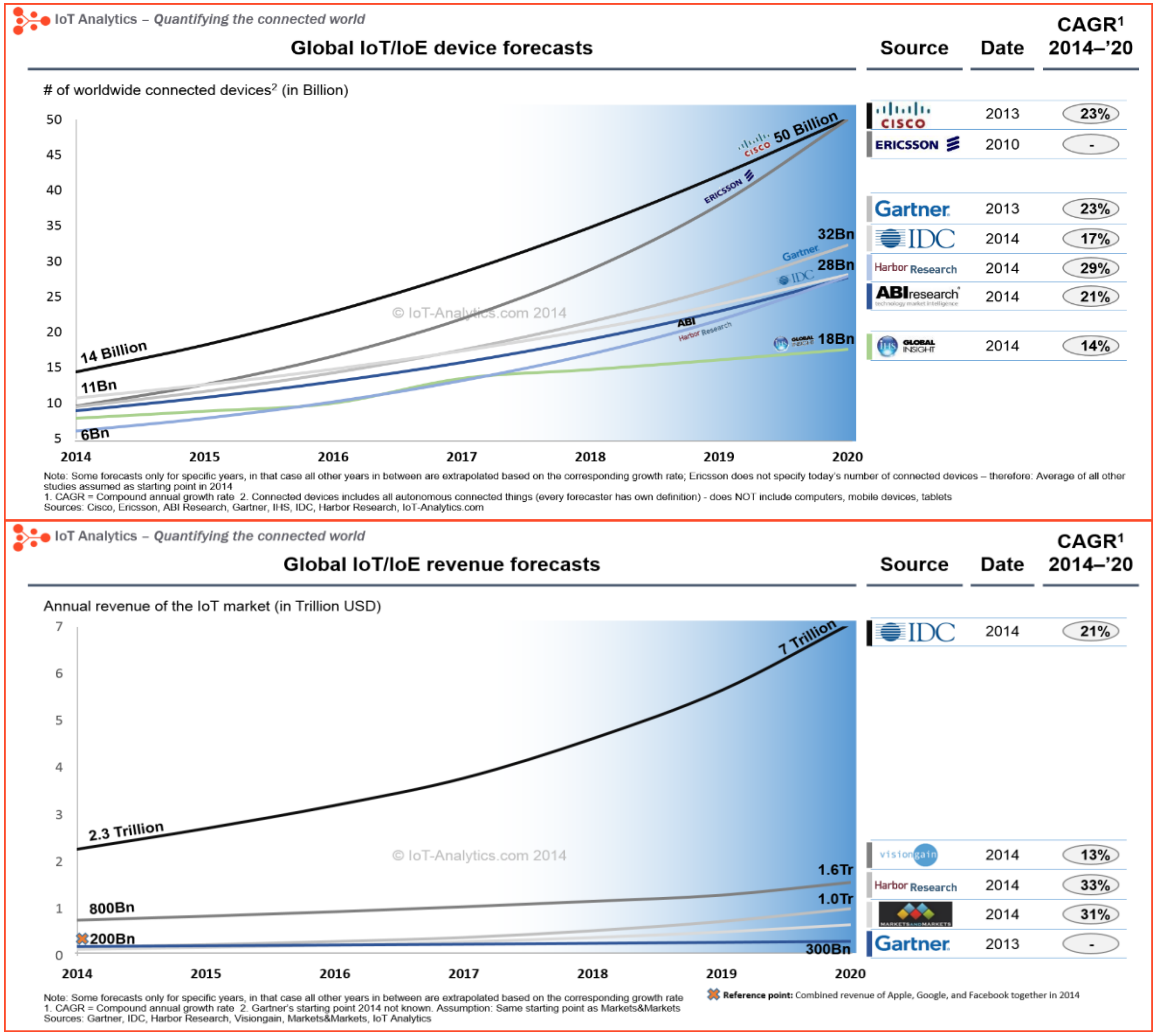
Managed Wireless and Internet of Things

UNIK4700 - Building Mobile and Wireless Networks

Maghsoud Morshedi

IoT Market



https://iot-analytics.com/iot-market-forecasts-overview/

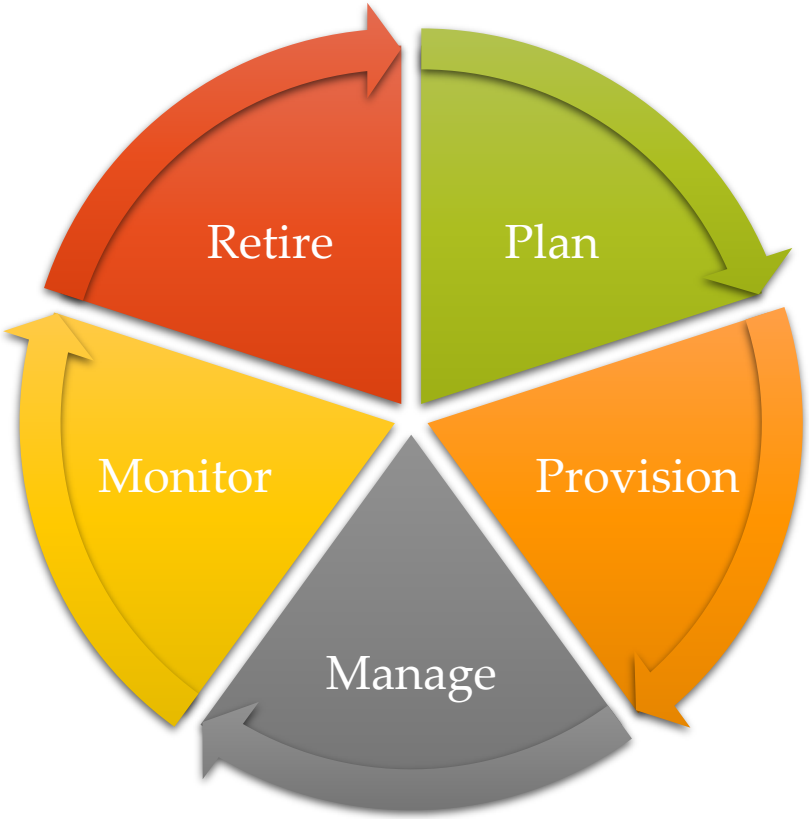
IoT Management Advantages

- Remote provisioning
  - Register and configure many devices simultaneously
- Scalability
  - The platform can scale to manage millions of devices
- Monitoring and diagnostics
  - Minimize device downtime and unforeseen operational problems
- Software maintenance and update
  - Update and maintain device software remotely; allow agile developments
- Configuration and control
  - Force device to certain desired state based on the system it is connected; Reset device to known-good state
- Security
  - Manage security updates and configurations for many devices

