

Catalyst 9800 – новая классика WLAN

Разворачивание, настройка и использование виртуального беспроводного контроллера Catalyst 9800

Спасибо за подключение!
Мы скоро начнем трансляцию.



Докладчик

Роман Подойницын
Consulting engineer
Cisco CX Russia



План сессии

Введение

Варианты внедрения

Внедрение в Private Cloud

Внедрение в Public Cloud

New Cisco Catalyst 9800 Series Wireless Controllers



Always on



- Software updates with no disruption
- Rolling Access Point (AP) upgrades
- Seamlessly add new AP models

Secure



- Detect encrypted threats with Cisco® Encrypted Traffic Analytics (ETA)
- Automate macro and micro segmentation with Cisco Software-Defined Access (SD-Access)
- WPA3 support

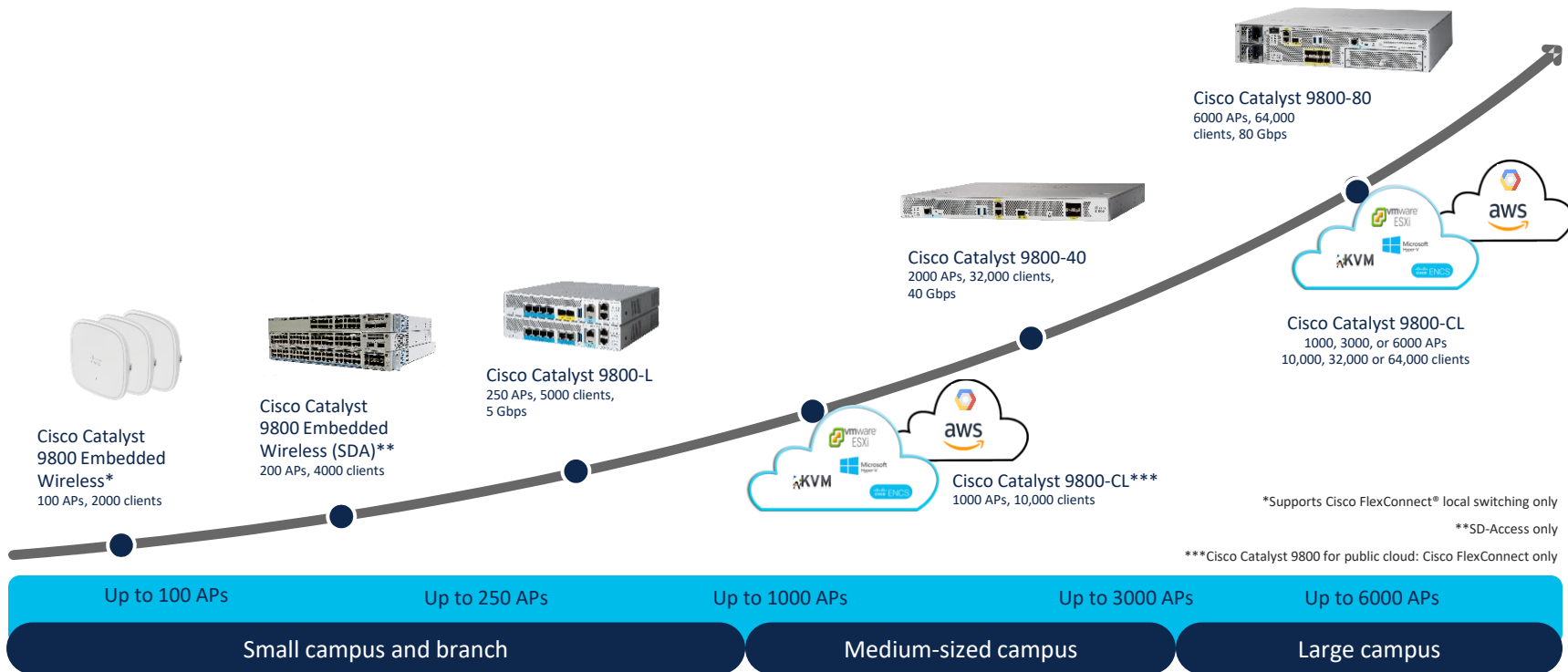
Deploy anywhere



- On-premises, private or public cloud, embedded wireless on a switch
- Scale as you grow

Catalyst 9800 Wireless Controller

Deploy @ Any Scale



The background is a dark blue field filled with numerous small, semi-transparent squares and dots. These elements are scattered across the frame, with a higher concentration of larger squares in the upper left and lower right corners. The colors of these elements include various shades of blue, cyan, green, yellow, orange, and red, creating a vibrant, pixelated effect.

Deployment Models



Someone said Cloud??



Some definitions first...



- ❑ You have exclusive access to dedicated DC virtualized or physical resources
- ❑ The resources are on-prem DC or hosted by a colocation provider
- ❑ WLC as a Virtual Machine



- ❑ You don't own the infrastructure (computing, storage, networking).
- ❑ WLC is consumed as Infrastructure as a Service (IaaS)



- ❑ Simply the reality...
- ❑ You will have both Private and Public cloud deployments for some time

Catalyst 9800 Cloud - Traditional Use Cases



FlexConnect Remote WLC



Remote Teleworker WLC



Guest Anchor WLC



Local Controller WLC



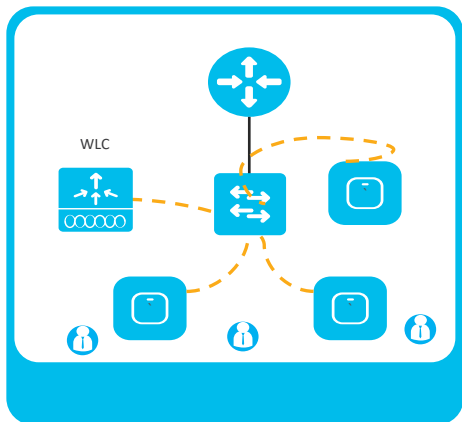
Testing & Proof of Concept

- Self-Education
- Lab Testing
- Practice Change Management Procedures

Catalyst 9800 Cloud - Design Options

Dedicated Local Controller

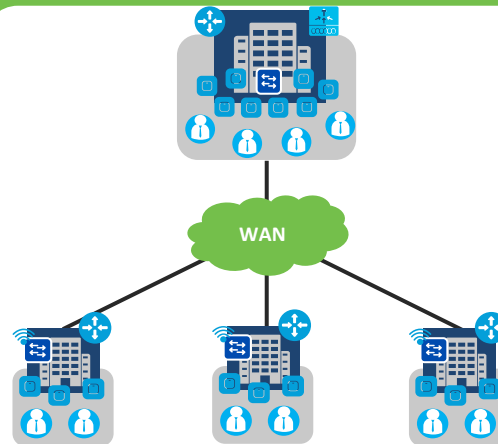
Local Wireless Controller



- ✓ Local WLAN Controller

Remote Controller

Flex Connect



FlexConnect

- ✓ Controller running in Data Center
- ✓ Distributed Network
- ✓ Highly Scalable



Policy



Automation



Assurance



Security

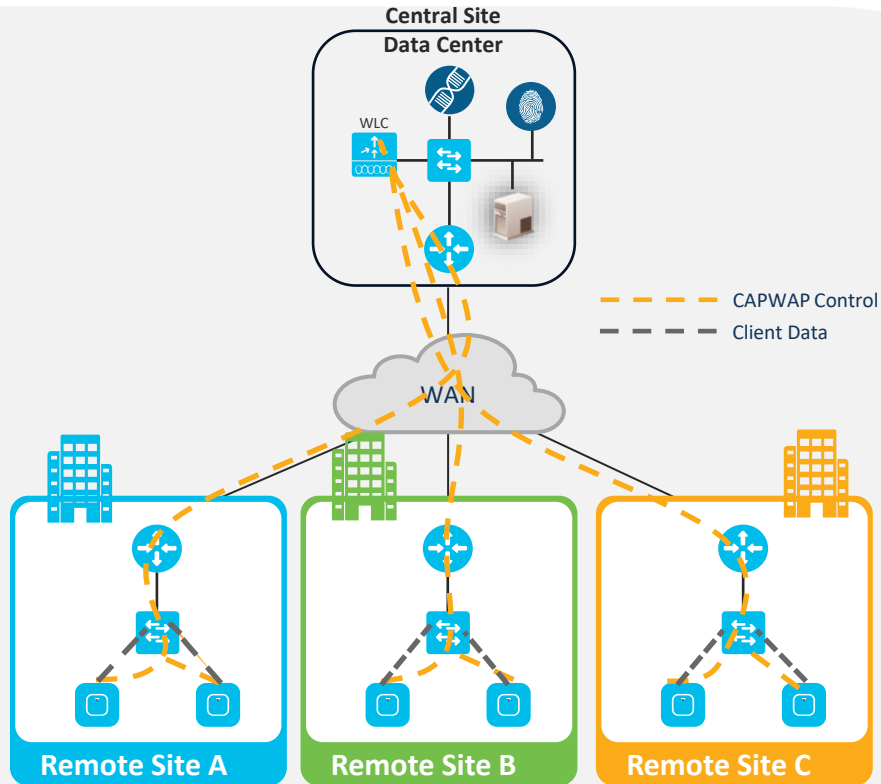


ISE



Location Services

Catalyst 9800 Cloud - Remote Controller



- Wireless Controller is at a central site managing APs across sites/branches
- Clients in branch roam independently



- Each site can have up to 100 APs in a FlexConnect group for seamless roaming
- L2 roaming only
- Supports standalone mode operations



- Highly Scalable
- Central management
- Ideal for cookie cutter branch configuration
- Supports optional central switching



WAN Guidance

- Minimum Bandwidth per-AP: ~ 24 kbps
- Latency – Data: 300 ms (RTT)
- Latency – Voice + Data: 100 ms (RTT)

Вопросы?

