Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Routing in The Internet of Things M2M Networks

BRKSPG-1661

TOMORROW starts here.

A place for everything and everything in its place.

The Naughty Girl Won, Religious Tract Society, circa 1799

A network for everything and everything in its network.

Me, just then.

Agenda

What — What is IoT, IoE, M2M?

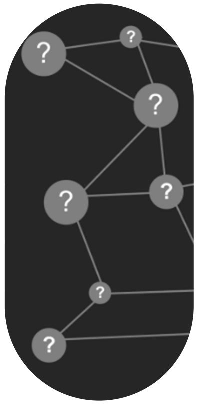
How — How does IP routing work for IoT?

Where — Where would you use it?

CHILLI SCALE OF COMPLEXITY AND CONFUSION

4

Internet of Things



Internet of Things Philosophy

Drivers

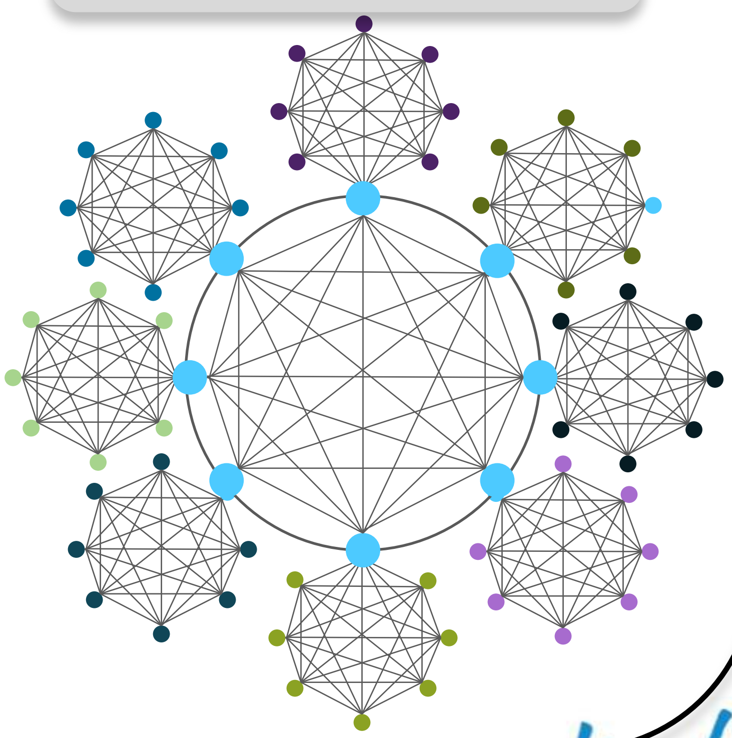
Ubiquitous computing
Intelligence in things at the edge (Fog)

Ubiquitous use of IP
Convergence of proprietary protocols

Ubiquitous connectivity
Radio, Cellular, Fixed

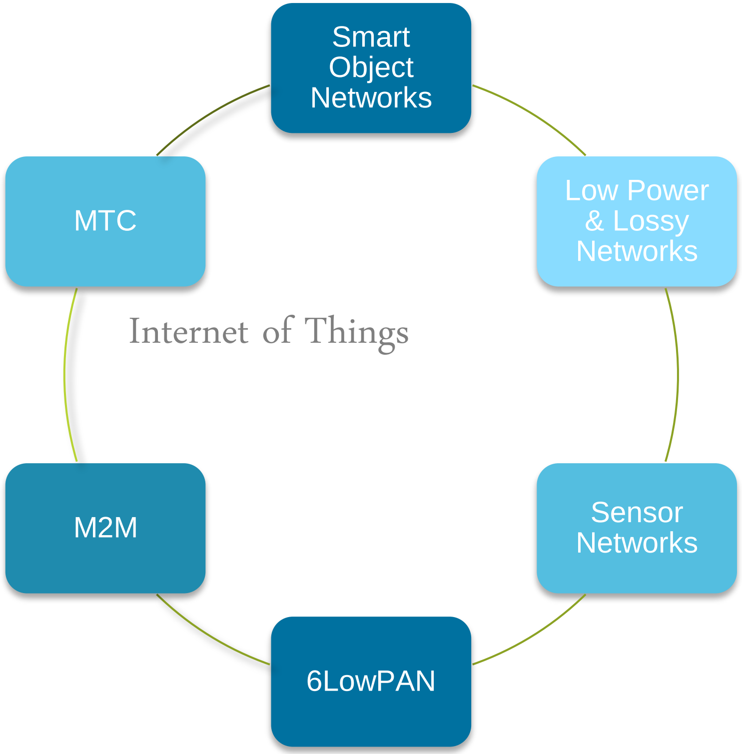
Architectural Philosophy

From	To
Interaction with capable devices via proprietary/closed systems	Distributed intelligence & actions across standardised networks & interfaces



Internet of Things

- Standardise IP into sensors and other objects
- Any object or environmental condition can be monitored
- Give silent things a voice…(make them Smart Objects)



"A pervasive and ubiquitous network which enables monitoring and control of the physical environment by collecting, processing, and analysing the data generated by Smart-Objects"

Enabling Technologies

Routing Protocol for LLNs (RPL)

Lightweight Protocols

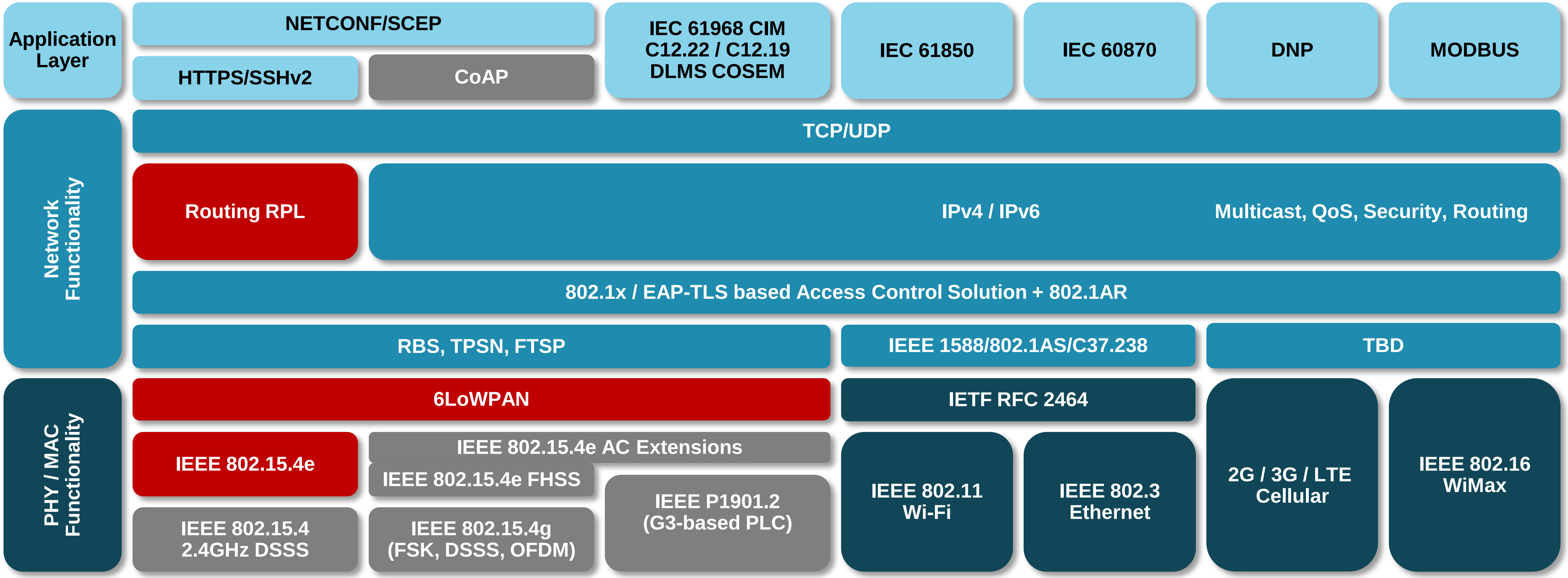
Constrained Application Protocol (COAP)

Embedded Network O/S

COAP Simple Management Prorocol (CSMP)

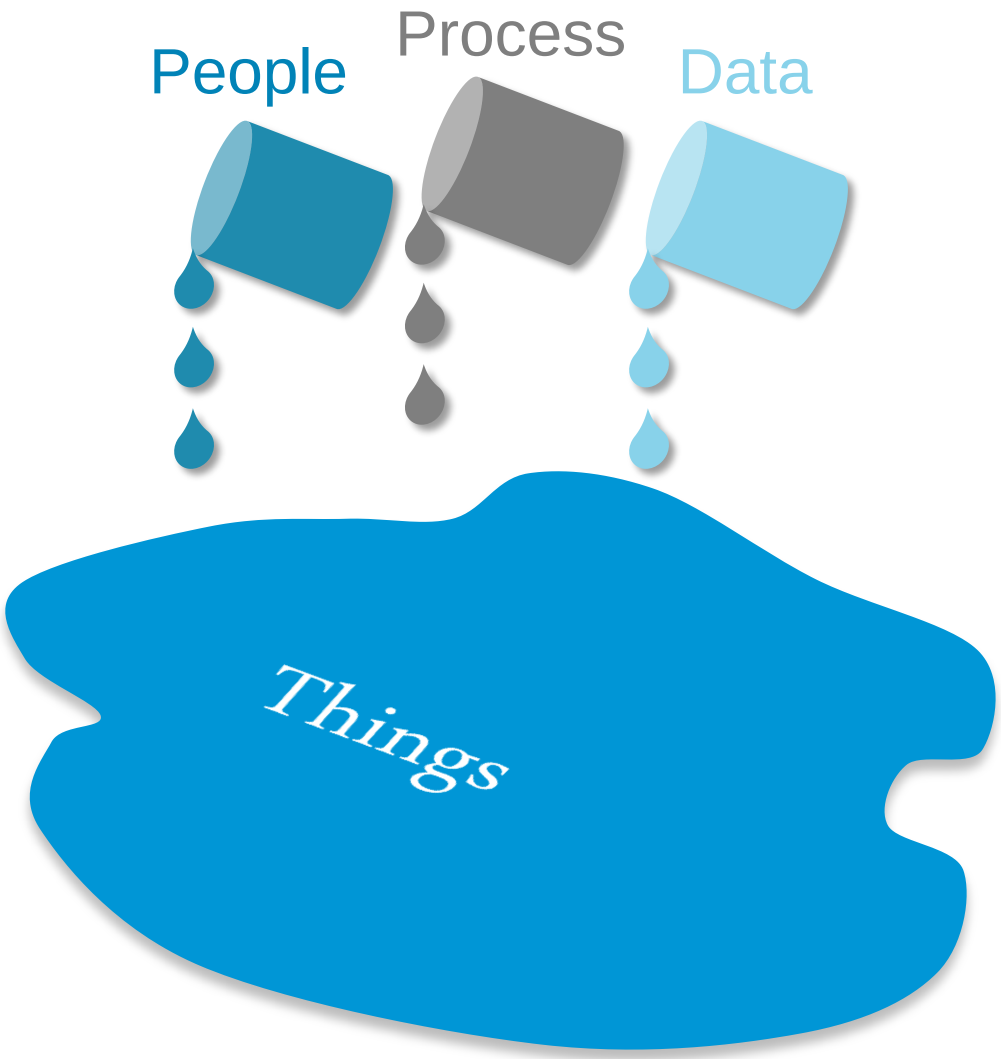
Contiki uIPv6

IoT Based on Open Standards Architecture

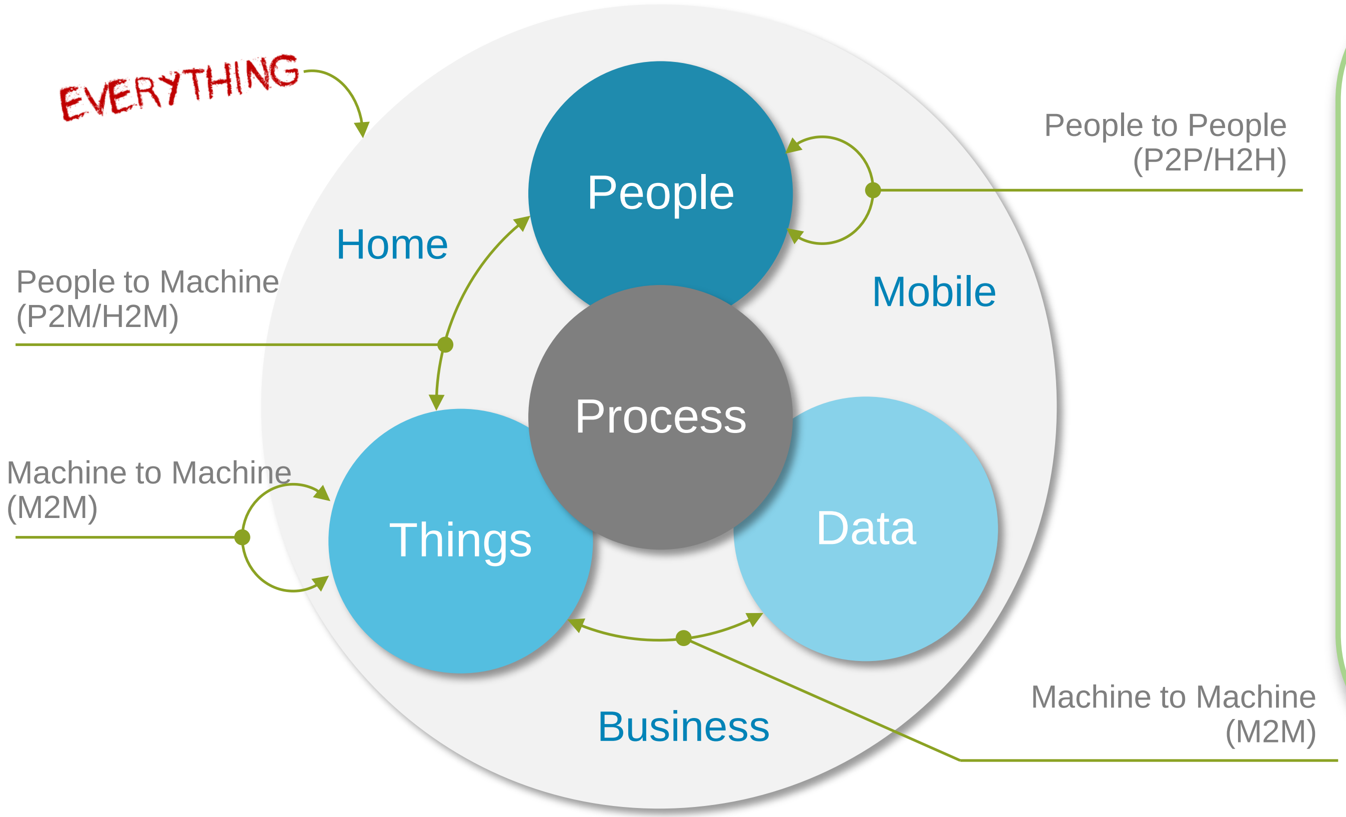


- A well proven layered architecture for the IoT, with a migration path for “Legacy” protocols.
- Flexibility and extensibility is KEY

Take Some Things and Add Stuff

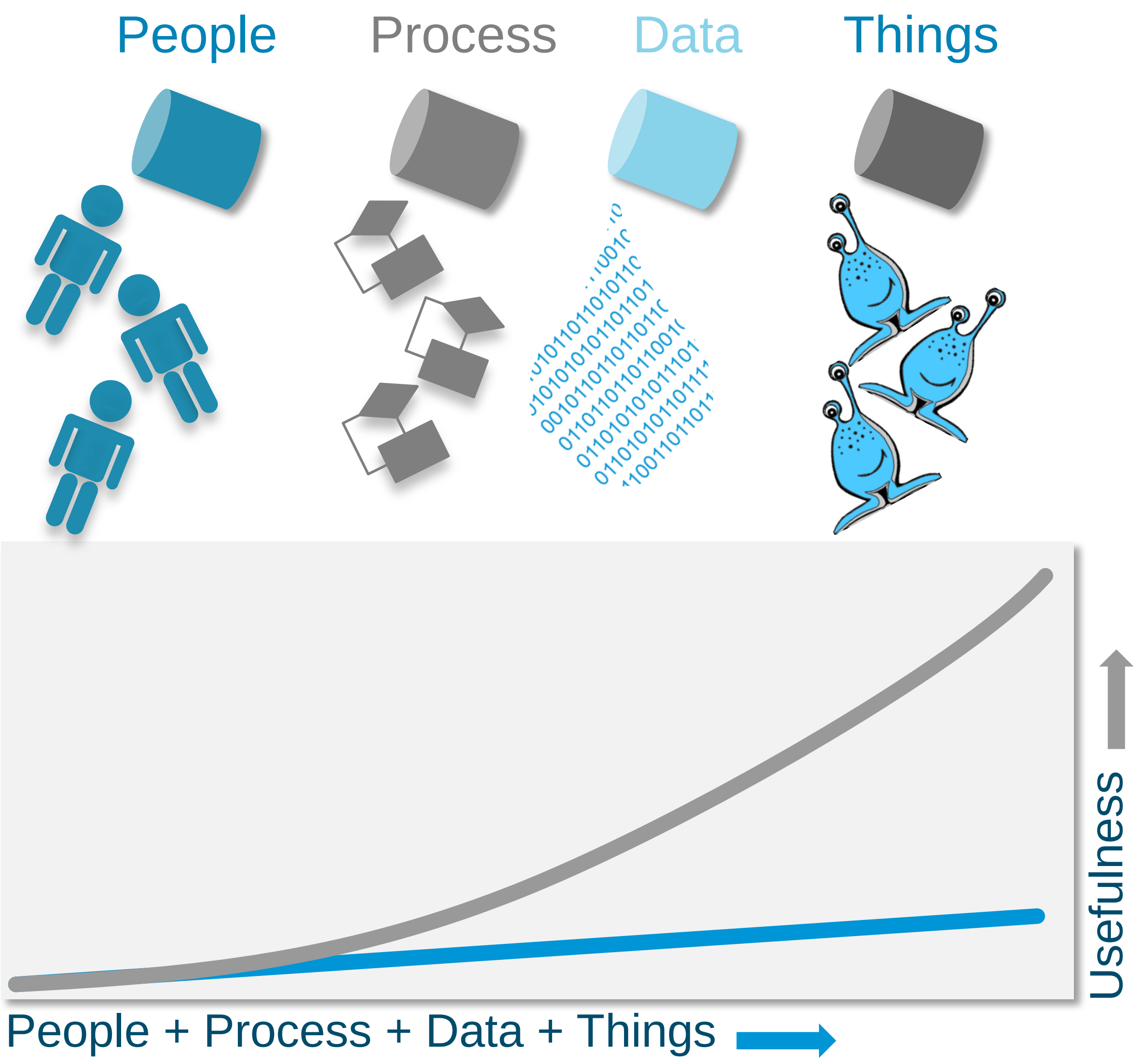


Internet of ~~Things~~ EVERYTHING



"The IoE as brings people, process, data and things together to make networked connections more relevant and valuable than ever before—turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries."

