The Internet of Things

Powered by IPv6

Jeff Apcar

Distinguished Services Engineer, Cisco Systems

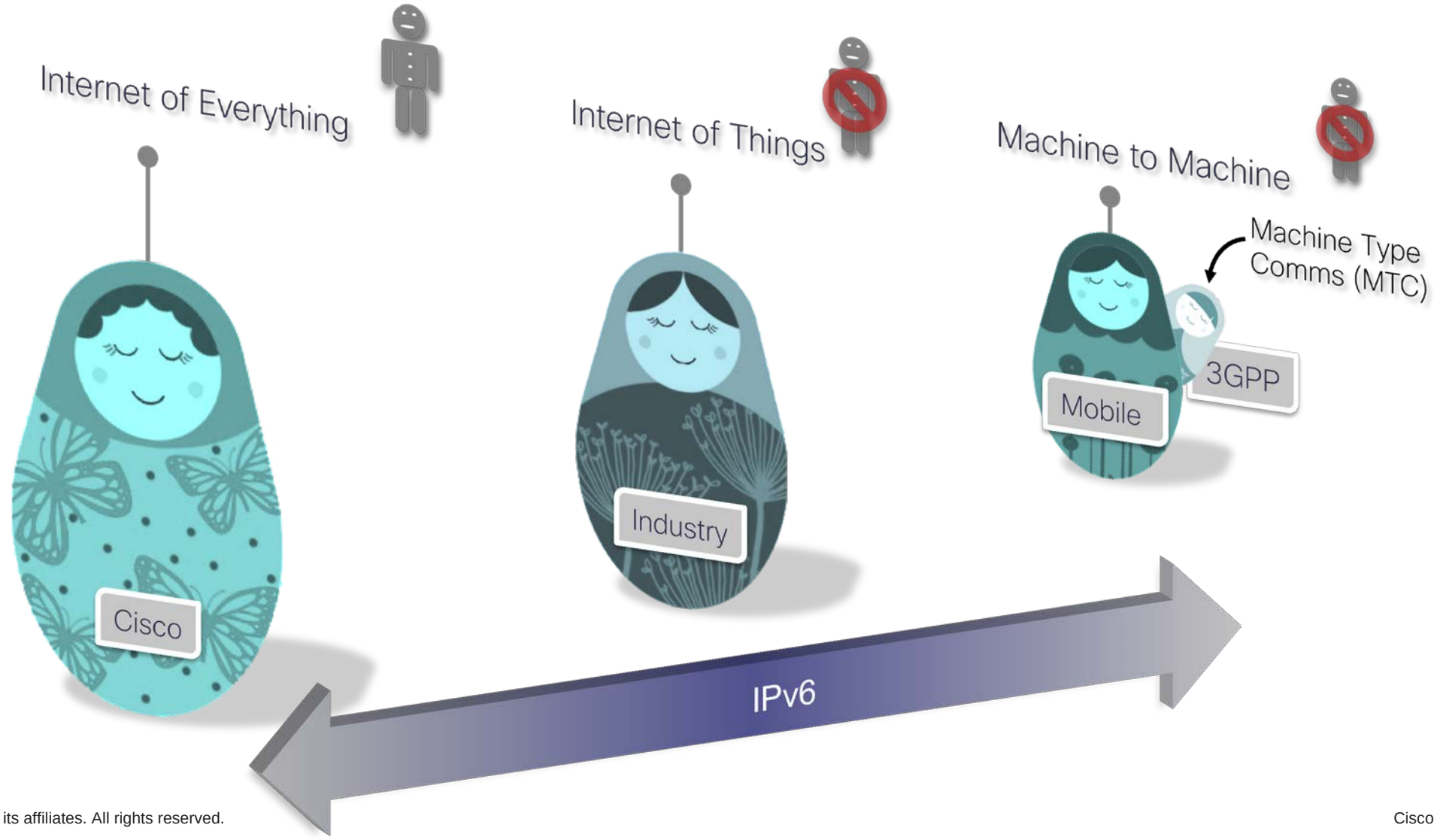
March 14th 2014, iDA IPv6 Conference

IoT Definition

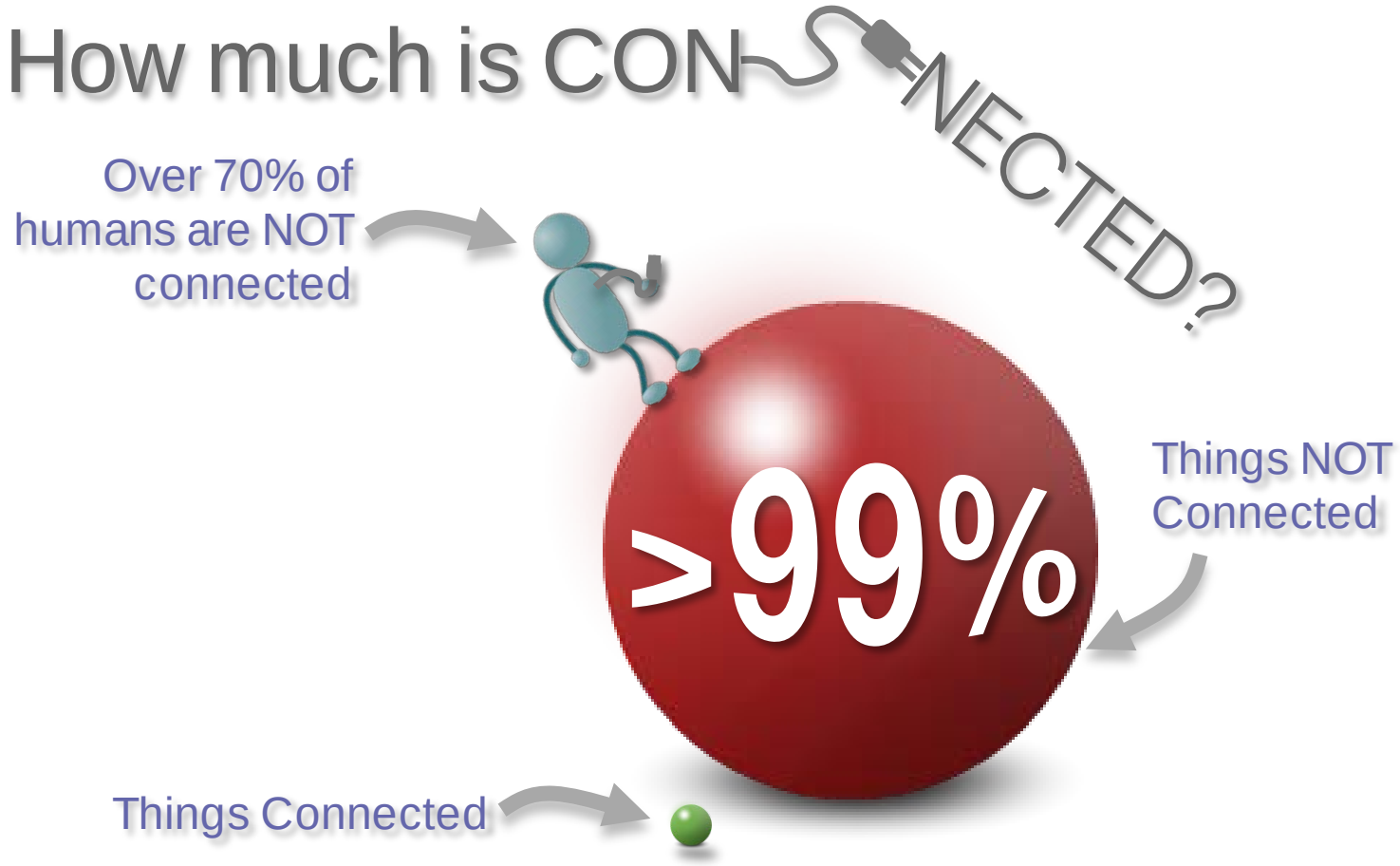
"A pervasive and ubiquitous network which enables monitoring and control of the physical environment by collecting, processing, and analysing the data generated by sensors or smart objects**"

