Wireless Remote Management

UNIK4700 - Building Mobile and Wireless Networks

Maghsoud Morshedi

Wireless Networks

- The global handheld mobile devices have predicted to reach 8.3 billion by 2021[1]
  - machine-to-machine (M2M) connections will grow to 3.3 billion
- The Wi-Fi will transfer half of the total IP traffic by 2020 [2]

[1,2] Cisco, "Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper," 7 Feb 2017

Best Effort Wireless Networks Challenges

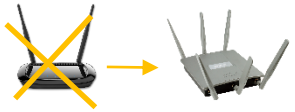
- Capacity
  - Lack of insight into access points impedes proper capacity planning and management .
- Scalability
  - Manually configuring and updating access points do not scale in large deployments
- Quality of Service (QoS)
  - Although wireless networks should support all connected clients, they 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 even though the issue is not hardware related

- Too many repeated calls and technician dispatches

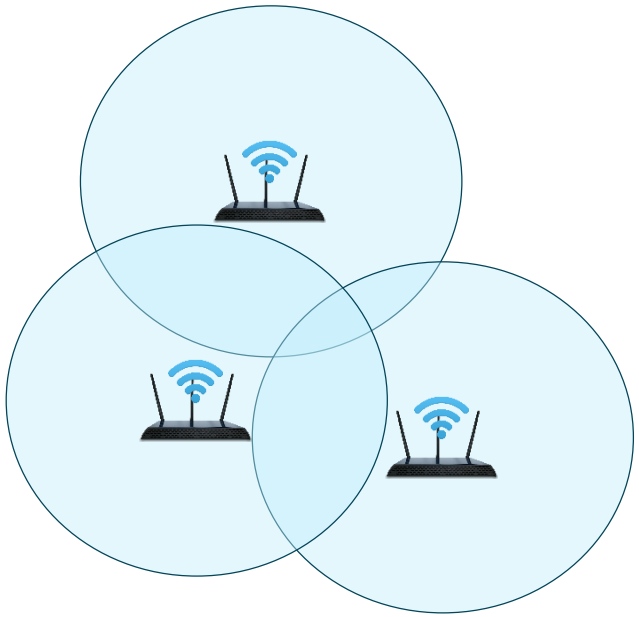
[1] ASSIA, "Deliver Real Quality of Experience to Wi-Fi Residential Subscribers," [Online]. Available: http://www.assia-inc.com/products/cloudcheck/

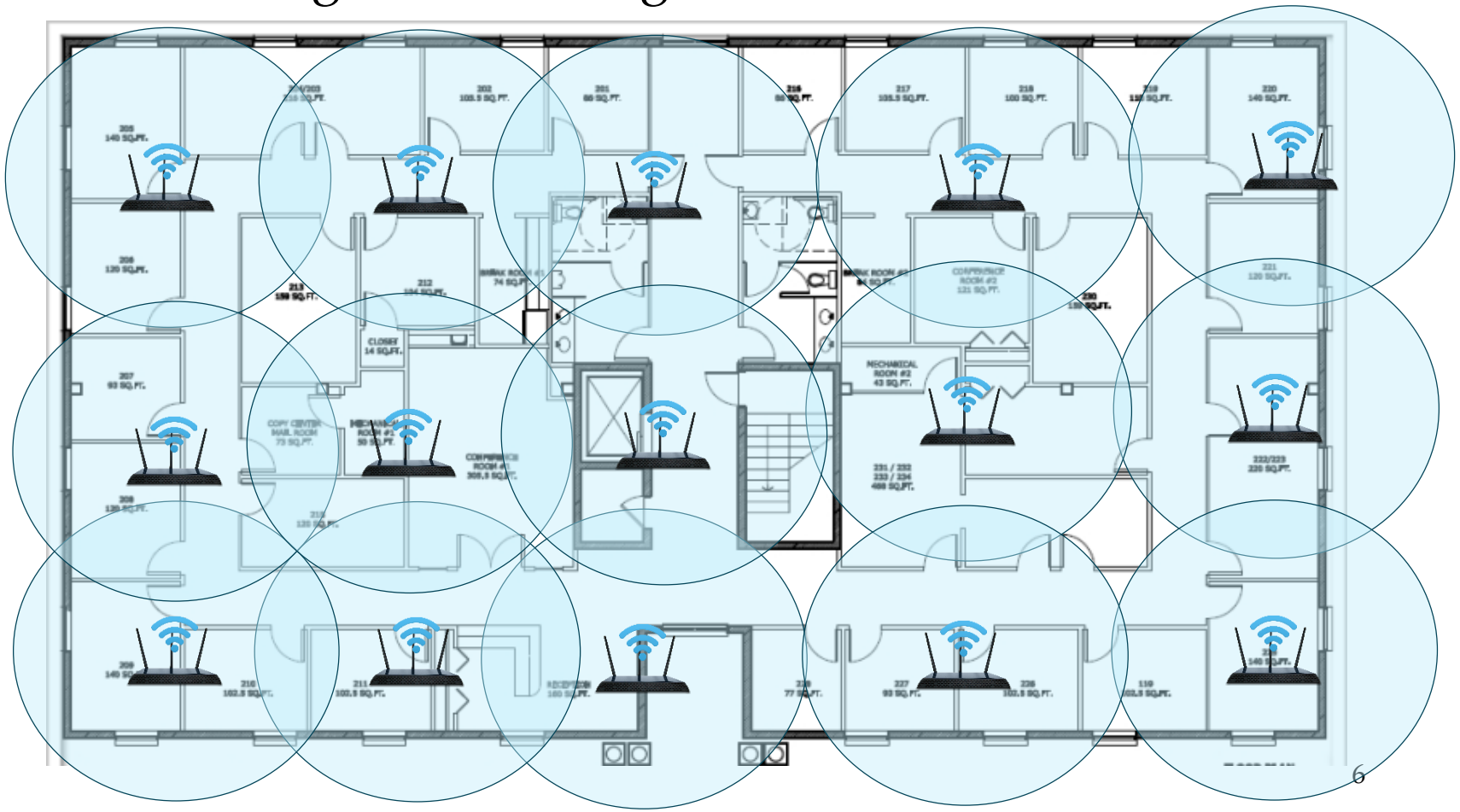
Build our Wireless Networks

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

Enhance our Wireless Networks

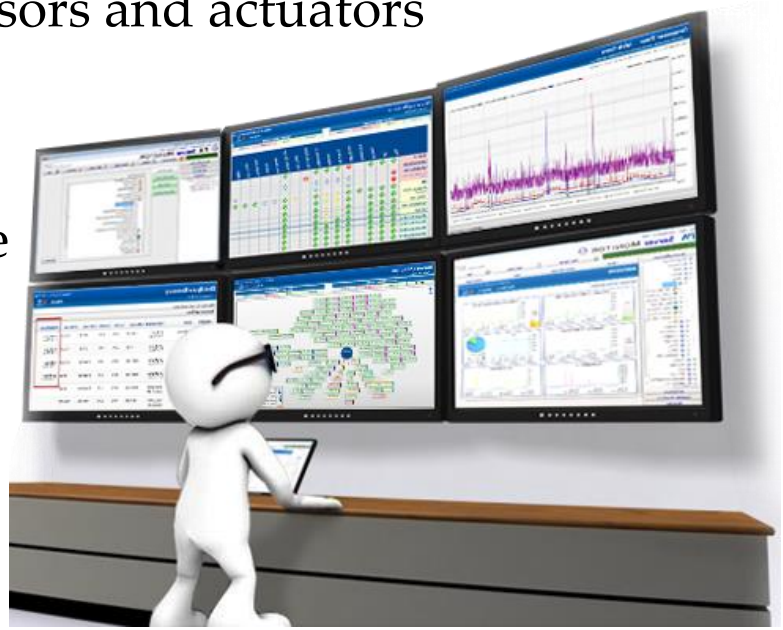
- How would you monitor and configure following networks?





Remote Management

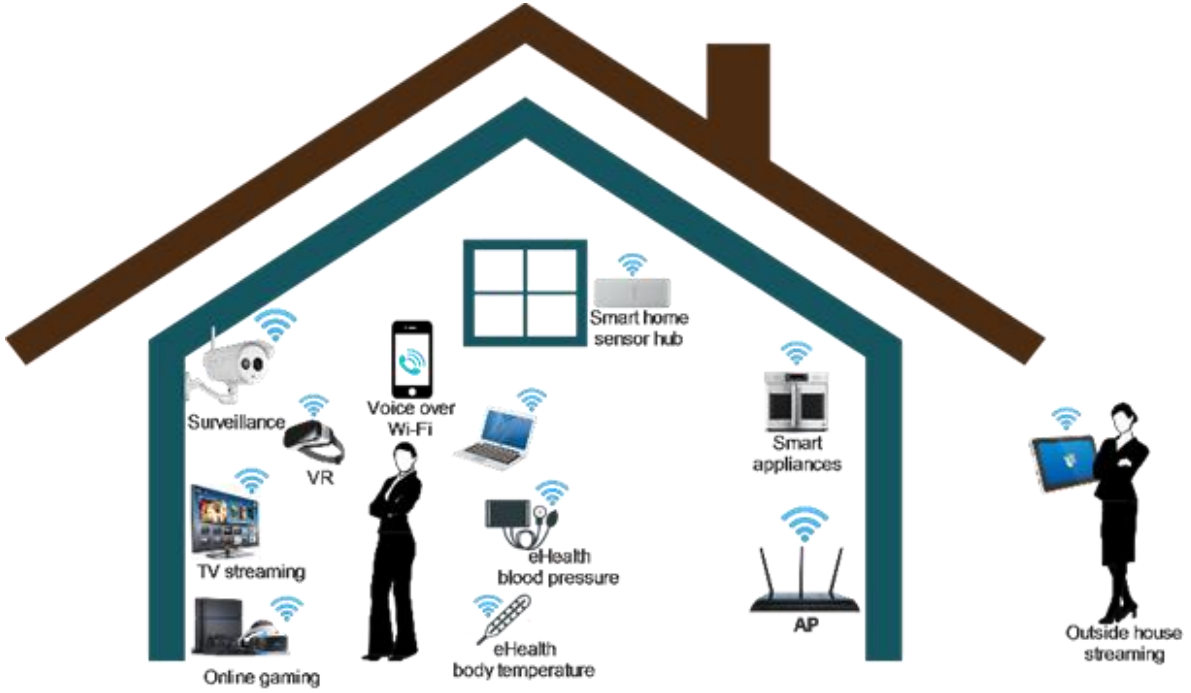
1. Simplify the service provisioning in wireless infrastructures
2. Real-time monitoring can detect wireless issues
3. Enable dynamic wireless network supporting mobility
4. Control the sensors and monitor their unpredictable behaviour
5. Reduce the operational cost and improve interoperability of sensors 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



