15–25.FEB.2011 | HONGKONG
Main_Conference::21–25.FEB.2011
Workshops@Cyberport::15–19.FEB.2011

WWW.APRICOT-APAN.ASIA

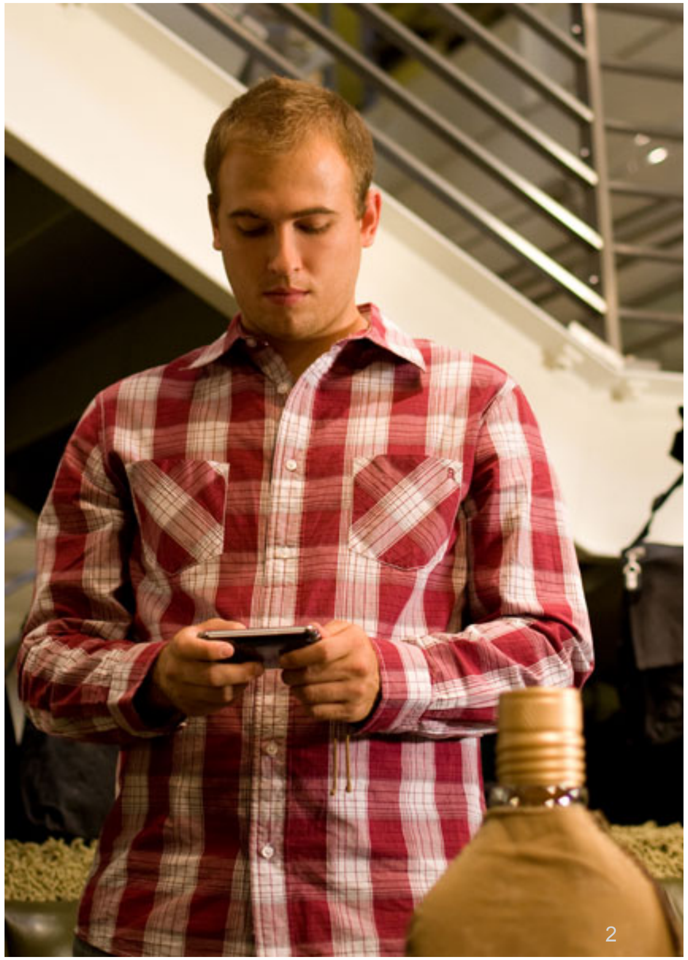
IP in Smart Object Networks

Jeff Apcar, Distinguished Services Engineer, Cisco Systems

With acknowledgement to JP Vasseur Cisco Distinguished Engineer, Co-Chair IETF Roll Working Group, TAB Chair IPSO Alliance

Agenda

- A world of sensors
- Smart Objects
- Low Power Lossy Networks (LLN)
- 802.15.4 Low Power PAN
- Using IP for Smart Objects
- 6LoWPAN Working Group
- Roll Working Group
- Routing over Low Power Lossy Networks (RPL)
- Conclusion

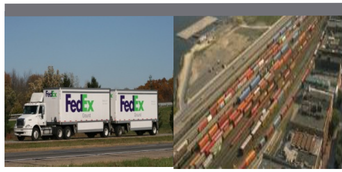


A World of Sensors

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

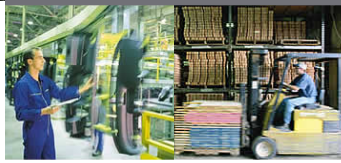
Predictive Maintenance

Energy Saving Smart Grid

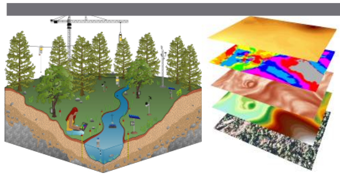


High-Confidence Transport and Asset Tracking

Intelligent Buildings



Improve Productivity



Enable New Knowledge

Enhanced Safety & Security

Improve Food and H^2O

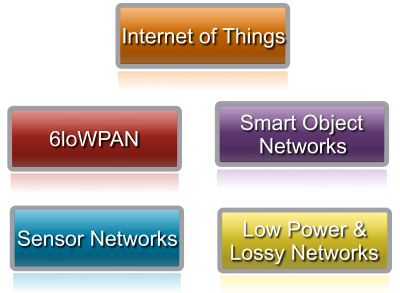
Healthcare

Smart Home S+CC

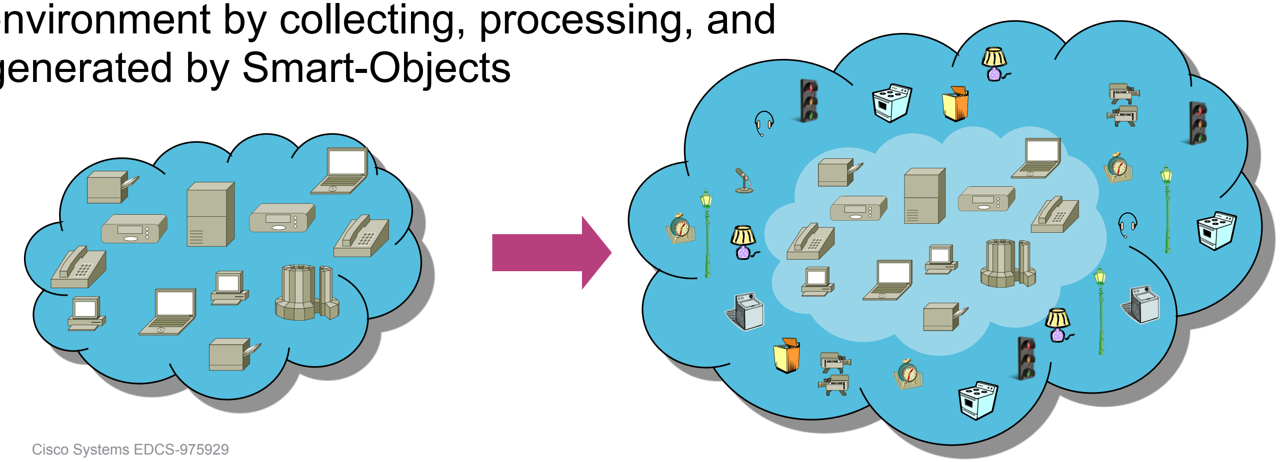
A World of Proprietary Protocols

- Many legacy networks use closed and 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 (poorly) 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, VINES
  - Interconnected using multiprotocol gateways

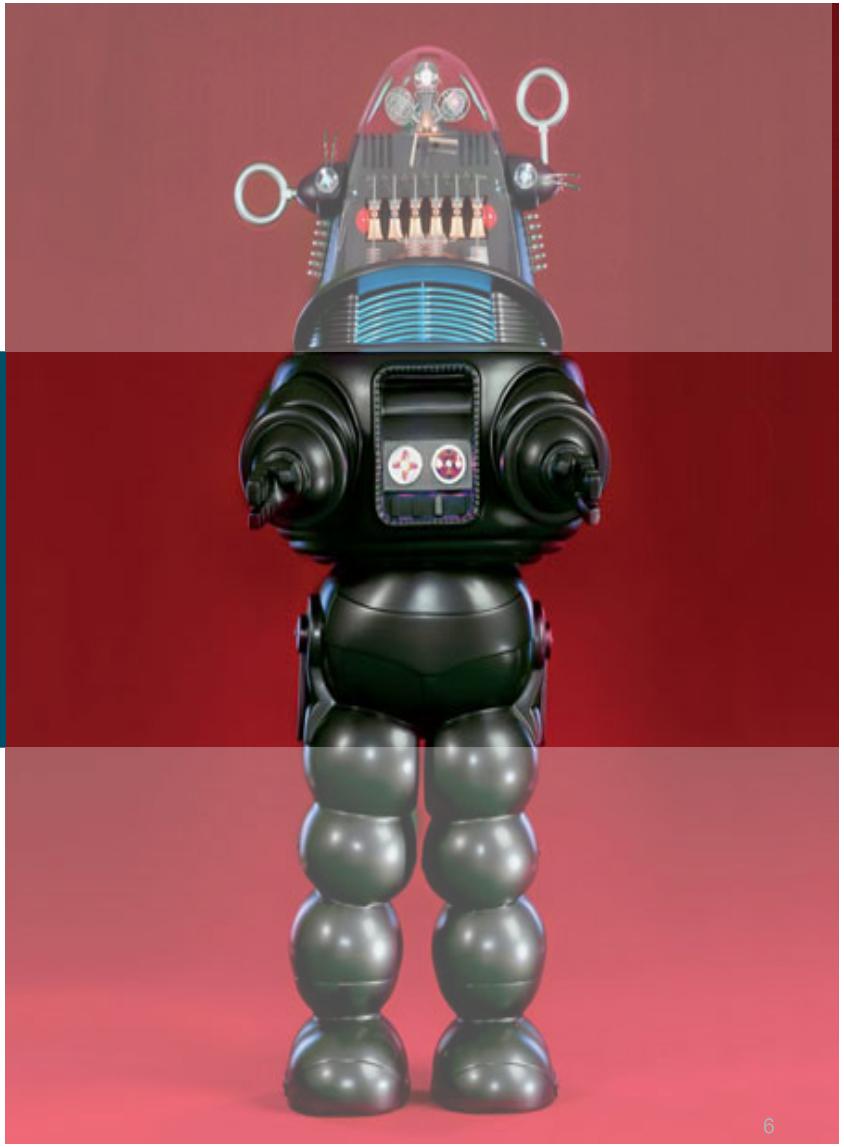
Standardise to Build The Internet of Things



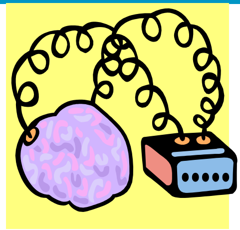
- Next iteration of the Internet
  - Standardise IP into sensors and other smart objects
  - Any object or environmental condition can be monitored
  - Expand the current Internet to virtually anything and everything
- Internet of Things (IoT)
  - Pervasive and ubiquitous network which enables monitoring and control of physical environment by collecting, processing, and analyzing the data generated by Smart-Objects



Smart Objects



What is a Smart Object?