IoT Management Challenges

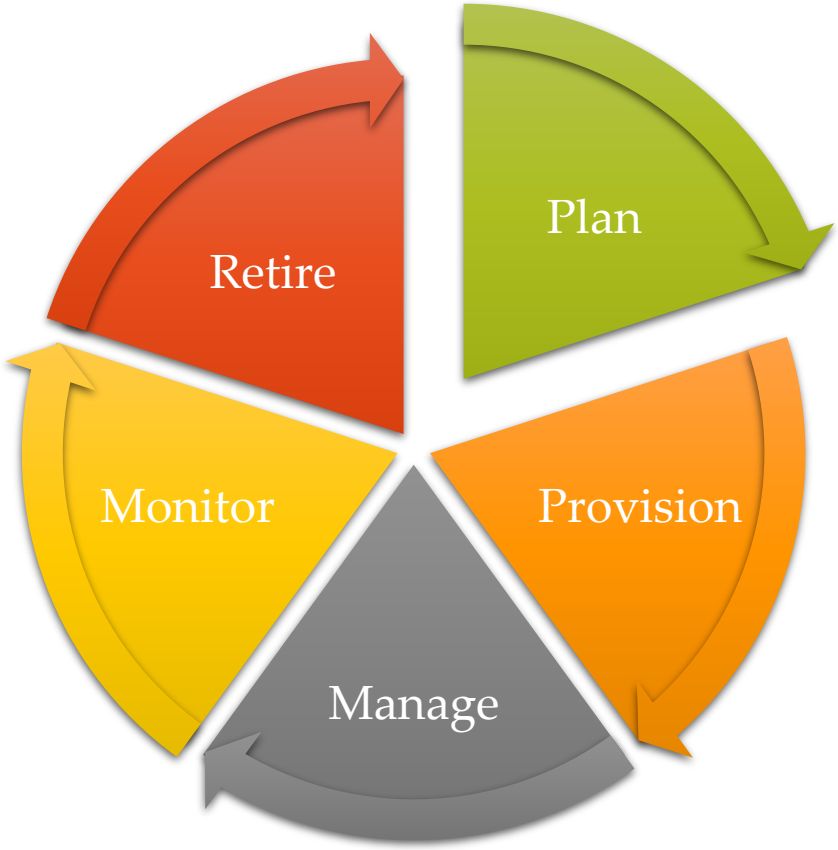
- Power and energy consumption
  - Many IoT devices need to run for years over battery.
- Connectivity
  - Varity of connectivity standards such as Zigbee, Zwave, Bluetooth, etc.
- Computation capabilities
  - Many IoT devices use low-end microchips with very limited capabilities.
- Lack of standard-Interoperability
  - Need to adapt management platform according to each deployed sensor type or manufacturer
- Security and privacy
  - Management platform security and privacy issues will affect millions of devices
- Storage Management
  - Store petabytes of information gathered from IoT devices
- No human-interaction interface

IoT Device Lifecycle



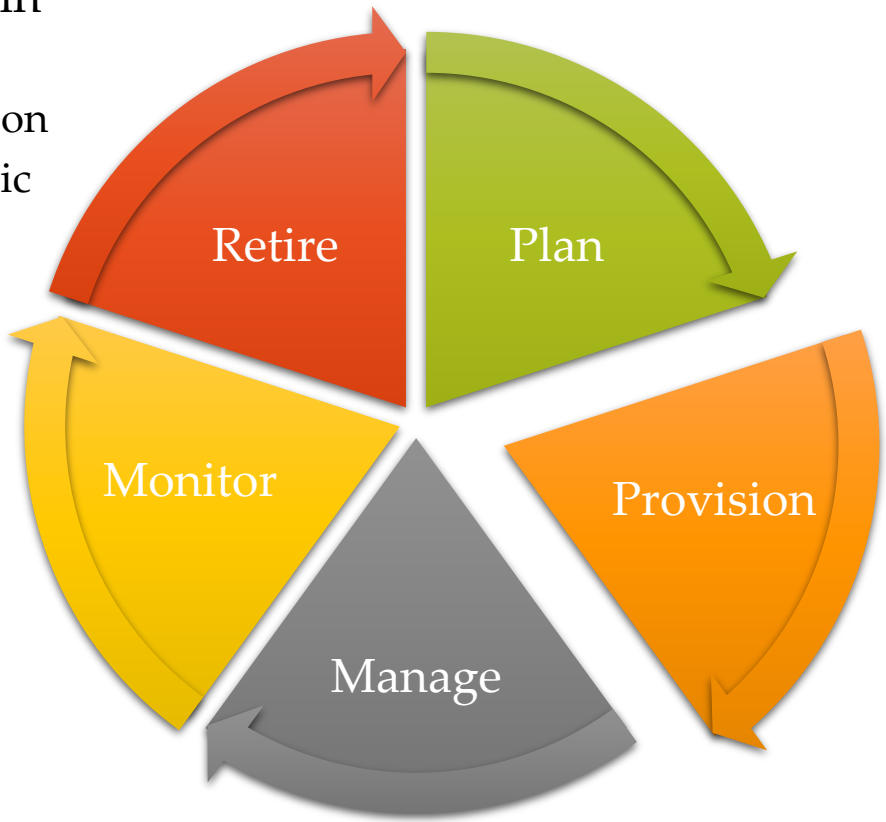
IoT Device Lifecycle-Planning

- Why do you want to manage IoT?
- Plan your IoT devices deployment based on your system requirements
  - Device naming scheme
  - Group devices
  - Define access control policies



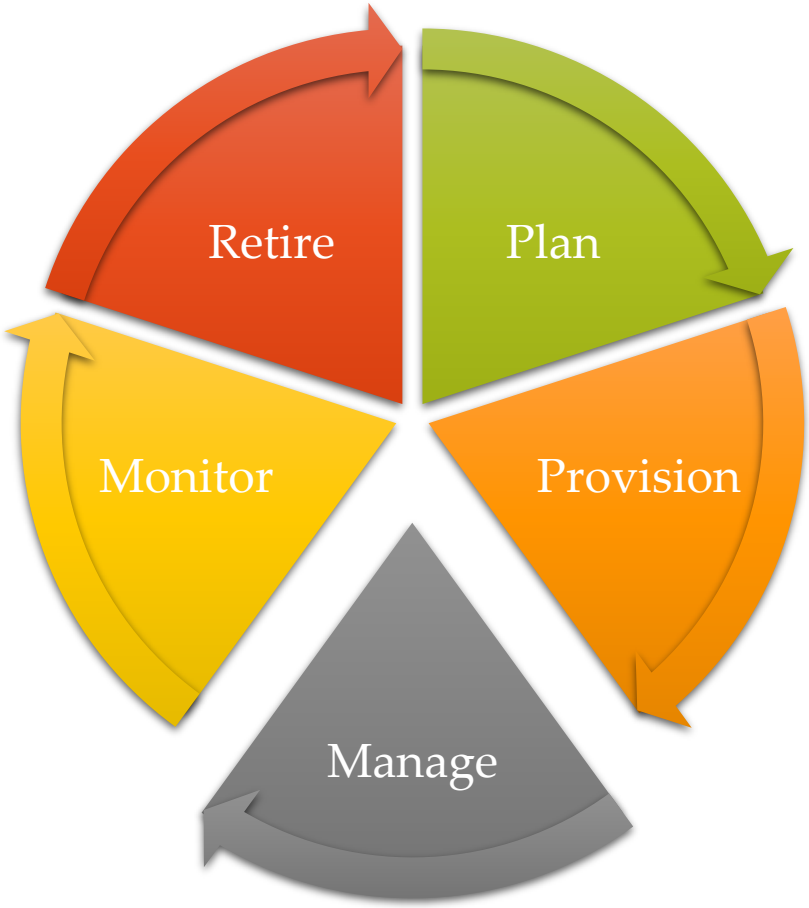
IoT Device Lifecycle-Provisioning

- Authenticate and register IoT devices in the management platform
  - Zero-touch authentication and registeration
  - Public key infrastructure (PKI)- IoT public key and certificate management
    - Key generation
    - Key expiration and reporting (different device different key lifetime)
    - Key destruction
    - Certificate revocation
- Provisioning scenarios
  - Ownership based
  - Geolocation based
  - Load balancing
  - Re-provisioning



