



# Communications Overview for \_\_\_\_\_ Embedded Smart Grid Applications

Roland Acra – Cisco Systems

VP, Connected Energy Group

[acra@cisco.com](mailto:acra@cisco.com)

# Agenda

- Brief introduction to smart objects and sensor networks
- Setting context – embedded networking in the smart grid
- Illustrating requirements development through use cases
- Importance of open and interoperable standards, with IP
- Protocols and network mechanisms, beyond the buzzwords
- Opportunities for further innovation around the smart grid
- Back-up material and alphabet soup

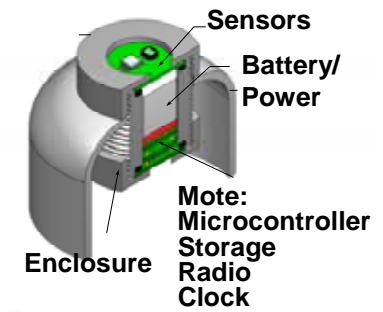
# What is a smart object?

a tiny computer (micro, memory, flash)

+ a (few) sensor(s) and/or actuator(s)

+ a communications capability

- may be battery powered or energy scavenging (or mains powered)
- may use wireless or wired communications
- may be active or passive
- may push (or be polled for) its information



# Technology evolution

- Legacy

Sensor → A/D → PLC\* → ModBus/Serial → Data Logger

Mostly wired, application specific, stove-piped, stranded

Myriad stacks – Modbus, SCADA, BACnet, LON, HART

“Co-dependent” designs (“Layer 1-2-7”: Media ↔ App)

*\* PLC = Programmable Logic Controller*

- What changed?

Low power microcontrollers with A/D and radio (TI, Atmel, ST...)

Low power narrowband media (IEEE 802.15.4/e/g, IEEE 1901.2 PLC, ...)

Small footprint, embedded OS (TinyOS, Thread-X, ucLinux, Contiki, ...)

Efficient implementations of IPv6 stack (6LoWPAN, RPL, CoRE, EXI, ...)

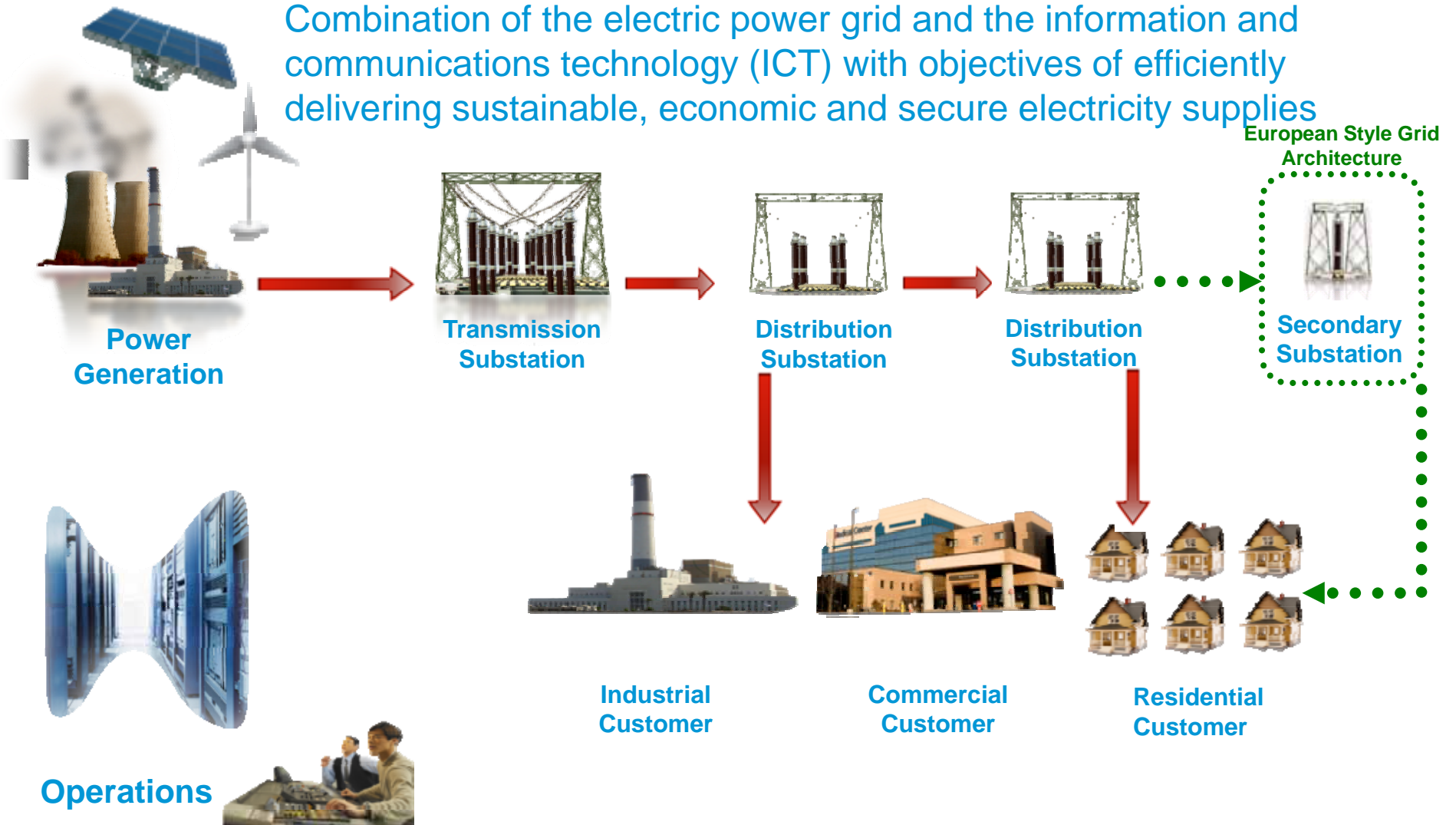
- Where does it go from here?

Sensors become info servers and stranded data becomes network-accessible

New insights and services emerge from data mash-ups previously unimagined

# Smart grid landscape

Combination of the electric power grid and the information and communications technology (ICT) with objectives of efficiently delivering sustainable, economic and secure electricity supplies