- A tiny and low cost computer 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 is embedded into objects (to make them smart ☺)
  - For example, thermometers, car engines, light switches, gas 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
  - Predominantly IEEE 802.15.4 (2.4 GHz *and* 900 MHz)
  - Newer RF technologies IEEE 802.15.4g (Smart Utility Network PHY)

Low Power Lossy Networks

What is a Low Power Lossy Network (LLN)?

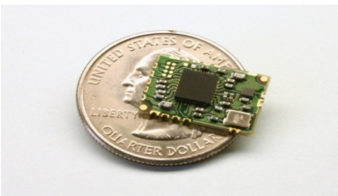
- LLNs comprise a large number of highly constrained devices (smart objects) interconnected by predominantly wireless links of unpredictable quality
- LLNs cover a wide scope of applications

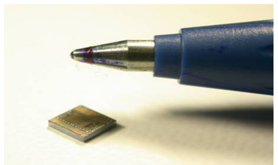
  Industrial Monitoring, Building Automation, Connected Home, Healthcare, Environmental Monitoring, Urban Sensor Networks, Energy Management, Asset Tracking, Refrigeration

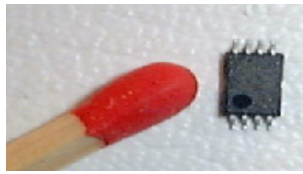
- Several IETF working groups and Industry Alliance addressing LLNs

  IETF - CoRE, 6Lowpan, ROLL

  Alliances - IP for Smart Objects Alliance (IPSO)





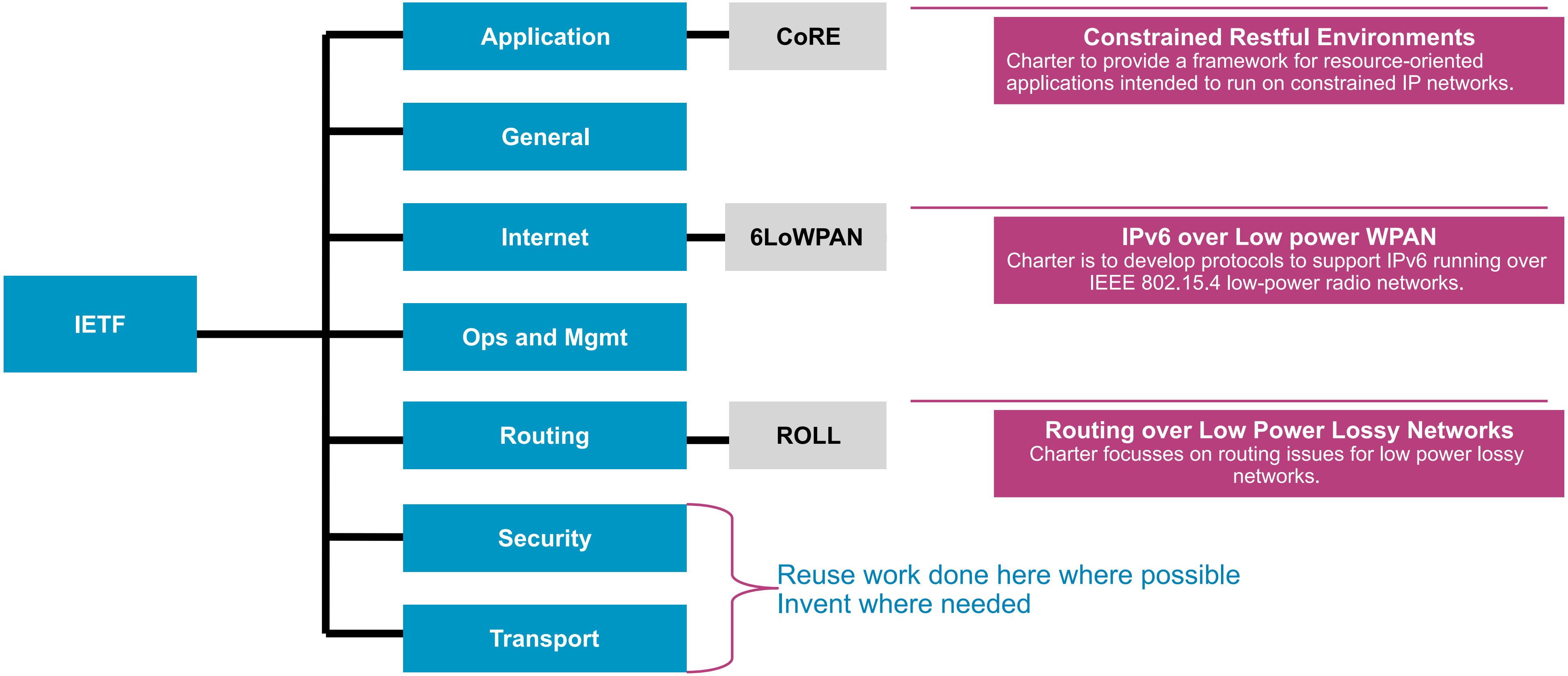


World's smallest web server

Characteristics of LLNs

- LLNs operate with a hard, very small bound on state
- In most cases LLNs optimised for saving energy
- 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 in the air hence the small frame size
  - 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 2010 More than 65 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 parties
- Coordinate and combine member marketing efforts
- Support and organise interoperability events
  - COMPLIANCE program (Based on IPv6 forum)
- http://www.ipso-alliance.org

IEEE 802.15.4 PAN

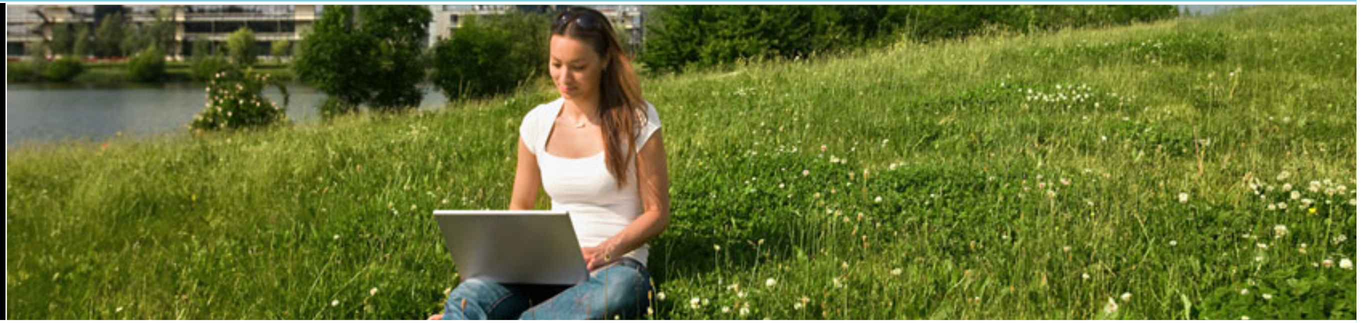
IEEE Wireless Standards

- 802.11 – Wireless Local Area Networks (WiFi)
  802.11a, 802.11b, 80211g, 802.11n
- 802.15 – Wireless Personal Access Networks (WPAN)
  Task Group 1 – Bluetooth (802.15.1)
  Task Group 2 – Co-existence (802.15.2)
  Task Group 3 – High Rate WPAN (802.15.3)
  Task Group 4 – Low Rate WPAN (802.15.4 or 802.15 TG4) } Used in LLNs
  Task Group 5 – Mesh Networking (802.15.5)
- 802.16 – Wireless Metropolitan Area Networks (WiMax)
- 802.20 – Mobile Broadband Wireless Access (Mobile-Fi) - Defunct
- 802.22 – Wireless Regional Access Network (WRAN)
  Utilise free space in the allocated TV spectrum

"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

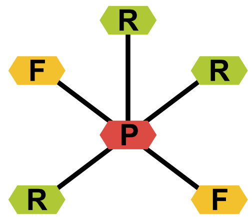
IEEE 802.15 WPAN™ Task Group 4 (TG4) Charter



IEEE 802.15.4 Features

- Designed for low bandwidth, low transmit power, small frame size
  - More limited than other WPAN technologies such as Bluetooth
  - Low bit rate and packet size to ensure reasonably low packet error rates
  - Packet size (127 bytes) reflects minimal buffering capabilities in Smart Objects
  - Low power allows batteries to last for years
- Data rates of 250 kbps, 40 kbps, and 20 kbps
- Two addressing modes; 16-bit short (local allocation) and 64-bit IEEE (global allocation)
- Communicates over multiple hops
  - Range is in tens of metres, reduces transmission power
- 3 possible unlicensed frequency bands
  - (Europe 868-868.8 MHz – 3 chans , USA 902-928 MHz – 30 chans, World 2400-2483.5 MHz – 16 chans)

IEEE 802.15.4 Node Types

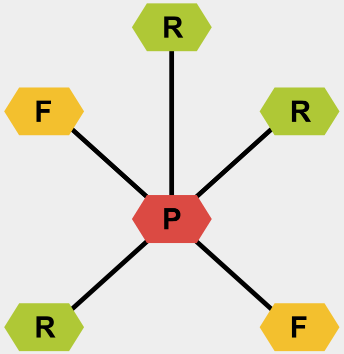


- Full Function Device (FFD)
  - Can operate as a PAN co-ordinator (allocates local addresses, gateway to other PANs)
  - Can communicate with any other device (FFD or RFD)
  - Ability to relay messages (PAN co-ordinator)
- Reduced Function Device (RFD)
  - Very simple device, modest resource requirements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