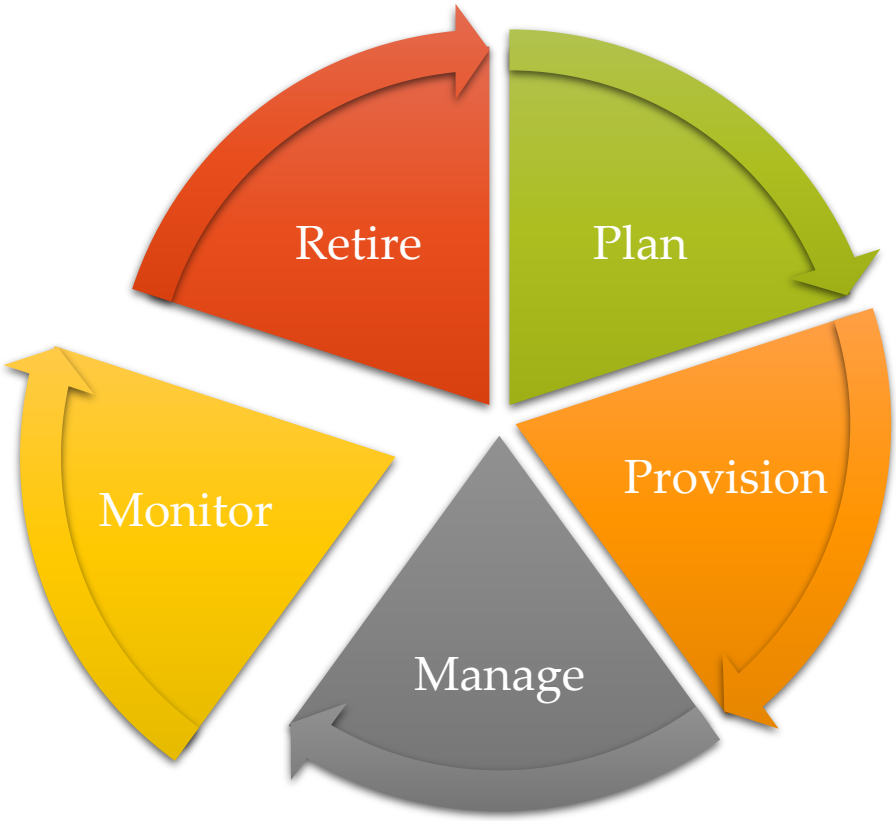
IoT Device Lifecycle-Management

- Force IoT device to a desired state
  - Device configuration
    - Assign IoT device to specific system
    - Change parameters value
  - Device update
    - Firmware update
    - Security update



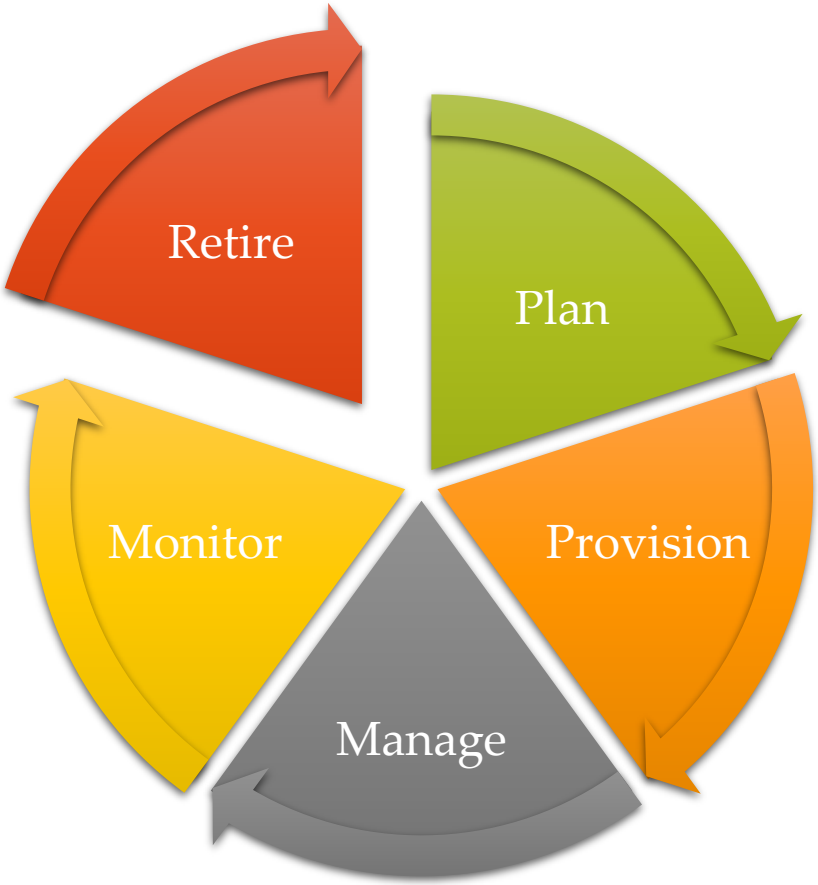
IoT Device Lifecycle-Monitoring

- Monitor devices health and state
  - Monitor device status
    - Wireless connectivity parameters
    - Resource consumption
    - Battery level or power consumption
    - Maintenance planning
  - Monitor security issues
    - Anomaly detection
    - Unauthorized access



IoT Device Lifecycle- Retirement

- Replace the failed device with new one
  - Device lifecycle is ended
  - Defective devices
  - Device failed
    - Re-provision new replaced device
  - Upgrade to a new model
    - New features and functionalities



