
TOMORROW
starts here.
CISCO
Cisco live!

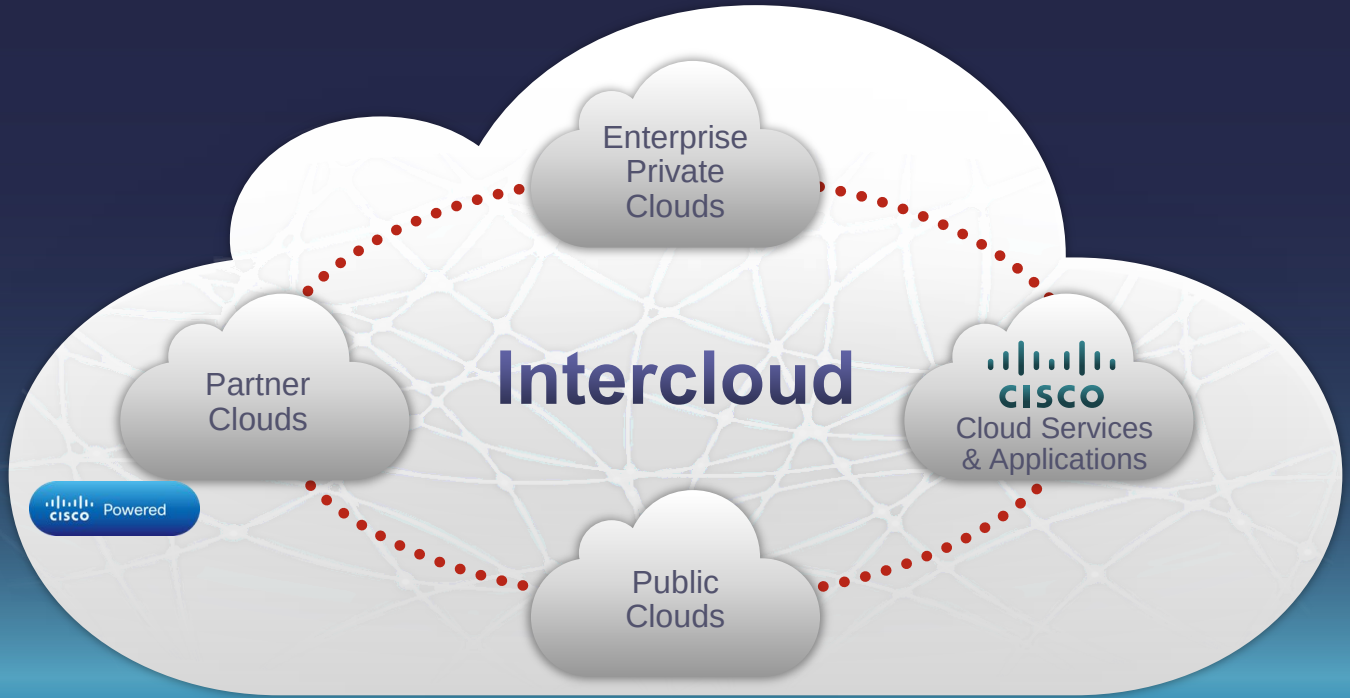
Virtualizing Cisco Service Provider Wi-Fi core

BRKSPM2006

Ravi Shankar & Piyush Patel

Cisco live!

Cisco Intercloud Strategy



Cisco Cloud Portfolio

Cisco Cloud Enablement Products and Solutions

Application Centric Infrastructure

Cisco Cloud Enablement Platform

- Service Catalog
- Orchestration and Automation
- Infrastructure Controller

Cisco Powered Architectures for Cloud Providers

Network Function Virtualization (NFV)

Integrated Infrastructure

FlexPod®

VBLOCK READY

Intercloud Fabric

Cloud Consulting Services

Cisco Cloud

Applications

- Cisco Cloud Apps
- Partner & ISV Apps
- IoE & Vertical Apps

Customer's Private Cloud

- On Premise
- Managed
- Hybrid

Application Enablement Platform & APIs

OpenStack Cloud Libraries

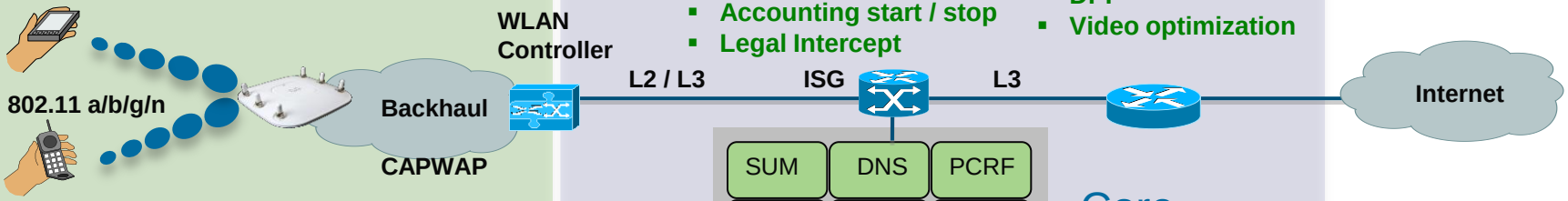
Platform & Infrastructure Services

Application Centric Infrastructure

Agenda

- Virtualizing existing architecture
  - Service instances
  - Subscriber experience and provider highlights
- Hospitality case study
- 3G/4G integration options
- Scaling and orchestration
  - Openstack
  - Elastic Services controller
  - Prime fulfillment

WiFi end to end solution architecture: ISG



- Session management
- L4 Redirection
- Transparent Auto Logon
- Policy enforcement
- Accounting start / stop
- Legal Intercept

- NAT
- Firewall
- DPI
- Video optimization

Core Network

- WLAN Policy
- RRM
- WiFi Mobility
- EAP Authentication
- Rouge AP detection
- Client Link
- Band Select
- Hotspot 2.0
- WiFi security
- Flexconnect
- Cleanair

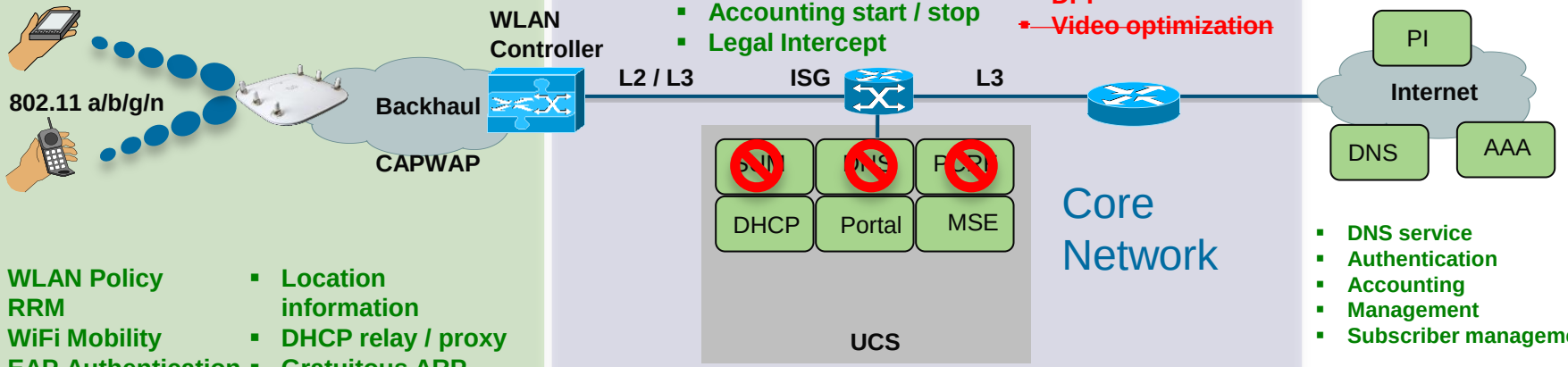
- Location information
- DHCP relay / proxy
- Gratuitous ARP
- WLAN / VLAN bridging

WLAN Access

- Subscriber management
- Subscriber authentication
- Service authorization
- Web portals
- Policy definition
- Roaming

- Address assignment
- Accounting / Billing
- Whitelisting
- Location awareness
- Network Analytics

What to virtualize?



- WLAN Policy
- RRM
- WiFi Mobility
- EAP Authentication
- Rouge AP detection
- Client Link
- Band Select
- Hotspot 2.0
- WiFi security
- Flexconnect
- Cleanair

- Location information
- DHCP relay / proxy
- Gratuitous ARP
- WLAN / VLAN bridging

WLAN Access

- Session management
- L4 Redirection
- Transparent Auto Logon
- Policy enforcement
- Accounting start / stop
- Legal Intercept

- NAT
- Firewall
- ~~DPI~~
- ~~Video optimization~~

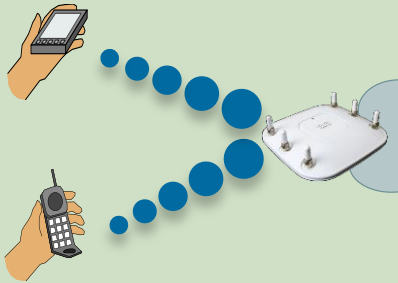
Core Network

- ~~Subscriber management~~
- ~~Subscriber authentication~~
- ~~Service authorization~~
- Web portals
- Policy definition
- Roaming

- Address assignment
- ~~Accounting / Billing~~
- Whitelisting
- Location awareness
- Network Analytics

- DNS service
- Authentication
- Accounting
- Management
- Subscriber management

Virtualized WiFi instance



- WLAN Policy
- RRM
- WiFi Mobility
- EAP Authentication
- Rouge AP detection
- Client Link
- Band Select
- Hotspot 2.0

- WiFi security
- Flexconnect
- Cleanair
- Location information
- DHCP relay / proxy
- Gratuitous ARP
- WLAN / VLAN bridging

WLAN Access

WLAN Controller

Backhaul

CAPWAP

L2 / L3

ISG

L3

NAT

- Session management
- L4 Redirection
- Transparent Auto Logon
- Policy enforcement
- Accounting start / stop
- Legal Intercept