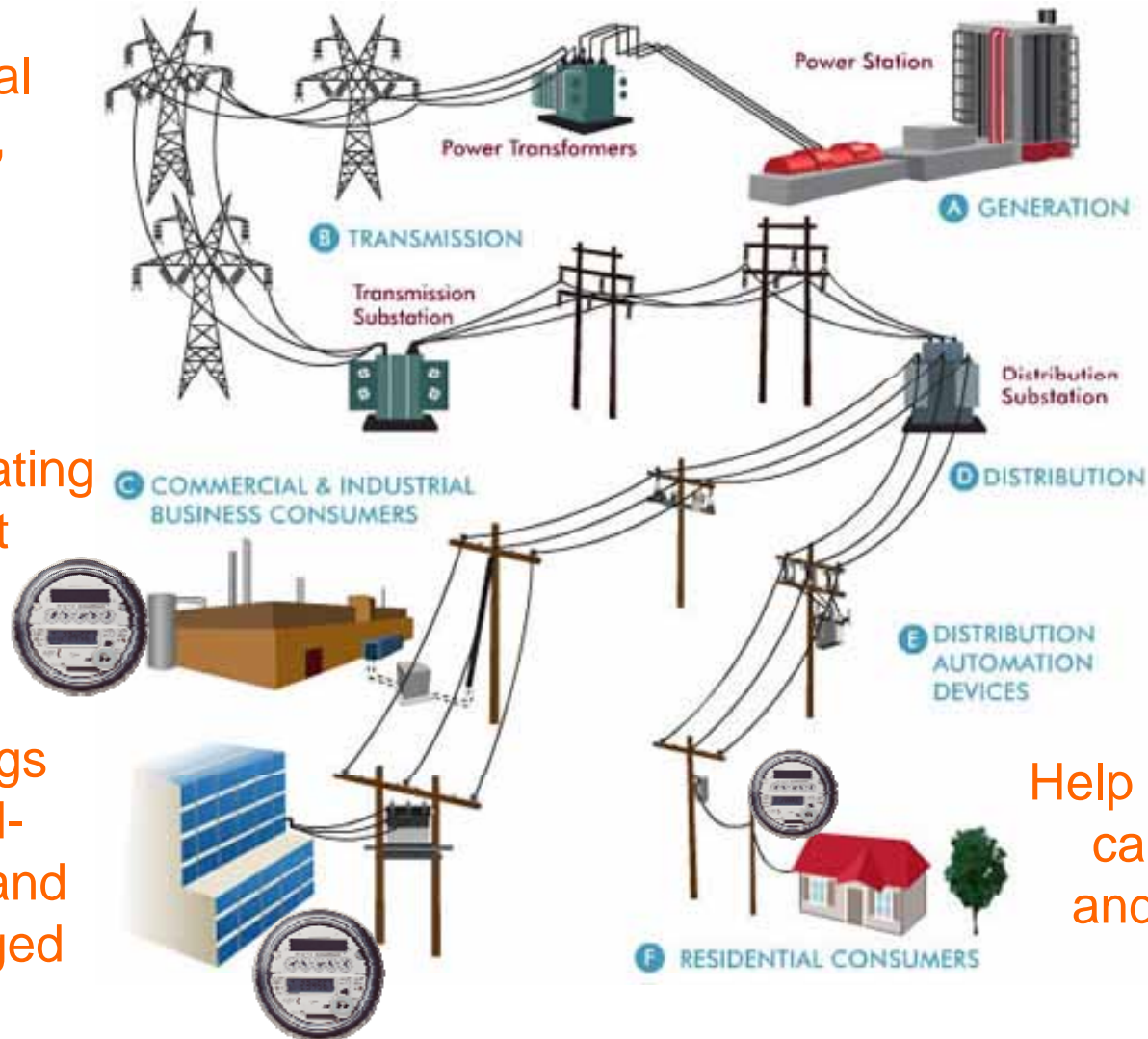


# What can smart objects do for energy?

Make electrical grids “visible”, more reliable, adaptive, and efficient

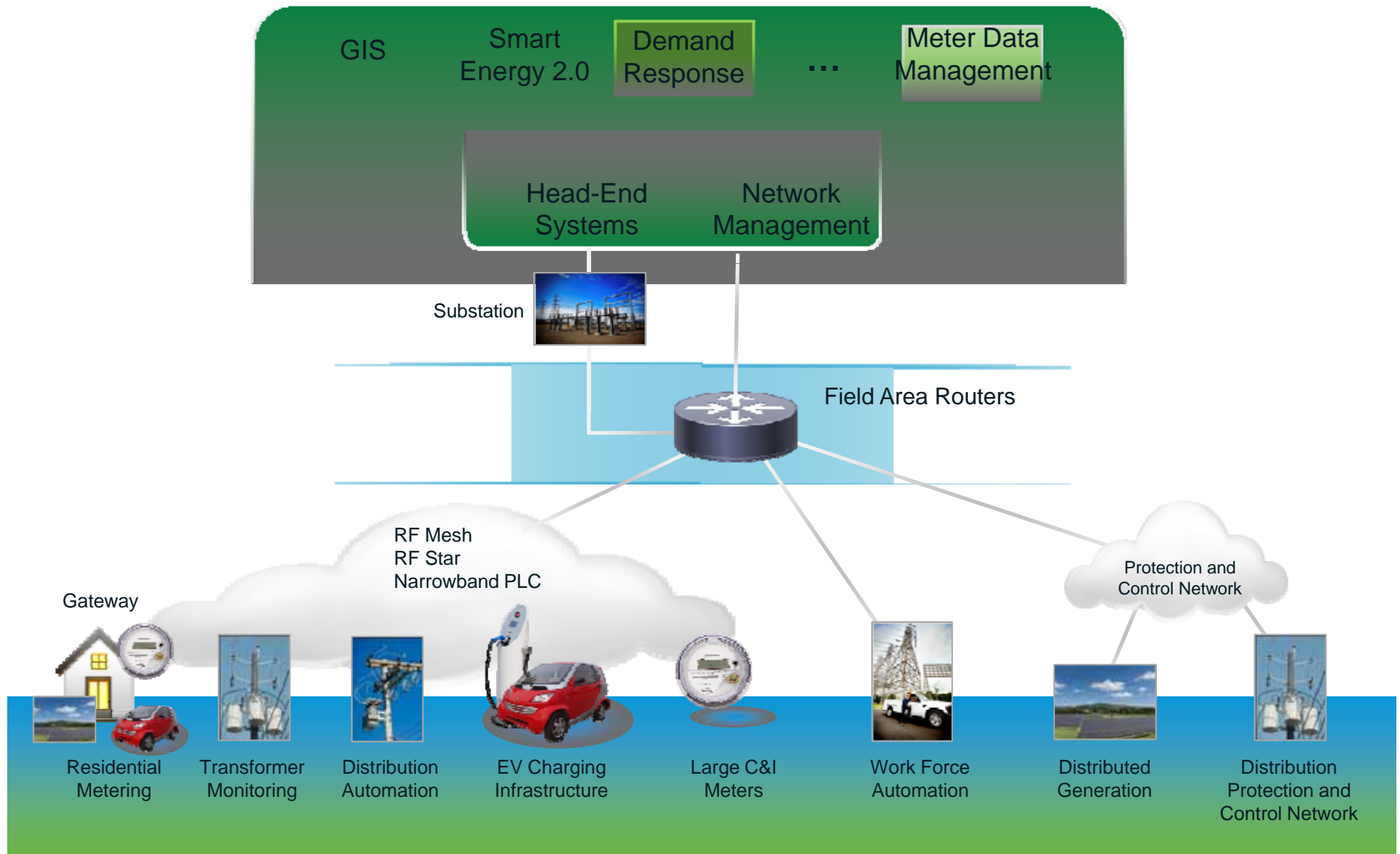
Reduce operating costs, prevent theft

Make buildings efficient, load-responsive, and better managed

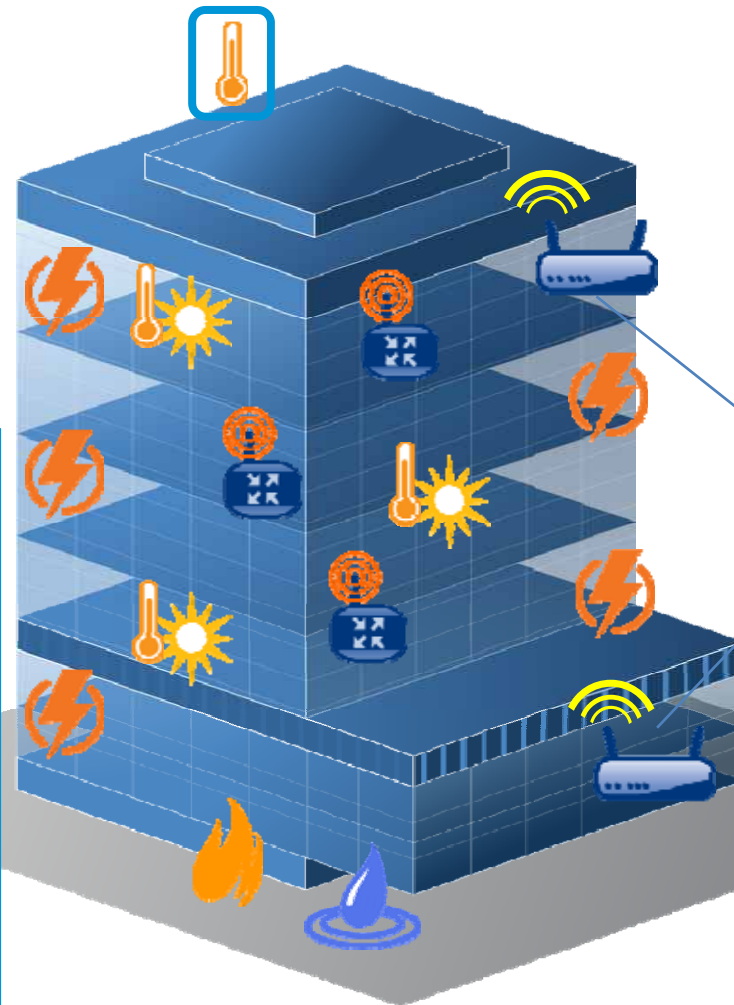


Help reduce home carbon footprint and save money

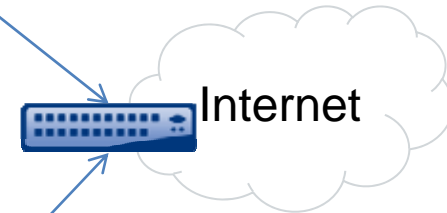
# Diverse applications, common infrastructure









# Connected buildings



Dashboards



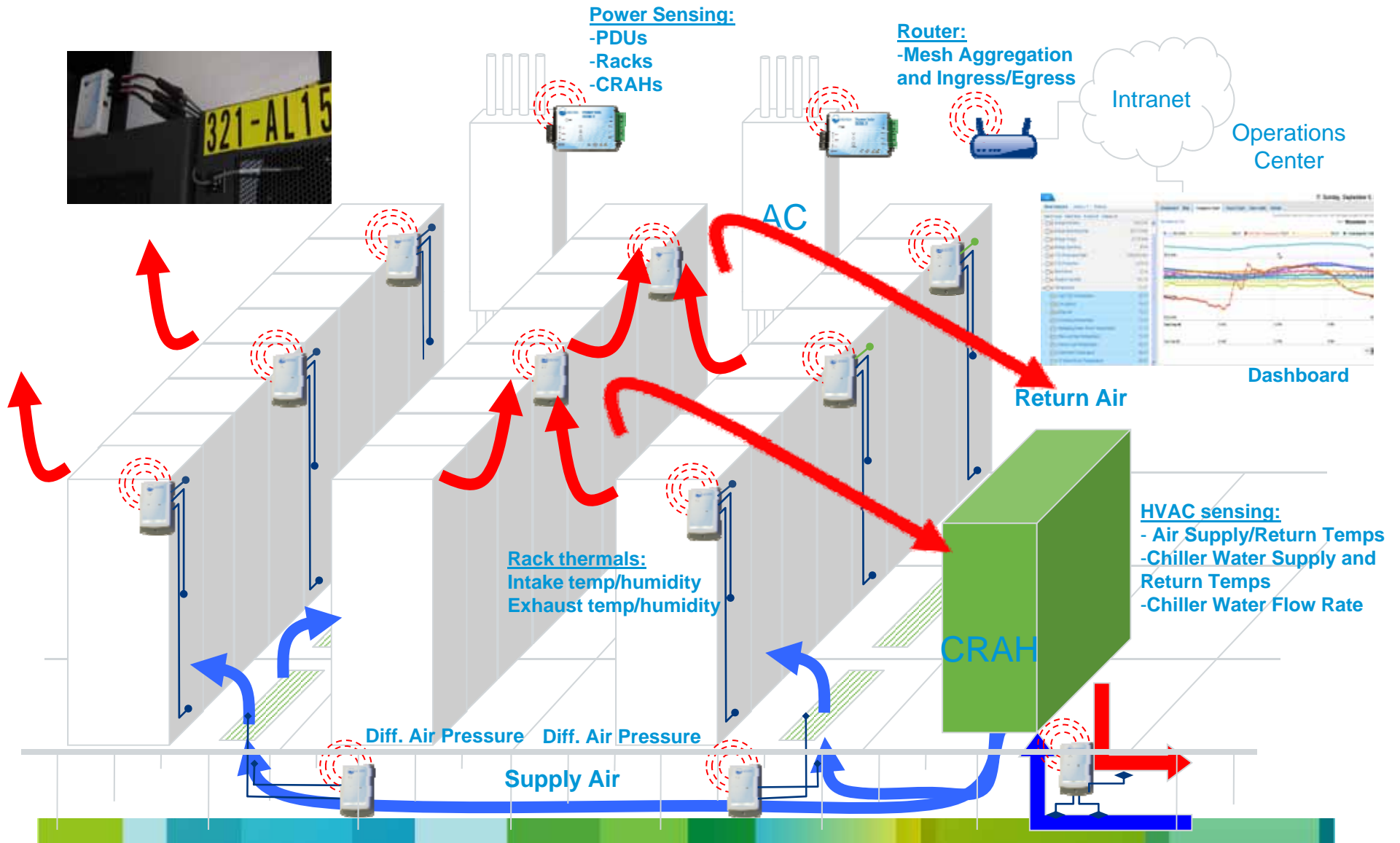
Internet

-  AC power sub-meters
-  Gas/Water sub-meters
-  Temp, Hum., Light, CO<sub>2</sub> sensors
-  Outdoor temperature
-  Relay nodes
-  Routers





# Instrumented data centers



# Development of requirements: app → sense → compute → communicate

- Application needs should drive all underlying design requirements
  - Information content vs sensed data: raw or “processed”/ “reduced” data
    - e.g., simple sensing / complex back-end versus “in-situ” processing (ALU, DSP)
  - Timeliness of data delivery: sampling frequency  $\leftrightarrow$  comms frequency
    - e.g., sample and store every minute, and daily batch “roll up” of stored data
  - Time resolution of data: sampling frequency in time
    - e.g., time-constant of physical phenomenon or business problem
    - e.g., air temperature changes slowly, kWh can move quickly...
  - Spatial resolution of data: sampling frequency in space, physical placement
    - e.g., by point in space (environment), or by device (infra), or by subscriber (\$\$)
    - e.g., indoor, outdoor/rugged, with/without mains power access, mean distance...
  - Sensor precision, accuracy: calibration, cost, analog/digital
    - e.g., basic thermistor (\$0.10) or billing grade meter (\$50) or flow sensor (\$1000)
  - Security considerations: reliability / non-repudiation / authentication / privacy
    - e.g., benign micro-climate sensing or critical actuation or meter-based billing

# Example 1 – Protection switching

app → sense → compute → communicate

- Application: sense and actuate / react to conditions on feeder / transformer
- Sensing: one or more of voltage, frequency, true/reactive power, phase, ...
- Time constant: milliseconds, or “utility of sensing” decreases dramatically
- Legacy solutions:
  - High-speed TDM transmission (SONET/F.O. where affordable)
  - Point-to-point private microwave links
- Emerging solutions:
  - “Latency controlled” packet networks (e.g., IP / Ethernet)
  - Traffic engineering, non-blocking designs, traffic priority
- Wired is costly...
  - Stretch: “latency guaranteed wireless”?
- Security considerations: high