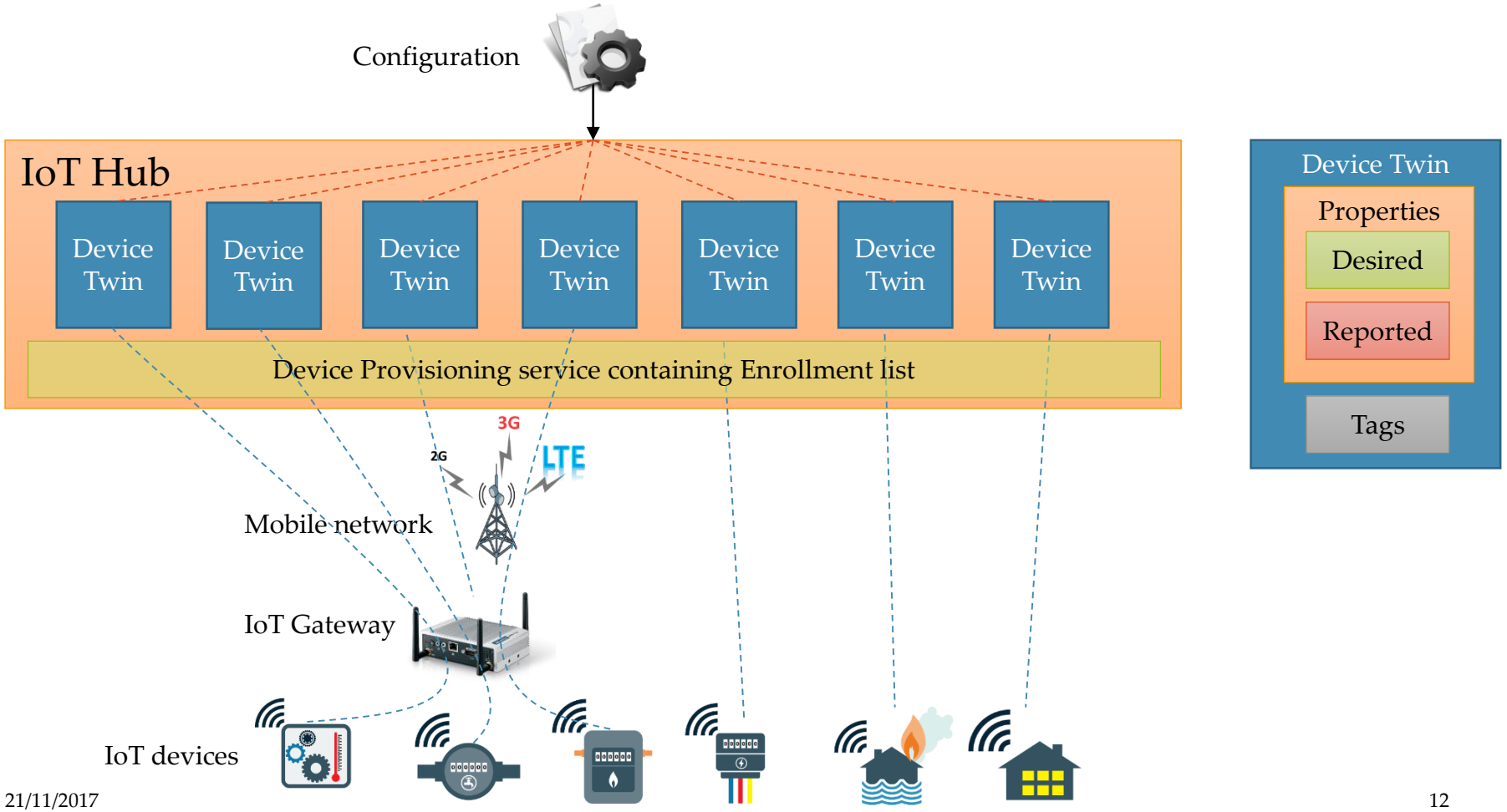
Recap: Conventional system administration tools

- Configuration management
  - Puppet
  - Chef
  - Ansible
  - Kubernetes
- Software defined networking (SDN)
- Open standard management protocols
  - NETCONF+YANG
  - CPE WAN management protocol (CWMP)

Can we use conventional system administration tools for IoT management?