- NAT
- Firewall

DHCP

Portal

MSE

UCS

Core Network

- Web portals
- Policy definition
- Roaming
- Address assignment
- Whitelisting

- Location awareness
- Network Analytics
- BBX – Ad insertion

PI

Internet

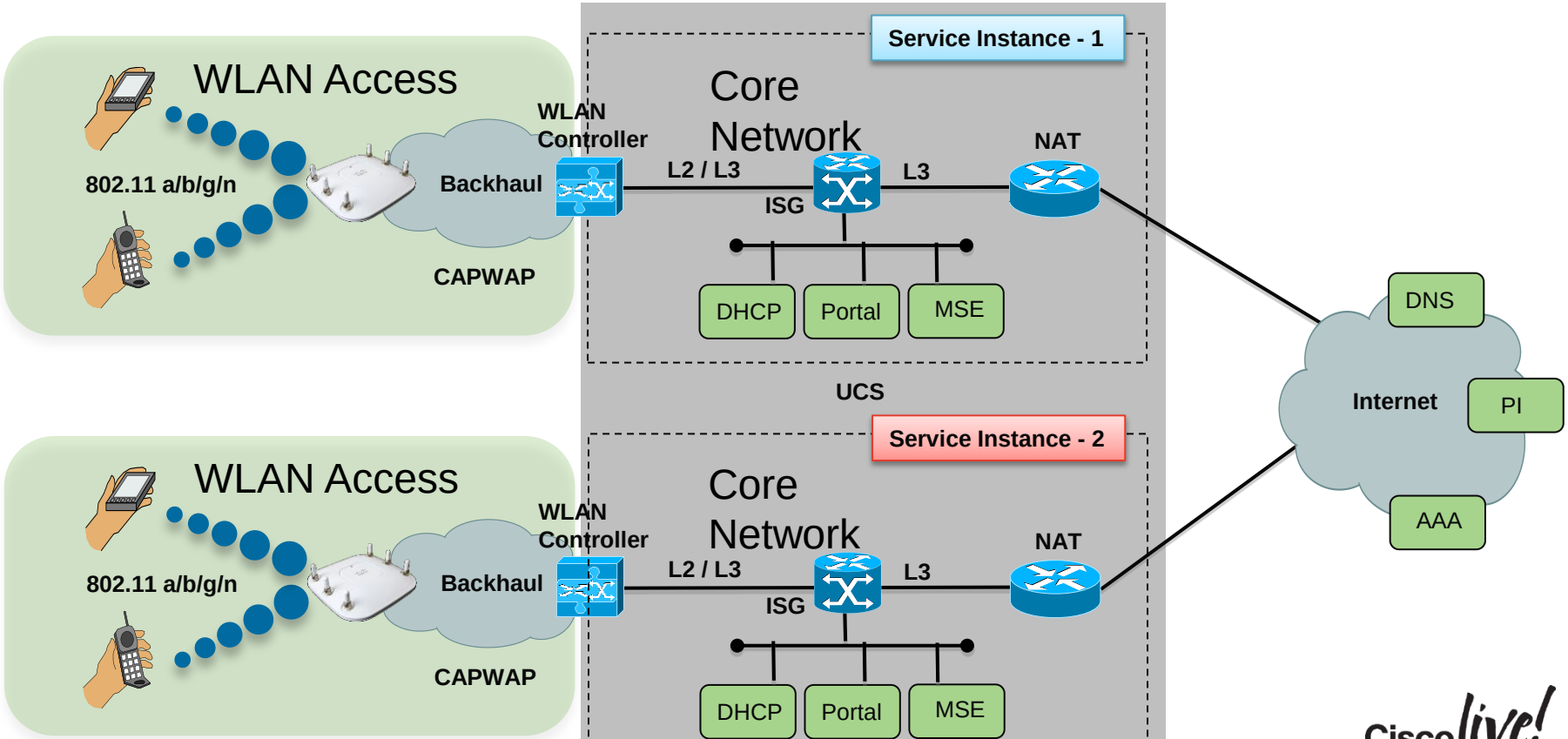
DNS

AAA

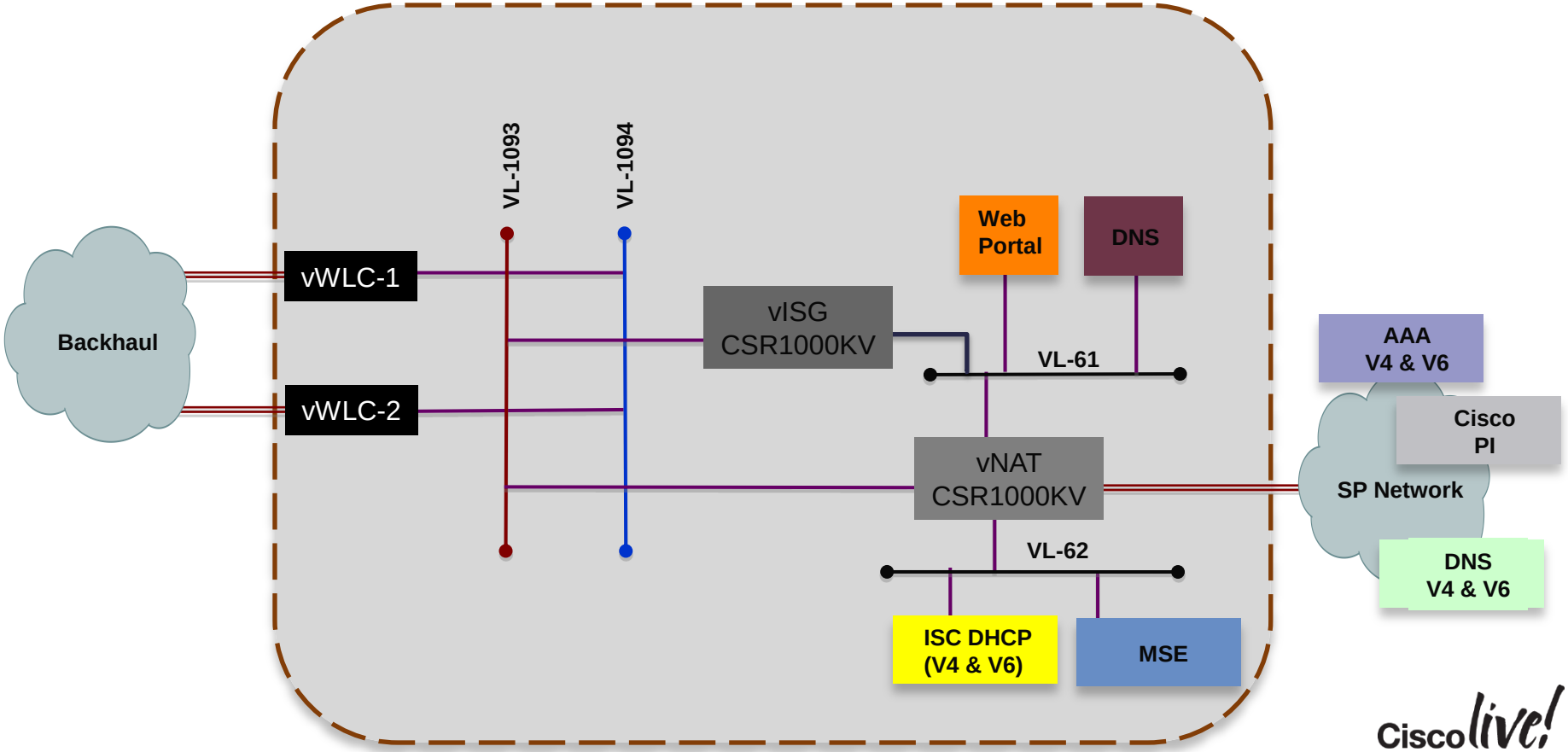
- DNS service
- Authentication
- Accounting
- Management
- Subscriber management

Cisco live!

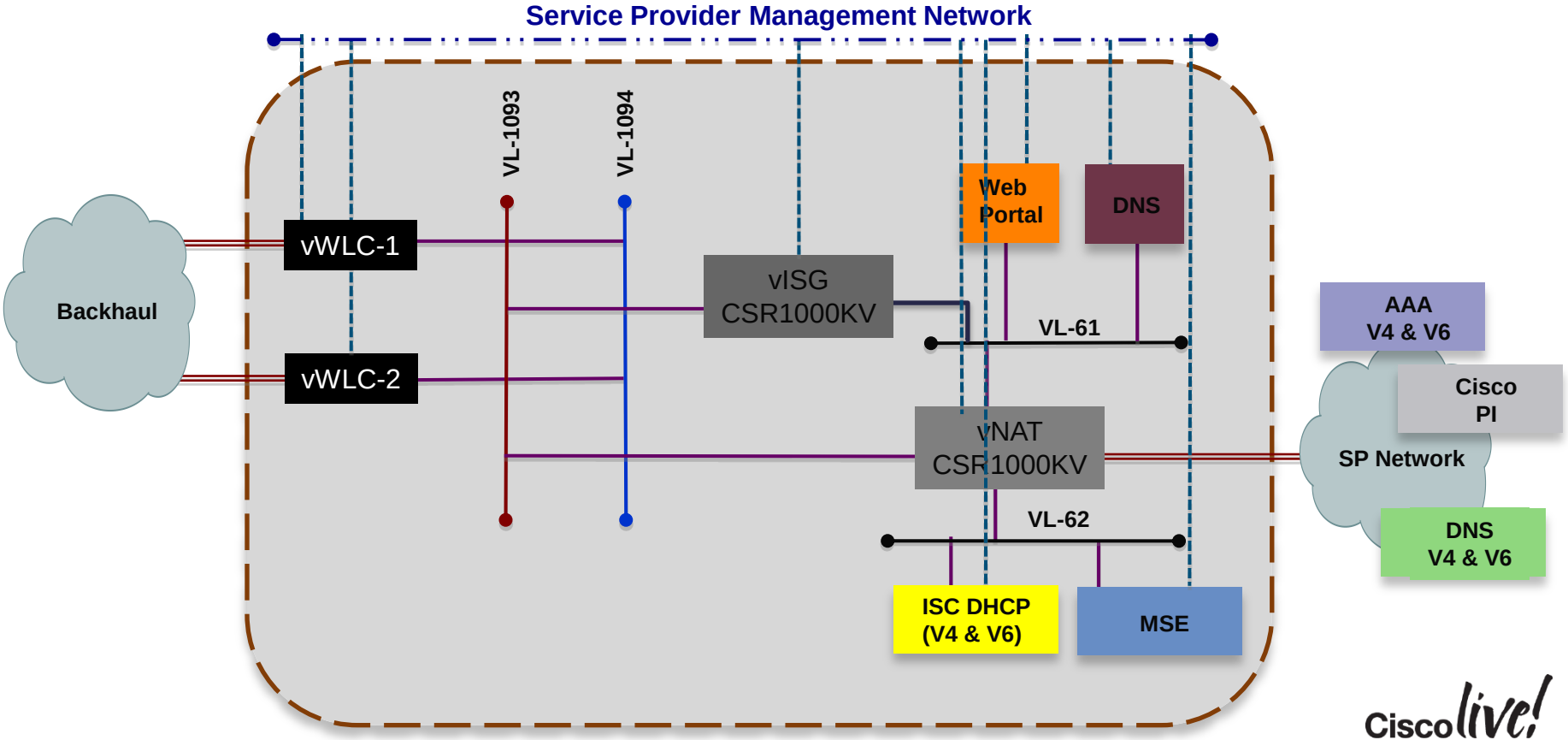
Virtualized WiFi Service Instances



Virtual WiFi



Out of band management access



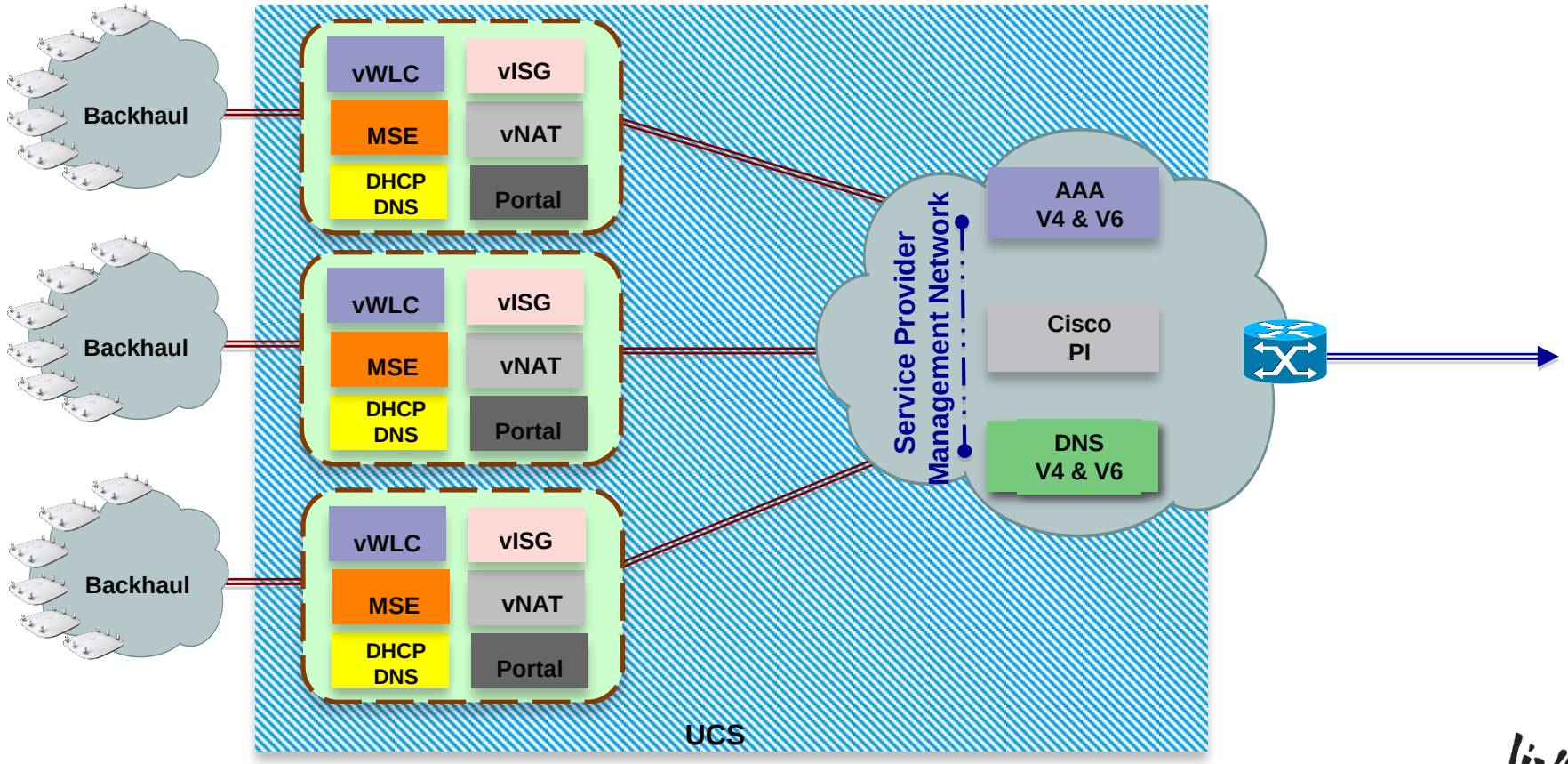
Differences between service instances

- IP addresses for all components on the SP **management** network
- Public IP addresses for virtual WLC's
- NAT pool for each service instance
- VLAN's must be unique per service instance within a cluster

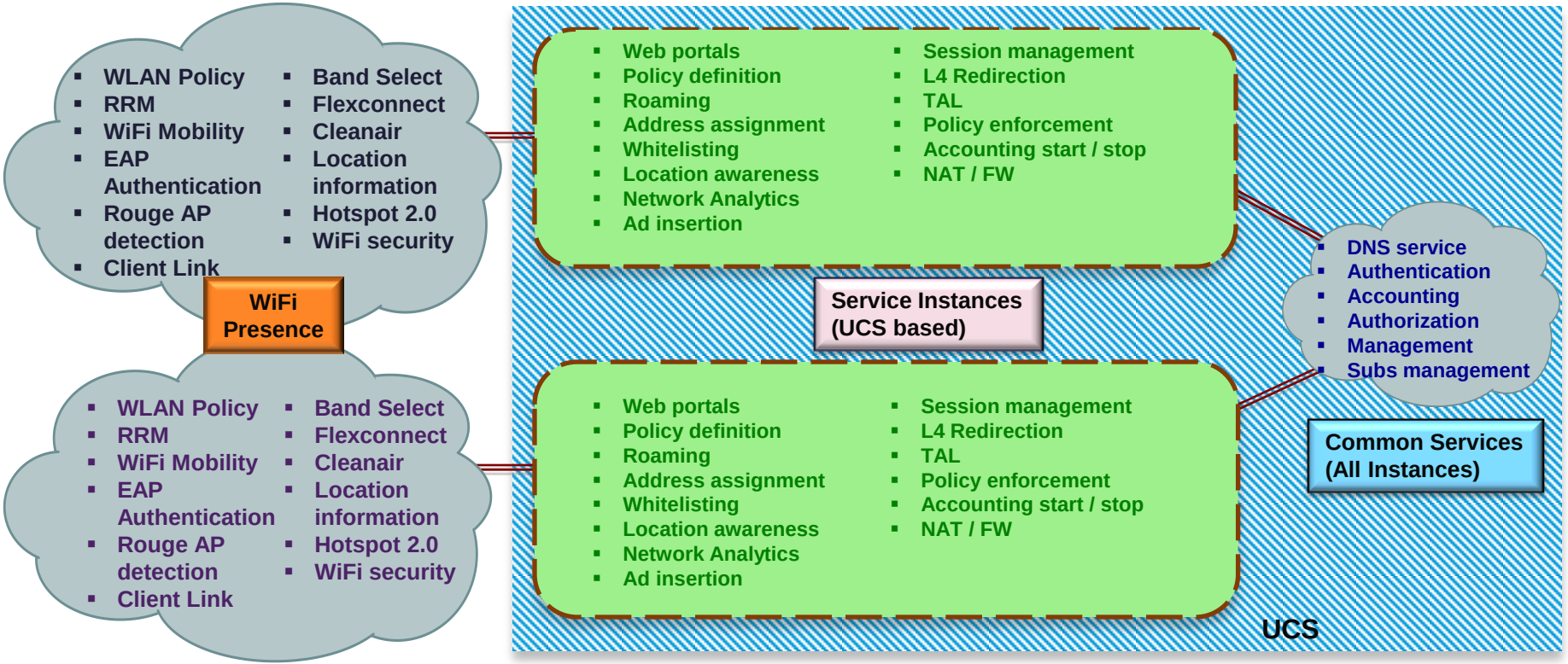
Everything else remains the same across ALL service instances

Cisco live!