** A collection of "things"

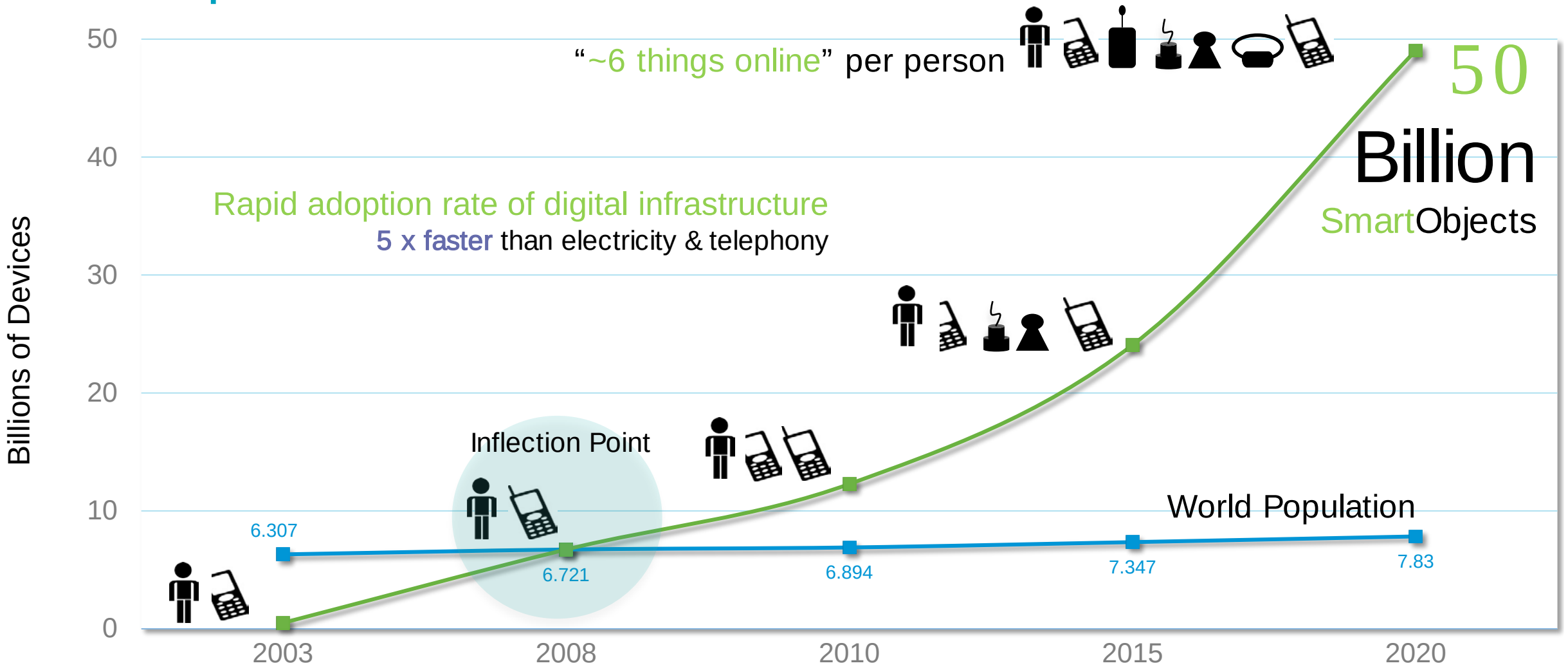
IoE/IoT/M2M Relationship to IPv6 (Russian Dolls)