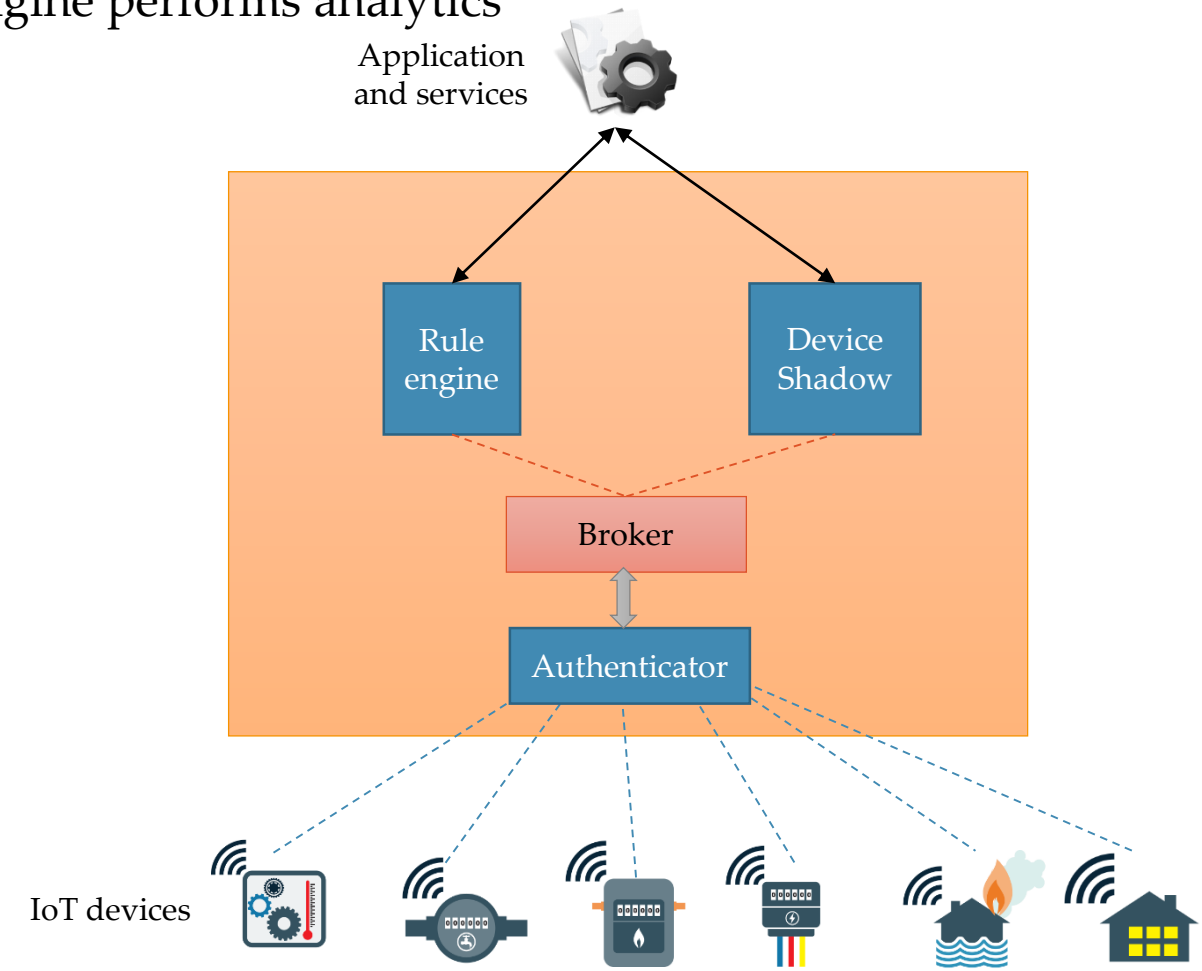
State of the art IoT platform 1

IoT devices connect to platform through IoT hub



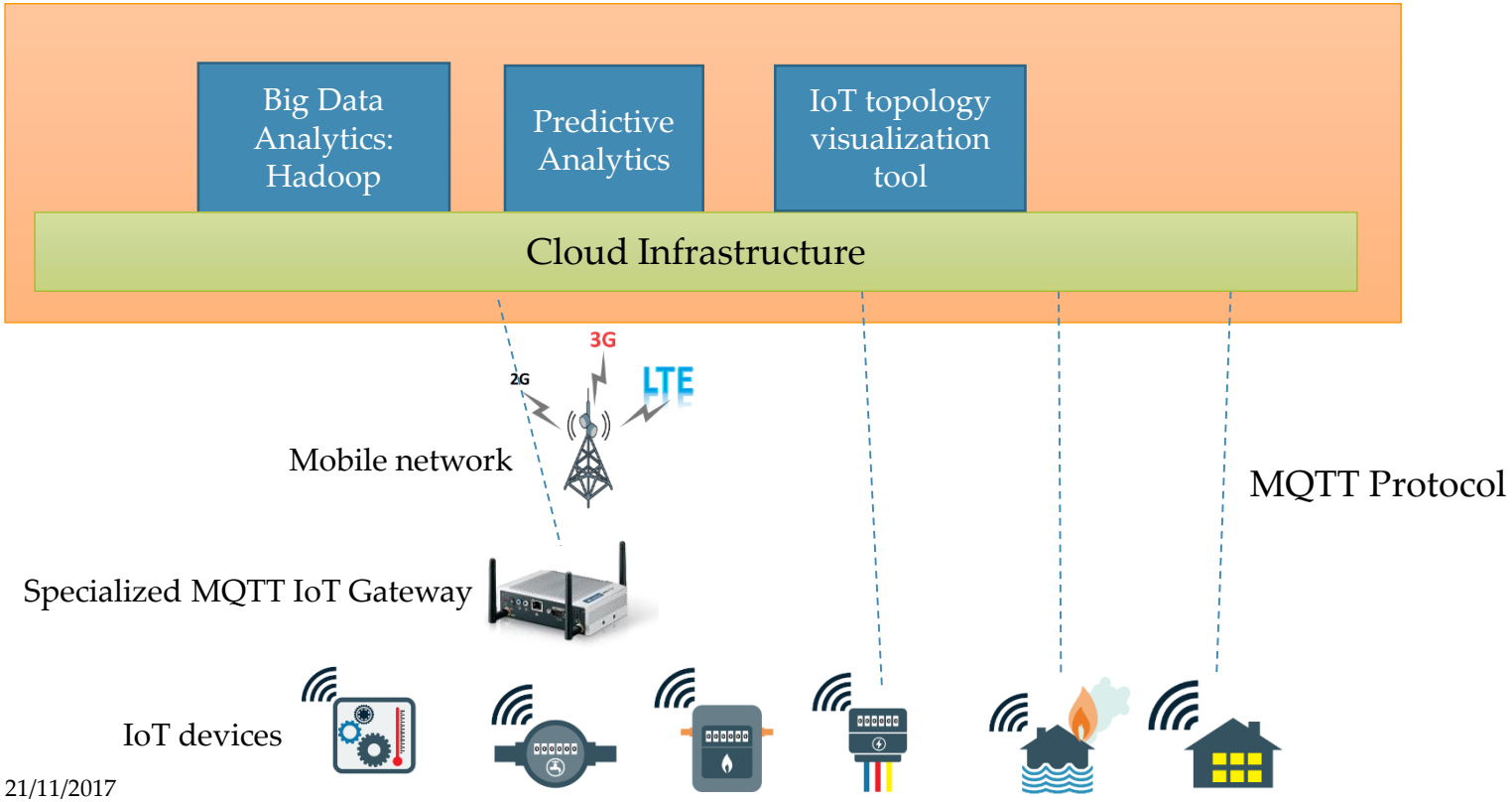
State of the art IoT platform 2

- Device shadow is metadata store for device capabilities
- Rule engine performs analytics



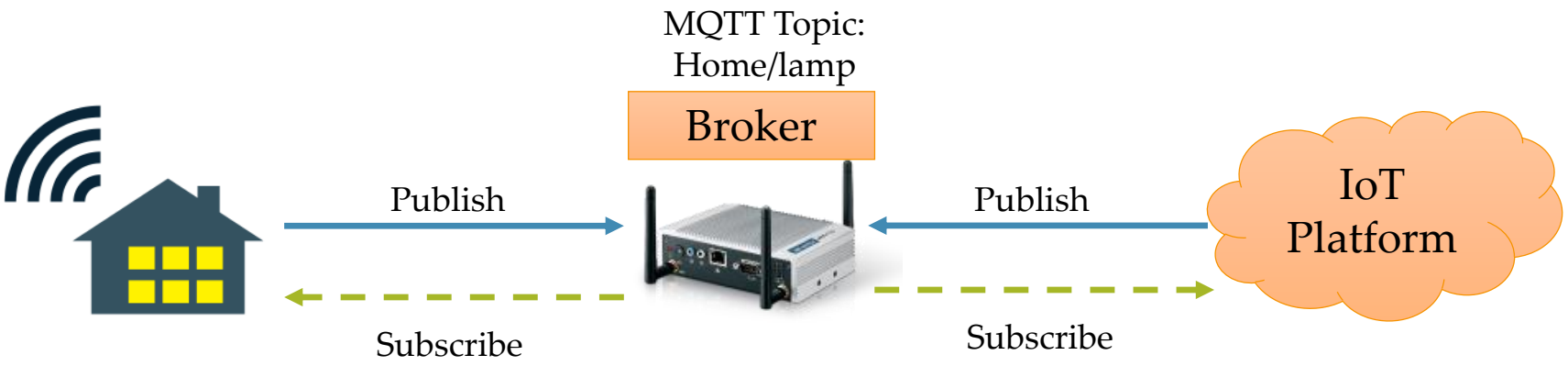
State of the art IoT platform 3

- Platform managed IoT devices through specialized gateway
- Platform managed specific IoT devices directly
- MQTT is main protocol connecting IoT to platform



MQTT Protocol – MQ Telemetry Transport

- MQTT is real-time protocol connecting IoT to platform
- MQTT run over TCP/IP protocol
- Designed for limited bandwidth networks
- MQTT has small code footprint so it can run on limited capability devices
- MQTT uses publish and subscribe system
- MQTT topics
  - Interest for incoming messages
  - Specify where to publish



IoT wireless technologies

Technology	Frequency	Data rate	Range	Power	Cost
2G/3G	Cellular bands	10Mb/s	Several km	High	High
802.15.4	2.4 GHz	250 kb/s	100m	Low	Low
Bluetooth	2.4 GHz	1, 2.1, 3 Mb/s	100 m	Low	Low
LoRa	< 1 GHZ	< 50 kb/s	2-5 km	Low	Medium
LTE cat 0/1	Cellular bands	1-10 Mb/s	Several km	Medium	High
NB-IoT	Cellular bands	0.1-1 Mb/s	Several km	Medium	High
SiGFOX	< 1GHz	Very low	Several km	Low	Medium
Weighless	< 1 GHz	0.1 – 24 Mb/s	Several km	Low	Low
Wi-Fi (11 f/h)	2.4, 5	0.1-1 Mb/s	Several km	Medium	Low
WirelessHART	2.4 GHz	250 Kb/s	100 m	Medium	Medium
ZigBee	2.4 GHz	250 Kb/s	100 m	Low	Medium
Z-Wave	908.42 MHz	40 Kb/s	30 m	Low	Medium
EnOcean	< 1 GHz	120 Kb/s	30 m	Low	Medium

What to Monitor and Manage in IoT?