IoE Network Effect



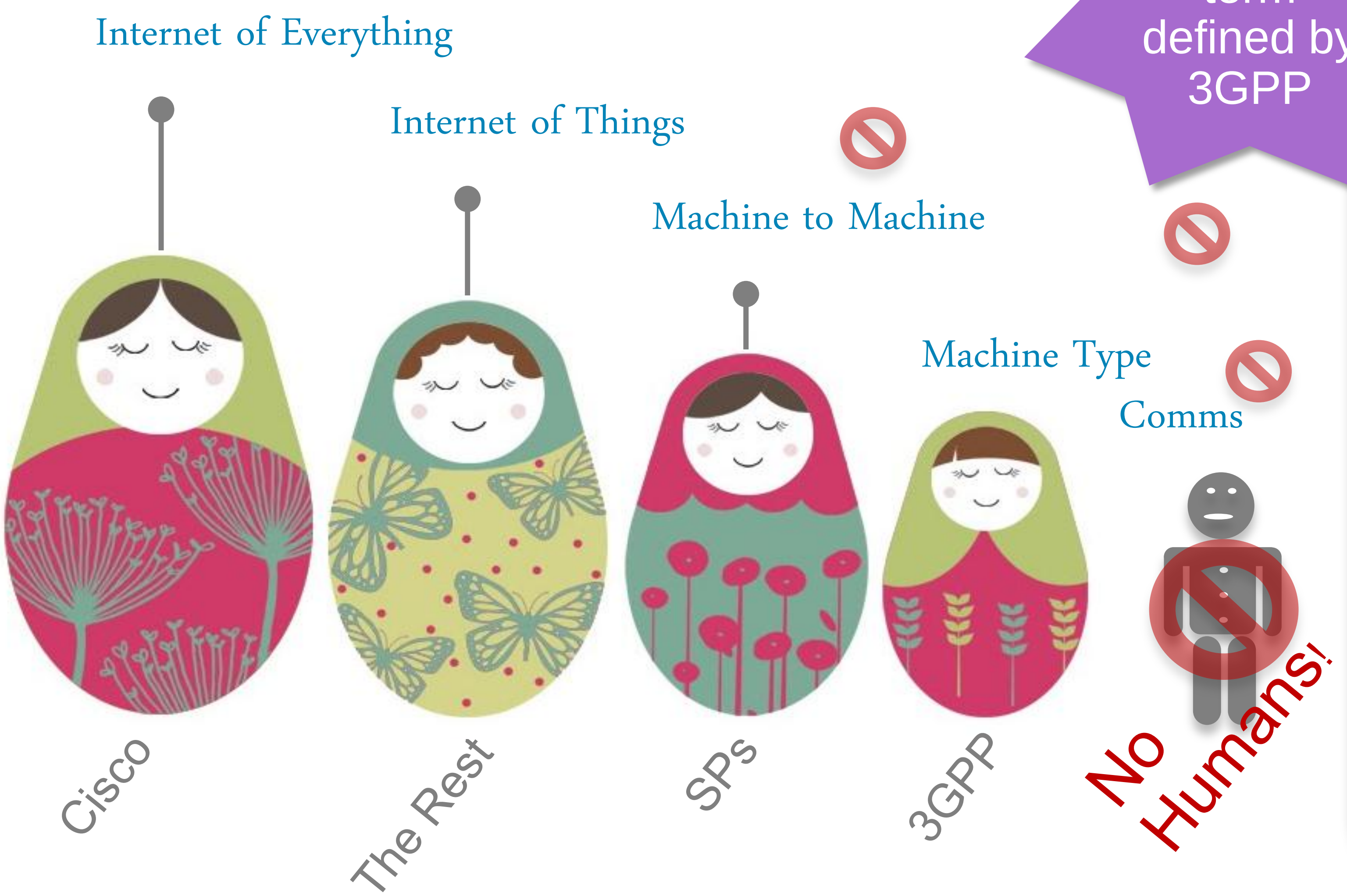
Metcalfe's Law applied to IoE

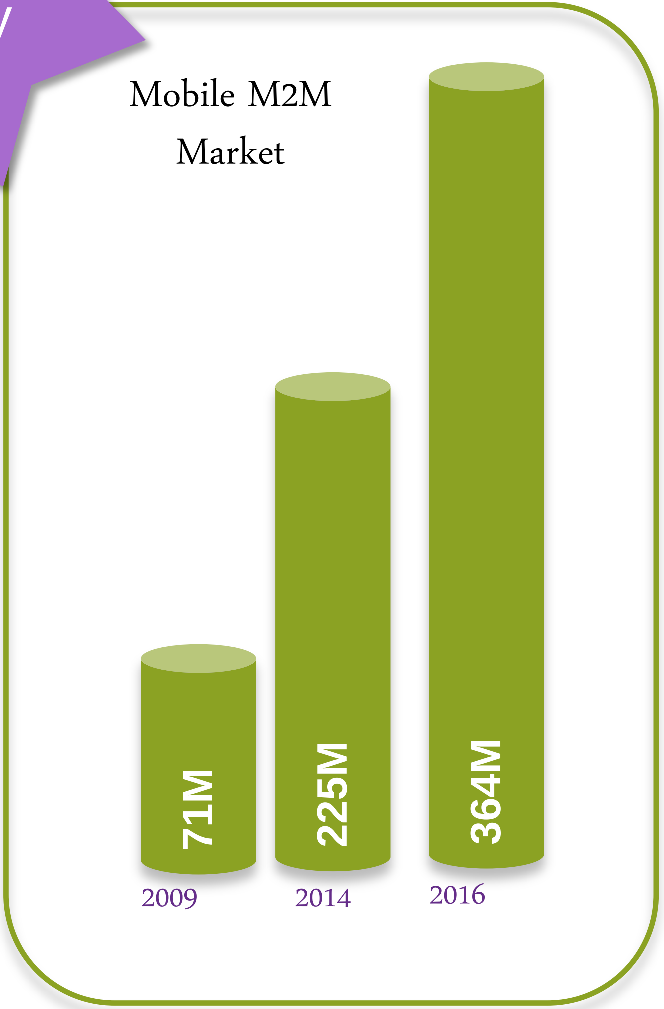
The more People+Things+Data are connected the more useful the intrinsic/stored value of the Internet becomes (content, reputation, usage…)

Machine to Machine

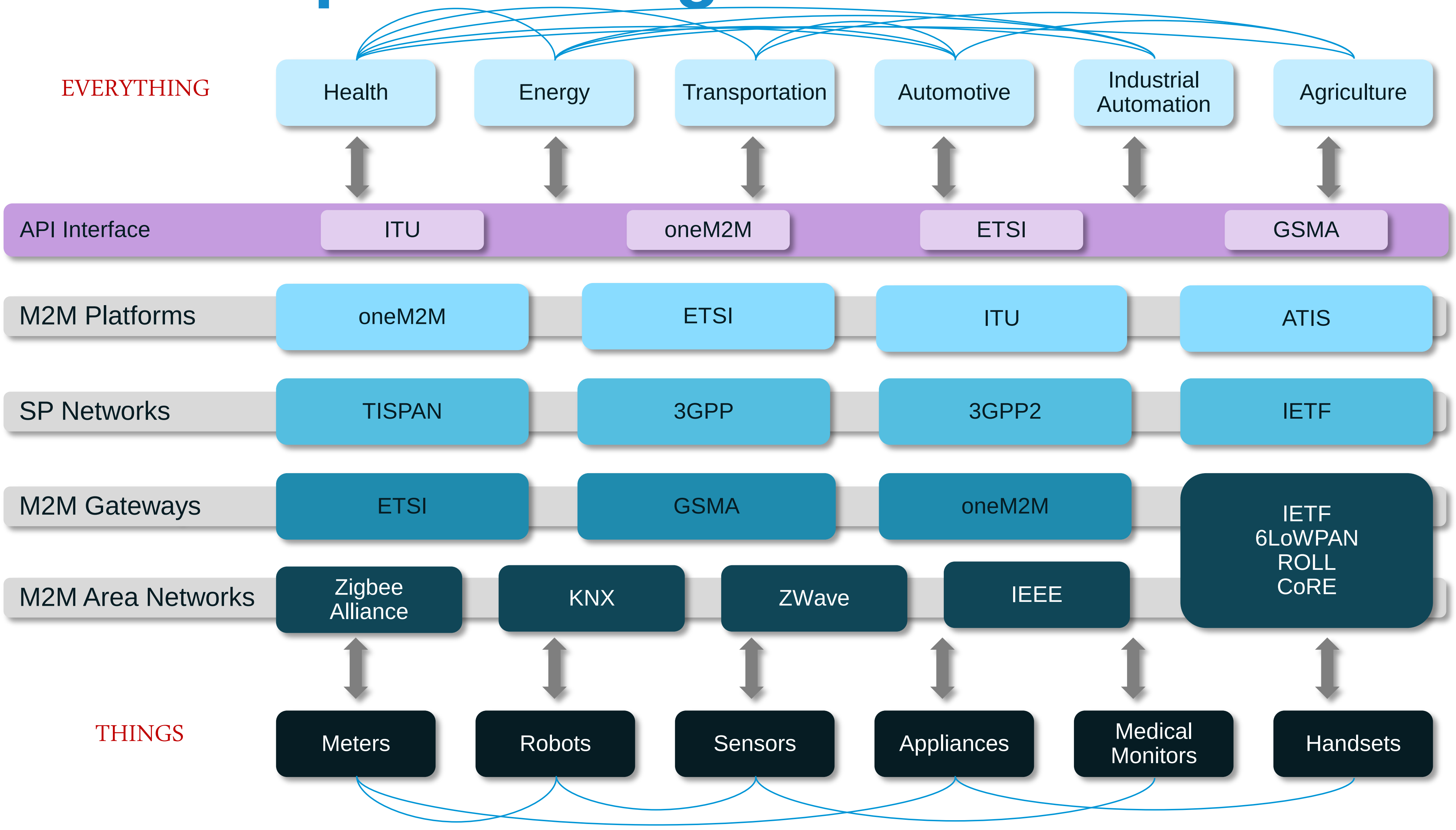
Where Does M2M Fit?

"MTC" is a term defined by 3GPP





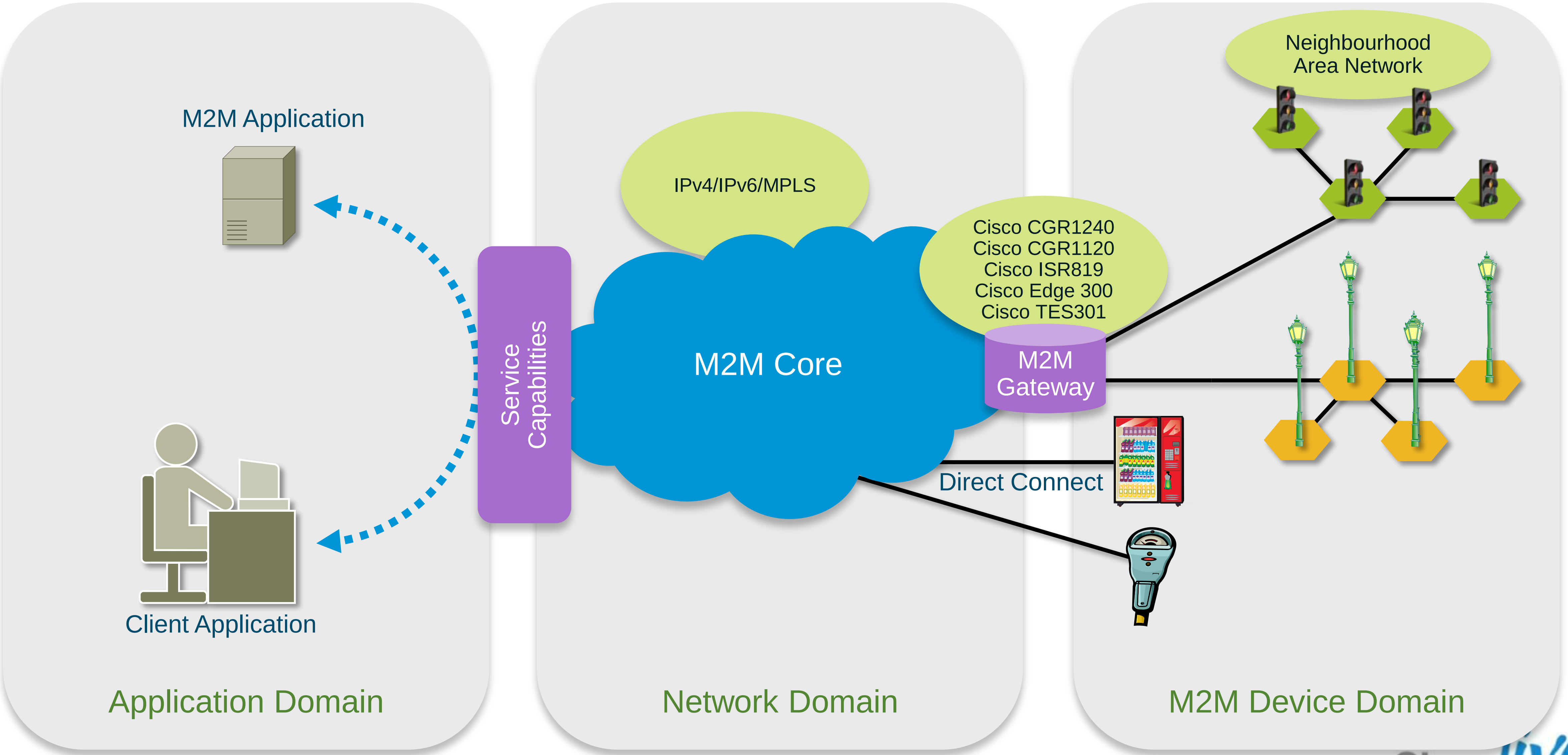
Groups Working on M2M Standards



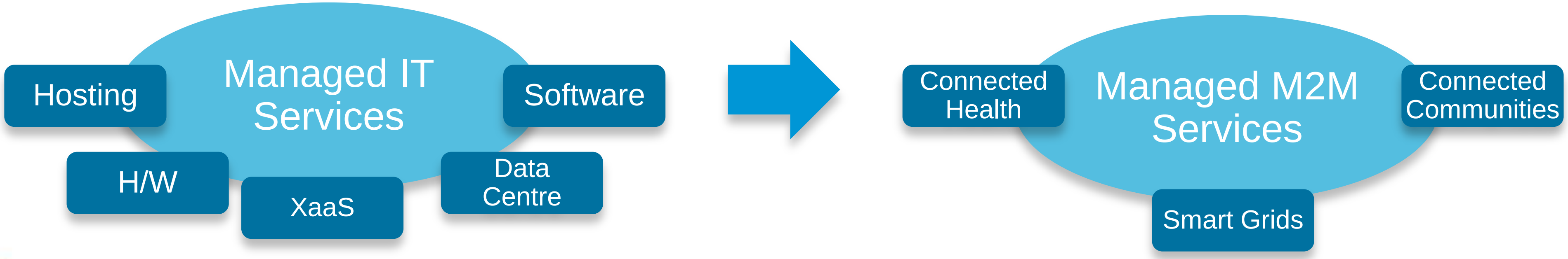
Standards….

Original Source: HTTP://IMGS.XKCD.COM/COMICS/STANDARDS.PNG

ETSI M2M High-Level Architecture



M2M Will Transform Service Providers

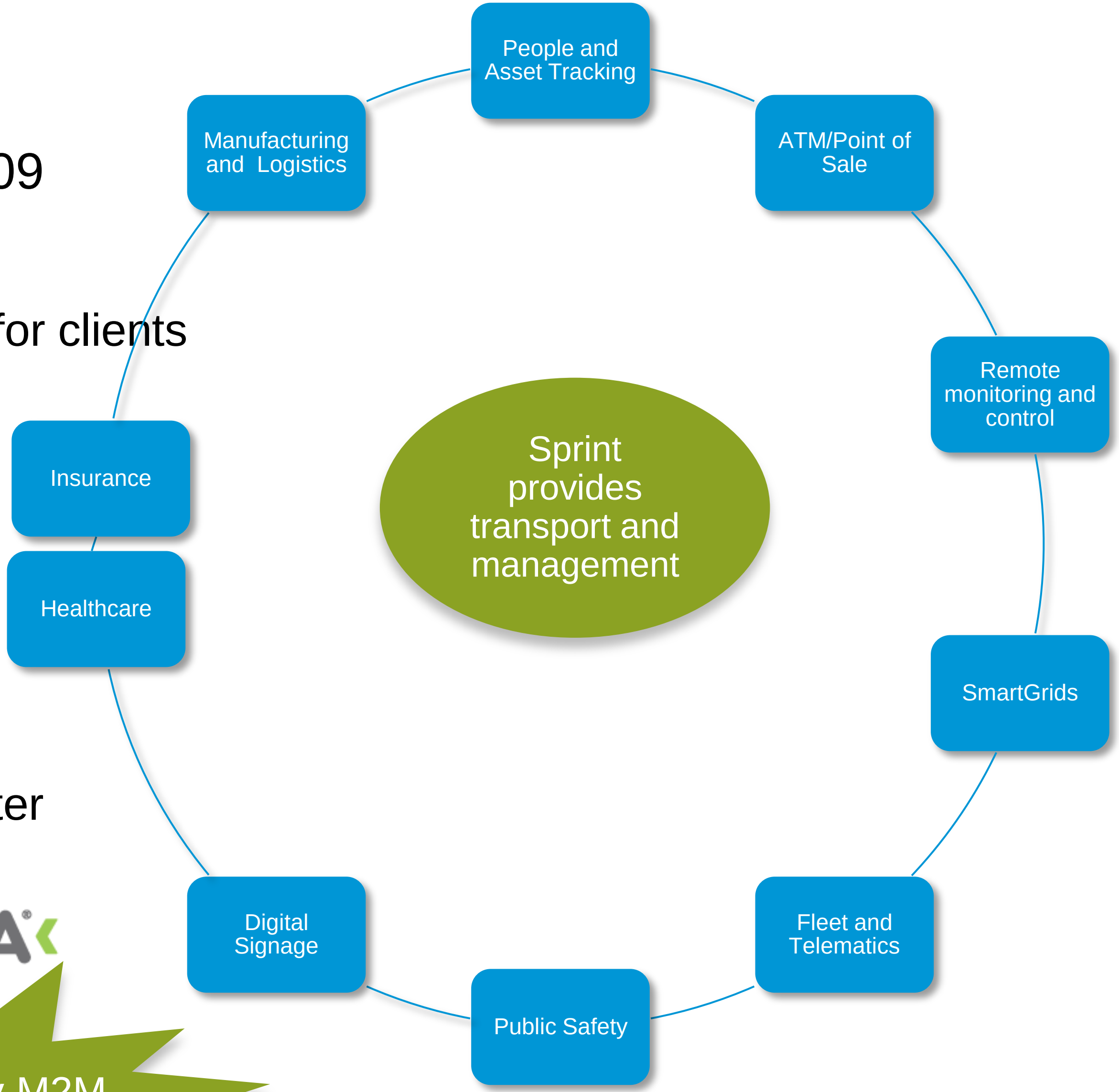


- Enable greater utilisation (hence monetisation) of cellular infrastructure
  - – 1000/10000s of mobile device large data usage vs millions of things small data usage
- Where does the SP play in IPv6 M2M networks?
  - – Transport? Managed Service? Partner with M2M ASPs? Does SP have expertise?
- ARPU for M2M much lower than mobile broadband but still can be profitable
  - – Low or non-existent churn for M2M vs Cell/Mobile Phone
  - – Large number of devices with small bandwidth requirements
- Scalability is an issue

M2M Example Sprint

- Sprint launched Emerging Solutions Group in 2009
  - Focuses on incubating and offering M2M solutions
  - Sprint Command Center offers self-service access for clients
  - Sprint has SME to deal with M2M providers
- Implemented M2M Service examples
  - Remote monitoring of Alzheimer's patients
  - News/weather updates for digital signage
  - Remote monitoring and control of equipment

    Primarily SCADA RTUs for oil wells and waste water
- Sprint have partnered with M2M providers
  - Eg, Fleet & Telematicss



Sprint uses Dual-Stack IPv6

Sprint certify M2M products

www.sprint.com/m2m for more information

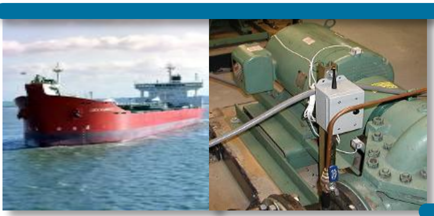
Scalability in M2M

- Mobile networks designed for cell phones H2M/H2H rather than M2M
  - Current M2M implementations primarily use SMS or cellular data (EV-DO, HSPA+)
- M2M networks involve a huge amount of autonomous devices
  - Regular cellular technology is not designed to scale to these numbers
  - Congestion may occur due to simultaneous signalling or data messages
- M2M focus by standards bodies is not necessarily IP end-to-end
  - The Internet of Things is generally predicated on IP end-to-end connectivity
- What is required is a scalable solution for routing huge numbers of machines
- This presentation focusses on how to provide innovative routing in this environment
  - We refer to these M2M devices as Smart Objects in this presentation

Smart Objects

A World of Sensors

- Mostly RS485 wired actuators/sensors
- Generally proprietary architectures for specific applications



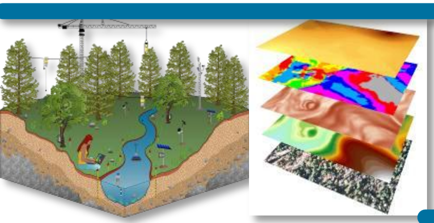
Predictive Maintenance

Energy Saving Smart Grid

High-Confidence Transport and Asset Tracking

Intelligent Buildings

Improve Productivity



Enable New Knowledge

Enhanced Safety & Security

Improve Food and H^{2}O

Healthcare

Smart Home S+CC

A World of Proprietary Protocols

- Many legacy networks use closed/proprietary protocols
  - Each with different implementations at each layer (Physical, Link, Network)
  - Many non-interoperable "solutions" addressing specific problems
  - Resulting in different architectures and protocols
- Interoperability partially addressed by protocol gateways
  - Inherently complex to design, deploy and manage
  - Results in inefficient and fragmented networks, QOS, convergence
- Similar situation to computer networks in the 1980s
  - Islands of systems communicating using SNA, IPX, Appletalk, DECnet
  - Interconnected using multiprotocol gateways

What is a Smart Object?