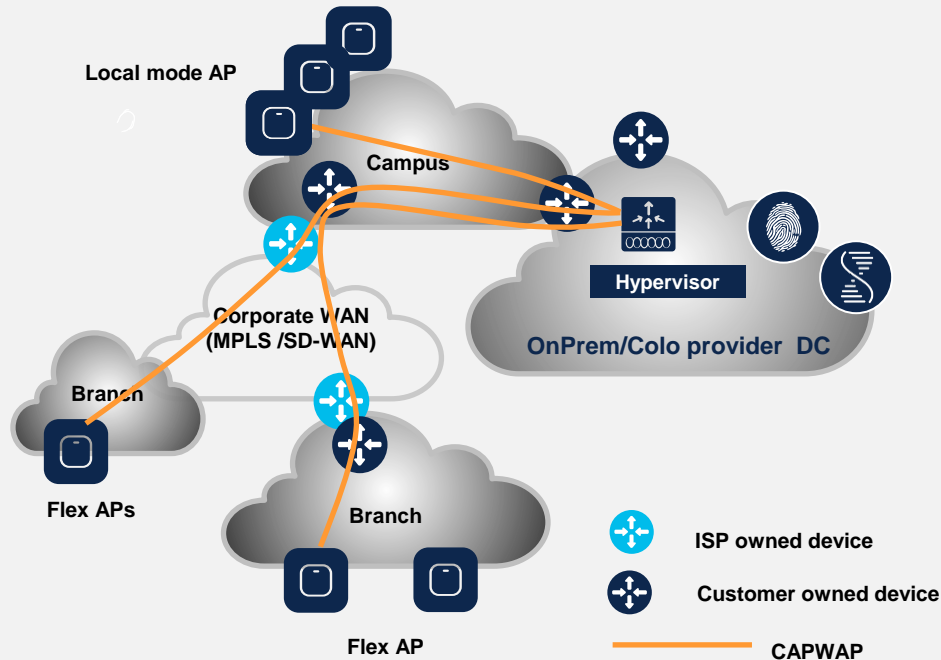


The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, teal, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares forming a diagonal streak from the top right towards the bottom right. The overall effect is a dynamic, pixelated or digital aesthetic.

Private Cloud Deployment



Catalyst 9800 Private Cloud Deployment



Value Prop:

- Deploy wireless controller where you want it, how you want it
- All AP modes supported (Local, Mesh, Flex, SDA)
- Feature parity with appliance (**exception GuestShell**)

Support

- VMware ESXi
- Microsoft Hyper-V
- KVM and ENCS
- Wi-Fi 6, Wave2 and Wave1 APs *
- Centrally switched traffic ≤ 2.1 Gbps
- ESXi vCenter or KVM Virt-Mgr for VM provisioning
- Automated VM bootstrap flow (ESXi vCenter only)

* Refer to Software Compatibility Matrix

Differences between AireOS vWLC vs C9800-CL on Private Cloud

	AireOS vWLC	C9800-CL
SSO High Availability	No	Yes
Deployment Modes	Flex Only	Flex, Local, Fabric
Guest Anchor	No	Yes
DNA-C Automation & Assurance	No	Yes
Max central throughput	500 Mbps	2.1 Gbps
Max AP and Client Scale	3k APs, 32k Clients	6k APs, 64k Clients
Installation Image	Multiple	Single for any scale

* XE 16.12 = 1.5 Gbps
** SR-IOV = 5 Gbps

Catalyst 9800 Private Cloud Capabilities



Management Support

- Cisco DNA Center = Yes
- Prime Infrastructure = Yes

AP Modes Supported

- Local & SD Access Fabric = Yes
- FlexConnect Central Switching = Yes
- FlexConnect Local Switching = Yes
- Mesh = Yes

Feature Support

- SSO = Yes
- N+1 = Yes
- Anchor Controller = Yes
- Foreign Controller = Yes
- mDNS Gateway = Yes

Location Services

- Cisco DNA Spaces = Yes
- Cisco CMX = Yes



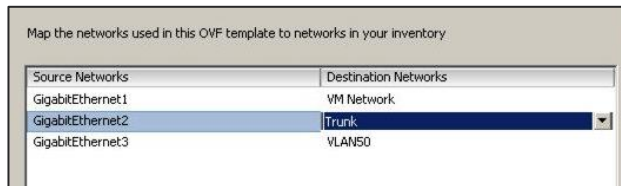
Private Cloud – Life Lessons



- Deploy using the tested interface configuration.

		Recommended Use	Port Group Config	C9800-CL Config
Device Management	GigabitEthernet1	Service Port (OOB)	VLAN	Routed Interface
Wireless Management	GigabitEthernet2	WMI & Wireless Clients	Trunk	L2 Trunk
High Availability	GigabitEthernet3	Redundancy Port	VLAN	HA SSO

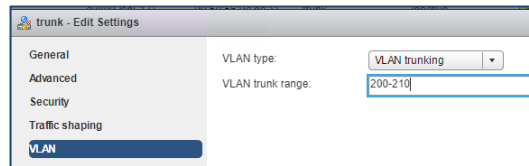
- Map each interface to a different virtual network! Otherwise, you will introduce a network forwarding loop.





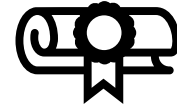
Private Cloud – Life Lessons

- Reduce WMI routing inconsistencies. Don't install a default route on the Service Port (GigabitEthernet1).
 - Install routes that are targeted.
- When configuring a trunk, define the allowed VLANs.
 - Don't permit/trunk all VLANs.
- GUI HTTPS certificate issues are easily fixed. Assign the self-signed certificate to the HTTPS process.
 - SSH to C9800-CL
 - show running-config | section trustpoint
 - no ip http secure-server
 - ip http secure-trustpoint TP-self-signed-<id>
 - ip http secure-server



```
c9800-demo#sh run | sect trustpoint
crypto pki trustpoint TP-self-signed-3343909324
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3343909324
revocation-check none
rsa-keypair TP-self-signed-3343909324
```


Trustpoint – some additional info



- A Trustpoint is a certificate authority (CA) who you trust, and it is called a trustpoint because you implicitly trust this authority
- Public Key Infrastructure (PKI) provides certificate management in C9800
- By trusting a given self-signed certificate, PKI system will automatically trust any other certificates signed with that trusted certificate.
- This is used for providing certificate management for various functions and protocols such as DTLS , HTTPS , SSH , SSL and so on
- Used on C9800 for: AP Join (DTLS tunnel), HTTPs connection (GUI), Webauth redirection, Mobility Tunnel

Trustpoint for AP

- Trustpoint for AP join secures the connection between WLC and AP
- You can view this in CLI by using command
 - “show wireless management trustpoint”
 - All Physical appliances will use Manufacturing Install Certificate (MIC) by default
 - All virtual appliances use (Self-signed Certificate (SSC)

Physical Appliance

```
C9800-1-C#show wireless management trustpoint
Trustpoint Name : CISCO_IDEVID_SUDI
Certificate Info : Available
Certificate Type : MIC
Private key Info : Available
FIPS suitability : Not Applicable
```

Virtual Appliance

```
WLC#show wireless management trustpoint
Trustpoint Name : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : c347ed2b4a9db7c4c582e676842a77d5ba27c63e
Private key Info : Available
FIPS suitability : Not Applicable
```

Name of the Trustpoint

Simplified Day 0 Experience

Standard across all form factors

Same DAY zero GUI across all flavors of the Catalyst 9800 Wireless Controller

- If the box has not been configured before (specifically AP **Country Domain** has not been set), when user connects to the GUI it will be automatically redirected to DAY zero page and process
- For Catalyst 9800 Wireless Controller for **Cloud**, the user has the option to automatically create a **trustpoint**, a self-signed certificate. This is needed the first time AP joins a VM Controller

The image shows a screenshot of the Catalyst 9800 Wireless Controller configuration GUI. It is divided into two main sections: '1. General Settings' and '3. Advanced Settings'. In the 'General Settings' section, 'Deployment Mode' is set to 'Standalone' and 'Country' is set to 'US,IT'. In the 'Advanced Settings' section, 'Client Density' is set to 'Typical', 'RF Group Name*' is 'default', 'Traffic Type' is 'Data an...', and 'Virtual IP Address' is '192.0.2.1'. Under the 'AP Certificate' section, 'Generate Certificate' is set to 'YES' with a green checkmark, 'RSA Key-Size' is '2048', 'Signature Algorithm' is 'sha1', and 'Password*' is masked. On the right side of the 'Advanced Settings' panel, there are two circular icons: a dark blue one labeled 'PRIVATE' and a light blue one labeled 'PUBLIC'.

