNS, without changing each wireless end-point.

Figure 2: AT&T CCS Reference Diagram



AT&T Enterprise On-Demand

AMI deployments are large in scale with millions of possible end-points. Wireless deployments of this magnitude require device activation and inventory management tools to ensure operational ease.

AT&T's Enterprise on Demand solution provides a unique set of services to give utility customers added flexibility with sizable wireless data deployments. EOD is a SIM ordering, activation and management platform that helps high-volume customers to self-manage large numbers of wireless end-points more cost-effectively. It provides customers flexibility and autonomy to control and administer wireless data services.

EOD activities are administered via a custom web portal. Some of the key functionalities include self-activation of SIM, SIM inventory management, feature management and reporting tools. It also provides access to enterprise help desk with ability to enter and track service tickets.

AMI Smart Meter Site Selection

Wireless coverage is variable in nature and smart device and cell relay (CR) location is a critical consideration. Unlike traditional mobile devices, the CR location is in the meter attached to a pole or a house and therefore fixed. RF conditions may change over time and a poor location choice will be detrimental to the CR performance.

CR placement can be a source of many issues. These issues are generally around the topic of accuracy of coverage information provided by service providers. Anecdotal reports points to a variance of up to 20dB between the RF propagation information provided to the customer and the actual observed signal levels. This can result in a reevaluation of the site selection process. Wireless propagation modeling is an estimation that depends on the accuracy of terrain and morphology information used in the tools.

Following are some best practices for the CR site selection process:

- Utility customer should develop a comprehensive Methods and Procedures (M&P) document for site survey and selection process to standardize the field team activities. This M&P will help vendors and sub-contractors adhere to the policies and best practices outlined by the utility customer.
- Prescreen site candidates using network data and other operational criteria; select a minimum of four candidates. Do not solely rely on wireless propagation data, combine propagation maps with drive test data and cell site information. Cell location, antenna height and orientation can help better predict expected coverage. Note that drive test data is not readily available in all areas and available data is generally at street level. AT&T can provide network data under NDA, but the customer should have the expertise to interpret and effectively utilize this information to streamline the site selection process.
- Survey each candidate; take at least ten measurements per candidate, and use the median value for final decision. Define multiple measurement points per location to identify any multipath effects in the area. Wireless coverage is non-line of sight in nature; coverage can vary at a location due to obstructions and moving objects close to or far from the measurement point. Build a fading margin of +/- 5dB in the measurements. Document the measurement by taking pictures of the location and identifying measurement points. Ensure no possibility of physical obstruction and analyze foliage growth. If possible, mount a cell relay close to the final location for measurement. Create a diagram onsite to document the test location and signal strength.
- Utilize a coverage validation tool or a cell relay in test mode as the survey device. Ensure proper calibration to avoid incorrect measurements. Do not use a phone in test mode; different phones have different front-end sensitivity and can provide readings not representative of a CR. Ensure that RSSI measurements are recorded in dBm (signal strength relative to 1mW) Some measurement devices may require correlating the actual reading with a translation table to calculate dBm values. Please refer to the user guide of the test equipment for details.
- Select a location with coverage from one dominant server (cell site). If possible, avoid hand off borders. This will result in consistent coverage, by avoiding 'ping-pong' between two or more cell sites. Record dominant cell ID and strong neighbor ID for future reference.
- Select the best overall candidate for installation, only select locations registering RSSI greater than -85dBm. Consider the +/- 5dB fade margin in making the final decision.
- Consider pole mounted CR with external antenna option to address locations with marginal coverage. External antenna options can help improve received signal strength.

AMI Deployment and Acceptance Testing

Deployment and acceptance testing refers to methods and procedures to install, turn up, test and document the CR installation.

Typically, CRs are installed if the selected location has an RSSI better than -85dBm. The technician installs and turns up the CR and confirms successful connectivity by visual inspection. No actual burn-in tests are conducted and backhaul connectivity is verified through Network Management Systems. This methodology is not comprehensive and can overlook common problems that can be easily addressed in the installation and commissioning process.

If after deployment the CRs encounter connectivity failure, the troubleshooting process determines the best course of action. The corrective measures can range from the use of previously surveyed alternate site or the use of pole-mounted, external antenna or repeater solution.