# Example 2 – Advanced metering (I)

app → sense → compute → communicate

- Application:
  - Meter usage for billing, disconnect “bad” (non-paying) user
- Sensing:
  - Residential: interval-based (15min or 1hr) kWh (“billing grade”)
  - Comm. / Industrial: additional modalities such as power factor
- Time constants:
  - Actual power sampling: sub-second resolution for raw data
  - Data reduction / aggregation: (quarter-) hourly bins of cumulated data
  - Information timeliness: “day prior” good enough (per PUC regulation)
- Data loads, computing, communication:
  - In-meter sampling and data reduction into, e.g., 15-min intervals
  - Daily roll-ups result in O(KB) amount of data per subscriber
  - If polled in sequence (to reduce congestion), results in O(1-10 bps) / node
- Security considerations:
  - High due to billing: DoS, impersonation, repudiation, tampering, privacy
- Multi-layered: link, network, application

# Example 2 – Advanced metering (II)

app → sense → compute → communicate

- Spatial resolution:
  - Subscriber spread patterns (homes, offices)
  - Urban density versus suburban versus rural
  - One measure of concentration: customers per distribution transformer
  - North America: ~ 6 customers per transformer
  - Western Europe: ~ 100-200 customers per transformer
- Communication medium impact: suitability of power-line comm. (PLC)
  - Hypothesis (fact?): transformers too noisy to be traversed by PLC
  - So PLC concentration devices must be “south of” transformer
  - N.A.: would mean one concentrator (O(\$1K)) per handful of customers
    - No thanks is common answer, and gravitation to wireless (mesh or star)
  - Europe: would mean one concentrator (O(\$1K)) per 100-200 users
    - Yes thanks is common answer, and G3/PLC (FR), PRIME (ES), P1901.2

# Example 2 – Advanced metering (III)

app → sense → compute → communicate

- Wireless varieties:
  - Metering application non real-time, low bit rate (design point: 1bps/user!)
  - Licensed spectrum versus unlicensed (900MHz ISM, 2.4GHz)
  - Typical design goal = O(1K) devices per concentrator (star or mesh)
  - Star topologies (large link budgets) vs mesh topologies (multi-hop)
  - Emerging standard for low power in unlicensed band = IEEE 802.15.4g
  - Specs include DSSS, FSK/FHSS (prevalent now), OFDM (coming soon)
  - Large frame size (1500 bytes), O(100Kbps)@FHSS, O(1Mbps)@OFDM
- Wired varieties
  - N.A.: meters not UL, not grounded, often “off limits” to wired I/O (safety)
  - Otherwise: fiber (FTTH), DSL, but most attractive is PLC (power line comm.)
  - E.U.: CENELEC band A [0 – 95kHz] dedicated to utility applications
  - G3 (EDF) and PRIME (Iberdrola) “duking it out” for standards adoption
  - OFDM (~60 – ~90 carriers), broad modulation suites (ROBO, B/OQ/8/PSK...)
  - Max bit rates O(100Kbps), typically lower
  - G3 design goal is to **traverse distribution transformers** (to be determined)

# Example 3 – Physical security

app → sense → compute → communicate

- Application and requirements:
  - Video cameras capturing ongoing images of sub-station based facilities
  - Goals: safety, prevention of theft, vandalism, “remote situational awareness”
  - Additional benefit layered on: asset monitoring (esp. after weather, fire, disaster)
  - High data rates, real-time or near real-time information availability requirement
  - Best pushed over Ethernet or Wi-Fi type speeds to deliver needed data rates
  - Variation: leverage common multi-service network with substation automation
  - Technique: segregate traffic classes within virtual private networks with SLAs
  - SLA: service-level agreement (priority delivery, bounded latency, committed BW)

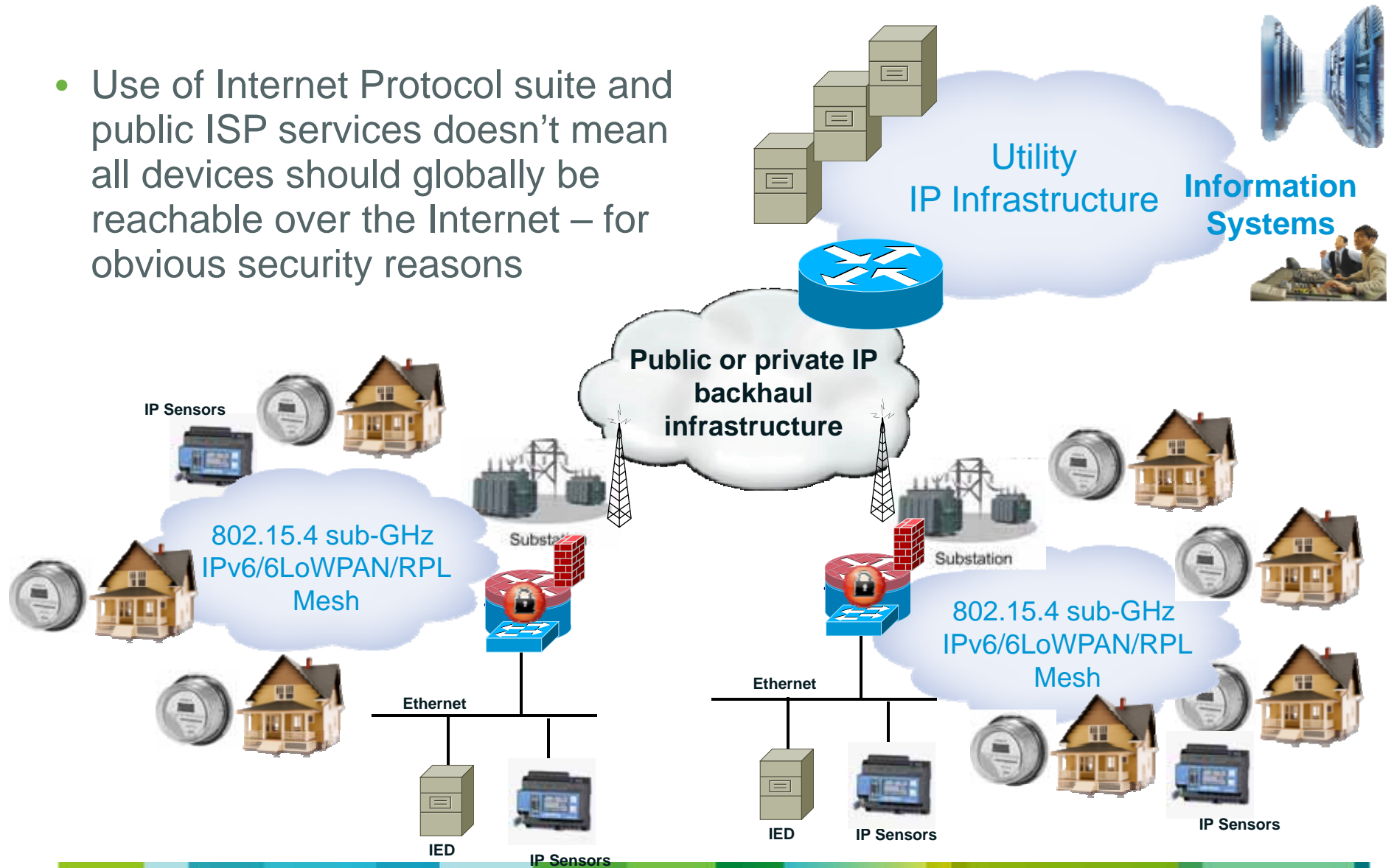
# Example 4 – Distribution automation app → sense → compute → communicate

- Application (emerging):
  - Obtain visibility beyond sub-stations down to distribution network tier
  - Generic wording referring to any new sensing/control for that new tier
  - Additional design goal: co-exist with AMI traffic on shared network (\$)
- Sensing:
  - Existing (stranded): attach to devices around relays, fuses, with stranded serial I/O
  - New (emerging): visibility from synchro-phasers, wave shape or micro-climate sensors
- Time constants:
  - Highly dependent on sensing modality – micro-climate (benign) vs synchro-phasers
  - Data reduction / aggregation: some local scope, also opportunistic on a topological basis
  - Information timeliness: highly dependent on sensing modality and local/global scope
- Data loads, computing, communication:
  - Mostly near real time visibility requirements (some real time)
  - Opportunity to share Field Area Network with AMI and other last-mile apps
  - Given “catch all” nomenclature, scope of requirements still broad / loose



# Smart Grid – a scalable, distributed architecture

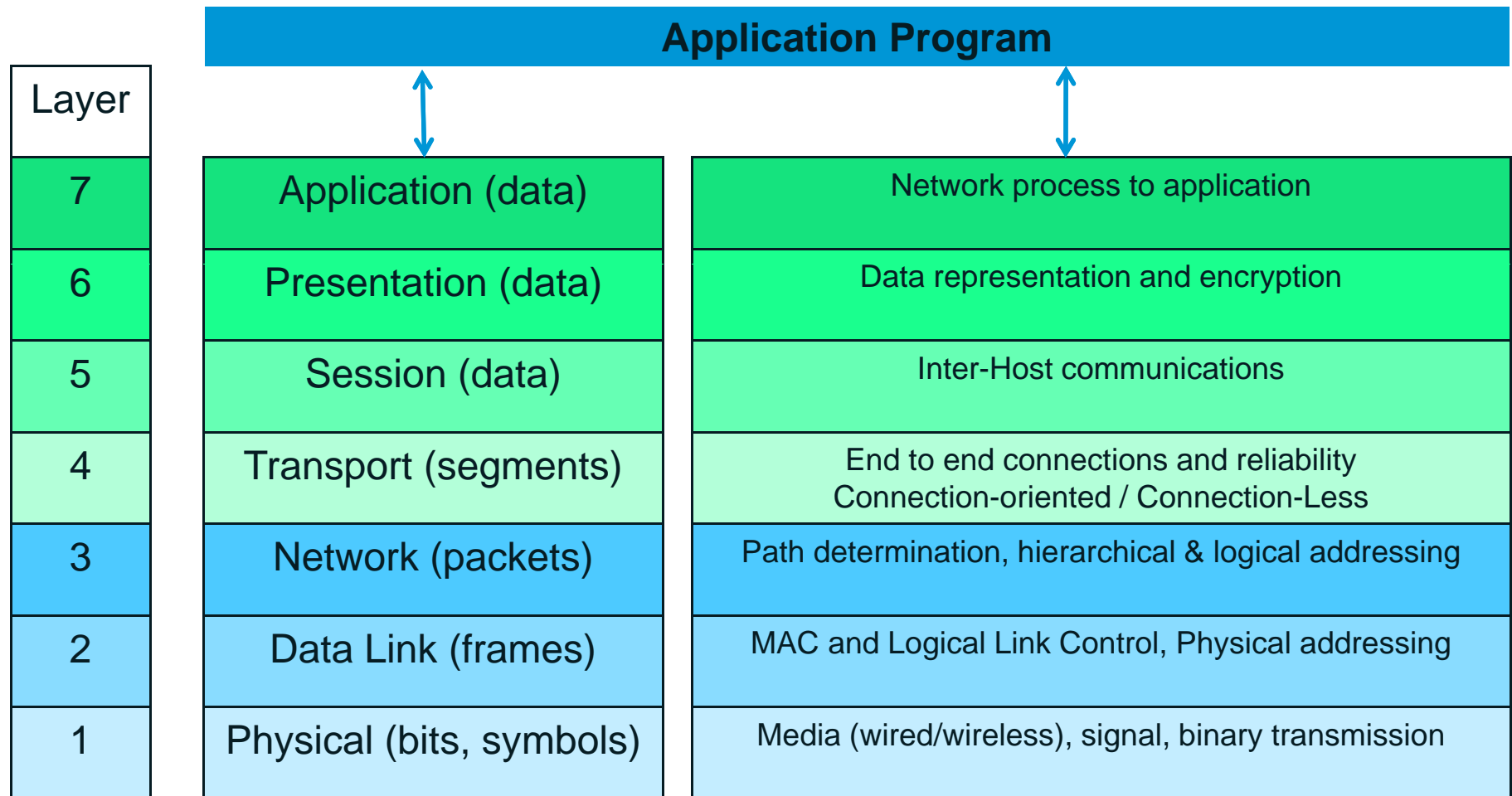
- Use of Internet Protocol suite and public ISP services doesn't mean all devices should globally be reachable over the Internet – for obvious security reasons