After going through DAY 0 APs and clients can immediately join!

9800-CL on Private Cloud – DAY 0 GUI caveats

- Day 0 guided flow assumes that the box has **two separated interfaces** (one for device management and one for wireless management) and that the **first login happens on the device management** (out of band) interface.

Configuration Setup Wizard

1. General Settings

NTP Servers

Enter NTP Server +

Added NTP servers

AAA Servers

Enter Radius Server IP Enter Key +

Added AAA servers

Wireless Management Settings

Port Number

VLAN*

IPv4

GigabitEthernet2
GigabitEthernet2
GigabitEthernet3

- Gig #1 is the Device Management interface:

```
WLC#sh run int gig 1
Building configuration...

Current configuration : 135 bytes
!
interface GigabitEthernet1
 no switchport
 ip address 10.58.55.14 255.255.255.0
 negotiation auto
 no mop enabled
 no mop sysid
end
```

- If you want to **use only one interface**, you need to skip DAY 0 guided flow and configure the initial settings via console. For more info please check the Deployment Guide [here](#)
- Don't forget to create a default route and to manually generate the truspoint
C9800(config-if)#ip route 0.0.0.0 0.0.0.0 172.20.229.1
C9800#wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <pwd>

Private Cloud: Linux KVM

KVM Specifications

Supported Linux distribution: RHEL 7.1 (minimum), Ubuntu 16.04 LTS (minimum)

Model Configuration	Small (16.12+)	Medium (16.12+)	Large (16.12+)
Maximum Access Points	1,000	3,000	6,000
Maximum Clients Support	10,000	32,000	64,000
Minimum Number of vCPUs	4	6	10
Minimum Memory (GB)	8	16	32
Required Storage (GB)	16	16	16
Virtual NICs (vNIC) 3 rd NIC is for High Availability	3	3	3
vNIC driver	VIRTIO	VIRTIO	VIRTIO
Virtual bridge	OVS Linux bridge (brctl)	OVS Linux bridge (brctl)	OVS Linux bridge (brctl)

KVM Specifications

Supported Linux distribution: RHEL 7.1 (minimum), Ubuntu 16.04 LTS (minimum)

	Low Throughput (IOS XE 16.12+)	High Throughput (IOS XE 17.3+)
SR-IOV Support	No	Yes
SR-IOV NIC Support	No	Intel x710 Cisco Intel x710
Max Throughput	2.1 Gbps	5 Gbps
Snapshot	No	No
NIC Teaming	No	No
L2 LAG	No	No

For KVM, check if your Intel/AMD Processor supports virtualization: **egrep -c '(vmx|svm)' /proc/cpuinfo**

0: Processor doesn't run virtualization

1 (or more): Processor supports virtualization. Ensure it's enabled in BIOS

SR-IOV

- SR-IOV allows a single PCIe physical device to appear as multiple separate physical devices to the hypervisor or the guest operating system
- A virtual machine can use an SR-IOV virtual function for **networking**
 - Removes CPU from moving the data between physical NIC and VM (DMA directly to VM)
 - Bypassing the VM kernel for networking reduces latency and improves CPU efficiency
- With a high (enhanced) throughput profile, up to 5 Gbps can be reached on ESXi and KVM with the right set of network cards and resources (SR-IOV-enabled NIC card)

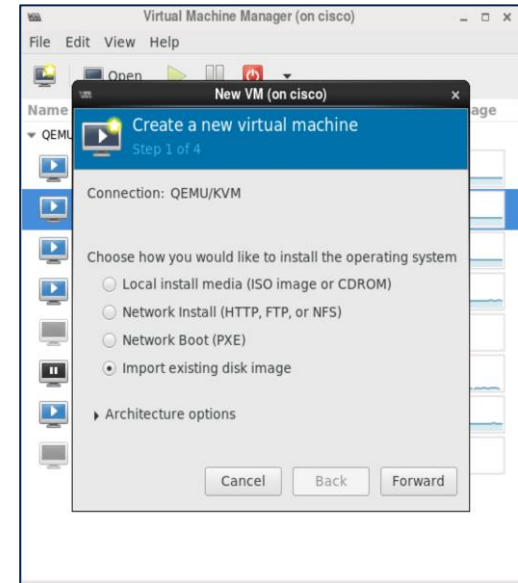
KVM Deployment and File Format Options

- Customer can use the provided .iso or .qcow2 image to deploy C9800-CL on KVM
- There are multiple ways to bootstrap the VM on KVM:
 - Create an iso for the configuration file and attach it as an IDE CD
 - Create a VM with with **virst-install** command
 - Use **virt-manager** leveraging the qcow2 or iso image

- File format types available from Cisco:

- Cisco C9800 deployment .qcow2 disk**
C9800-CL-universalk9.BLD_V***.qcow2
- Cisco C9800 deployment .iso disk**
C9800-CL-universalk9.BLD_V***.iso
- Cisco C9800 Upgrade image (bin)**
C9800-CL-universalk9.upgrade***.bin

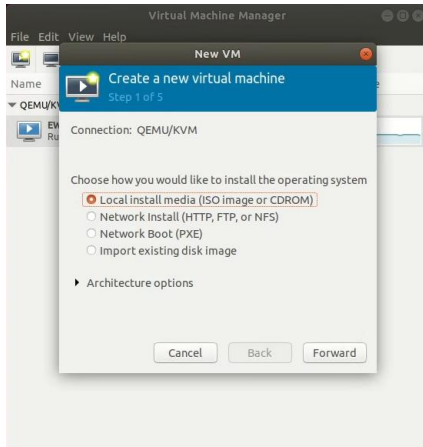
- The following features are enabled at bootstrap by default:
 - http/https server, scp, ssh, netconf-yang



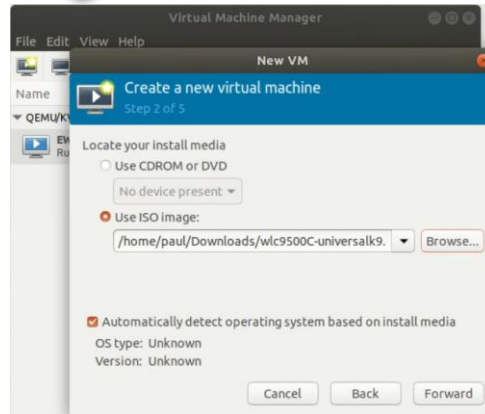
C9800-CL bootstrap flow with KVM

- Example using VIRT Manager and .iso image
- The workflow for deploying a VM is similar for **ESXi vCenter** and **direct host**

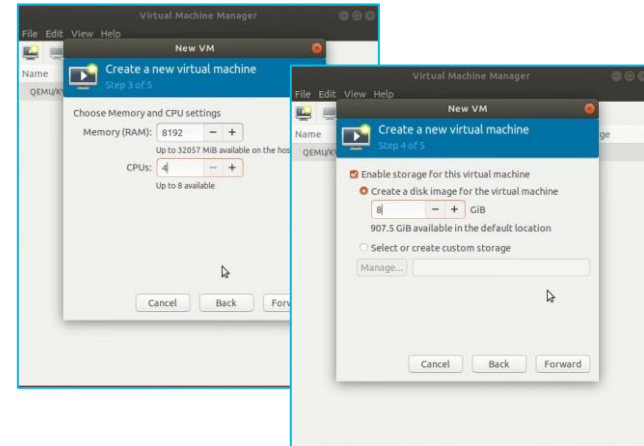
① On Virtual Machine Manager select “Create New Virtual Machine”



② Browse to the .ISO file



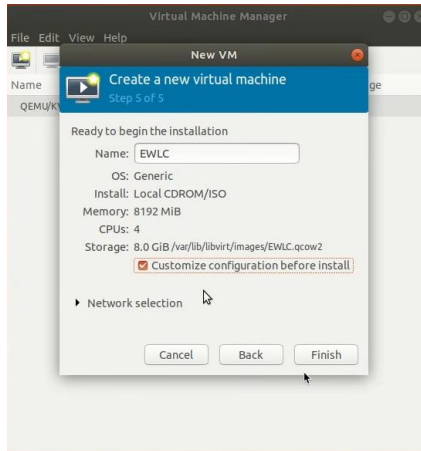
③ Define Scale (manual CPU, Memory & Disk)