IEEE 802.15.4 Topologies

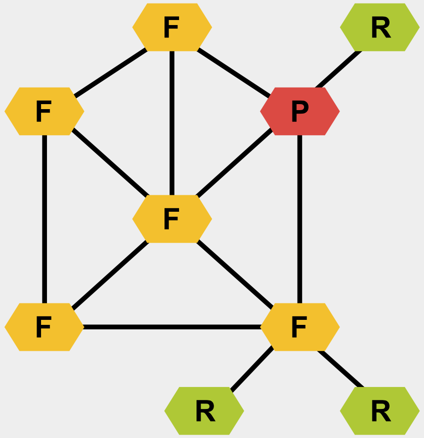
Operates at Layer 2

Star Topology



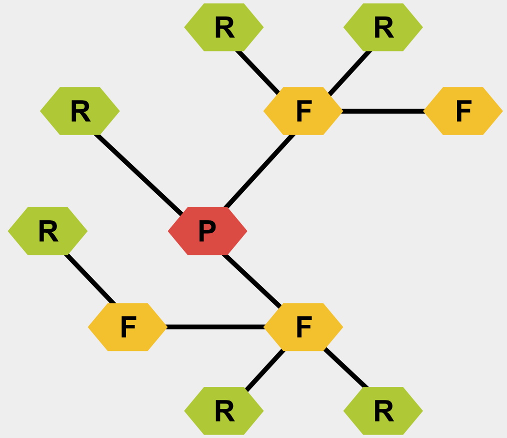
- All devices communicate to PAN co-ordinator which uses mains power
- Other devices can be battery/scavenger

Mesh Topology



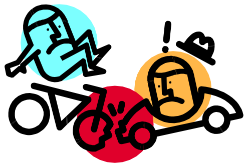
- Devices can communicate directly if within range

Cluster Tree



- Higher layer protocols like RPL may create their own topology that donot follow 802.15.4 topologies

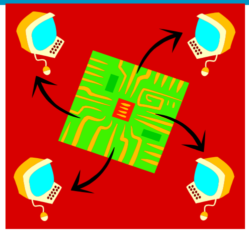
Single PAN co-ordinator exists for all topologies



802.15.4 uses CSMA-CA

- Carrier Sense Multiple Access with Collision Avoidance
- Wireless networks cannot detect collisions
  - Fundamental difference from wired networks
- Wired – CSMA/CD – Collision Detection
- Wireless – CSMA/CA – Collision Avoidance
  - RX/TX antennas immediately next to each other
  - Hence RX can only see its own TX when transmitting

Using IP for Smart Objects



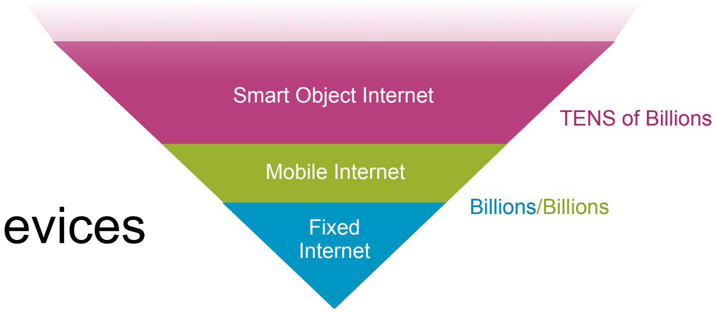
IP in Smart Object Networks

- 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
    - Email, WWW, VOIP, Video, Collaboration
- 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 applictions
  - Allows the creation of the "Internet of Things"

IP is both an Architecture & Protocol

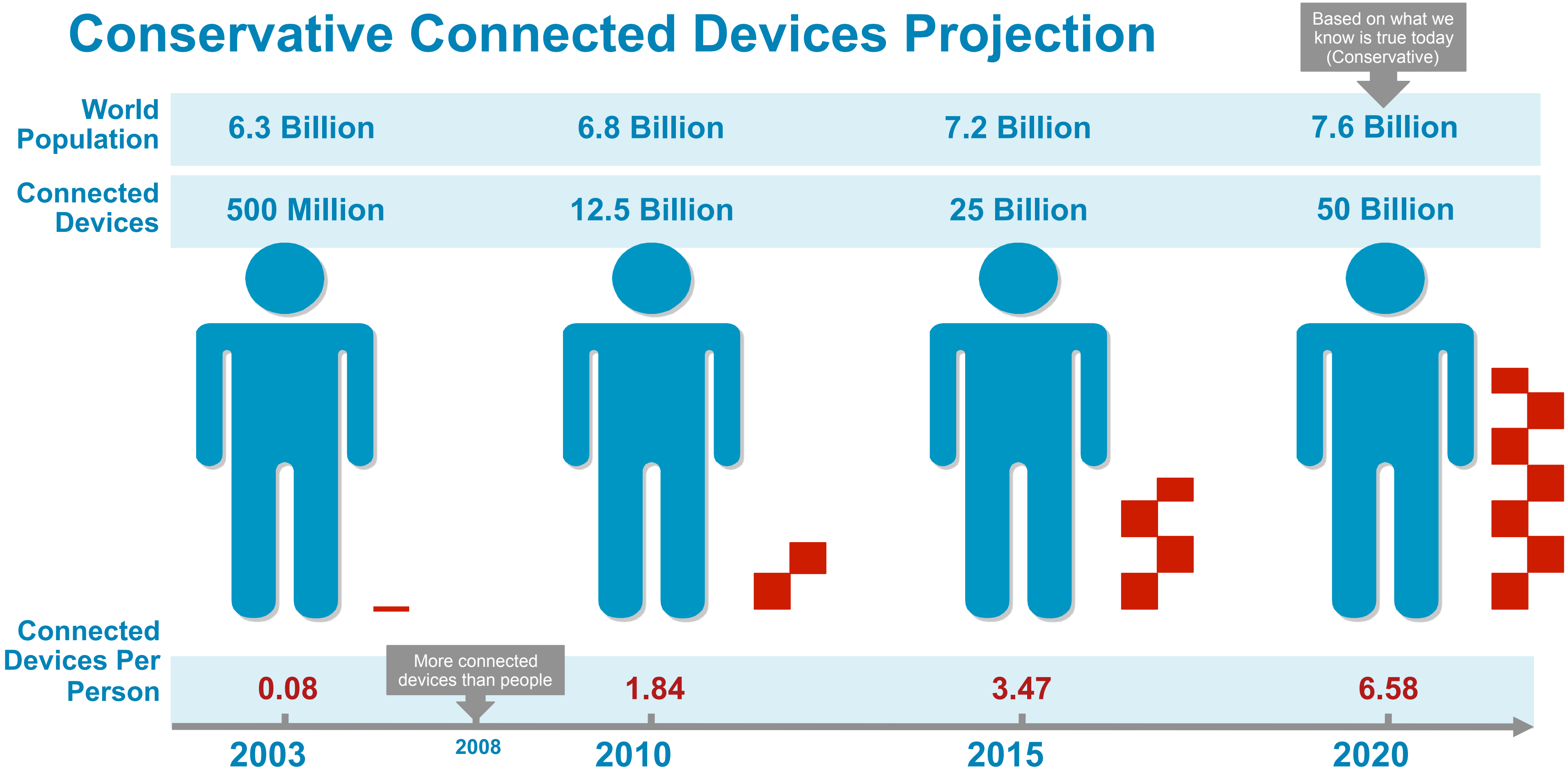
- It can meet all the requirements to support a Smart Object Network
- Based on open standards
  - IETF RFCs
- Flexibility in many dimensions
  - Support a wide range of media - Serial, SDH, Ethernet, DWDM, FR, ATM
  - Support a wide range of devices - From phones to routers
- Always favor global than local optimum
  - IP is capable of supporting many different applications; voice, video, data, mobile
- Secure
- Plug & Play
- Scalable
  - The Internet comprises billions of connected devices

IPv4 or IPv6



- The current Internet comprises several billion devices
  - Add to this growing 3G, 4G mobile devices
  - There is no scope for IPv4 to support Smart Object Networks
- 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)

Conservative Connected Devices Projection

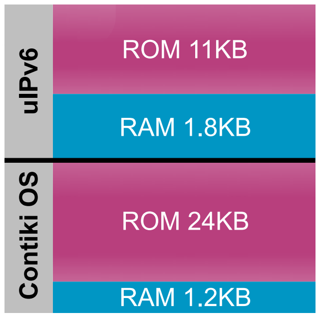


Source: Cisco IBSG, 2010

Contiki + uIPv6 Code for Smart Objects

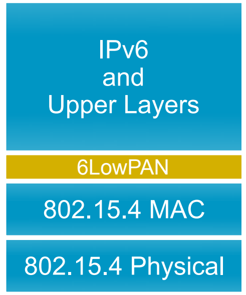
- Contiki is a memory efficient O/S for smart objects
  - Open source operating system for the Internet of Things
- uIPv6 is world’s small certified stack for objects such as actuators and sensors
  - uIPv6 does not require an O/S (such as Contiki)
  - Able to run over any link layer (for example, 802.15.4)
- All IPv6 features (except MLD) are implemented from RFC4294
- Obtained IPv6 ready phase 1 logo
- Open source release http://www.sics.se/contiki
- Memory requirements for IPv6/6LoWPAN/802.15.4
  - 35K ROM 3K RAM (minimal O/Sfeatures)
  - 40KB ROM 10KB RAM (full O/S features)

Minimal
Memory Requirements



6LoWPAN Working Group

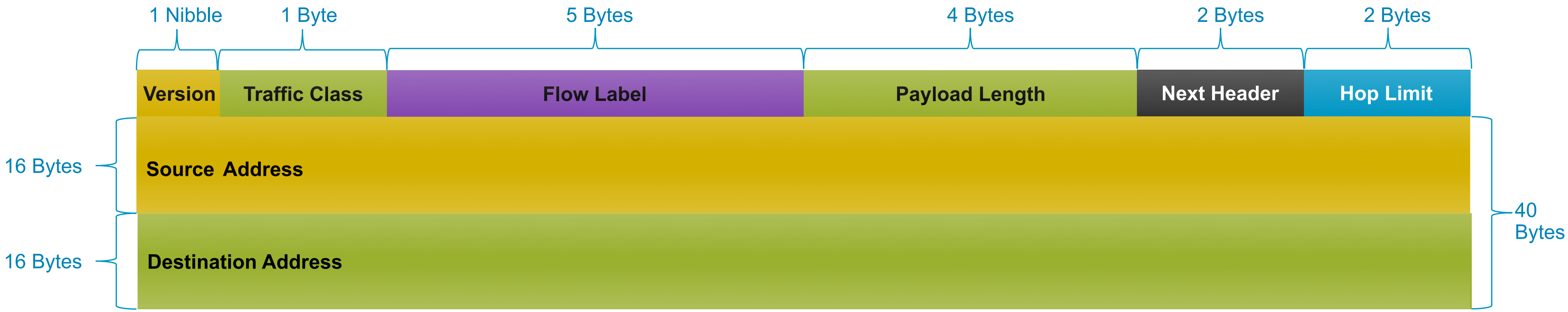
What is 6LoWPAN ?