Multiple Instances



Virtual WiFi service – feature mapping

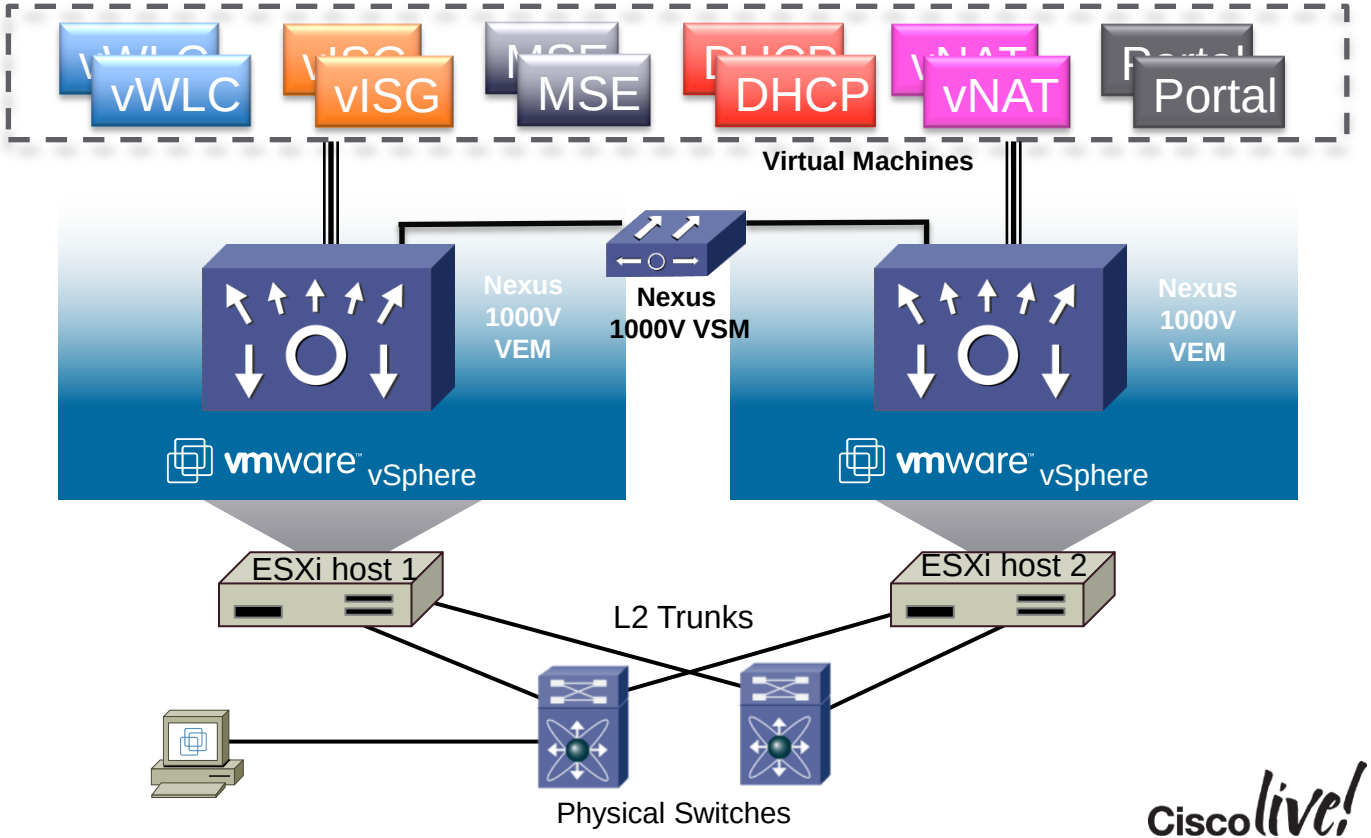


Layer 2 Connectivity with Nexus 1000v

Policy-Based VM Connectivity

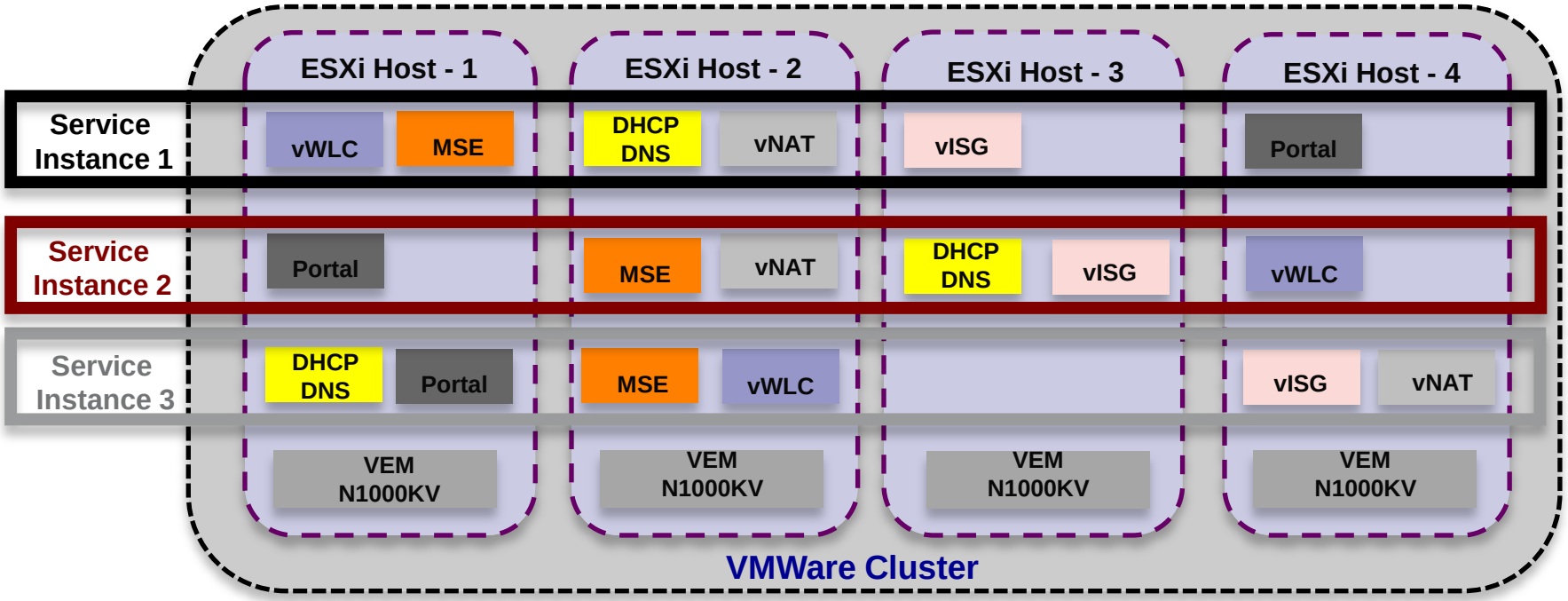
Network mobility

Non-Disruptive Operational Model

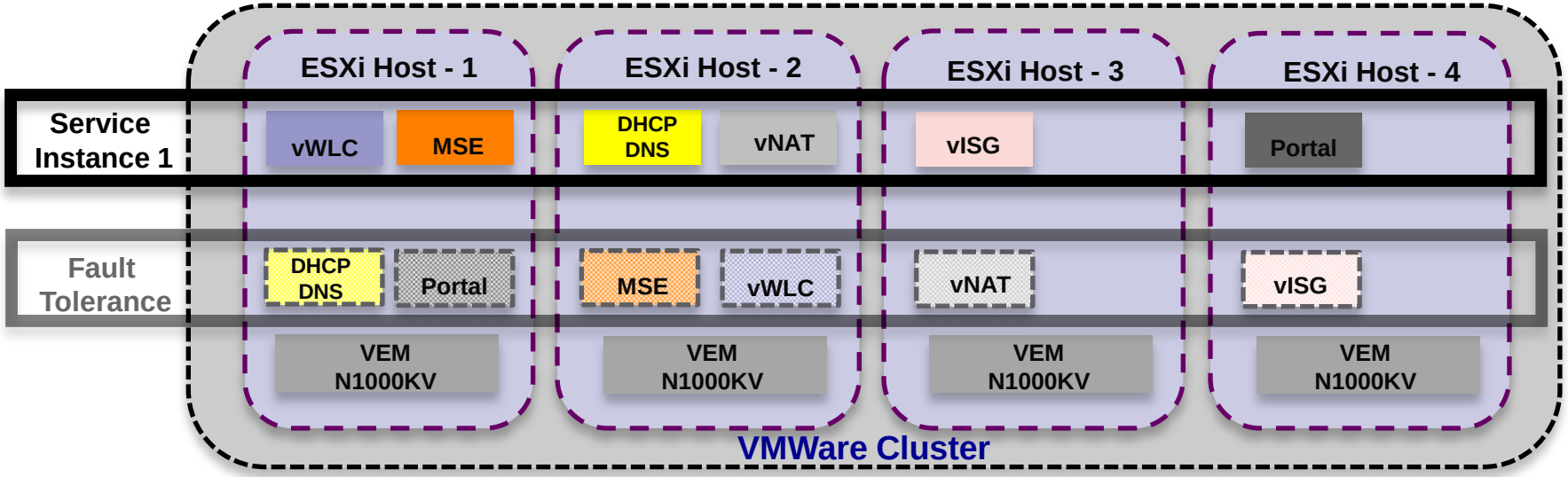


Cisco live!

Service Instances across a cluster



Fault tolerance for service instances



- Only VM's with a single vCPU can be made fault tolerant
- Virtual hard disk should be set up as Thick eager zeroed
- Only 4 Fault Tolerant VM's per ESXi host

Service Instance: subscriber experience

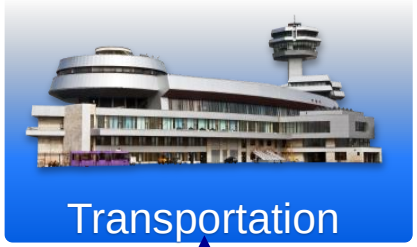
- VLAN based (Location based) portals
- User name / password based web authentication
- Transparent auto logon
- 3 Tiers of service (URANIUM, PLATINUM, TITANIUM)
- Support for dual-stack clients (IPv4 and IPv6)
- Policy enforcement on ISG (Downstream and upstream BW)
- Session management and AAA based accounting
- Location based Advertisement insertion

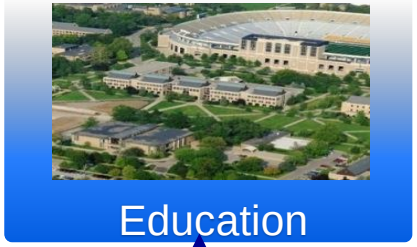
Service Instance: Provider feature highlights

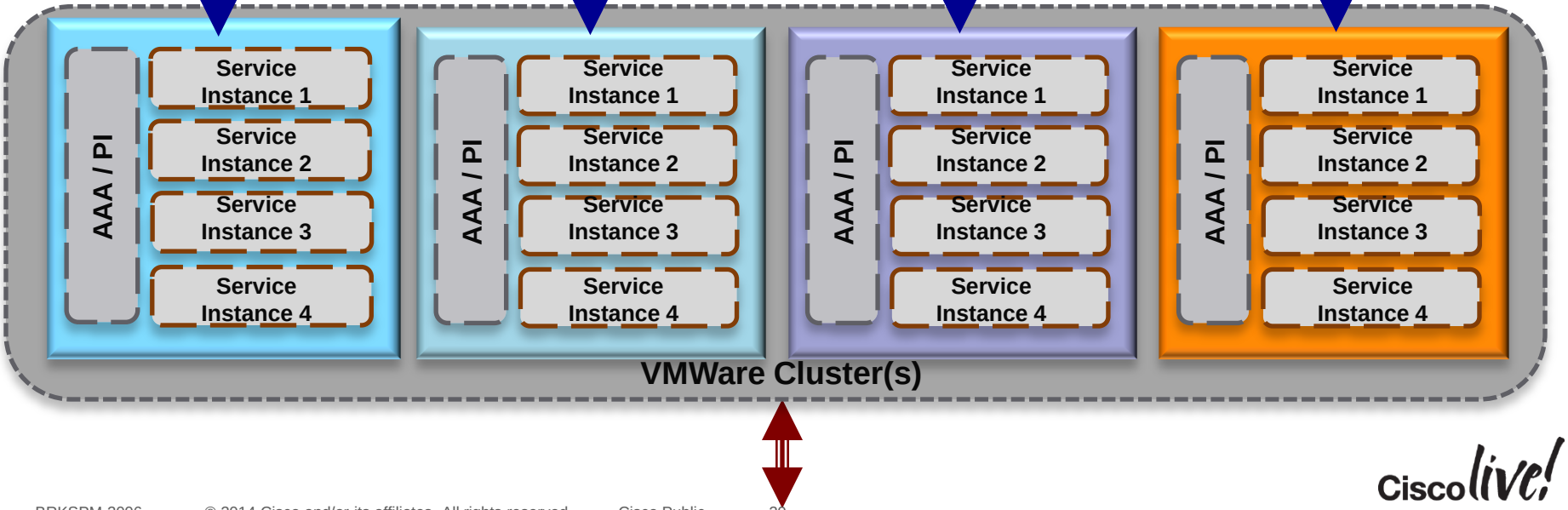
- License based solution (No actual hardware other than UCS)
- Rapid deployment of service instances – reduced risk
- On demand service replication with feature consistency
- Common accounting / authorization / authentication
- Common management of multiple instances
- Isolation between service instances (Separate external policy – DPI)
- VMWare cluster based service redundancy
- Consistent subscriber experience across all service instances
- Opportunity to customize service instances if required
- Monetization potential (Analytics, Ad insertion)

Reduced TCO

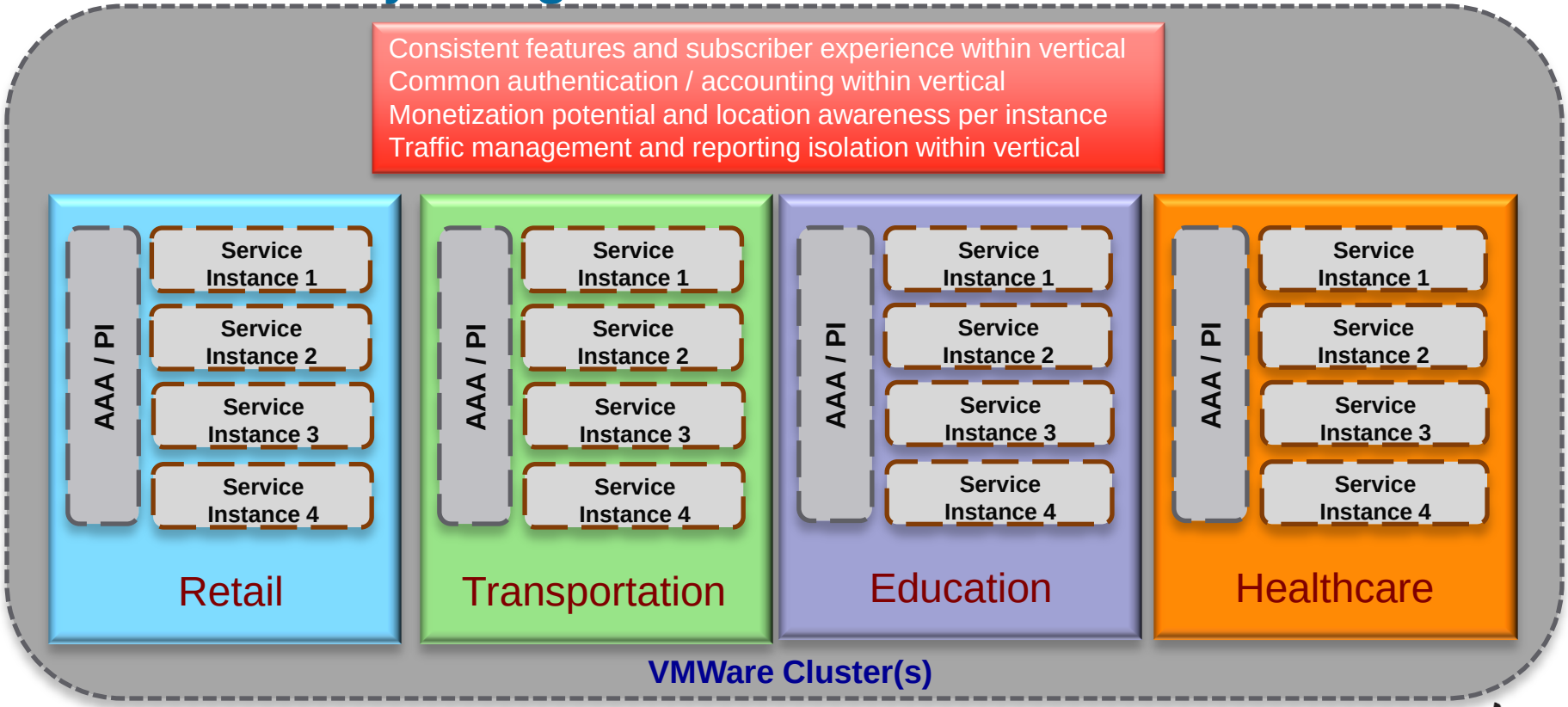
Other Verticals







Multi tenancy, single cluster



Hospitality Case Study

Cisco live!

