Managed Wireless
and
Internet of Things

TEK5110- Building Mobile and Wireless Networks
Department of Technology Systems
University of Oslo

Maghsoud Morshedi, Josef Noll

Best Effort Wireless Networks Challenges

- Capacity
  - Lack of insight into access points impedes proper capacity planning and management .
- Scalability
  - Manually configuring and updating access points do not scale in large deployments
- Quality of Service (QoS)
  - Although wireless networks should support all connected clients, they should prioritize mission-critical applications
- Security
  - Identifying rogue nodes, APs, and gateways as well as isolating detected issues can cause significant configuration burden and operational costs
- Operational cost
  - Troubleshooting cost, training the staff to be enabled to configure and tune heterogeneous wireless devices pose significant cost

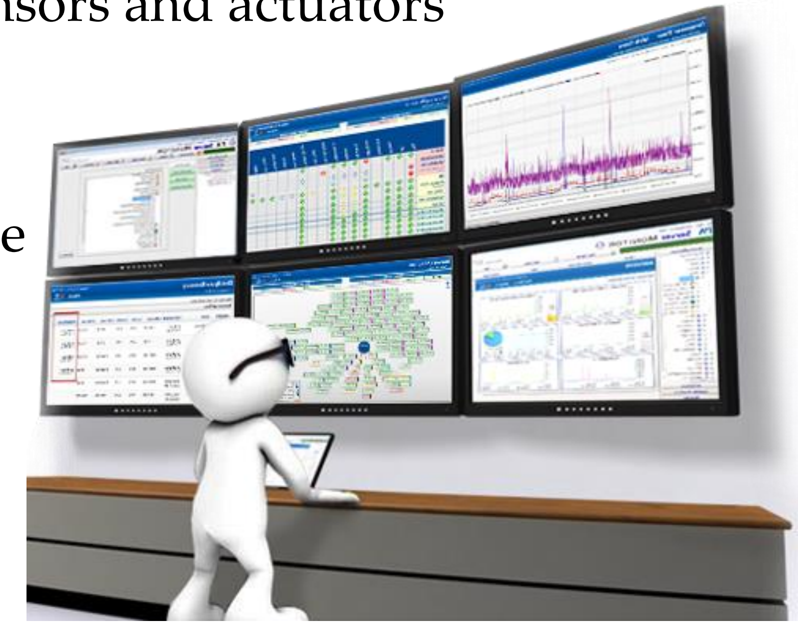
Impact of Best Effort Wireless Networks

- Technical support to the customers can impose a significant cost for service providers
- The service providers report that they approximately receive 50% of inbound technical calls related to wireless network [1]
- Send technicians to the location due to lack of insight, even though it can be possible to fix issue remotely
- Often hardware is replaced when the issue is not hardware related
- Too many repeated calls and technician dispatches

[1] ASSIA, "Deliver Real Quality of Experience to Wi-Fi Residential Subscribers," [Online]. Available: http://www.assia-inc.com/products/cloudcheck/

Remote Management

1. Simplify the service provisioning in wireless infrastructures
2. Real-time monitoring can detect wireless issues
3. Enable dynamic wireless network support
4. Control the sensors and monitor their unpredictable behaviour
5. Reduce the operational cost and improve interoperability of sensors and actuators
6. Secure the network against malicious activity by enforcing device security and restriction policies, isolating guest network from the private network and remote software/firmware update

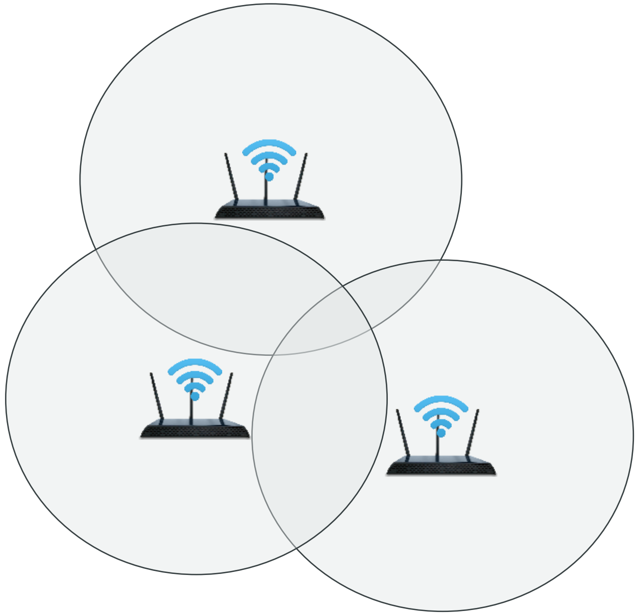


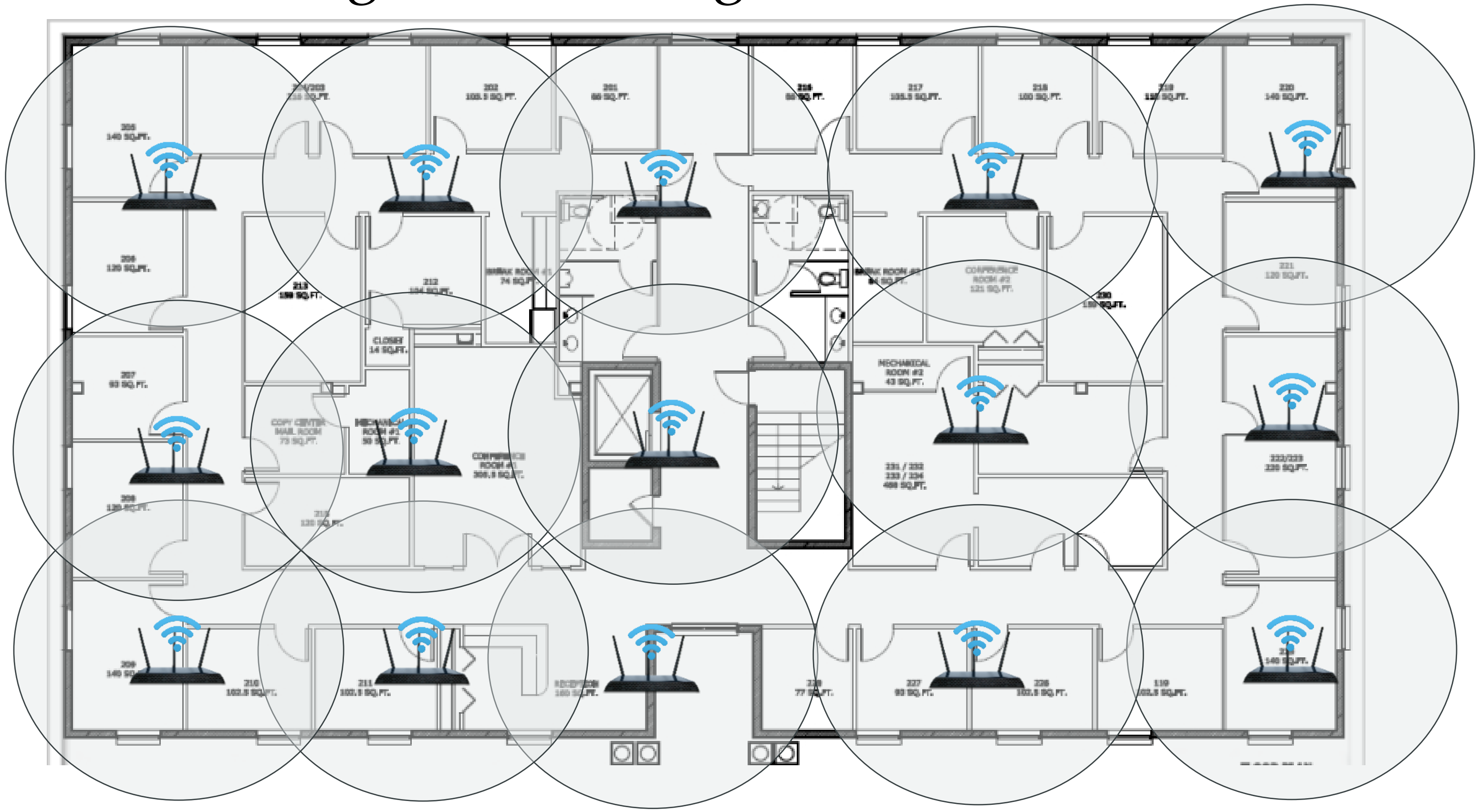
Build Your Wireless Networks

- When you buy a wireless equipment, what are the important factors?

Enhance our Wireless Networks

- How would you monitor and configure following networks?

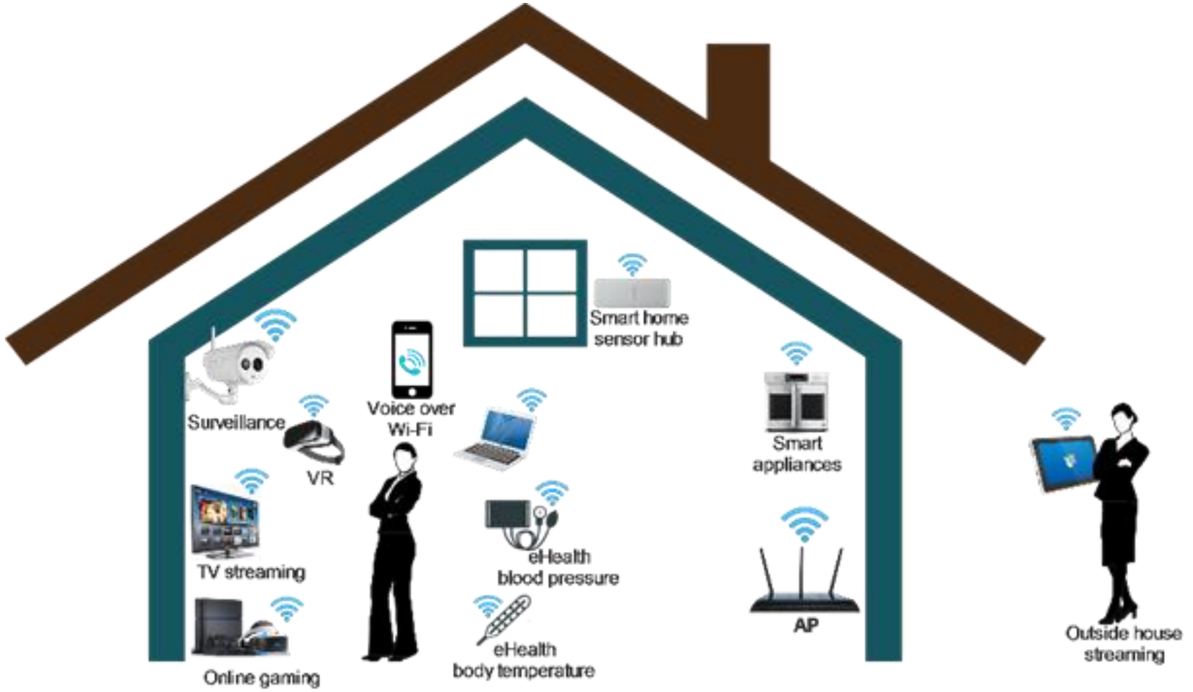




Managed Wireless

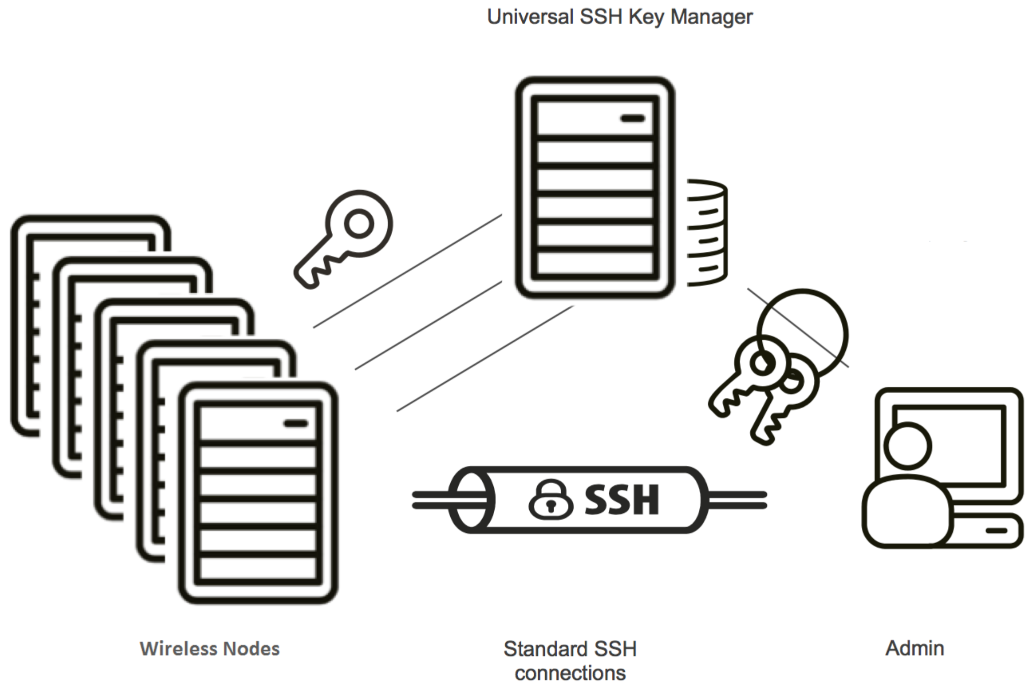
- Definition: A system that enables performance monitoring and configuration of the wireless system

- Different solutions
  - Remote managed wireless
  - Cloud managed wireless
  - Cloud controlled managed wireless



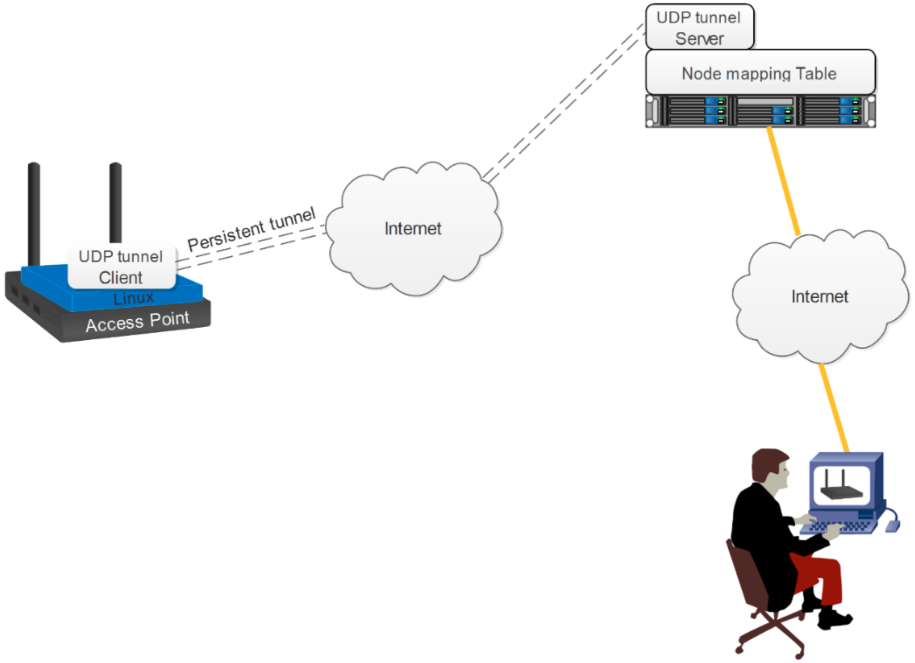
Remote Managed Wireless

- monitoring wireless performance as well as configuring the wireless devices with standard remote management systems such as TR-069, SSH.