Managed Wireless

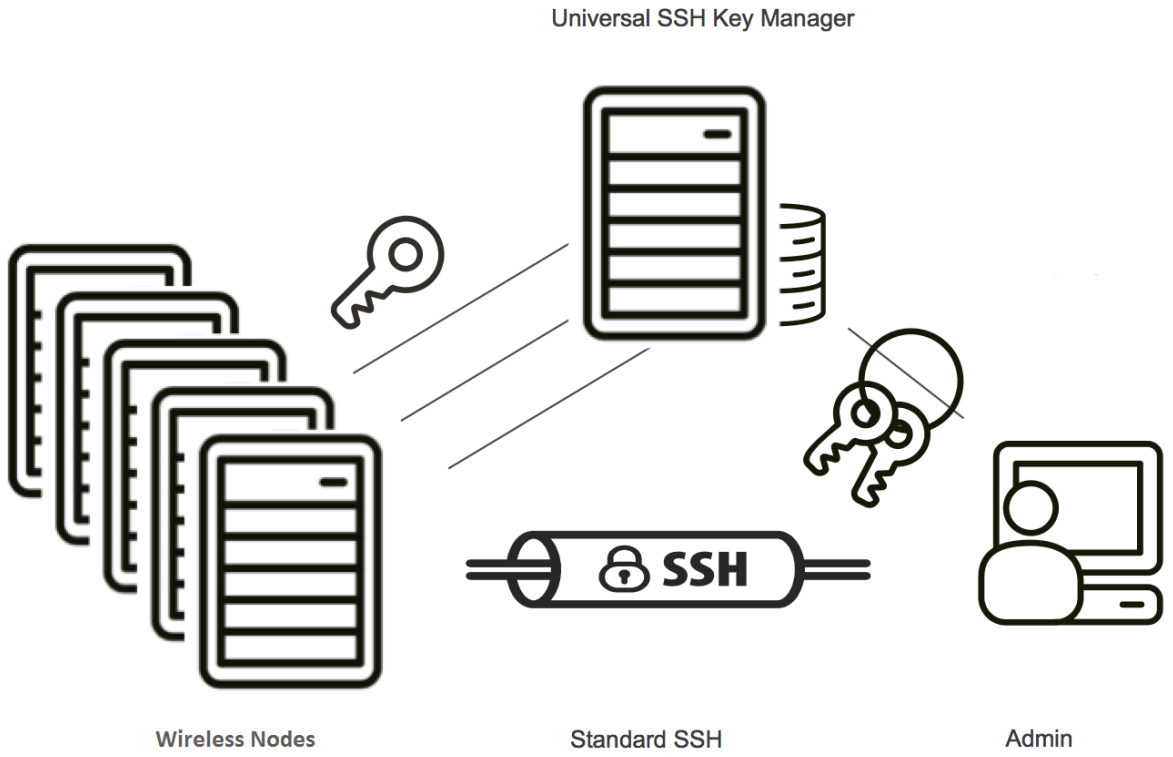
- Definition: A system that enables performance monitoring and configuration of the wireless system

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



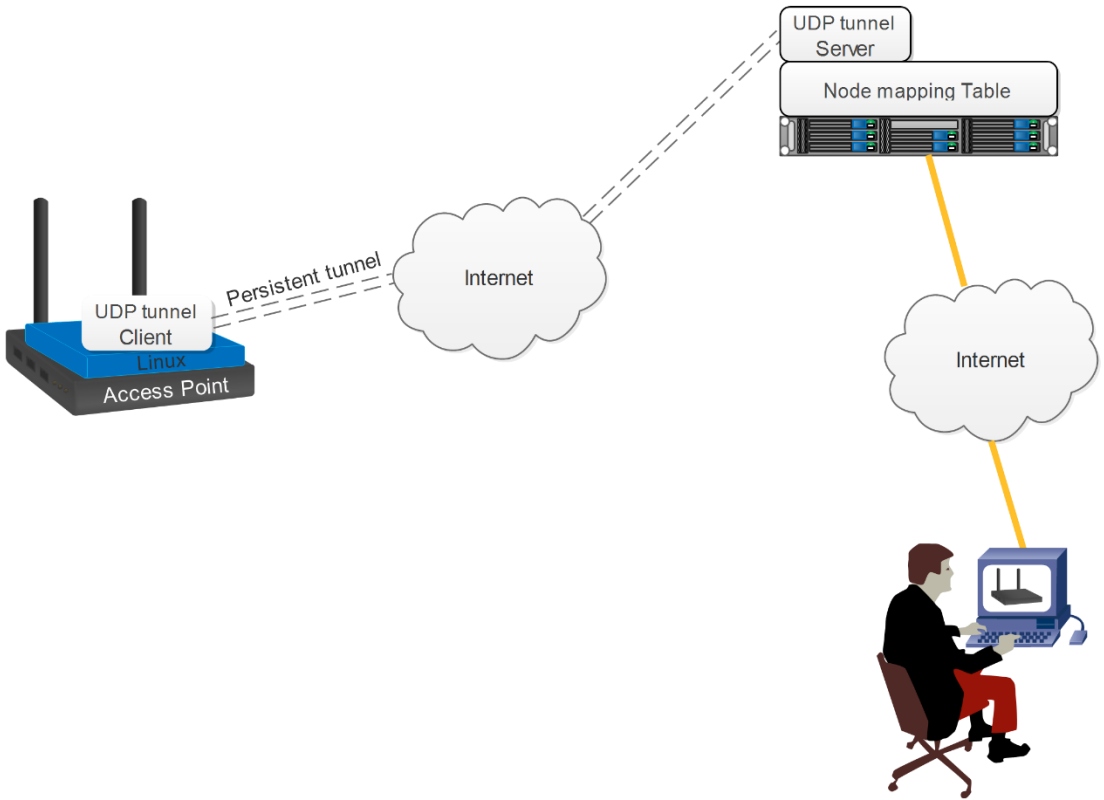
Remote Managed Wireless

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



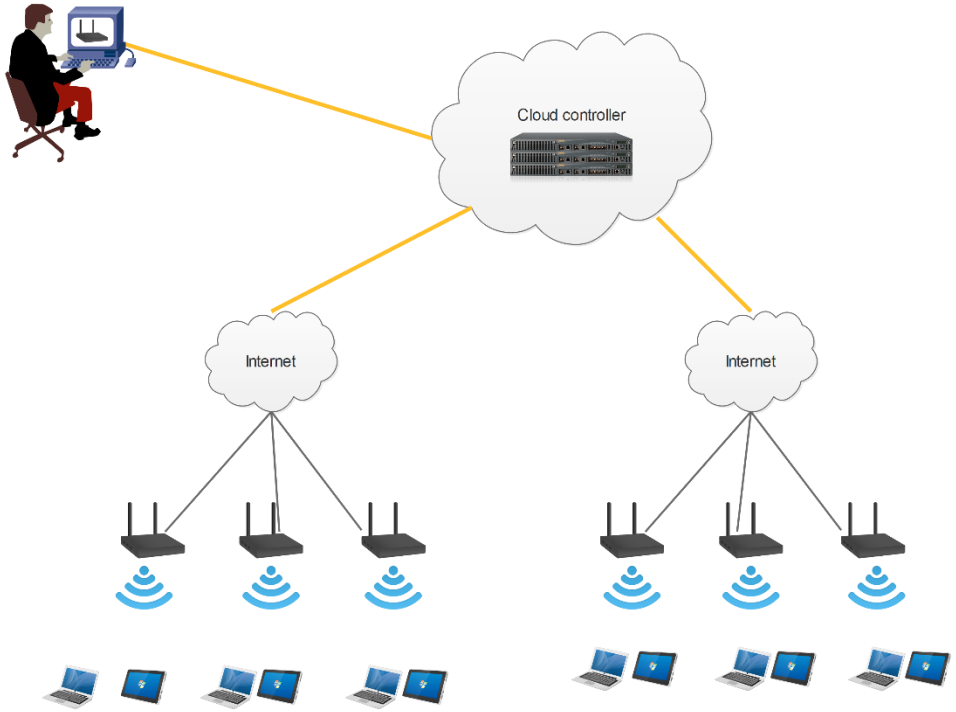
Cloud Managed Wireless

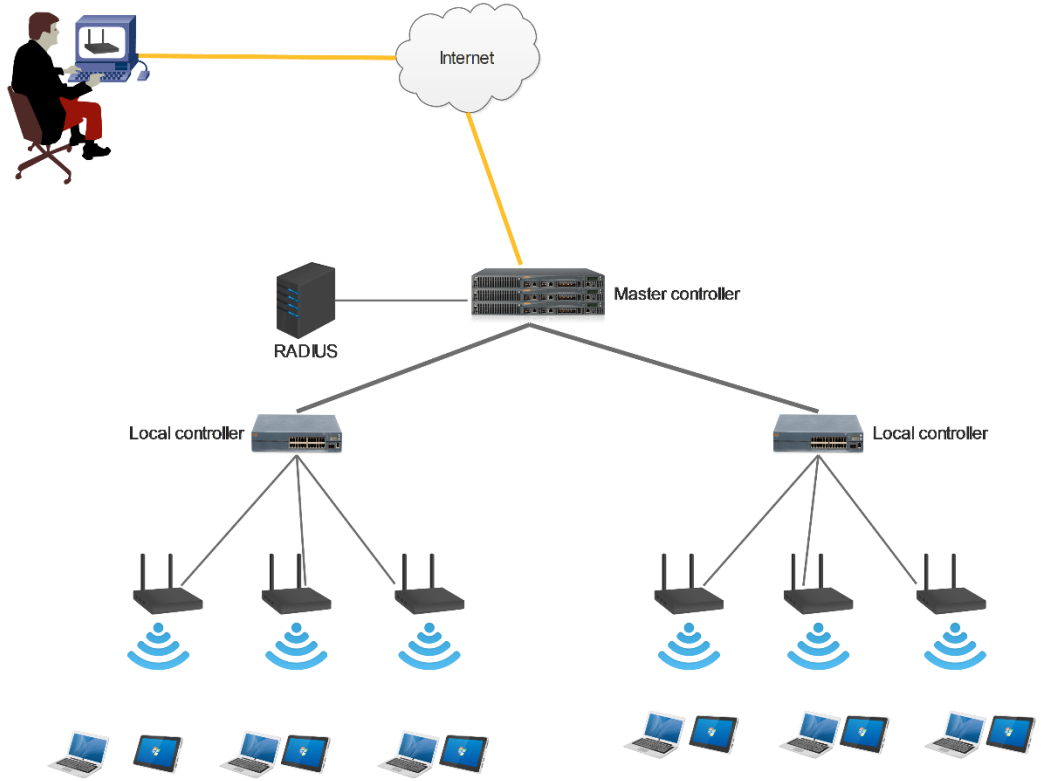
- Performing monitoring and configuration of wireless devices through the cloud dashboards such that wireless device downloads the configuration from cloud and execute it