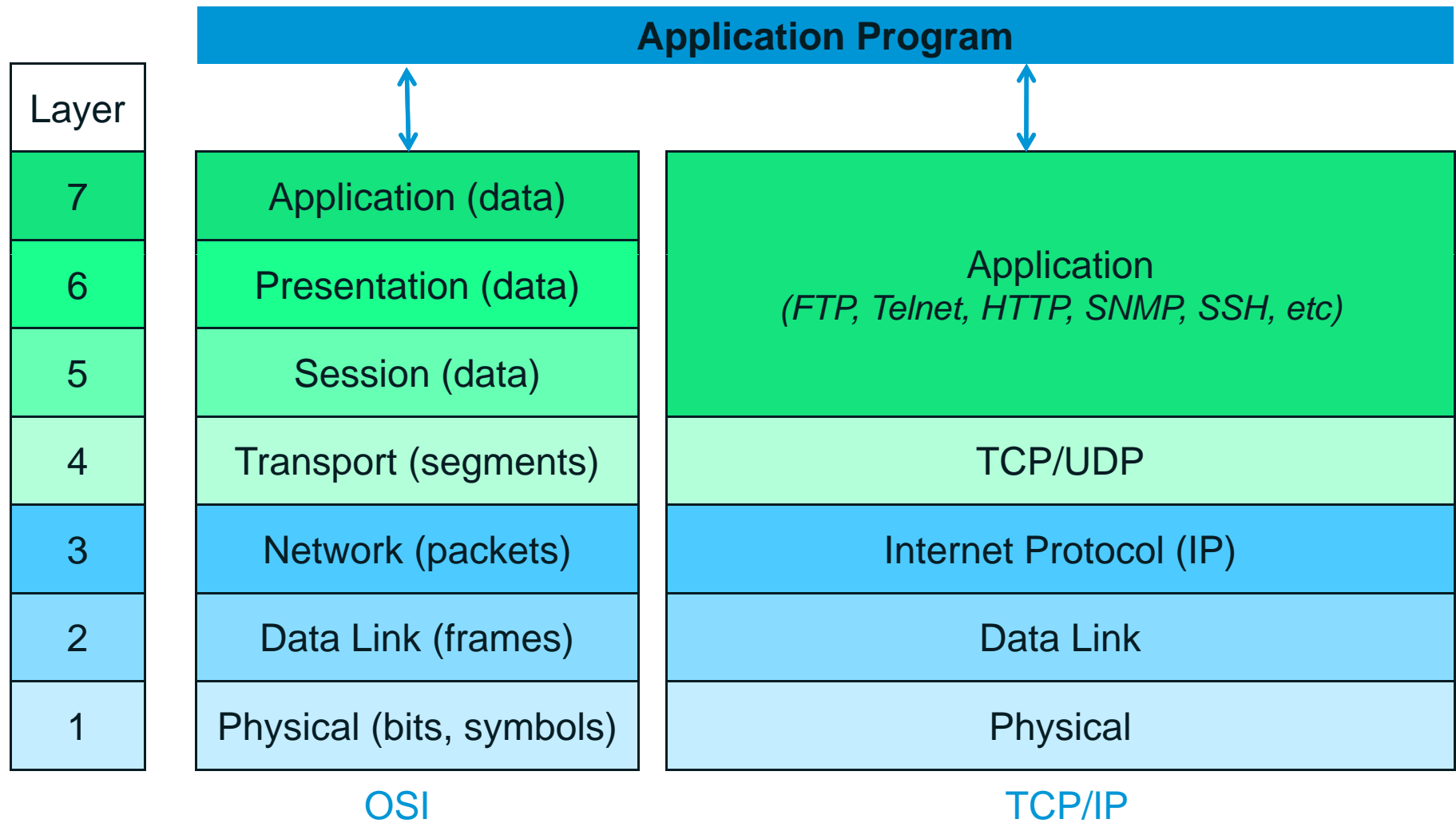
# Drivers and customer benefits of standards

- Open standards increase interoperability and multi-vendor choices
  - Utilities can issue RFPs and compare “apples to apples”
  - Utilities can “split the pie”, award partial wins, drive cost
- Physical and hardware layer considerations:
  - I.C.’s are a volume game → improved cost from several large players competing
  - Grid investment is long lived (decades) → mitigate single player’s survival risk
- Standard protocols and Software APIs allow mix-and-match of best-of-breed solutions
  - e.g.: network endpoint from X, network aggregation from Y, network management from Z
  - e.g.: open security spanning vendors and device classes (TLS, IPsec, 802.1x, etc.)
  - e.g.: suite of interoperable functional blocks available network-wide (data schemas)
- Open standards are most fertile terrain for innovation and cost reduction
  - e.g.: especially with layering and ability to innovate at the edge of infrastructure

# OSI 7-layer reference model



# TCP/IP reference model



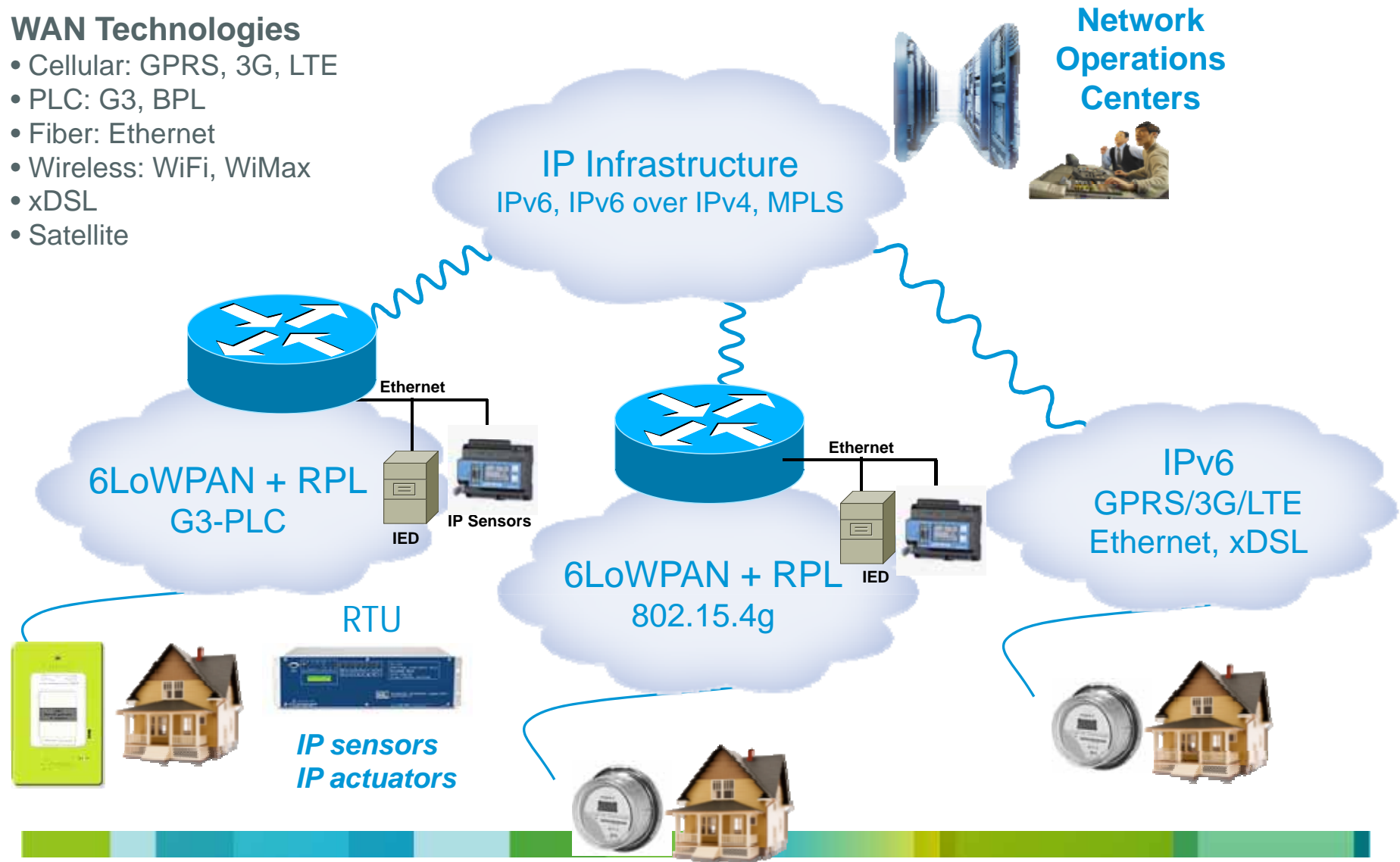
# Why the Internet Protocol (IP) and IPv6

- The Internet – no further proof of scaling
- Repeatedly demonstrated success as convergence layer
  - Data, voice, video, industrial (field) busses
  - Including with stringent SLA (e.g., 50ms link/path protection)
- Link diversity
  - Layering and adaptation layers for just about any link under the sun
  - Ethernet, Wi-Fi, DSL, Cell/3G, LTE, SONET/SDH, Serial, Dial-Up
  - New link types: IEEE 802.15.4, IEEE P1901.2, GreenPHY, etc.
  - Can span applications over mix-and-match patchwork of link types
  - Delivers investment protection and future-proof evolution
- Layered security models
  - Link layer (802.1x), network layer (IPsec), transport layer (TLS/SSL)
- Availability of trained staff, commissioning and management tools
- Specific IPv6 benefits:
  - Address space, auto-configuration critical to mesh, only choice for LLN
  - Only choice for new low-power link types (6LoWPAN for IEEE 802.15.4)