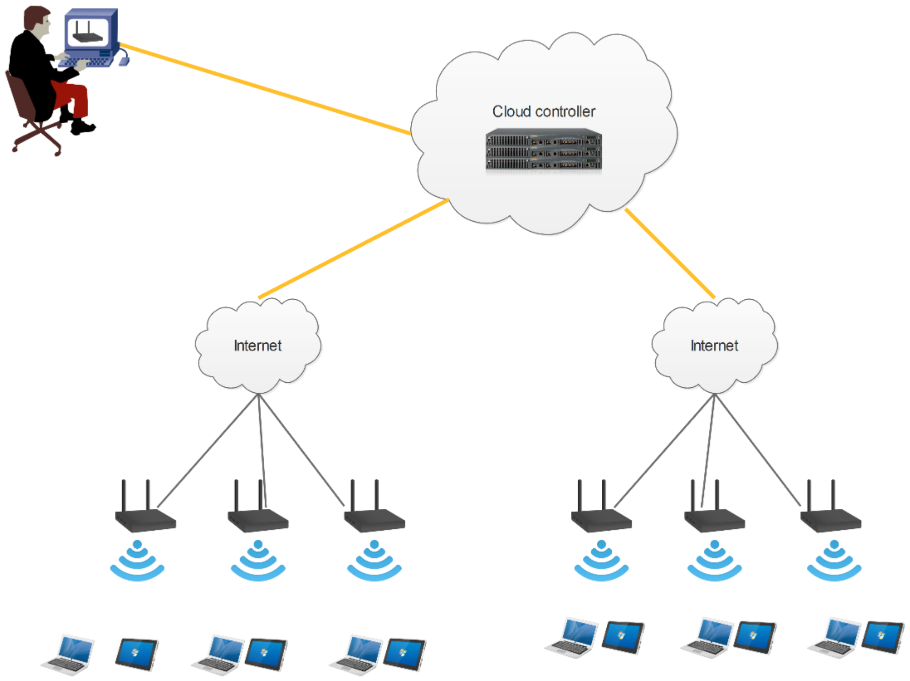
Cloud Managed Wireless

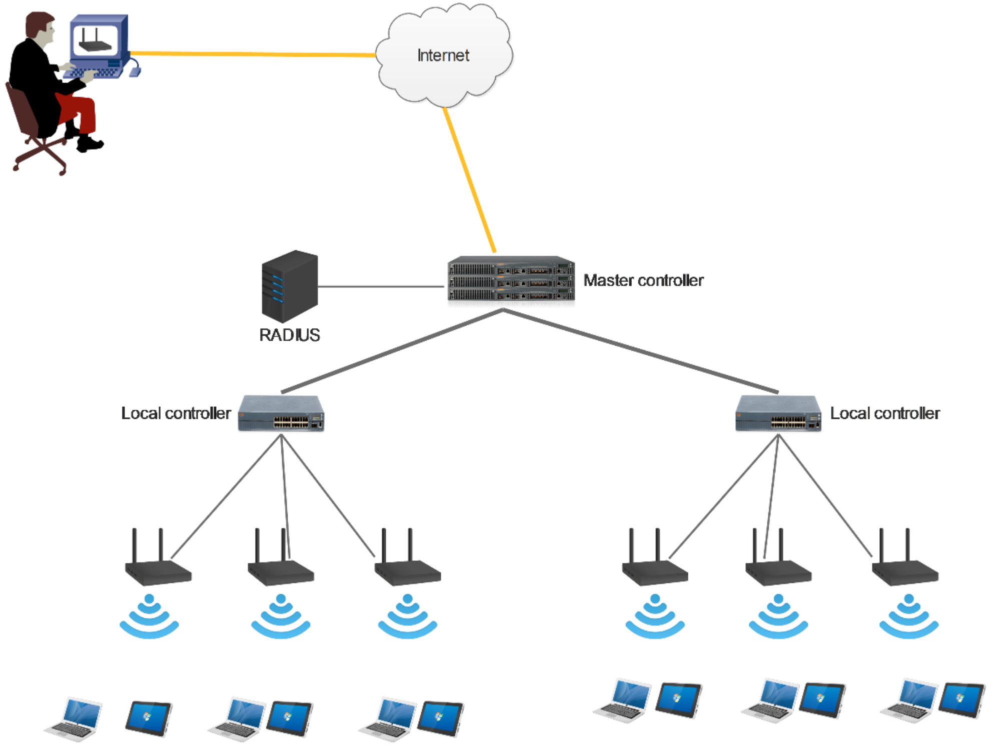
- Performing monitoring and configuration of wireless devices through the cloud dashboards such that wireless device downloads the configuration from cloud and execute it



Cloud Controlled Managed Wireless

- Placing the wireless controller in the cloud such that wireless device performs as a pure hardware and all the configuration and management resides in the cloud.





What to Monitor and Manage?

RSSI Queue length Delay SNR

Throughput Transmit Rate

Jitter Transmit power Airtime

Channel Receive Rate **Encryption**

Airtime Utilization Data volume Packet loss

Retransmission **Password length**

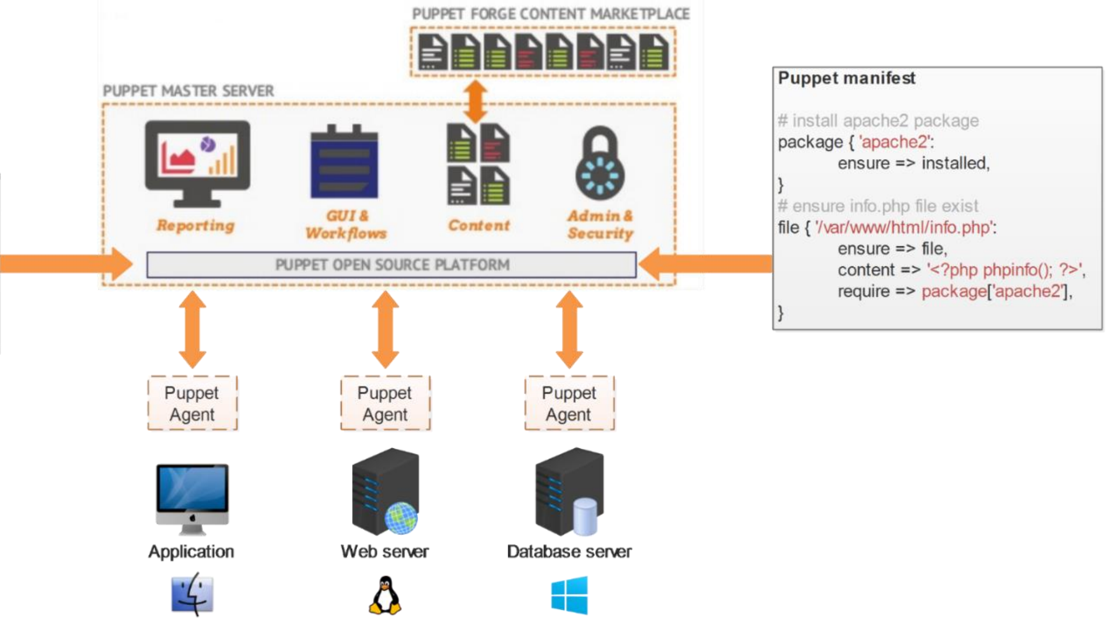
Conventional System Administration Tools

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

Puppet

- Require agent installation on remote devices using HTTPS
- Write manifest to manage remote hosts
- GUI interface using Foreman
- Supports Linux and Windows, MacOS
- There are modules to use Puppet in Android
- Open source and enterprise versions

Foreman

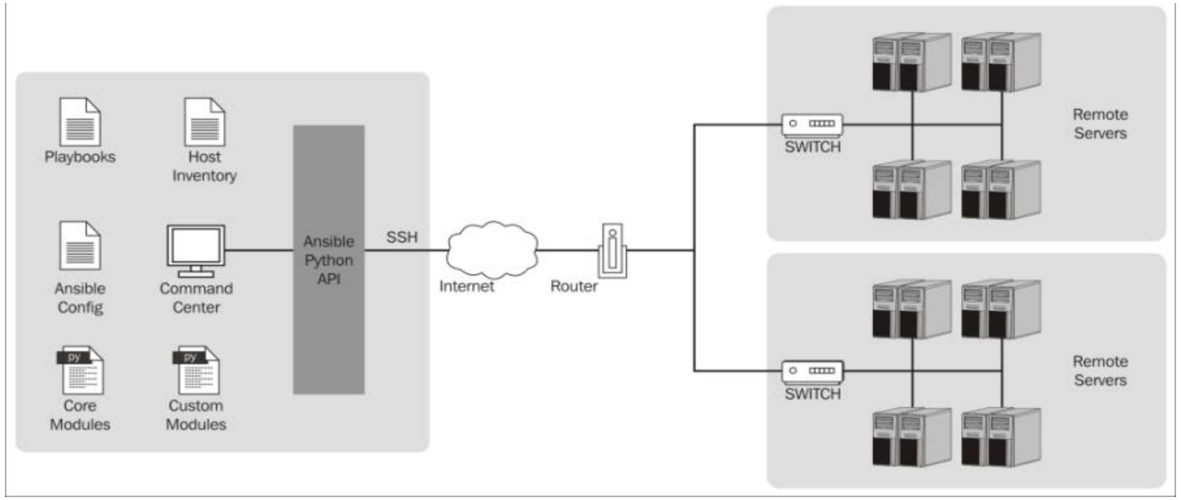


Puppet manifest

```
# install apache2 package
package { 'apache2':
        ensure => installed,
}
# ensure info.php file exist
file { '/var/www/html/info.php':
        ensure => file,
        content => '<?php phpinfo(); ?>',
        require => package['apache2'],
}
```

Ansible

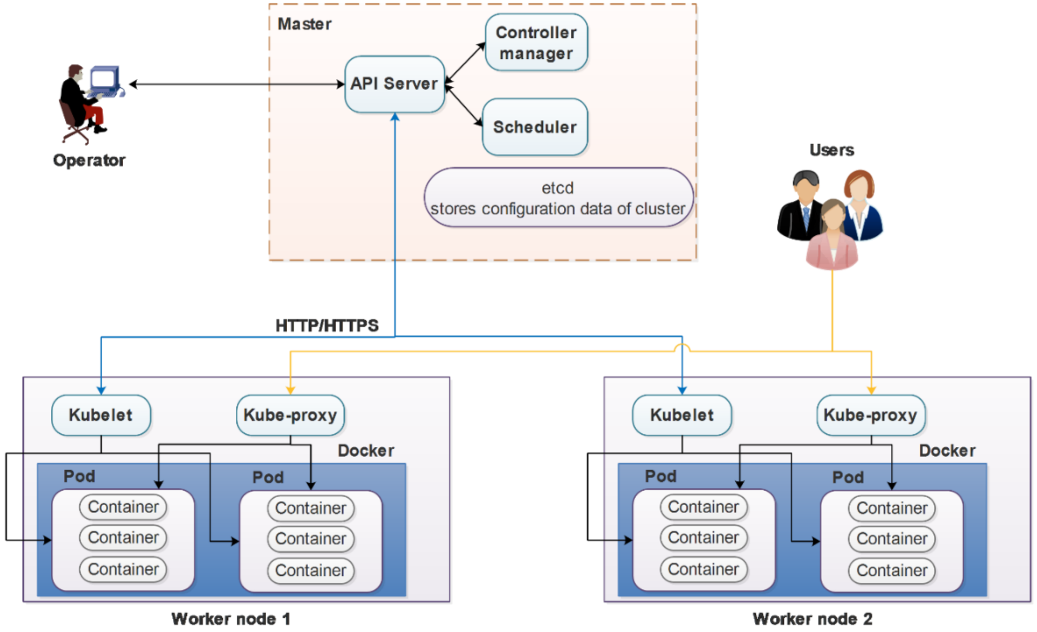
- Agent-less approach using SSH
- Write Playbooks to manage remote hosts
- Modules run on remote node to control resources and packages
- Provide modules for networking equipment produced by Cisco, HP, F5, Fortinent, etc.
- Supports operating systems that support SSH



https://www.packtpub.com/mapt/book/networking_and_servers/9781783550630/1/ch01lvl1sec09/the-ansible-architecture

Kubernetes

- Deploy and manage containers
- Pod represents group of one or more containers
- Kubelet is responsible for starting, stopping and maintaining containers
- Controllers create, update and delete resources they manage
- Scheduler tracks resource utilization of nodes



Configuration Management Tools for Wireless devices!?