Following are some best practices to facilitate smooth deployment and help minimize costly relocations:

- Create a pre-production/lab environment for configuration and change management. Test and verify all new and modified system parameters before deployment in the lab environment.
- Use standard coverage validation tool or CR to verify surveyed RSSI and covering cell site. Ensure the signal strength at the exact installation location is better than -85dBm.

- Define a standard set of tests that can be conducted from the CR or from the backend systems. These tests can include ICMP pings to and from the CR, transfer of typical files (e.g., 5MB) to and from the CR, opening and closing of specific ports on the CR (e.g., port 1153) and other application layer testing available in the solution.
- After installing the CR conduct burn in testing, repeat the set of tests at least 3 times. Document test results like success rates, throughput, latency, serving Cell ID and signal strength. Make note of any anomalies encountered during the testing.
- Utility customer must define a troubleshooting and triage process to isolate problem source. The complete AMI solution leverages multiple radio technologies, connectivity solutions, service providers, device vendors, backend systems, etc. A comprehensive troubleshooting process can help avoid confusion during outage resolution. Utility customers should have in-house expertise to isolate problems by connectivity segments and have the proper escalation paths defined to contact the proper resources. AT&T Enterprise Technical Support is a help desk to help desk service available to utility customers with AMI solutions from AT&T. AT&T Enterprise Technical Support can troubleshoot issues related to AT&T's wireless network.

AMI System Monitoring and Reporting

CR performance and status monitoring is an important component of the AMI solution. However, most vendors do not have a comprehensive Operational Support System (OSS) strategy.

In some instances ping tools are in-use to monitor the CR status after install. These tools ping the CR at a user configurable setting. Summary reports are available to identify unresponsive devices. Ping tools are limited in scope and cannot provide reliable performance statistics. Some cellular enabled devices are capable of providing modem specific logs; these logs can provide more comprehensive performance indicators.

As smart meters proliferate, more focus will shift towards comprehensive troubleshooting and reporting capabilities. It is important to incorporate such capabilities in the design phase of the solution. Ongoing operational aspects like status monitoring, key performance indicators and reporting must be defined in details. Monitoring and reporting of wireless devices can be performed from the device and network perspective.

Device Side Metrics

Device side statistic refers to parameters reported by the wireless modem on the smart meter. These can include usage and performance statistics. Metrics like connection attempts and failures, throughput, latency, and PDP context statistics can be extracted from the modem logs. These metrics can extend the monitoring capability beyond ICMP ping.

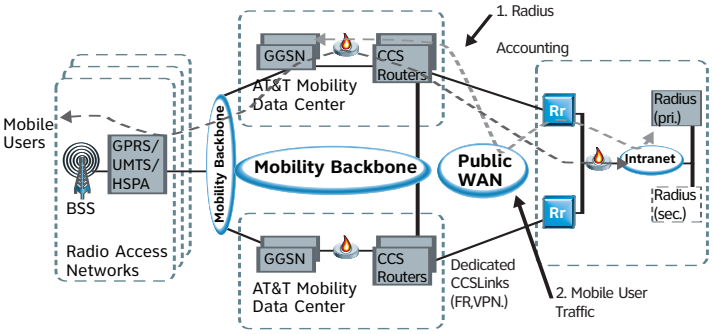
AMI vendors must provide Network Management Systems that can extract these statistics from individual end-points and provide canned reporting solutions. Care must be taken not to overload the smart device with management tasks.

Network Side Metrics

Network side statistics refer to metrics collected and reported by wireless networks. These statistics are reported at a cell site level; customer device specific reports are not readily available. Customer specific monthly manual reports can be generated, but they are not useful for near-real-time monitoring.

RADIUS accounting records is another option to collect, monitor and report CR activities from the wireless network perspective. These statistics can identify issues related to wireless connectivity. A utility customer wanting to leverage RADIUS records for end-point management must have a commercial RADIUS product that supports all required capabilities specified in the IETF RFCs defining the RADIUS protocol for accounting: RFC2866. This RFC is available online at www.ietf.org/rfc/rfc2866.txt .

