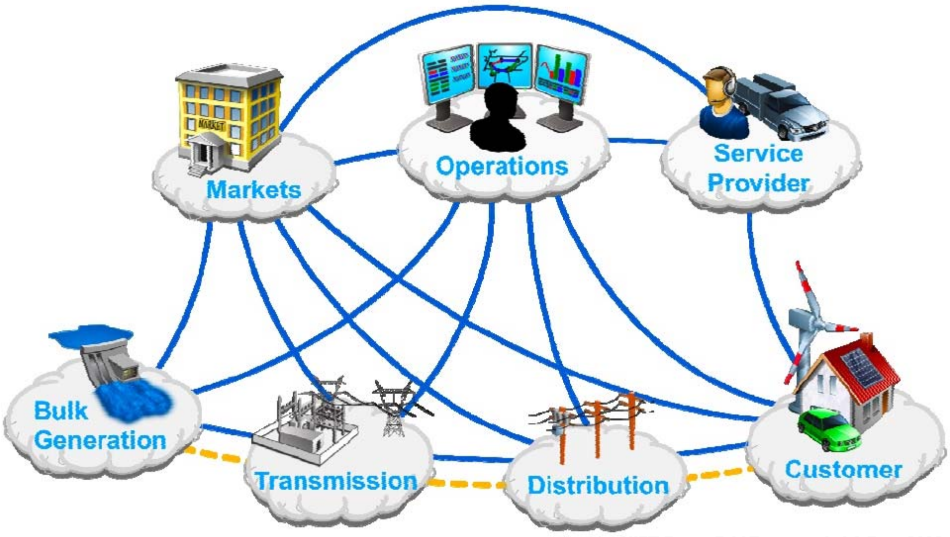
Collision of the Internet Architecture and the Smart Grid

Fred Baker, Cisco Fellow

Smart Grid operational domains

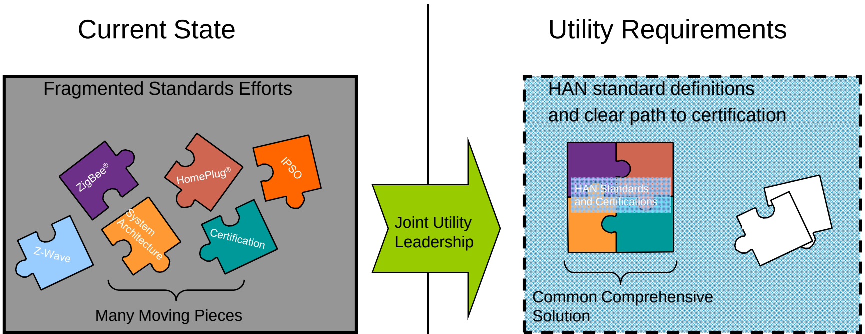


NIST Smart Grid Framework 1.0 Sept 2009

A brief overview of the Smart Grid

Figure 4: Domain Decomposition

Current State of the Industry – according to Zigbee/Homeplug



Minimal collaboration between industry resulting in proprietary processes to each utility

- Fragmented standards
- No common end-to-end system definition
- No comprehensive certification process

There is an opportunity to align around a common comprehensive solution

- Timing is good
- Standards bodies are open to utility engagement
- Pick the best minimum solution

Using the Internet Architecture in the Smart Grid

Internet Architecture, IP Protocol Suite

- Key architectural point in the Internet Protocol Suite: Flexibility
  - IP sessions end to end
  - MAC/PHY layers are interchangeable under IP
    - *No MAC/PHY religion*
    - *Don't tie long term applications to MACs that change from time to time*
  - Transports are interchangeable at application's option
    - *Include only what you use*
  - Each layer knows what is directly beneath, not what is below or beyond that
    - *Unnatural acts break things*

Layers	Protocols	Security Measures
Application	NTP, SNTP, DNS, DHCP, SIP, many others	SSH, Kerberos, SASL/GSSAPI
Transport	UDP, TCP, SCTP, DCCP, NORM, SRMP	TLS, SSL, DTLS
Network	IPv4, IPv6, ICMPv4, ICMPv6	IPsec AH/ESP
Link	IEEE 802 series, PPP, SONET/SDH, others	IEEE 802.1ar, 802.1X/AE
Physical	Various	Physical measures