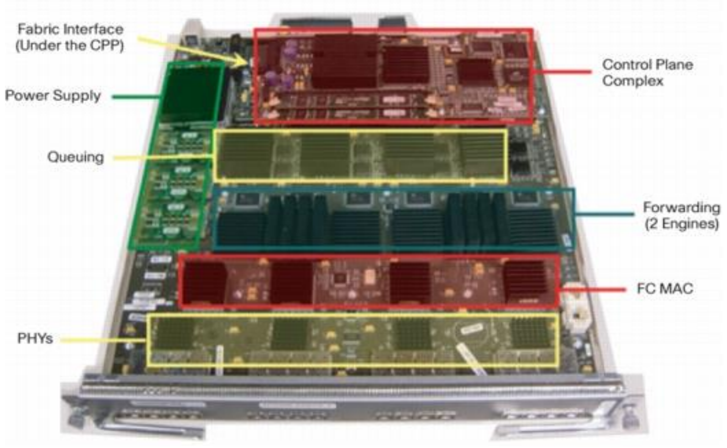
- Can we use Puppet to manage wireless devices?
- Can we use Ansible to manage wireless devices?
- Can we use Kubernetes to manage wireless devices?

Conventional System Administration Tools

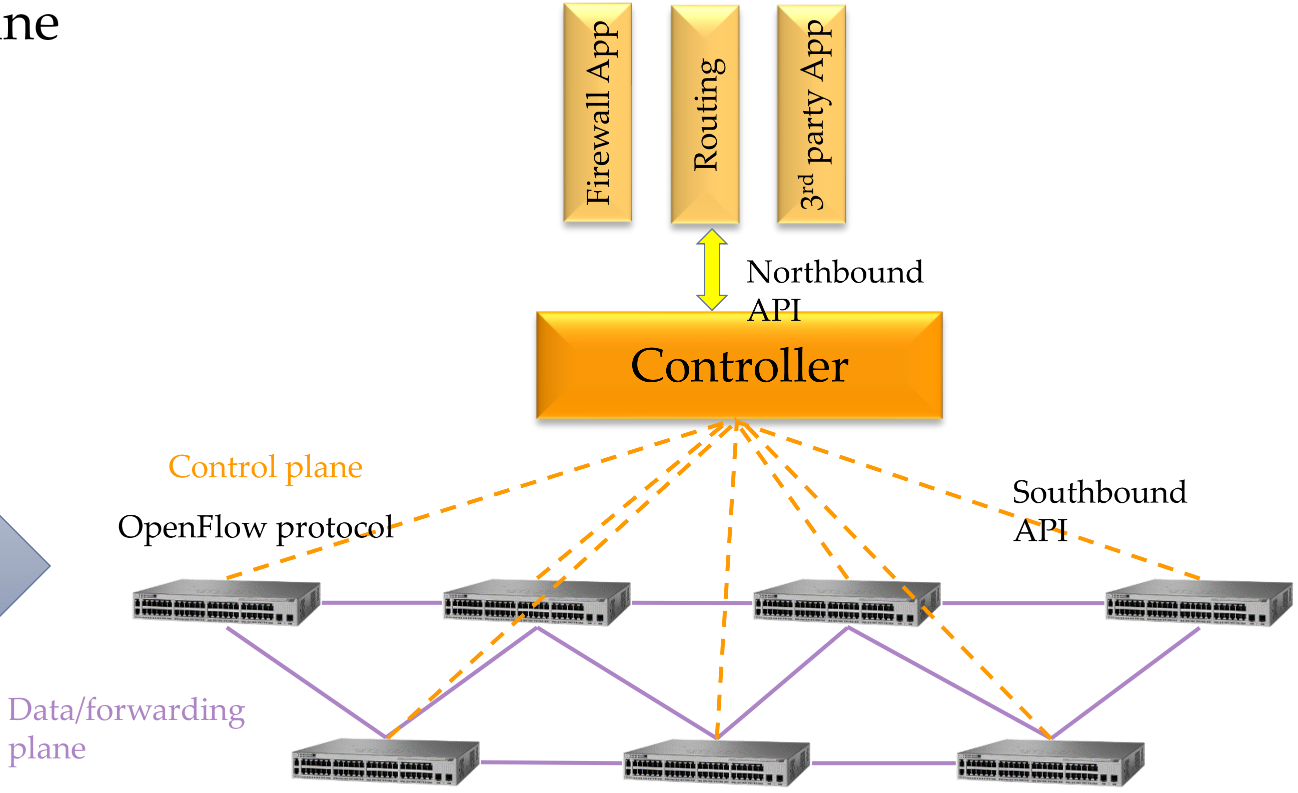
- Configuration management
  - Puppet
  - Ansible
  - Kubernetes
- Software defined networking (SDN)
- Open standard management protocols
  - CPE WAN management protocol (CWMP)

What is SDN?

- Software define networking (SDN) is developed to:
  - Separate control plane from data plane
  - Centralize network control
  - Define open programmable interfaces
  - Enable mobility

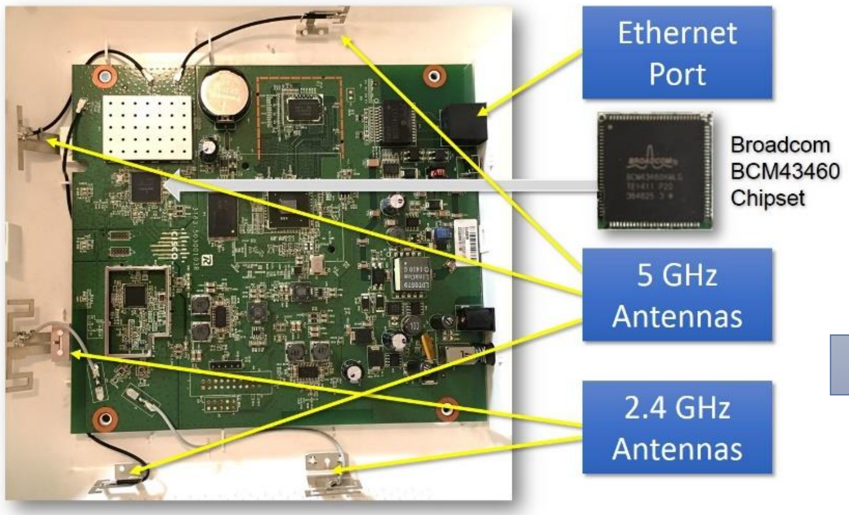


Cisco MDS9000 Family SAN Switch [1]

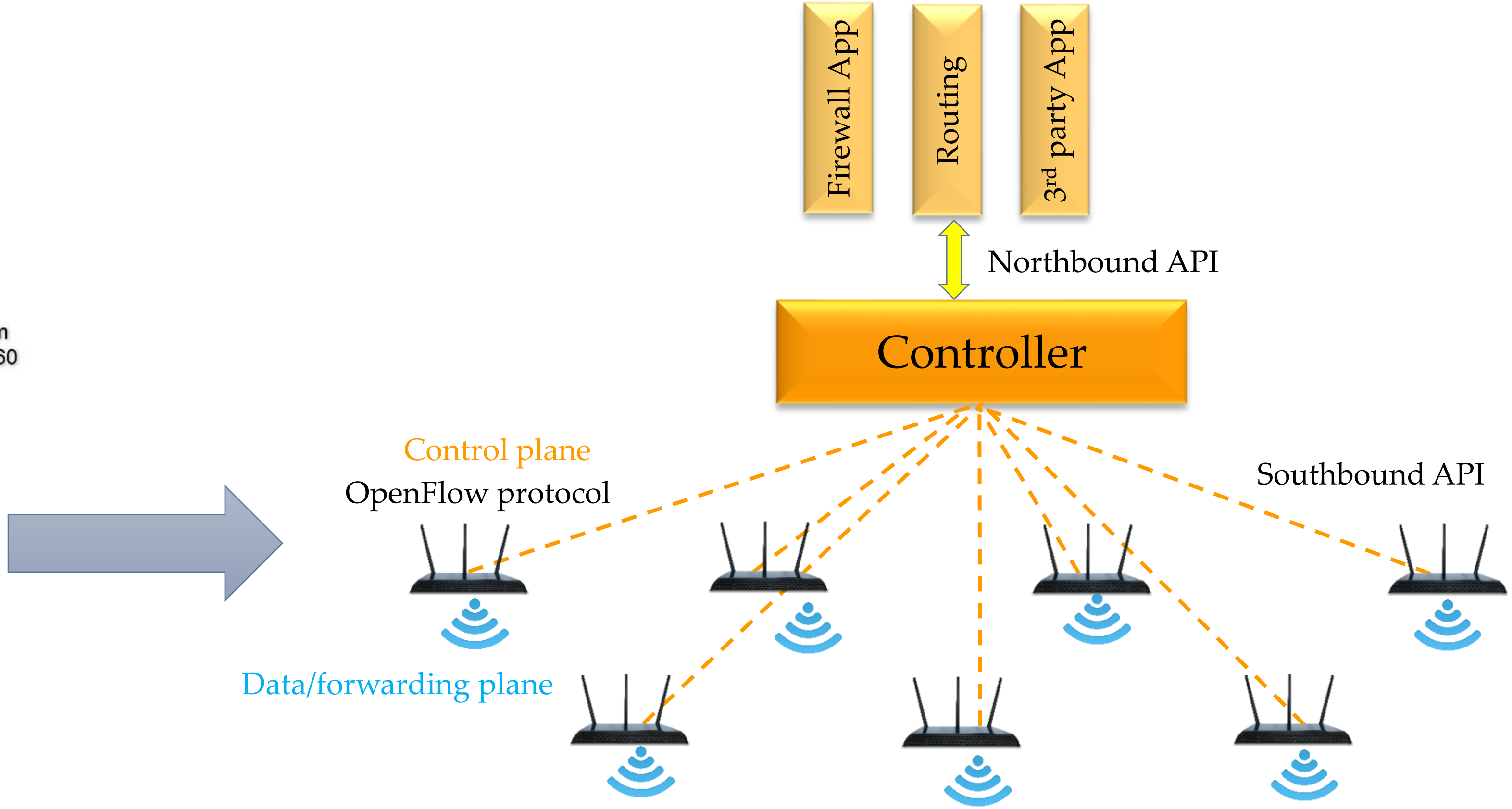


[1] https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/storage-networking-modules/prod_white_paper0900aecd8044c7e3.html

SDN with Wireless Access Points



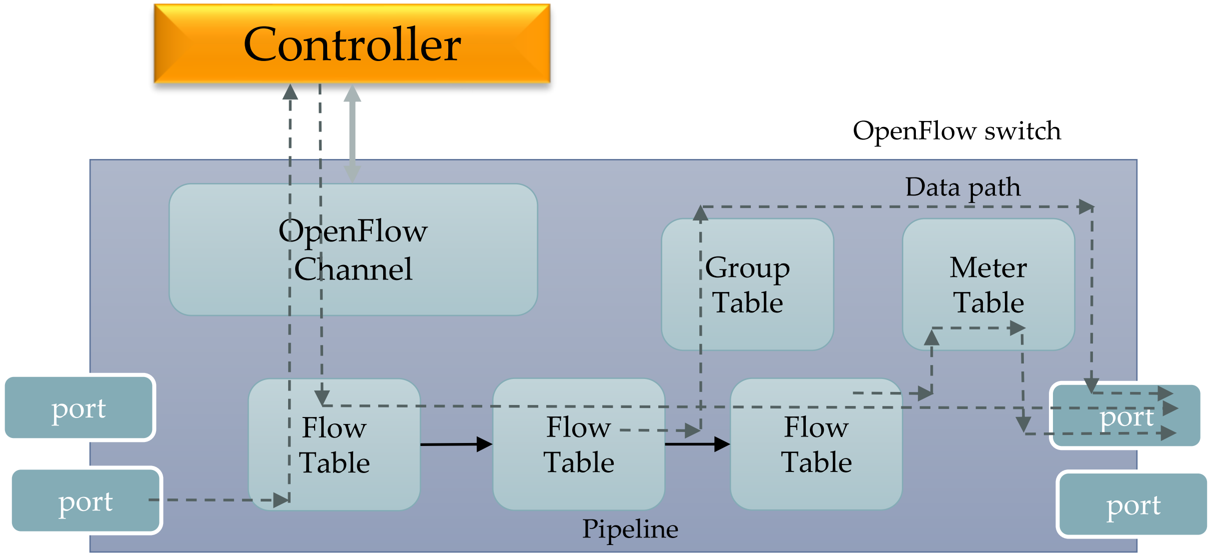
Cisco WAP371[1]



[1] http://www.tomcarpenter.net/2016/05/25/wireless-access-point-ap-internals-for-cisco-wap371/