C9800-CL bootstrap flow with KVM

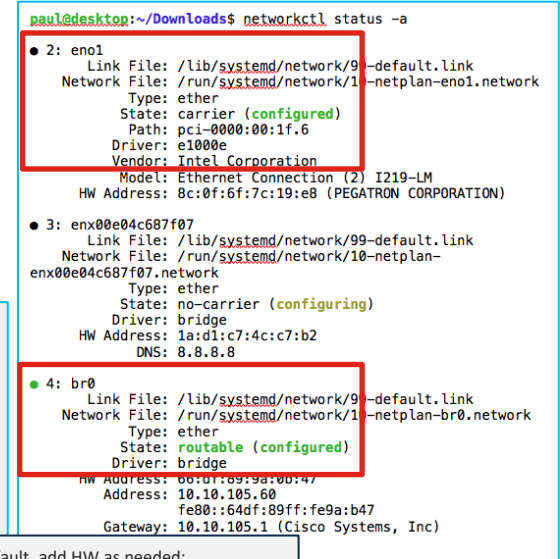
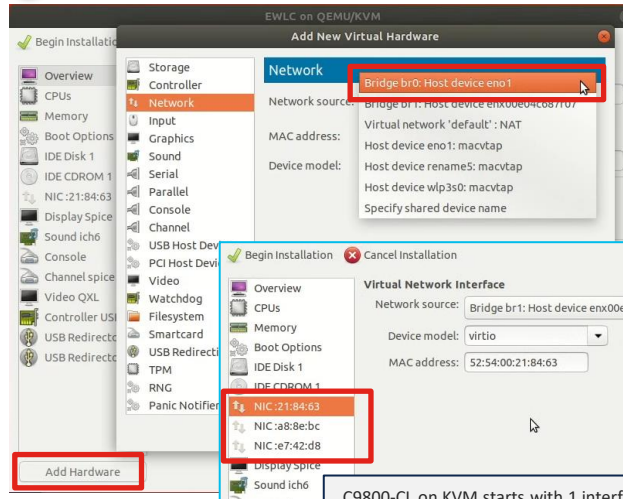
- Example using VIRT Manager and .iso image

④ Create Name and Customize



Select 'Customize configuration before install'

⑤ Customize Hardware and NIC Mapping



C9800-CL on KVM starts with 1 interface by default, add HW as needed:

- GE 1 = Management interface = Service port
- GE 2 = Wireless Management SVI
- GE 3 = HA port to communicate to peer

If HA port not present, connect to a dummy switch port

Private Cloud: Microsoft Hyper-V

Microsoft Hyper-V Specifications

Supported Hypervisor: Windows Server 2016 & 2019; Windows Server Core 2016 & 2019

	Small (17.1+)	Medium (17.1+)	Large (17.1+)
Maximum Access Points	1,000	3,000	6,000
Maximum Clients Support	10,000	32,000	64,000
Minimum Number of vCPUs	4	6	10
Required Memory (GB)	8	16	32
Recommended Storage (GB)	16	16	16
Virtual NICs (vNIC) - 3 rd NIC is for High Availability	2 / (3)	2 / (3)	2 / (3)
Max Throughput	2.1 Gbps	2.1 Gbps	2.1 Gbps

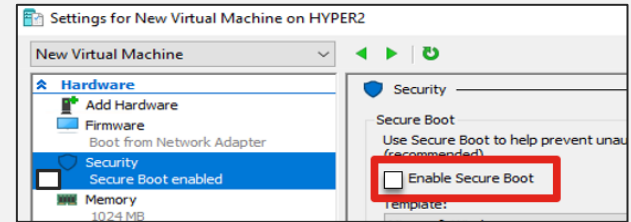
- ❑ VHDX dynamic resizing is not supported by C9800-CL. Static VHDX is supported .
 - ❑ (VHDX is the only disk type supported by Gen-2 Hyper-V)

Generation1 or Generation2 for C9800-CL

- C9800-CL is Supported on both Gen1 and Gen2 type of Hyper-V VM

Secure Boot (Gen2)

- ☐ Generation 2 type VM in Hyper-V enables secure boot by default
- ☐ C9800-CL does not support secure boot
- ☐ When deploying C9800-CL on a Generation-2 VM turn off secure boot in the VM settings



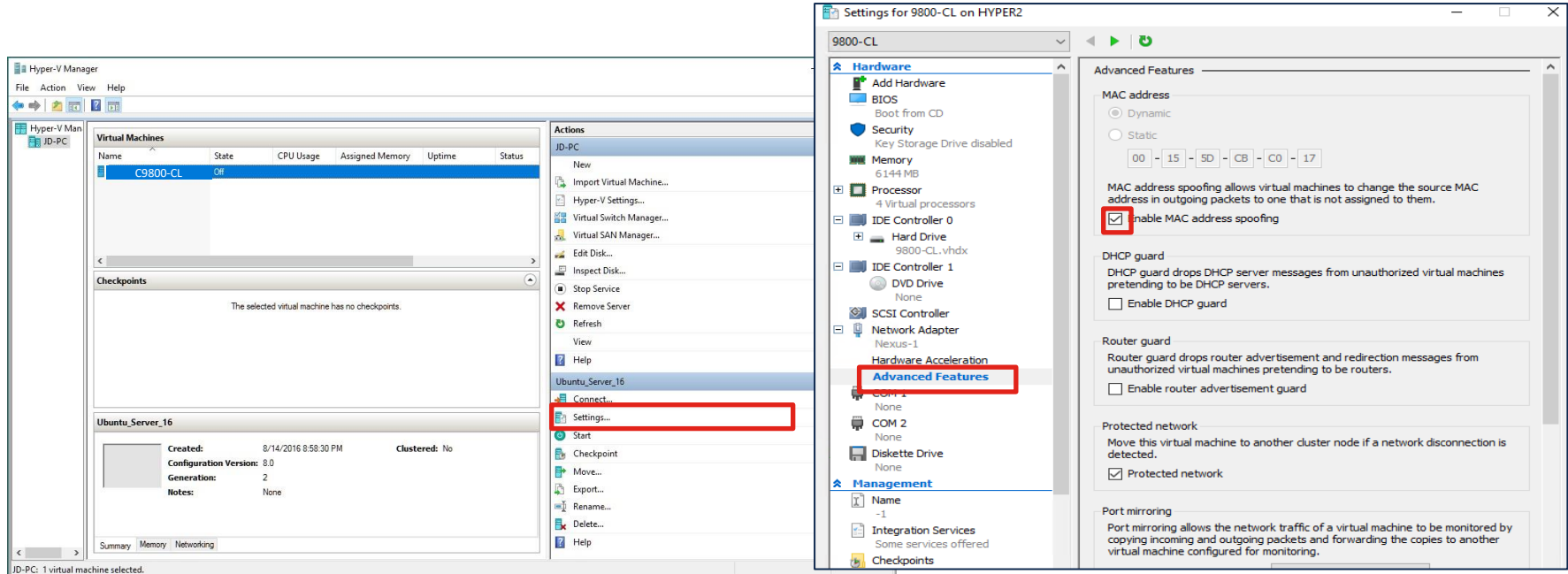
Serial console

- ☐ Serial console is not supported by Hyper-V . However, you can use 3rd party application like Named Pipes for serial console on a Generation1 VM
- ☐ Generation 2 VM, serial console can't be created using 3rd party application as it doesn't support COM port.

MAC Spoofing

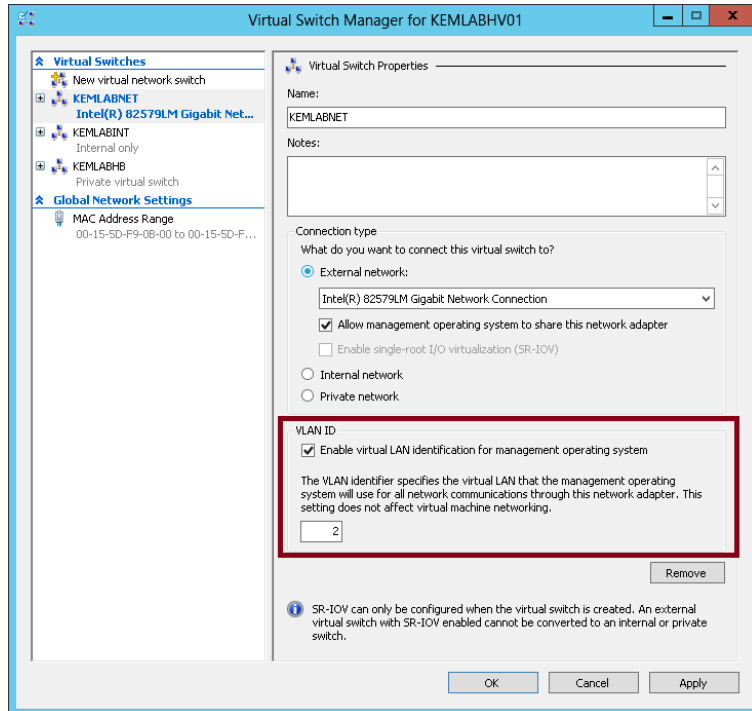
Enable MAC address spoofing for VM management/data mapping interface.

The Hyper-V vSwitch learns MAC addresses and forwards traffic based on MAC address destination.