IPv6: Connecting the Unconnected



IoT Rapid Growth



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

Shift In Dominant End Points

From IPv4 Consumer

Tablets, Laptops, Phones

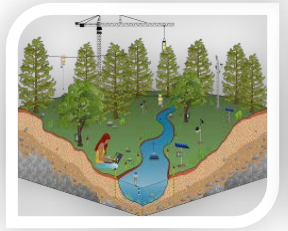
Human Interactions

To IPv6 Enterprise & Operational Technologies

Sensors, Smart Objects, Device Clustered Systems

Machine to machine interactions


Energy Saving
Smart Grid




Analytics and
Modelling


Intelligent
Buildings

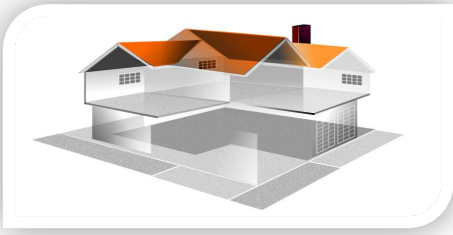
Transport and
Connected Vehicles


Improve
Productivity


Safety & Security


Precision
Agriculture


Predictive
Maintenance

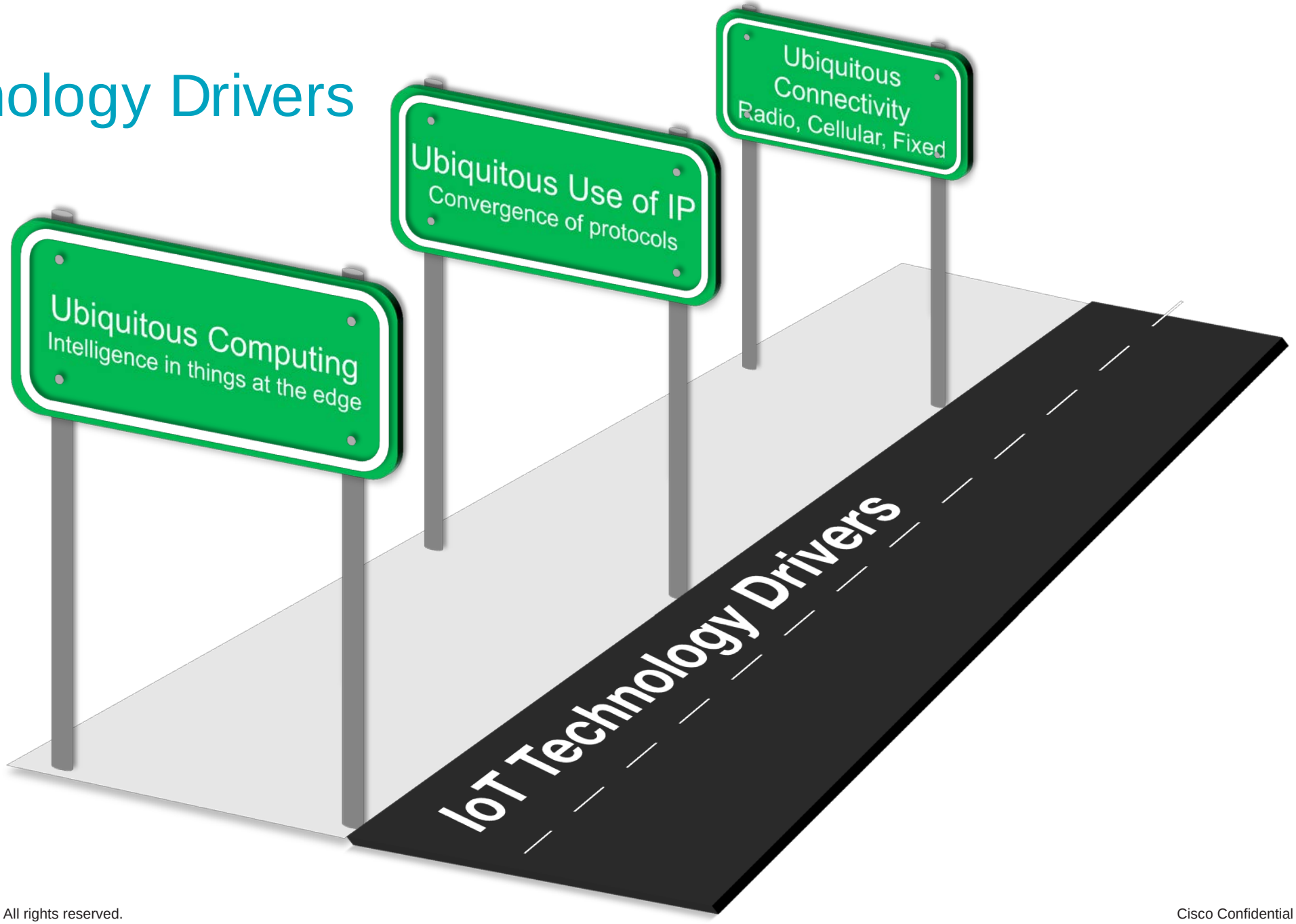


Smart Home
S+CC


Healthcare

Technology and Architecture

IoT Technology Drivers



IoT Architectural Philosophy

Closed Systems
(Little external interaction)

Various Protocols
(Modbus, SCADA, BACnet, LON, HART)

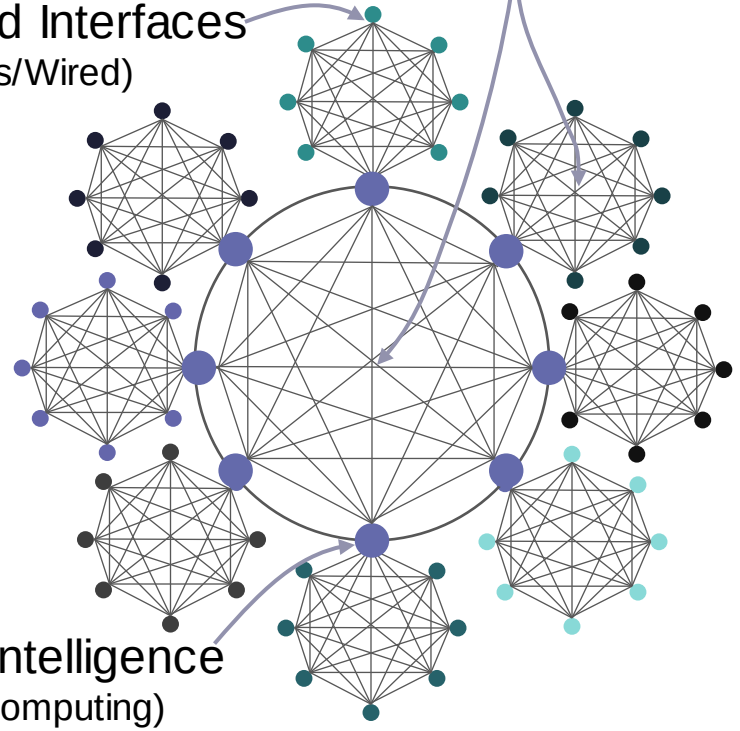
Protocol Gateways
(Inherently complex, inefficient and fragmented networks)

Proprietary Networks
(Usually layer 2 based)

From

Standardized Networks
(IP Based/ISO Stack)

Standardized Interfaces
(Wireless/Wired)



Distributed Intelligence
(e.g. Fog Computing)