- IPv6 over Low power Wireless Personal Area Networks
  - An adaptation layer for IPv6 over IEEE 802.15.4 links
- Why do we need an adaption layer?
  - IEEE 802.15.4 MTU is only 127 bytes, IPv6 minimum MTU is 1280 bytes
  - 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 defines the Problem Statement
- RFC4944 defines Transmission of IPv6 Packets over IEEE 802.15.4
  - Improved header compression being worked on may deprecate RFC4944

smart object networks go better with IPv6 & IEEE 802.15.4

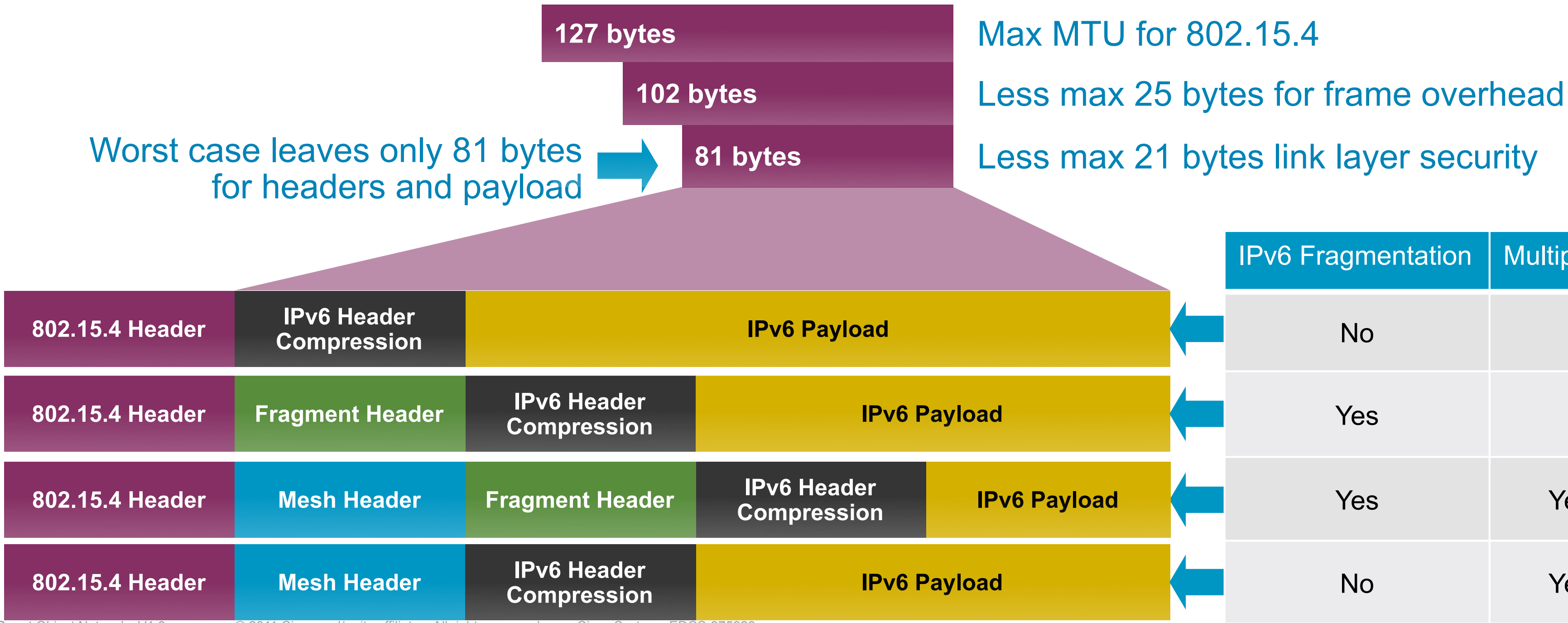
Basic IPv6 Header



- Minimum size is 40 bytes (double that of IPv4)
- Can be extended by additional headers
- Fragmentation must be performed by end nodes

Typical 6LoWPAN Header Stacks

- 6LoWPAN headers included only when needed
  - 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 requirements developed
  - Industrial (RFC5673)
  - Urban (RFC5548),
  - Home Automation (RFC5826)
  - Building Automation (RFC5867)
- Specifying the routing protocol for smart object networks
  - Routing Protocol for LLNs (RPL) adopted as WG document

Where Should Routing Take Place ?

- Historically, a number of interesting research initiatives on WSN
  - Work on Wireless Sensors Network focussed on algorithms … not architecture
- Most work assumed the use of MAC addresses
  - Layer 2 “routing” (mesh-under)
- Support of multiple PHY/MAC is a MUST
  - IEEE 802.15.4, Low Power Wifi, Power Line Communications (PLC)
- Use IP to route
  - Supports multiple PHY/MAC
  - Moves from mesh-under (L2) to router-over(L3)

Characteristics for Smart Object Routing

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

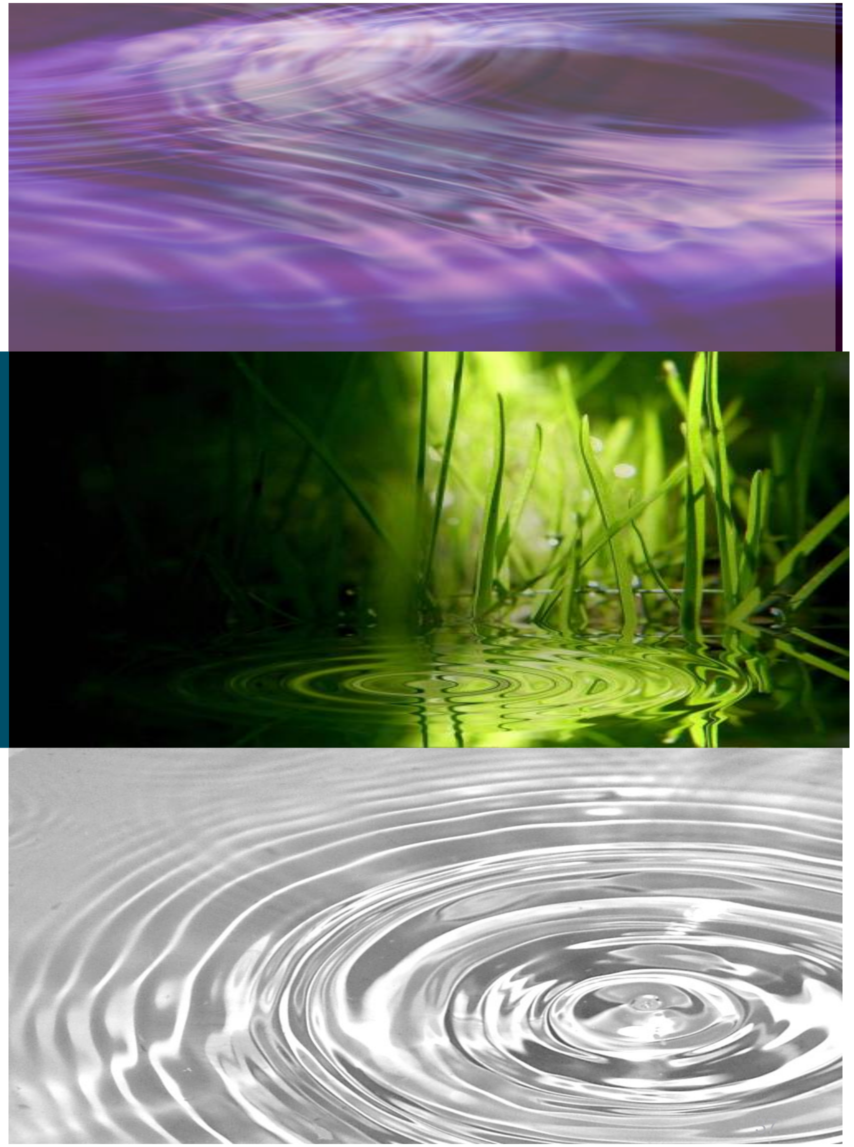
Technical Challenges

- Energy consumption is a major issue (battery powered sensors/actuators)
- Limited processing power
- Very dynamic topologies
  - Link failure (LP RF)
  - Node failures (triggered or non triggered)
  - Node mobility (in some environments),
- Data processing usually required on the node itself
- Sometimes deployed in harsh environments (e.g. Industrial)
- Potentially deployed at very large scale
- Must be self-managed (auto-discovery, self-organizing 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 is pronounced "Ripple"