# Link diversity in the smart grid context

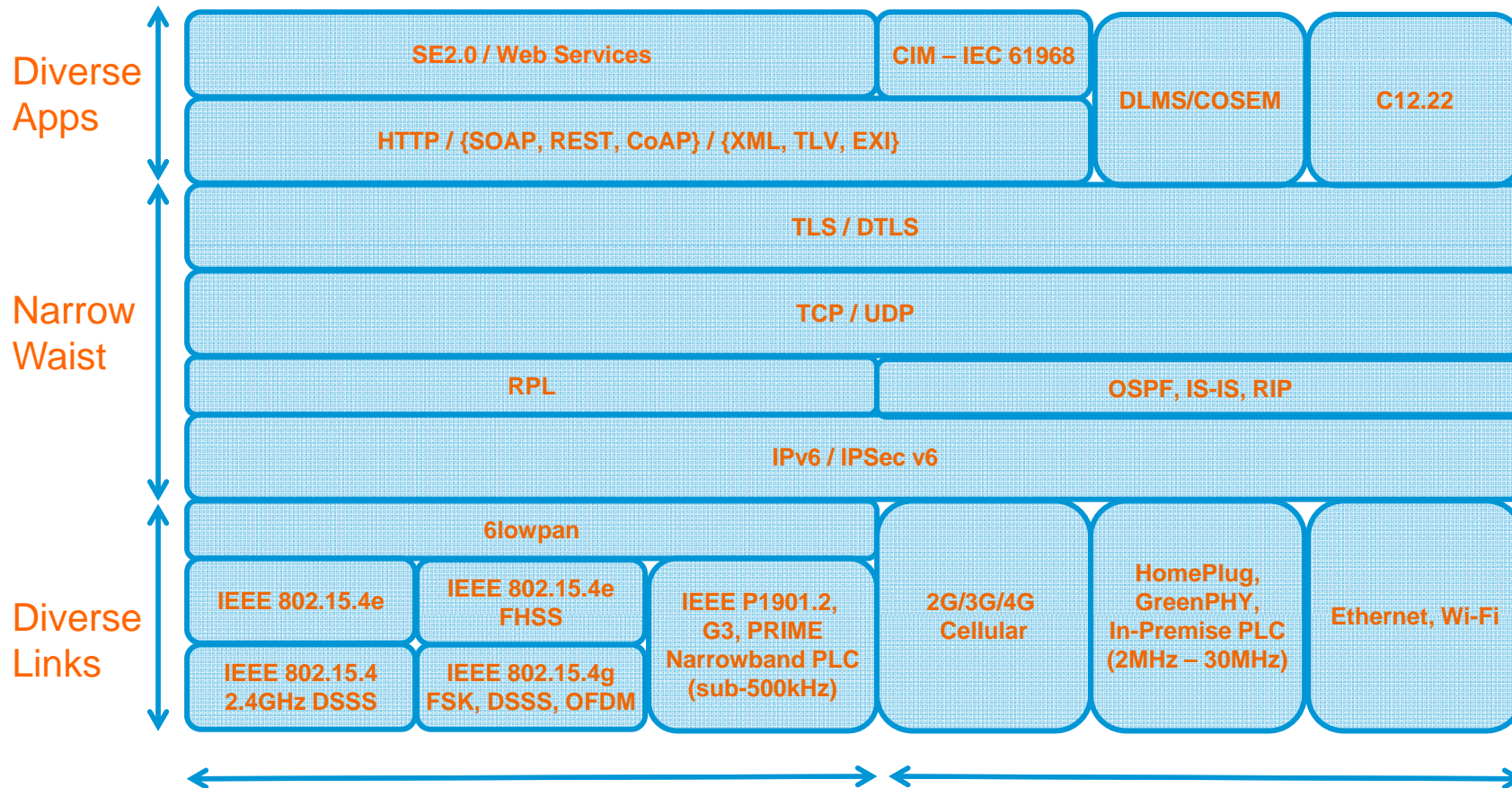
## WAN Technologies

- Cellular: GPRS, 3G, LTE
- PLC: G3, BPL
- Fiber: Ethernet
- Wireless: WiFi, WiMax
- xDSL
- Satellite



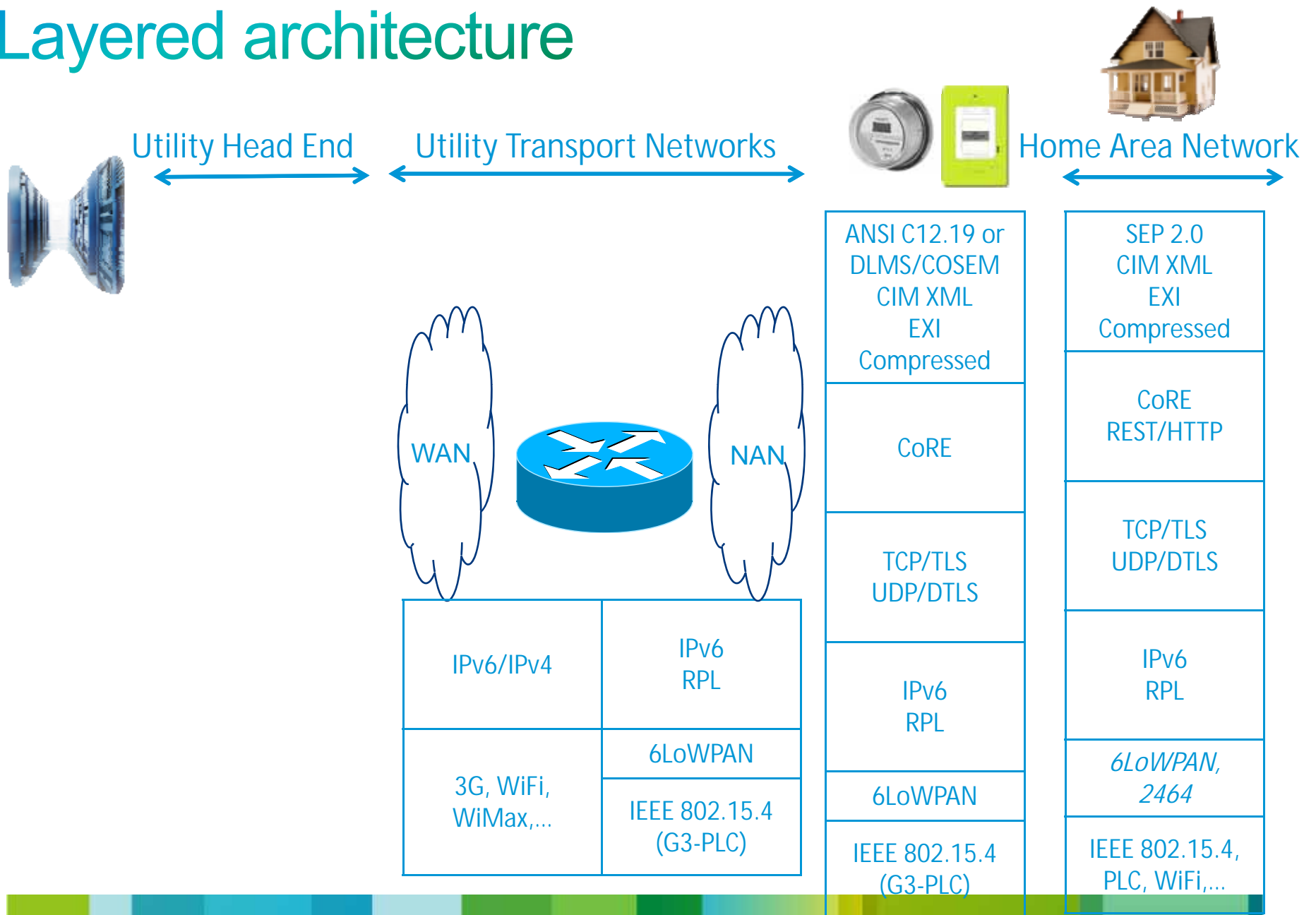
# Sample grid-embedded IPv6-based stacks

## Open standards views per layer



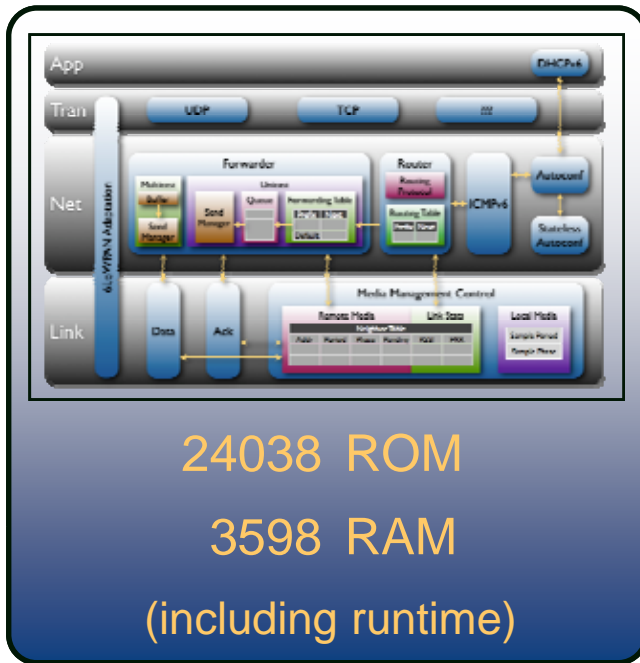
Low power, low bit rate, narrowband Higher power, bit rates, usually wideband