- A tiny and low cost computing device that may contain
  - A sensor that can measure physical data (e.g., temperature, vibration, pollution)
  - An actuator capable of performing a task (e.g., change traffic lights, rotate a mirror)
  - A communication device to receive instructions , send data or possibly route information
- This device can be embedded into objects (to make them smart ☺)
  - For example, thermometers, car engines, light switches, gas and power meters
- Smart Objects enable many sophisticated applications and solutions
  - Smart+Connected Communities
  - Smart Grid and Energy Management
  - Home and Building Automation
  - Connected Health
- Smart Objects can be organised into networks

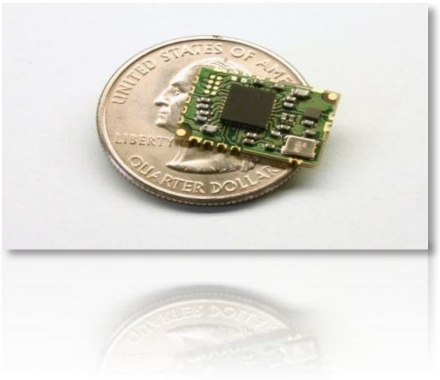
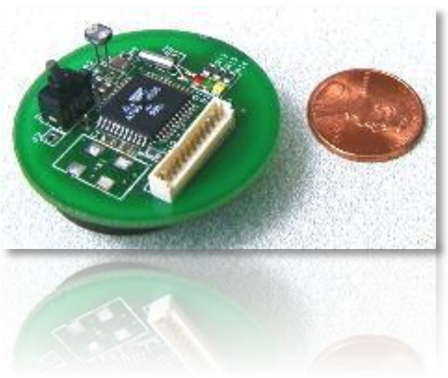
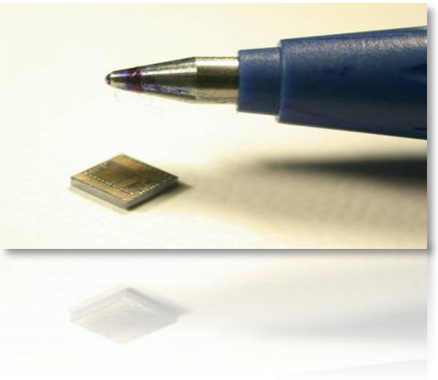
Characteristics of Smart Objects

- These devices are highly constrained in terms of
  - Physical size
  - CPU power
  - Memory (few tens of kilobytes)
  - Bandwidth (Maximum of 250 KB/s, lower rates the norm)
- Power consumption is critical
  - If battery powered then energy efficiency is paramount, batteries might have to last for years
- May operate in harsh environments
  - Challenging physical environment (heat, dust, moisture, interference)
- Wireless capabilities based on Low Power & Lossy Network (LLNs) technology
  - Wireless Mesh mainly uses IEEE 802.15.4 and amendments (802.15.4g Smart Utility Networks)
- May also run over wired technologies such as IEEE P1901.2 PLC (Power Line Comms)

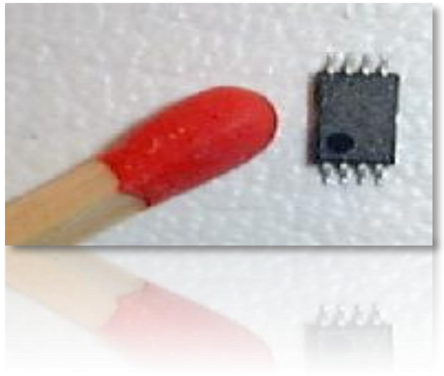
Low Power
Lossy Networks (LLN)

What is a Low Power Lossy Network (LLN)?

- LLNs comprise a large number of highly constrained devices (smart objects) interconnected by predominantly wireless links of unpredictable quality
- LLNs cover a wide scope of applications
  - Industrial Monitoring, Building Automation, Connected Home, Healthcare, Environmental Monitoring, Urban Sensor Networks, Energy Management, Asset Tracking, Refrigeration
- Several IETF working groups and Industry Alliance addressing LLNs
  - IETF - CoRE, 6Lowpan, ROLL
  - Alliances - IP for Smart Objects Alliance (IPSO)

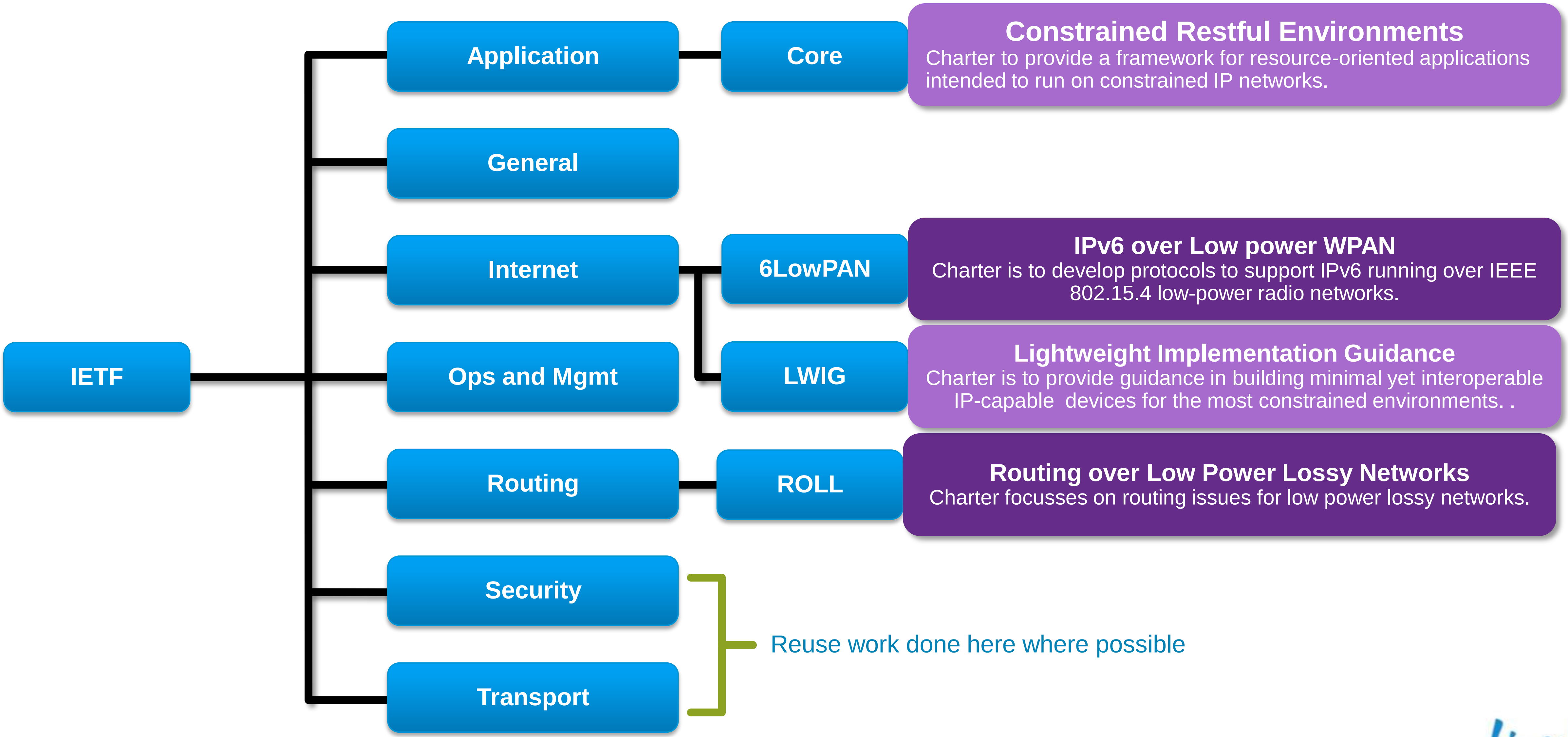
World's smallest web server



Characteristics of LLNs

- LLNs operate with a hard, very small bound on state
- LLNs are optimised for saving energy in the majority of cases
- Traffic patterns can be MP2P, P2P and P2MP flows
- Typically LLNs deployed over link layers with restricted frame-sizes
  – Minimise the time a packet is enroute (in the air/on the wire)
- The routing protocol for LLNs should be adapted for such links
- LLN routing protocols must consider efficiency versus generality
  – Many LLN nodes do not have resources to waste

IETF LLN Related Workgroups



IP for Smart Objects (IPSO) Alliance

- IPSO Alliance formed drive standardisation and inter-operability
  - Create awareness of available and developing technology
- As of 2012 More than 50 members in the alliance
- Document use of new IP based smart object technologies
  - Generate tutorials, webinars, white papers and highlight use cases
  - Provide an information repository for interested parti
- Coordinate and combine member marketing e
- Support and organise interoperability events
  - COMPLIANCE program (Based on IPv6 forum)
- http://www.ipso-alliance.org

Promoters

Contributors

ipso Alliance
Enabling the
INTERNET OF THINGS

IEEE 802.15.4 PAN

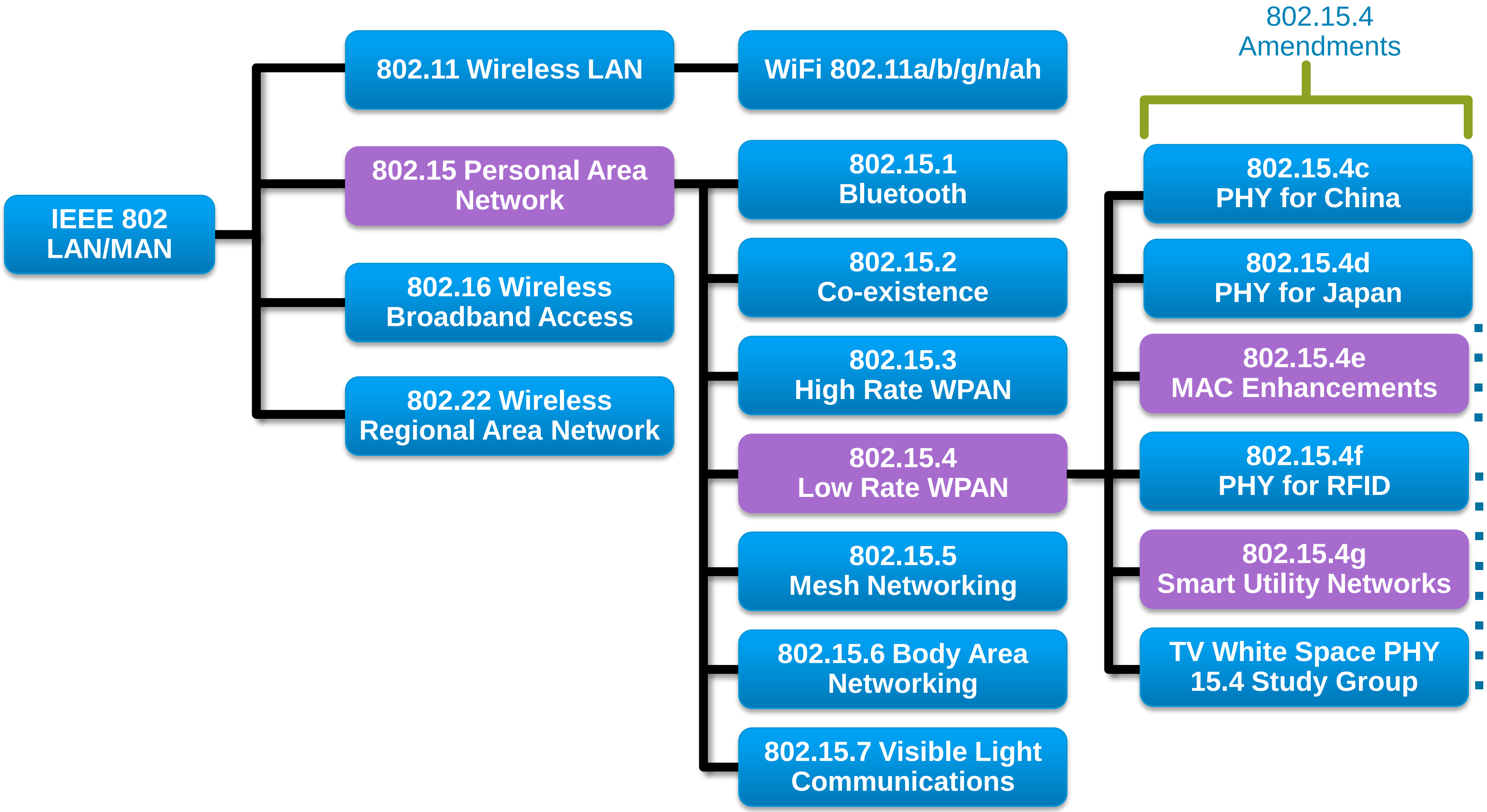
802.15.4 Scope

- Initial activities focused on wearable devices “Personal Area Networks”
- Activities have proven to be much more diverse and varied
  - Data rates from Kb/s to Gb/s
  - Ranges from tens of metres up to a Kilometre
  - Frequencies from MHz to THz
  - Various applications not necessarily IP based
- Focus is on “specialty”, typically short range, communications
  - If it is wireless and not a LAN, MAN, RAN, or WAN, it is likely to be 802.15 (PAN)
- The only IEEE 802 Working Group with multiple MACs

“The IEEE 802.15 TG4 was chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.”

- http://www.ieee802.org/15/pub/TG4.html
  IEEE 802.15 WPAN™ Task Group 4 (TG4) Charter

IEEE Wireless Standards



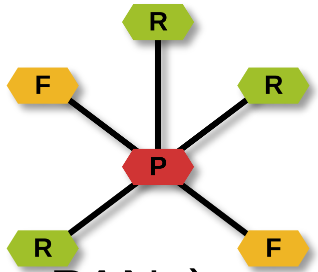
- Industrial strength
- Minimised listening costs
- Improved security
- Improved link reliability

- Support smart-grid networks
- Up to 1 Km transmission
- >100Kbps
- Millions of fixed endpoints
- Outdoor use
- Larger frame size
- PHY Amendment
- Neighbourhood Area Networks

IEEE 802.15.4 Features

- Designed for low bandwidth, low transmit power, small frame size
  - More limited than other WPAN technologies such as Bluetooth
  - Basic packet size is 127 bytes (802.15.4g is up to 2047 bytes) (Smaller packets, less errors)
  - Transmission Range varies (802.15.4g is up to 1km)
- Fully acknowledged protocol for transfer reliability
- Data rates of 851, 250, 100, 40 and 20 kbps (IEEE 802.15.4-2011 05-Sep-2011)
  - Frequency and coding dependent
- Two addressing modes; 16-bit short (local allocation) and 64-bit IEEE (unique global)
- Several frequency bands (Different PHYs)
  - Europe 868-868.8 MHz – 3 chans , USA 902-928 MHz – 30 chans, World 2400-2483.5 MHz – 16 chans
  - China - 314–316 MHz, 430–434 MHz, and 779–787 MHz Japan - 920 MHz
- Security Modes: None, ACL only, Secured Mode (using AES-CCM mode)

IEEE 802.15.4 Node Types

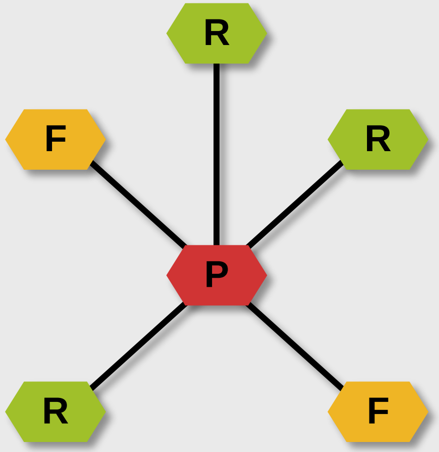


- Full Function Device (FFD)
  - Can operate as PAN co-ord (allocates local addresses, gateway to other PANs)
  - Can communicate with any other device (FFD or RFD)
  - Ability to relay messages (PAN co-ordinator)
- Reduced Function Device (RFD)
  - Very simple device, modest resource requirements
  - Can only communicate with FFD
  - Intended for extremely simple applications

IEEE 802.15.4 Topologies

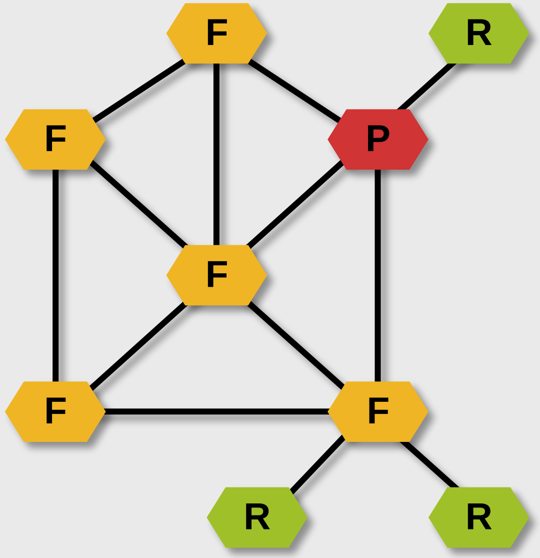
Operates at Layer 2

- Star Topology



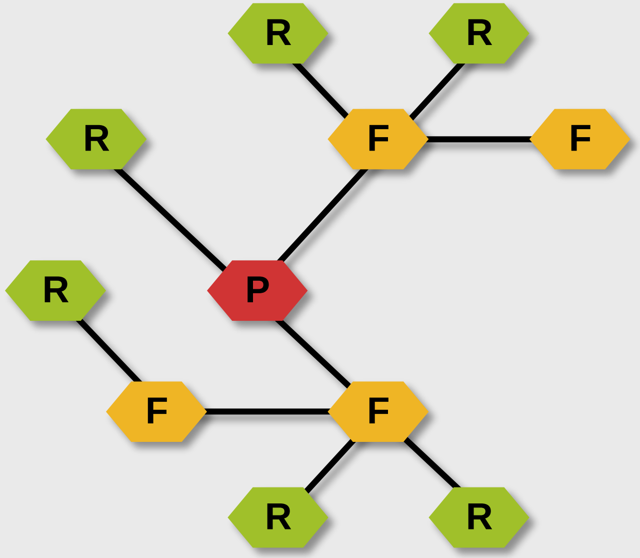
- All devices communicate to PAN co-ordinator which uses mains power
- Other devices can be battery/scavenger

- Mesh Topology



- Devices can communicate directly if within range

- Cluster Tree

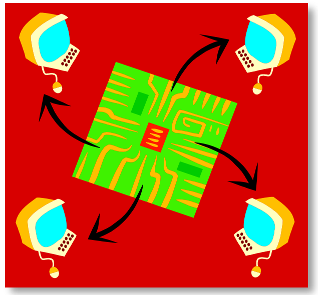


- Higher layer protocols like RPL may create their own topology that do not follow 802.15.4 topologies

Single PAN co-ordinator exists for all topologies

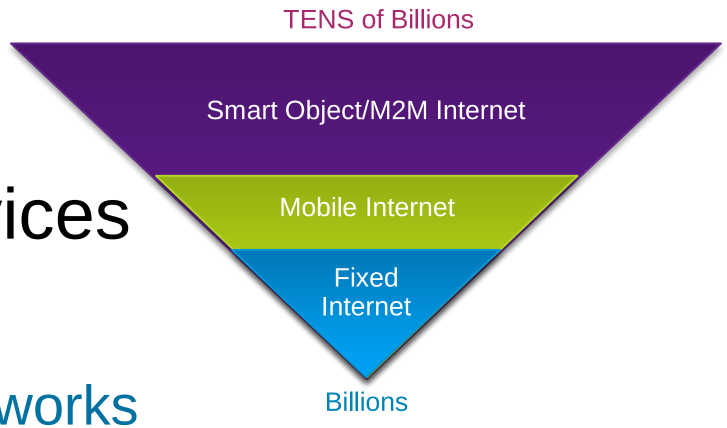
Using IP in Smart Object Networks

IP in Smart Object Networks



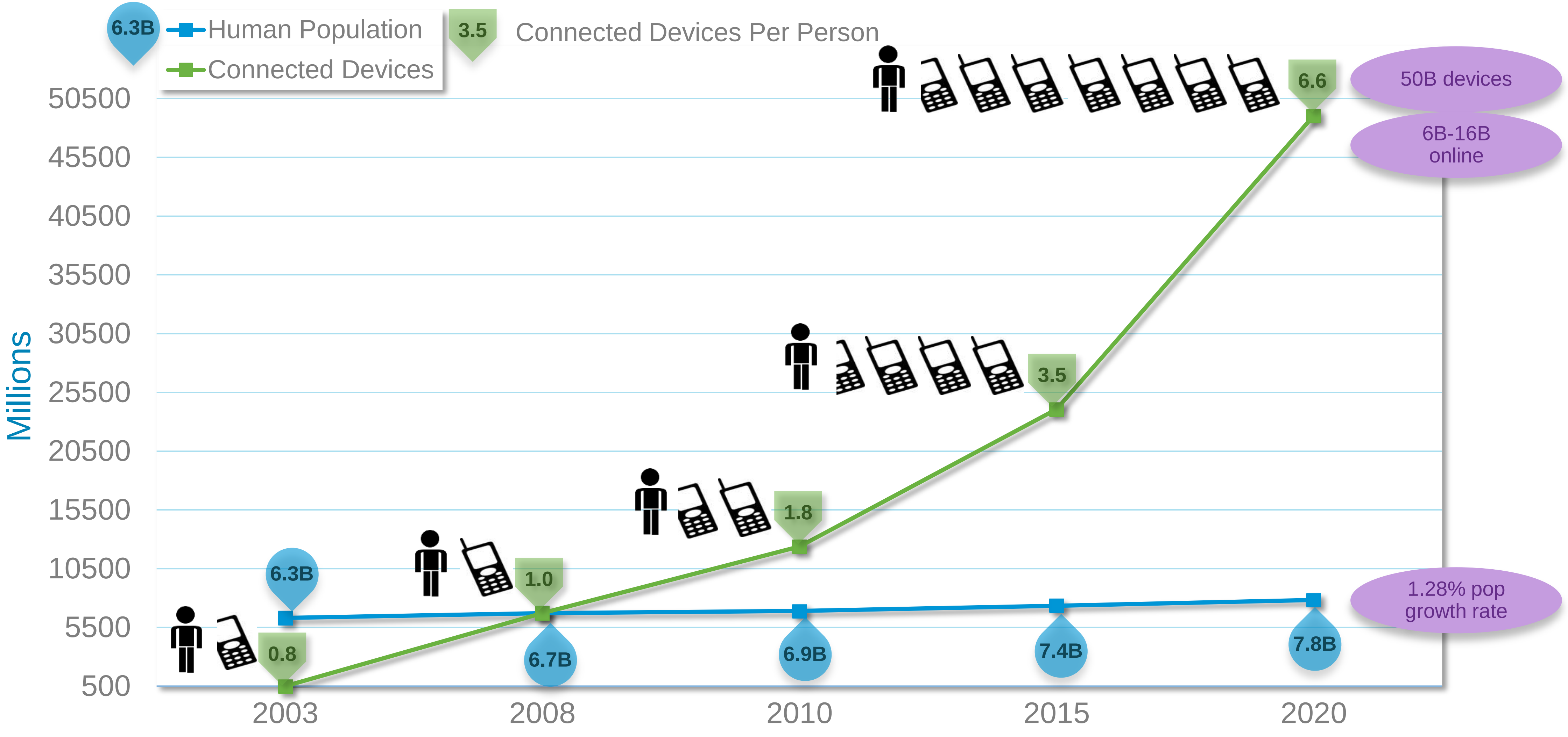
- Today's computer networks are almost exclusively IP based
  - Provides end-to-end reliable connectivity
  - Brings scalability, flexibility and reliability
  - Supports wide a range of devices, transports and applications
- Smart Object Networks standardising on IP
  - General consensus is that IP based Smart Objects networks are the future
  - Move away from proprietary and closed protocols
  - Solid standardisation base allows future innovation
  - Allows quick adoption of emerging applications
  - Allows the creation of the "Internet of Things"
- IP is both an architecture and a protocol
  - Based on standards, Link agnostic
  - Micro operating systems like Contiki provide uIPv6 stack over 802.15.4 radio

IPv4 or IPv6?