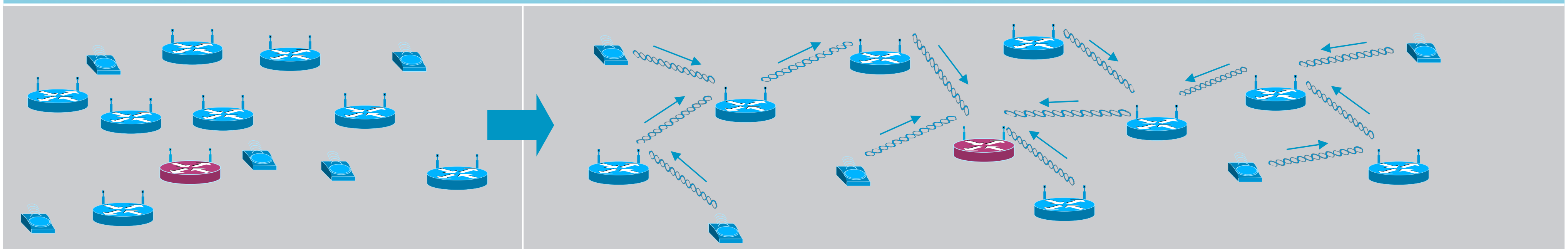
RPL - Routing Protocol for LLNs

- RPL is an extensible proactive IPv6 distance vector protocol
  - Builds a Destination Oriented Directed Acyclic Graph (DODAG)
  - 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
  - Should not be categorised as a WSN routing protocol
  - Agnostic to underlying link layer technologies (802.15.4, PLC, Low Power Wireless)
- RPL supports different LLN application requirements
  - RFC 5548 (Urban) RFC 5673 (Industrial) RFC 5826 (Home) RFC 5867 (Building)
- http://datatracker.ietf.org/doc/draft-ietf-roll-rpl/
  - Currently on last call implementation 18 (Feb 2011)

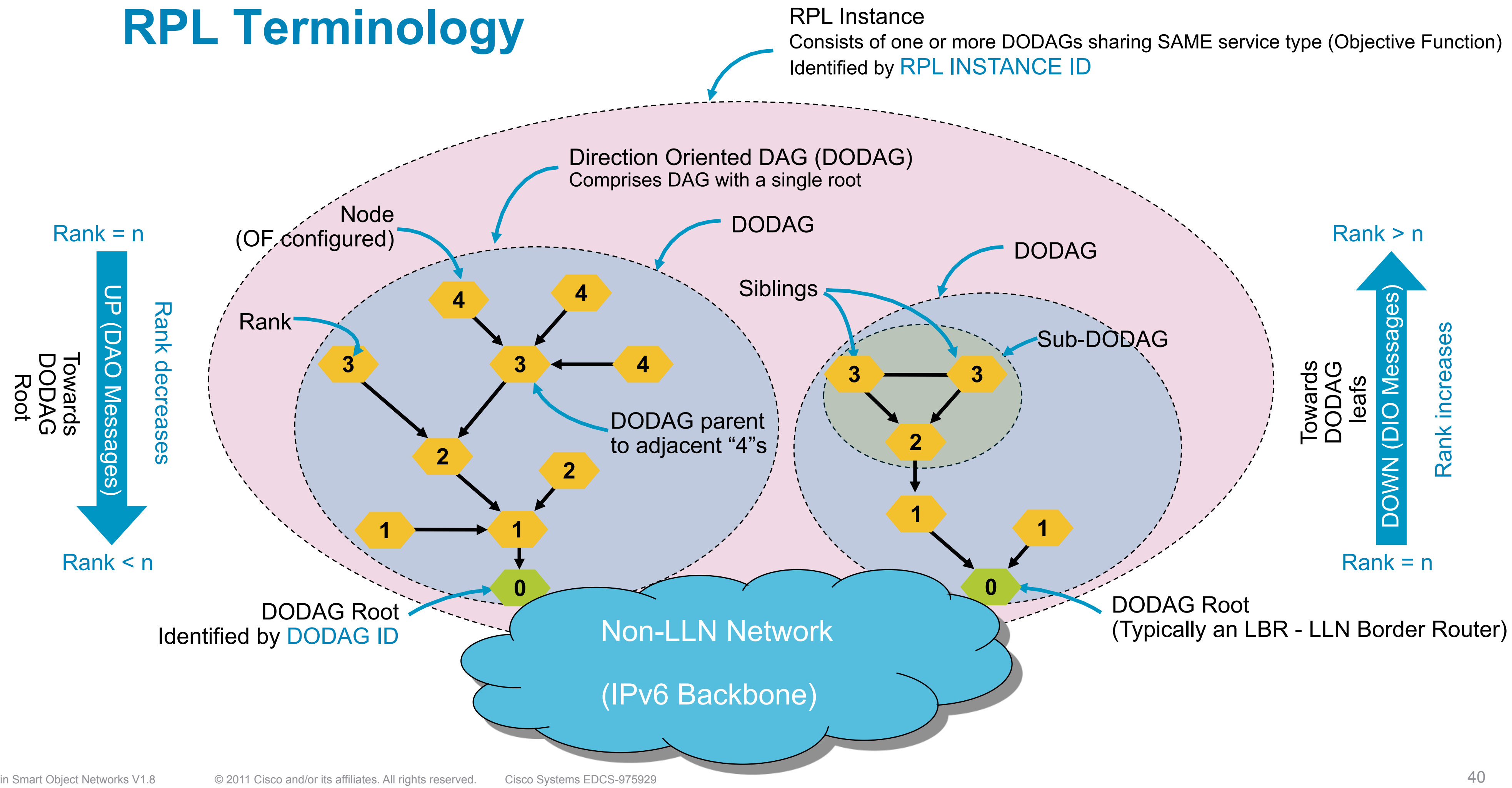
What is a Directed Acyclic Graph?

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)*.

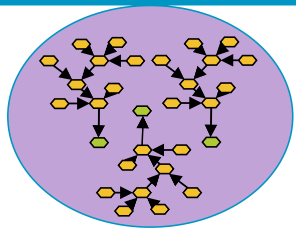
A Destination Oriented DAG is a DAG that comprises a single root node.



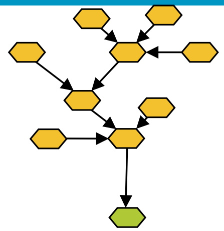
RPL Terminology



RPL Instances



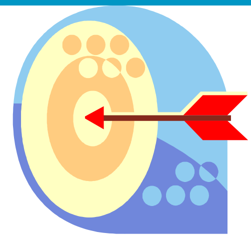
- RPL can form multiple instances
  - Each instance honours a particular routing objective/constraint
  - Instance consists one or more DODAGs derived from the *same* objective function
  - Nodes select a parent (towards root) based on metric, OF and loop avoidance
- Allows upwards and downwards routing (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 special ICMPv6 control messages
- Each root uses a unique {DODAG ID} to identify itself within an RPL Instance
- Routing performed over the DODAG using distance vector techniques
- Every hop to the root MUST have an alternate path
  - (Quite possible 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)
  - Actual routing metrics and constraints carried ICMPv6 control messages
- A rank in the DODAG reflects its distance from the root

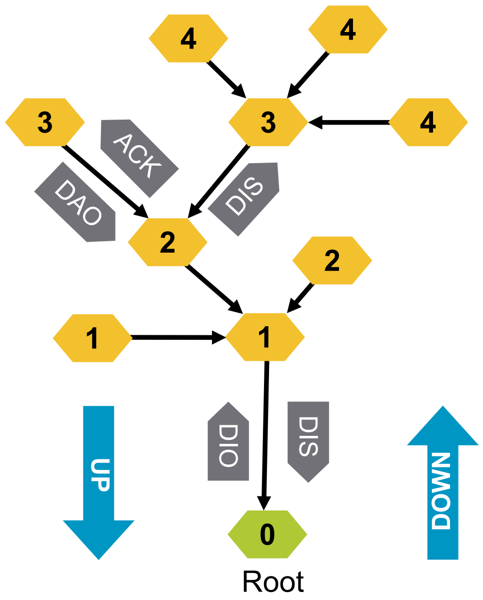
Rank =

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

Rank is higher as distance increases from DODAG root

- There is a single Objective Function per RPL Instance
  - An instance can comprise one or more DODAGs (share same OF)
- http://datatracker.ietf.org/doc/draft-ietf-roll-of0/ (Basic OF specification)

ICMPv6 RPL Control Messages



- DIO - DODAG Information Object

  Used for DODAG discovery, formation and maintenance

- DIS - DODAG Information Solicitation Message

  Used to probe for DIO messages from RPL nodes

- DAO - DODAG Destination Advertisement Object

  Propagates prefix availability from leaves up the DODAG

  Supports P2MP and P2P traffic

- DAO-ACK - DODAG Destination Advertisement Object

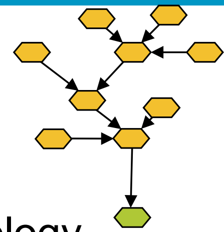
  Unicasted by a DAO recipient in response to a unicast DAO message

Link-local Destination	Link-local Source	RPL Control Payload
All-RPL-Nodes FF02::1A	Link-local Source	RPL Control Payload

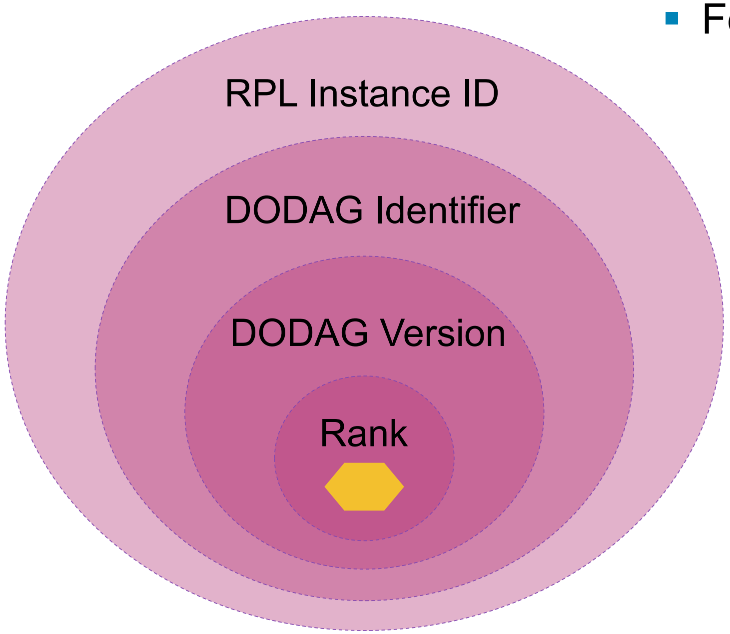
Most RPL control messages have scope of a link

Global or Unique-Local	Global or Unique-Local	RPL Control Payload

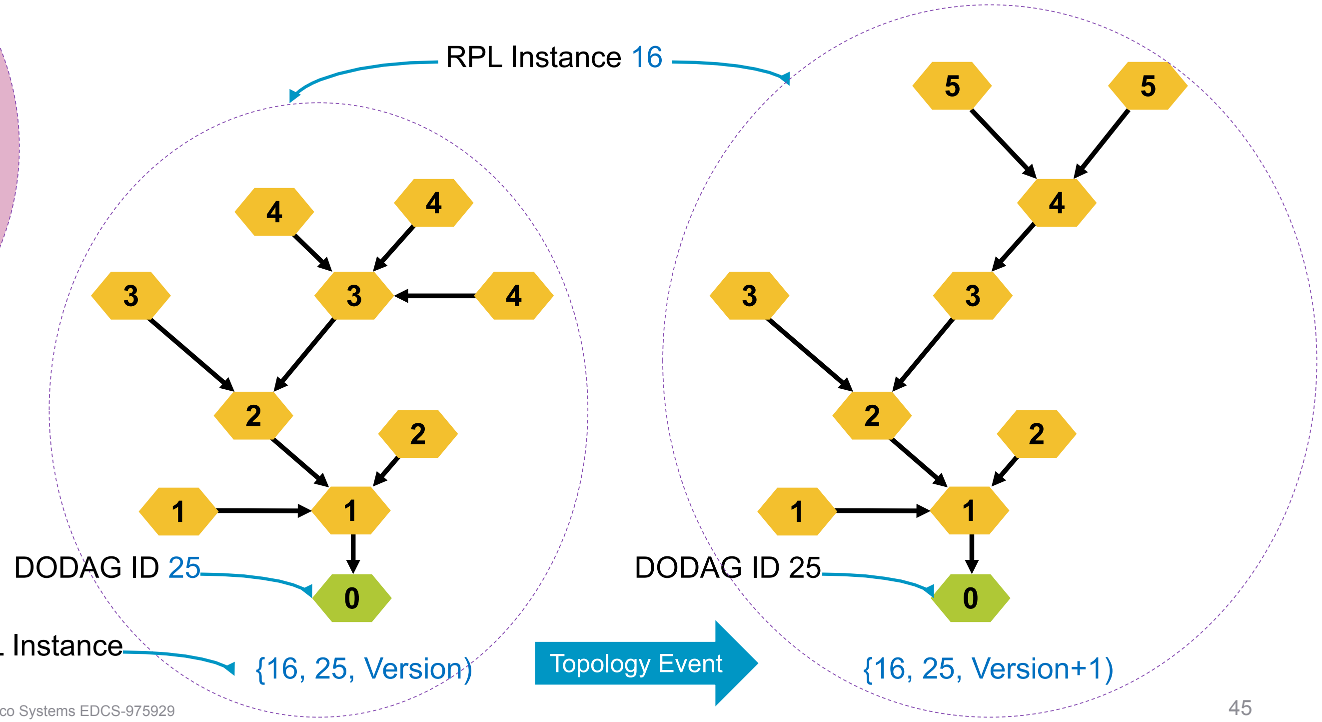
DAO/DAO-ACK in non-storing mode passes over multiple hops



RPL Identifiers

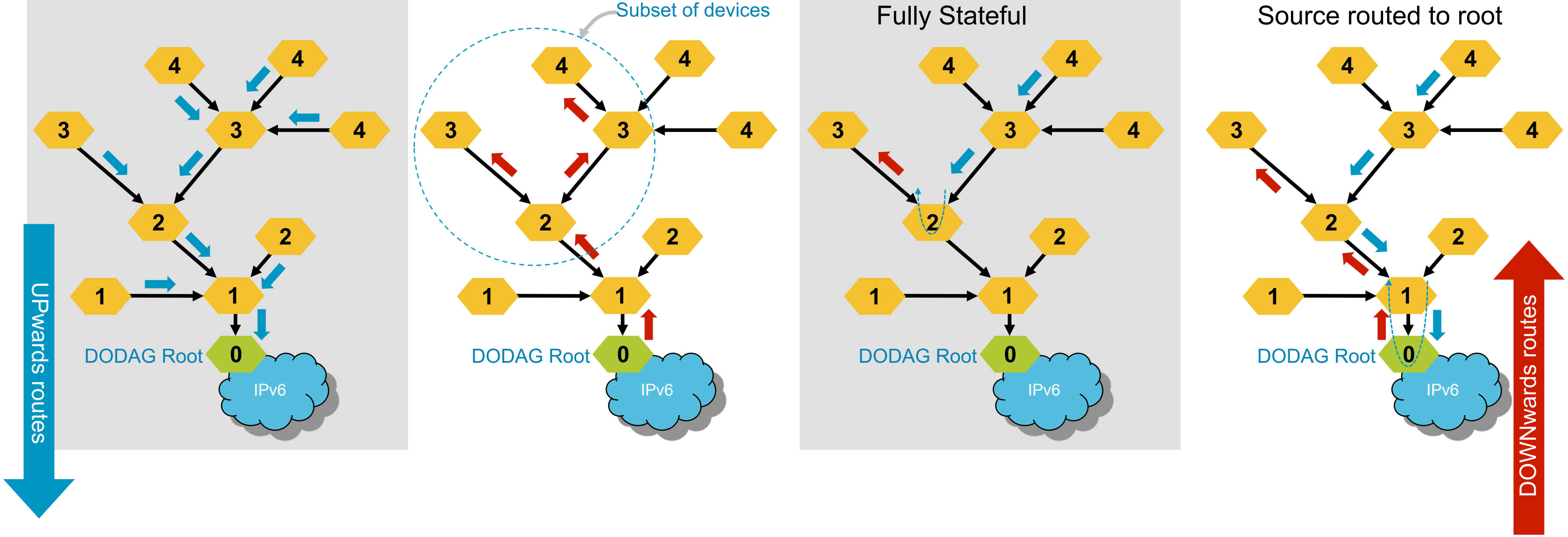


- Four values used to identify and maintain DODAG topology
  - Nodes in a particular topology will belong to the same DODAG version
  - Rank within {RPL Instance ID, DODAG ID, DODAG Version} scope

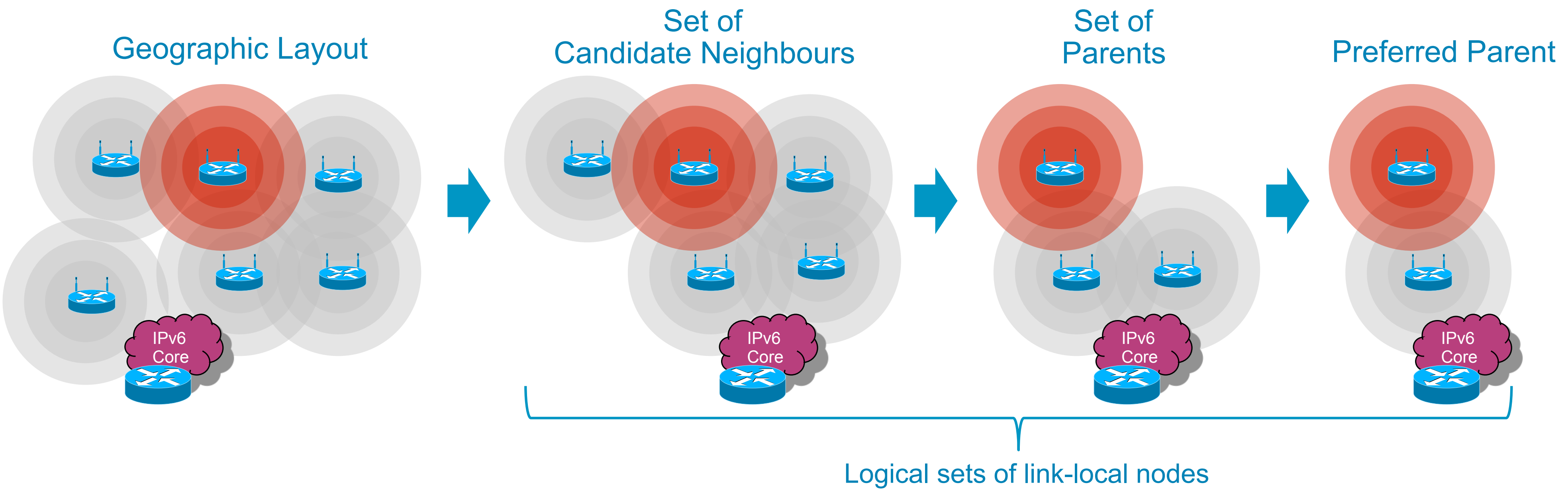


RPL Supported Traffic Flows

- 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 Routes)



- **Upward route discovery**

  Comprises three logical sets of link-local nodes

  Neighbours are learnt from DIO advertisements

- **Candidate Neighbour Set**

  Subset of nodes reachable via link-local multicast

  Elements in the set may belong to different DODAG versions

- **Parent Set**

  Consists of nodes with a higher rank (lower #)

  Elements in the set must belong to SAME DODAG version

- **Preferred Parent**

  Preferred next-hop to the DODAG Root

  Multiple preferred parents possible if ranks are equal

RPL Security

- RPL has three basic security modes
- Unsecured Mode

  Relies on underlying link layer security mechanisms
- Pre-Installed Mode

  RPL nodes use same pre-shared/installed key to generate secure messages
- Authenticated mode

  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

Routing Metrics and Constraints in LLNs

- http://datatracker.ietf.org/doc/draft-ietf-roll-routing-metrics/
  - Specifies a set of link and node LLN routing metrics and constraints
- Constraints provide a path "filter" for more suitable nodes and links
- Metrics are the quantitative value used to evaluate the 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
- Computing dynamic metrics takes up power and can change rapidly
  - Solved by abstracting number of discrete values to a metric

Link Quality Metric	
Value	Meaning
0	Unknown
1	High
2	Medium
3	Low

Tradeoff

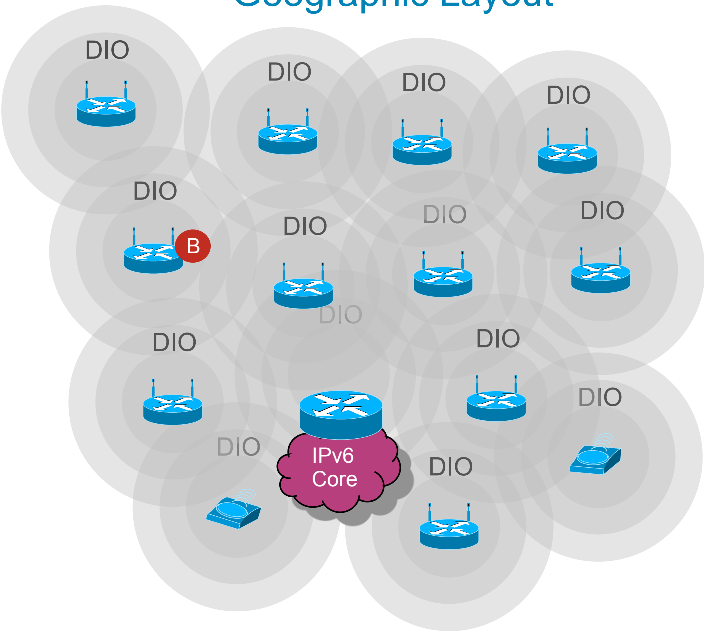
Reduced accuracy vs overhead and processing efficiency

Routing Metrics in LLNs

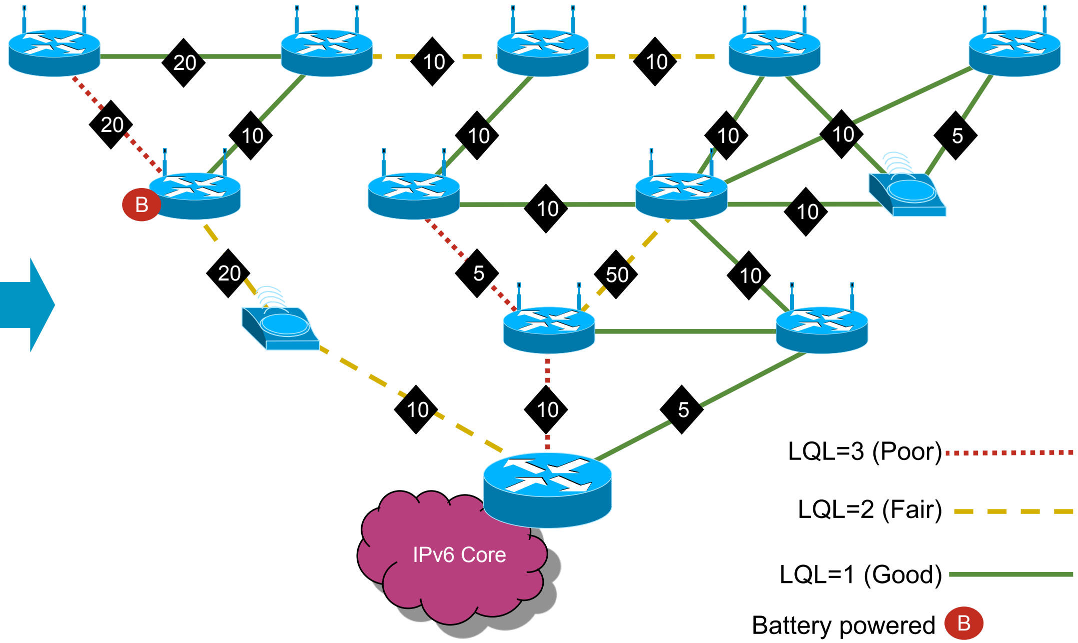
Node Metrics	Link Metrics
Node State and Attributes Object Purpose is to reflects node workload (CPU, Memory…) “O” flag signals overload of resource “A” flag signal node can act as traffic aggregator	**Throughput Object** Currently available throughput (Bytes per second) Throughput range supported
Node Energy Object “T” flag: Node type: 0 = Mains, 1 = Battery, 2 = Scavenger “I” bit: Use node type as a constraint (include/exclude) “E” flag: 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=High, 2=Medium, 3=Low Expected Transmission Count (ETX) (Average number of TX to deliver a packet)
	Link Colour Metric or constraint, arbitrary admin value

DODAG Example

Geographic Layout

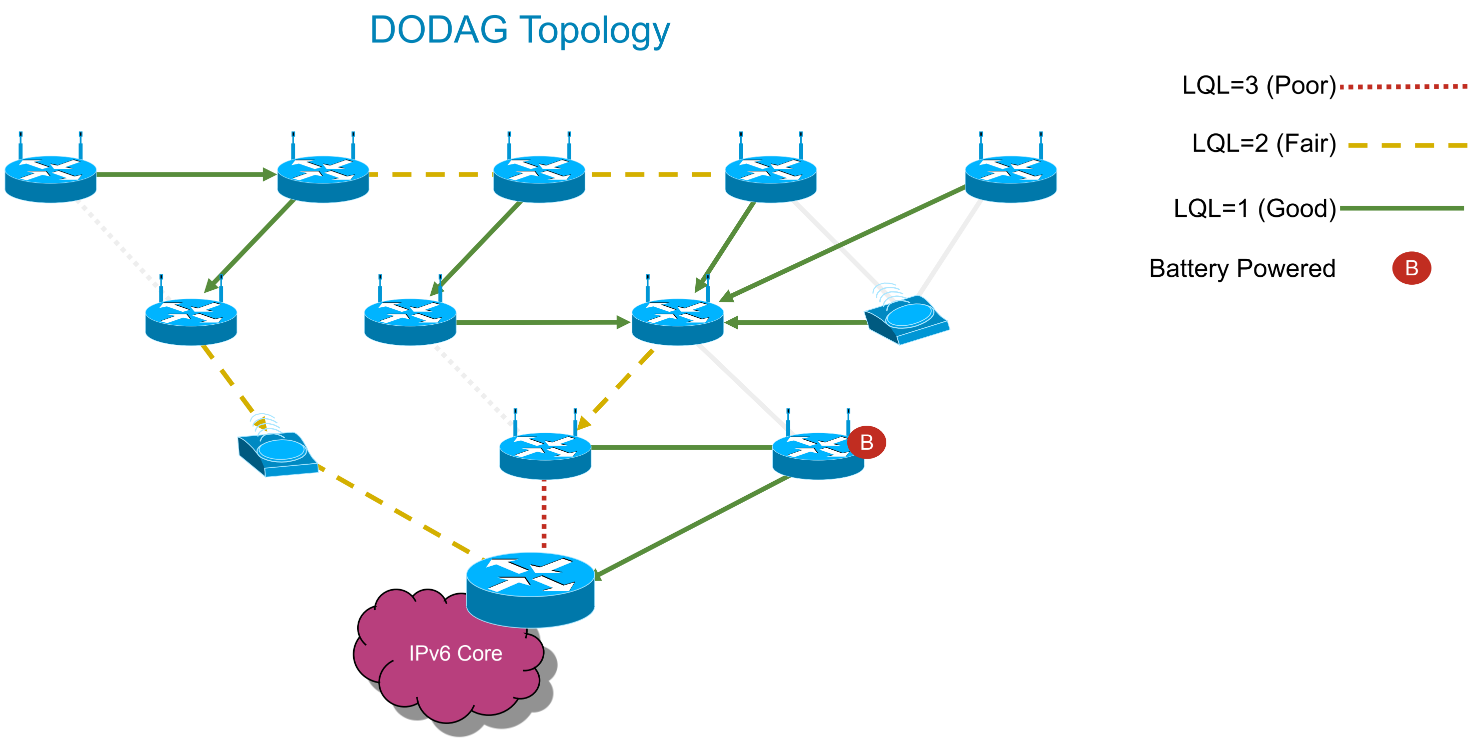


DODAG Topology

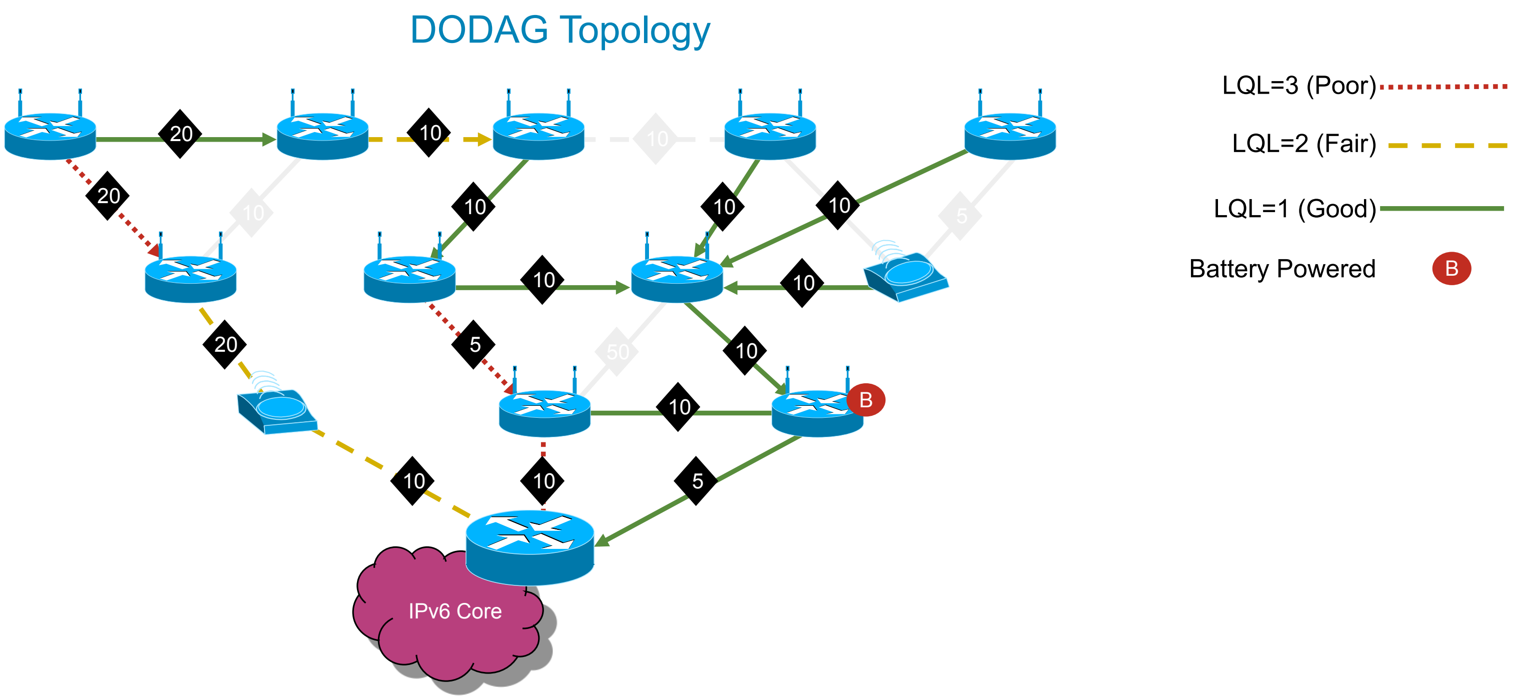


- DIO messages are propagated from the DODAG root

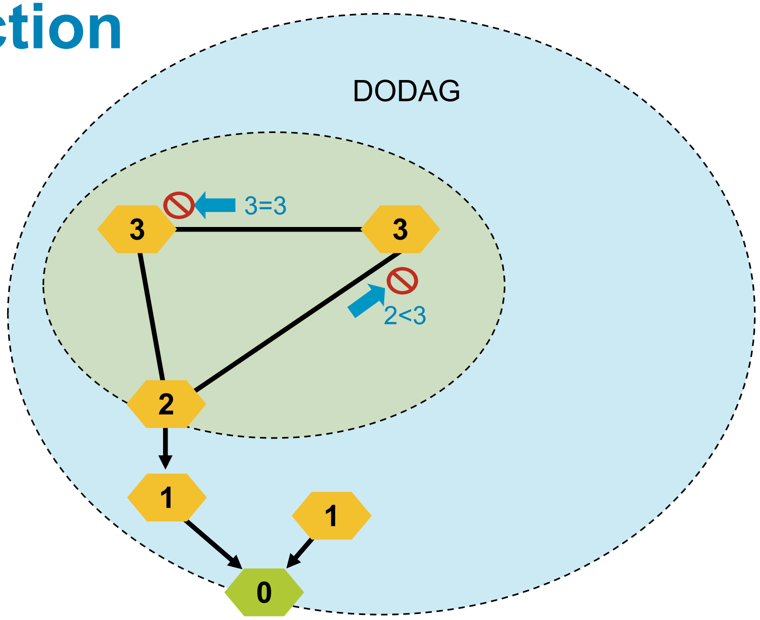
OF: Use High Quality Links, Avoid battery powered nodes



OF: Low Latency Paths only



RPL Loop Detection

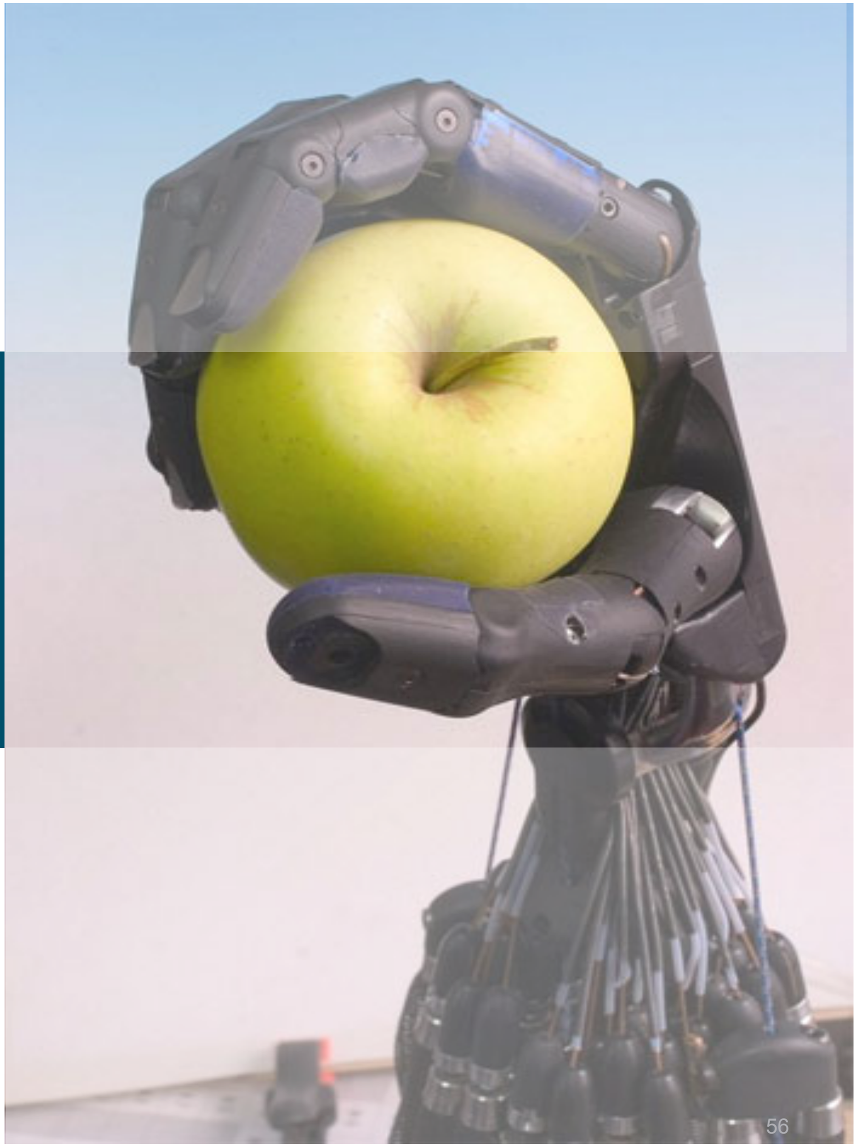


- Data path validation used to check for loops (Simple mechanism)
  - IPv6 options header carries rank of transmitter
- If node receives packet with rank <= to its own, drop packet
  - Detection happens when link is actually used.

RPL Summary

- RPL is a foundation 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
  - Passed execute commit, planned for IOS 15.2PI16
  - In roadmap for SGBU nextgen routers
- Standardisation Status (Dec 2010)
  - Passed WG and IETF last call
  - Adopted by several alliances: Zigbee/IP, Wavenis, IEEE P1901.2 (Power line comms)

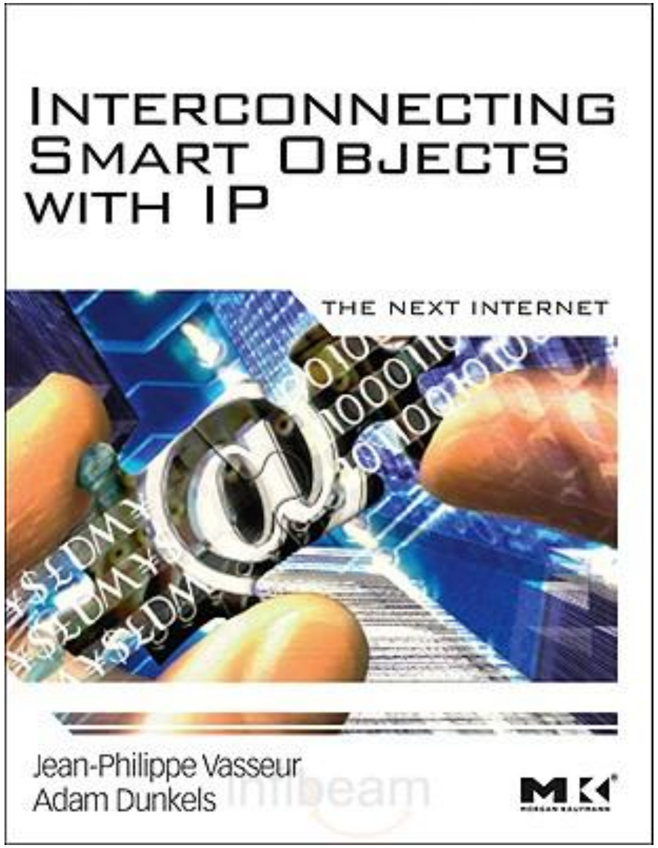
Conclusion



Conclusion

- Smart Objects have several major applications
  - 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 and now CoRE
  - IPSO alliance
  - Adoption of IP by several other SDOs/alliance: Zigbee/IP for SE2.0, Bacnet, ….
- Internet of Things is coming
  - Current Internet = Some things (computers and hosts)
  - Next Internet = Everything!

Recommended reading



- Covers the trends in Smart Objects
- RPL protocol
- Detailed application scenarios
- Written by

  JP Vasseur (Cisco DE)

  Adam Dunkels (Inventor of Contiki O/S, uIPv6)


CISCO