Hospitality case study – requirements 1

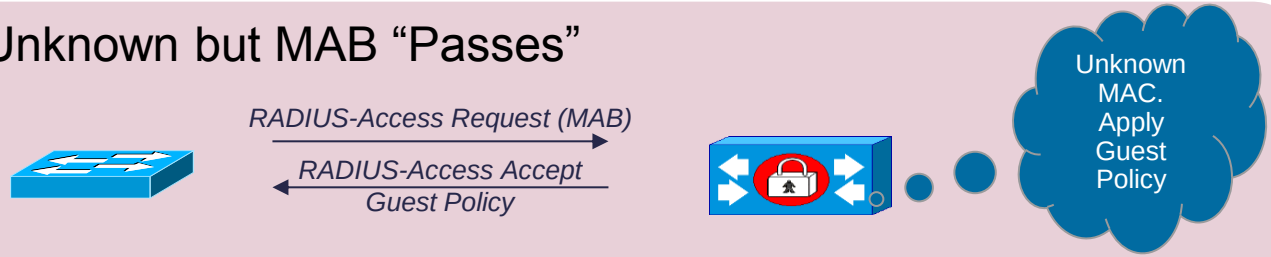
- Wireless Access
  - Open SSID for guests with Web-portal authentication
  - Hotel-only hidden SSID for staff with 802.1X based authentication
  - On demand conference SSID
- Wired Access
  - Guest VLAN has limited access to local resources
  - Staff / Hotel VLAN is protected by 802.1X (MAB – MAC authentication bypass)
- Transport
  - All guest traffic (Wired and wireless) backhauled to SP NOC
  - All hotel traffic (Wired and wireless) is locally switched
- Policy enforcement
  - QoS applied locally on switch ports and ISR for hotel staff
  - Guest QoS centrally enforced by SP
  - Per SSID QoS for conference SSID

Hospitality case study – requirements 2

- Authentication
  - Central AAA interface to on property PMS (Wired and Wireless guest access)
  - 802.1X (MAB – MAC authentication bypass) for hotel-only wired access
- Billing and accounting
  - Centralized billing / accounting and reporting
- Management
  - All WiFi routing and switching assets on property are centrally managed by SP
  - Guest access is validated against local PMS entries (Room No: and last name)
  - Wired access (MAB) for printers and other devices preconfigured by SP
- Same IP address range across all properties
- Guest portal customized per property

WIRED Users – MAB (MAC Auth Bypass)

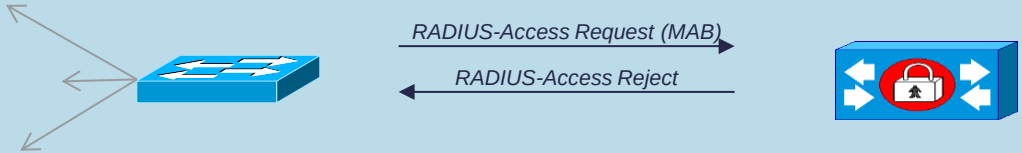
Option1: MAC is Unknown but MAB “Passes”



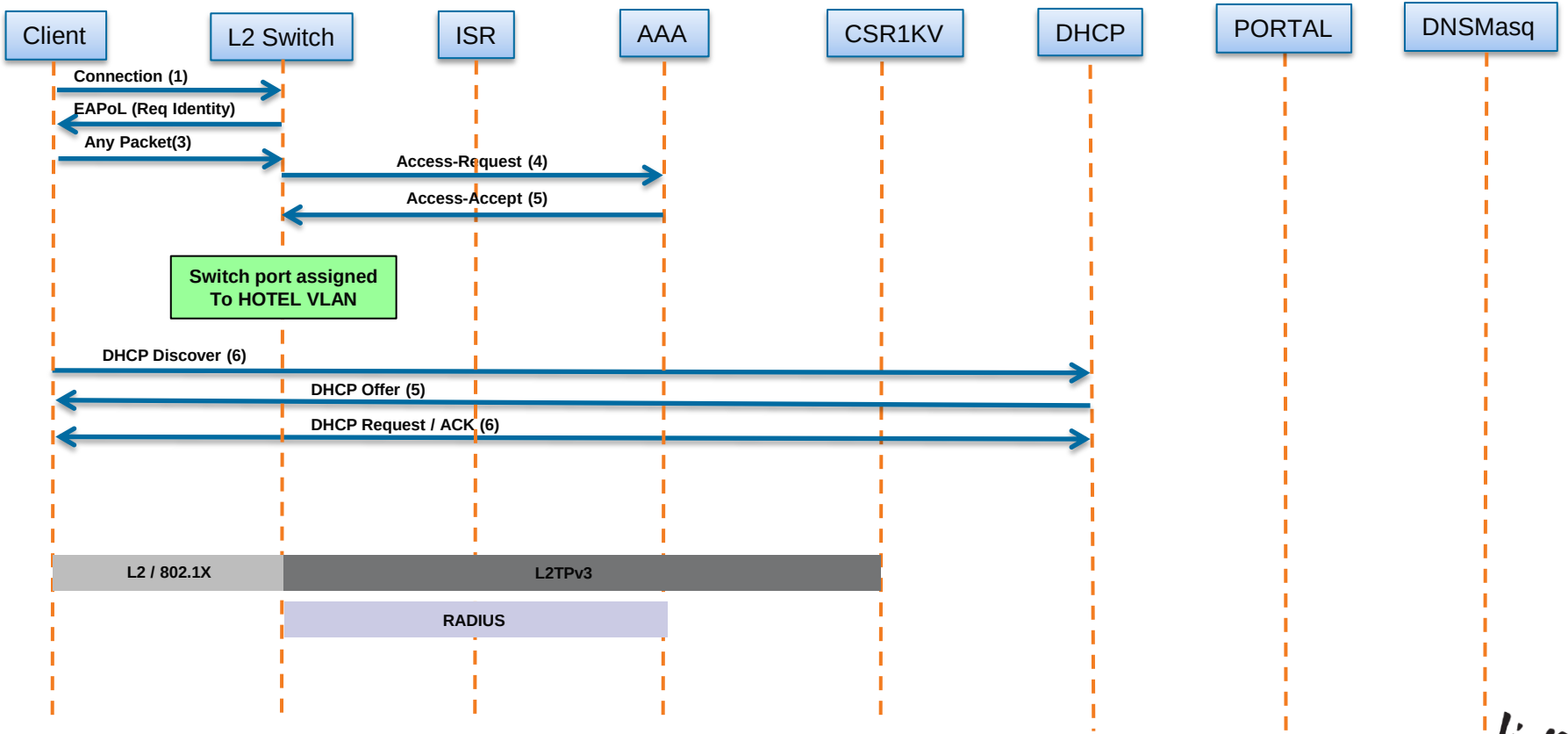
- AAA server determines policy for unknown endpoints (e.g. network access levels, re-authentication policy)
- Good for centralized control & visibility of guest policy (VLAN, ACL)

Option 2: MAC is Unknown and MAB Fails

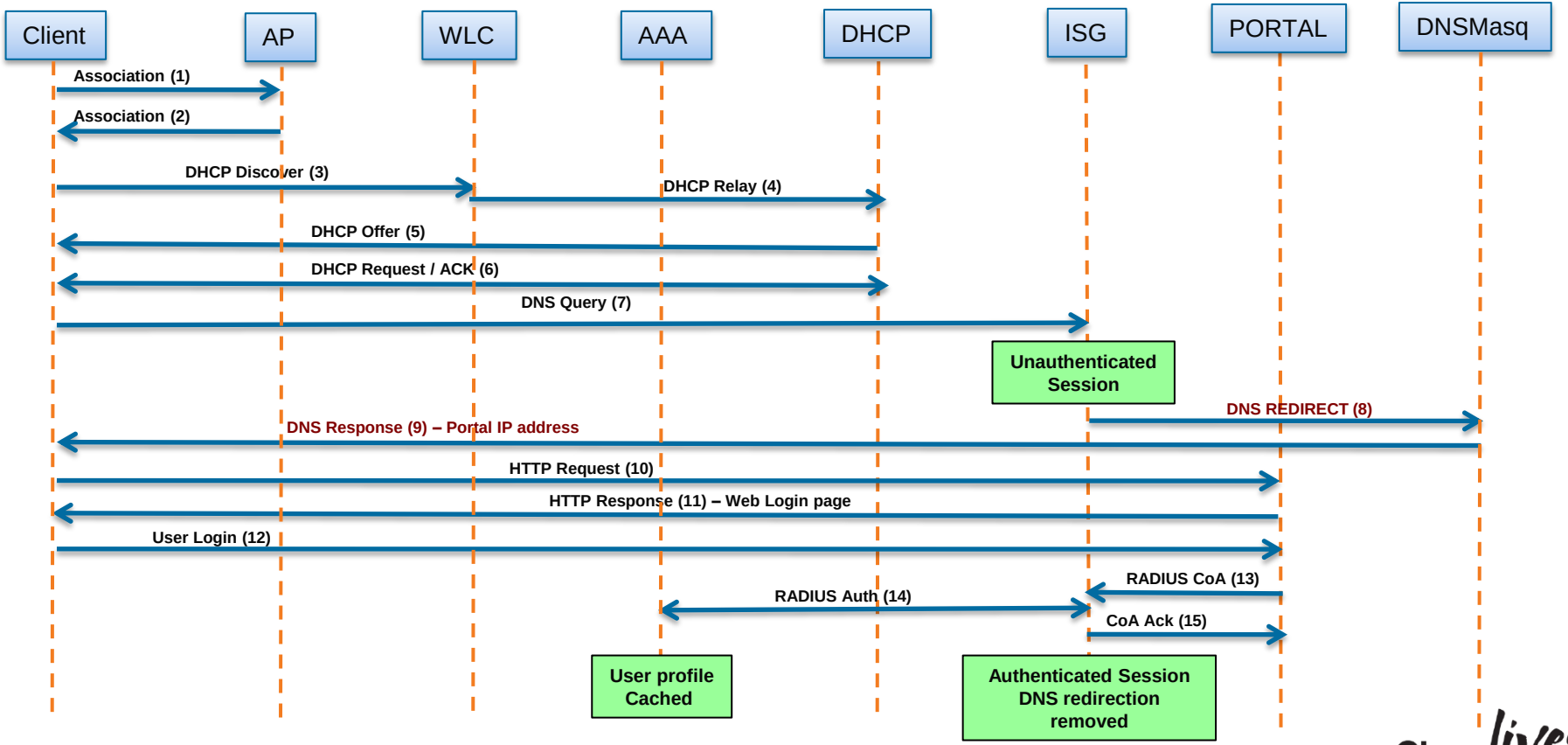
- No Access
- Switch-based 802.1X auth
- Guest VLAN



Hospitality: Wired Access for approved devices



Hospitality: Web-Auth with DNS redirect



WiFi service instance for hospitality

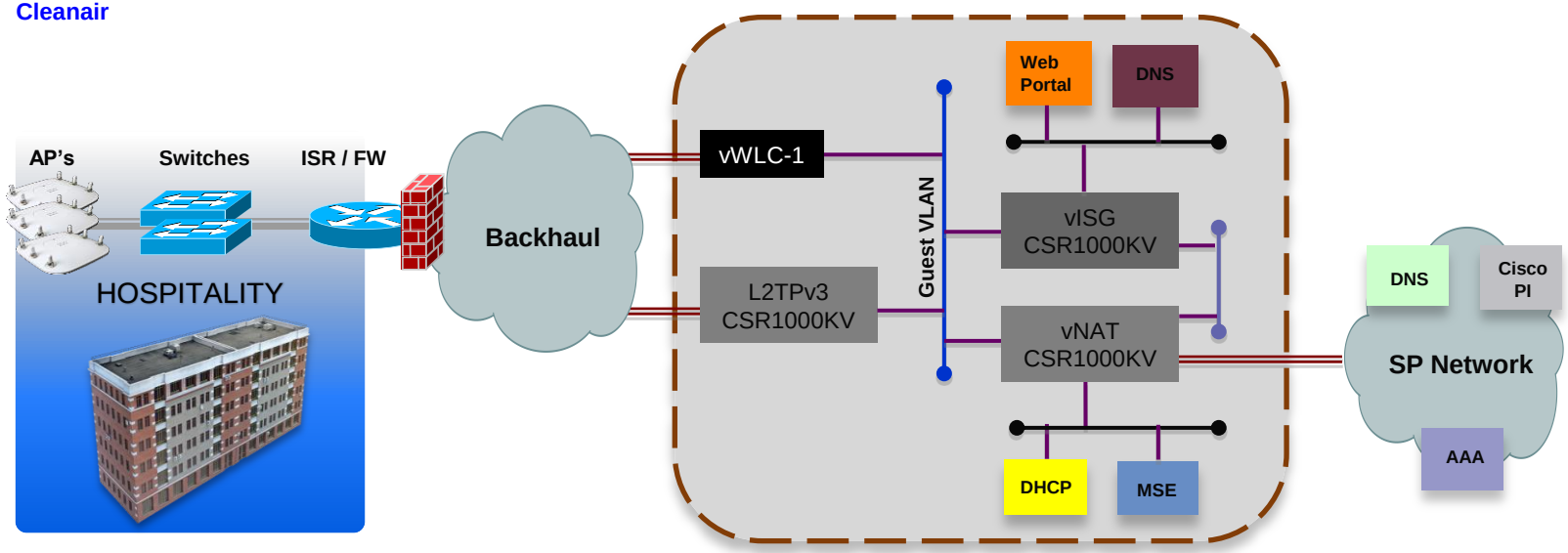
- WiFi Access
- RRM
- WiFi Mobility
- Rouge AP detection
- Client Link
- Band Select
- Flexconnect
- Cleanair

- Location information
- Wired Access
- L2TPv3
- PMS
- MAB

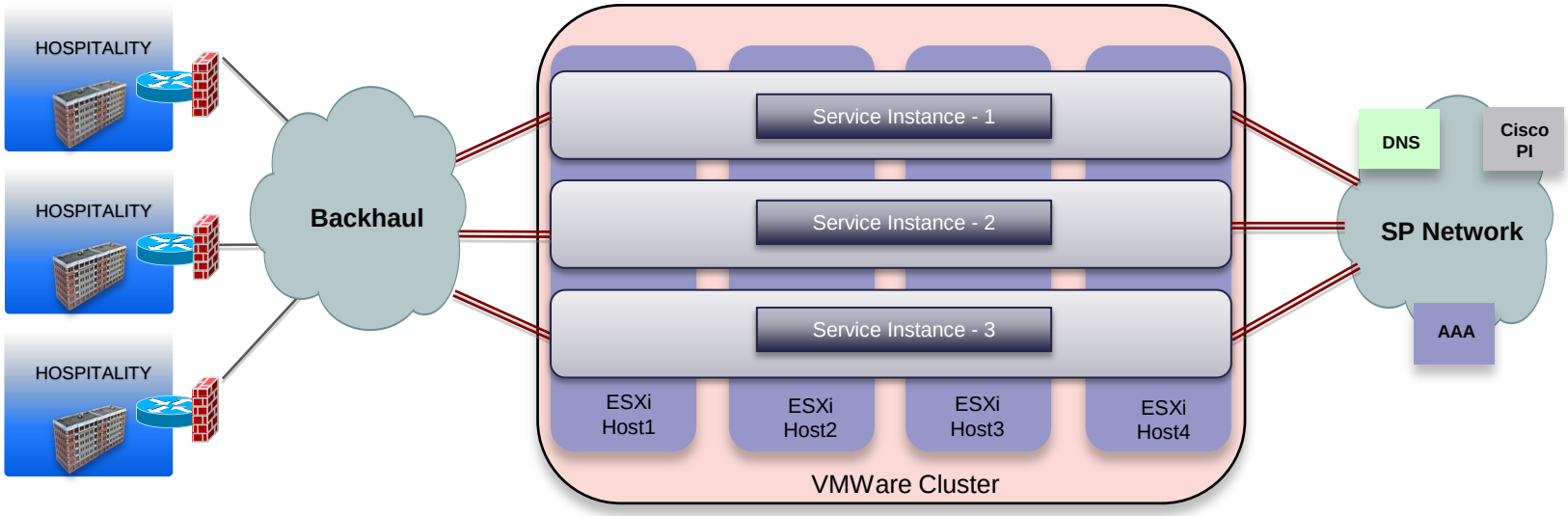
- Customized web portals
- Address assignment
- Whitelisting
- Location awareness
- Network Analytics
- Session management
- L4 Redirection
- TAL

- Policy enforcement
- Accounting
- NAT
- Billing
- L2TPv3

- Asset management
- Authentication
- DNS resolution
- Whitelisting
- Policy definition
- Subscriber management
- Service authorization

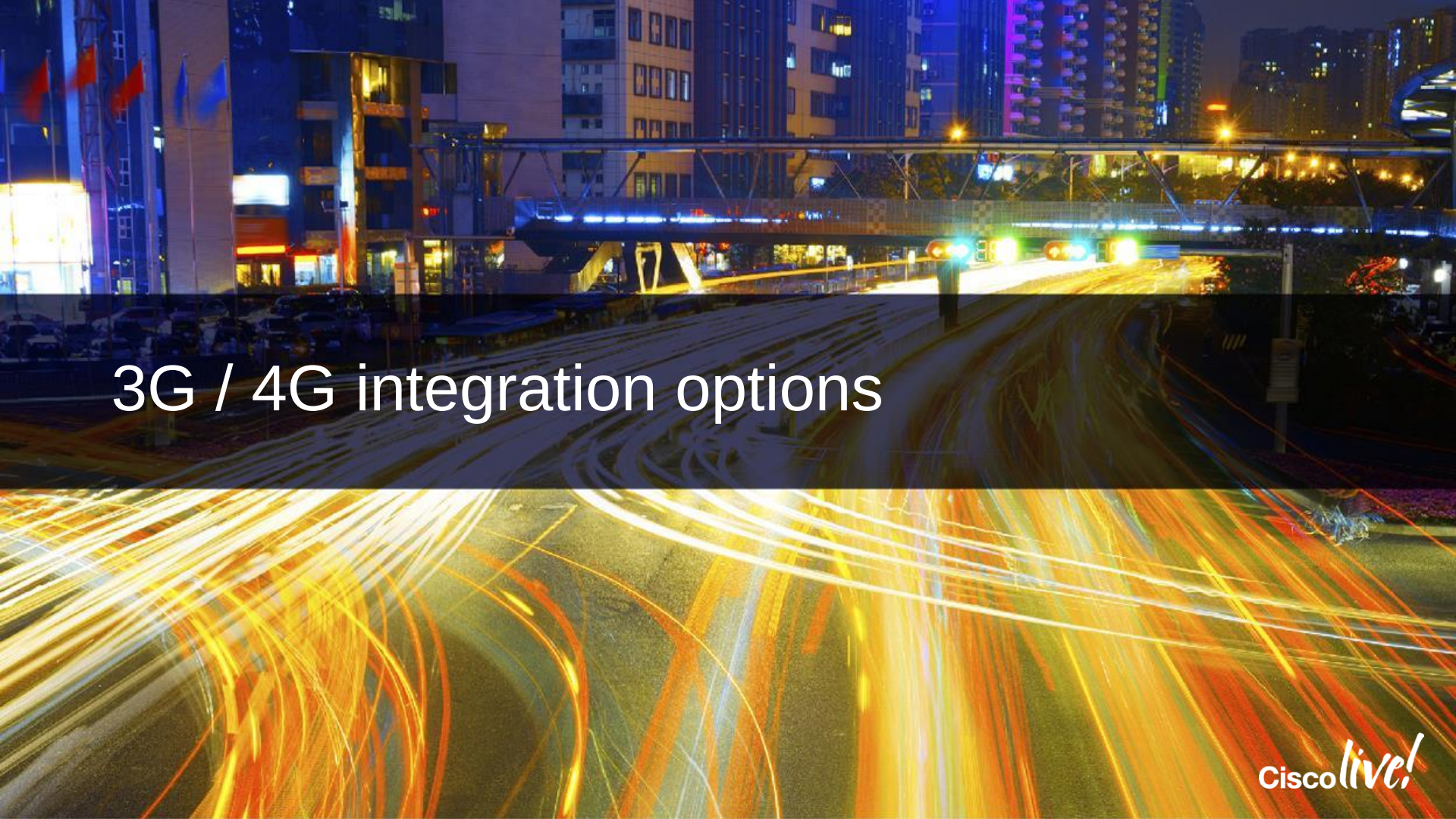


Hospitality - WiFi service instances



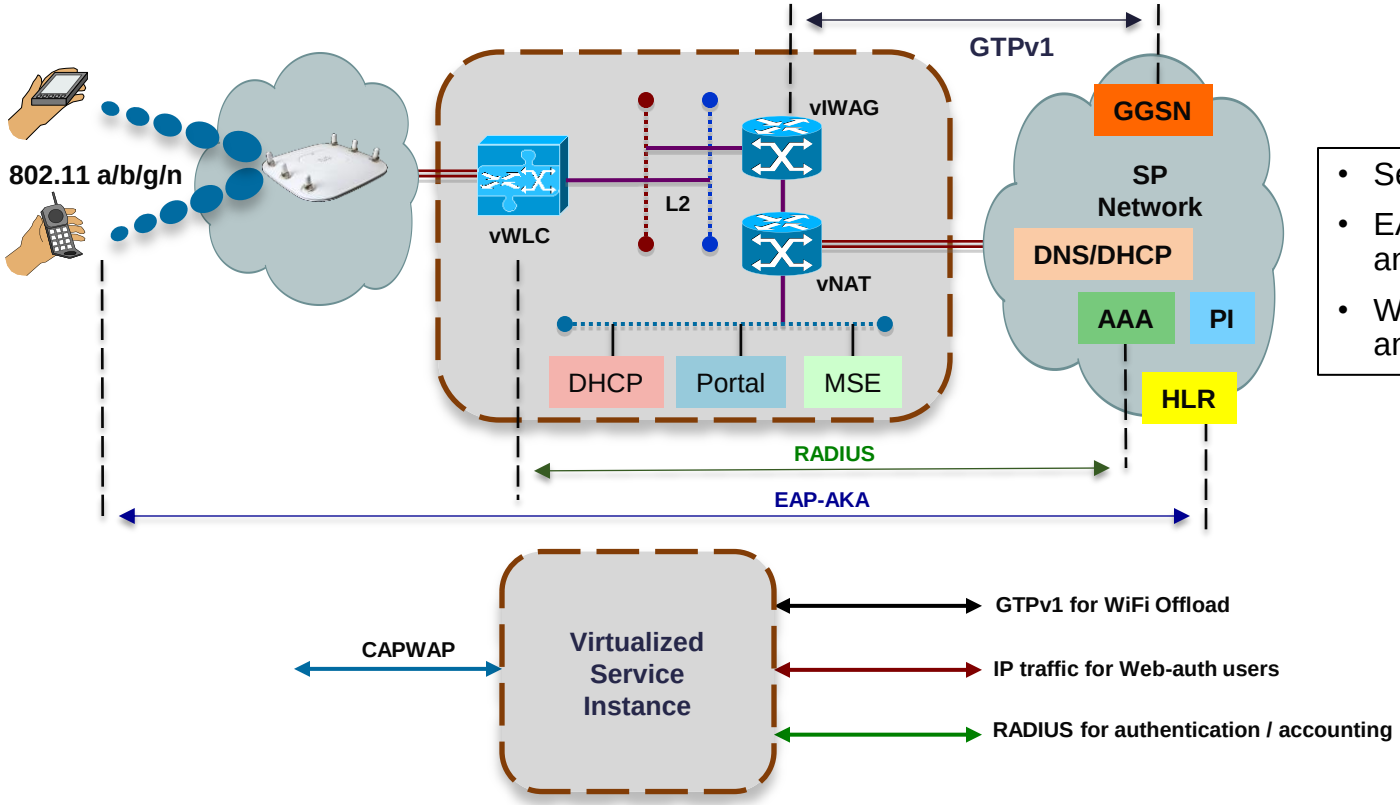
- Consistent subscriber experience
- Centralized asset management
- Customized portal experience
- Shared IP address space
- Separate administration domain
- Custom billing / reporting

- Centralized asset management
- Fault isolation / troubleshooting
- Rapid “cookie cutter” deployment
- Opportunity to customize
- Self service management portals
- License based solution



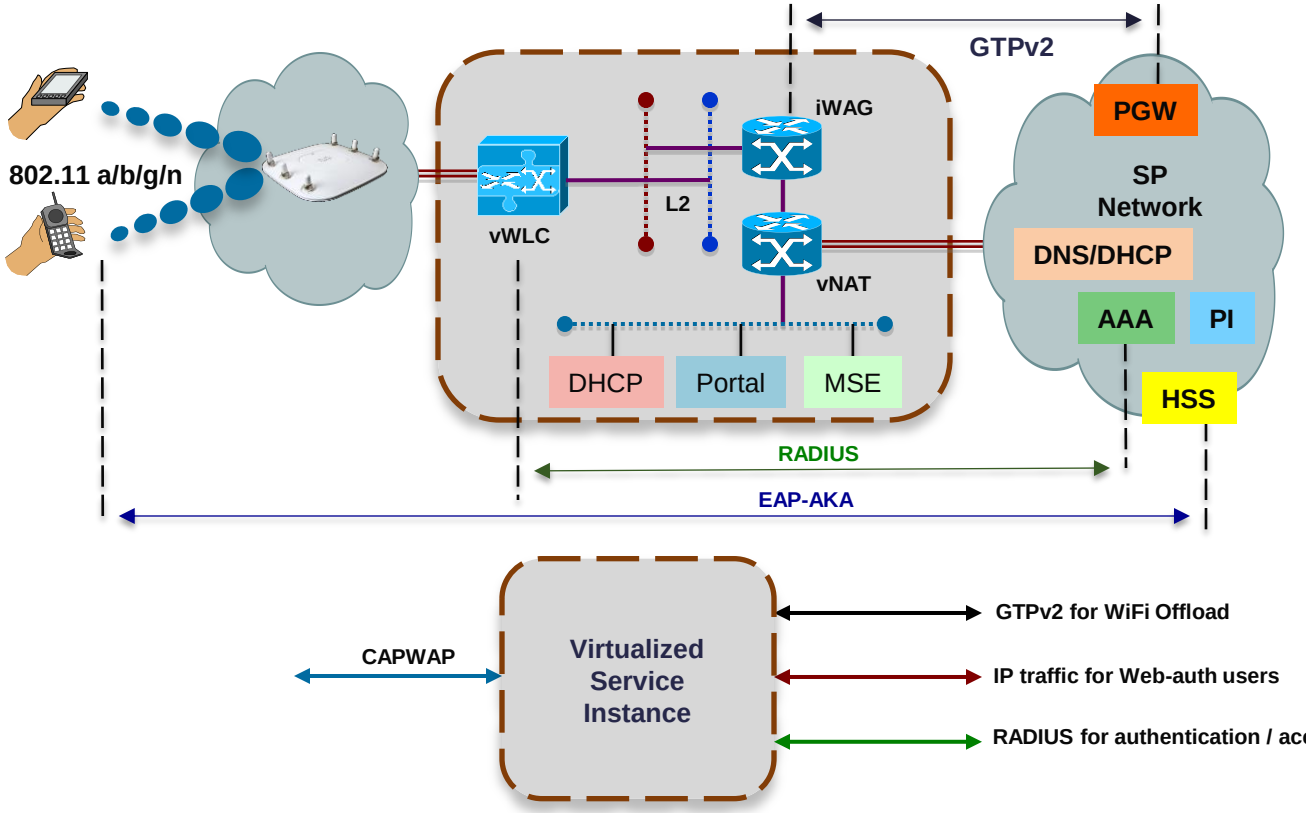
3G / 4G integration options

3G integration with iWAG



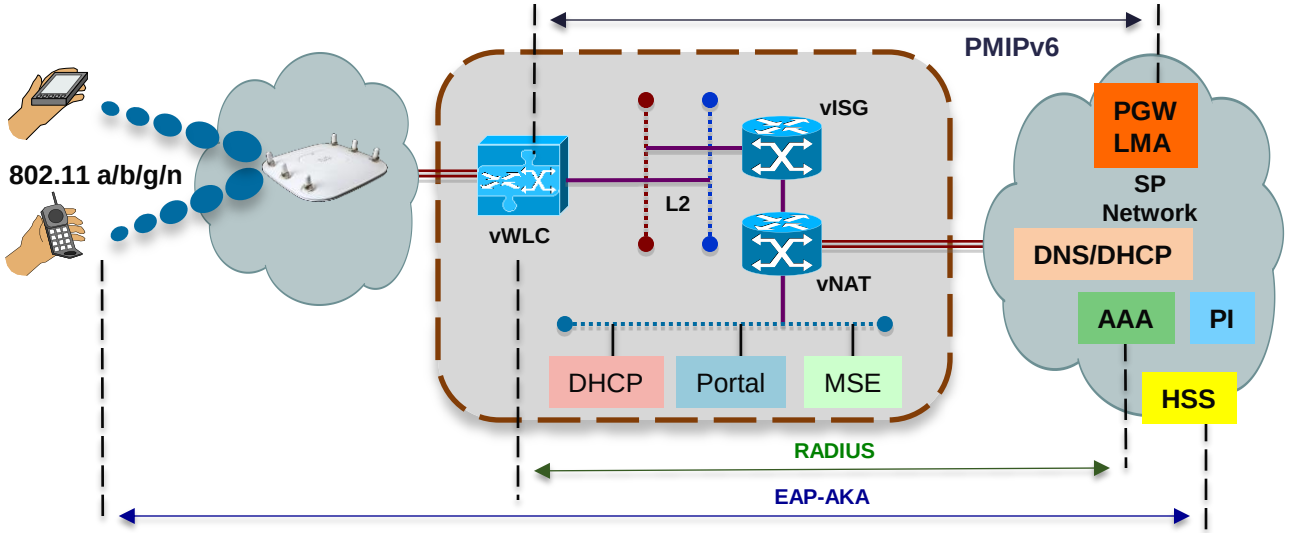
- Separate SSID for EAP-SIM
- EAP-SIM subscribers anchored on GGSN
- Web-auth subscribers anchored on iWAG

4G integration with iWAG

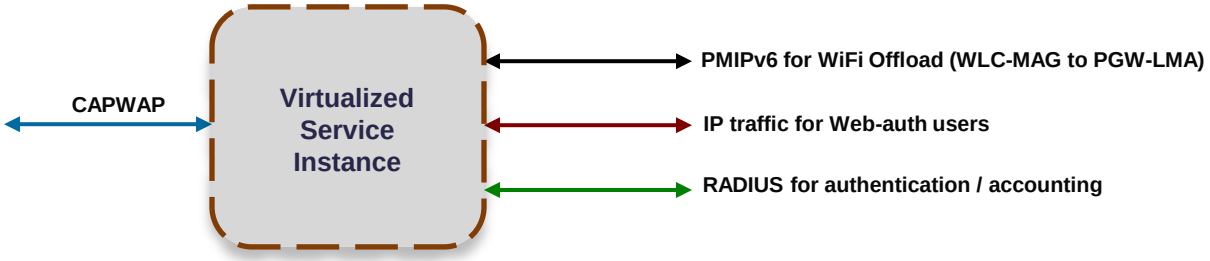


- Separate SSID for EAP-AKA
- EAP-AKA subscribers anchored on PGW
- Web-auth subscribers anchored on ISG

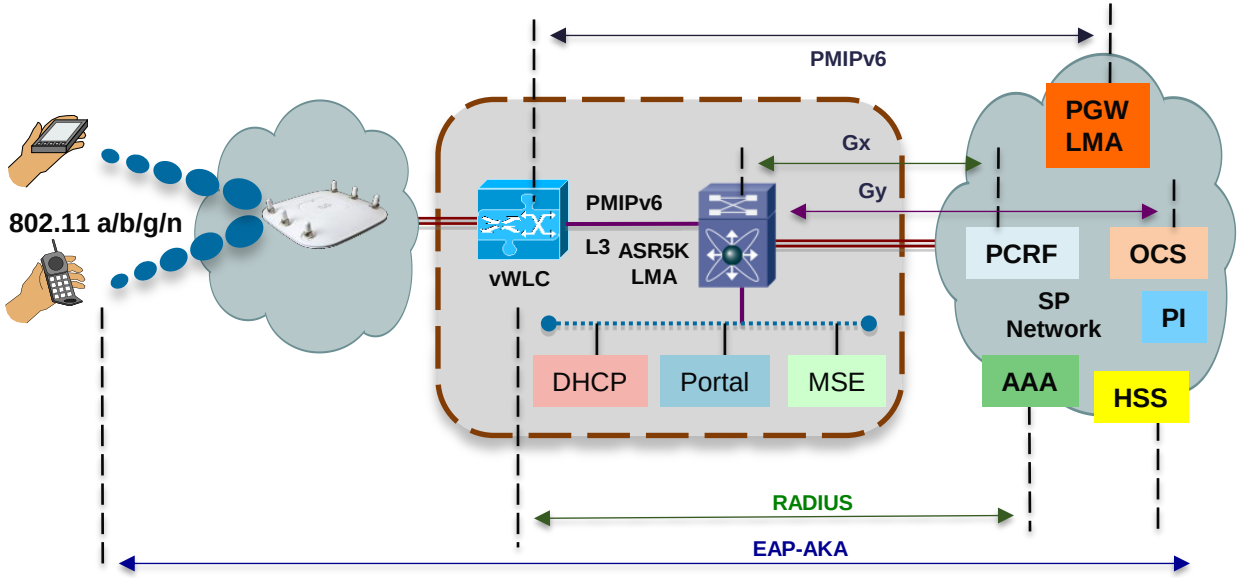
4G WiFi offload with WLC-MAG



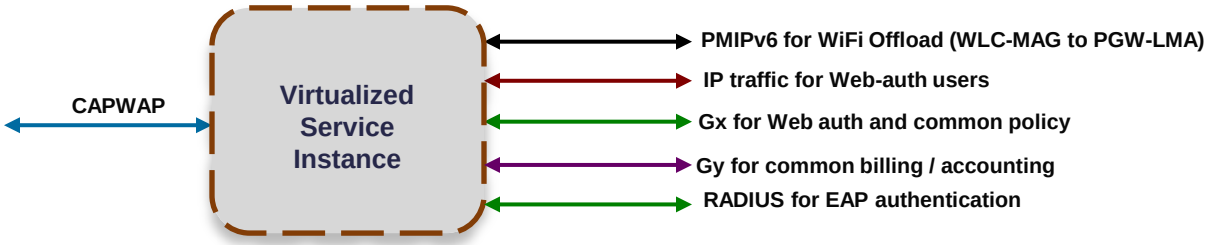
- Separate SSID for EAP-AKA
- EAP-AKA subscribers anchored on PGW
- Web-auth subscribers anchored on ISG



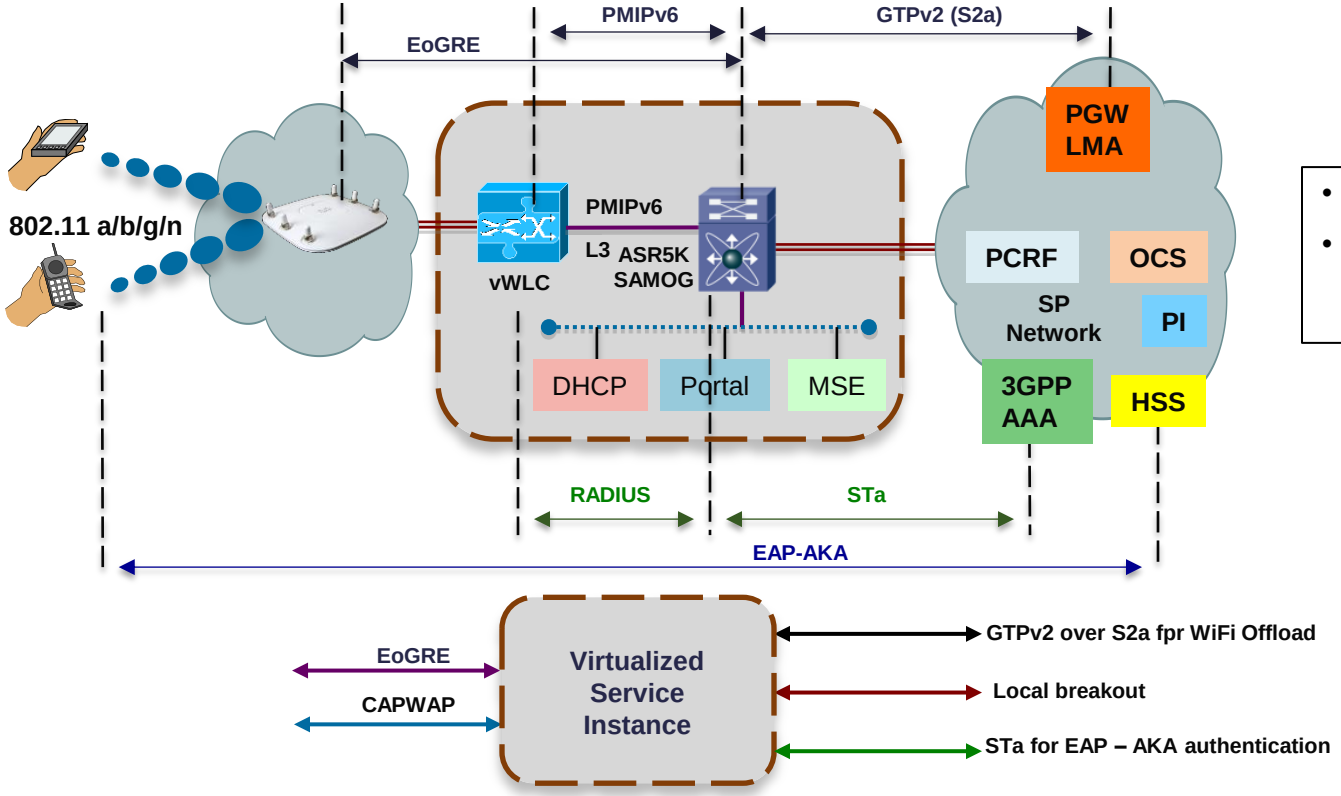
4G integration with LMA



- Separate SSID for EAP-AKA
- EAP-AKA subscribers anchored on PGW / LMA
- Web-auth subscribers anchored on ASR5K / LMA
- Common Policy / Billing



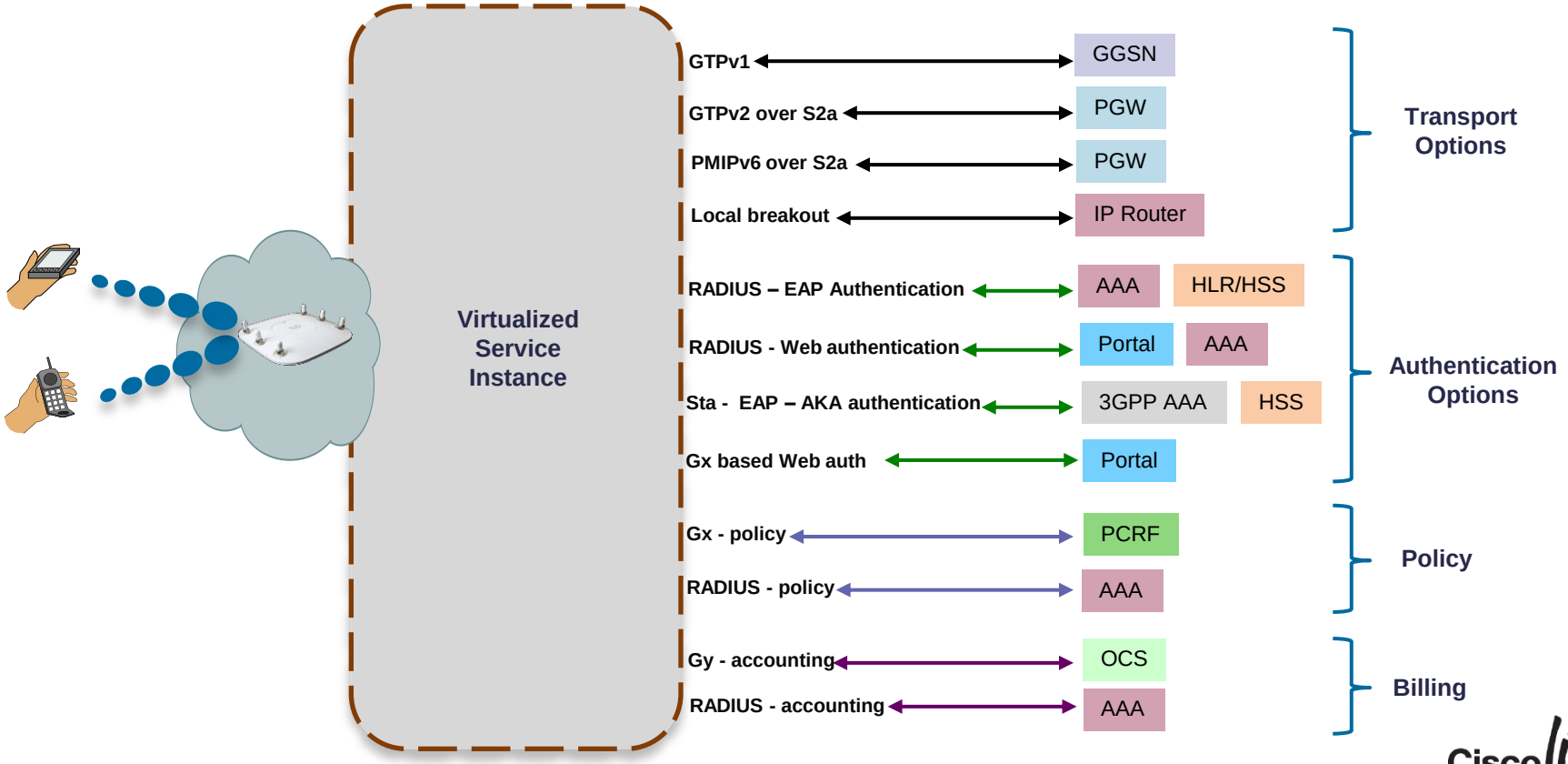
4G integration with SAMOG



- Separate SSID for EAP-AKA
- EAP-AKA subscribers anchored on PGW with GTPv2 over S2a

Cisco live!