Important take-away for the Internet Community

- Internet Protocol Suite seen as
  - "Complex"
    - *Many optional protocols*
    - *Not engineered to AMI needs*
  - "Threatening"
    - *Business issues – "let's not Osborne the business"*
    - *Technical issues – not easily used in existing architecture and yet pressed by us and some utilities*
- To make progress, we need to show flexibility
  - Make a building network a collection of 6lowpan and 6lowpan-like networks plus Ethernet/WiFi/WiMax sensors
    - *MAC/PHY independence*
  - Let vendor EMS manage our systems
    - *The entire market is about management*
  - Provide solutions that solve problems they are concerned about

Why use the Internet Architecture?

- It works…
  - Demonstrably flexible, adaptable to various requirements
    - *New link layers or algorithms fit in readily*
  - Many kinks worked out
    - *We do wish people would turn on the security solutions instead of complaining about security*
  - Other known solutions not necessarily better
- Administrative control
  - IEEE 802 series switching designed to **connect**
    - *Wire replacement*
  - Internet architecture designed to **organize**,
    - *Connect when and how appropriate*
- Resilient
  - Robust multipath routing

For the Internet layer, please use IPv6

Why? Two arguments

- **IPv4 is running out of addresses**
  - Latest estimates at current allocation rates disregarding final allocation strategy
    - *IANA supply depleted early 2011*
    - *RIR supply depleted mid-2012*
  - ARIN is discussing reserving IPv4 addresses for Internet use while they remain
- **IPv6 is an improvement**
  - More addresses
  - Improved address management
  - Other functionality improvements
  - Specific support for low power networks and applications

RIRs to Smart Grid: **New services should use IPv6!**

 9

Lessons from the Internet

 10

Important lessons from the Internet

- Things we did well
  - The service is **connectivity**
  - Design for **scale** beyond your imagination
  - **Simplicity** is the watchword; elegance and re-usability are keys to both scaling and innovation
  - **Robust Interoperability** is more important than mere correctness
- Things we wish had been done better
  - Avoid design & protocol limitations based on how hardware/technology works today
  - Design for secure channels and secure objects
  - Design for managability

Security: Peer authentication/authorization

"Don't talk with strangers"

- Applications have different views of their clients and peers:
  - May simply respond to requests – DNS, WWW
  - May have some peers they trust more than others – SMTP
  - May only trust certain peers – routing
- In general, authenticate and verify authorization of peers
  - Expend as little resources as possible rejecting peers
  - IPsec, TLS examples of tools
- Largely about *securing a channel* for information exchange
  - Limit it to trusted parties when possible

Security: exchange authenticated information

"How do you know this is relevant and true?"

- *Secure the information exchanged* when it will survive the communication
  - Signed MIME/XML: "I know the pedigree of this information"
  - DKIM for mail: "I know the sender of this email"
  - Secure Interdomain Routing proposals
- Apply policies based on degree of trust
  - Example: treat mail from a company that uses DKIM and has a valid signature differently than mail from the same company that lacks a signature or signature is invalid

Telemetry: status and statistics

What telemetry is interesting and useful?

- During technology design:
  - Identify probable significant network events
  - Indentify probable significant statistics
  - Enable autonomous recording/reporting of statistics
- Example:
  - Routing protocols see neighbors change state
  - Log and potentially report state changes to a monitoring system as they change
  - Record counter history at stated times for offline delivery rather than waiting for poll

Operational control: diagnostic and configuration management

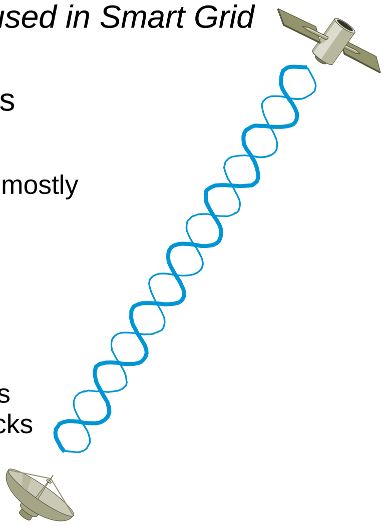
- Scalable+predictable configuration changes
  - Download and test new configuration
  - Configuration takes effect at stated time
  - Failing configurations fall back to previous configuration

Places the shoe may not fit…

Vendor AMI solutions in the Smart Grid

Background: Command/Telemetry Architectures

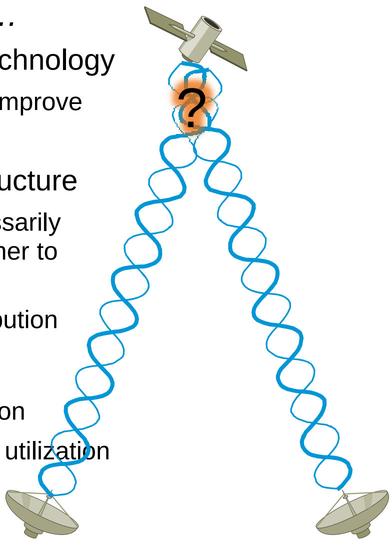
Developed for deep space, used in Smart Grid



- Unlike common Internet applications, spacecraft has
  - Severely limited power
  - Communications capabilities mostly allocated
  - Long round trip delays
- Implications:
  - Every bit counts!
  - Can't depend on synchronous responses like TCP/DCCP Acks

Background: ALOHA multiaccess networks

CSMA without carrier sensing…



- Ethernet is based on ALOHA technology
  - Preamble length and frame size improve carrier sense behavior
- Many users of a shared infrastructure
  - In radio networks, we can't necessarily depend on them hearing each other to avoid collisions
  - Therefore mostly statistical distribution
- Implications:
  - ALOHA achieves O(17%) utilization
  - Slotted ALOHA achieves O(38%) utilization

Power line networks

Homeplug

- Primarily consumer and commercial
  - Building control
  - Apartment buildings
  - Residential use
- Nice aspects
  - Common wiring
  - Naturally isolated to a building or campus
  - Speed variable to 200 MBPS
- Issues:
  - Potentially noisy due to wiring issues
  - CSMA (ALOHA)
  - Security issues similar to 802.11 SSID security
  - User Interface Design

Wide area radio networks

Sensus

- Primarily consumer meter reading, Field Area Network
  - Apartment buildings
  - Residential use
- Nice aspects
  - Relatively simple to deploy
    - *A few "cell towers"*
    - *Meters with radio interfaces*
  - Naturally isolated from other solutions by frequency
- Issues:
  - Relatively low capacity
  - Small messages (50-100 bytes)
  - CSMA (ALOHA)
  - Security issues
  - Large subnets - $O(10^5)$ homes
- Command/telemetry
  - Meter might "speak" hourly, reporting status
  - Controller might "speak" quite a bit during firmware downloads
  - Uses a form of reliable multicast

Neighborhood and Field Radio Networks

Zigbee/802.15.4g

- Primarily consumer, commercial, automotive
  - Residential use
  - Vehicular Networks
- Nice aspects
  - Peer-to-peer wireless
- Issues:
  - Less than 1 MBPS
  - Unusual relationship to routed networks
  - Relatively small messages (128 byte)
  - Limited range
  - CSMA (ALOHA)
  - Security issues similar to 802.11 SSID security
  - Signal through meter base plate

 21

So what are we doing about it?

 22

Present IETF developments

- IPv6 for Low Power and Lossy Networks (6lowpan)
  - Compression to improve ALOHA behavior
- Routing on Low Power and Lossy Links (roll)
  - Routing for overlaid 6lowpan networks
- Applications for Low Power and Lossy Networks (6lowapp)
  - Application protocol design
- Draft advice to future users of the Internet Architecture, including the Smart Grid
  - http://tools.ietf.org/html/draft-baker-ietf-core

Your thoughts?