# Layered architecture





# Will it fit? How small a footprint?

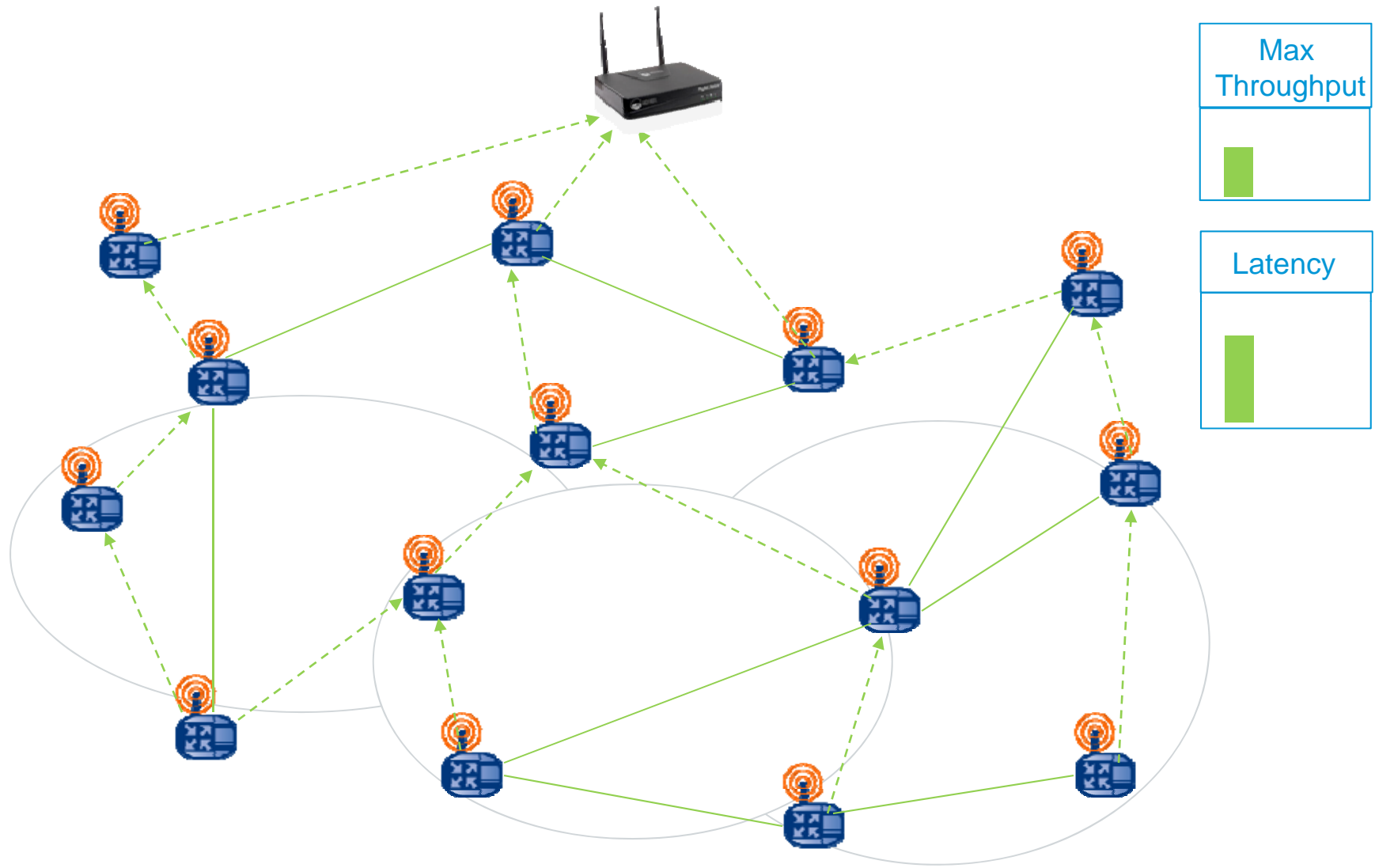


\* Production implementation on TI msp430/cc2420

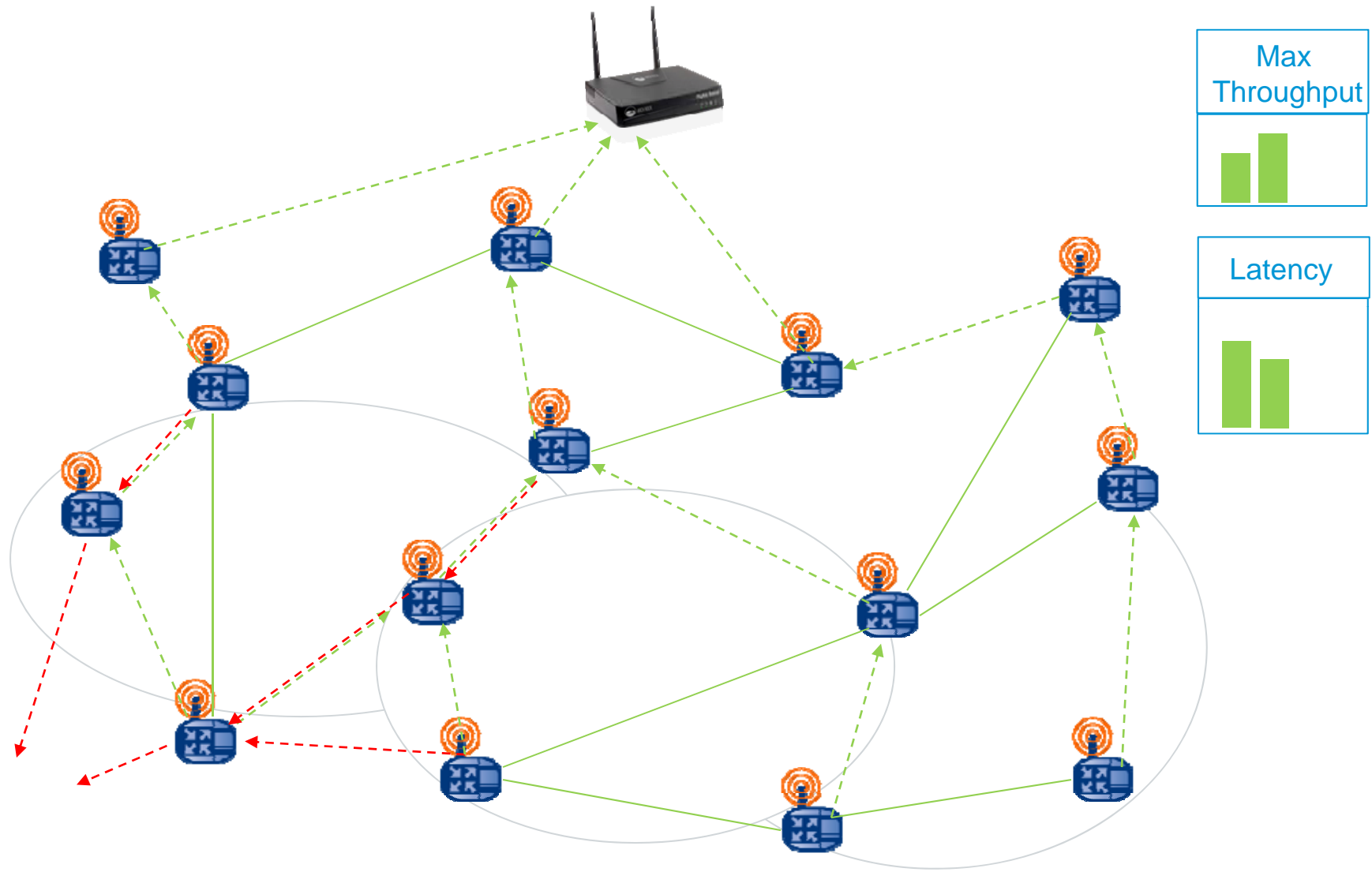
- With low-power extensions
- < 1 mW power consumed

	ROM	RAM
CC2420 Driver	3149	272
802.15.4 Encryption	1194	101
Media Access Control	330	9
Media Management Control	1348	20
6LoWPAN + IPv6	2550	0
Checksums	134	0
SLAAC	216	32
DHCPv6 Client	212	3
DHCPv6 Proxy	104	2
ICMPv6	522	0
Unicast Forwarder	1158	451
Multicast Forwarder	352	4
Message Buffers	0	2048
Router	2050	106
UDP	450	6
TCP	1674	50

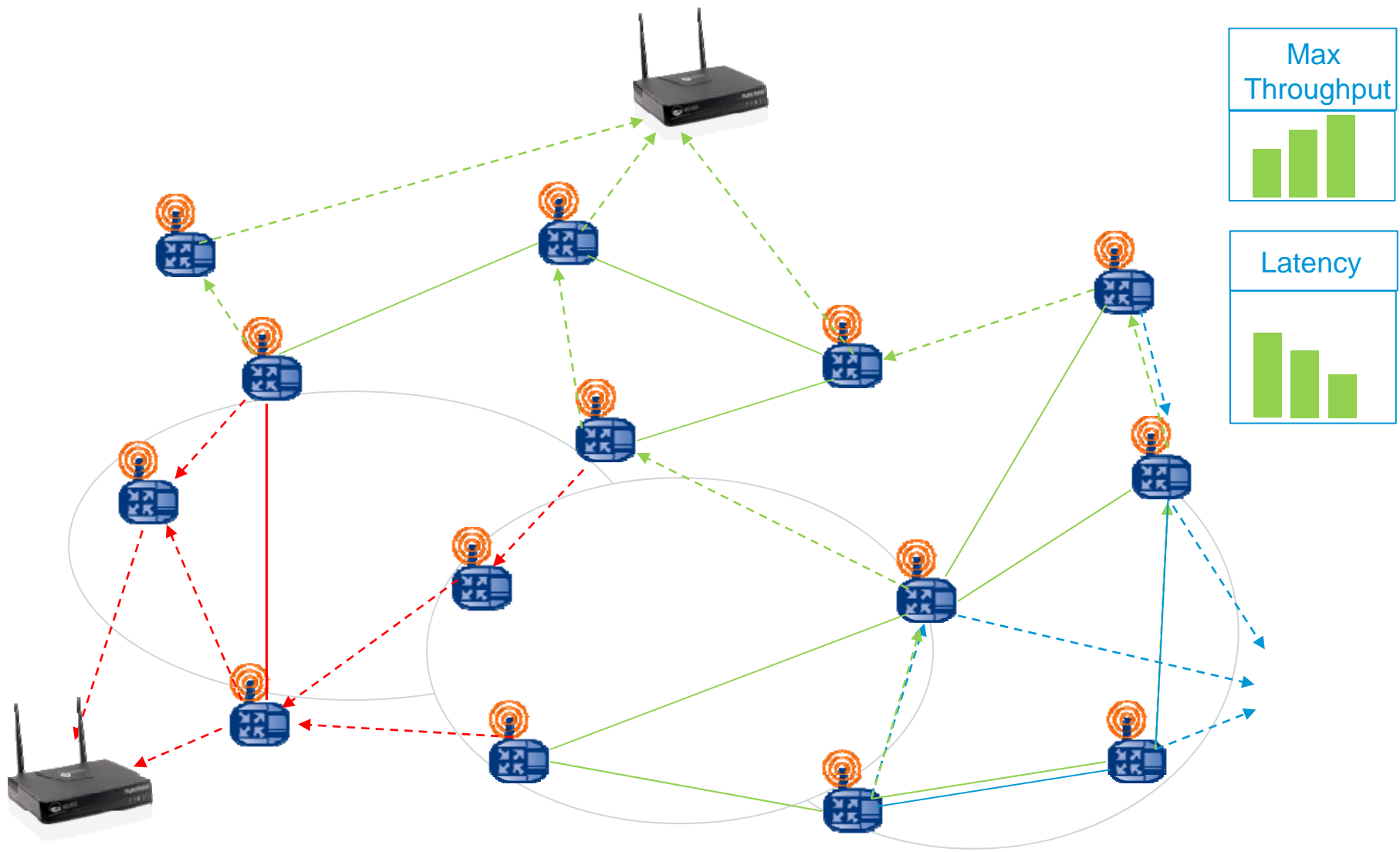
# Benefits of IPv6 – ad-hoc auto-configuration