RSSI Sensors value SNR

Power consumption Transmit Rate

CPU utilization Memory Certificate

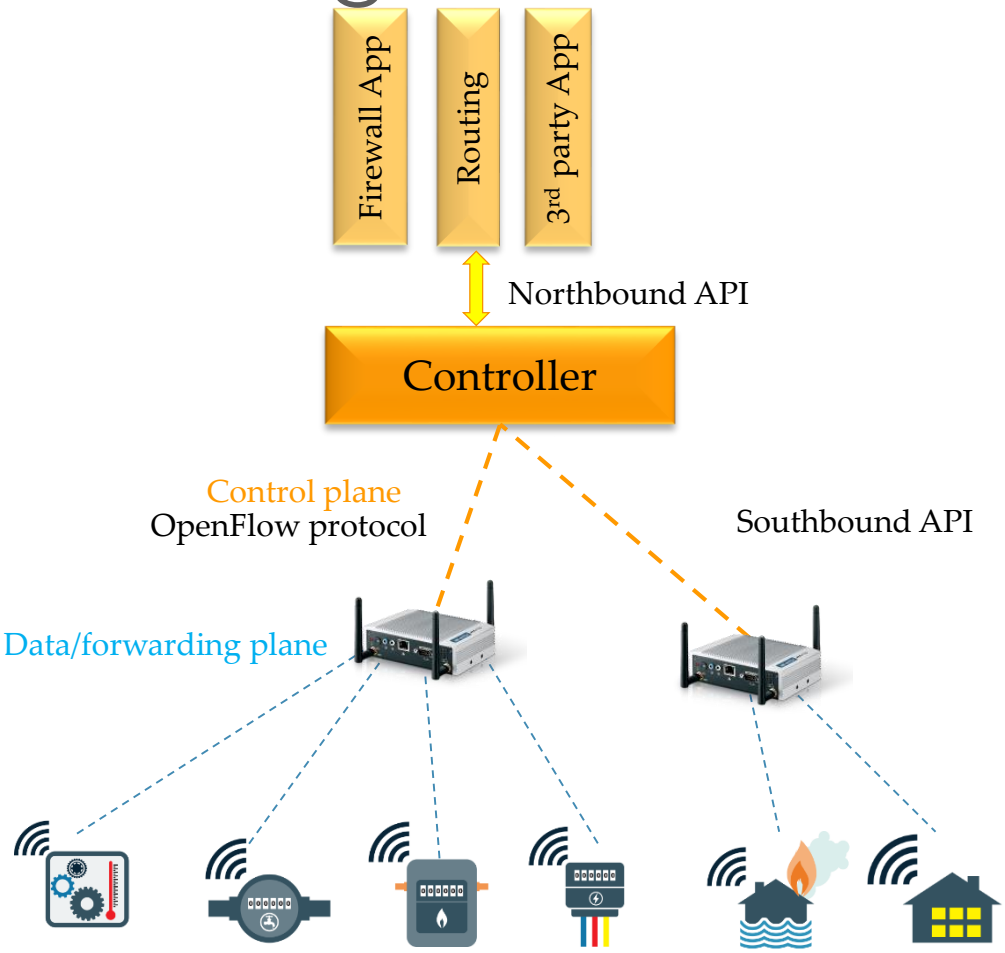
Receive Rate **Encryption key**

Security logs

Open Source IoT Platforms

- Kaa IoT Platform
  - Device monitoring, provisioning and configuration
- SiteWhere
  - Easily integrate development boards such as Raspberry Pi
  - Support different communication protocols and perform monitoring using Graphana
- ThingSpeak
  - Analyze and visualize data using MATLAB
  - Compatible with development boards such as Raspberry Pi
- DeviceHive
  - Install on public and private cloud
  - Supports big data solutions such as Elasticsearch and Apache Spark
- Thingsboard.io
  - Provides device management, monitoring, data collection and processing
  - Supports multitenant installations

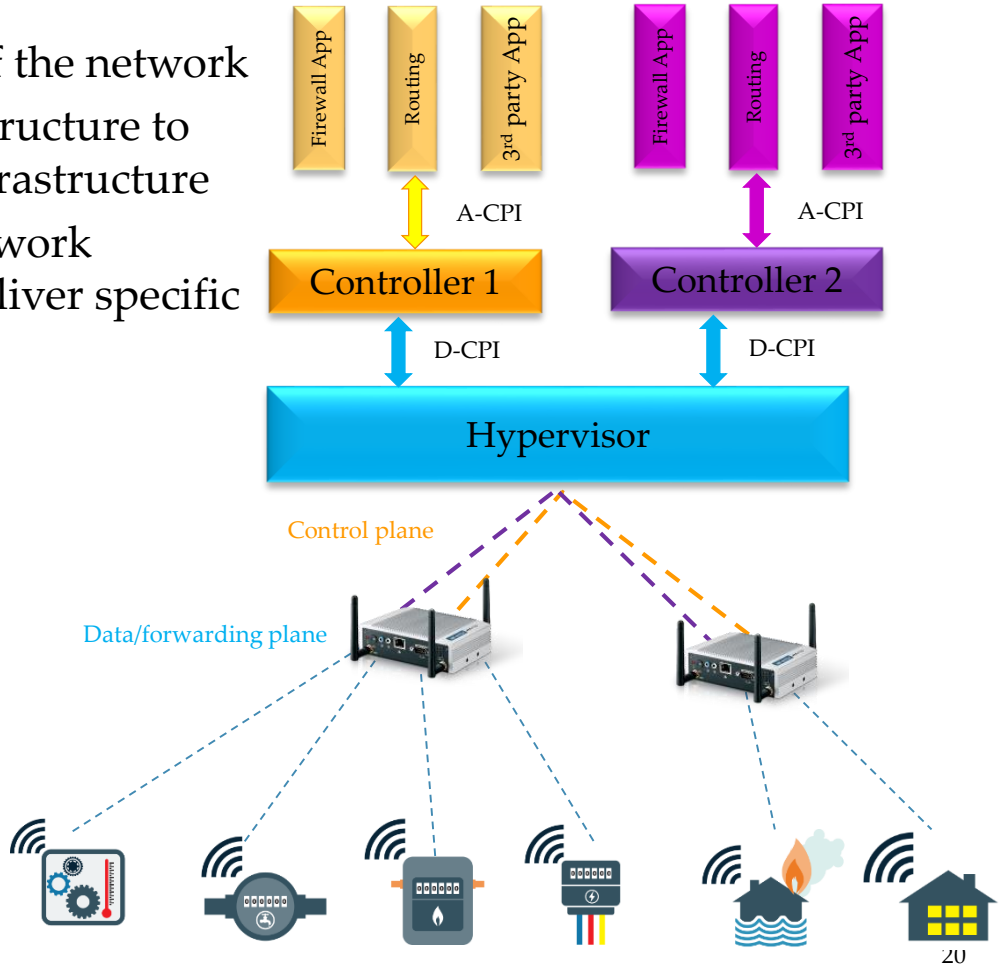
SDN for IoT Management



What would be optimal architecture of the SDN IoT management?
What would be monitoring time interval in SDN IoT management?