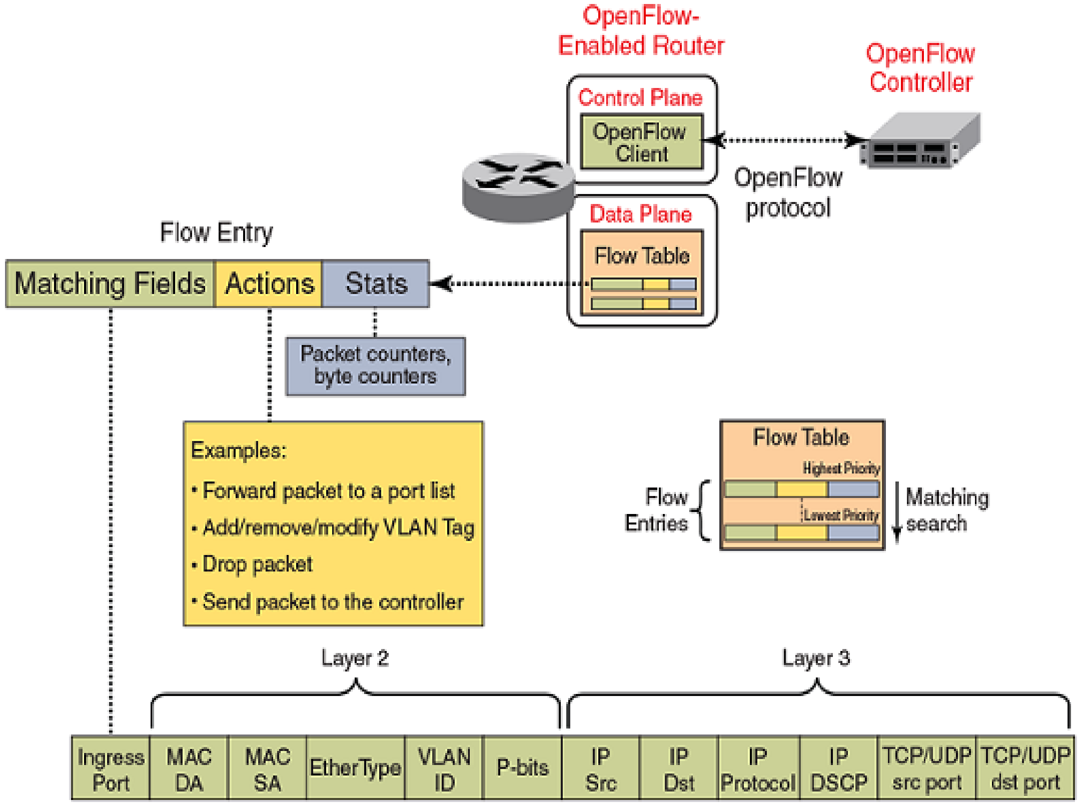
What is OpenFlow?

- OpenFlow is a key protocol in many SDN solutions
  - Separate control plane and data plane
  - Move control decision to separate controller, typically a standard server



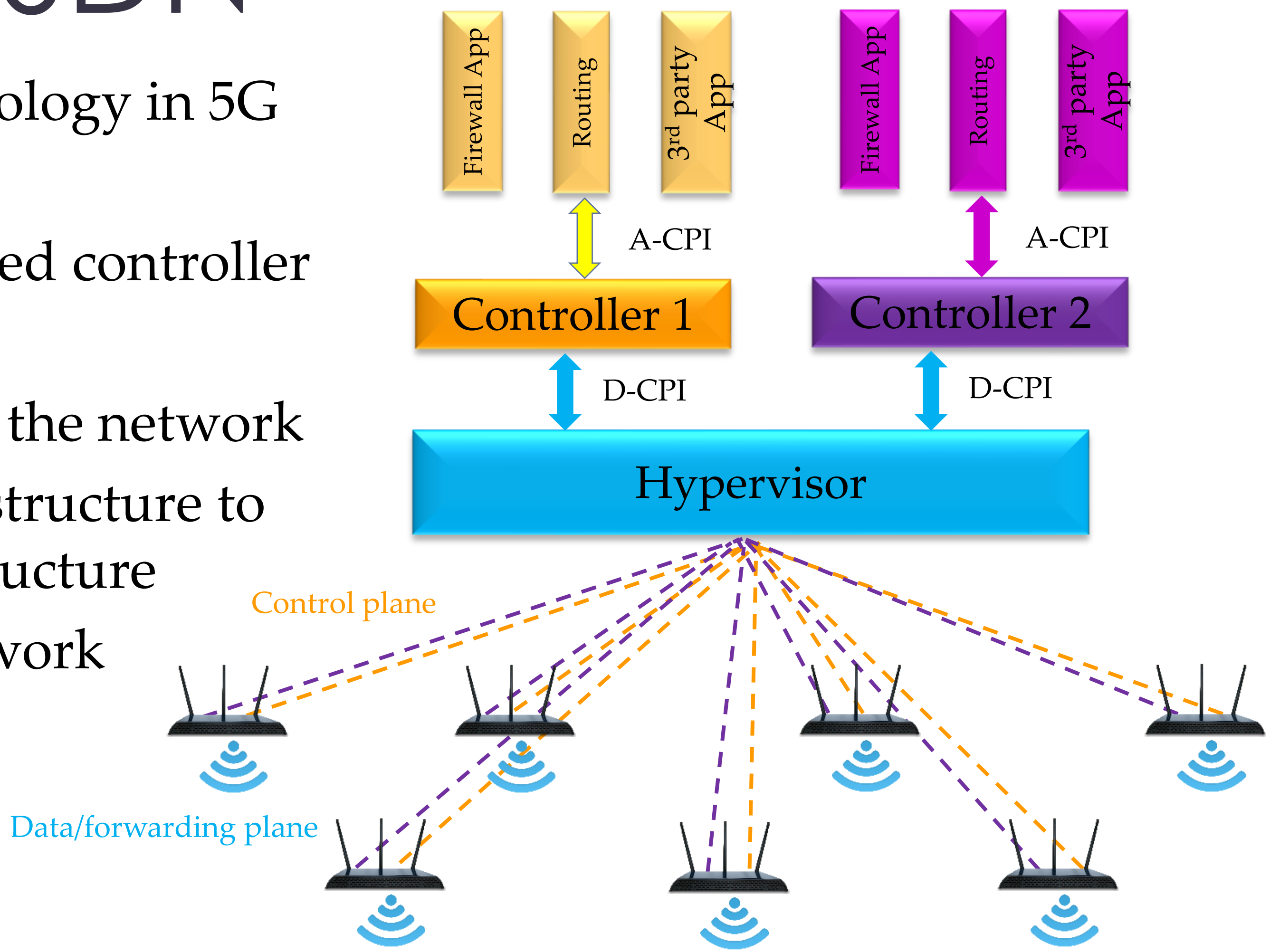
OpenFlow Components

- Flow table: forward packet to single port
- Group table: used for special actions such as multicast and broadcast
- Meter table: per-flow meters to implement QoS
- OpenFlow channel: exchange OpenFlow messages between device and controller
- Flow: defined as all the packets matching a flow-entry in a device’s flow-table.
- Flow entries: are quite general, and resemble ACL entries found in firewalls



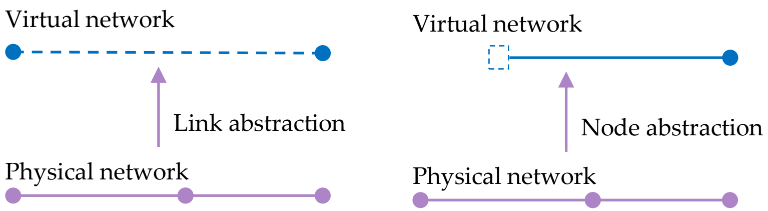
Virtualization of SDN

- Enabler for future networking technology in 5G
- Isolates different services
  - Video and voice can run on isolated controller
- Enable virtual SDN (vSDN) testbed
- Each vSDN corresponds to a slice of the network
- Virtualize given physical SDN infrastructure to allow multiple tenants share infrastructure
- Each tenant can operate its own network operating system in controller

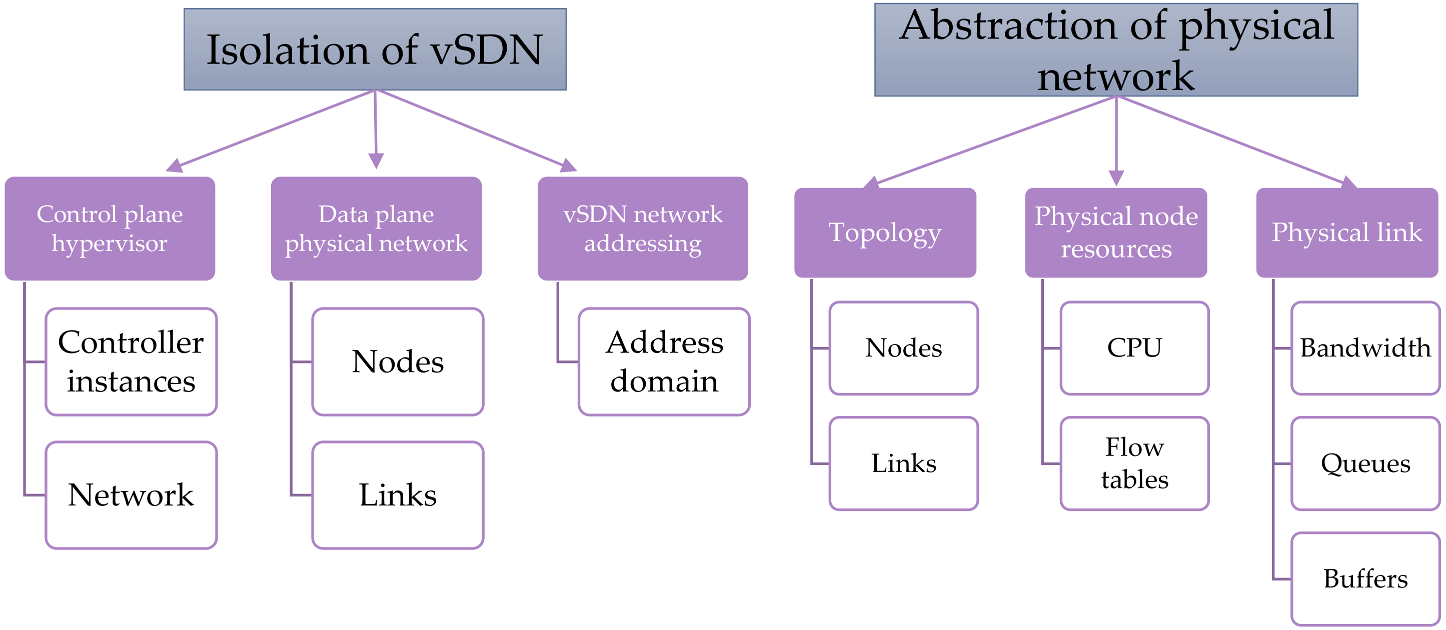


Network Attribute Virtualization

- Hypervisor abstracts the specific characteristic details (attributes) of physical SDN network
- There are three type of SDN network attributes:
  - Topology
  - Physical node resources
  - Physical link resources



Topology Abstraction

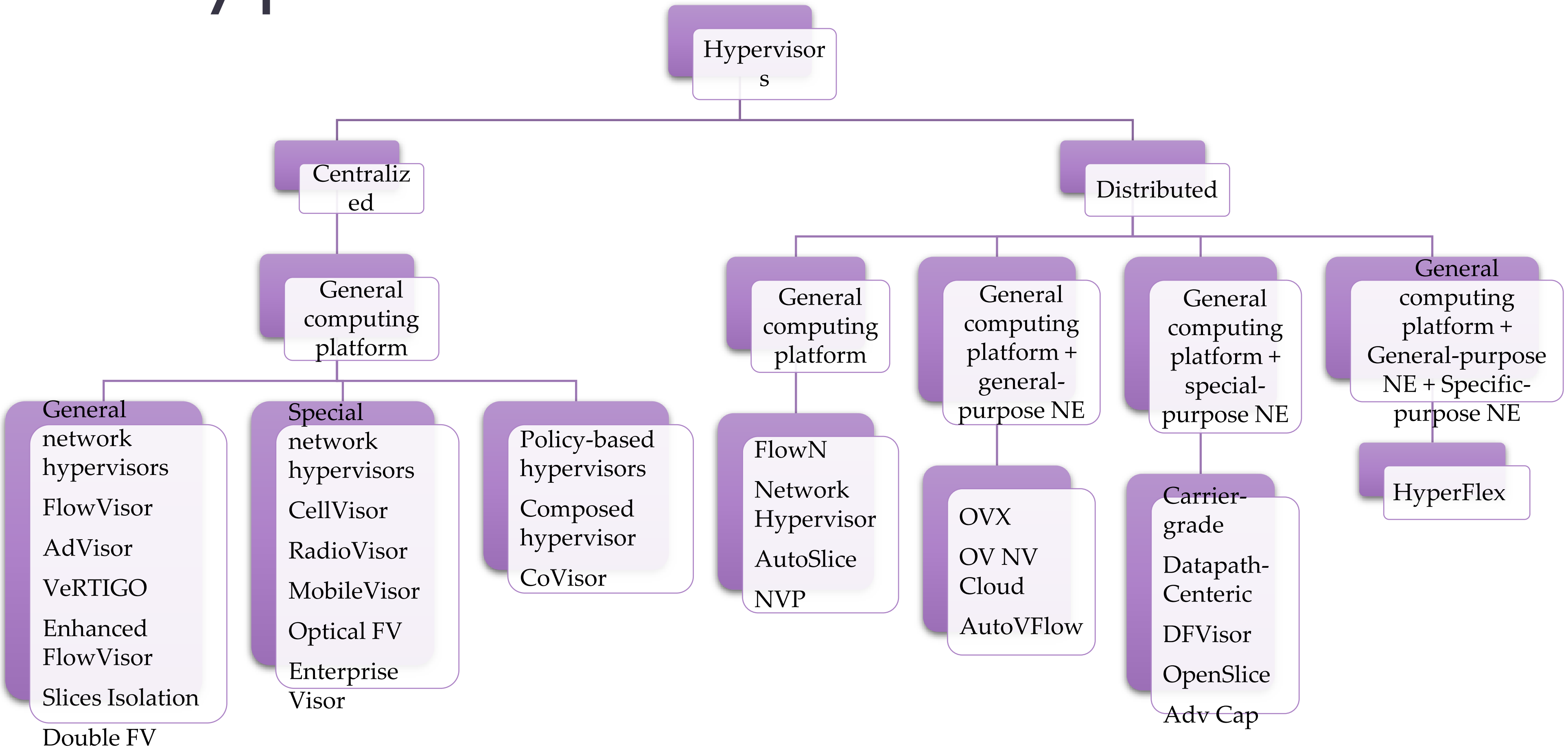

Isolation of vSDN

- Control plane hypervisor
  - Controller instances
  - Network
- Data plane physical network
  - Nodes
  - Links
- vSDN network addressing
  - Address domain