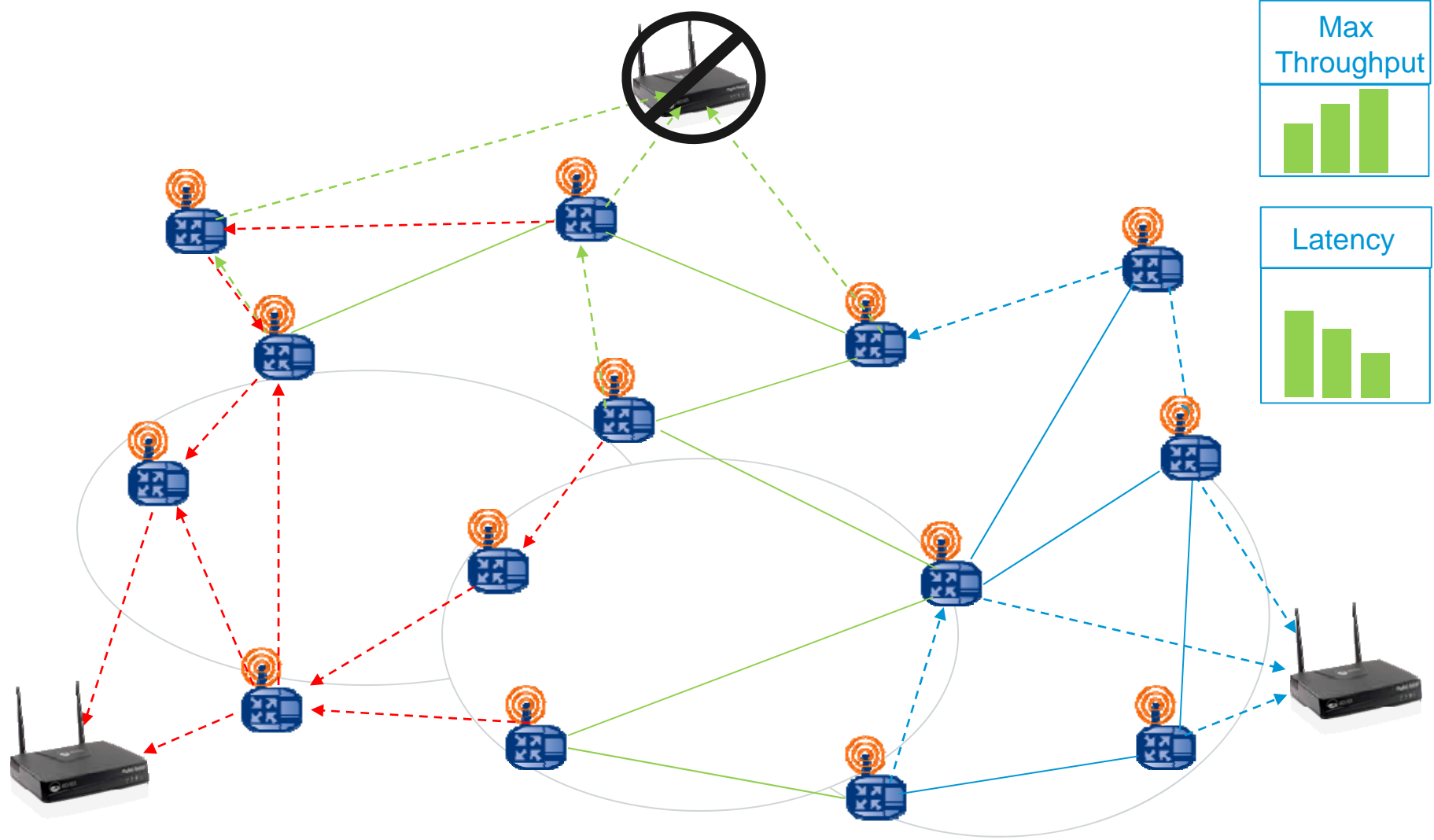
# Benefits of stateless routing – scale, performance



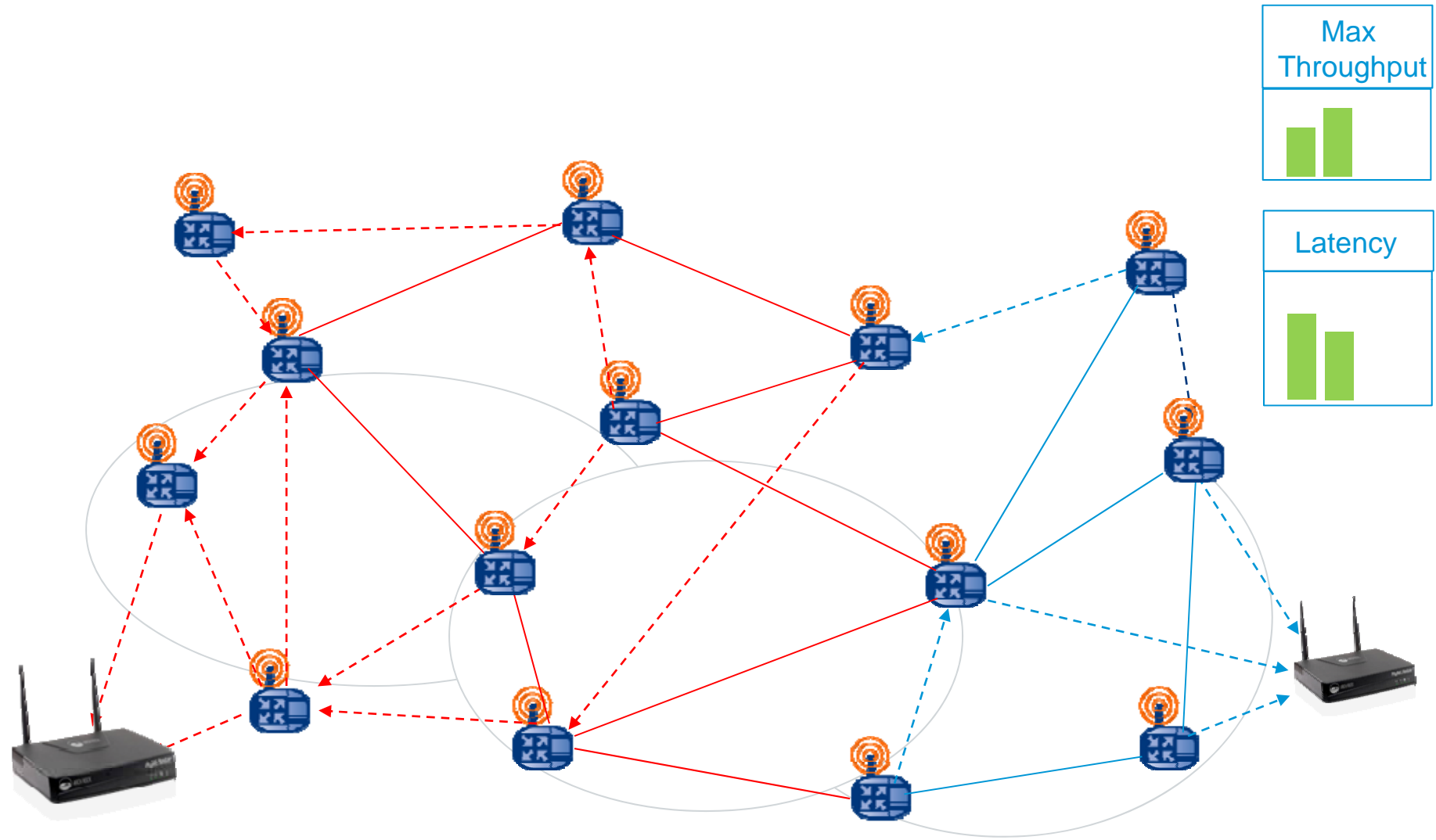
# Benefits of stateless routing – growth path



# Benefits of stateless routing – availability

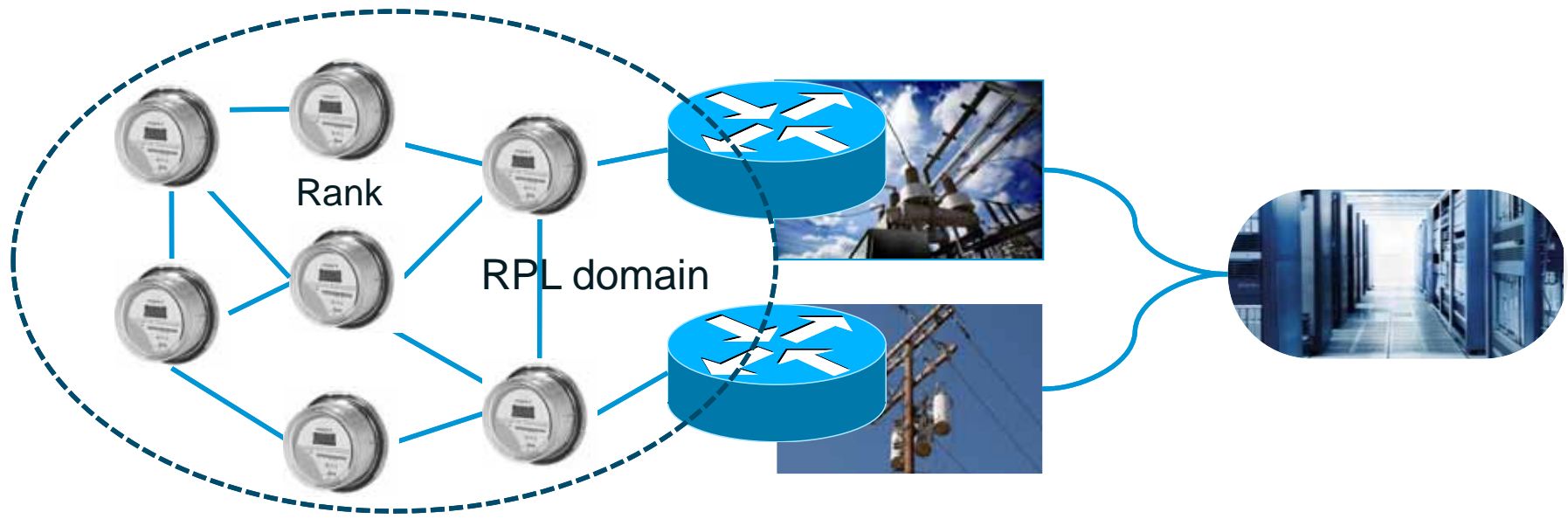


# Benefits of stateless routing – failover



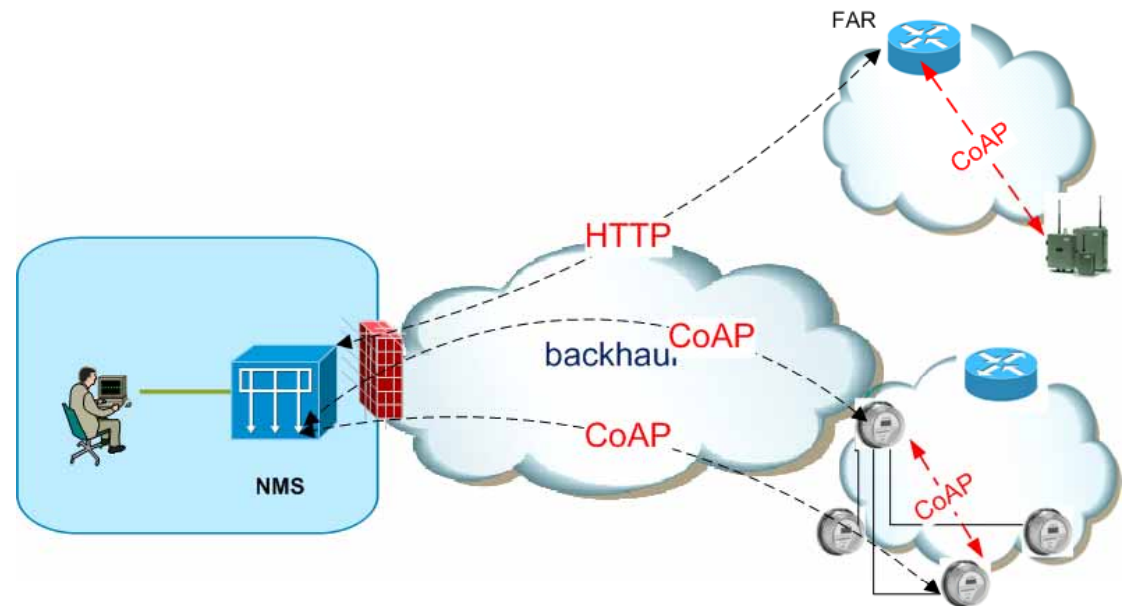
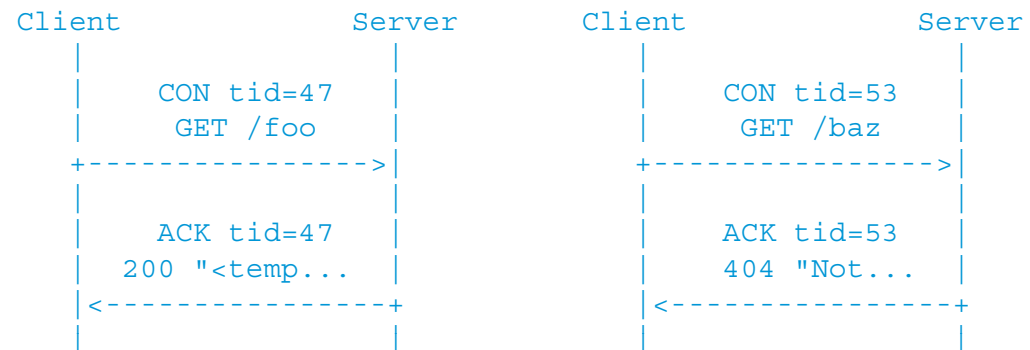
# IPv6 routing protocol for low power and lossy networks (RPL)