Virtualization of SDN

- Enabler for future IoT services
- Isolates different service providers
- Each vSDN corresponds to a slice of the network
- Virtualize given physical IoT infrastructure to allow multiple tenants share IoT infrastructure
- Each tenant can operate its own network operating system in controller or deliver specific services
  - Smart grid services
  - Remote management of smart home
  - Enabler for open data concept



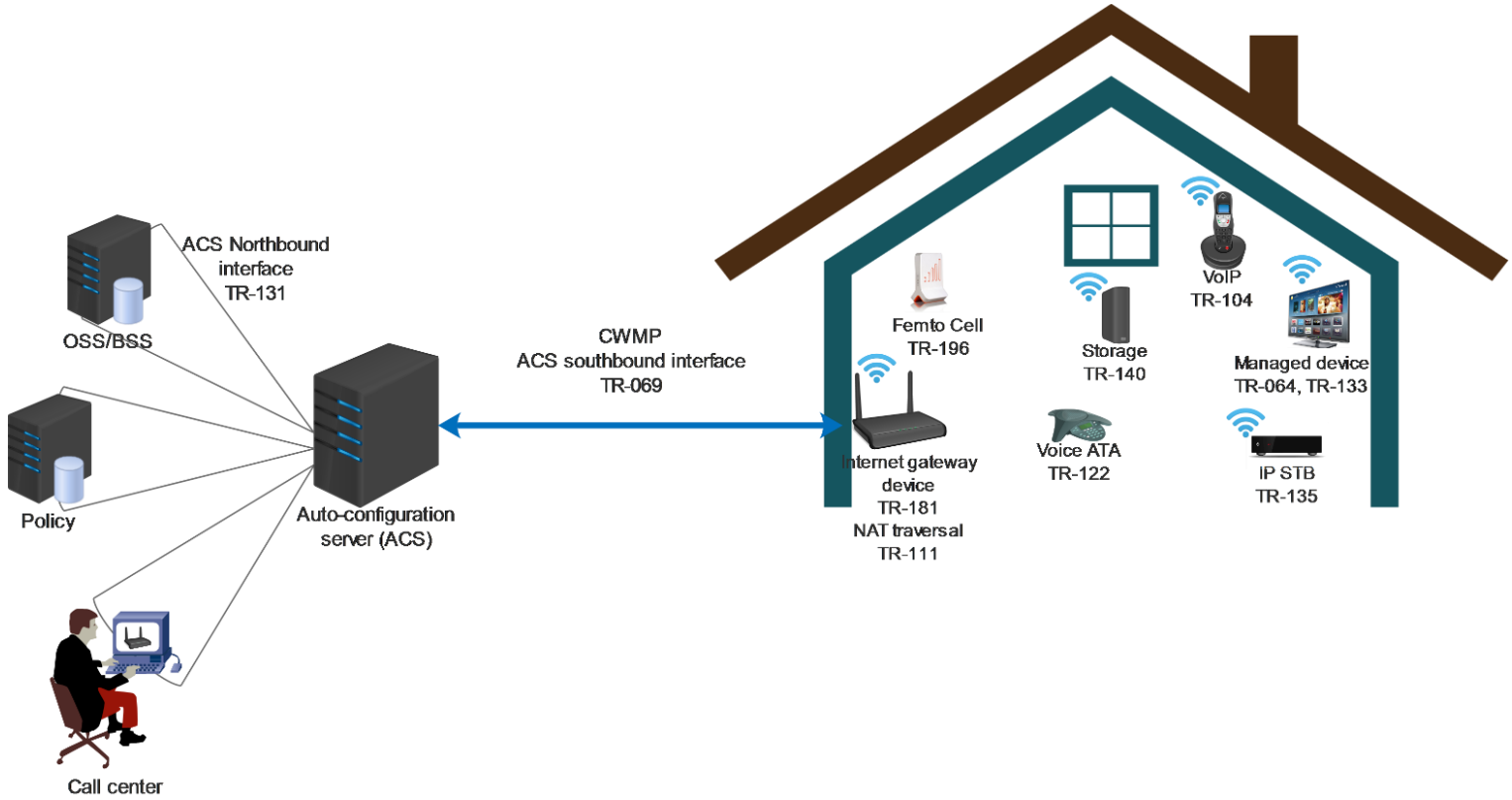
SDN and vSDN Challenges

- Latency overhead
  - Time from sending a packet into control plane, processed and send back to data plane to being forwarded
- Controller OF message throughput
  - Rate of messages that an SDN controller can process on average
- Controller response time
  - Time the SDN controller needs to respond to a message
- vSDN hypervisor throughput
  - Rate of messages that an vSDN hypervisor can forward on average
- Resource allocation of sensors to each vSDN tenant

What would be optimal architecture for SDN or vSDN IoT management?

CWMP Architecture

- Provisions CPE based on class of CPE such as vendor, software version or model
- Uses HTTP authentication and TLS to secure the communication between CPE and ACS



Recap: TR-069 Data Models

- Parameters of a different class of CPE are defined separately in a specific data model
- Each data model comprises a hierarchical set of parameters to define managed objects within a particular device or service
- data models enable the CWMP to manage remote devices based on their capabilities and set of parameters

Data Model	Description
TR-064	LAN side DSL CPE configuration
TR-104	Provisioning parameters for VoIP CPE
TR-111	Applying TR-069 to remote management of home networking devices
TR-106	Data Model Template for TR-069-Enabled Devices
TR-135	Data model for a TR-069 enabled STB
TR-196	Femto access point service data model
TR-317	Network enhanced residential gateway (SDN/NFV)

Recap: TR-069 Remote Management Requirements

1. All CPE should obtain an IP address in order to be able to communicate with an auto-configuration server (ACS)

2. When the CPE is behind the NAT or assigned a private IP address then only CPE can initiate connection otherwise the tunnelling mechanism should be used

3. The CPE must be able to discover the ACS through the URL of ACS or a preconfigured default ACS URL

4. The ACS URL must be in the form of HTTP or HTTPS

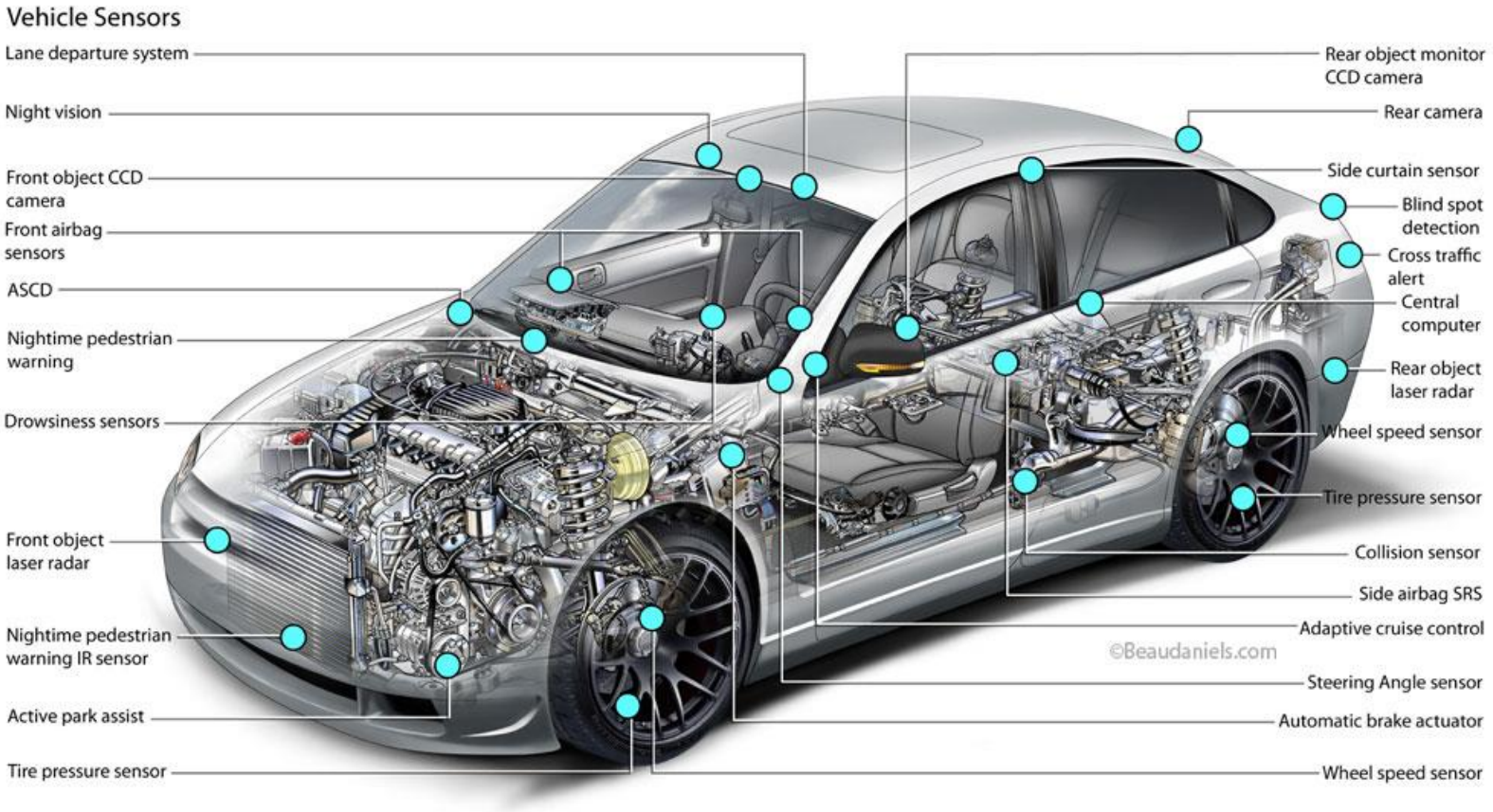
5. The CPE must support the uses of HTTP request, response and redirect in order to be able to communicate with ACS

Recap: TR-069 Implementation Challenges

1. The remote device should be capable of performing TR-069 client as an active process
2. Most of consumer-grade wireless access points used at home have limited capability to send statistics less than 15 minutes intervals.
3. Different devices require different data models due to their different use cases and parameter set
4. The auto-configuration server should use the HTTPS in order to secure data transfer to/from remote devices
5. Using certificates for HTTPS, operator should implement a certificate management platform in order to monitor certificates for expiration and audit, centralized certificate creation, re-provision a device with a new certificate (certificate rollover), recover certificates that are no longer operational (certificate escrow), certificate revocation
6. Different factors including traffic flows, network topology, available bandwidth, energy efficiency consideration, hardware, and software capabilities pose management challenges

IoT Management Example 1

- How do you manage sensors in following use case?



IoT Management Example 2

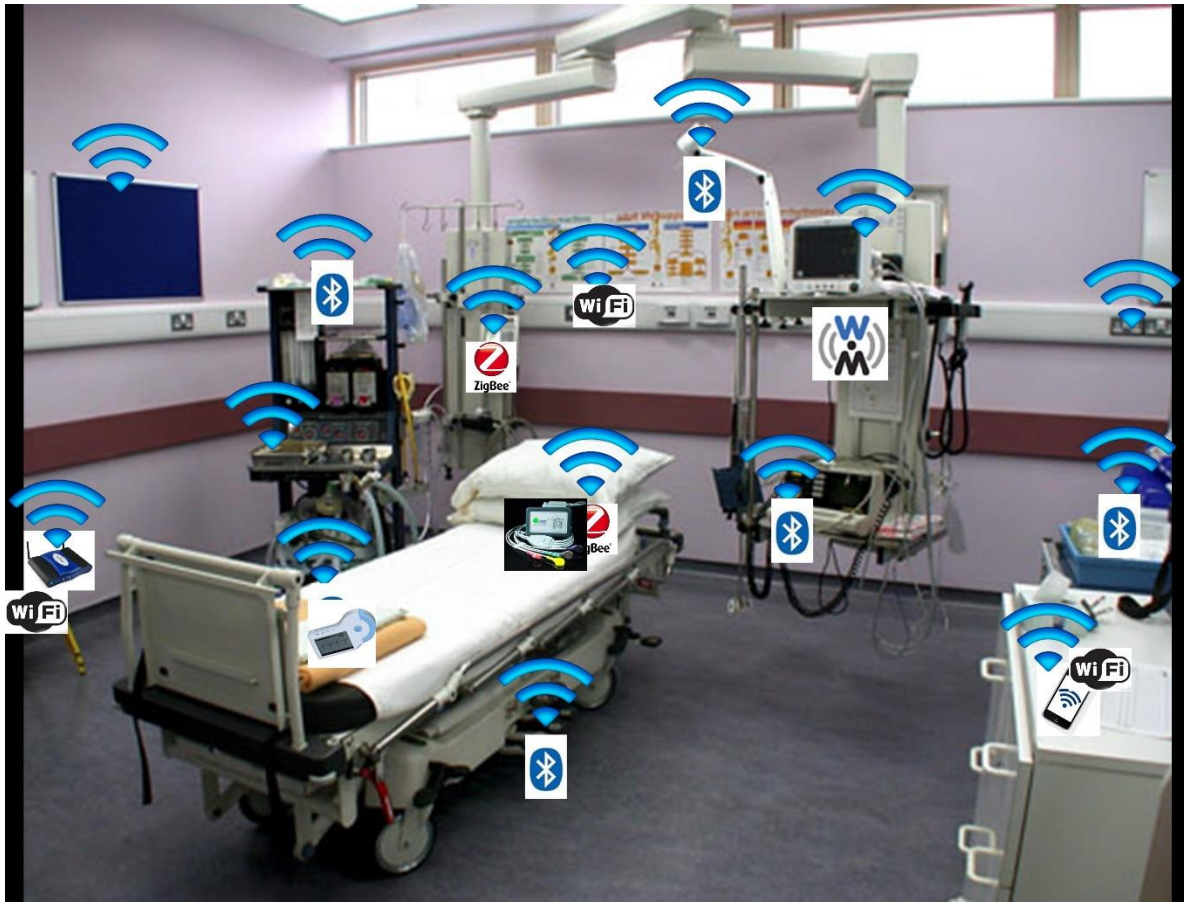
- How do you manage sensors in following use case?

IoT Management Example 3

- How do you manage sensors in following use case?

IoT Management Example 4

- How do you manage sensors in following use case?



Discussion

- Why should we monitor and manage IoT?
- What would be optimal monitoring time intervals for IoT?
- What would be optimal IoT management architecture (using gateway or direct connection)?
- Which approach will you use for IoT management in your infrastructure? (configuration management, SDN, open standard protocols or enterprise cloud platforms)
- What are the IoT management security and privacy consideration?


Q&A