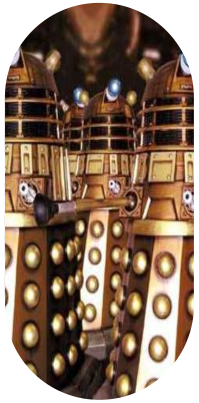
- The current Internet comprises billions of devices
  - Add to this growing 3G, 4G mobile devices
  - There is no scope for IPv4 to support Smart Object Networks
- Not much IPv4 legacy in Smart Object Networks or LLNs
- Smart Objects will add tens of billions of additional devices
- IPv6 is the only viable way forward
  - Solution to address exhaustion
  - Stateless Auto-configuration thanks to Neighbour Discovery Protocol
- Some issues with IPv6 address size
  - Smart Object Networks use low power wireless with small frame size
  - Solution to use stateless and stateful header compression (6LoWPAN)

Connected Devices Growth



Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

6LoWPAN
Working Group



What is 6LoWPAN ? (RFC 6282)

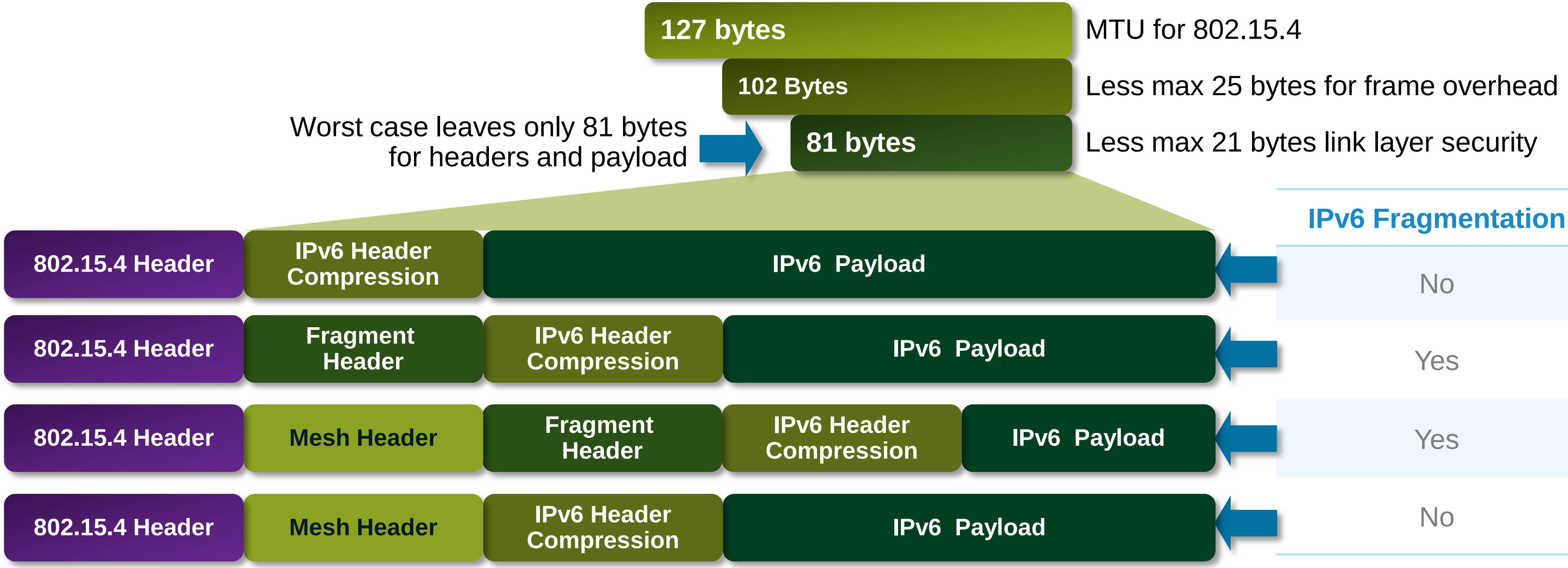
IPv6 and Upper Layers
6LowPAN
802.15.4 MAC
802.15.4 PHY

- IPv6 over Low power Wireless Personal Area Networks
  - Initially an adaptation layer for IPv6 over IEEE 802.15.4 links
  - Now used by IEEE P1901.2 (PLC), Bluetooth Low Energy,DECT Ultra Low Energy
- Why do we need an adaption layer?
  - IEEE 802.15.4 MTU originally 127 bytes, IPv6 minimum MTU is 1280 bytes
  - Even though 15.4g enables larger frame size, bandwidth optimisation is still required
  - IPv6 does not do fragmentation, left to end nodes or lower layers
- Performs 3 functions each with its own 6LoWPAN header
  - IPv6 Header compression
  - IPv6 packet fragmentation and re-assembly
  - Layer 2 forwarding (also referred to as mesh under)
- RFC4919 - Overview, Assumptions, Problem Statement, and Goals
- Cisco SmartGrid endpoints implement RFC 6282

Internet things go better with IPv6 & IEEE 802.15.4

6LoWPAN Header Stacks

- Several 6LoWPAN headers are included when necessary
  – IPv6 compression header
  – Fragmentation header (eliminated if single datagram can fit entire IPv6 payload)
  – Mesh or Layer 2 forwarding header (currently not used/implemented)



IPv6 Fragmentation	Multiple L2 Hops
No	No
Yes	No
Yes	Yes (Future)
No	Yes (Future)

ROLL Working Group

What is ROLL?

- Routing Over Low power and Lossy Networks (2008)
  - http://www.ietf.org/html.charters/roll-charter.html
  - Co-chairs: JP Vasseur (Cisco), David Culler (Arch Rock)
- Mission: To define routing solutions for LLNs
- Application specific LLN routing RFC have been developed

RFC	Application	Title
RFC 5673	Industrial	Industrial Routing Requirements in Low-Power and Lossy Networks
RFC 5548	Urban	Routing Requirements for Urban Low-Power and Lossy Networks
RFC 5826	Home	Home Automation Routing Requirements in Low-Power and Lossy Networks
RFC 5867	Building	Building Automation Routing Requirements in Low-Power and Lossy Networks

- Specifying the routing protocol for smart object networks
  - Routing Protocol for LLNs (RPL) currently WG document

Internet vs Smart Object Networks

Current Internet	Smart Object Networks
Nodes are routers	Nodes are sensor/actuators and routers
IGP with typically few hundreds of 100 nodes	An order of magnitude larger in nodes
Links and Nodes are stable	Links are highly unstable Nodes fail more frequently
Node and link bandwidth constraints are generally non-issues	Nodes & links are high constrained
Routing is not application aware	Application-aware routing, in-Band processing is a MUST

Technical Challenges for Routing Protocols

- Energy consumption is a major issue (battery powered sensors/actuators)
- Limited processing power
- Very dynamic topologies
  - Link failure
  - Node failures (triggered or non triggered)
  - Node mobility (in some environments)
- Data processing usually required on the node itself
- Sometimes deployed in harsh environments (Industrial)
- Potentially deployed at very large scale (millions of nodes)
- Must be self-managed (auto-discovery, self-organising networks)

Current Routing Protocols

- The current IGPs (OSPF, ISIS) rely upon static link metrics
  – Used to create best/shortest path to destination
  – No account taken of node/router status (high CPU, hardware failures)
- Not suitable for the dynamic nature of an LLN with many variables
  – Wireless Signal Strength and Quality
  – Node resources such as residual energy
  – Link throughput and reliability
- IGP needs the ability to consider different metric/constraint categories
  – Node vs Links
  – Qualitative vs Quantitative
  – Dynamic vs Static

Routing over low Power Lossy Networks (RPL)

RPL - Routing Protocol for LLNs

RPL is pronounced "Ripple"

- RPL is an extensible proactive IPv6 distance vector protocol
  - Developed for mesh routing environments
  - Builds a Destination Oriented Directed Acyclic Graph (DODAG) based on an objective
  - RPL supports shortest-path constraint based routing applied to both links and nodes
  - Supports MP2P, P2MP and P2P between devices (leaves) and a root (border router)
- RPL specifically designed for "Lossy" networks
  - Agnostic to underlying link layer technologies (802.15.4, PLC, Low Power Wireless)
- RFC 6202: The trickle algorithm
- RFC 6550: RPL: IPv6 Routing Protocol for LLNs
- RFC 6551: Routing Metrics Used for Path Calculation in LLNs
- RFC 6552: Objective Function Zero for the Routing Protocol for LLNs
- RFC 6553: RPL Option for Carrying RPL Information in Data-Plane Datagrams
- RFC 6554: An IPv6 Routing Header for Source Routes with RPL

What is a DAG?

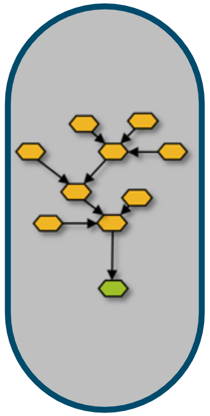
Directed Acyclic Graph

In the context of routing, a DAG is formed by a collection of vertices (nodes) and edges (links).

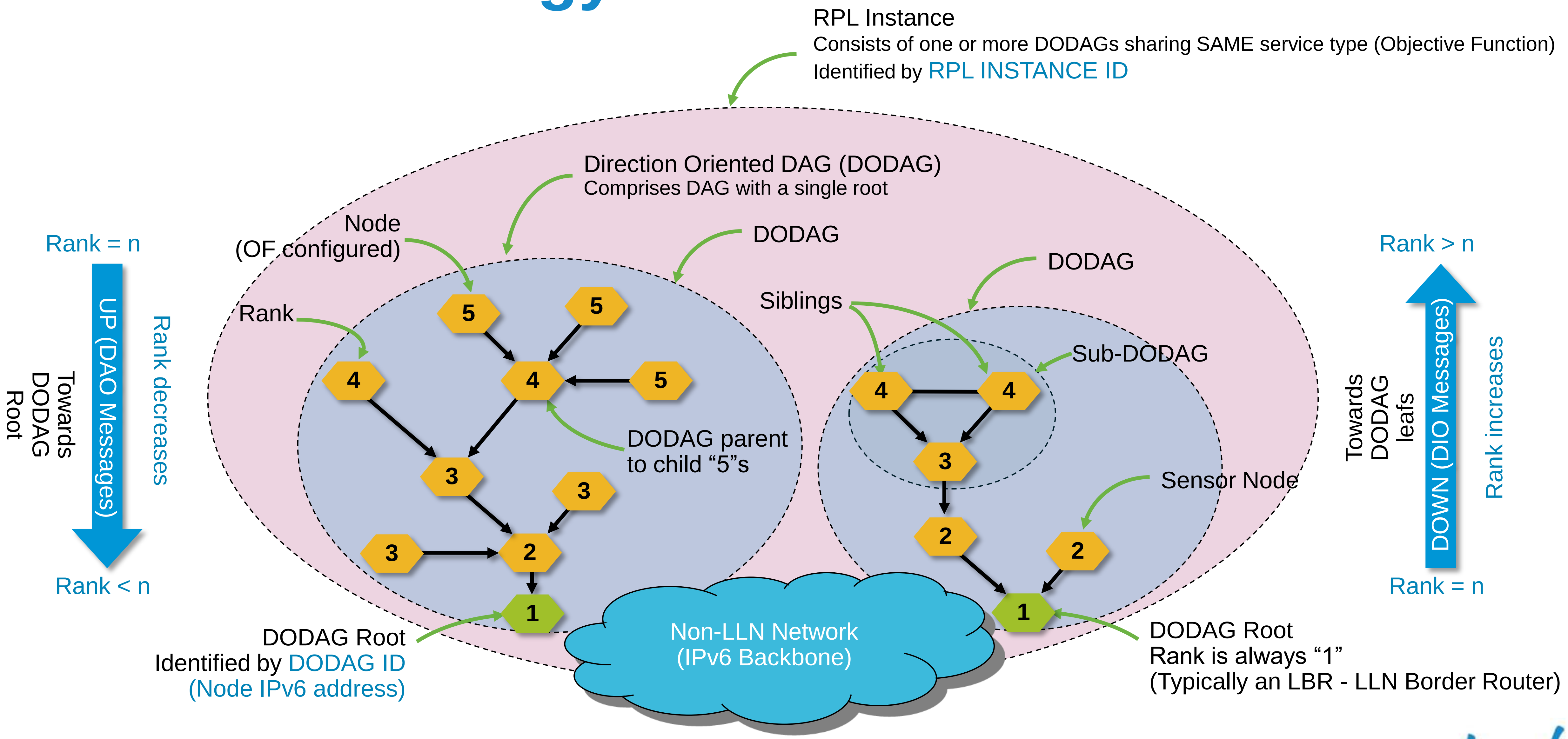
Each edge connecting one node to another (directed) in such a way that it is not possible to start at Node X and follow a directed path that cycles back to Node X (acyclic).

A Destination Oriented DAG is a DAG that comprises a single root node.

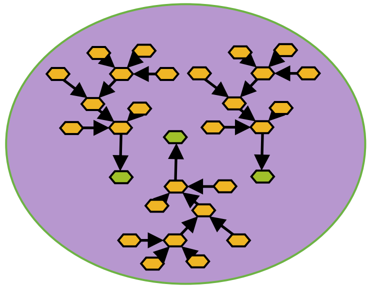
It'is a way to create a loop free path



RPL Terminology

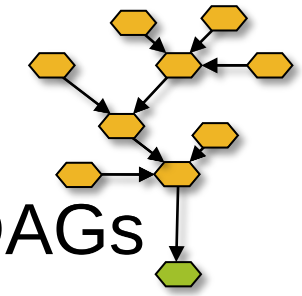


RPL Instances



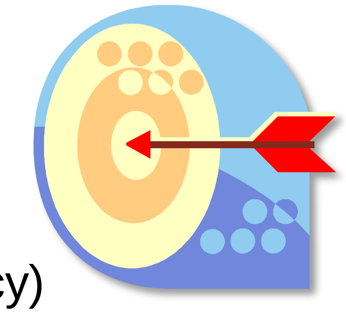
- RPL can form multiple instances
  - Each instance honours a particular routing objective/constraint
  - Instance consists one or more DODAGs derived from the same OBJECTIVE FUNCTION (OF)
  - Nodes select a parent (towards root) based on metric, OF and loop avoidance
- Allows upwards and downwards routing (from DODAG root)
- Trickle timers used to suppress redundant messages
  - Saves on energy and bandwidth (Like OSPF exponential backoff)
- Under-react is the rule
  - Local repair preferred versus global repair to cope with transient failures

RPL DODAGs



- RPL enables nodes to discover each other and form DODAGs
  – Uses ICMPv6 control messages with RPL message codes
- Each root uses a unique DODAG ID (IPv6 address) to identify itself within an RPL Instance
- Routing is performed over the DODAG using distance vector techniques
- Every hop to the root MUST have an alternate path
  – (Quite possible and expected with wireless/radio networks)
- A DODAG will ensure nodes always have a path up towards the root
- A DODAG is identified by {RPL Instance ID, DODAG ID}

Objective Function (OF)



- An OF defines how nodes select paths towards DODAG root
  - Dictates rules on how nodes satisfy a optimisation objective (e.g., minimise latency)
  - Based on routing metrics and constraints carried ICMPv6 control messages
- The OF computes a device rank relative to its distance from the DODAG root

Rank =

Objective Function Example	
Optimisation Objective	Routing Metrics
•Energy Minimisation •Latency •Other Constraints	•Link Metrics •Node Metrics

Rank is higher as distance increases from DODAG root

- Derived rank is advertised to other nodes
- OF decoupled from the routing protocol
- The RPL specification does not include OF definitions
  - OF related to specific applications defined in separate documents (RFCs)
- One Objective Function = One RPL Instance {One or more DODAGS}

Objective Code Points (OCP)

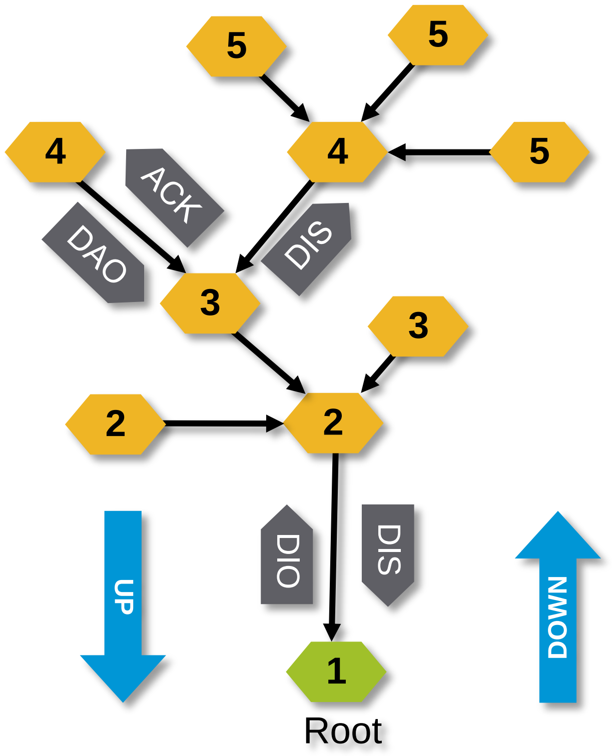
- The OCP indicates the method to be used to construct the DODAG to meet an OF
  – Defines how nodes should combine a set of metrics and constraints in a consistent manner to derive a rank
  – The OCP is the implementation of an Objective Function
- RPL allows OCP to be very flexible in its methods and use of constraints

Example	OCP Method	DODAG Root
Fixed	Link Latency MUST be < 10 seconds	DODAG root cannot override latency constraint
Flexible	Link Latency SHOULD be < 10 seconds	DODAG root can advertise new latency constraint
General	Use link with best latency	DODAG root does not advertise any constraint
Defer	Link Latency should meet advertised constraint	DODAG root advertises actual constraint

- DODAG root can advertise constraints in ICMPv6 messages
- Objective Code Points are 16 bit values assigned by IANA
  – OCP0 defined as the default objective function RFC 6552

ICMPv6 RPL Control Messages

Message	Meaning	Function
DIO	DODAG Information Object	DODAG discovery, formation, maintenance
DIS	DODAG Information Solicitation	Probe neigbourhood for nearby DODAGs (DIO messages)
DAO	Destination Advertisement Object	Propagates destination information up DODAG
DAO-ACK	DAO Acknowledgement	Unicast acknowledgement to a DAO message
CC	Consistency Check	Check secure message counters (for secure RPL)



- ICMPv6 message type 155 - RPL Control message
  - Each RPL control message has a secure variant (Refer Section 6.1 of RPL specification)
- Most RPL control messages have scope of a link

Destination	Source	
Link Local FE80::/64	Link Local FE80::/64	RPL Control Payload
All RPL Nodes FF02::1A	Link Local FE80::/64	RPL Control Payload
Global/Unique Local 2000::/3 or FC00::/7	Global/Unique Local 2000::/3 or FC00::/7	DAO/DAO-ACK Payload (non-storing)

Routing Metrics and Constraints in LLNs (RFC 6551)

Constraint	Provides a path filter for more suitable nodes and links
Metric	A quantitative value used to evaluate a path cost

- Concept of routing objects that can be treated as a metric or a constraint
  - Low pass thresholds used to avoid unnecessarily recomputing DAG
  - Metrics and constraints are advertised in DIO messages
- Computing dynamic metrics takes up power and can change rapidly
  - Solved by abstracting number of discrete values to a metric