VLAN Tagging

- ☐ By default, Hyper-V will block packets with a vlan tag
- ☐ Allow vlan-tagged packets for the VM connected interface
- ☐ Use the Virtual switch manager to set the VLAN ID on the interface

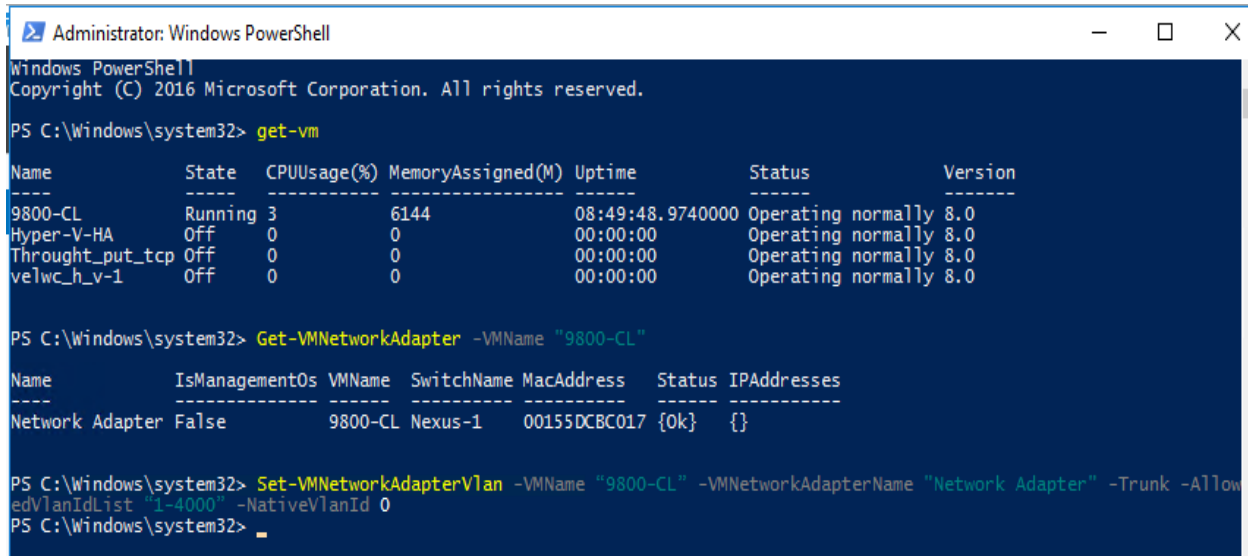


Note : Virtual switch manger does not let you set the trunk option on the interface

Setting Interface to Trunk

- ❑ To configure trunk : set native vlan id 0 from the PowerShell for VMNetwork adapter
- ❑ This will allow all VLANs as below

Set-VMNetworkAdapterVlan -VMName "9800-CL" -VMNetworkAdapterName "Network Adapter" -Trunk -AllowedVlanIdList "1-4000" -NativeVlanId 0



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> get-vm

Name                State      CPUUsage(%)  MemoryAssigned(M)  Uptime                Status              Version
-----
9800-CL              Running    3             6144                08:49:48.9740000      Operating normally  8.0
Hyper-V-HA           Off        0             0                   00:00:00              Operating normally  8.0
Throught_put_tcp     Off        0             0                   00:00:00              Operating normally  8.0
velwc_h_v-1          Off        0             0                   00:00:00              Operating normally  8.0

PS C:\Windows\system32> Get-VMNetworkAdapter -VMName "9800-CL"

Name                IsManagementOs  VMName  SwitchName  MacAddress  Status  IPAddresses
-----
Network Adapter     False           9800-CL  Nexus-1     00155DCBC017 {0k}    {}

PS C:\Windows\system32> Set-VMNetworkAdapterVlan -VMName "9800-CL" -VMNetworkAdapterName "Network Adapter" -Trunk -AllowedVlanIdList "1-4000" -NativeVlanId 0
PS C:\Windows\system32>
```

Вопросы?



Private Cloud: VMware ESXi

VMware Specifications

Supported Hypervisor: VMware ESXi 6.0 Update 2 (minimum)

	Small (16.12+)	Medium (16.12+)	Large (16.12+)
Maximum Access Points	1,000	3,000	6,000
Maximum Clients Support	10,000	32,000	64,000
Minimum Number of vCPUs	4	6	10
Required Memory (GB)	8	16	32
Recommended Storage (GB)	16	16	16
Virtual NICs (vNIC) - 3 rd NIC is for High Availability	2 / (3)	2 / (3)	2 / (3)
vNIC driver	VMXNET3, E1000E, E1000	VMXNET3, E1000E, E1000	VMXNET3, E1000E, E1000
Virtual bridge	vSwitch	vSwitch	vSwitch

VMware Specifications

Supported Hypervisor: VMware ESXi 6.0 Update 2 (minimum)

	Low Throughput (IOS XE 16.12+)	High Throughput (IOS XE 17.3+)
SR-IOV Support (VMware ESXi 6.5+)	No	Yes
SR-IOV NIC Support (VMware ESXi 6.5+)	No	Intel x710 Cisco Intel x710
Max Throughput	2.1 Gbps	5 Gbps
VMware vMotion *	Yes	No
VMware Snapshot *	Yes	No
VMware Cloning from Snapshot	No	No
VMware Distributed Resource Scheduling	Yes	No
VMware NIC Teaming	Yes	No
VMware Fault Tolerance	No	No
VMware Suspend & Resume	No	No
VMware L2 LAG	Roadmap	Roadmap

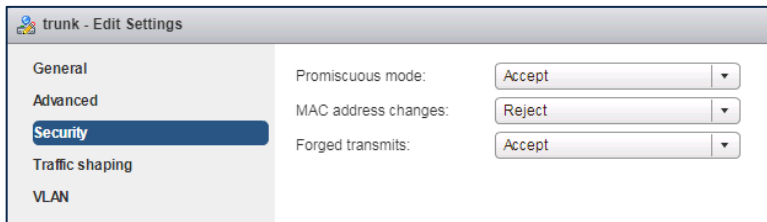
* If using HA SSO, this may cause a failover.



9800-CL on Private Cloud – ESXi deployment

Recommendations

- Both Promiscuous and Forged Transmits need to be set to “Accept” on the PortGroup where 9800-CL is connected. This is needed both for both trunk and non-trunk connections:



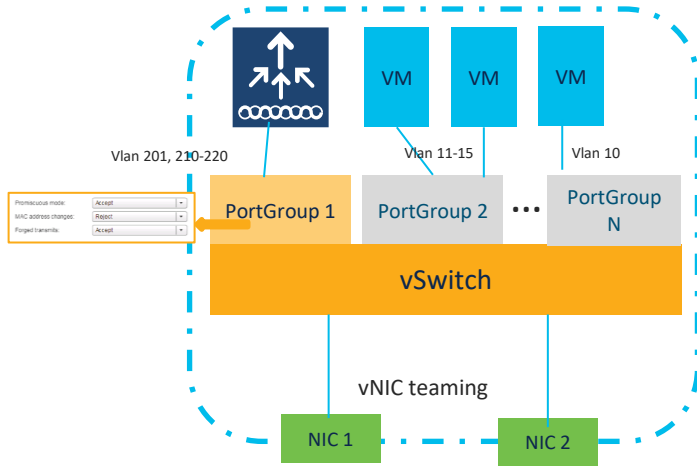
- C9800-CL uses multiple MAC addresses on the same VM and VMware doesn't support MAC learning on the virtual switch, so the only solution is to... flood!
 - Promiscuous mode allows other MAC addresses other than the one of the vNIC to be delivered to the C9800 (so it's used for the incoming traffic);
 - Forged Transmit is used for the outgoing traffic
- Why does C9800-CL use multiple MACs? Multiple reasons: the WLC uses an SVI for Wireless management, it bridges client traffic (in centralized mode), it might use also other SVIs or loopback interface. All these use different MACs other than the one assigned to the vNIC of the VM.

9800-CL on Private Cloud – ESXi deployment

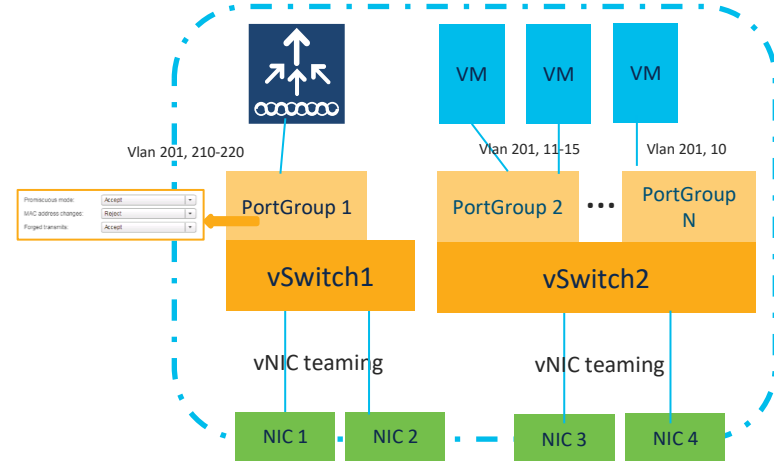
What if you don't want to turn on Promiscuous and Forged Transmits on the vSwitch?

- **For single C9800-CL per server:** dedicate a PortGroup with these security settings only to C9800. If any VLAN is shared with other VMs, put the C9800 on a dedicated vSwitch (or Distributed vSwitch) and enable Promiscuous or Forged only on that C9800 vSwitch

No VLAN shared across C9800 and other VMs

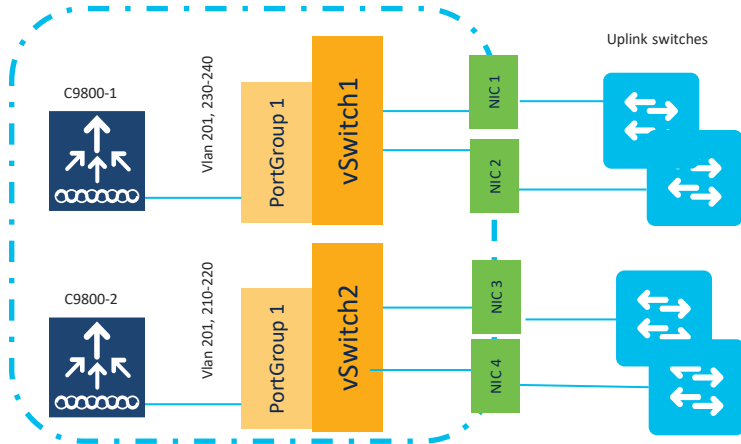


VLANs shared across C9800 and other VMs



9800-CL on Private Cloud – ESXi deployment

- **Multiple C9800-CL per server:** If deploying multiple C9800s on the same ESXi host and VLANs are shared (like the Management VLAN), leverage multiple physical uplinks and put each C9800 on its own vSwitch and PortGroup, each mapped to a different physical uplink. In this case traffic to/from different C9800-CL will be separated by the MAC learning capability of the physical uplink switch that the host is connected to



- The physical uplink switches perform MAC learning
- Traffic coming from C9800-1 on the common VLAN will only be forwarded to the vSwitch-1
- This traffic will not reach C9800-2 even if the VLAN is the same
- Uplink switches configuration depends on the vNIC teaming configuration

- The other option is to use different ESXi hosts all together

9800-CL on Private Cloud - IMPORTANT UPDATES

ESXi Direct Host on 6.7 now supported

Home / VMware vSphere

Download VMware vSphere

Select Version:

6.7

VMware Software Manager makes it easy to find, select, and download the content needed to install or upgrade a VMware product or suite with the push of a button.

Get Your vSphere License Key

[Read More](#)

Product Resources

[View My Download History](#)

[Product Information](#)

[Documentation](#)

[vSphere Community](#)

[Support Resources](#)

[Get Free Trial](#)

Product Downloads

Drivers & Tools

Open Source

Custom ISOs

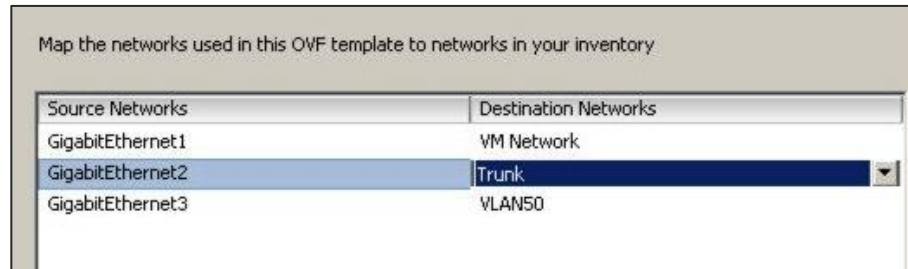
Product	Release Date	
▼ Essentials		
VMware vSphere Hypervisor (ESXi) 6.7U2	2019-04-11	Go to Downloads
VMware vCenter Server 6.7U2	2019-04-11	Go to Downloads

- VMware has released the fix for .ova to be installed on ESXi Host 6.7
- It's a partial fix: **it only works for small template**