Abstraction of physical network

- Topology
  - Nodes
  - Links
- Physical node resources
  - CPU
  - Flow tables
- Physical link
  - Bandwidth
  - Queues
  - Buffers

SDN Hypervisor Classification



Hypervisors

Centralized

General computing platform

General network hypervisors
FlowVisor
AdVisor
VeRTIGO
Enhanced FlowVisor
Slices Isolation
Double FV

Special network hypervisors
CellVisor
RadioVisor
MobileVisor
Optical FV
Enterprise Visor

Policy-based hypervisors
Composed hypervisor
CoVisor

Distributed

General computing platform
FlowN
Network Hypervisor
AutoSlice
NVP

General computing platform + general-purpose NE
OVX
OV NV Cloud
AutoVFlow

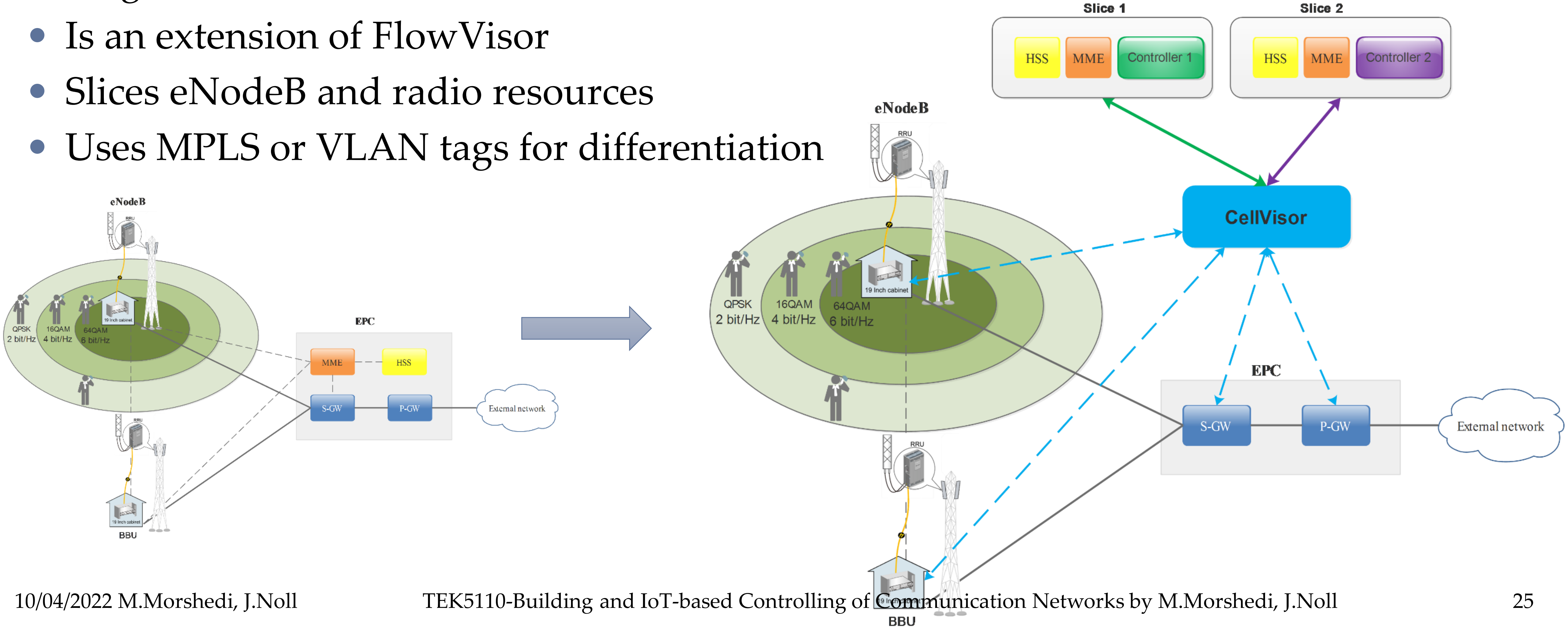
General computing platform + special-purpose NE
Carrier-grade
Datapath-Centeric
DFVisor
OpenSlice
Adv Cap

General computing platform + General-purpose NE + Specific-purpose NE
HyperFlex

A. Blenk, A. Basta, M. Reisslein and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 655-685, Firstquarter 2016. doi: 10.1109/COMST.2015.2489183

CellVisor

- Targets cellular core networks
- Is an extension of FlowVisor
- Slices eNodeB and radio resources
- Uses MPLS or VLAN tags for differentiation



SDN Challenges

- Latency overhead
  - Time from sending a packet into control plane, processed and send back to data plane to being forwarded
- Controller OpenFlow 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

Can we use SDN for wireless management? (WLAN and distributed networks)
If YES then what would be optimal topology for implementing SDN?

vSDN Challenges

- Latency overhead
  - Time from forwarding a packet into control plane, processed and forward back to data plane
- vSDN hypervisor throughput
  - Rate of messages that an vSDN hypervisor can process on average
- vSDN hypervisor resource management
- vSDN hypervisor reliability and fault tolerance
- vSDN hypervisor security in order to provide trusted platform
- SDN virtualization hardware requirements

Can we use vSDN for wireless management? (WLAN and distributed networks)

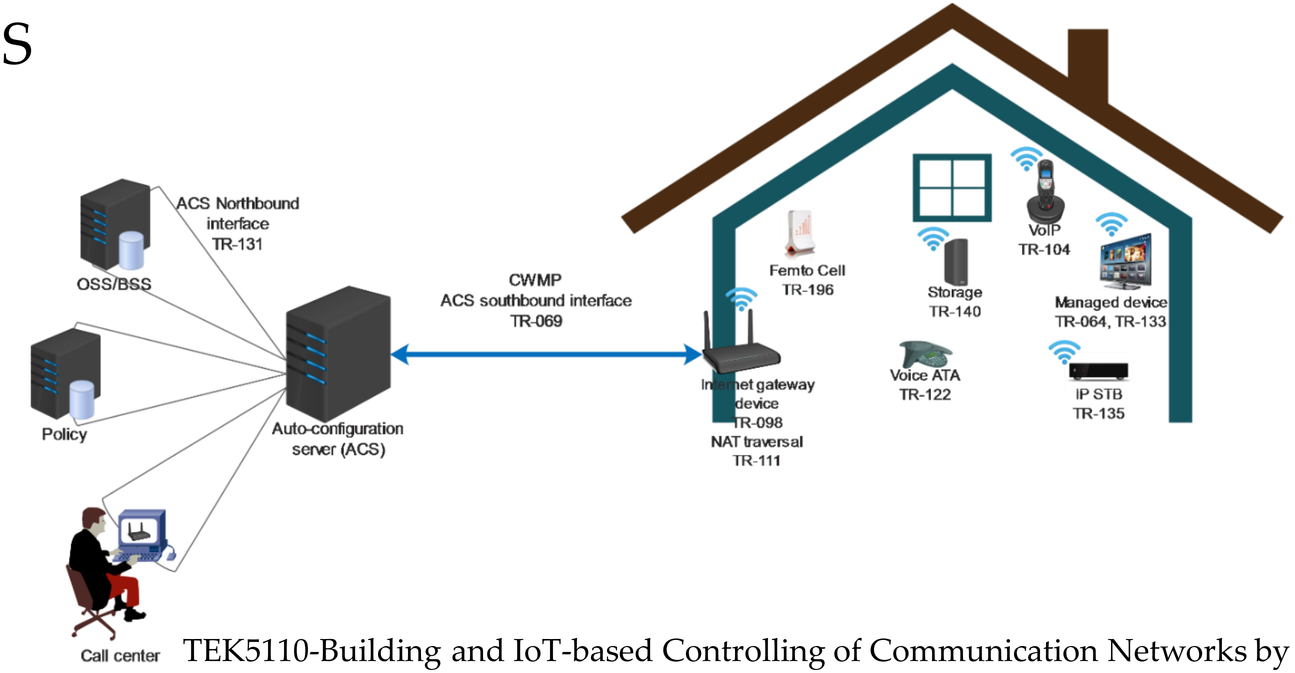
If YES then what would be optimal topology for implementing vSDN?

Conventional System Administration Tools

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

CPE WAN Management Protocol (CWMP) Architecture

- The CWMP often is referred as TR-069
- 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



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

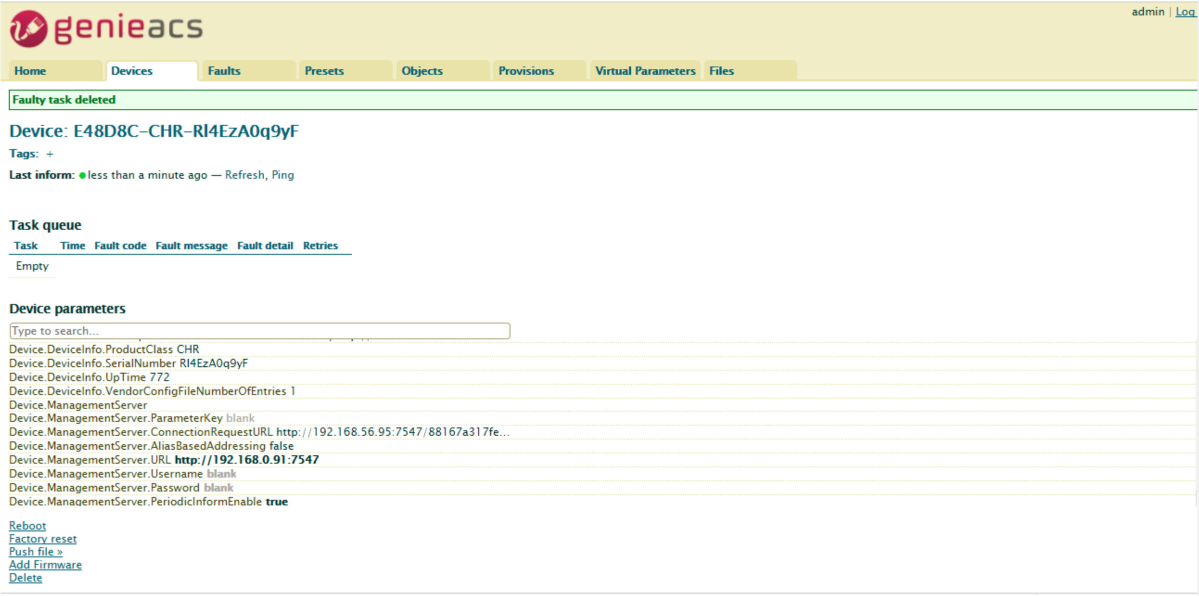
Data Model	Description
TR-064	LAN side DSL CPE configuration
TR-104	Provisioning parameters for VoIP CPE
TR-111	Applying TR-069 to remote management of home networking devices
TR-131	ACS Northbound interface requirements
TR-135	Data model for a TR-069 enabled STB
TR-196	Femto access point service data model
TR-317	Network enhanced residential gateway (SDN/NFV)

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

TR-069 CPE and ACS

- Open source ACS
  - GenieACS
- EyeSaaS
- Axiros



Faulty task deleted

Device: E48D8C–CHR–RI4EzA0q9yF

Tags: +

Last inform: ● less than a minute ago — Refresh, Ping

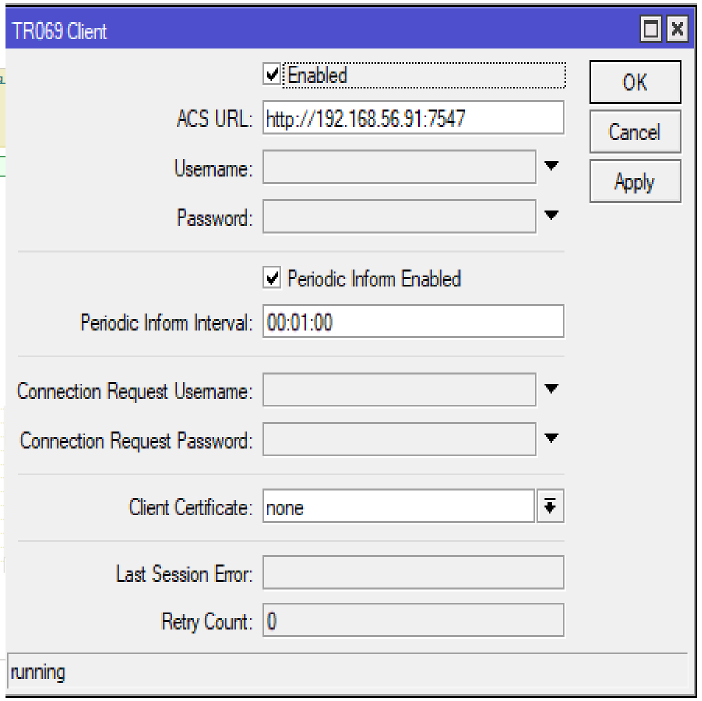
Task queue

Task	Time	Fault code	Fault message	Fault detail	Retries
Empty					

Device parameters

Type to search...