Link Quality Metric Example	
Value	Meaning
0	Unknown
1	High
5	Medium
7	Low

Tradeoff

Reduced accuracy vs overhead and processing efficiency

- RFC 6551 Routing Metrics in LLNs

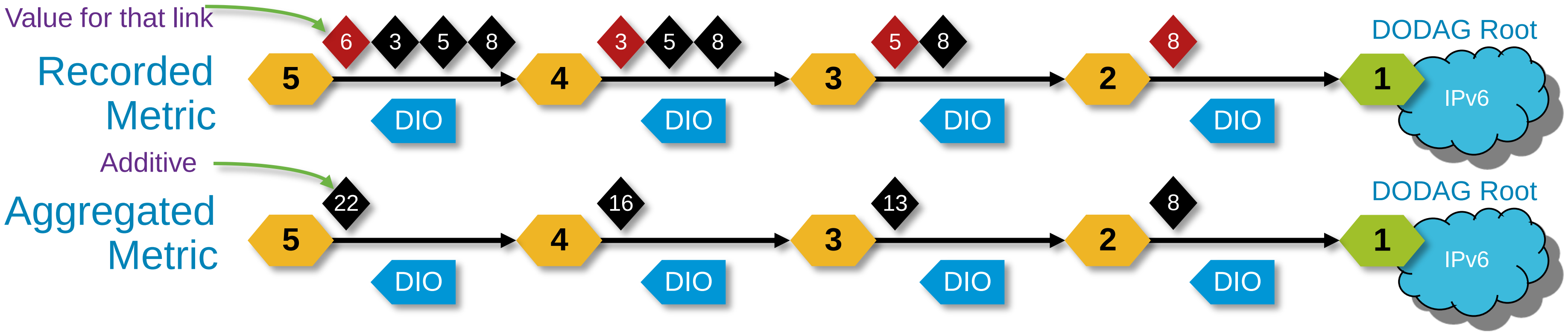
Current Routing Metric/Constraint Objects in LLNs

Node Object	Link Object
Node State and Attributes Object Purpose is to reflects node workload (CPU, Memory…) "O" flag signals overload of resource "A" flag signal node can act as traffic aggregator	**Throughput Object** Currently available throughput (Bytes per second) Throughput range supported
Node Energy Object "T" flag: Node type: 0 = Mains, 1 = Battery, 2 = Scavenger "I" bit: 0 = Exclude, 1 = Include (bits set in node type field) "E" flag: Estimated energy remaining flag "E-E" field contains estimated % energy remaining	**Latency** Can be used as a metric or constraint Constraint - max latency allowable on path Metric - additive metric updated along path
Hop Count Object Can be used as a metric or constraint Constraint - max number of hops that can be traversed Metric - total number of hops traversed	**Link Reliability** Link Quality Level Reliability (LQL) 0=Unknown, 1=Highest … …7=Lowest Expected Transmission Count (ETX) (Average number of TX to deliver a packet)
	Link Colour Metric or constraint, arbitrary admin value

Link and Node metrics are usually (but not necessarily) additive along a path to the DODAG root

Advertising Routing Metrics

- Node advertise node and link metrics in a DIO message metric container
- Metrics can be recorded or aggregated along the path up to the DODAG root

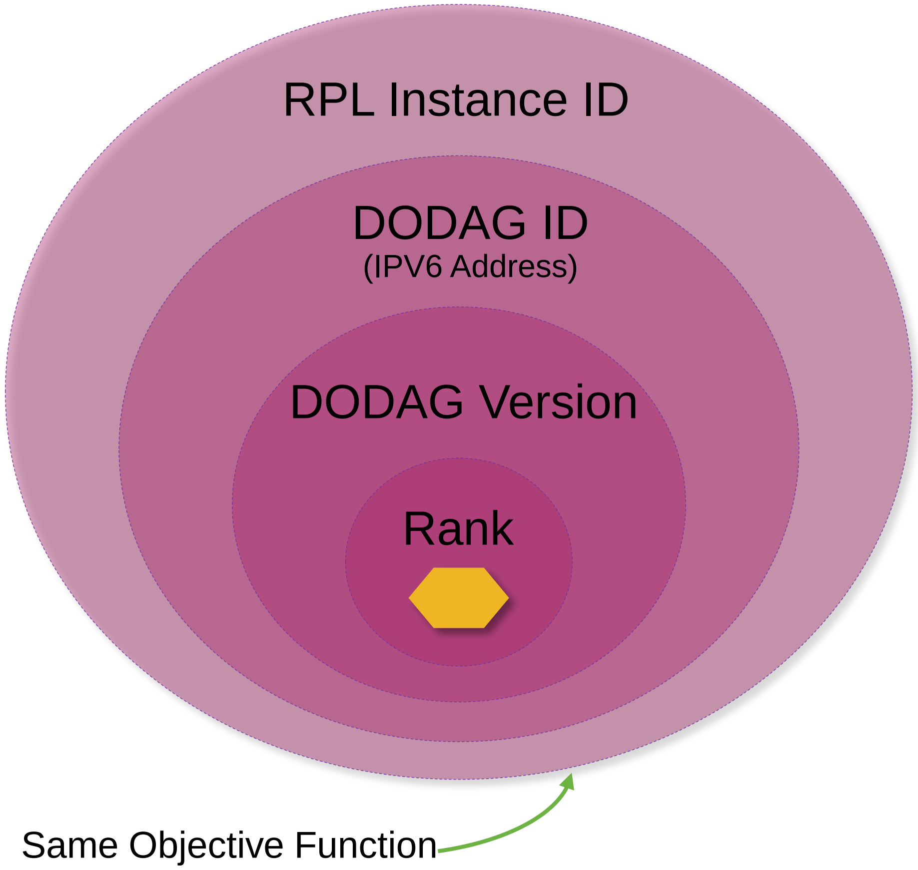


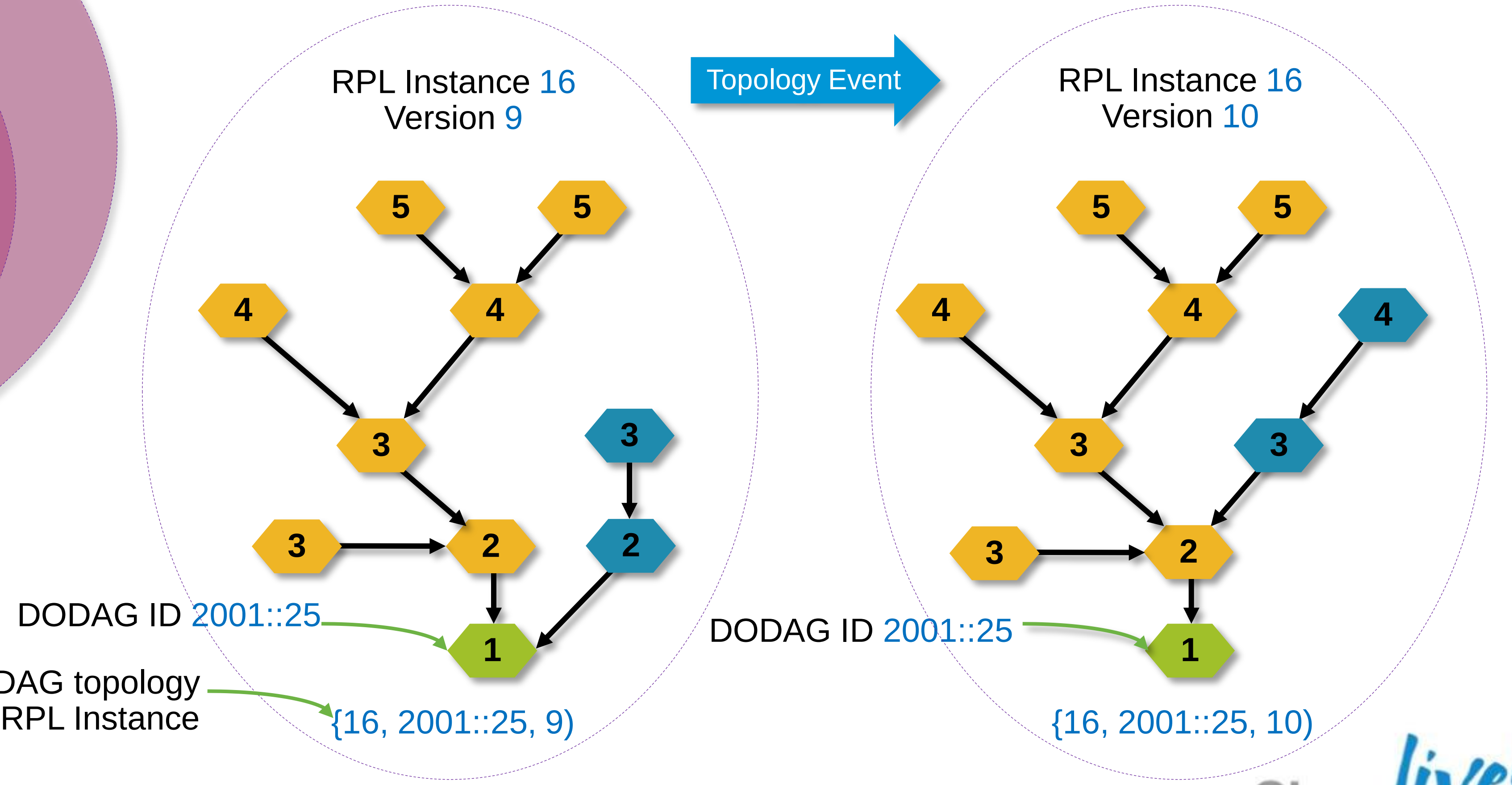
- An aggregated routing metric can be processed in several ways

Agg Type	Processing	Example at 5
0x00	The routing metric is additive	22
0x01	The routing metric reports a maximum	8
0x02	The routing metric reports a minimum	3
0x03	The routing metric is multiplicative	5760

RPL Identifiers

- Four values used to identify and maintain DODAG topology
  - Nodes in a particular topology will belong to the same DODAG version
  - Rank within {RPL Instance ID, DODAG ID, DODAG Version} scope

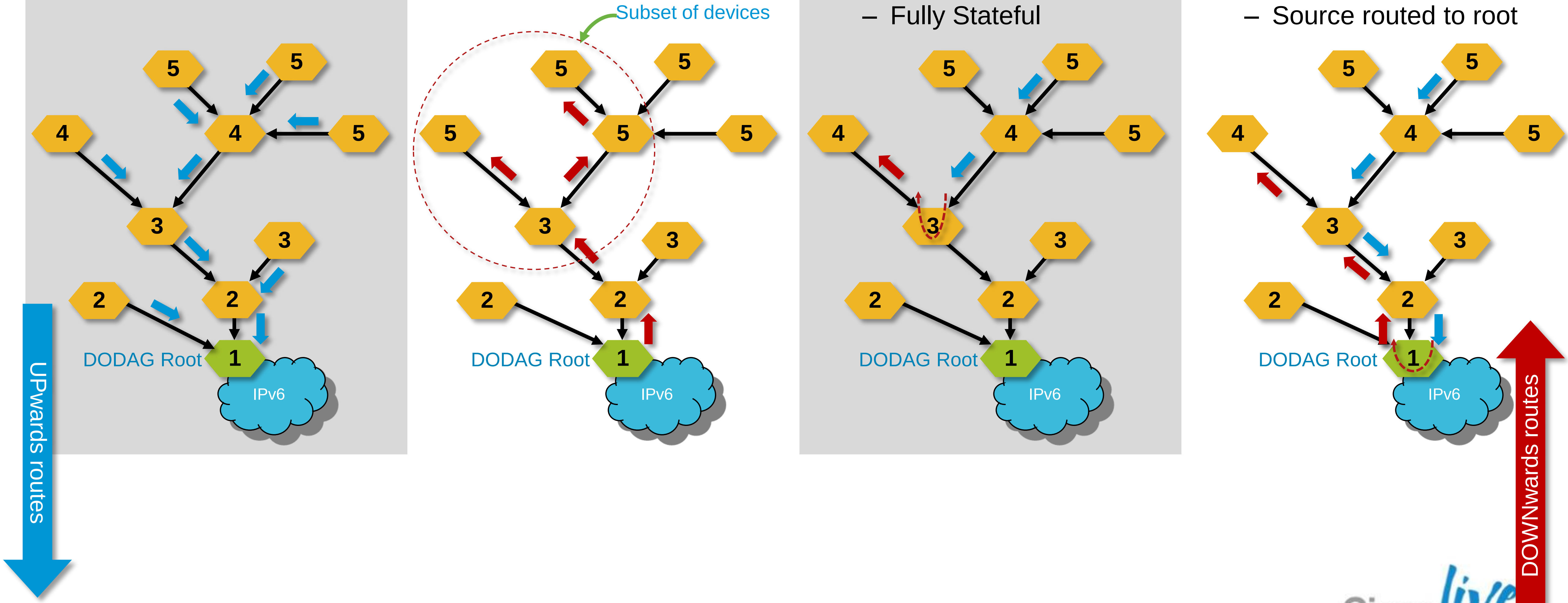




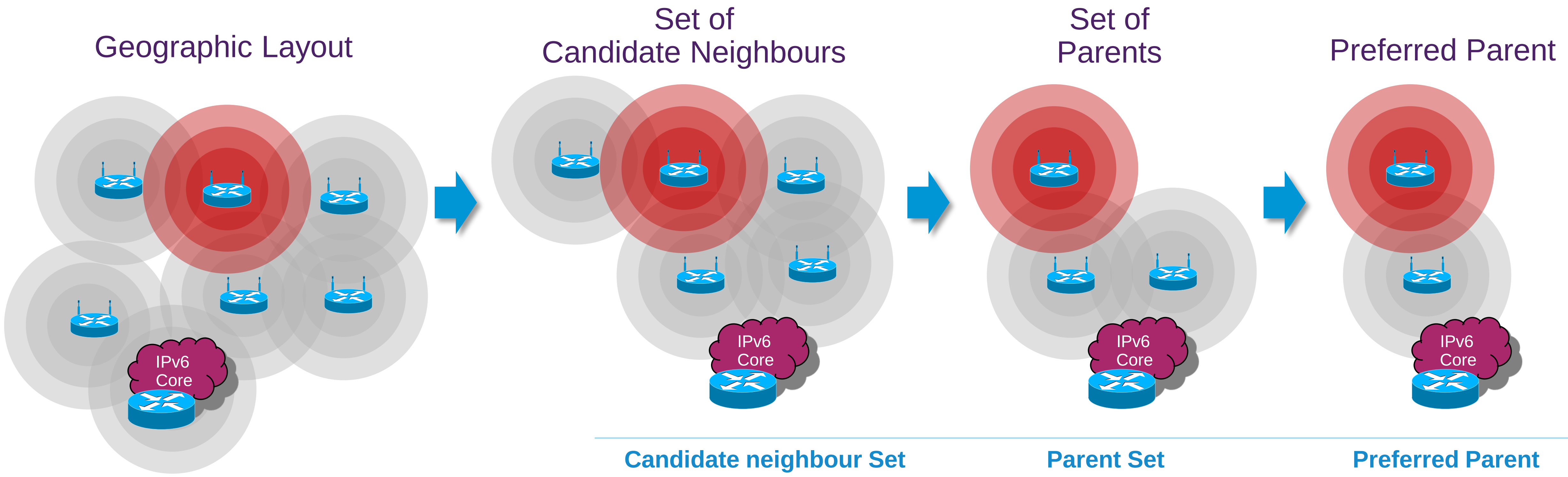
Cisco live!

RPL Supported Traffic Flows

- Multipoint to Point
  - DIO messages
- Point to Multipoint
  - DAO messages
- Point to Point
  - Storing Mode, DAO
  - Fully Stateful
- Point to Point
  - Non-Storing Mode, DAO
  - Source routed to root



DODAG Neighbours and Parent Selection



- Upward route discovery
  - Comprises three logical sets of link-local nodes
  - Neighbours are learnt from DIO advertisements

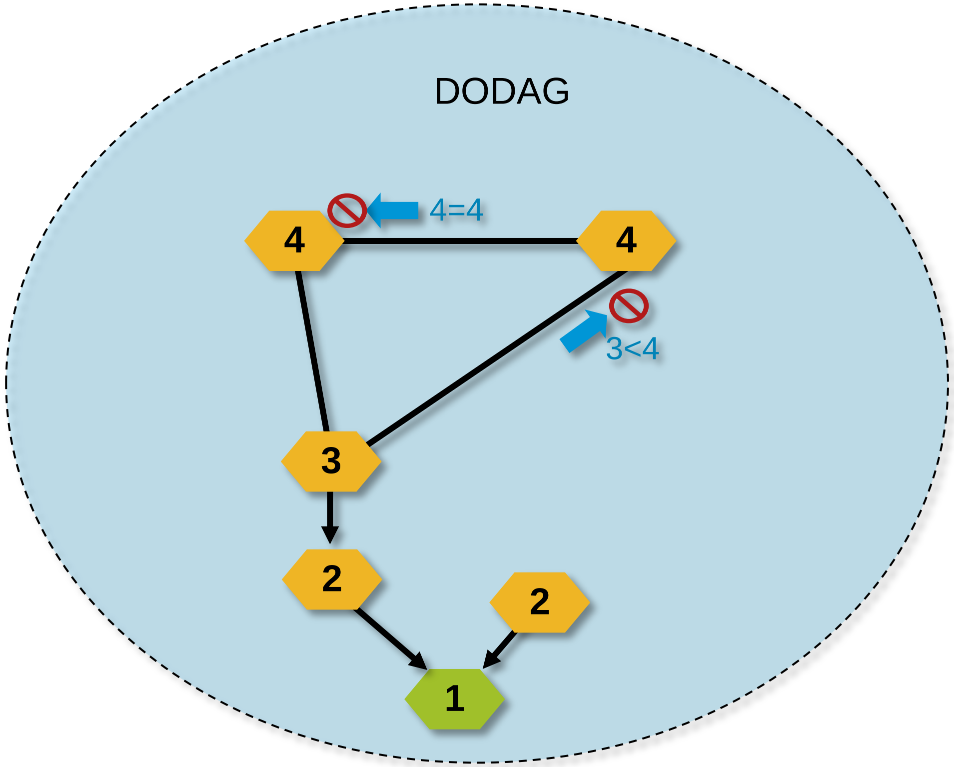
Candidate neighbour Set	Parent Set	Preferred Parent
Subset of nodes reachable via link-local multicast	Consists of nodes with a higher rank (lower #)	Preferred next-hop to the DODAG Root
Elements in the set MAY belong to different DODAG versions	Elements in the set MUST belong to SAME DODAG version	Multiple preferred parents possible if ranks are equal

RPL Security

- RPL supports optional message confidentiality and integrity
  - Link-layer mechanisms can be used instead when available
  - RPL security mechanisms can be used in the absence of link-layer
  - Refer to Section 10 of RPL standard
- RPL supports three security modes

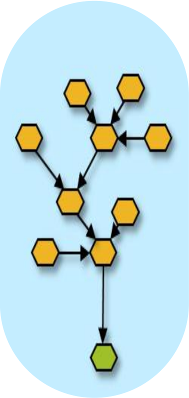
Security Mode	Description
Unsecured	RPL message sent unsecured - may underlying security mechanisms
Pre-installed	RPL nodes use same pre-shared/installed key to generate secure RPL messages
Authenicated	Uses pre-installed key to allow RPL node to join as a leaf only To function as a router requires obtaining a key from authentication authority

RPL Loop Detection



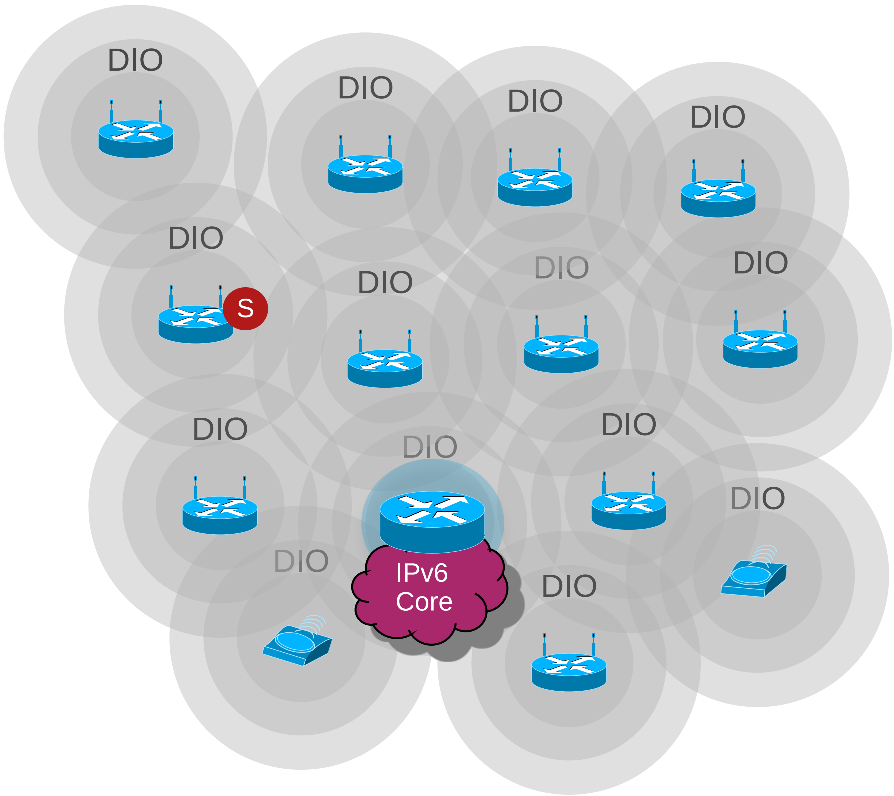
- Data path validation used to check for loops (Simple mechanism)
  - IPv6 options header carries rank of transmitter
- If node receives packet with rank <= to its own, drop packet
  - Detection happens when link is actually used.