- Go to MyVMware download the offline bundle (update-from-esxi6.7-6.7_update02.zip)
- [Here](#) is a link on how to install the patch

Do not deploy OVA files directly to VMware ESXi 6.5.
We recommend that you use an OVF tool to deploy the OVA files.

9800-CL on ESXi: Life Lessons

- Tagged traffic will not flow to 9800-CL unless Promiscuous Mode is enabled
- Check vNIC to Physical NIC mapping is correct
- If cloning, check that you aren't accidentally duplicating Mac addresses
- Check Memory usage – ensure 9800-CL has enough allocated memory. It may hang or become unresponsive otherwise
- Map each interface to a different virtual network! Otherwise, you will introduce a network forwarding loop.





Private Cloud – Life Lessons

- Follow the requested compute requirements. Don't overcommit resources.
 - Hyper-Threading isn't supported.
 - CPUs ought to be dedicated, not shared.
- Don't exceed the client and throughput requirements of the platform/profile.
 - SR-IOV support for KVM and ESXi begins with IOS XE 17.3. Review deployment guide.
- Review the network configuration on the virtual host(s).
 - Physical Port – Interface Speed & Redundancy
- Don't exceed TCAM resources on the upstream switch
- vMotion, DRS, Snapshots, and vNIC Teaming not supported when SR-IOV mode is enabled

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, teal, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of larger squares in the upper left and a trail of smaller dots and squares extending from the upper right towards the bottom right.

Public Cloud Deployment



Why a Wireless Controller in the Public Cloud?

- 1 Exploit the advantages of the Public Cloud**
- 2 Retain the customization and control of onPrem**

Advantages of C9800-CL in Public Cloud

\$0

The C9800-CL Wireless Controller price

7 minutes

Time taken to deploy C9800-CL for AWS/GCP

Up to 50%

Cost Savings seen by a large enterprise by deploying C9800-CL for Private Cloud*^



AWS GovCloud

Host the Catalyst 9800 Series controller in AWS' FedRAMP certified GovCloud



Agility - simple to deploy



Scale based on network size



Global Footprint



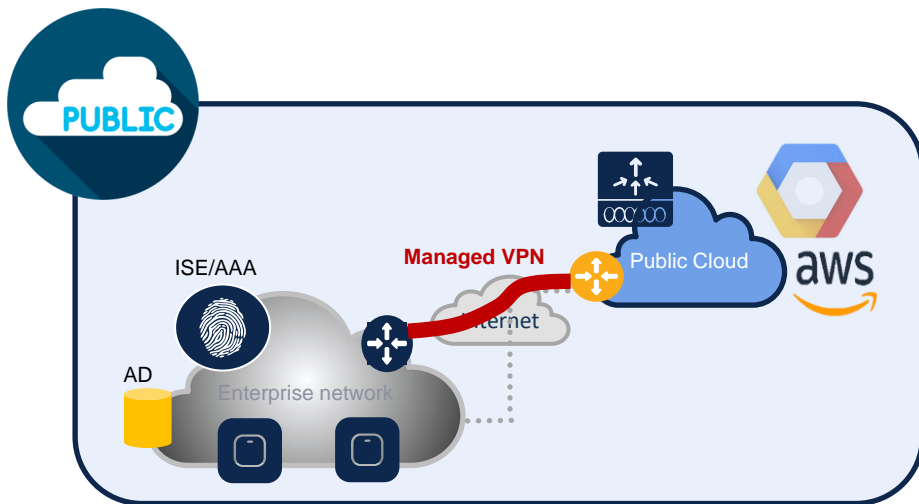
Cost Effective

*Calculation done replacing 5x8540 WLCs with Large C9800-CL instances running on KVM. Flex mode only

^Future

Public Cloud

Catalyst 9800 IaaS



Amazon Web Services
& Google Cloud Platform Marketplaces

Managed VPN *required*

ISE and AD typically on Prem

FlexConnect Local Switching only

Bring Your Own AP License

Guest Anchor – not supported

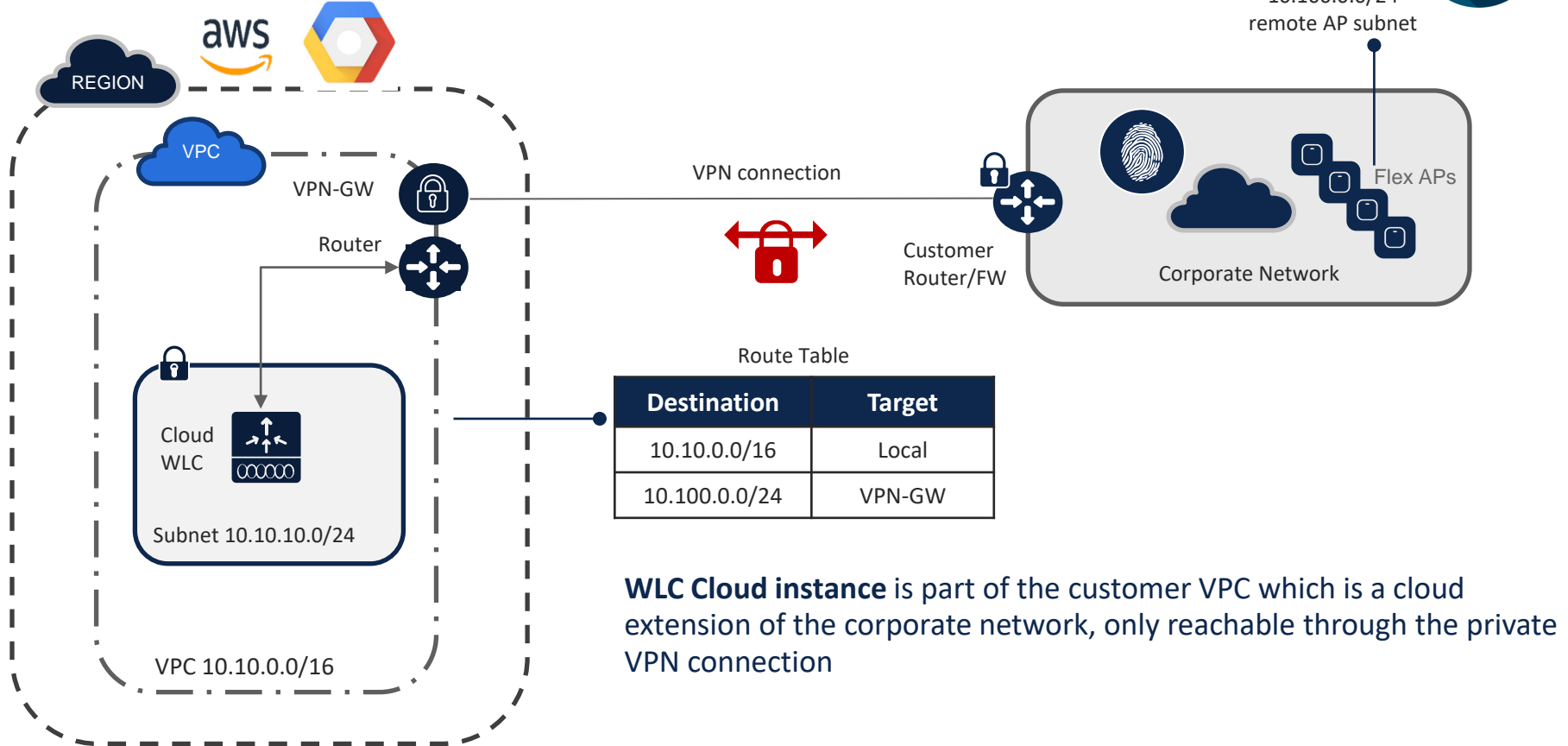
N+1 High Availability only

Cisco DNA Center or Prime Infrastructure -
not supported

C9800-CL Public Cloud Profile Specs

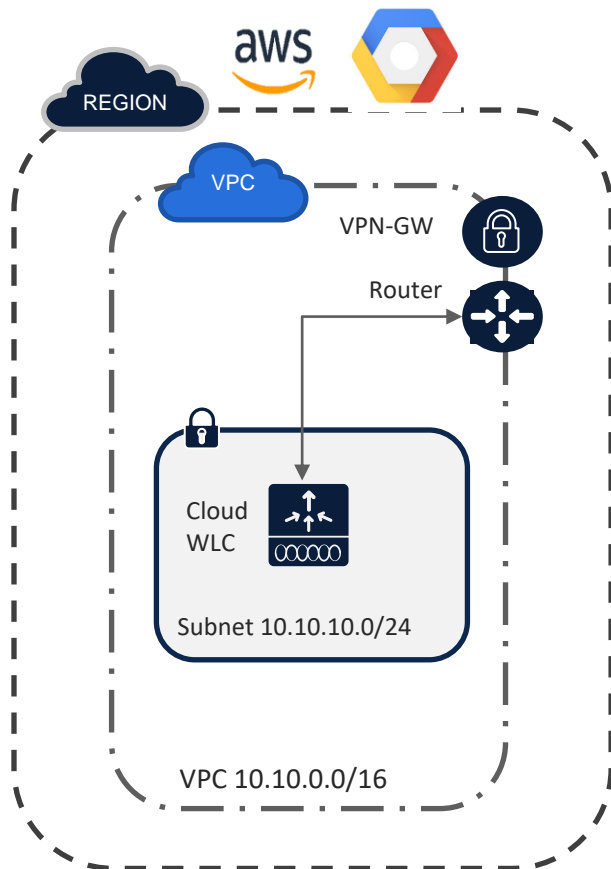
Parameters	Small	Medium	Large
vCPUs	4	6	10
RAM (in GB)	8	16	32
Disk (in GB)	16	16	16
# of NIC	1	1	1
AP Count	1,000	3,000	6,000
Client Count	10,000	32,000	64,000
Deployment Mode	Cisco FlexConnect (Local Switching only)	Cisco FlexConnect (Local Switching only)	Cisco FlexConnect (Local Switching only)
Cloud Providers	AWS, GCP	AWS, GCP	AWS, GCP

Cloud Networking – Managed VPN





Cisco Catalyst 9800 Wireless Cloud Controller



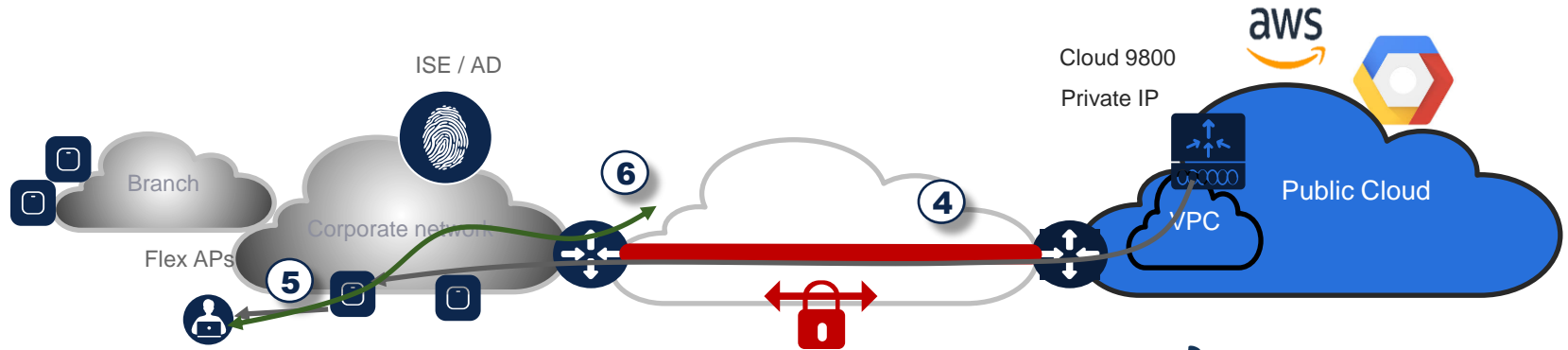
Important things to know:

- All interfaces in Public Cloud are Layer 3, there is **no concept of trunk interfaces**
- In Public Cloud **IP allocations** are done **via DHCP**
 - Customer can decide which IP to allocate to the controller but it's still via DHCP
- For Catalyst 9800 Cloud Wireless Controller in Public Cloud only **one interface deployment is supported**
 - Management and Wireless Management are same

Supported Authentication Modes

Public Cloud – Authentication flow

FlexConnect Central auth – VPC with managed VPN



Authentication and Data traffic flow:

1. EAP traffic is received by AP and sent to WLC
2. WLC talk Radius to ISE/AAA back on-site
3. ISE replies with authentication result and authorization policy to the WLC
4. WLC forwards the reply to AP
5. AP relays authentication frames to client
6. Clients gets IP from a local DHCP server and traffic is locally switched at AP



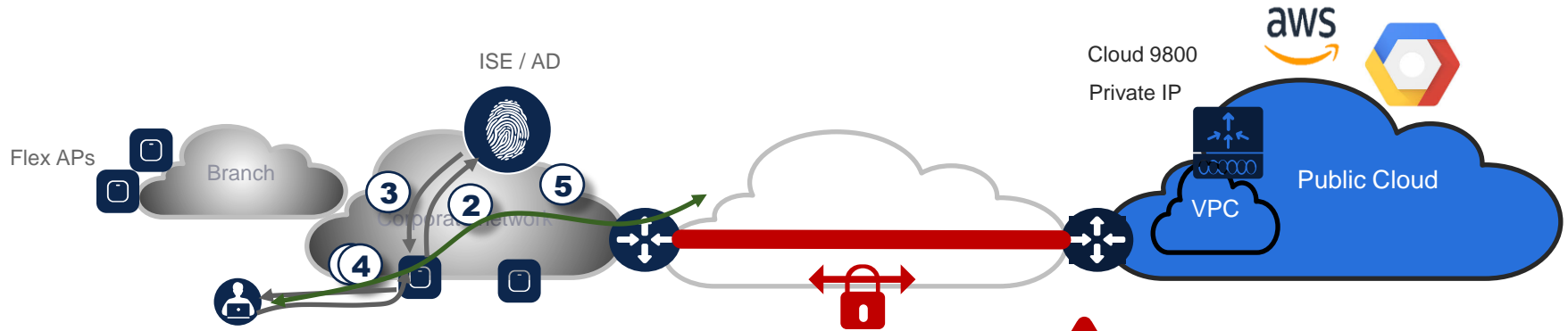
Fully Featured



Only high-level traffic flow is represented

Public Cloud – Authentication flow

FlexConnect Local Auth – VPC with managed VPN



Authentication and Data traffic flow:

1. EAP traffic terminates at Flex AP
2. AP talks directly Radius to ISE/AAA
3. ISE responds with authentication result
4. AP sends response to client
5. Traffic is locally switched at AP



No extra latency