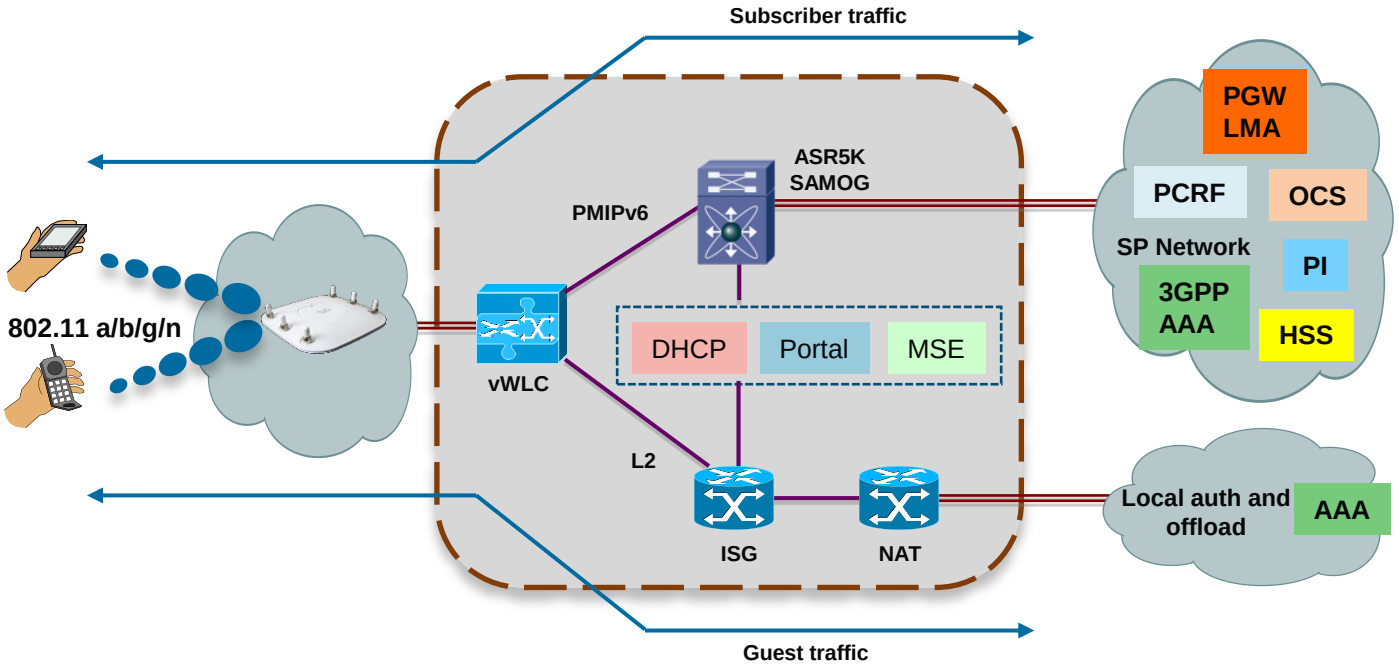
3G / 4G integration summary



Sample stadium deployment

- All MSP subscriber data traffic offloaded with EAP-AKA
- MSP subscribers can use their login credentials when using non-SIM devices
- Subscribers will receive service consistent with their subscription level
- All guests will be use open SSID
- Guests will be required to enter voucher based credentials for authentication
- Guest authentication uses local AAA service
- Guest traffic is locally switched (Not backhauled to the provider)

Customized service instance



- EAP-AKA authentication
- Seamless WiFi offload
- Subscription based svcs
- Consistent subscriber experience

- Local authentication
- Billing (Voucher based)
- Offload

Scaling and Orchestration

Cisco live!

Scaling the virtualized WiFi core

- Elasticity
  - On demand expansion or contraction of the number of instances of a single function or service
- Orchestration
  - Automation, provisioning, coordination and management of physical, virtual and network resources across multiple data centers
- Programmability
  - Dynamically program network functions based on policy

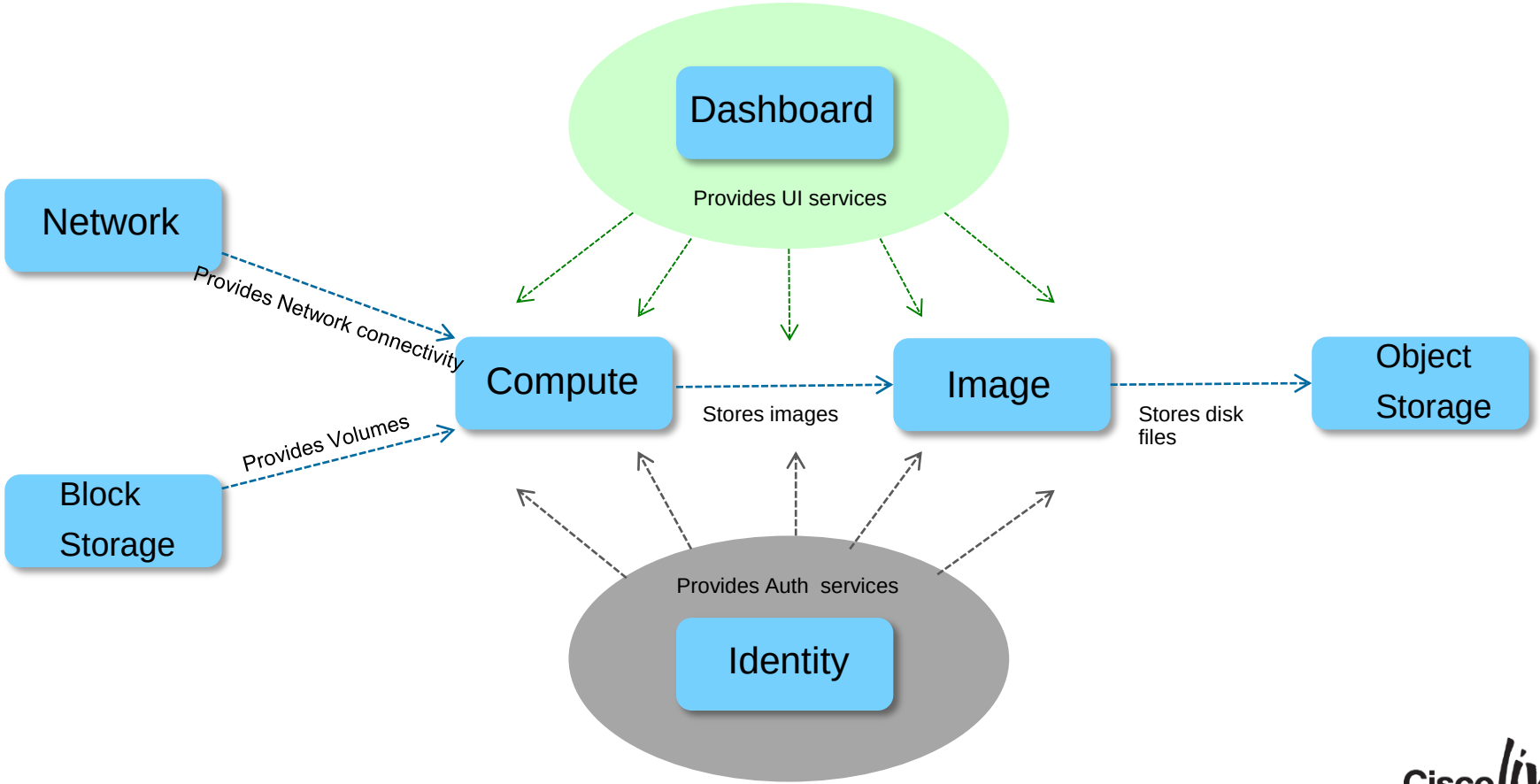
What is Openstack?

- A community driven cloud operating system that turns datacenters into pools of resources – the next evolution from server virtualization
- Provides a framework for controlling, automating, and efficiently allocating these resources
- Empowers operators, sys admins and end users via self-service portals
- Gives developers the capability to build cloud-aware applications via standard APIs

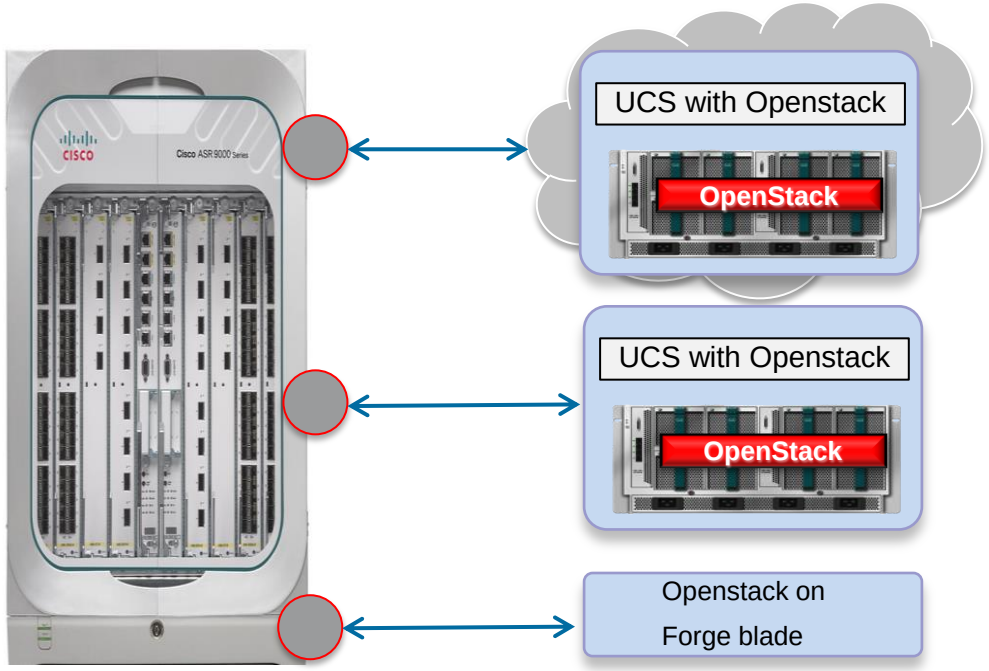
Openstack components

- Object Store (Swift)
  - Store and retrieve files using commercial storage services
- Image (Glance)
  - Provides a catalog and repository for virtual disk images
- Compute (Nova)
  - Provides virtual servers on demand
- Dashboard (Horizon)
  - Web based GUI for all Openstack services
- Identity (Keystone)
  - Catalogs Openstack services and provides authentication and authorization
- Network (Quantum)
  - Abstracts the network as a service providing connectivity between Openstack services
- Block Storage (Cinder)
  - Persistent block storage to guest VM's

Open Stack functional diagram



Attaching compute nodes



Multiple UCS blades running OpenStack connected via a network to a single 10GB port on the ASR9k

- Minimizes number of data ports needed on the ASR9k
- Lower network bandwidth services

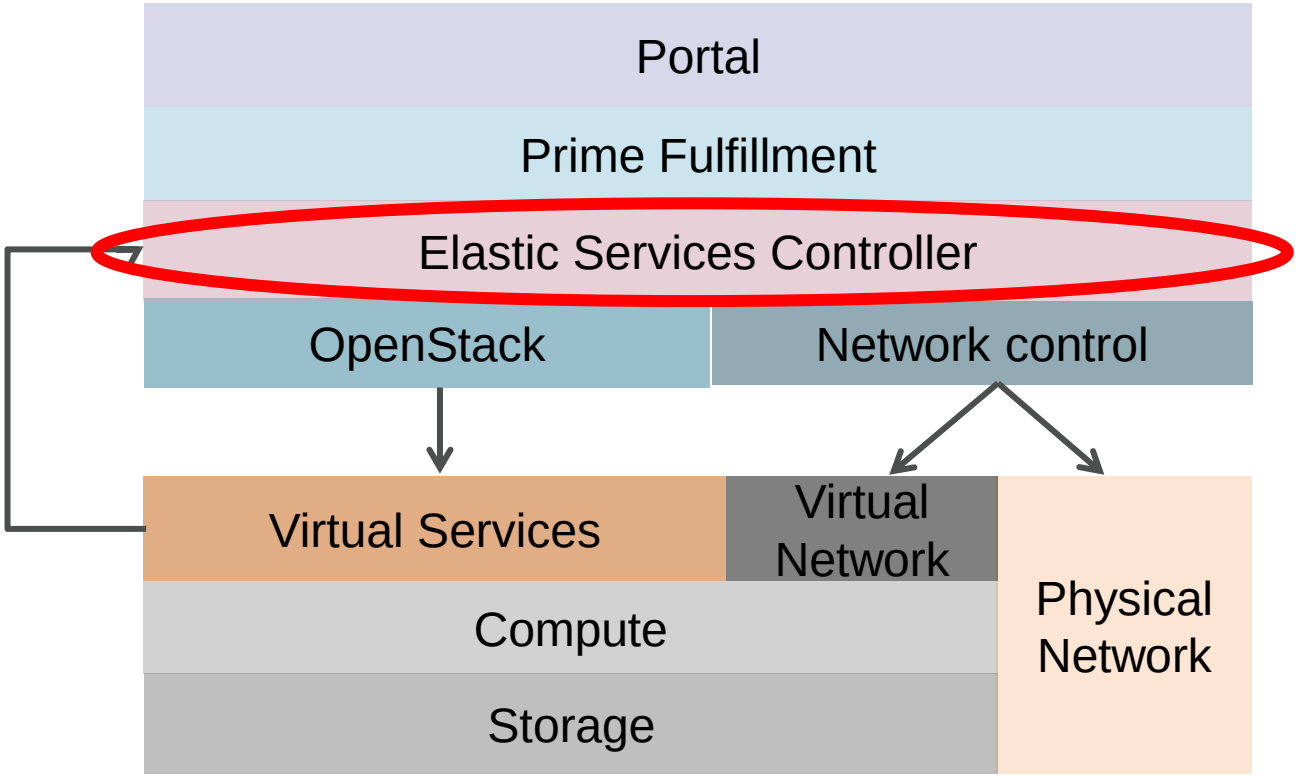
Each UCS chassis (running OpenStack) directly connected to a 10G port on the ASR9K