DODAG Examples

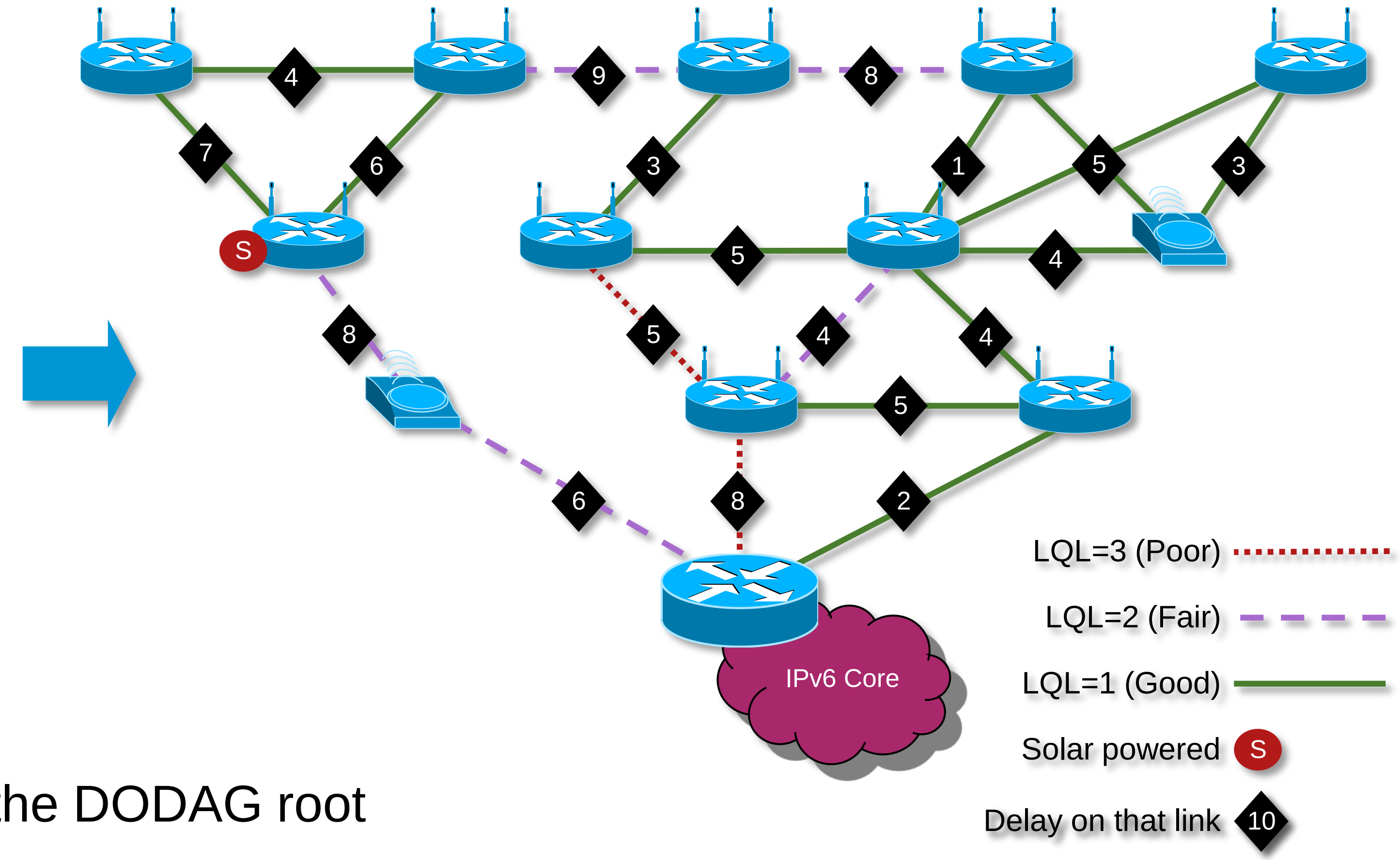


DODAG Examples

Geographic Layout



DODAG Topology

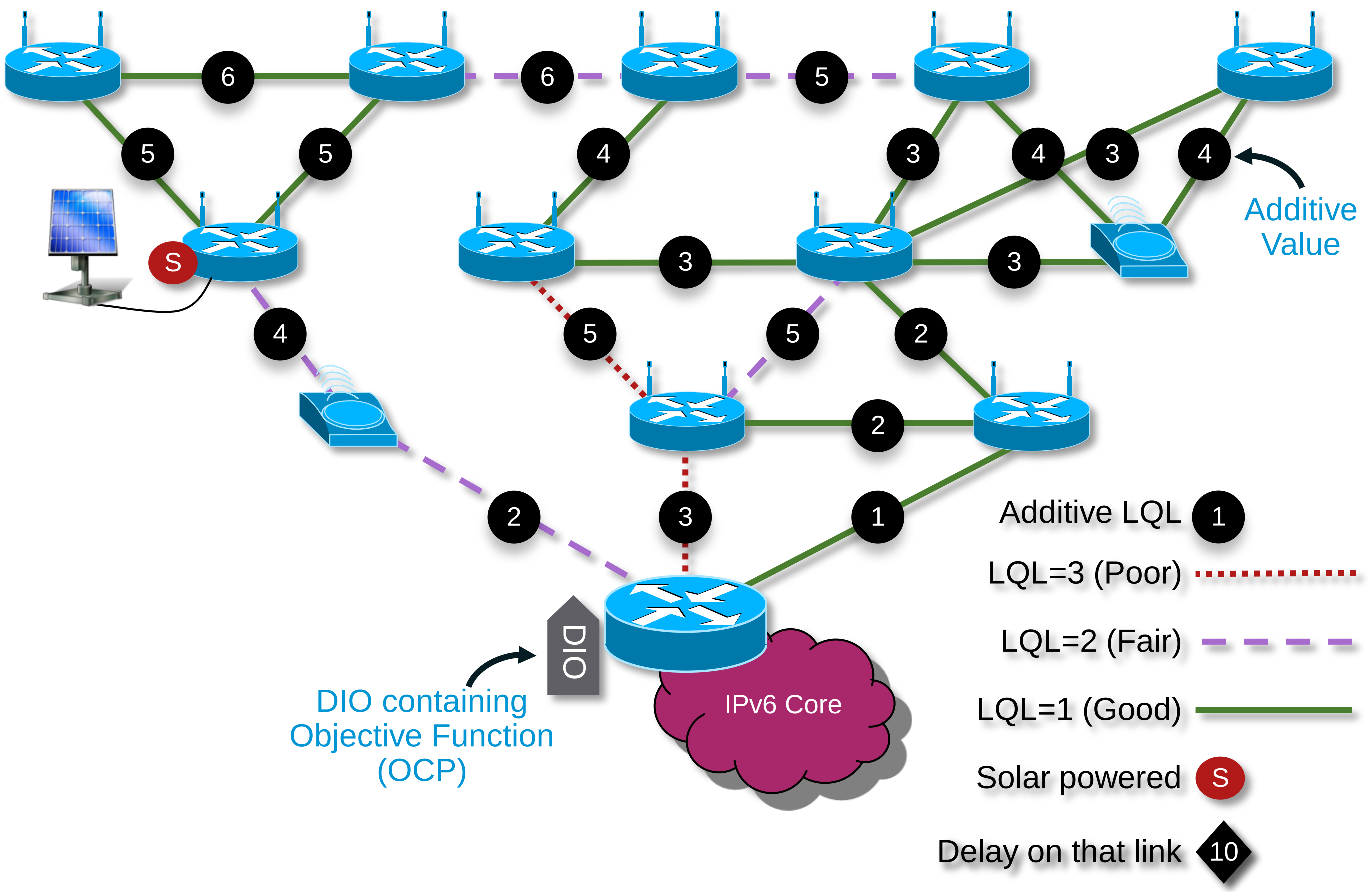


- DIO messages are propagated from the DODAG root
- Can carry OCP, metrics (recorded or aggregated), constraints

Objective Function Ex #1 - Candidate Neighbours

Avoid solar powered nodes and use the best available links (additive) to get to the DODAG root

DODAG Topology



Objective Function

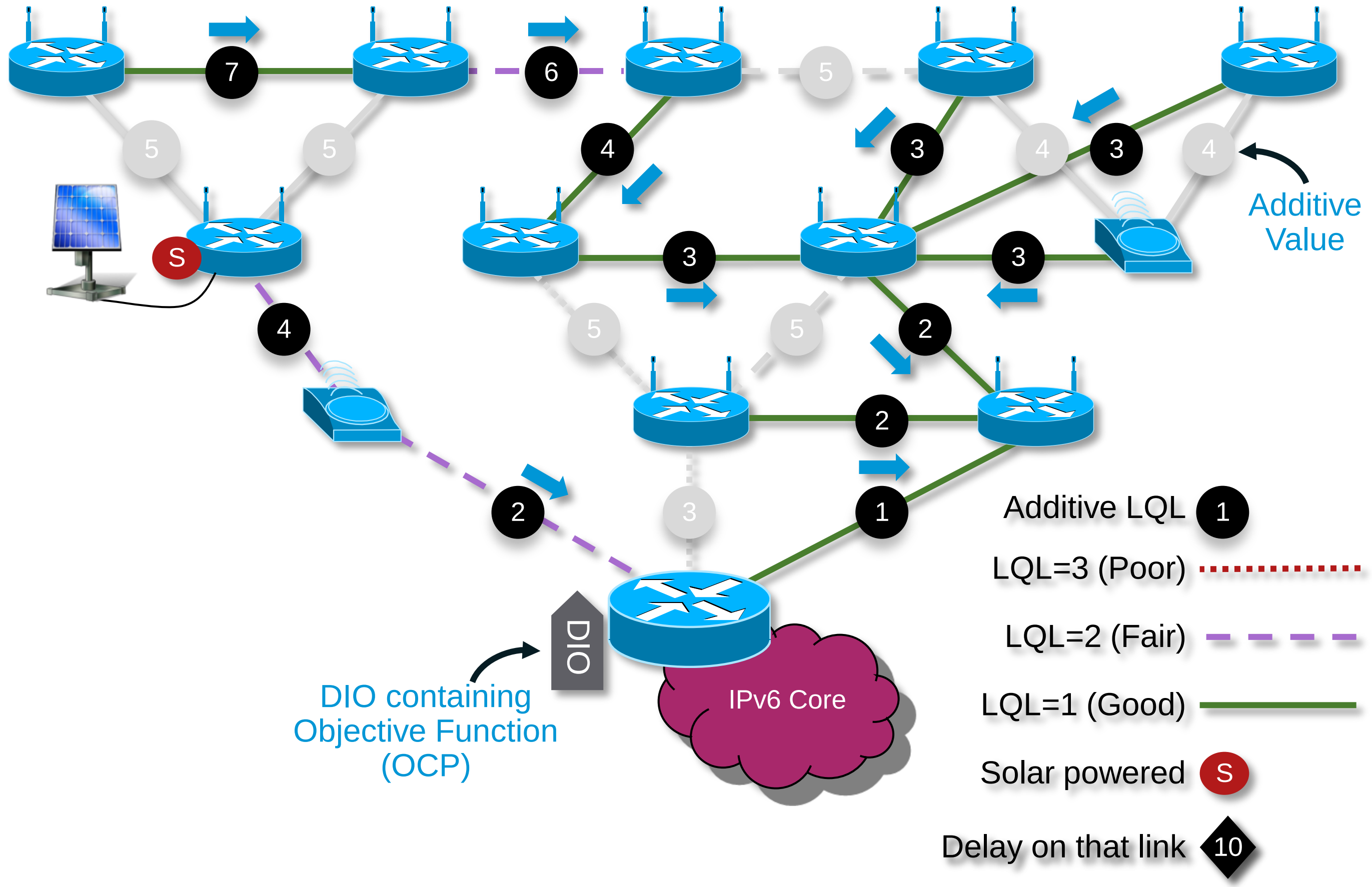
Object	Constraint	Advertised
Node Energy	Exclude Scavenger	As per OCP
Link Quality	Best Available (additive)	As per OCP
Hop Count	Maximum 20	Explicitly configured on DODAG root

- LQL metric advertised as additive
- Nodes choose links with lower LQL total

Objective Function Ex #1 - Preferred Parents

Avoid solar powered nodes and use the best available links (additive) to get to the DODAG root

DODAG Topology



Objective Function

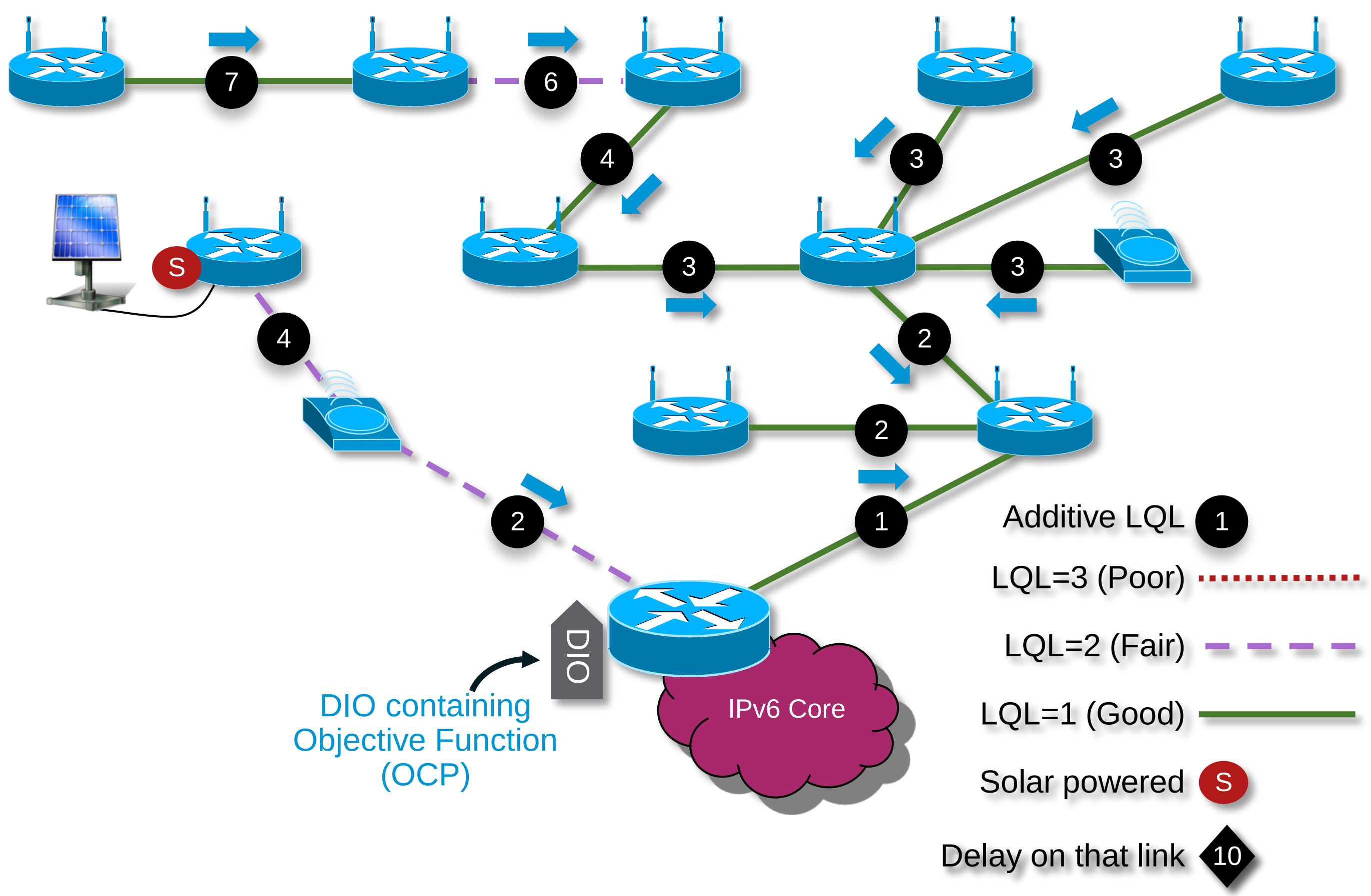
Object	Constraint	Advertised
Node Energy	Exclude Scavenger	As per OCP
Link Quality	Best Available (additive)	As per OCP
Hop Count	Maximum 20	Explicitly configured on DODAG root

- LQL metric advertised as additive
- Nodes choose links with lower LQL total

Objective Function Ex #1 - Resulting DODAG

Avoid solar powered nodes and use the best available links (additive) to get to the DODAG root

DODAG Topology



Objective Function

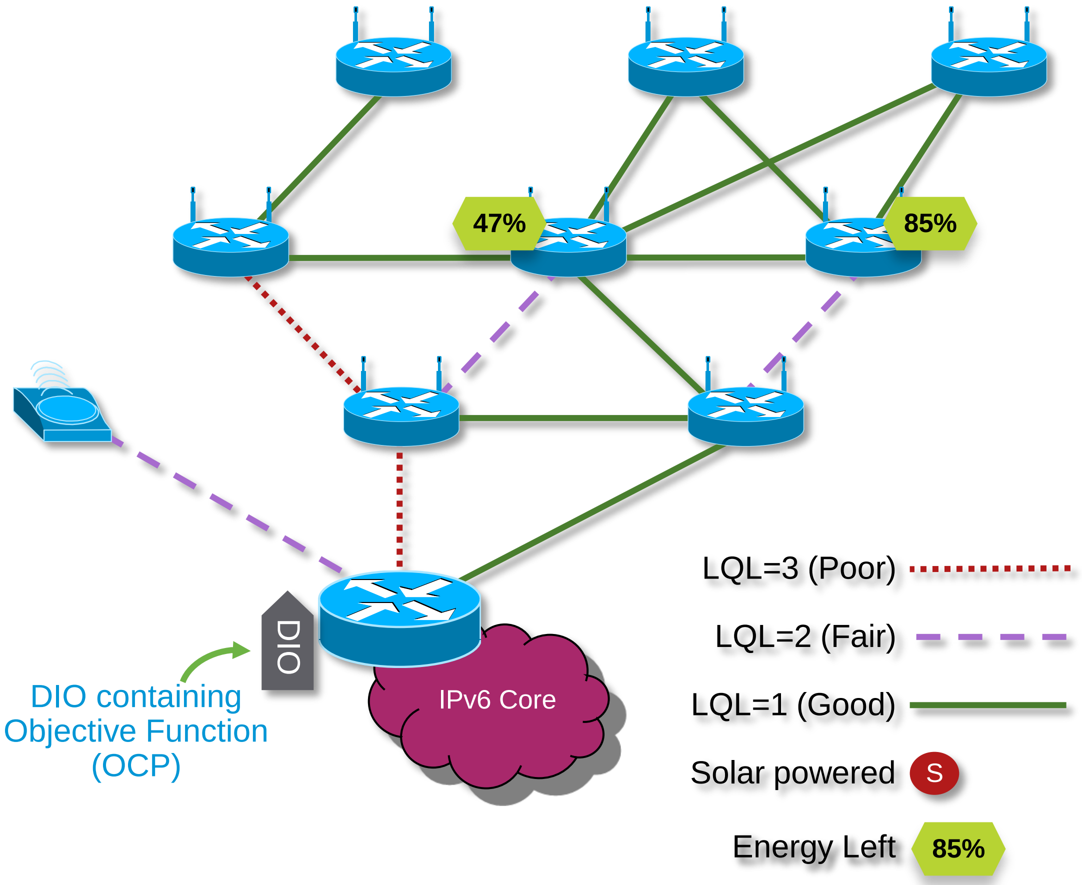
Object	Constraint	Advertised
Node Energy	Exclude Scavenger	As per OCP
Link Quality	Best Available (additive)	As per OCP
Hop Count	Maximum 20	Explicitly configured on DODAG root

- LQL metric advertised as additive
- Nodes choose links with lower LQL total

Objective Function Ex #2 - Candidate Neighbours

Use shortest number of hops and avoid low energy nodes

DODAG Topology



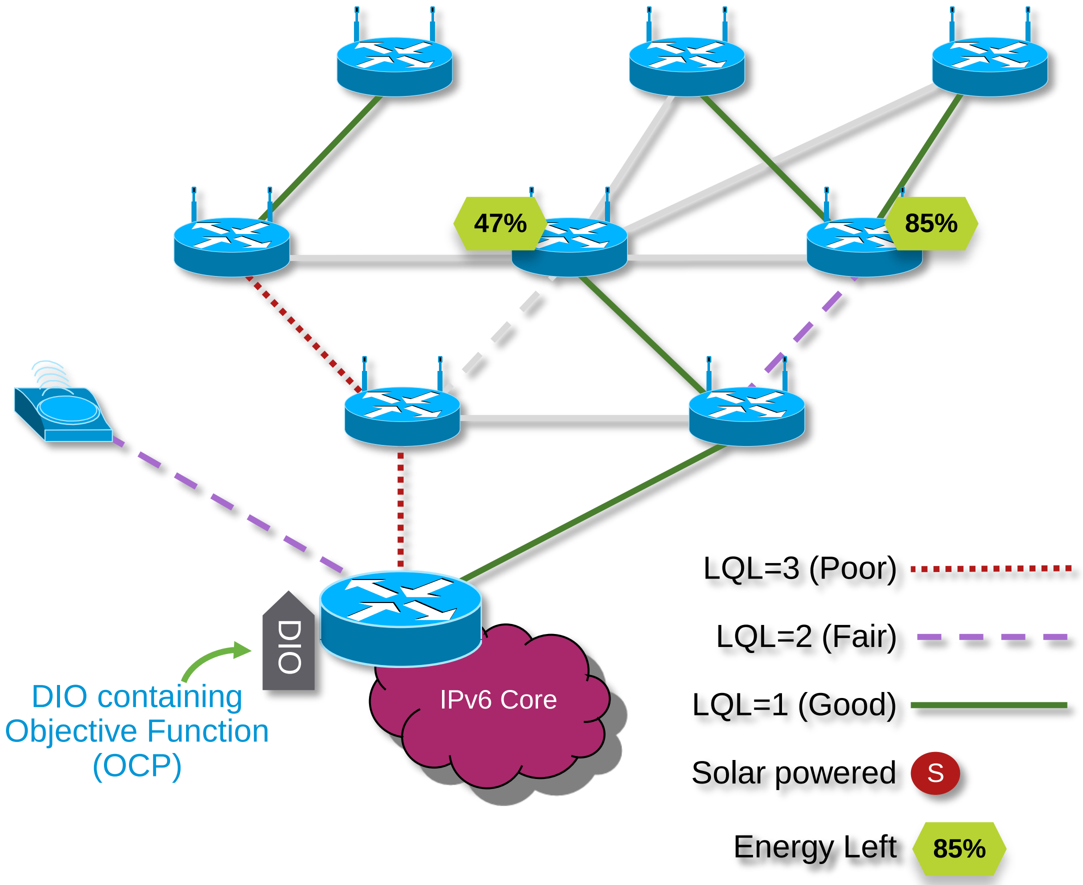
Objective Function

Object	Constraint	Advertised
Hops	Minimum Hops	As per OCP
Energy	Avoids nodes in path with < 50% energy	As configured on DODAG root