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

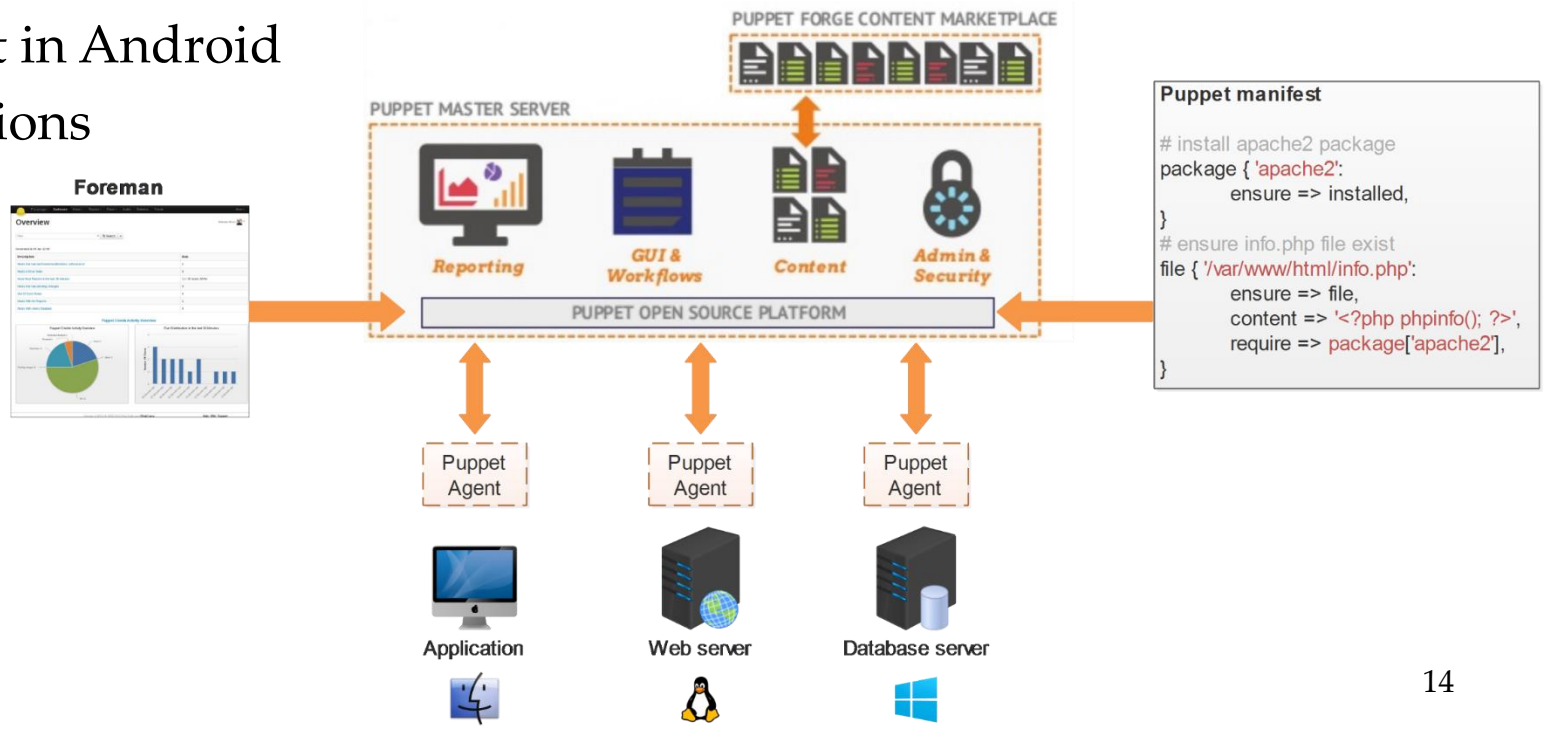
Retransmission Password length

Conventional System Administration Tools

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

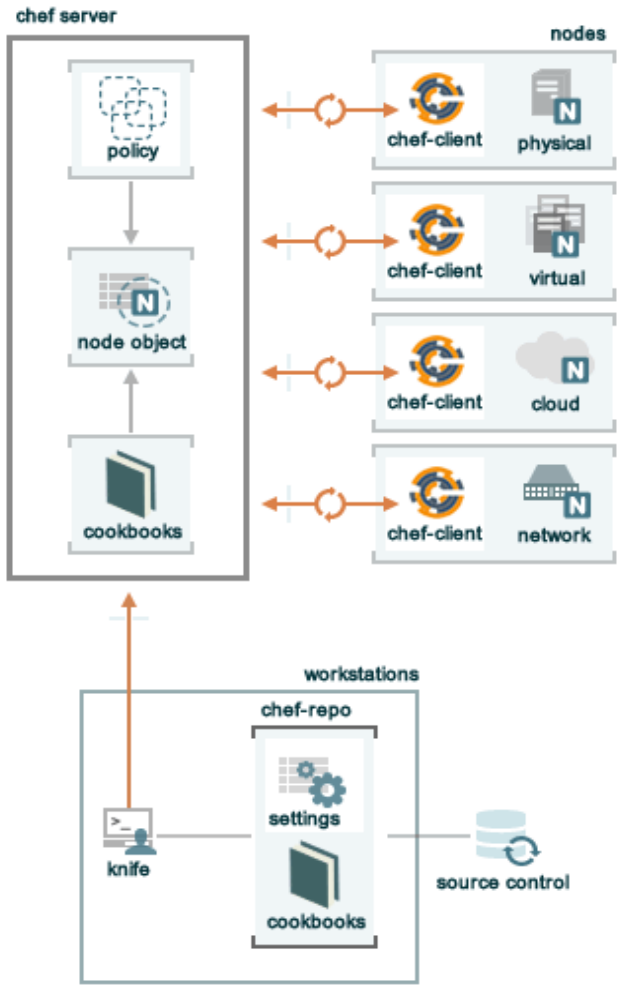
Puppet

- 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



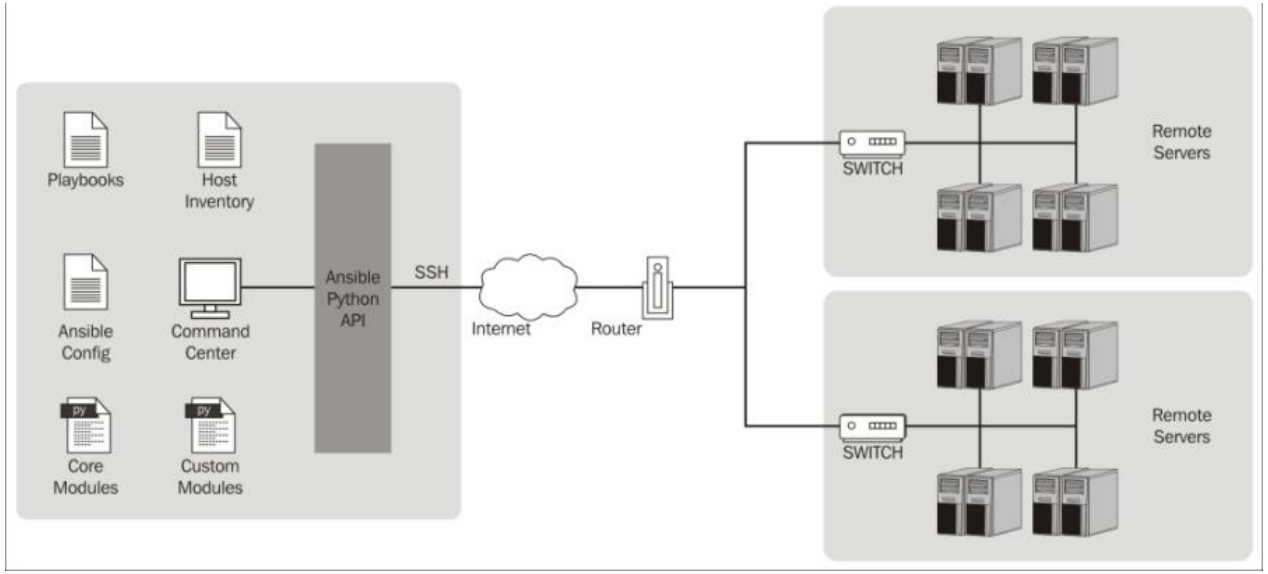
Chef

- Install Chef client on remote nodes
- Write cookbooks to manage remote hosts
- Use Knife as CLI to manage Chef server
- Supports Linux and Windows, MacOS
- Open source and enterprise versions



Ansible

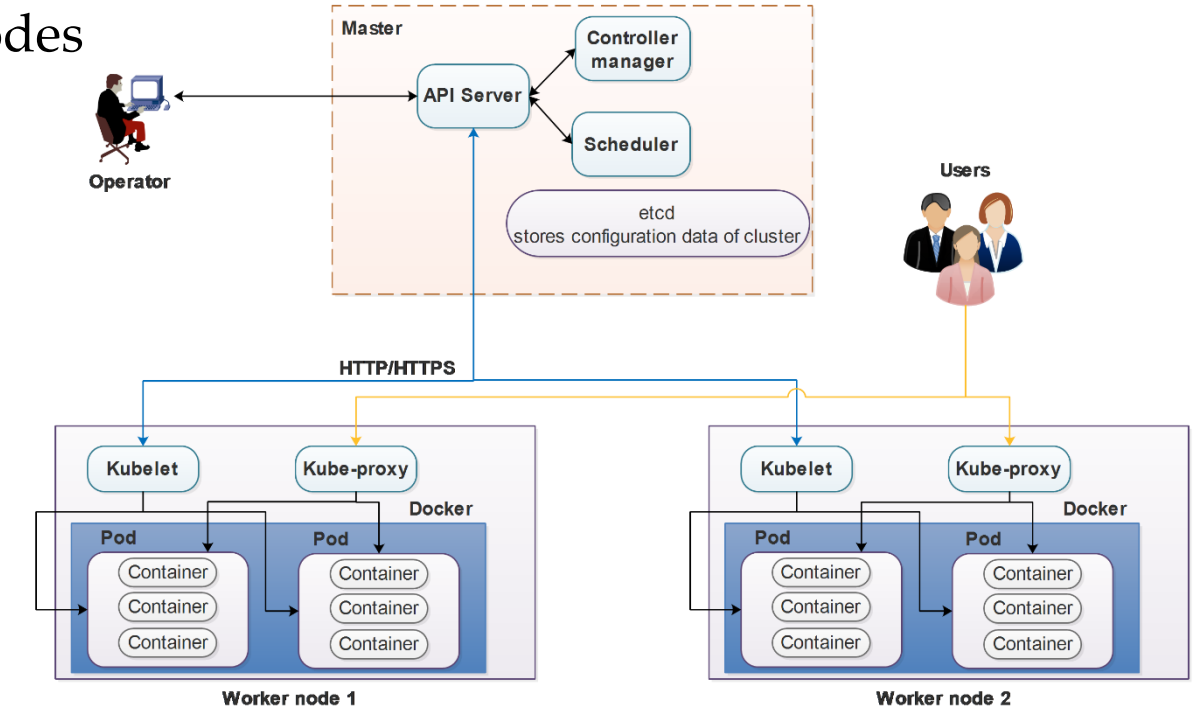
- Agent-less approach using SSH
- Write Playbooks to manage remote hosts
- Modules run on remote node to control resources and packages
- Provide modules for networking equipment produced by Cisco, HP, F5, Fortinent, etc.
- Supports operating systems that support SSH



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!?

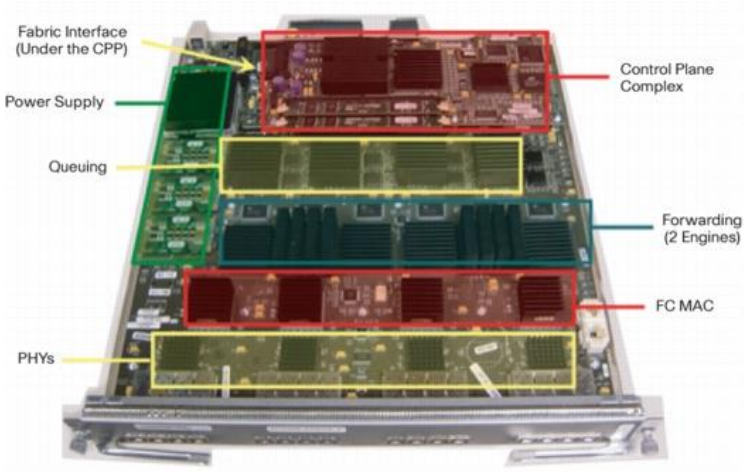
- Can we use Puppet to manage wireless devices?
- Can we use Chef to manage wireless devices?
- Can we use Ansible to manage wireless devices?
- Can we use Kubernetes to manage wireless devices?