To

IoT Architecture

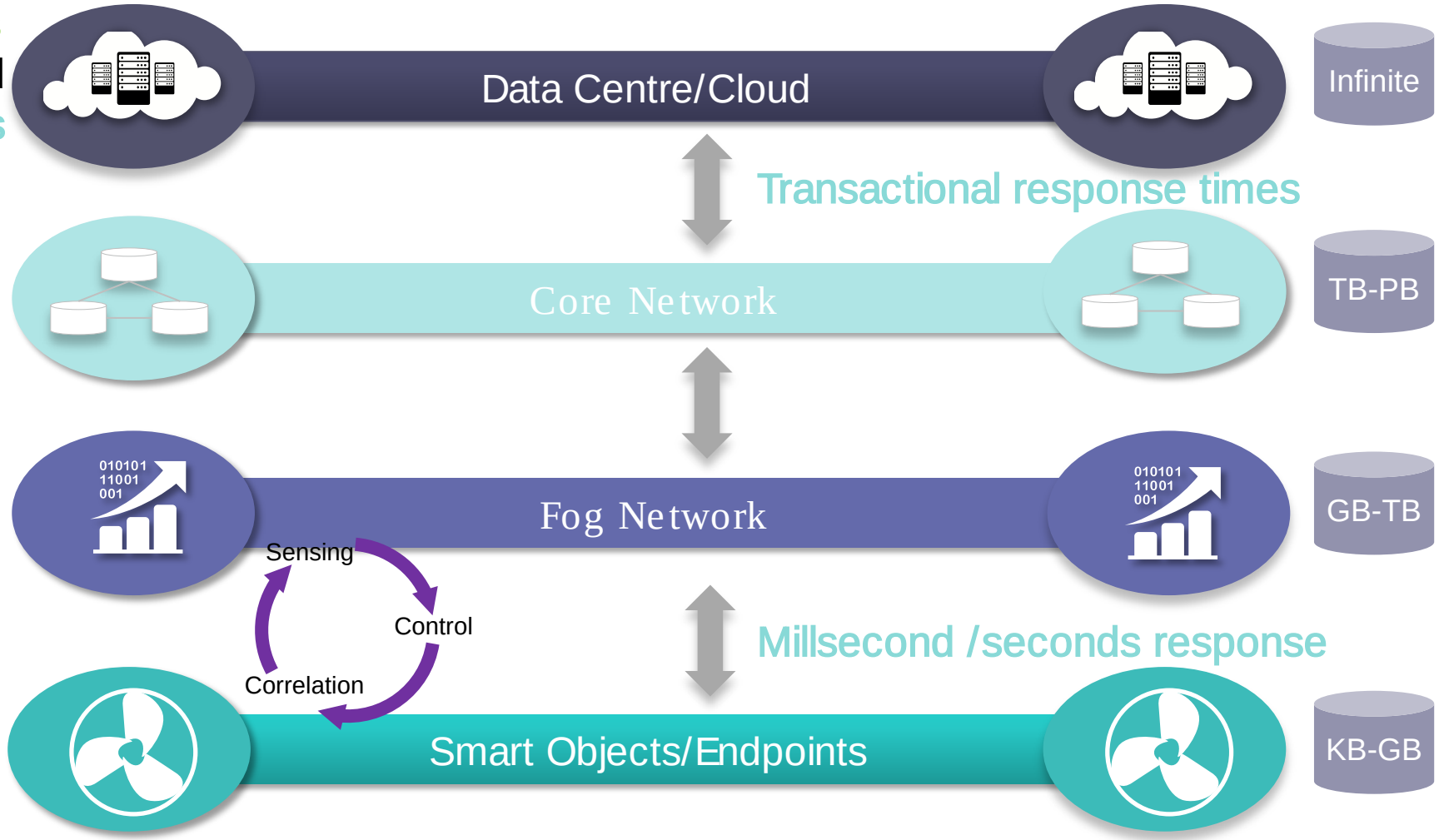
Data Points, Variety & Velocity, Security, Resiliency, Latency

Hundreds
Data Centre/Cloud
Hosting IoT Analytics

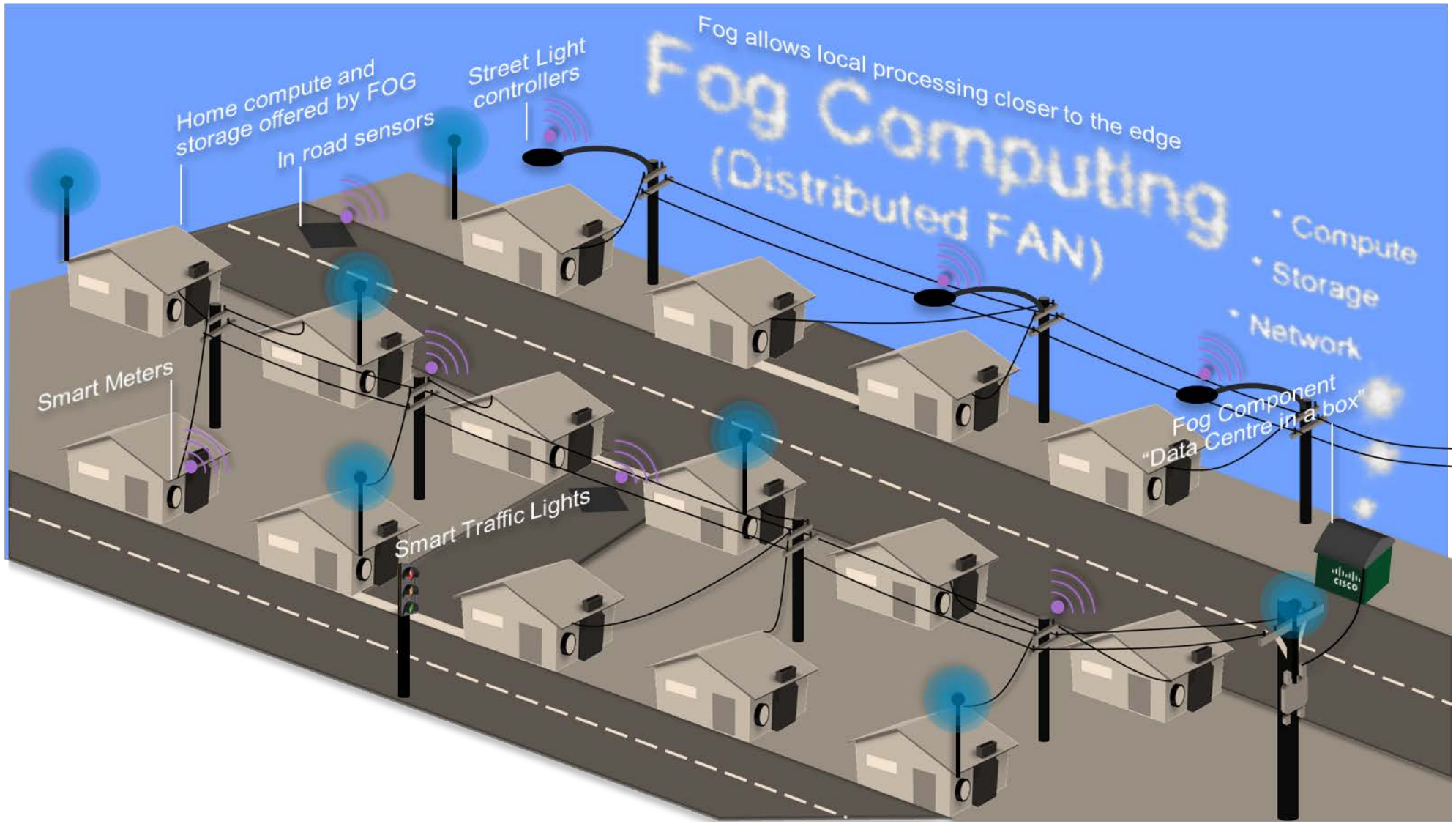
Thousands
Backhaul
IP/MPLS, Security, QoS, Multicast

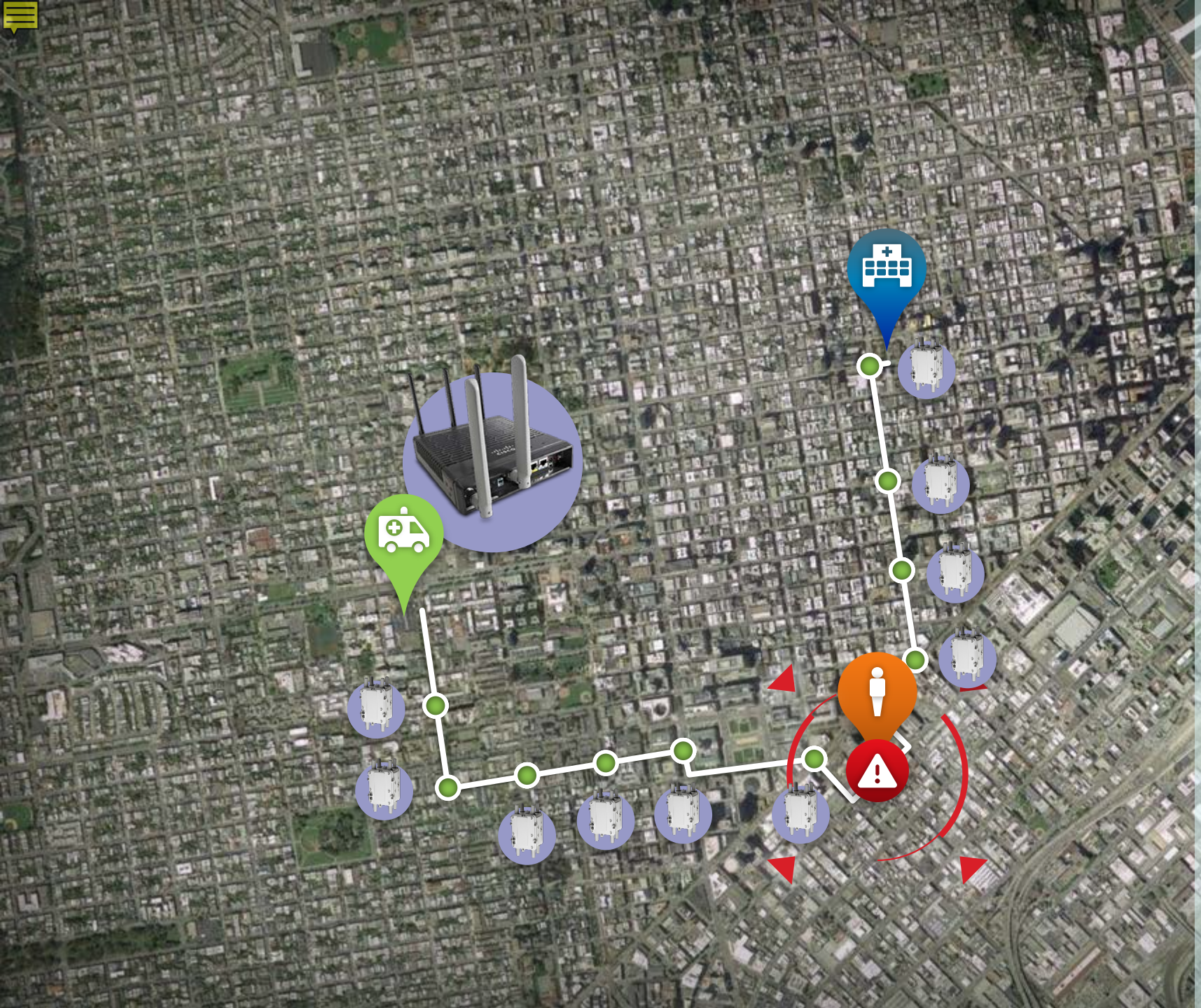
Tens of Thousands to Millions
Multi- Service Edge
3G/3G/LTE/WiFi/RF Mesh/PLC

Tens of Millions to Billions
Embedded Systems & Sensors
Low power, low bandwidth



Fog Computing – Field Area Networks





City Infrastructure

Synchronize Signals for Emergency Vehicles

Improve Congestion Management

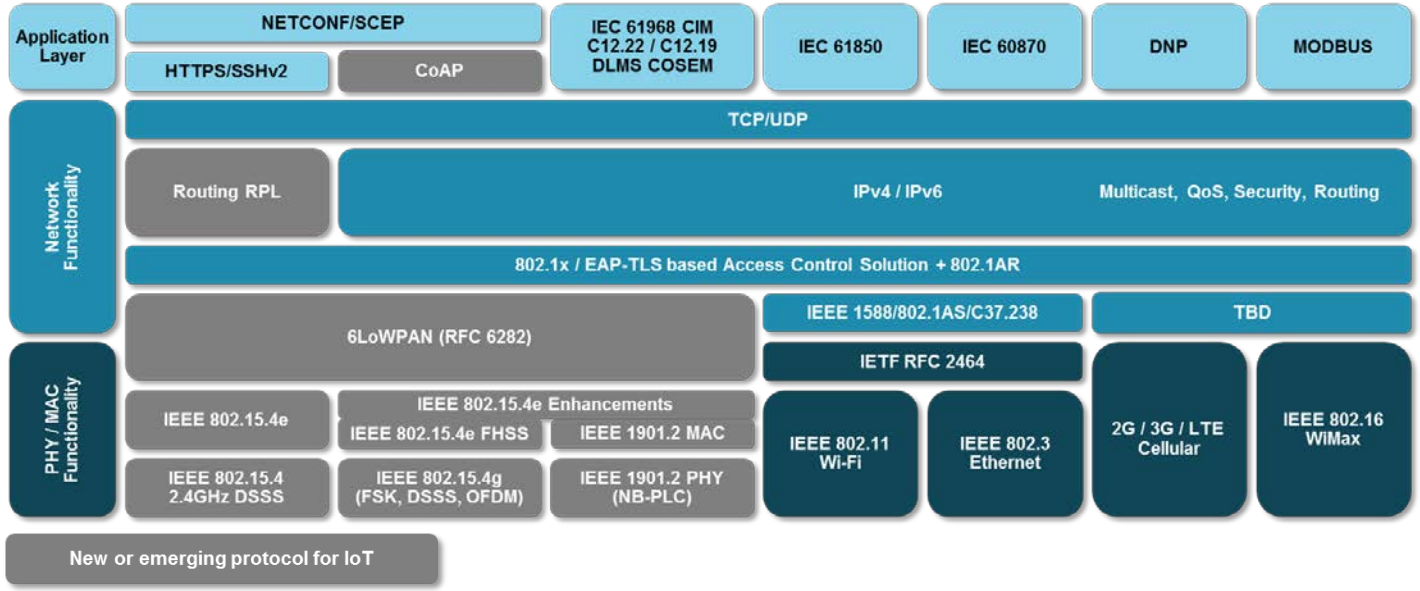
Better Profitability

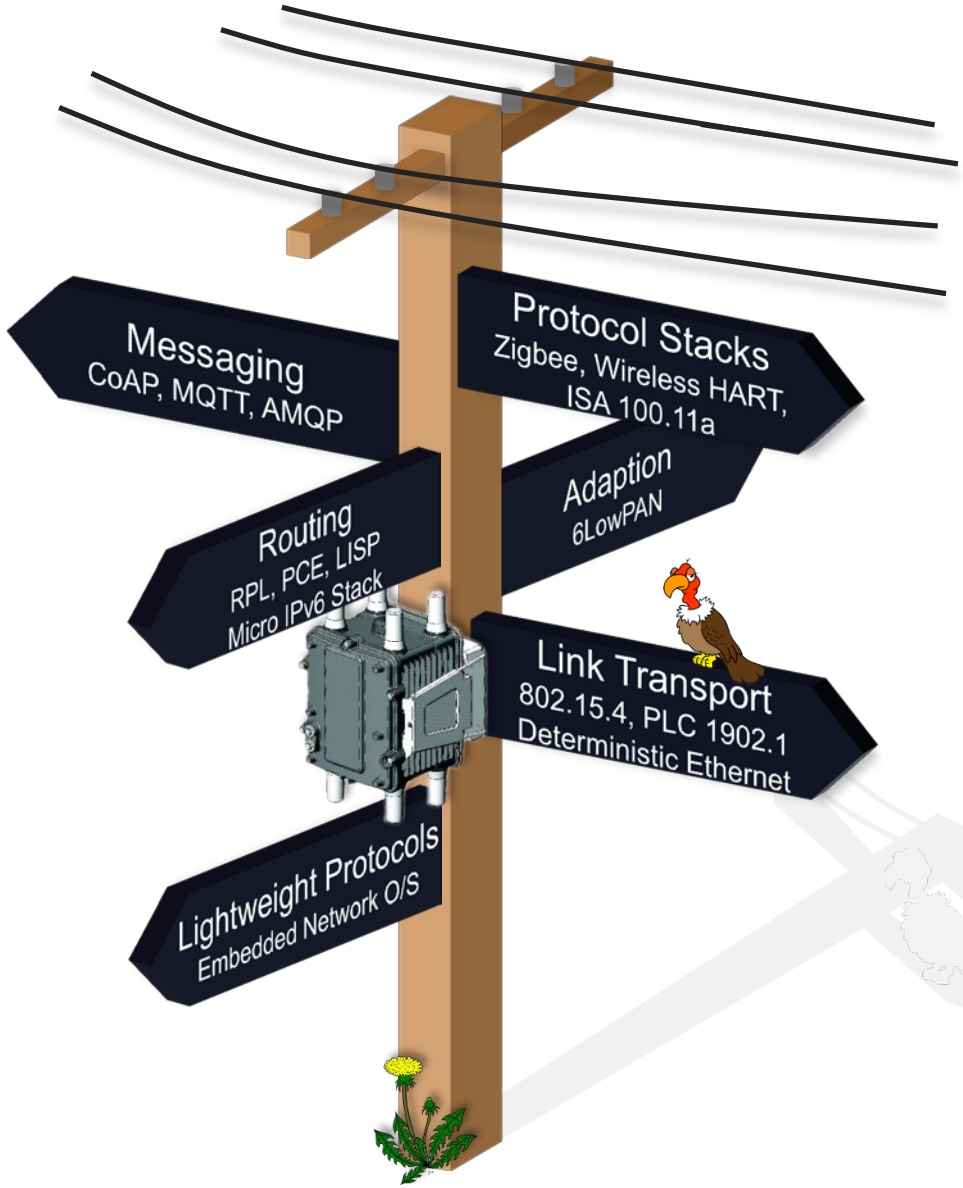
Protocols for IoT Networks

- Various protocols applied to IoT networks
- Relevant Protocols for different layers
  - Link Layer (eg., 802.15.4, PLC)
  - Adaption Layer (6LowPAN)
  - Routing (eg., RPL)
  - Messaging (eg., CoAP)
  - Security: (D)TLS, 802.1AR, 802.1X

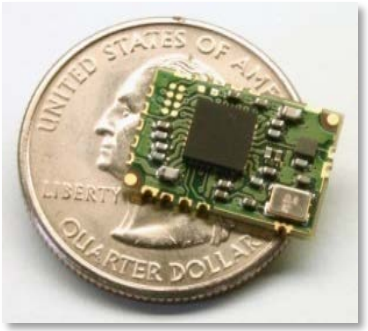
Designed for IPv6

Smart Grid Protocol Stack Example





IoT Device Characteristics



IoT Device or Smart Object
Embedded intelligence, IP Stack ...

Sensor
That can measure physical data
(temperature, vibration, pollution ...)

Actuator (optional)
Capable of performing a task
(change traffic lights, rotate a mirror ...)