Objective Function Ex #2 - Preferred Parents

Use shortest number of hops and avoid low energy nodes

DODAG Topology



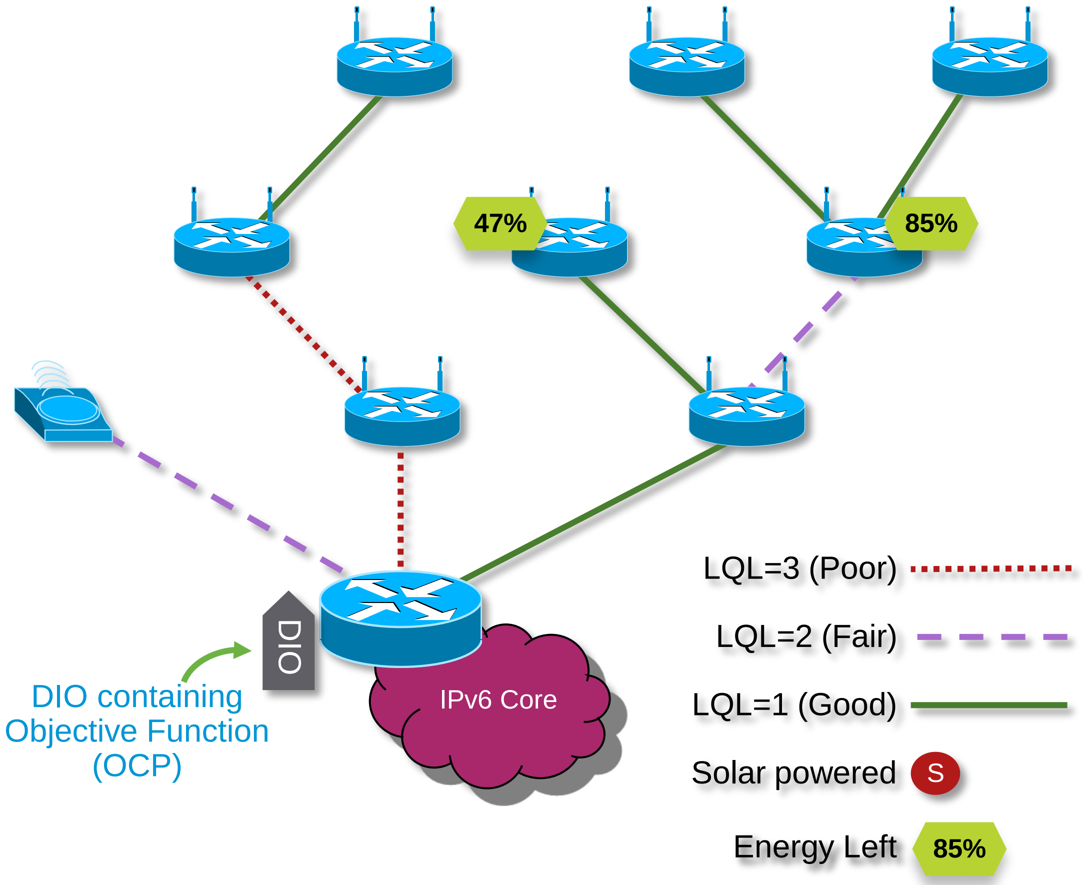
Objective Function

Object	Constraint	Advertised
Hops	Minimum Hops	As per OCP
Energy	Avoids nodes in path with < 50% energy	As configured on DODAG root

Objective Function Example #2 - Resulting DODAG

Use shortest number of hops and avoid low energy nodes

DODAG Topology



Objective Function

Object	Constraint	Advertised
Hops	Minimum Hops	As per OCP
Energy	Avoids nodes in path with < 50% energy	As configured on DODAG root

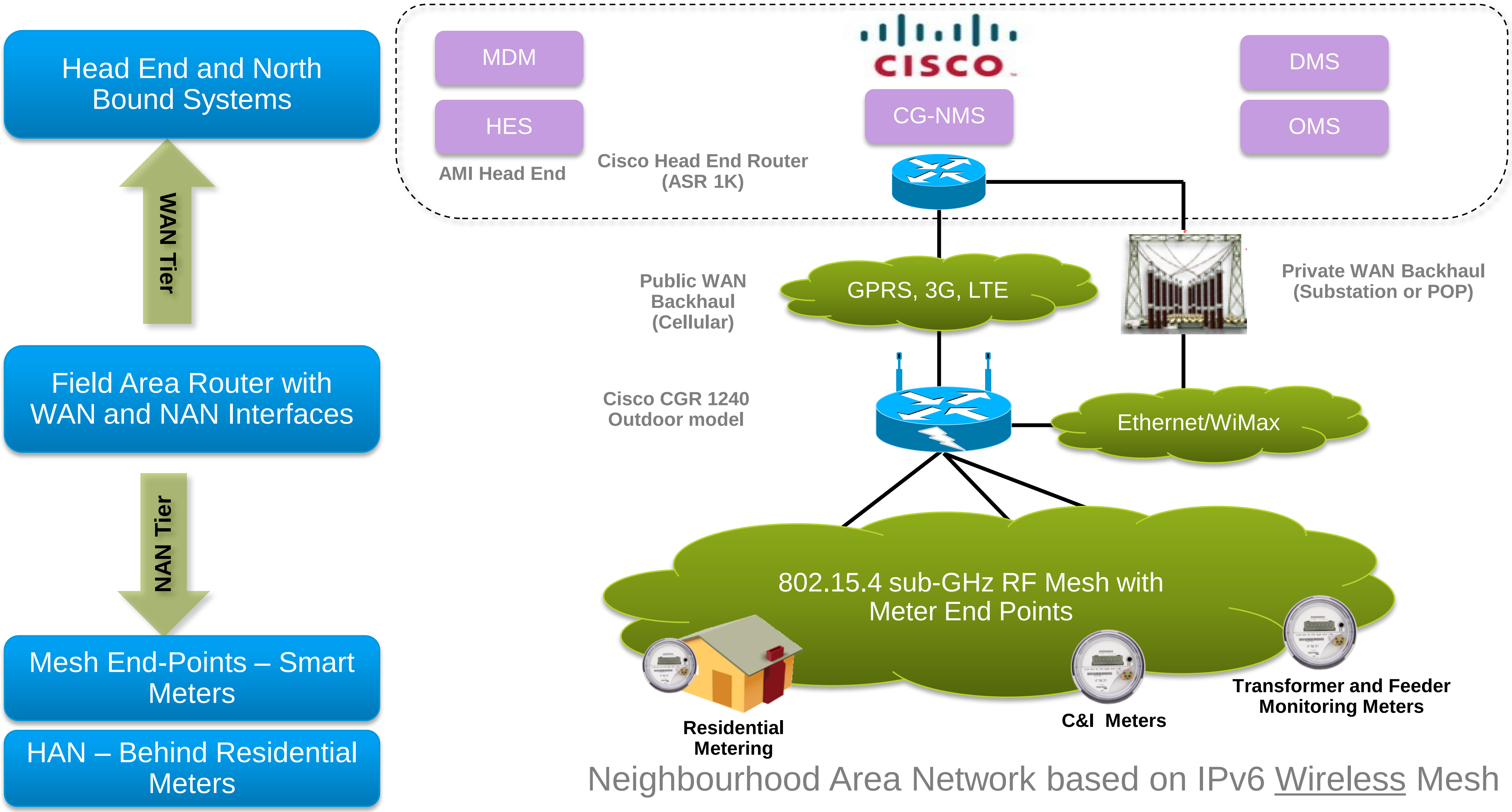
RPL Summary

- RPL is a foundation protocol of the Internet of Things
  - Open standard to meeting challenging requirements
- Promising technology to enable IP on many billions of smart objects
- Very compact code
  - Supports wide range of media and devices
- Cisco Implementation
  - Incorporated into Cisco Grid Blocks Architecture
  - Available on Cisco CGR1000 series routers (indoor and poletop outdoor)

RPL Use Case

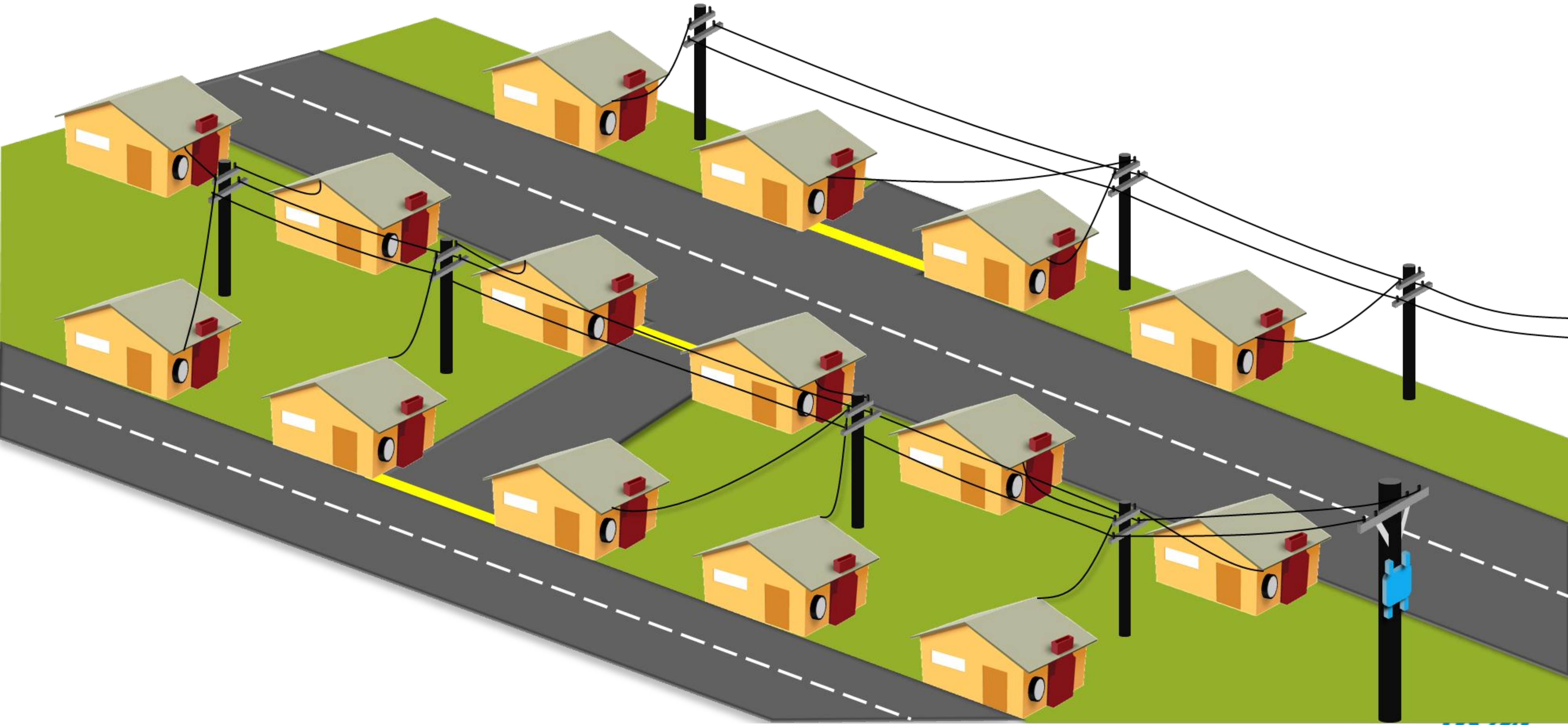
802.15.4g RF Mesh
Advanced Metering Infrastructure (AMI)

AMI IEEE 802.15.4g RF Mesh Architecture

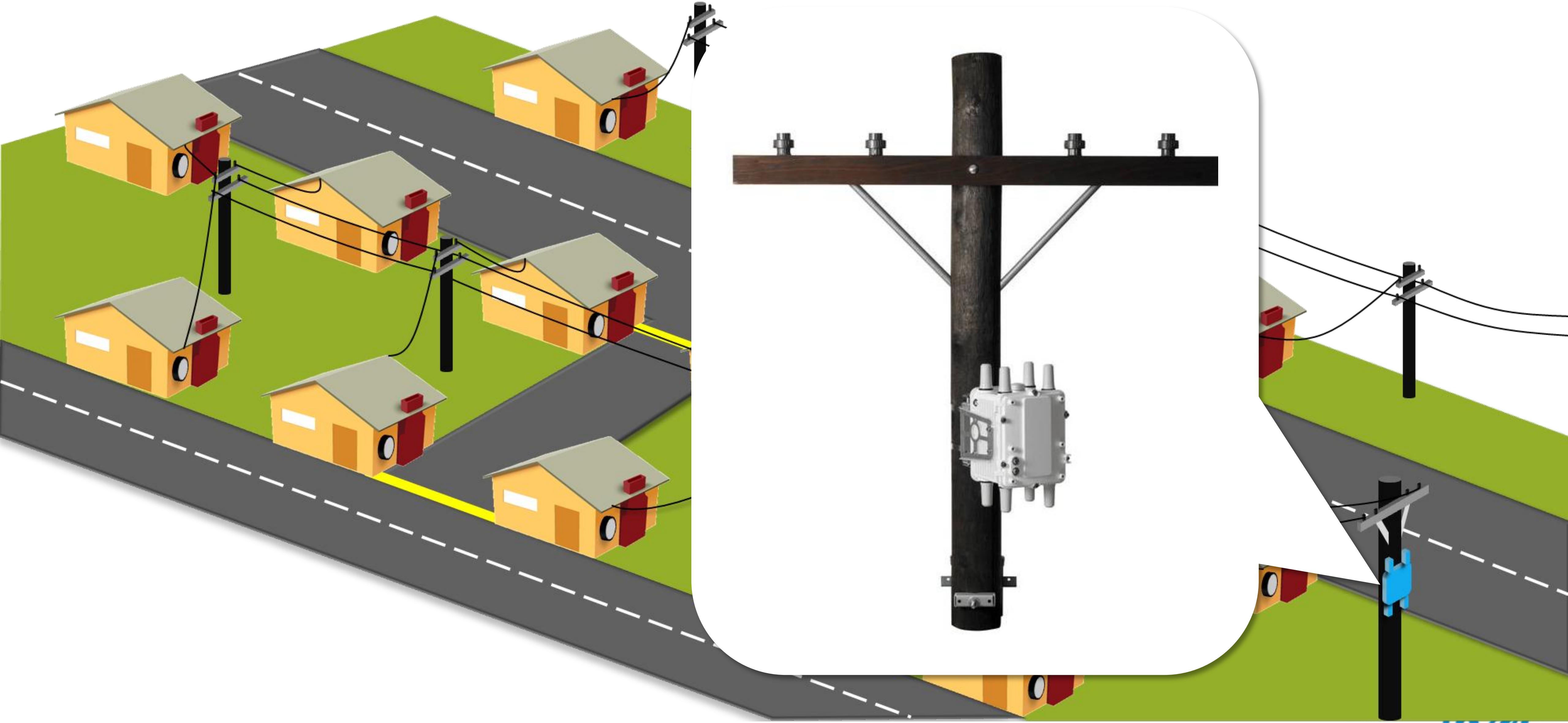


Neighbourhood Area Network based on IPv6 Wireless Mesh

AMI NAN Urban Environment



DODAG Root - Cisco CGR 1240 (Field Area Router)



DODAG Root - Cisco CGR 1240 (Field Area Router)

IEEE 802.15.4g (902-928 Mhz)
IETF 6LowPan, IPv6, RPL
IEEE802.1ar device identity

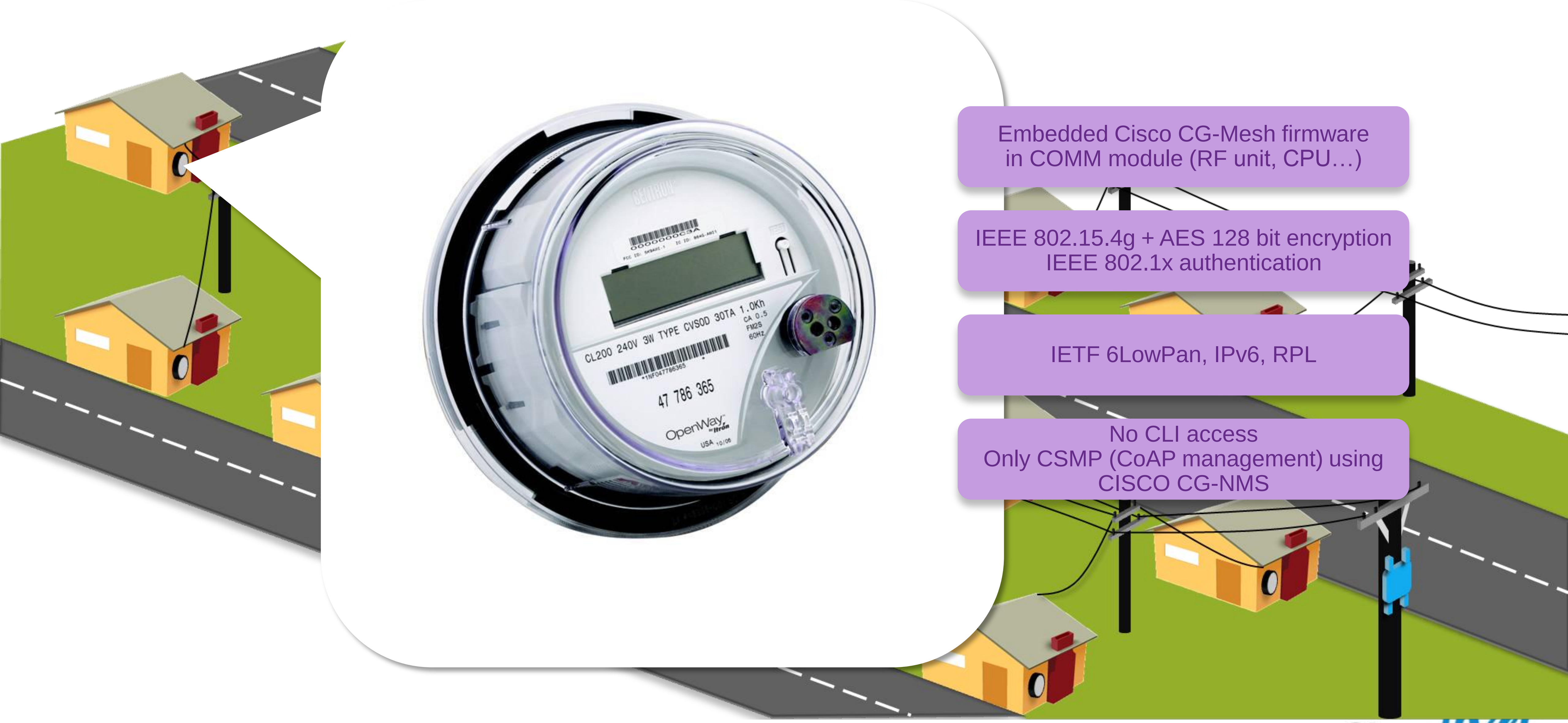
3G GSM HSPA+, 3G CDMA 1xEV-DO
IEEE 802.16e (WiMAX)

WiFi, GigEthernet , FastEthernet
GPS

CGR1000 supports up to 5000 RPL nodes
(Currently tested with over 3600)

Outdoor/Pole Top version
CGR 1120 is the indoor version

ITRON Smart Meter with Cisco Firmware



Embedded Cisco CG-Mesh firmware
in COMM module (RF unit, CPU…)