- Requires a dedicated data port per UCS
- Higher network bandwidth services

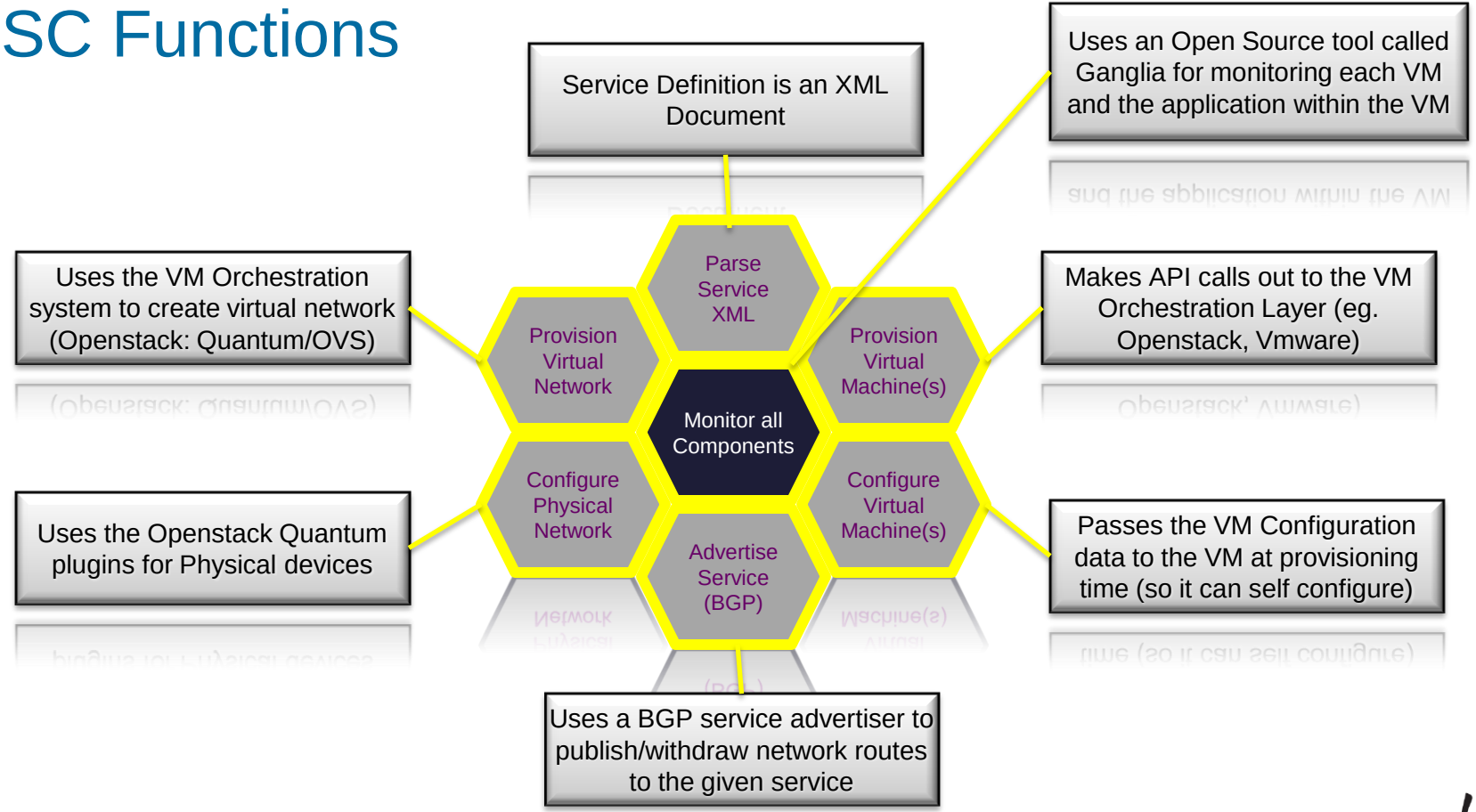
OpenStack running on the Forge Blade (VSM)

- Takes up a service blade slot
- Suitable for small number of services that
- benefit from being connected to the ASR9K fabric

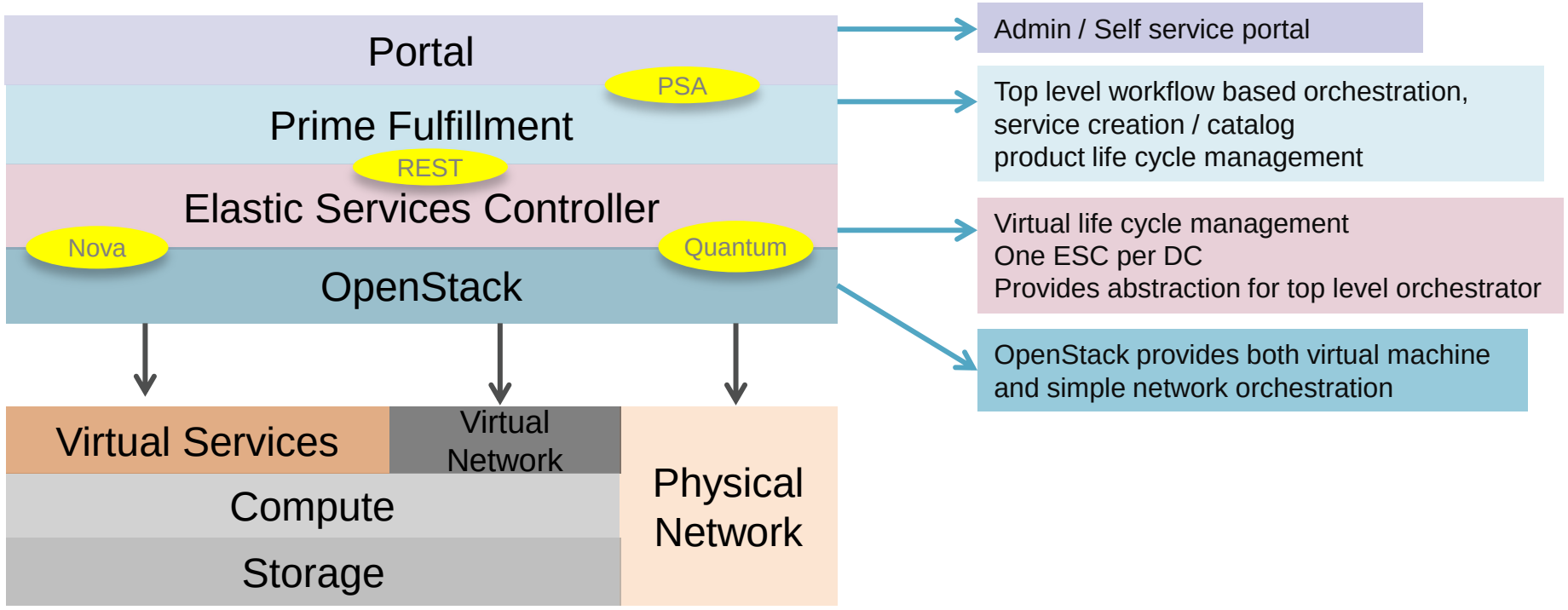
Elastic Services controller



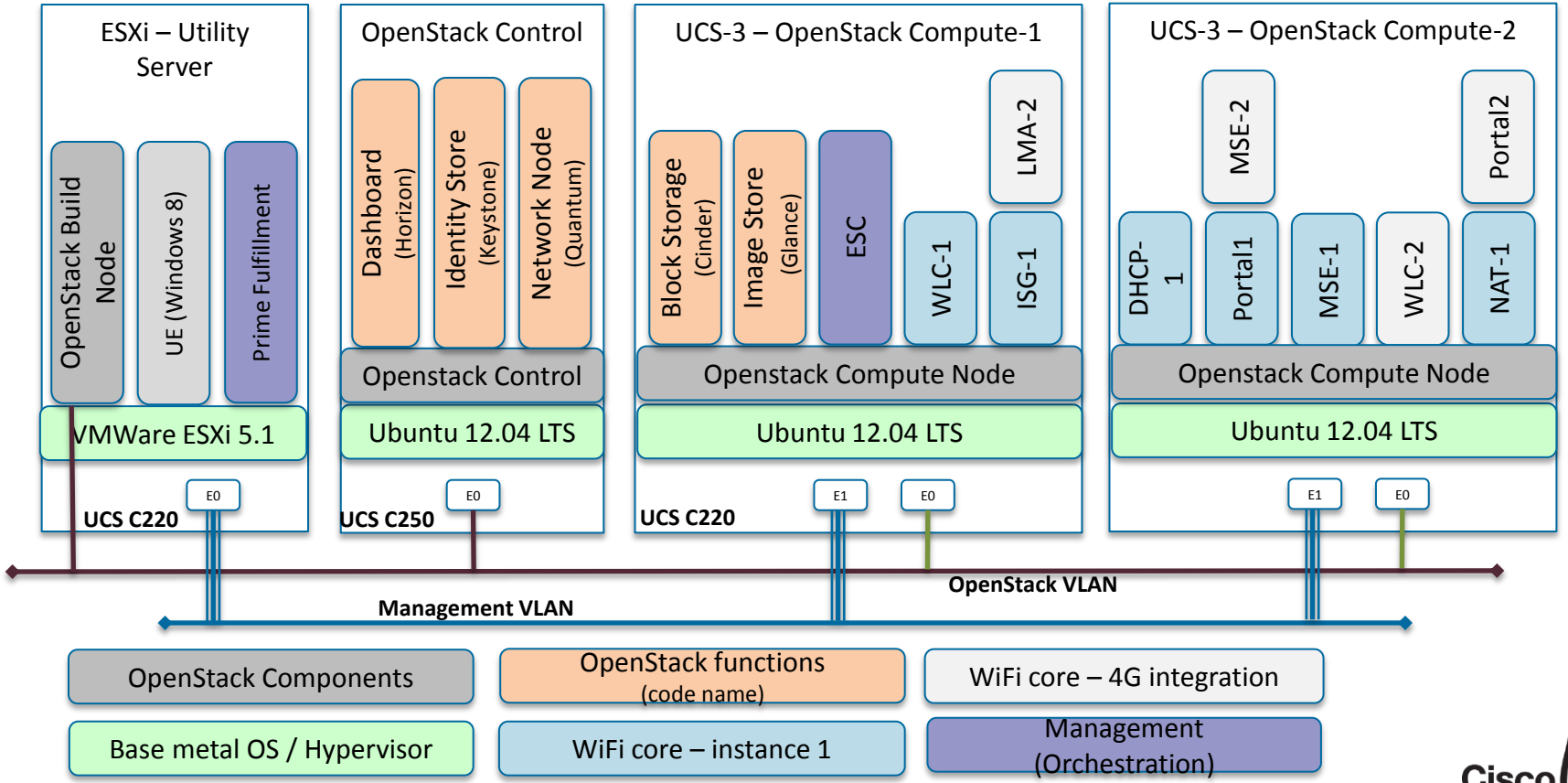
ESC Functions



NFV Orchestration



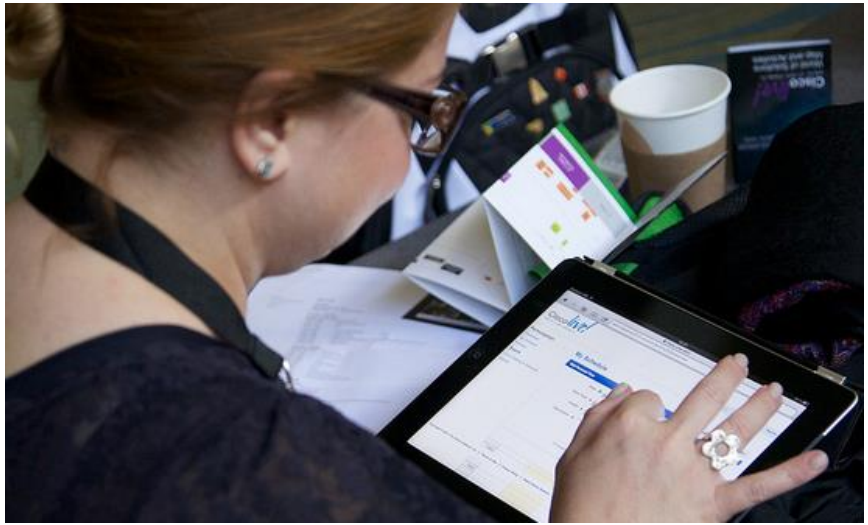
Openstack example



Session ID	Title	Room	Start Time	End Time
	Monday, May 19, 14			
BRKSPM2013	High Density WiFi for Stadiums and Large Public Venues	Moscone West 3016	8:00 AM	9:30 AM
BRKSPM2005	Cisco Small Cell Solutions	Moscone South 307	10:00 AM	12:00 PM
BRKSPM-2007	Small Cell Backhaul	Moscone West 2022	1:00 PM	3:00 PM
	Tuesday, May 20, 14			
BRKSPM2011	Cisco Quantum Policy Suite	Moscone West 3010	8:00 AM	9:30 AM
BRKSPM2010	Cisco Quantum Self Optimizing Network	Moscone North 114	12:30 PM	2:30 PM
PNLSPM-2000	Under the Top: The Mobile Operator Advantage	Moscone West 2010	3:00 PM	4:30 PM
	Wednesday, May 21, 14			
BRKSPM3004	Cisco Quantum Service Bus	Moscone North 113	1:30 PM	3:30 PM
BRKSPM2001	GiLAN and Service Chaining	Moscone North 114	4:00 PM	5:30 PM
BRKSPM3002	Cisco Virtual Mobile Packet Core	Moscone South 308	4:00 PM	5:30 PM
BRKSPM2012	SP Mobility Analytics – Transforming Big Data into Bigger Profits	Moscone North 112	4:00 PM	5:30 PM
	Thursday, May 22, 14			
BRKSPM2008	Unified MPLS Design and Deployment Case Study for Mobile Service Provider	Moscone North 125	8:00 AM	10:00 AM
BRKSPM2009	ASR5500 Next Gen Architecture	Moscone North 113	12:30 PM	2:00 PM
BRKSPM2003	SDN for Service Provider	Moscone North 123	12:30 PM	2:00 PM
BRKSPM2006	Virtualized SP WiFi Core	Moscone North 113	2:30 PM	4:00 PM
	World of Solution - Walk-in Self Paced Labs			
WSPSPM2014	SP Wi-Fi integration into PMIPv6-based 4G Evolved Packet Cores	Hands-lab (World of solution – Cisco Booth)		
WSPSPM2017	SP Wi-Fi integration into 3G GTP-based Mobile Packet Cores	Hands-lab (World of solution – Cisco Booth)		

Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Complete your session evaluation through the Cisco Live mobile app or visit one of the interactive kiosks located throughout the convention center.



Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings


Thank you.


CISCO