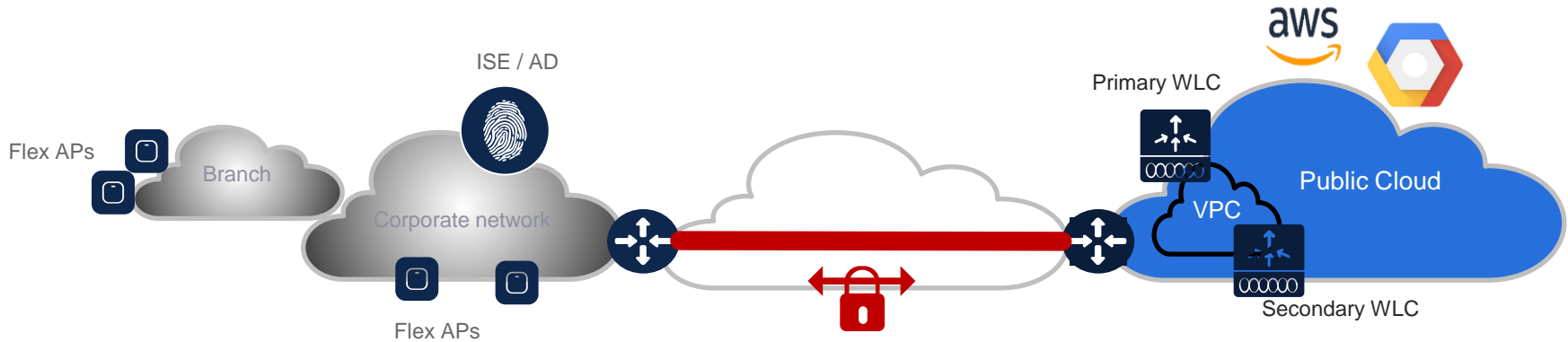
- Important features missing: BYOD, WebAuth, CoA, etc.
- APs need to reach ISE and be configured as NAS

802.11r support IOS XE 17.2+

Flex Local Auth is supported only as fall back if AP loses communication with Cloud WLC

Supported High Availability Modes & Software Updates

Public Cloud – High Availability



N+1 HA for WLC in the Cloud:

- Create a WLC instance in the same VPC but in a different subnet
- Associate this subnet to a different availability zone than Primary WLC
- Configure the AP with a Secondary controller

A dark blue circle containing a white lowercase letter 'i'.

- Cloud provides support only for L3 interfaces
- No SSO HA for WLC in the Cloud



Public Cloud – High Availability

Best Practice - Configure the AP's Primary and Secondary Controller

Edit AP

General Interfaces High Availability Inventory Advanced

	Name	Management IP Address
Primary Controller	<input type="text"/>	<input type="text"/>
Secondary Controller	<input type="text"/>	<input type="text"/>
Tertiary Controller	<input type="text"/>	<input type="text"/>

AP failover priority



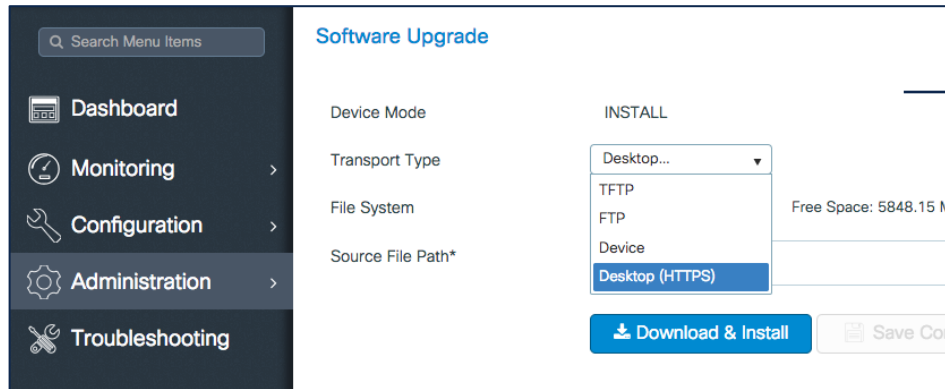
Utilize scripting or programmatic model (YANG) for bulk AP updates.

Software Upgrade – Option 1

Upgrade public cloud C9800 instance

Upgrade the software using the .bin file (Install Mode)

- Download the “.bin” image from CCO locally to a PC or to an FTP/TFTP server
- Go to Administration > Software Upgrade and select one of the available methods



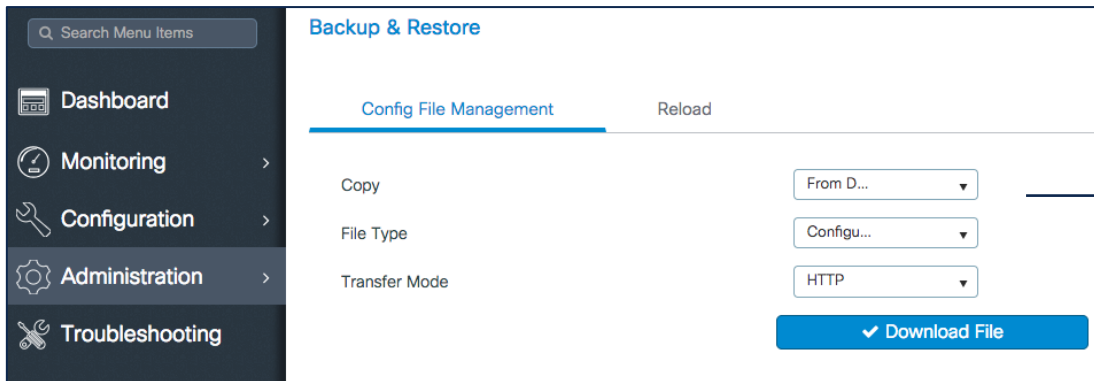
Same procedure used for
the appliance or VM

Software Upgrade – Option 2

Migrate a public cloud C9800 instance

Create a new cloud instance and migrate the existing configuration

- Create a new instance (e.g. launching the instance from Marketplace); go through the WLC DAY 0 GUI on the new instance
- On the old/existing instance go to Administration > Backup & Restore and download the configuration that you want to migrate. Download it to PC or to a server.



- Choose “from device”
File type “Configuration”
Transfer mode (FTP/TFTP/HTTP)

9800-CL on Public Cloud – Life Lessons

- No real console (read-only console output feasible)
- Cisco only support **VPN based deployment**: use either AWS VPN GW (easy but limited) or deploy your own (CSRv)
- Public cloud supports only Wireless Management on a L3 interface: IP configured on the GigabitEthernet interface. **No VLANs and no “interface vlan” (SVI) in AWS/GCP.**
- **Features gap**: AP sniffer mode, Hyperlocation, Multicast, and Client IPv6 are NOT supported with a Wireless Management L3 interface deployment (management IP assigned to a L3 physical or loopback interface)
- Same throughput considerations as per C9800-CL on Private Cloud

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, teal, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares forming a diagonal band from the top right towards the bottom right. The text 'Key Takeaways' is positioned in the lower-left area of the image.

Key Takeaways

Catalyst 9800 Cloud – Guides

Cisco Catalyst 9800-CL Wireless Controller for Cloud Deployment Guide

- <https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-wirel-cloud-dep-guide-cte-en.html>

Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide (Public & Private Cloud Options)

- <https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/9800-cloud/installation/b-c9800-cl-install-guide.html>

Public Cloud – Deployment Guides

Deployment guide for Cisco Catalyst 9800 Wireless Controller for Cloud on Amazon Web Services (AWS)

- https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_cisco_catalyst_9800_wireless_controller_aws.html
- <https://youtu.be/kXPPeP3Ah3Y>

Deployment Guide for Cisco Catalyst 9800 Wireless Controller for Cloud on Google Cloud Platform

- <https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/9800-cloud/deployment/c9800-cl-gcp-deployment-guide.pdf>

Learn More



[Migration to the New Catalyst Wireless Stack, a practical guide!](#)



[Campus LAN and WLAN Solution Design CVD](#)

[C9800 Release Notes](#)

[C9800 Configuration Guides](#)

[C9800 Technical References](#)

[C9800 Configuration Examples and Tech Notes](#)

[C9800 Command References](#)

[C9800 Deployment Best Practices](#)

[C9800 WLC Configuration Model](#)

[WLC Configuration Converter](#)

[WLC Compatibility Matrix](#)

[AireOS to IOS-XE Command Mapping](#)

[AireOS to Catalyst 9800 Wireless Controller Feature Comparison Matrix](#)

[Cisco WLAN YouTube Channel](#)



Thank you