Tiny low cost computer
Embedded into objects to make them smart
Can be organised into networks

Communication Device
Receive instructions , sends or routes data
Self organising into networks

Power Source
Harvesting (Solar/Wind), battery, mains,
Energy Scavenging (friction, braking)

Many applications & Solutions
Smart+Connected Communities
Smart Grid, Energy Management
Home and Building Automation
Connected Health

IoT Threats

IPv6 Protocol Is Subject To The Usual Attack Suspects

Reconnaissance

Viruses & Worms

Ping Ponging

Smurfing

Routing Attacks

Flooding

L4 Spoofing

L3 Spoofing

DHCP Attacks

Fragmentation

Denial of Service

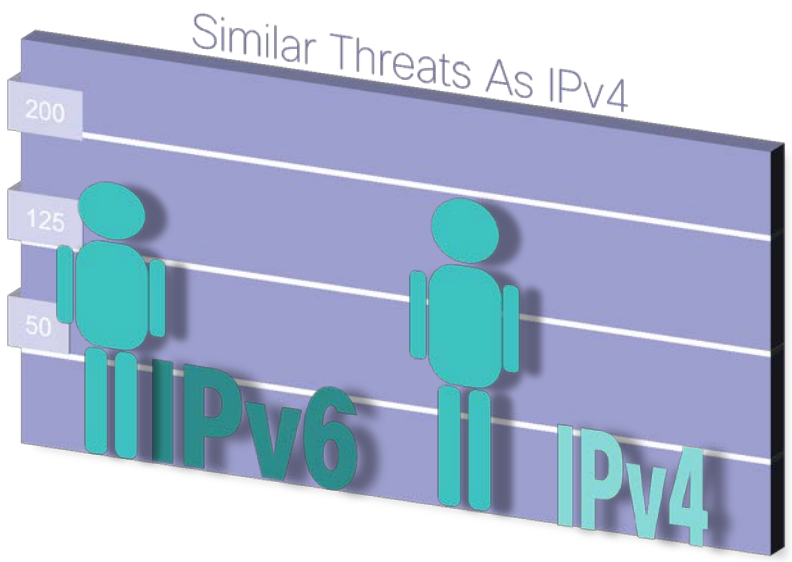
Rogue Devices

Unauthorised access

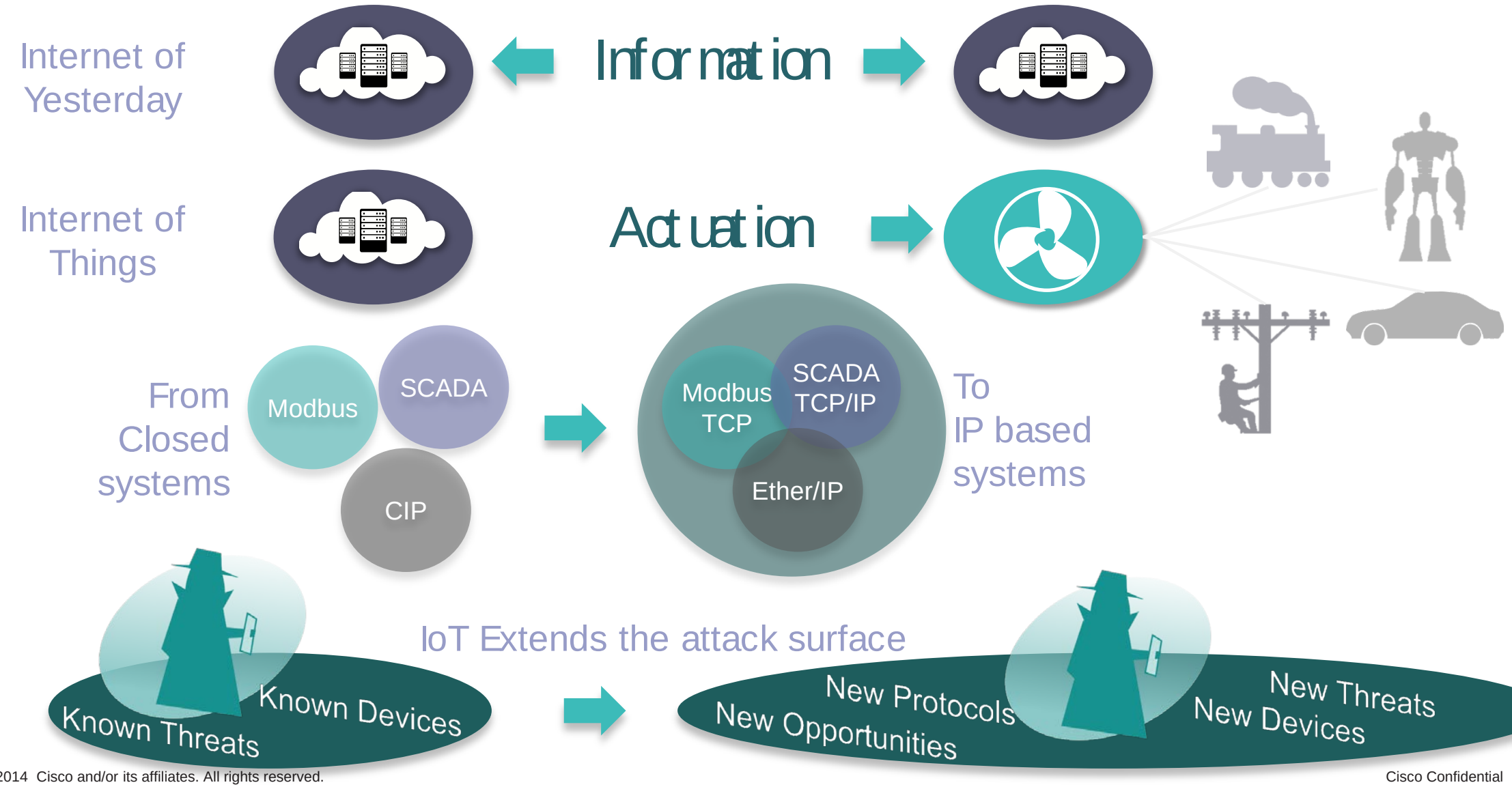
Man in the middle attacks

Sniffing

Neighbour Discovery Attacks



IoT: Where The Internet Meets The Physical World



Some IoT Threats

Too many to mention, here are a few…

Common worms jumping from ICT to IoT

Generally limited to things running consumer O/S: Windows, Linux, iOS, Android

Script Kiddies* or other targeting at residential IoT

Unprotected webcams
Stealing content
Breaking into home control systems

Organised Crime

Access to intellectual property
Sabotage and espionage

Cyber Terrorism

Nuclear plants (Stuxnet virus)
Traffic monitoring
Railways
Critical infrastructure