Conventional System Administration Tools

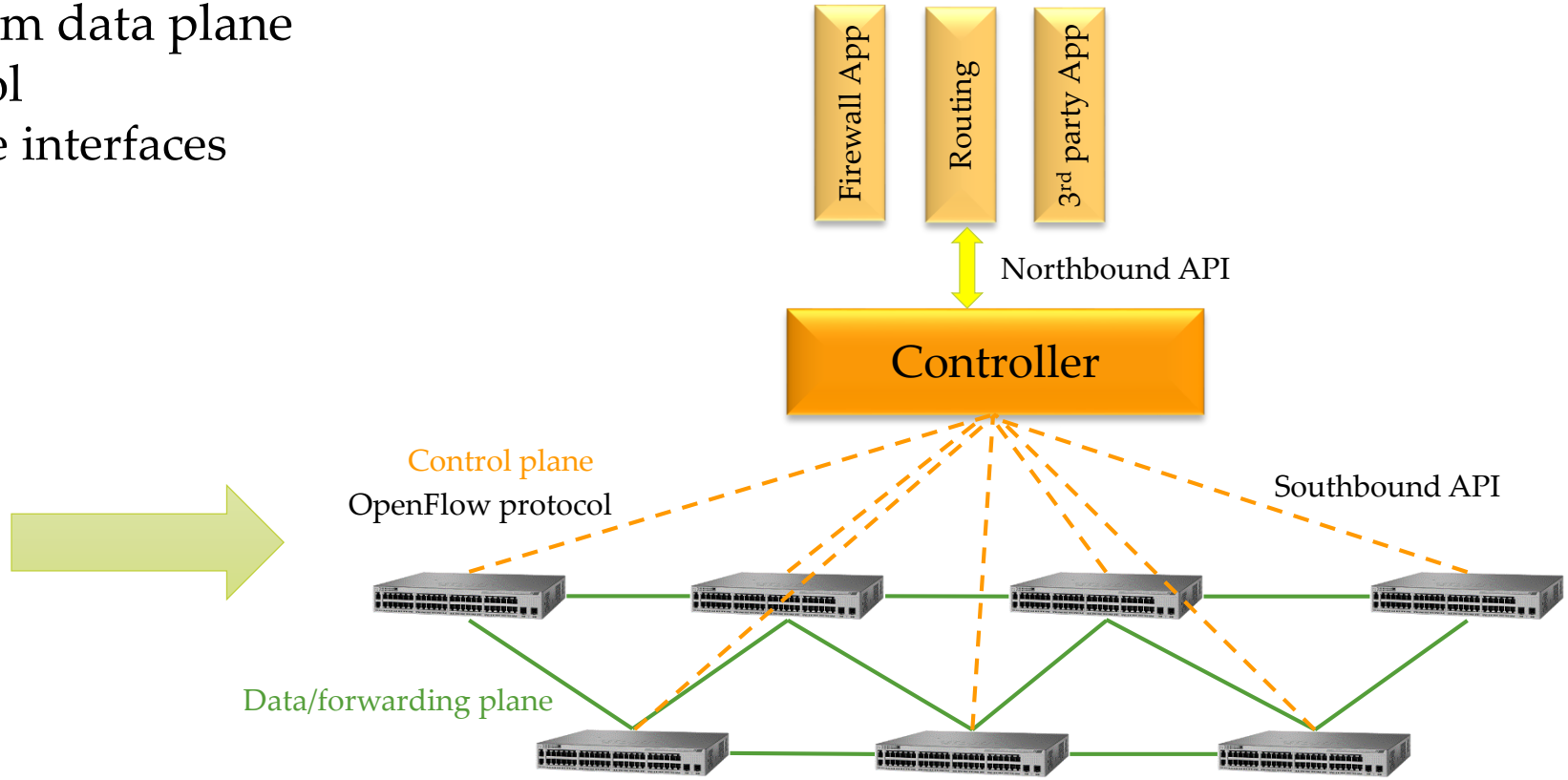
- Configuration management
  - Puppet
  - Chef
  - Ansible
  - Kubernetes
- Software defined networking (SDN)
- Open standard management protocols
  - NETCONF+YANG
  - CPE WAN management protocol (CWMP)

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

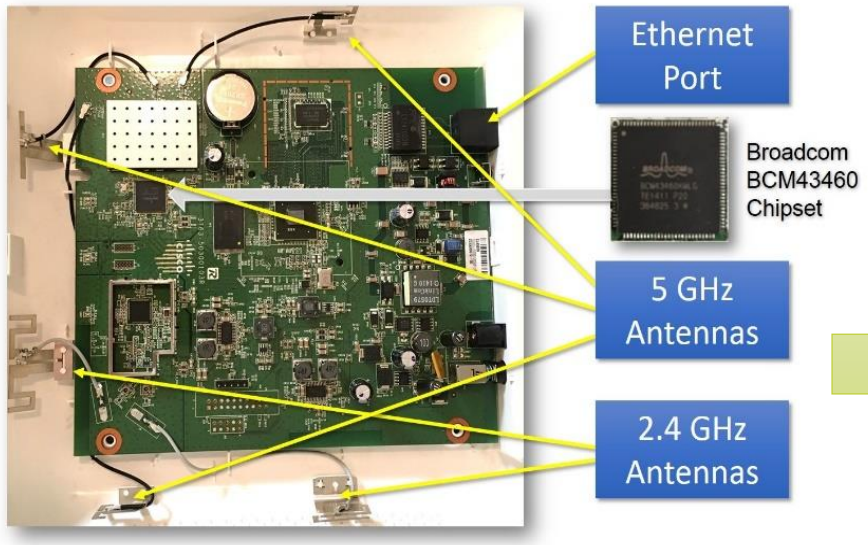


Cisco MDS9000 Family SAN Switch [1]

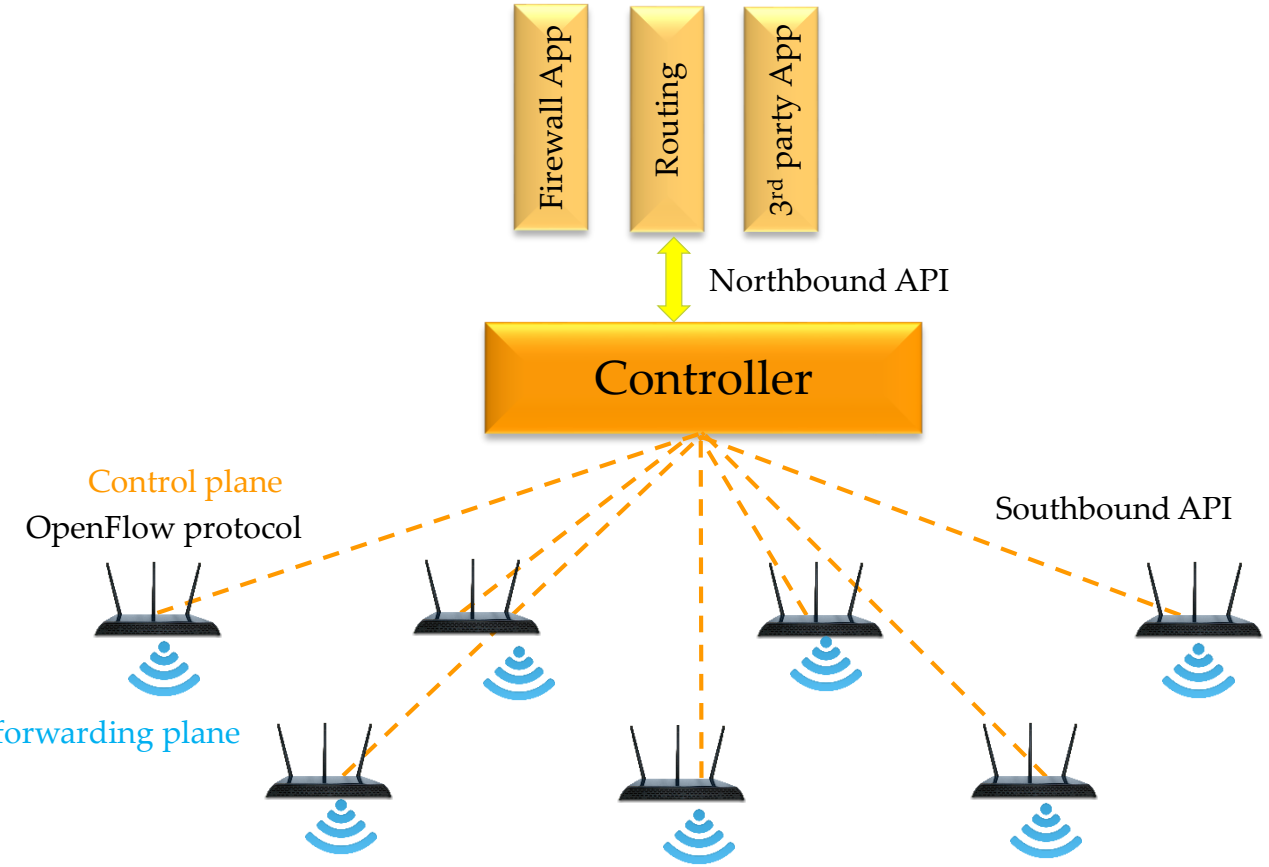


[1] https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/storage-networking-modules/prod_white_paper0900aecd8044c7e3.html

SDN with Wireless Access Points



Cisco WAP371[1]

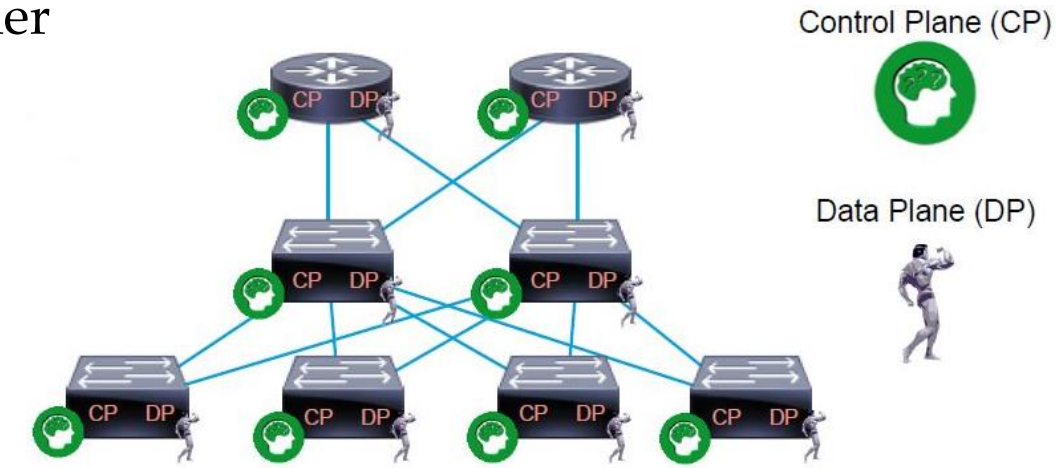


[1] http://www.tomcarpenter.net/2016/05/25/wireless-access-point-ap-internals-for-cisco-wap371/

Control Plane vs Data Plane

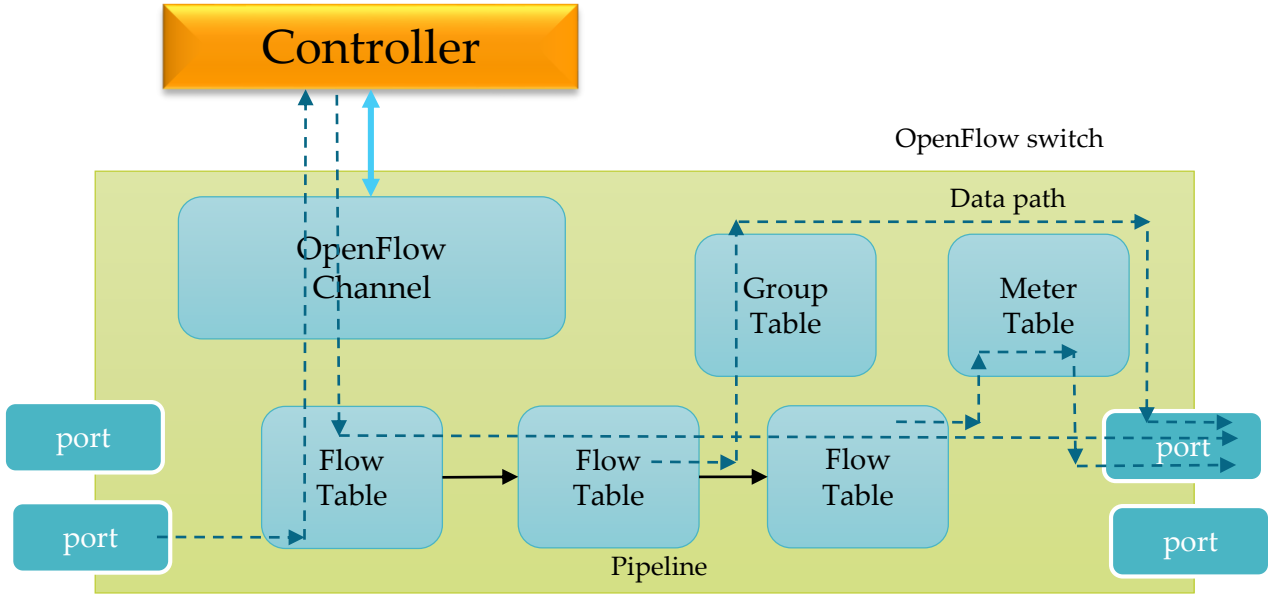
- Control Plane
  - Makes decisions how packet should be forwarded
  - Performs system configuration, management, and exchange of routing/forwarding tables

- Data/Forwarding Plane
  - Forwards traffic to from one client to another



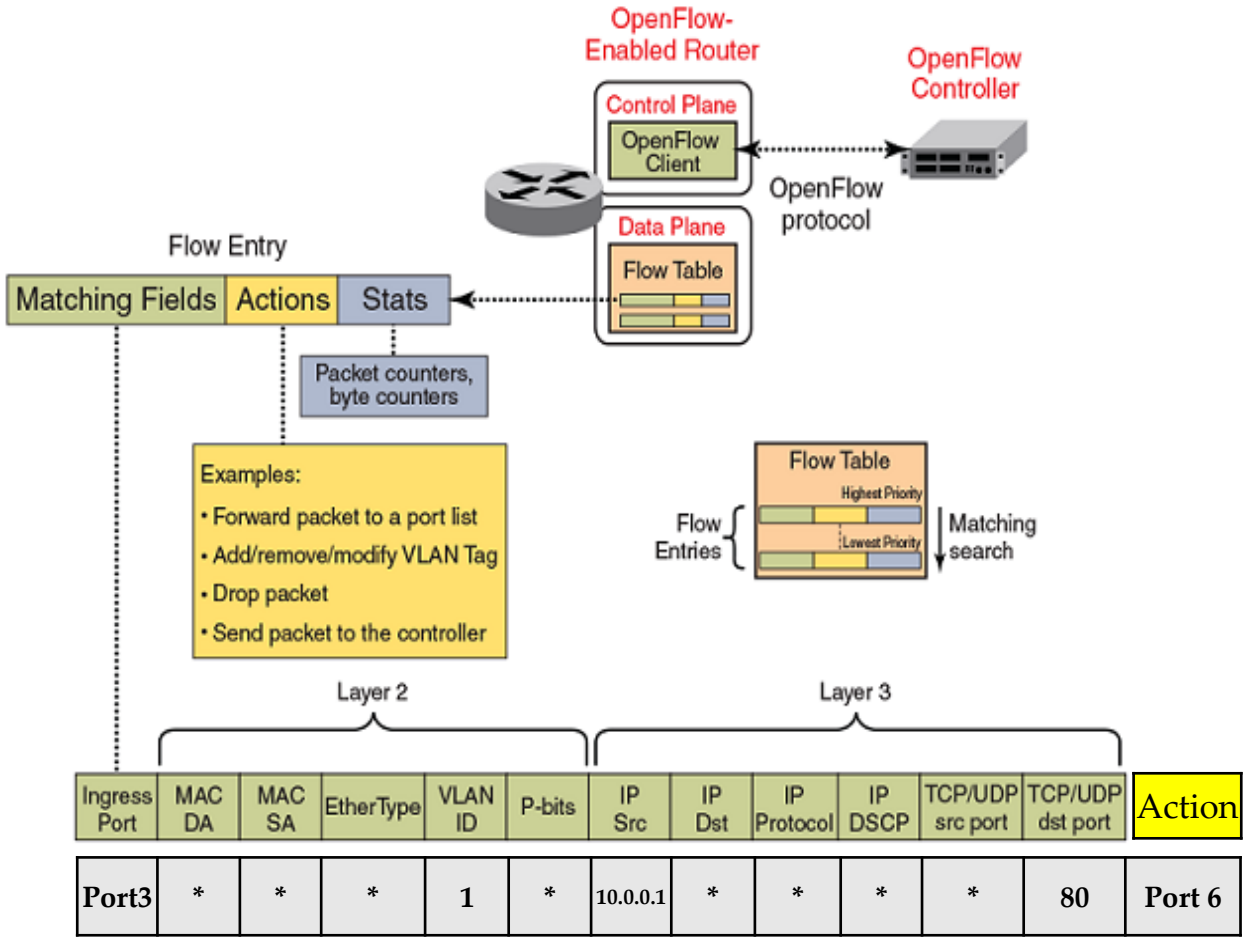
What is OpenFlow?

- 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



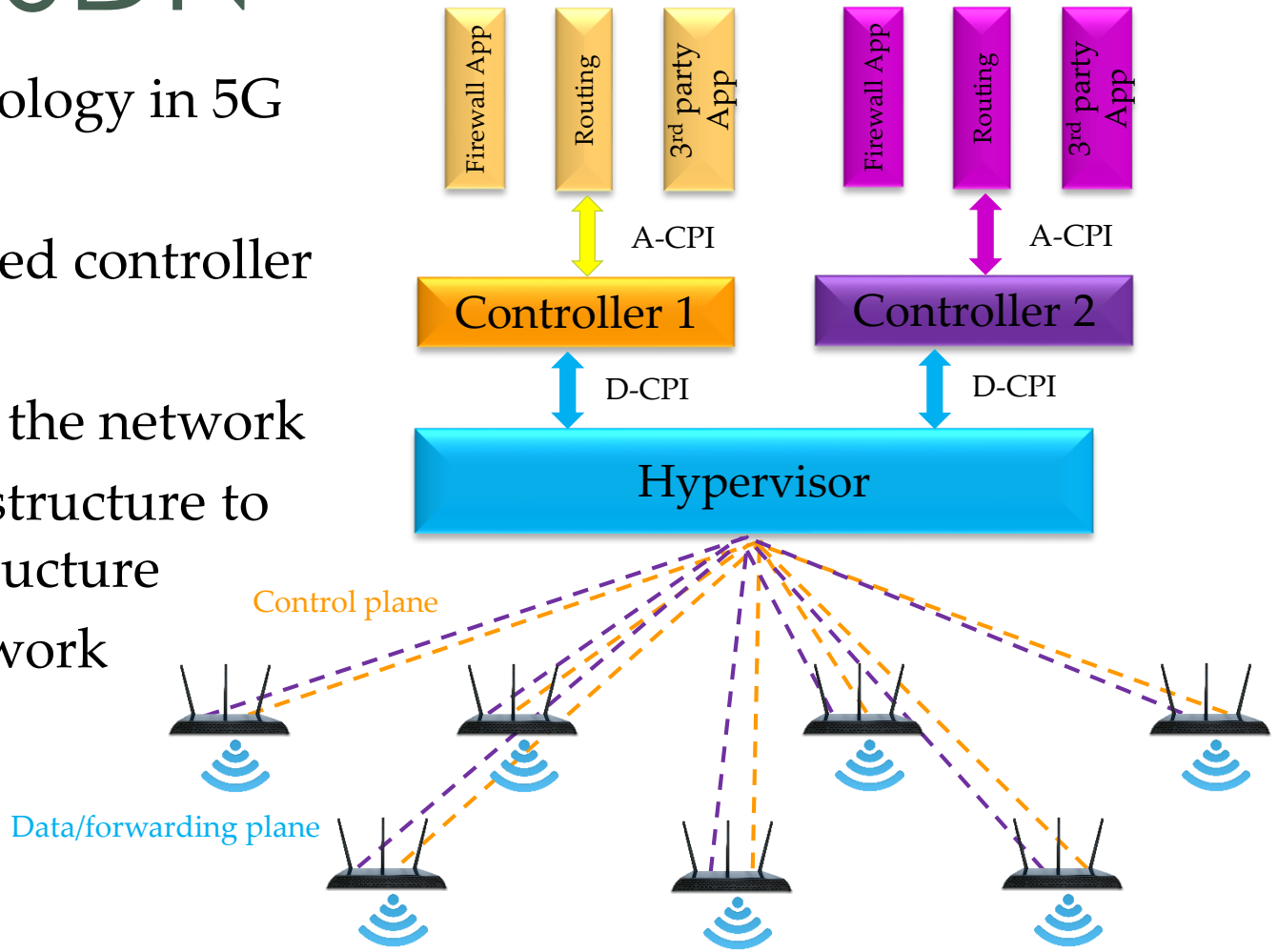
OpenFlow Components

- 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 switch and controller
- Flow: defined as all the packets matching a flow-entry in a switch'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

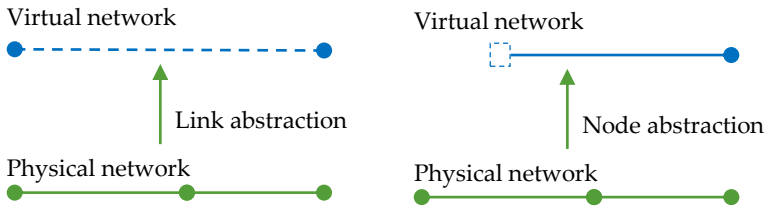


Network Virtualization

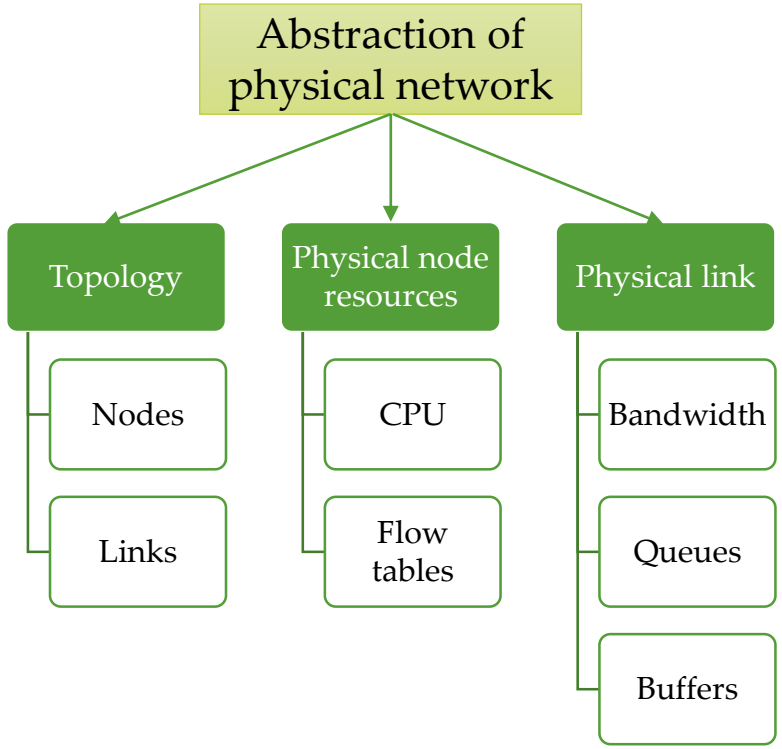
- Slice a given physical network infrastructure to multiple isolated virtual networks
- Existing network slicing techniques
  - Wavelength division multiplexing (WDM) at physical layer
  - Virtual local area networks (VLAN) at link layer
  - Multiple protocol label switching (MPLS)- creates slices of forwarding tables in switches

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

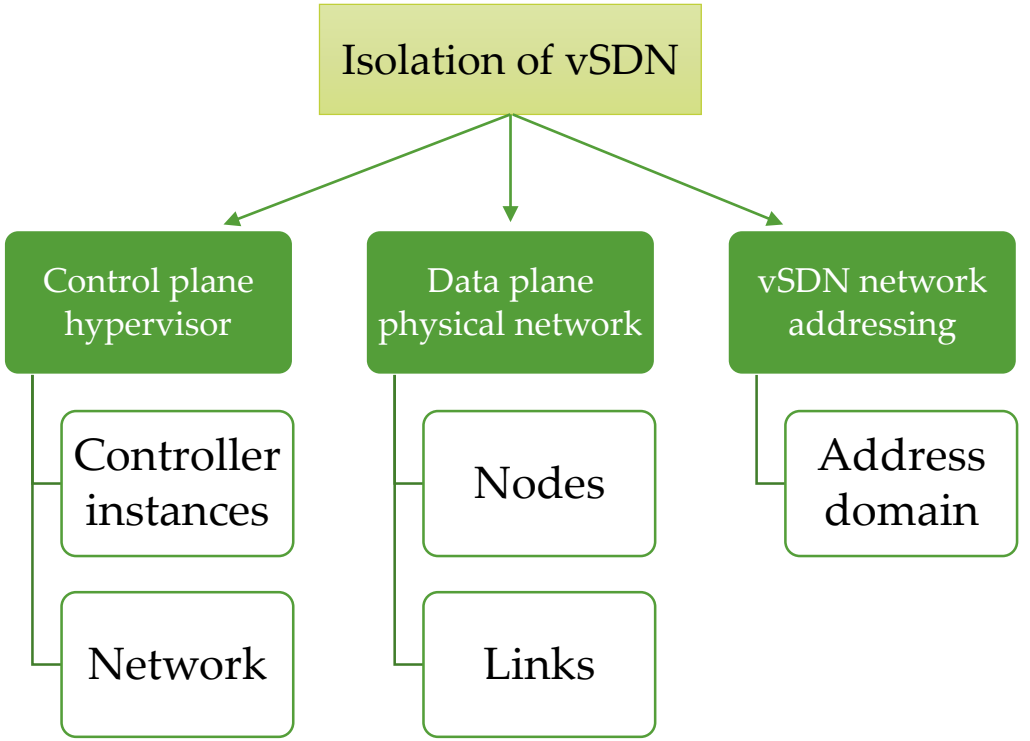


Topology Abstraction

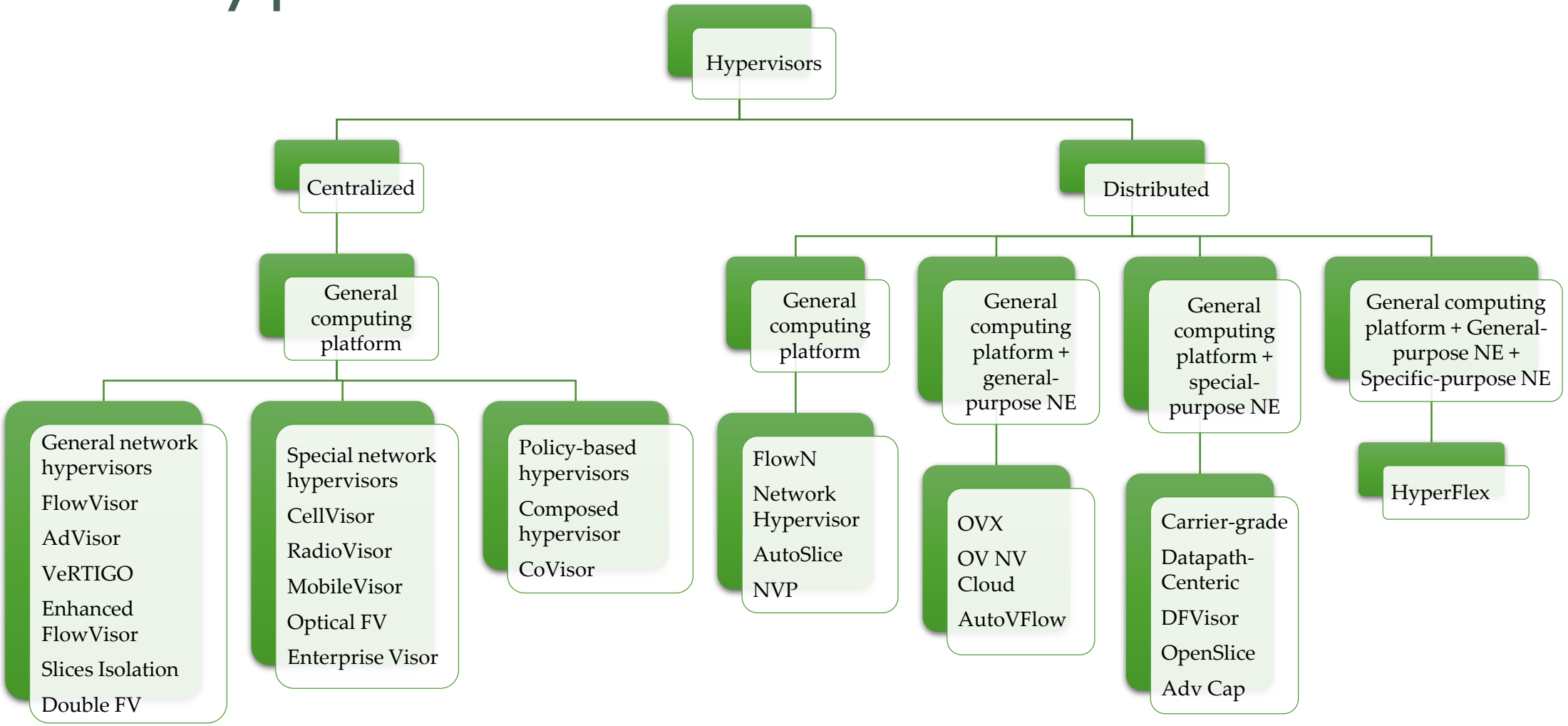


Isolation Attributes

1. Control plane isolation
2. Data plane isolation
3. vSDN addressing isolation



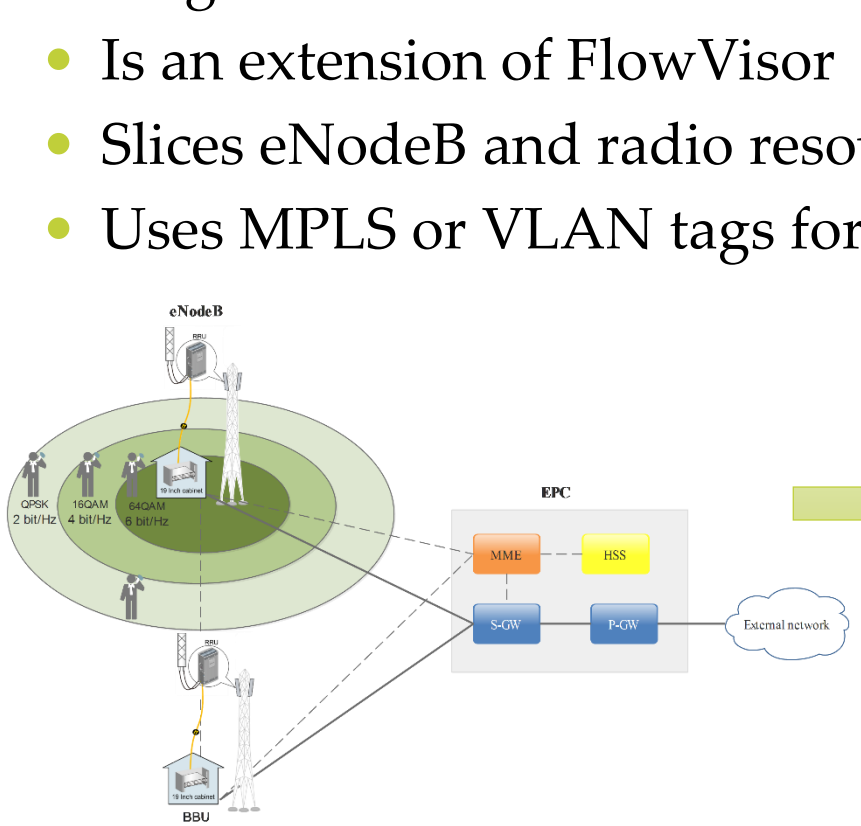
SDN Hypervisor Classification

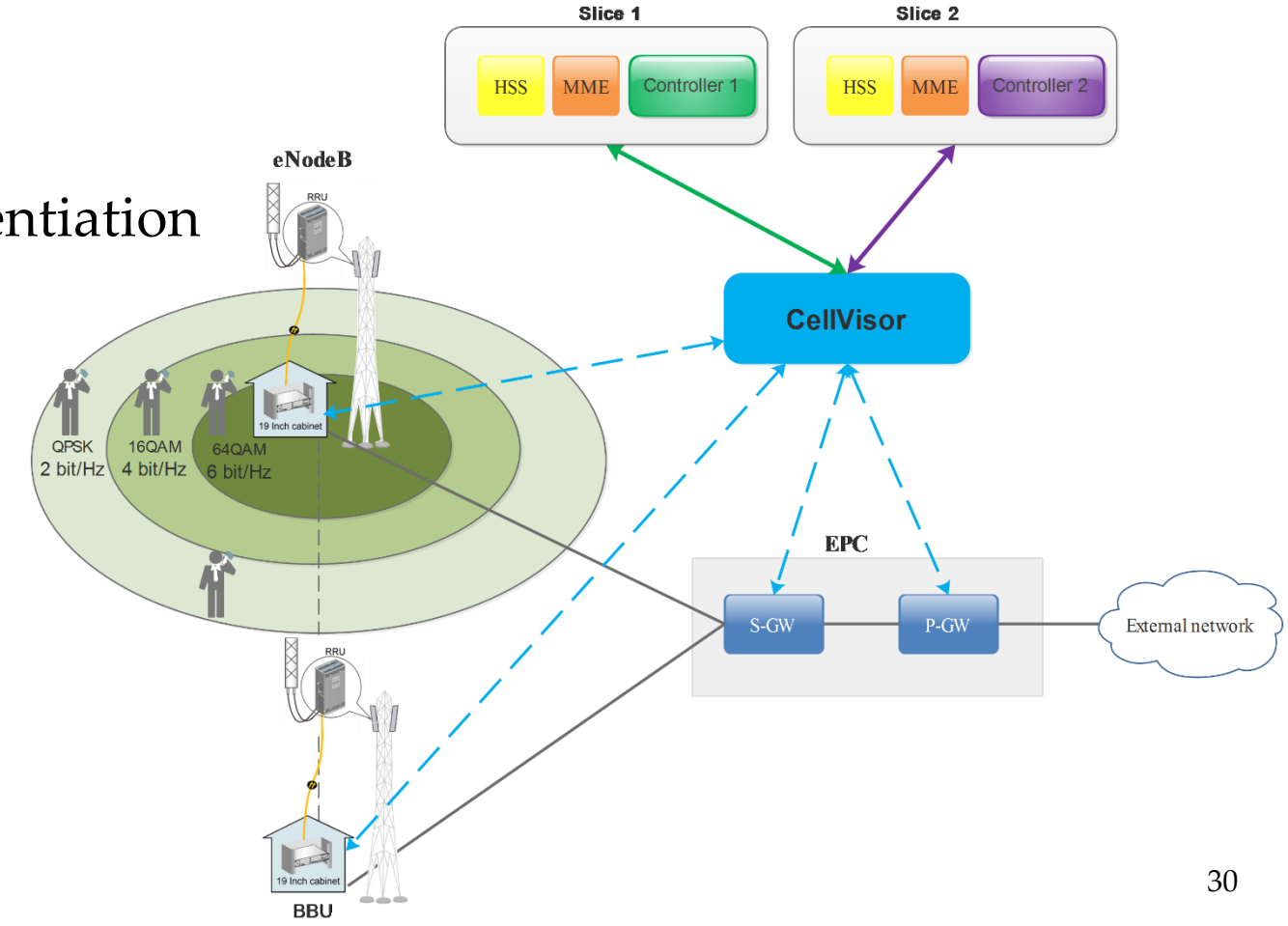


A. Blenk, A. Basta, M. Reisslein and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 655-685, Firstquarter 2016. doi: 10.1109/COMST.2015.2489183

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 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

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

NETCONF [1]

- Uses XML data encoding for configuration
- Uses data store concept
- Uses YANG [2] modelling language for defining semantics of configuration and operation data

Layer	Description
Content	Configuration data
Operations	Retrieve specified configuration (<get-config>) Edit configuration (<edit-config>)
RPC	RPC invocation (<rpc> message), RPC results (<rpc-reply> messages)
Transport Protocol	SSH, SSL, console

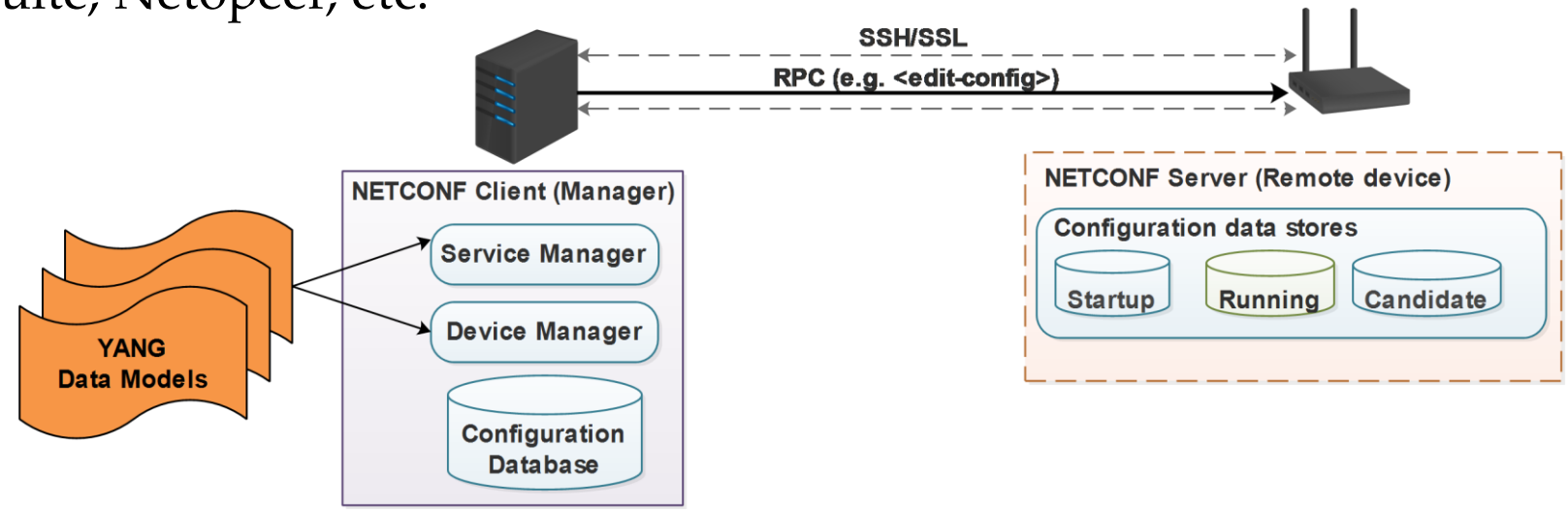
[1] https://tools.ietf.org/html/rfc4741
[2] https://tools.ietf.org/html/rfc6021

NETCONF Basic Operations

Layer	Description
<get>	Retrieve running configuration and device state information
<get-config>	Retrieve all or part of a specified configuration data store
<edit-config>	Edit a configuration data store by creating, deleting, merging or replacing content
<copy-config>	Copy an entire configuration data store to another configuration data store
<delete-config>	Delete a configuration data store
<lock>	Lock an entire configuration data store of a device
<unlock>	Release a configuration data store lock previously obtained with the <lock> operation

NETCONF

- NETCONF implemented on device by Cisco, Juniper, Huawei, etc.
- There are NETCONF open source implementations
  - YUMA, EnSuite, Netopeer, etc.

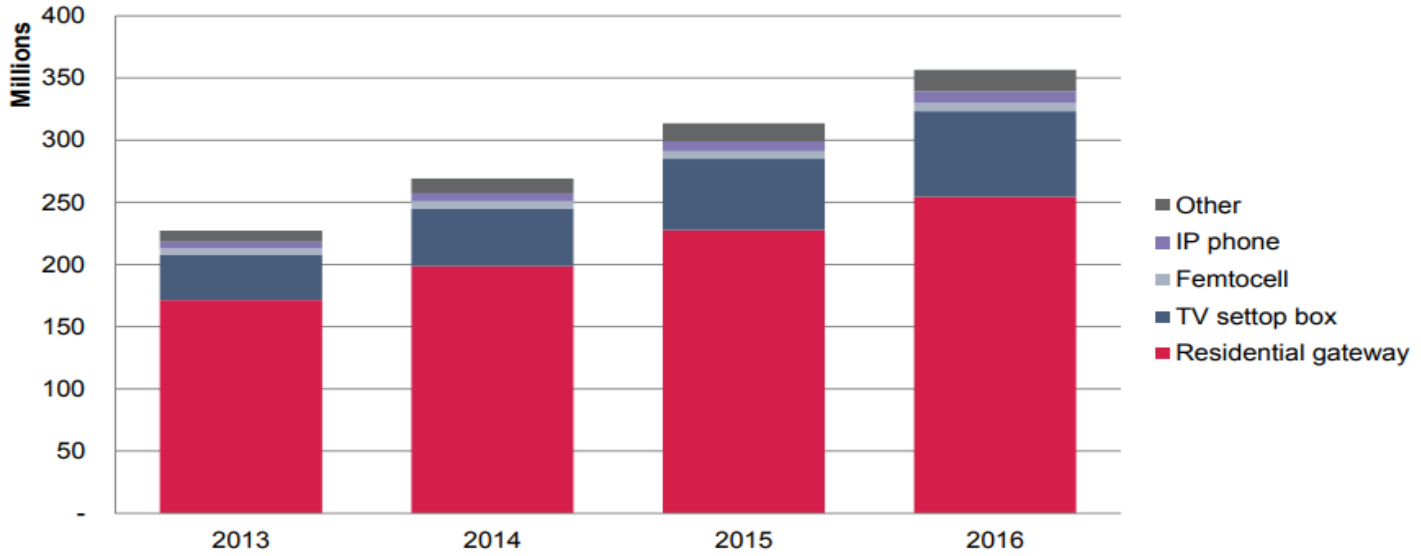


Can we use NETCONF for wireless management? (WLAN and distributed networks)

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

CPE WAN Management Protocol (CWMP)

- The CWMP which is referred as TR-069
- Enables communication between an auto-configuration server (ACS) and the customer premise equipment (CPE)

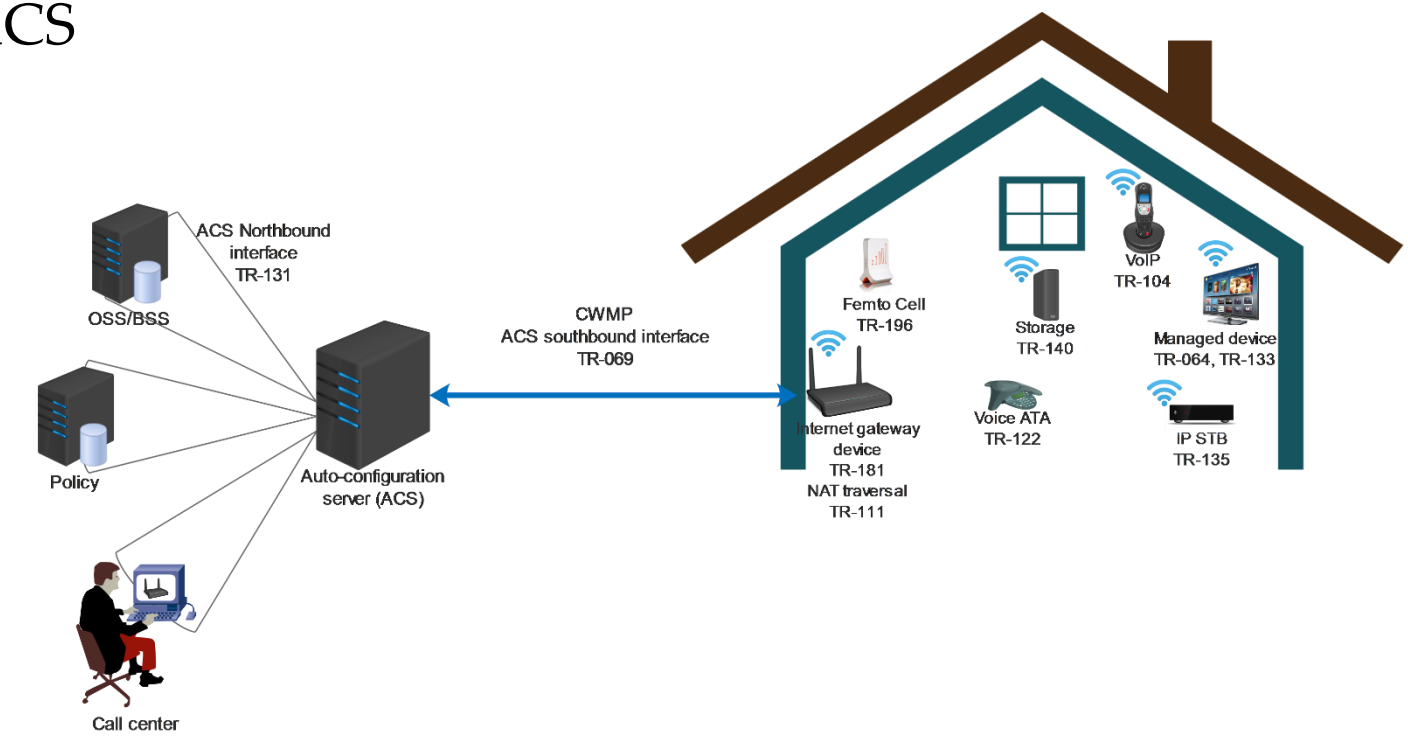


Estimated number of installed TR-069 based CPE globally by type during 2013-2016 in connected homes [1]

[1] http://info.ovum.com/uploads/files/TR_069_and_the_road_to_the_smart_home_webinar.pdf.

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



CWMP Protocol

- CWMP architecture consists of other standard protocols
- The RPC (remote procedure call causes a procedure to execute in a different address space) methods define generic mechanisms to read and write parameters of a CPE
- Parameters of a different class of CPE are defined separately in a specific data model
- SOAP is a protocol specification for exchanging XML

Layer	Description
CPE/ACS application	The application uses CWMP to establish connection
RPC methods	Define a generic mechanism to read and write specific parameters on CPE
SOAP	Standard XML based syntax to encode RPC methods
HTTP	Standard HTTP
SSL/TLS	Standard TLS, particularly TLS 1.2
TCP/IP	Standard TCP/IP

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 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

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

TR-069 Security Considerations

1. It is recommended to use TLS 1.2 or later version
2. It is recommended that auto-configuration server (ACS) URL is writable only through ACS
3. Different devices require different data models due to their different use cases and parameter set
4. The CWMP implementation must perform a data validation on the parameters used in the configuration in order to prevent code injection in TR-069 data model

Can we use TR-069 for wireless management? (WLAN and distributed networks)

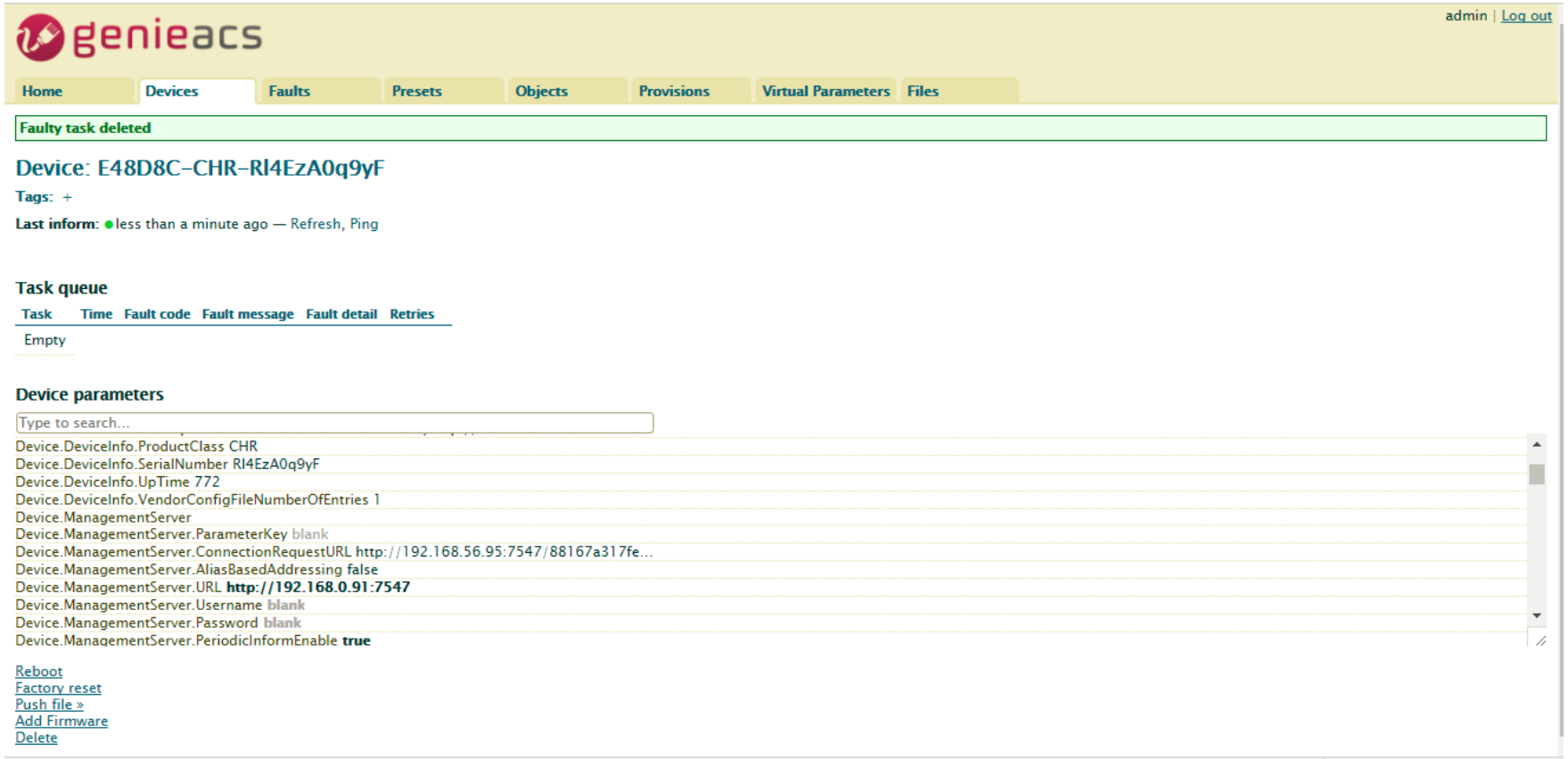
If YES then what would be optimal topology for implementing TR-069?

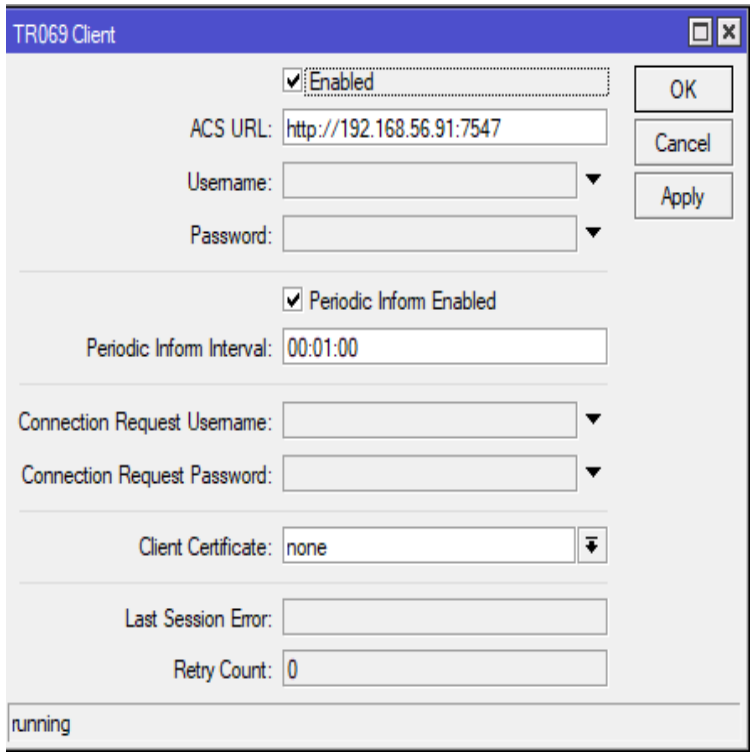
TR-069 CPE and ACS

- Open source ACS
  - GenieACS
  - FreeACS -> not maintained
  - LibreACS -> not maintained

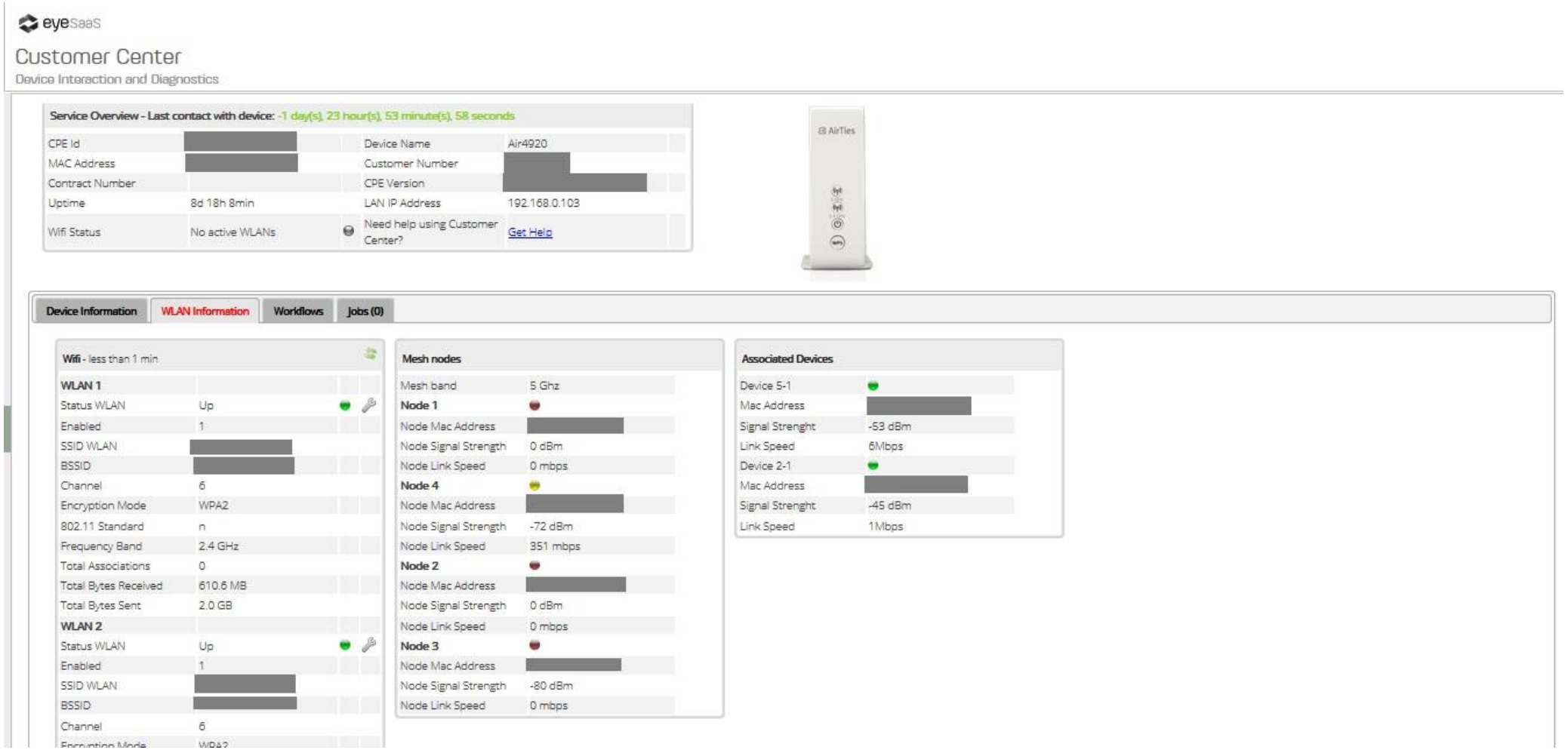
- EyeSaaS
- Axiros

GenieACS with Mikrotik TR-069 Client





EyeSaaS Platform



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)

Assignment

- Implement TR-069 environment for remote management of Mikrotik CPE
  1. Download Mikrotik Cloud Hosted Router (CHR) image on https://mikrotik.com/download then run VDI image on Virtualbox
  2. Install TR-069 client package on the CHR virtual machine
  3. Set up another virtual machine with Ubuntu 16.04 installed in the same network
  4. Run attached script to install GenieACS on the Ubuntu machine
  5. Open browser and enter your Ubuntu virtual machine IP address in address bar to access GenieACS GUI


Q&A