- Particularly designed for Low Power and Lossy Networks (LLNs)  
RPL Draft RFC – IESG processing
- “Route Over” guaranteeing the use of a variety of data links  
IEEE 802.15.4, G3-PLC, Bluetooth, Low Power WiFi, or others  
Include metrics specific to defined use case



# CoRE (Constrained RESTful environments)

- Maintain REST/HTTP methods and paradigm
- Device constraints
  - Microcontrollers
  - Limited RAM and ROM
- Network constraints
  - Low data rates
  - Small frame sizes
- Request – response
- Small message overhead
- Support multicast
- Support asynchronous messaging

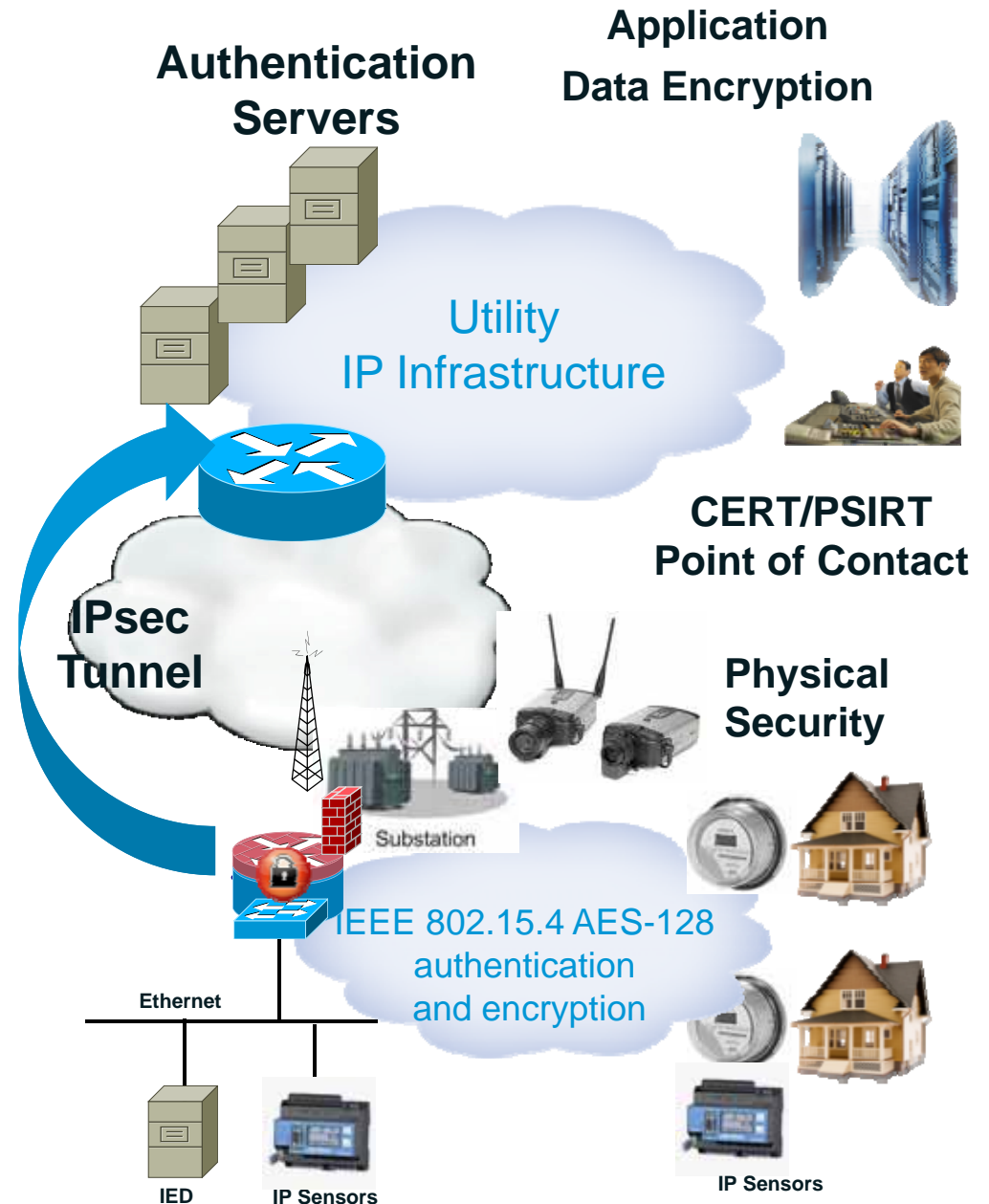




# Multi-layer security

Achieving security is a multi-layer challenge that includes

- Industry coordination  
CERT/PSIRT
- Physical security (hardware)
- Link security (local scope)
- Transport/session (end-to-end)  
IPsec or TLS/DTLS tunnel
- Authentication and Integrity  
802.1x and AES128  
Device authentication  
Certificate infrastructure
- Software integrity/signature
- Data encryption at application layer
- Reference: [NIST IR-7628](#) - Draft Smart Grid Cyber Security Strategy and Requirements



# Open frontiers

- Useful sensing modalities for distribution automation
- Robust and scalable security models (“zero touch”)
- Scalable network/system management ( $10^{**6}$  –  $10^{**7}$ )
- Address residential energy management “crisis”
- Harness information utility of new reams of data
- Build practical control models including demand
- Enable fast proliferation of micro-grids
- Leverage “TV white space”– cognitive radios?
- Ask someone below 30, not old me... 😊

# Standards - Applications

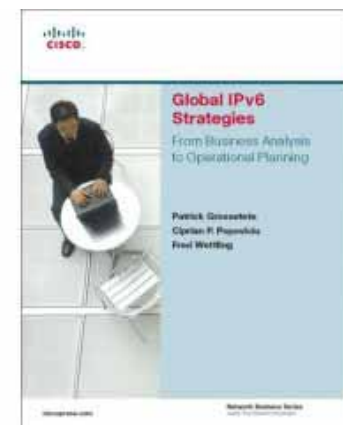
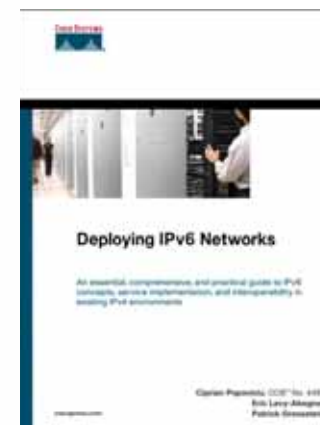
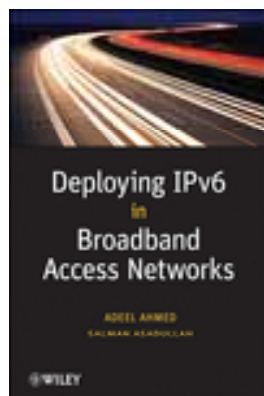
Standard Term	Source and Status	Description	Significance
CIM: Common Information Model	IEC (Standard Framework)	Enables application software to exchange information about configuration and status of electrical network	First open-standard API enabling web-based, multi-vendor utility applications
CIM	IEC 61968-9 (Standard)	CIM for Distribution Network and Metering Applications	Defines standard API between MDMS and AMI Head-Ends
C12.19	ANSI (Standard)	Electric Meter Data Tables	Predominant descriptor of data formats and tables in electric meters
C12.22	ANSI (Standard)	Layer 5/6/7 protocol for transport of C12.19 payload	IP-capable but older and less web-enabled AMI upper-layer spec.
SEP2.0	Smart Energy Profile (Draft)	Layer-7 standard for Home Area Network	Device profiles and procedures for HAN
EXI: Efficient XML Interchange	W3C – WWW Consortium (Draft)	Compact and efficient representation of XML	Enables web paradigm over bit-constrained networks such as AMI
CoRE: Constrained REST-ful Environments	IETF CoRE WG (Draft)	Compact and efficient messaging in the spirit of REST over HTTP	Enables web paradigm over bit-constrained networks such as AMI

# Standards - Networking

Standard Term	Source	Description	Significance
ROLL: Routing over Low-Power, Lossy Links	IETF (Working Group)	IETF Working Group specifying mesh routing protocol over IP for any type of low-power and lossy link	Working group with industry representation to define IP-based mesh routing for any low-power or lossy link type
LLN: Low-Power and Lossy Networks	IETF (Family of Links)	Generic description of link types with limited resources	Defines ROLL routing scope across multiple link types (e.g., 802.15.4, Wi-Fi, PLC)
RPL: Routing Protocol for LLN	IETF ROLL WG (Approved Draft)	Routing protocol under completion in IETF ROLL	Enables interoperable IP routing over LLN with IP layer topology visibility
6LoWPAN	IETF 6LoWPAN WG (Standard)	Adaptation layer for IPv6 over IEEE 802.15.4 links	First industry standard enabling highly efficient IP networking over 802.15.4
802.15.4e	IEEE (Draft – Final Ballot)	Draft standard for 802.15.4 MAC extensions including low-energy operation	Enables low-energy mode of operation for 802.15.4 mesh networks
802.15.4g	IEEE (Draft – Final Ballot)	Draft standard for 802.15.4 PHY for Smart Utility Networks (SUN)	First industry standard for Physical layer of RF Mesh networks for AMI and SUN

# References

- IPv6 Forum – [www.ipv6forum.org](http://www.ipv6forum.org)
- Cisco IPv6 – [www.cisco.com/go/ipv6](http://www.cisco.com/go/ipv6)
- Cisco Smart Grid <http://www.cisco.com/go/smartgrid>
- IP Smart Object alliance (IPSO) <http://www.ipso-alliance.org/>



# Glossary

- CIM: Common Information Model
- DHCP – Dynamic Host Control Protocol
- DNS – Domain Name System
- EGP – Exterior Gateway Protocol
- FAN – Field Area Network
- IANA – Internet Assigned Numbers Authority
- IETF – Internet Engineering Task Force
- IGP – Interior Gateway Protocol
- IP – Internet Protocol
- NAN – Neighborhood Area Network
- OSI – Open Systems Interconnection
- QOS – Quality of Service
- RPL – IPv6 Routing Protocol for Low power and Lossy Networks
- TCP – Transmission Control Protocol
- UDP – User Datagram Protocol
- WAN – Wide Area Network

Thank you.