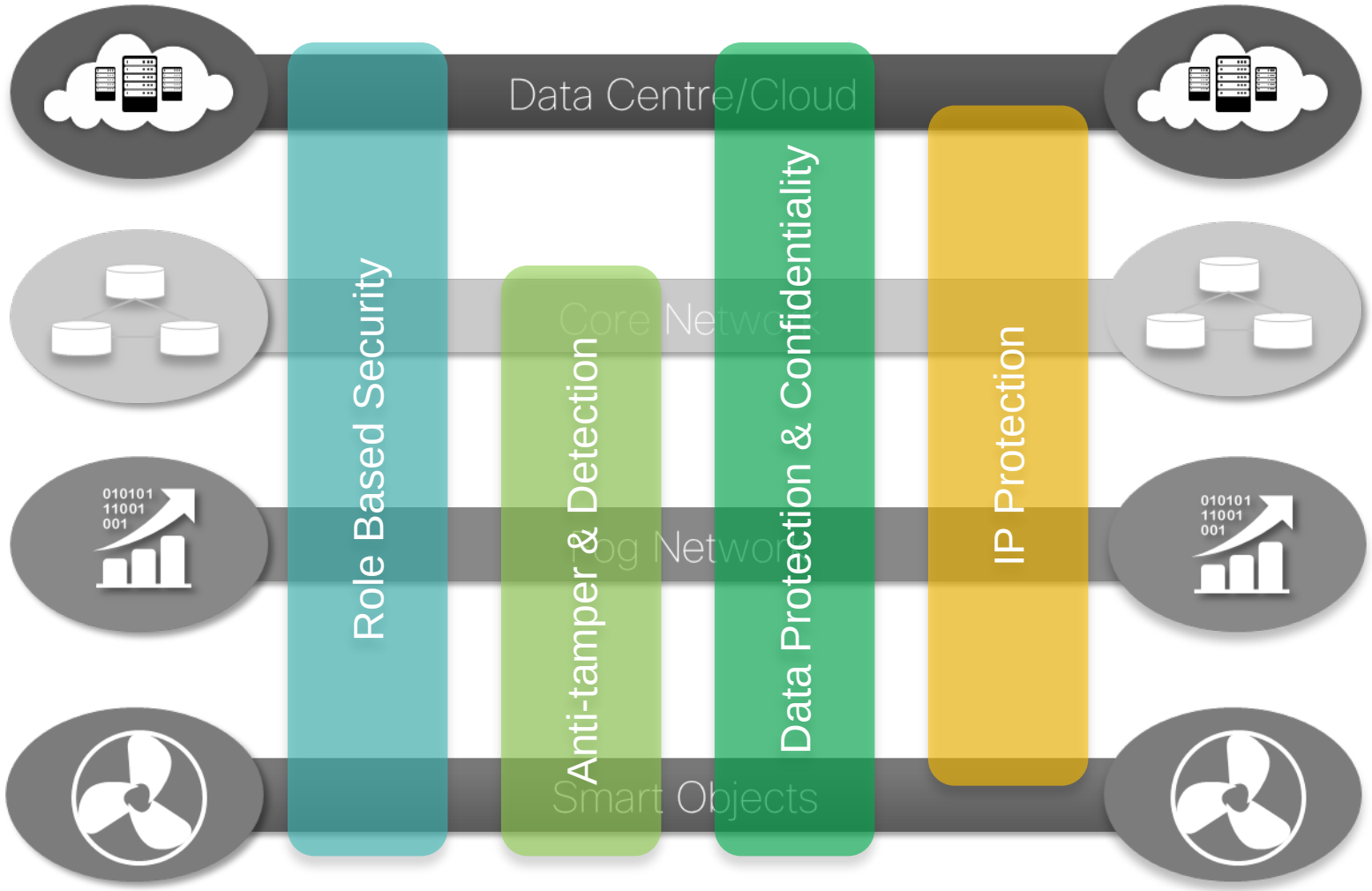
*Unskilled individuals who use scripts or programs developed by others to assemble attacks

Source: Eric Vynke, Cisco Systems

Shodan: The Google for hackers

Vulnerabilities go well beyond just IP protocols

IoT Security Framework



- Dynamic distributed intelligence
- Distributed Analytics & Management
- Network Enforcement/Segmentation
- Authenticated Encryption
- Connectivity Standards
- Stateful application visibility
- Auto enrollment & Provisioning
- Device Classification
- Standards for actuator & Sensors

What Next? The problem is more than IPv6

- IoE industry is still evolving, large potential for zero-day attacks
  - Opportunity to drive the security at the appropriate layer
- Embedded Endpoint layer comprises highly constrained devices
  - So far has limited the growth of malware to this layer
- Growth of IP based sensors corresponds to attack surface growth
  - New security protocols and identification techniques required
  - Corresponding to the capabilities of the device endpoint
- IoT presents new challenges to network & security architects
- Learning machines will play a big part in this area
  - Managed threat detection, anomaly detection, predictive analysis

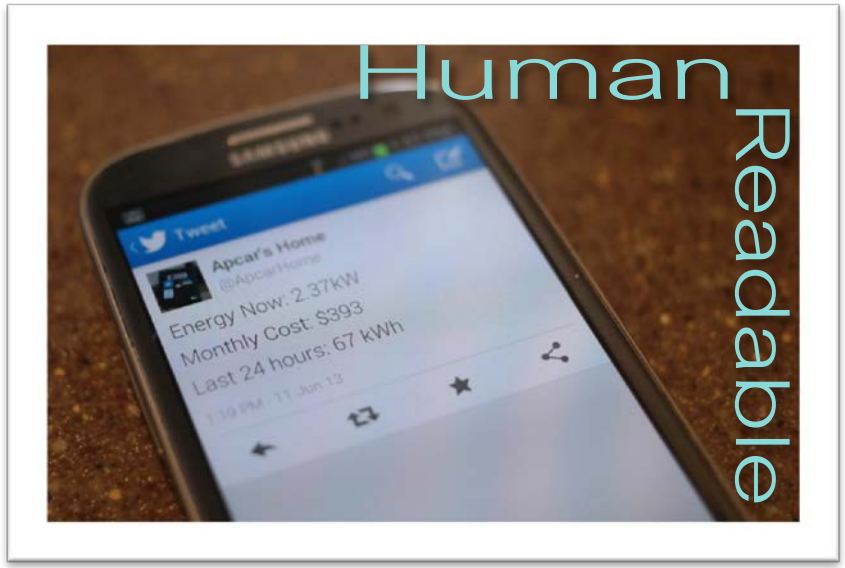
Some Food For Thought…

Near Enough IS Good Enough IoT

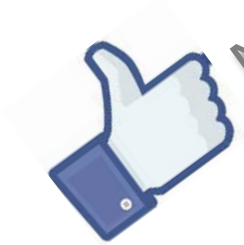
Social Media as the M2M Platform?

The old way...

Near Enough Is Good Enough IoT



Machine Readable XML



My House

Thank you.