Device.DeviceInfo.ProductClass CHR
Device.DeviceInfo.SerialNumber RI4EzA0q9yF
Device.DeviceInfo.UpTime 772
Device.DeviceInfo.VendorConfigFileNumberOfEntries 1
Device.ManagementServer
Device.ManagementServer.ParameterKey blank
Device.ManagementServer.ConnectionRequestURL http://192.168.56.95:7547/88167a317fe...
Device.ManagementServer.AliasBasedAddressing false
Device.ManagementServer.URL **http://192.168.0.91:7547**
Device.ManagementServer.Username blank
Device.ManagementServer.Password blank
Device.ManagementServer.PeriodicInformEnable **true**



☑ Enabled

ACS URL: http://192.168.56.91:7547

Username:

Password:

☑ Periodic Inform Enabled

Periodic Inform Interval: 00:01:00

Connection Request Username:

Connection Request Password:

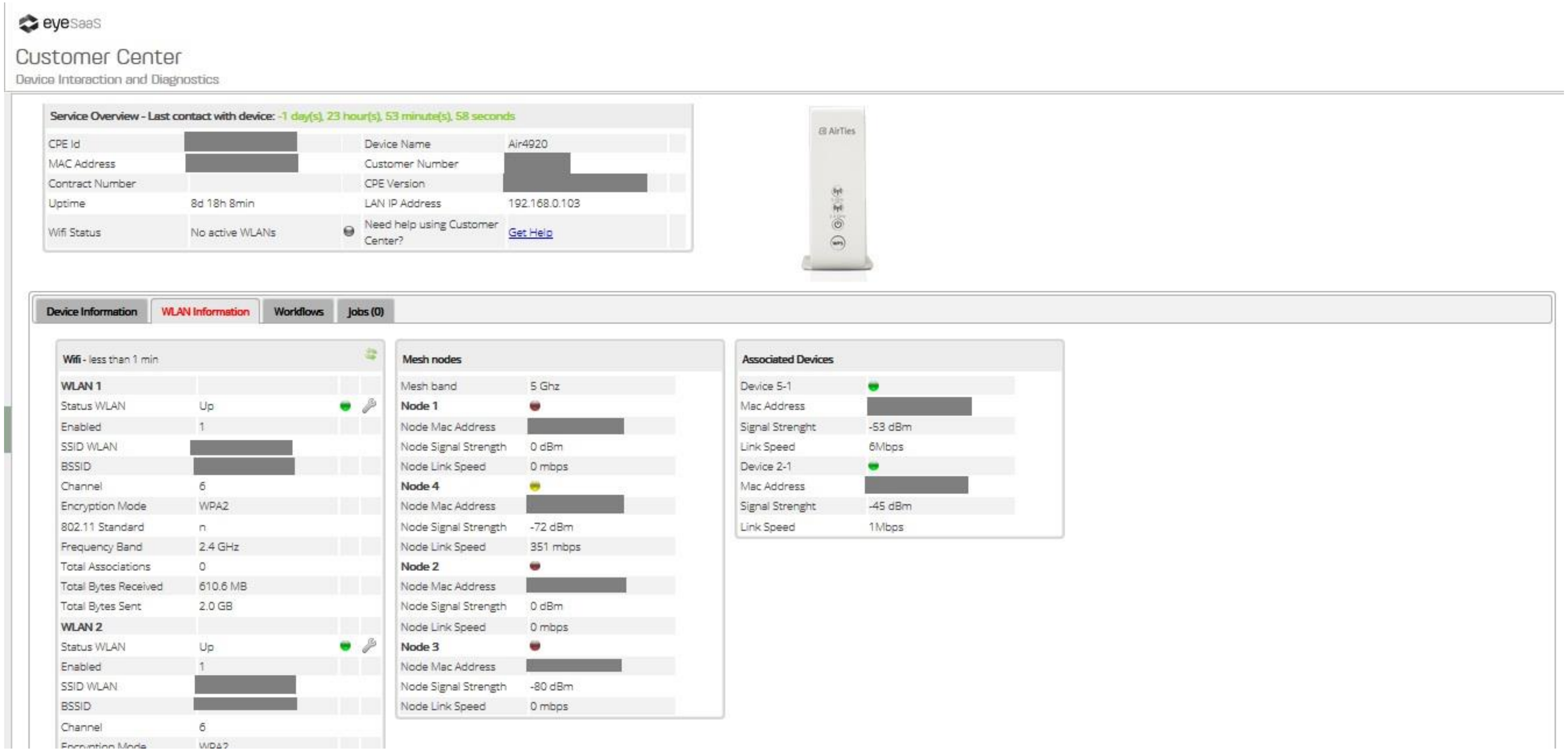
Client Certificate: none

Last Session Error:

Retry Count: 0

running

EyeSaaS Platform



eyeSaaS

Customer Center

Device Interaction and Diagnostics

Service Overview - Last contact with device: -1 day(s), 23 hour(s), 53 minute(s), 58 seconds

CPE Id	[redacted]		Device Name	Air4920
MAC Address	[redacted]		Customer Number	[redacted]
Contract Number			CPE Version	[redacted]
Uptime	8d 18h 8min		LAN IP Address	192.168.0.103
Wifi Status	No active WLANs	●	Need help using Customer Center?	Get Help

Device Information | WLAN Information | Workflows | Jobs (0)

Wifi - less than 1 min

WLAN 1			
Status WLAN	Up	●	
Enabled	1		
SSID WLAN	[redacted]		
BSSID	[redacted]		
Channel	6		
Encryption Mode	WPA2		
802.11 Standard	n		
Frequency Band	2.4 GHz		
Total Associations	0		
Total Bytes Received	610.6 MB		
Total Bytes Sent	2.0 GB		
WLAN 2			
Status WLAN	Up	●	
Enabled	1		
SSID WLAN	[redacted]		
BSSID	[redacted]		
Channel	6		
Encryption Mode	WPA2		

Mesh nodes

Mesh band	5 Ghz
Node 1	●
Node Mac Address	[redacted]
Node Signal Strength	0 dBm
Node Link Speed	0 mbps
Node 4	●
Node Mac Address	[redacted]
Node Signal Strength	-72 dBm
Node Link Speed	351 mbps
Node 2	●
Node Mac Address	[redacted]
Node Signal Strength	0 dBm
Node Link Speed	0 mbps
Node 3	●
Node Mac Address	[redacted]
Node Signal Strength	-80 dBm
Node Link Speed	0 mbps

Associated Devices

Device 5-1	●
Mac Address	[redacted]
Signal Strenght	-53 dBm
Link Speed	6Mbps
Device 2-1	●
Mac Address	[redacted]
Signal Strenght	-45 dBm
Link Speed	1Mbps

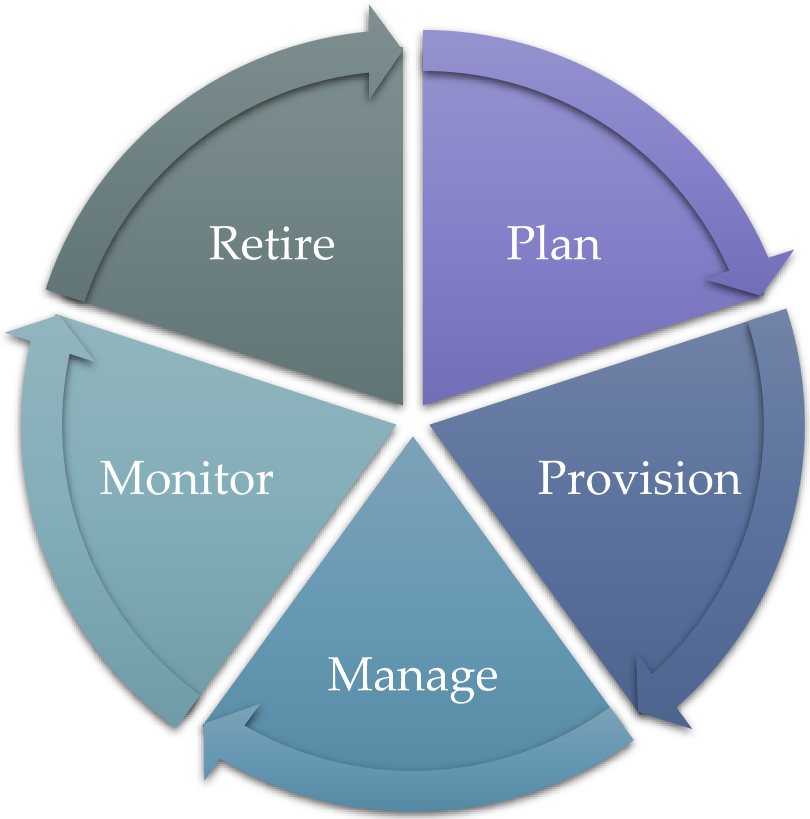
IoT Management Advantages

- 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

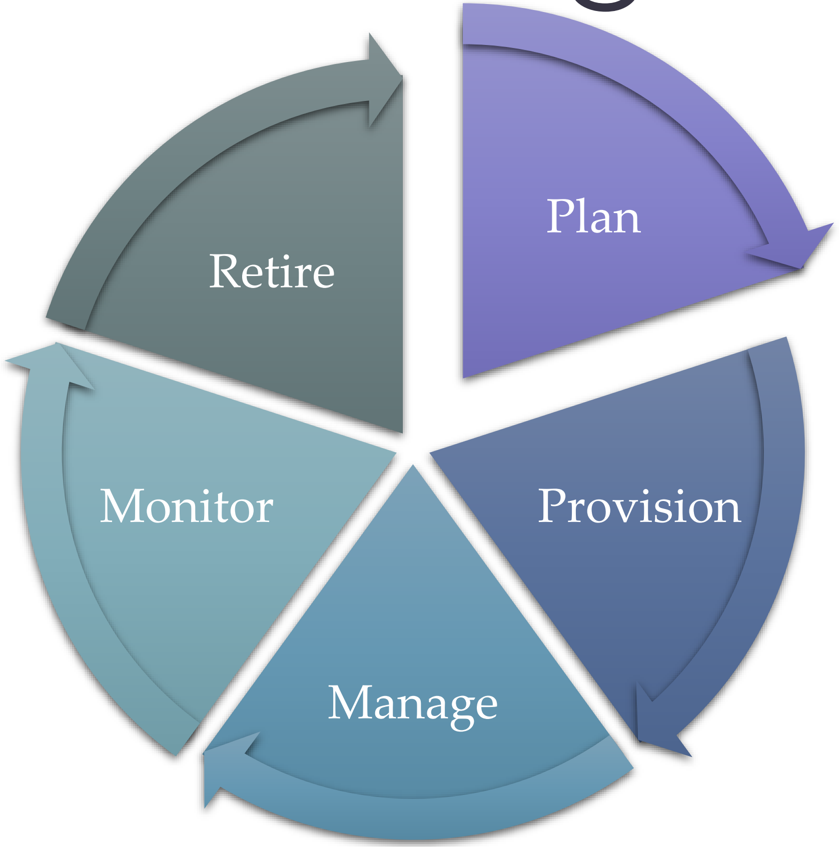
- Power and energy consumption
  - Many IoT devices need to run for years over battery.
- Connectivity
  - Varity of connectivity standards such as Zigbee, Zwave, Bluetooth, etc.
- Computation capabilities
  - Many IoT devices use low-end microchips with very limited capabilities.
- Lack of standard-Interoperability
  - 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



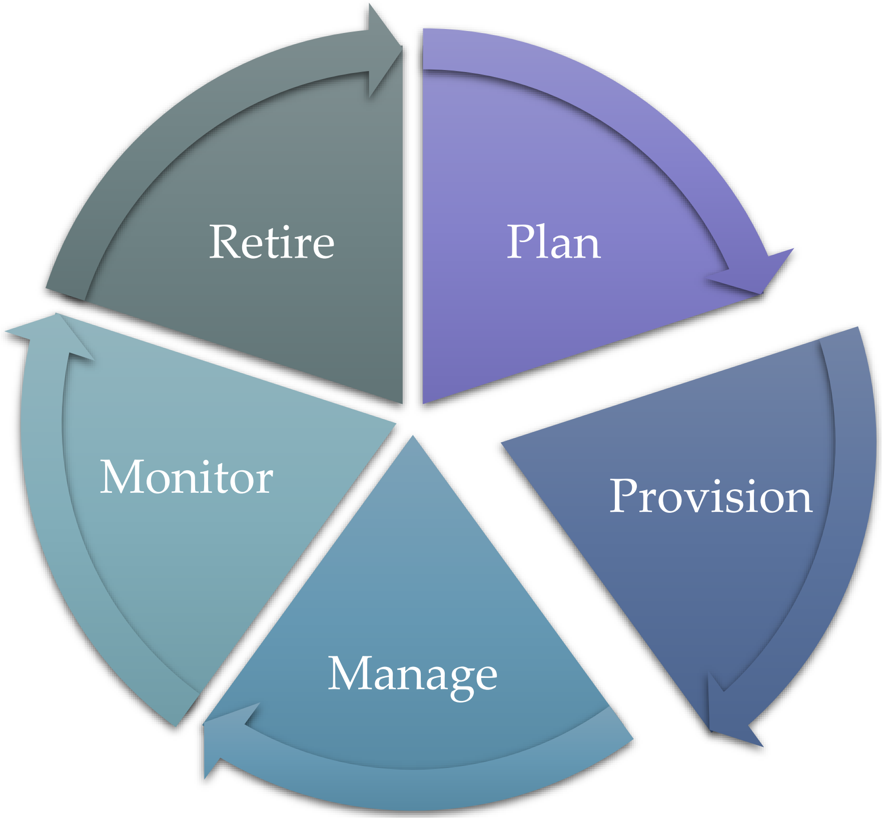
IoT Device Lifecycle-Planning

- 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



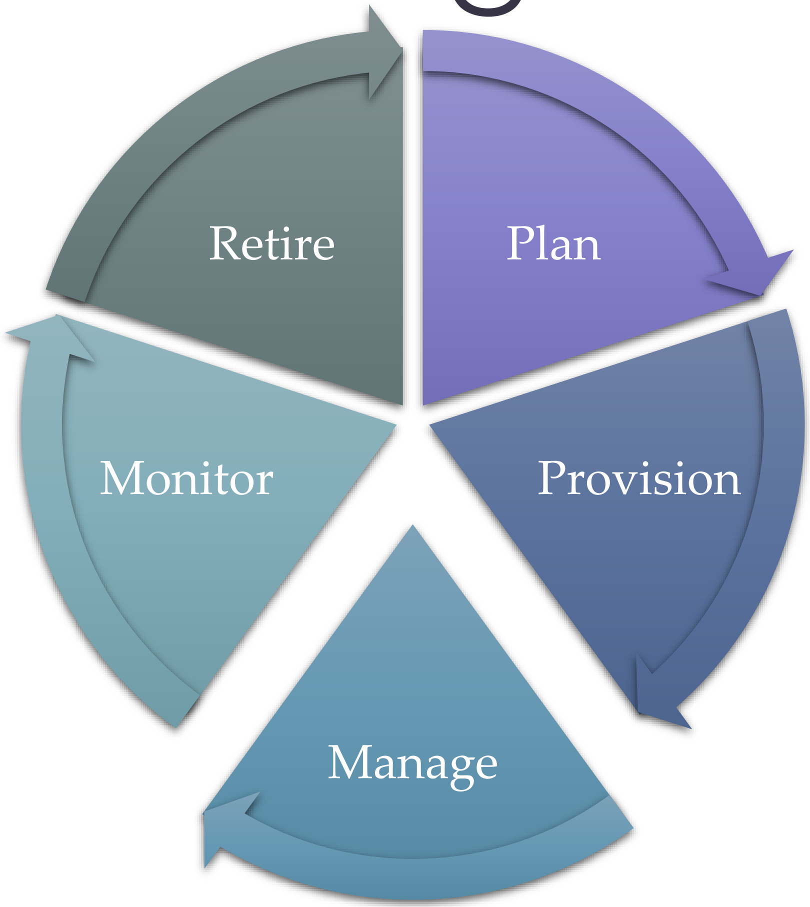
IoT Device Lifecycle-Provisioning

- Authenticate and register IoT devices in the management platform
  - Zero-touch authentication and registration
  - 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



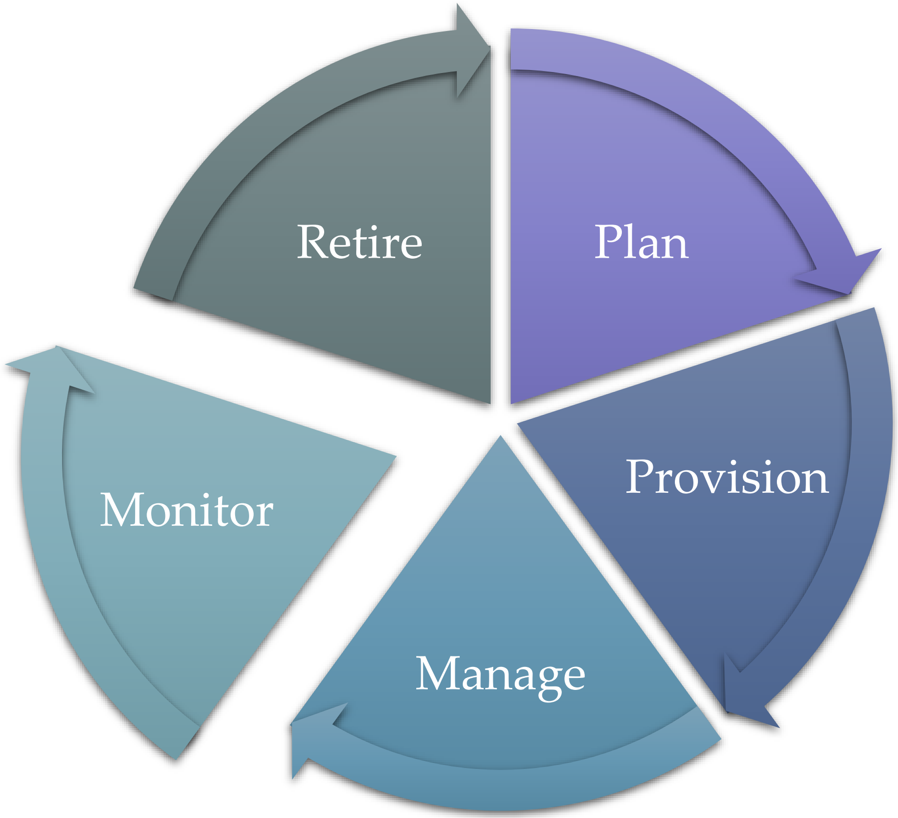
IoT Device Lifecycle-Management

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



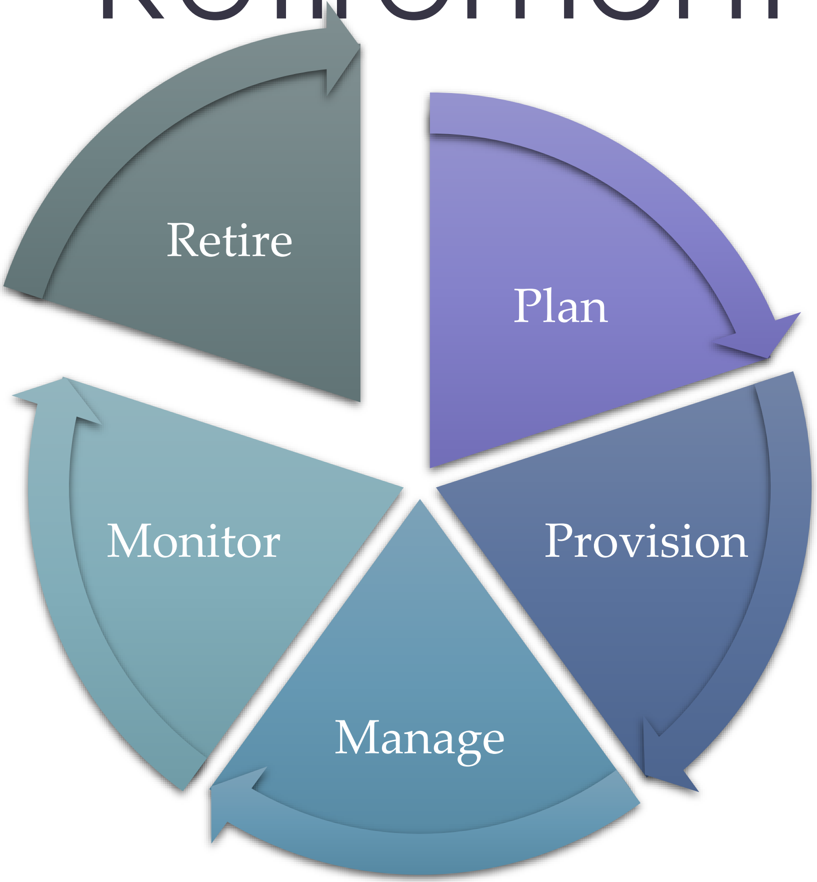
IoT Device Lifecycle-Monitoring

- 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



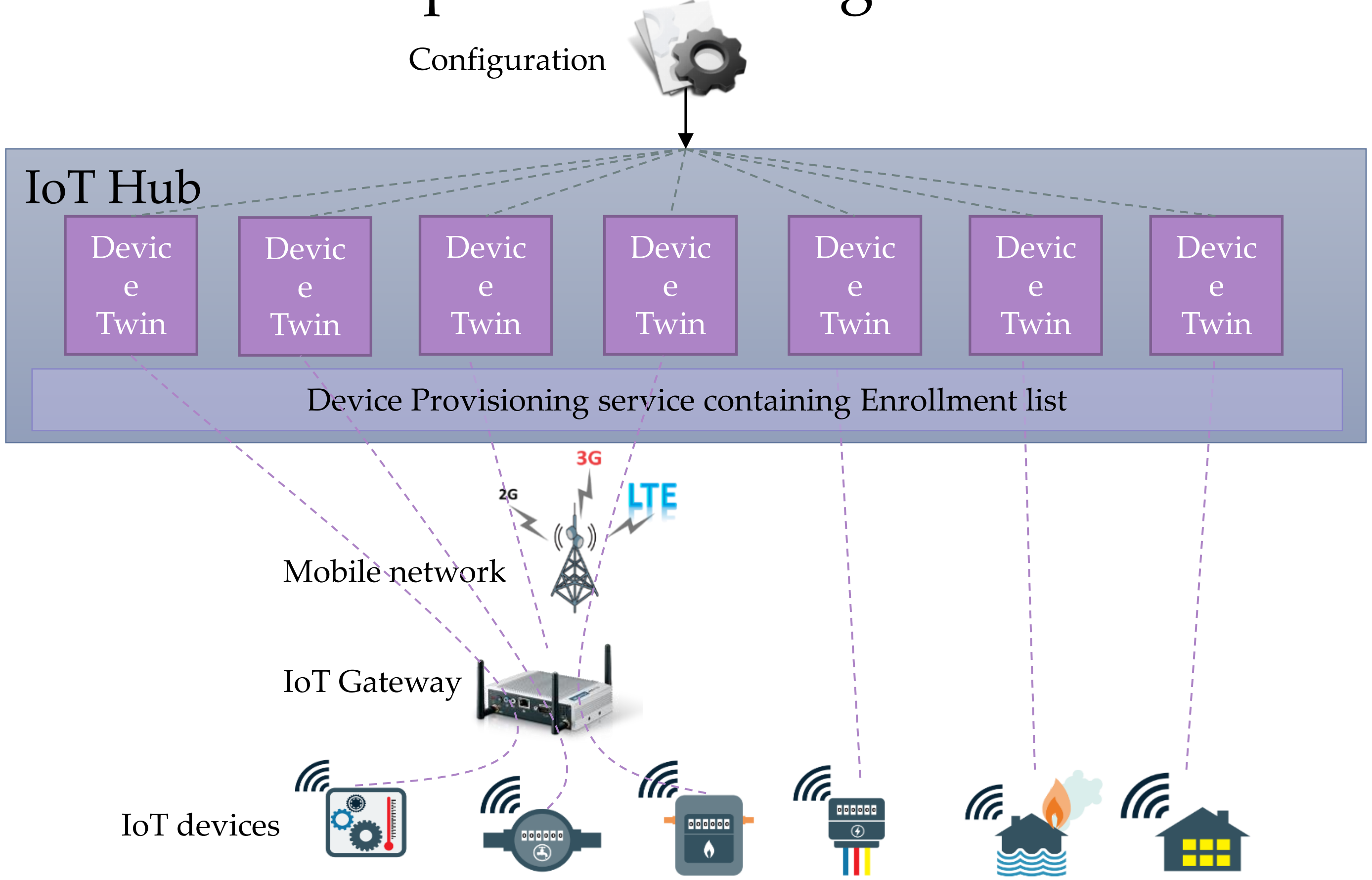
IoT Device Lifecycle- Retirement

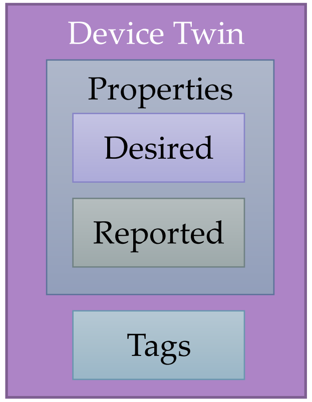
- Replace the failed device with new one
  - Device lifecycle is ended
  - Defective devices
  - Device failed
    - Re-provision new replaced device
  - Upgrade to a new model
    - New features and functionalities



IoT platform 1

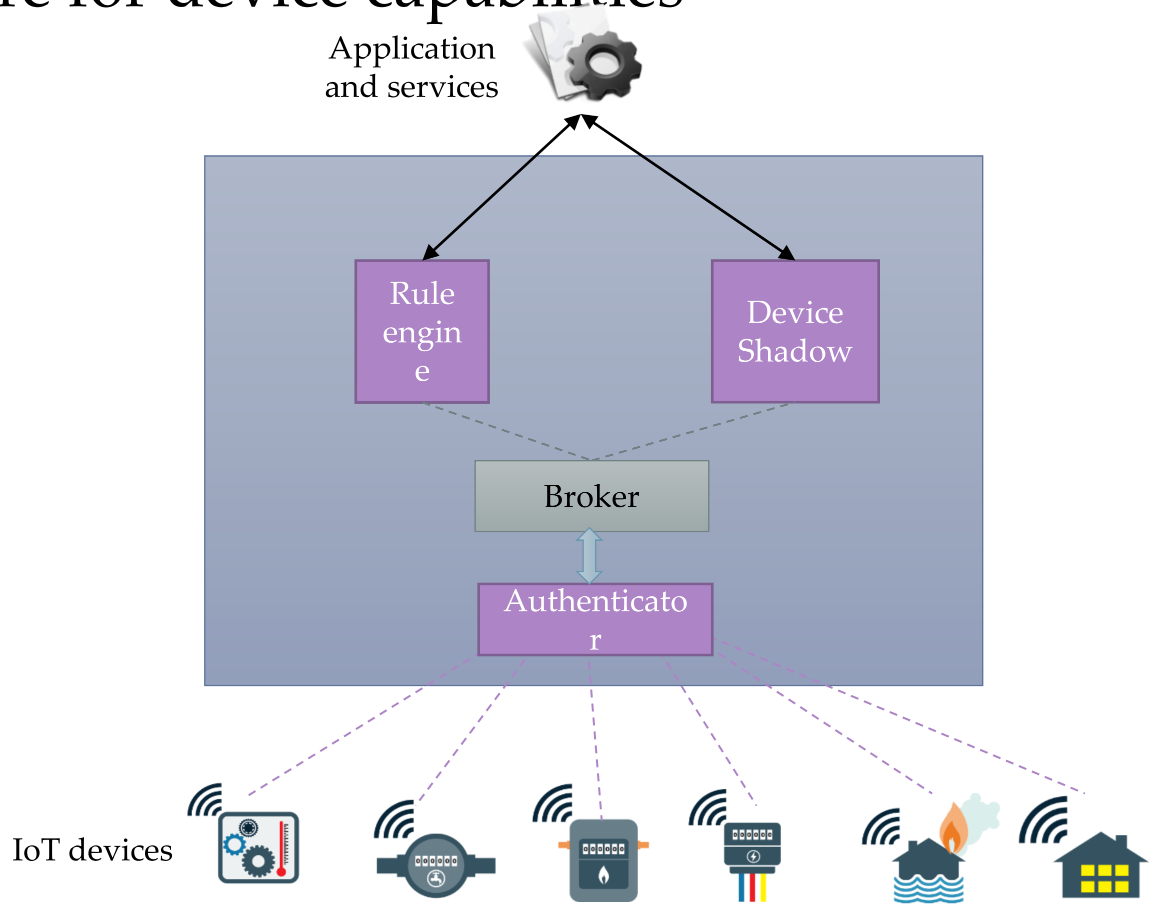
IoT devices connect to platform through IoT hub





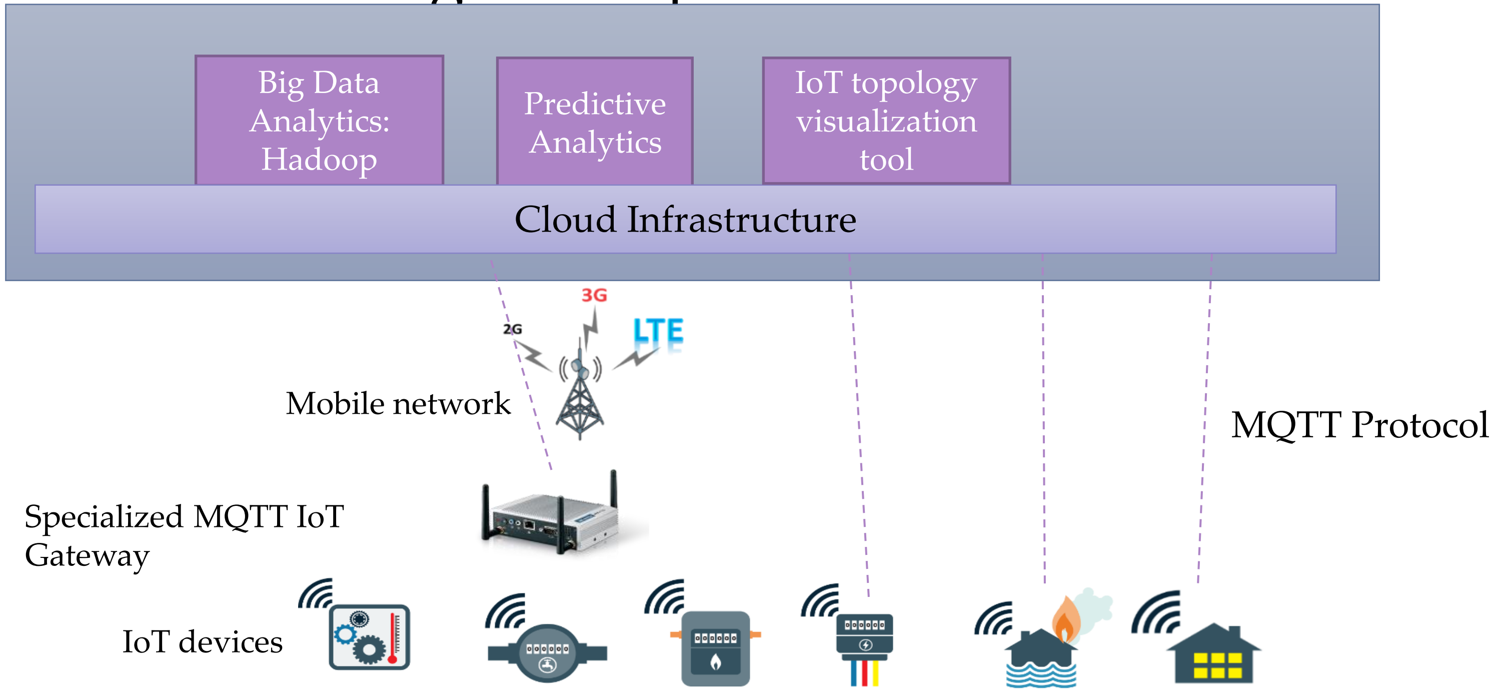
IoT platform 2

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



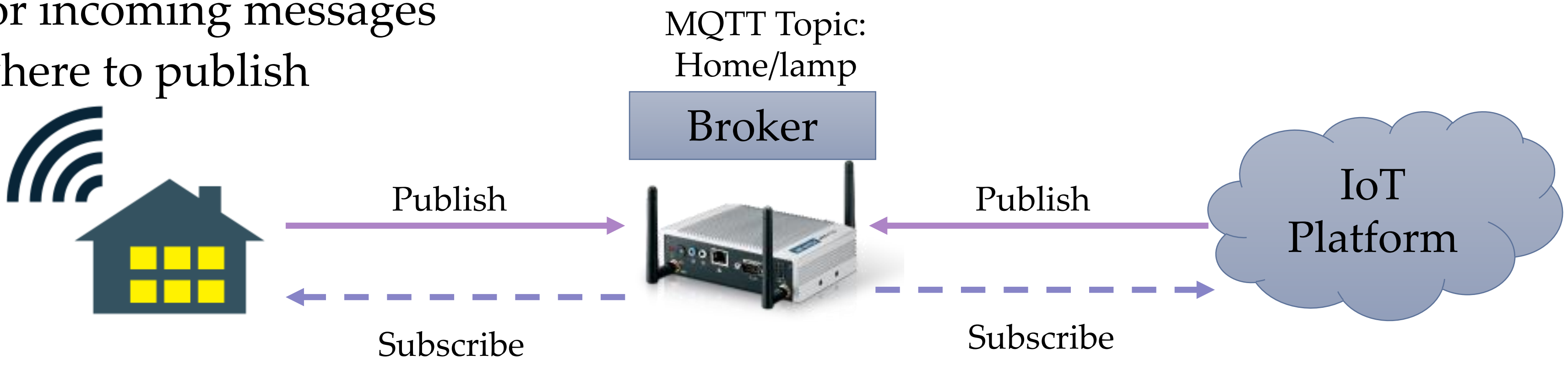
IoT platform 3

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


Big Data Analytics: Hadoop
Predictive Analytics
IoT topology visualization tool
Cloud Infrastructure
3G
2G
LTE
Mobile network
MQTT Protocol
Specialized MQTT IoT Gateway
IoT devices

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



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

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

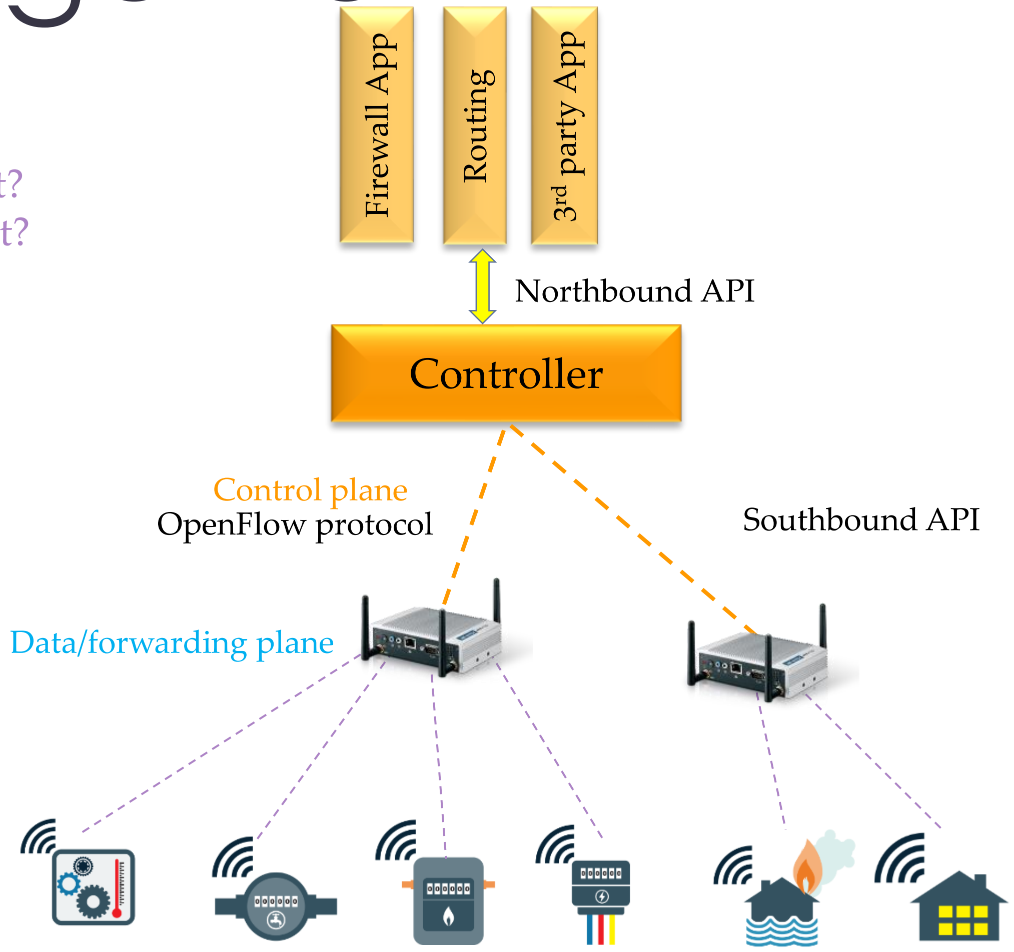
Recap: Conventional system administration tools

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

Can we use conventional system administration tools for IoT management?

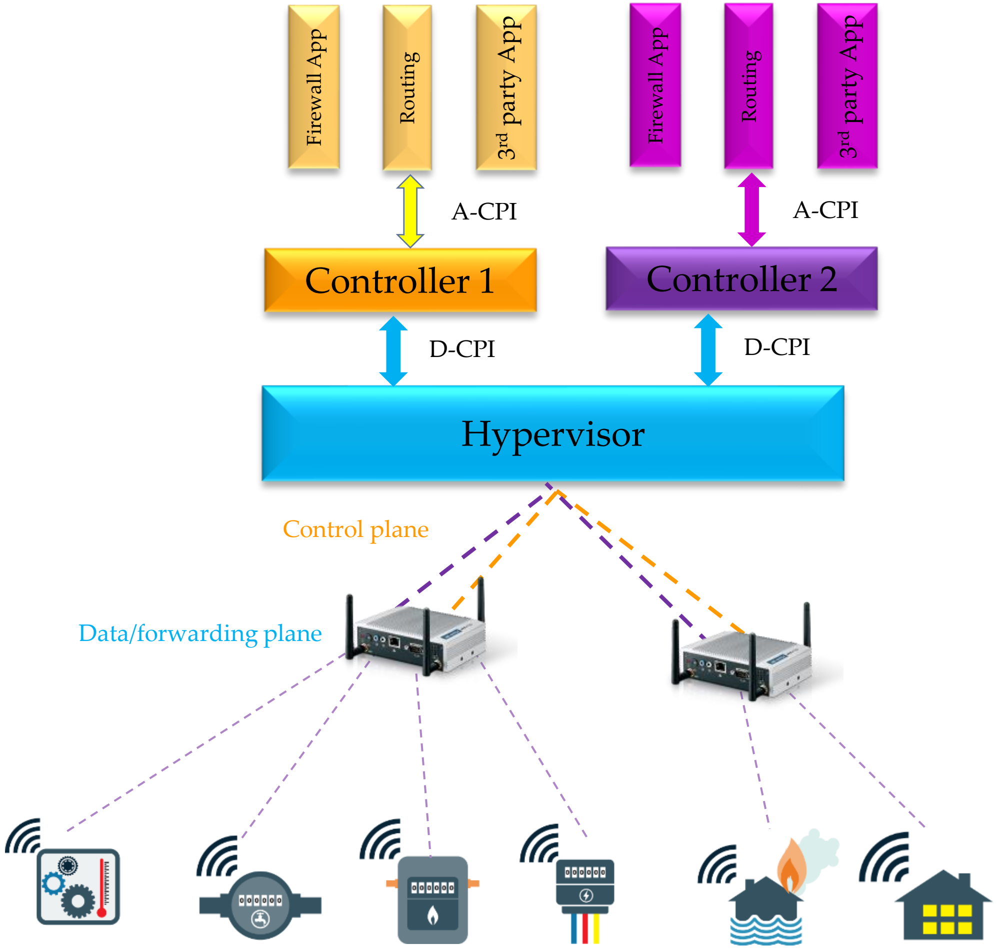
SDN for IoT Management

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



Discussion

- What would be optimal monitoring time intervals?
- What kind of characteristics should a wireless management system have?
- Which approach would you use for wireless management in your network? (configuration management, SDN or open standard protocols)
- Do the wireless device monitoring and management raise privacy concerns?
  - If yes then how we can mitigate privacy concerns? (pseudonyms, removal of identifiers (de-identification) or aggregation)

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