Figure 3: Sample Customer Hosted RADIUS Accounting Solution



The various attributes available in a RADIUS start and stop records are summarized in the following tables:

Figure 4: RADIUS Start Record

AVP Name	AVP Type Code (Decimal)	Value Format	Value Default
User-Name	1	String	
Class	25	String	
Acct-Session-ID	44	String	
Acct-Status-Type	40	Integer	(1)
NAS-IP-Address	4	IP Addres	
NAS-Port	5	Integer	(60,000)
Service-Type	6	Integer	(2)
Framed-Protocol	7	Integer	(7)
Framed-IP-Address	8	IP Address	
NAS-Port-Type	61	Integer	(5)
Calling-Station-Id	31	String	MSISDN
Calling-Station-Id	30	String	(APN name)
NAS-Identifier	32	String	
Acct-Authentic	45	Integer	
Acct-Delay-Time	41	Integer	
NAS-Port-ID	87	String	(GGSN name)

Figure 5: RADIUS Stop Record

AVP Name	AVP Type Code (Decimal)	Value Format	Value Default
User-Name	1	String	
Class	25	String	
Acct-Session-ID	44	String	
Acct-Status-Type	40	Integer	(1)
NAS-IP-Address	4	IP Addres	
Service-Type	6	Integer	(2)
Framed-Protocol	7	Integer	(7)
Framed-IP-Address	8	IP Address	
NAS-Port-Type	61	Integer	(5)
Calling-Station-Id	31	String	MSISDN
Calling-Station-Id	30	String	(APN name)
NAS-Identifier	32	String	
Acct-Authentic	45	Integer	
Acct-Delay-Time	41	Integer	
Acct-Input-Octets	42	Integer	
Acct-Output-Octets	43	Integer	
Acct-Input-Packets	47	Integer	
Acct-Output-Packets	48	Integer	
Acct-Termin.-Cause	49	Integer	
Acct-Session-Time	46	Integer	
NAS-Port-ID	87	String	(GGSN name)
NAS-Port	5	Integer	(60,000)

AT&T can provide RADIUS start and stop records; this option is available as a part of the CCS offer. RADIUS accounting records are provided on a best effort basis. Start and stop records may be delivered out of sync, and utility customer's collection and reporting tool must be able to account for this anomaly. Standard UDP port 1813 is used for all RADIUS accounting records. It is recommended that utility customers implement RADIUS servers in an N+1 redundant configuration. AT&T GGSN will deliver these records directly to the customer RADIUS servers.

Utility customers can collect the various attributes recorded in the RADIUS accounting records and develop metrics to monitor end-point usage and performance. Metrics like uptime, session time, transferred packets, termination cause, etc. can be used to monitor end-point status and performance.

Key Performance Indicators and Thresholds

Key Performance Indicators refer to summary statistics derived from individual counters. KPI can collect a variety of counters and combine them to summarize performance conditions.

KPI's can be utilized to monitor status or performance on a near real-time basis. It can also be used for daily/weekly/monthly summary reports. Performance thresholds can be defined based on historical averages or industry standards.

AMI Security

AMI solution security must be viewed within the larger context of Smart Grid security. Smart Grid security is sub-divided in three security domains: generation systems, transmission systems and distribution systems. Each domain poses unique security challenges. System availability, data integrity and confidentiality are all important to the smooth operation of any AMI solution.

AMI solutions of today leverage a variety of connectivity options for normal operation. A single smart meter can have multiple wired and wireless connections like Zigbee, EDGE/UMTS etc. Each link or connection point should employ security features and access should be restricted by the utility to authorized users.

Some AMI vendors leverage SMS for management tasks. As discussed earlier, this is a potential security risk and utility customers should minimize the risk by either disabling the SMS command functionality or by turning-off SMS via SIM provisioning. Similarly, voice call functionality should be disabled. Any management connections and ports should employ access control mechanisms established by the utility customer. Utility customers should also encrypt their transmitted and stored data to help protect consumer privacy and minimize device tampering.

AMI and Smart Grid security is an important topic and is addressed in depth in a separate white paper.

Summary

The use of wireless technologies in AMI solutions may be a new trend but the technologies themselves are not. Wireless packet data networks have been in operation for almost a decade. Many of the best practices gleaned from AT&T's experience with wirelessly enabling a variety of applications directly apply to AMI solutions. AT&T believes that AMI deployments can greatly benefit from these best practices.

Specifically, a comprehensive plan that leverages best practices around the solution design, deployment methods, management tools and security measures can result in a successful and smooth AMI deployment.

References

Department of Energy, The Smart Grid – An Introduction, prepared for the U.S. Department of Energy by Litos Strategic Communication http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf.

For more information contact an AT&T Representative or visit www.att.com/business.

07/21/09 AB-1649

at&t
Your world. Delivered.