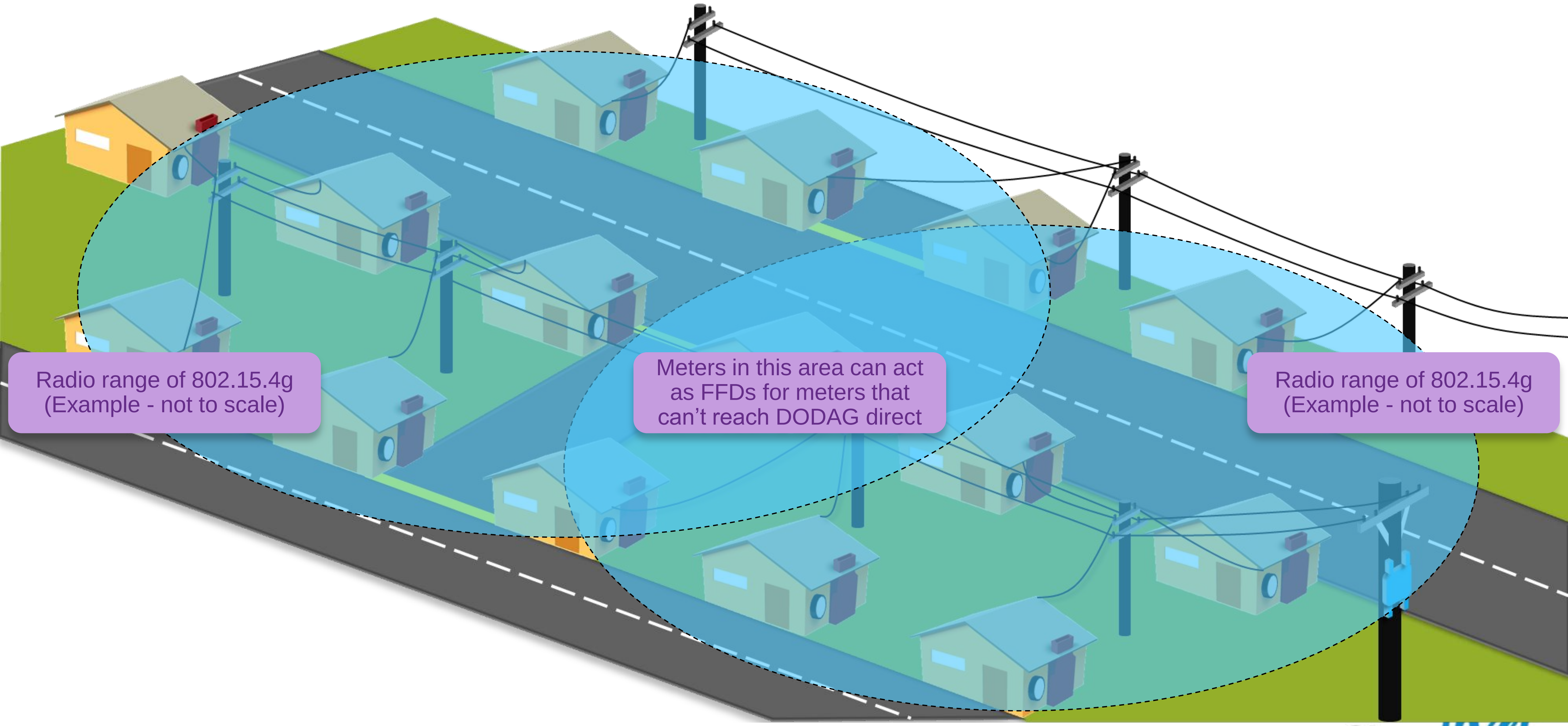
IEEE 802.15.4g + AES 128 bit encryption
IEEE 802.1x authentication

IETF 6LowPan, IPv6, RPL

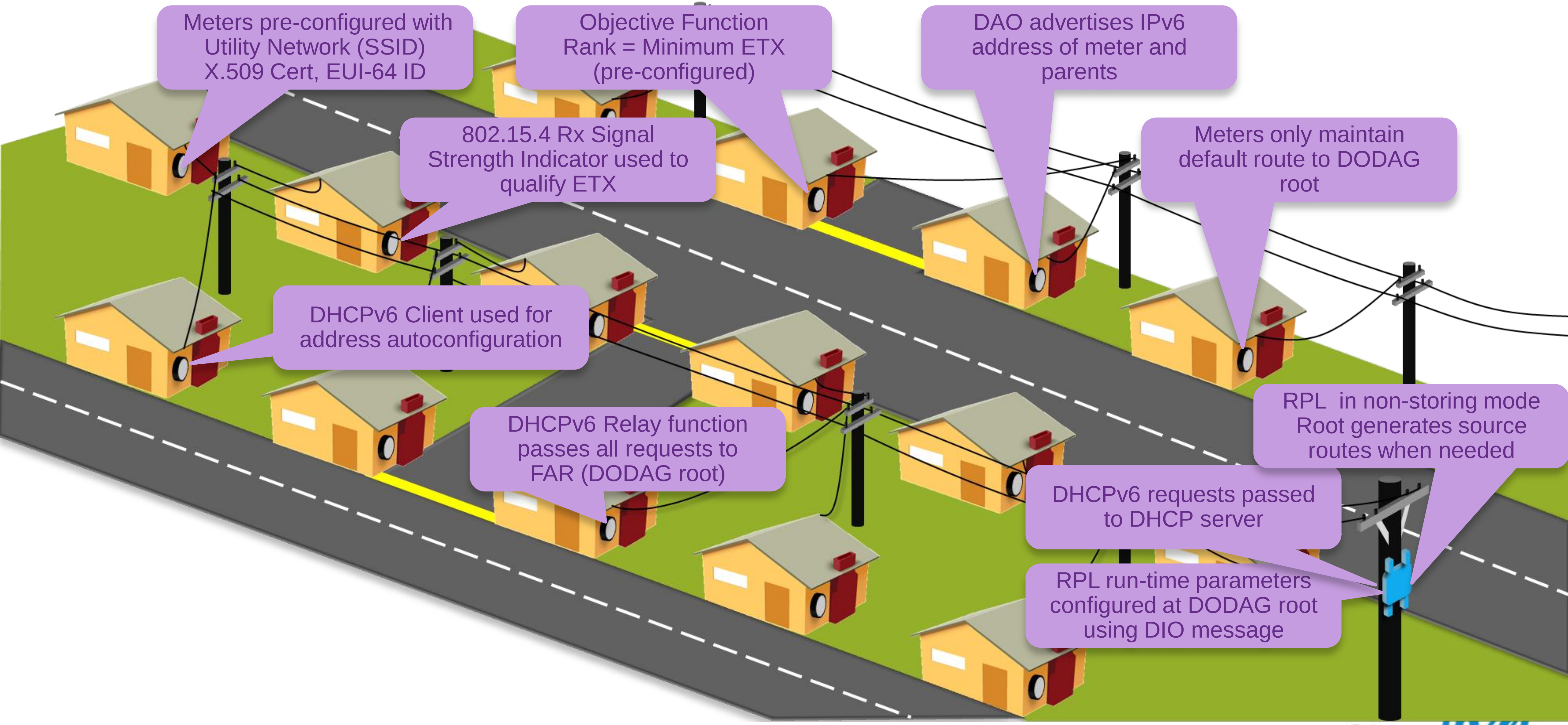
No CLI access
Only CSMP (CoAP management) using
CISCO CG-NMS

ITRON Dual Antenna

Smart Meters Can Be Used As Forwarders

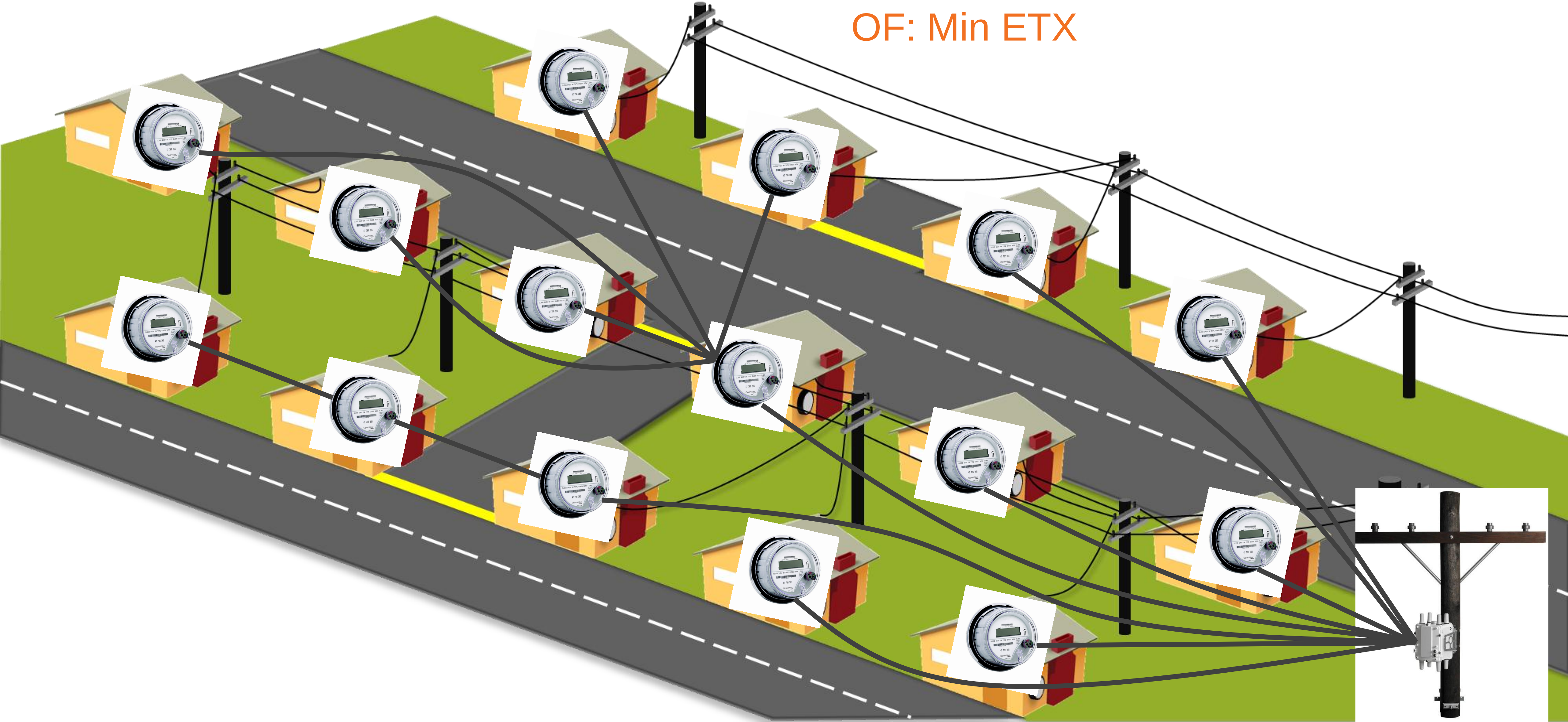


RPL Implementation

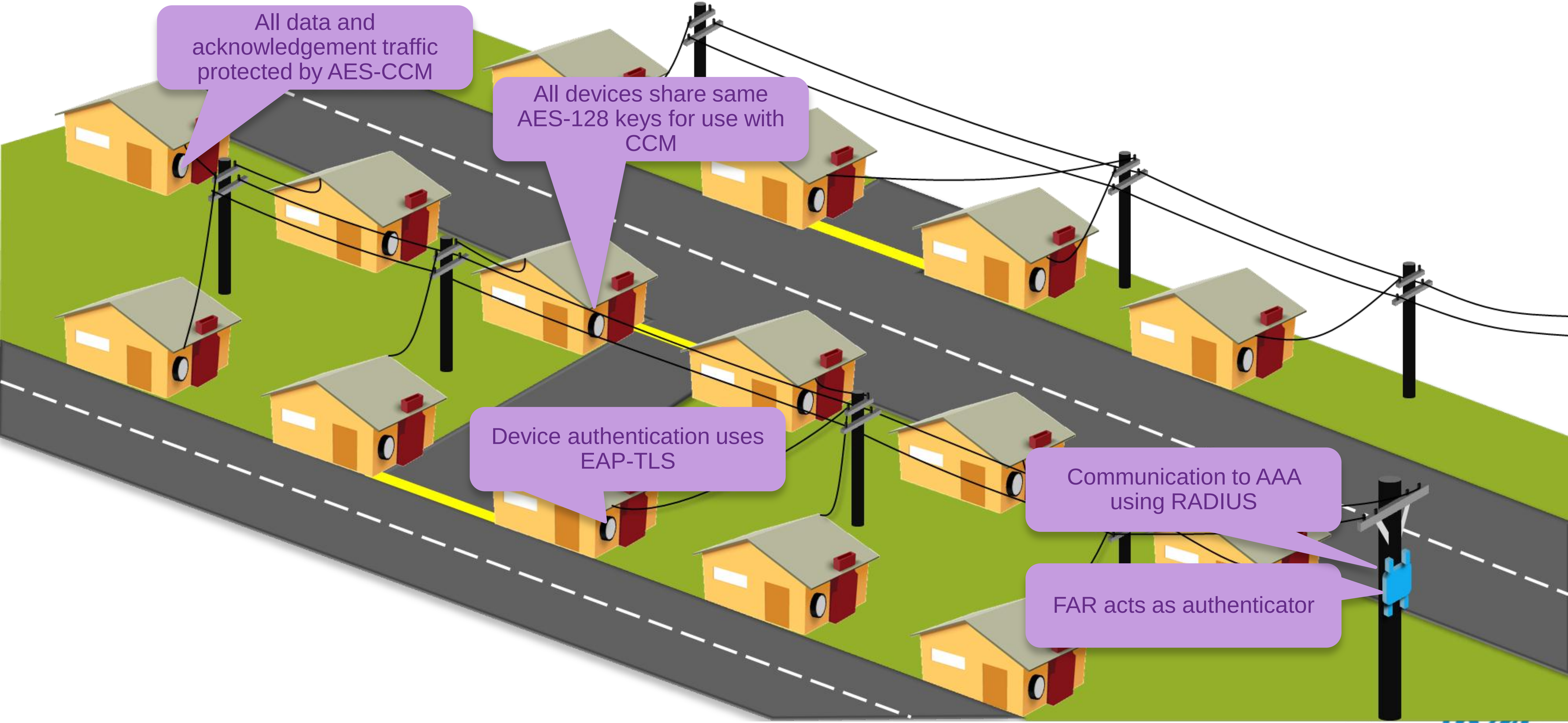


Possible Resulting DODAG Topology

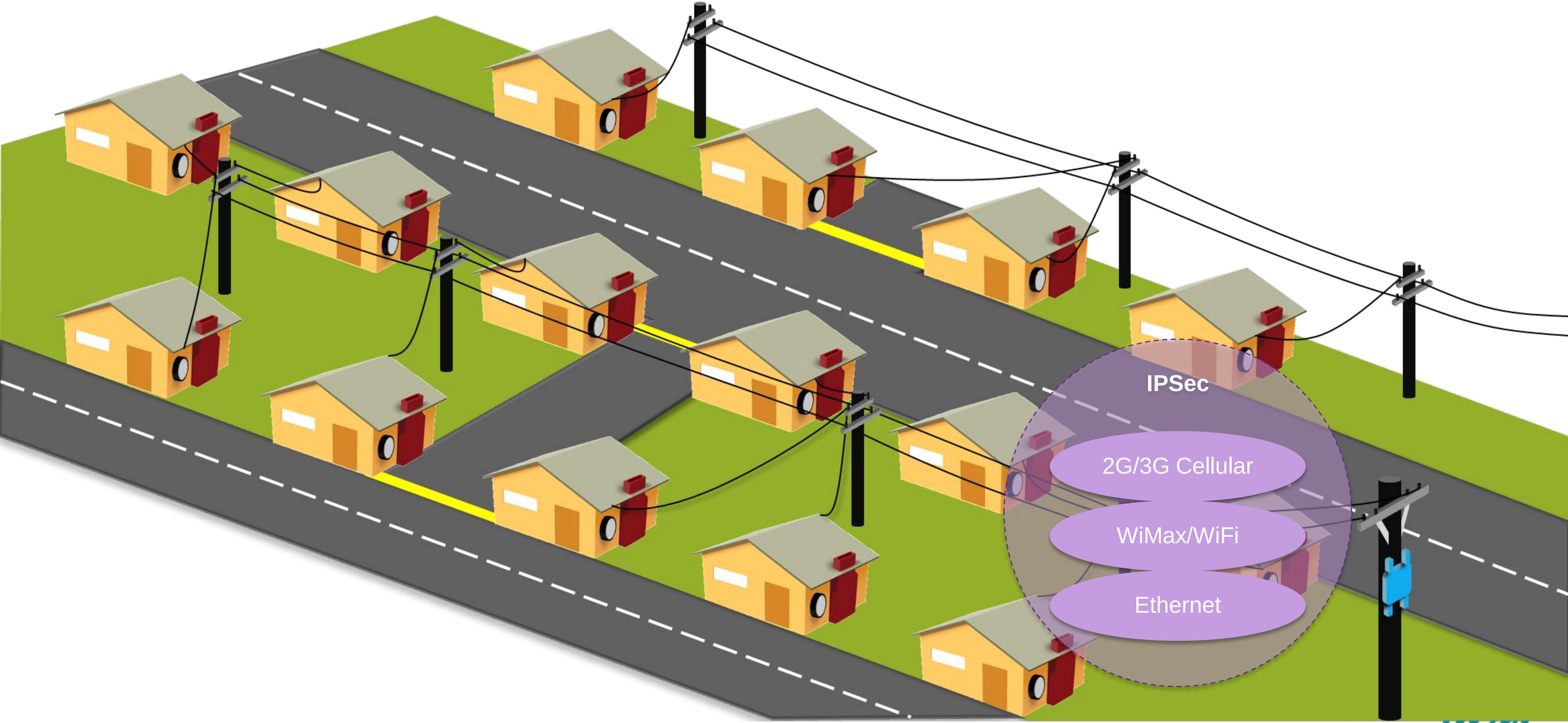
OF: Min ETX



Authentication and Security



WAN Backhaul from Field Area Router



RPL Configuration at DODAG Root

```
interface Ethernet2/3 !Interface to WAN side
  ipv6 address 2001:420:7bf:5f::99/64
  ipv6 dhcp relay destination 2001:420:7bf:5f::100! Upstream towards DHCP server
!
interface Wpan4/1 !Interface to Wireless Mesh (NAN)
  ipv6 address 2001:dead:beef:6104::/64
  rpl prefix 2001:dead:beef:6104::/64      !IP Subnet of RPL network
  panid 4660                               !802.15.4 PAN Co-ordinator ID
  ssid enercon_nan                         !Utility network name
  txpower -21
  ipv6 dhcp relay client-interface         ! Downstream towards meters in NAN
```

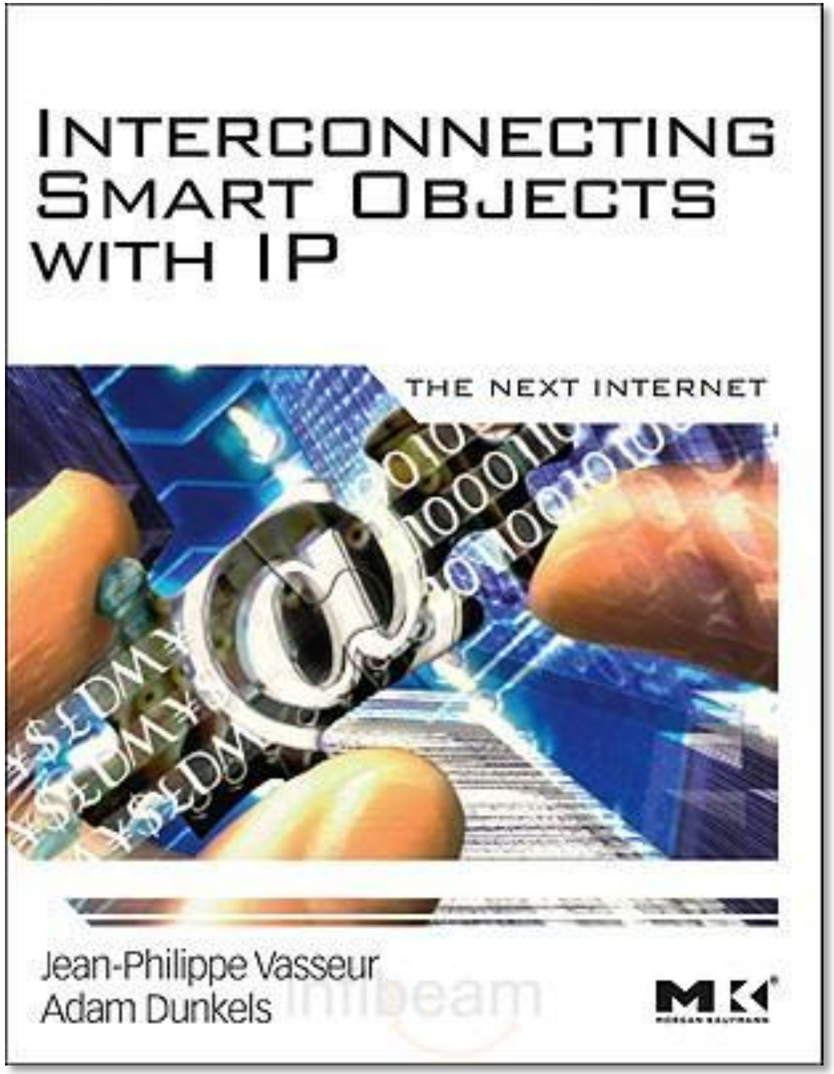
Meter Configuration via CG-NMS (Map View)

Conclusion

Conclusion

- Several major applications for RPL
  - Smart Grid, Green, Industrial, Connected building/homes, Smart Cities
  - There is a lot of momentum around using IP
- Major progress in several key areas
  - IP-based technologies: 6Lowpan, RPL, CoRE, CoAP, LWIG
  - IPSO alliance, ETSI
  - Adoption of IP by several other SDOs/alliance: Zigbee/IP for SE2.0, Bacnet, ….
  - RPL an important component of Cisco GridBlock Architecture
- Internet of Everythins is coming
  - Current Internet = Some things
  - Next Internet = Everything!

Recommended Reading



- Covers the trends in Smart Objects
- RPL protocol
- Detailed application scenarios
- Written by
  – JP Vasseur (Cisco Fellow)
  – Adam Dunkels (Inventor of Contiki O/S, uIPv6)

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww