



Information About Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution

- [Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution, on page 1](#)
- [Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Components, on page 2](#)

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution

As more applications move to the cloud, the traditional approach of backhauling traffic over expensive WAN circuits to a data center is no longer relevant. The conventional WAN infrastructure was not designed for accessing applications in the cloud. The infrastructure is expensive and introduces unnecessary latency that degrades the experience.

Network architects are reevaluating the design of the WANs to achieve the following:

- Support a cloud transition.
- Reduce network costs.
- Increase the visibility and manageability of the cloud traffic.

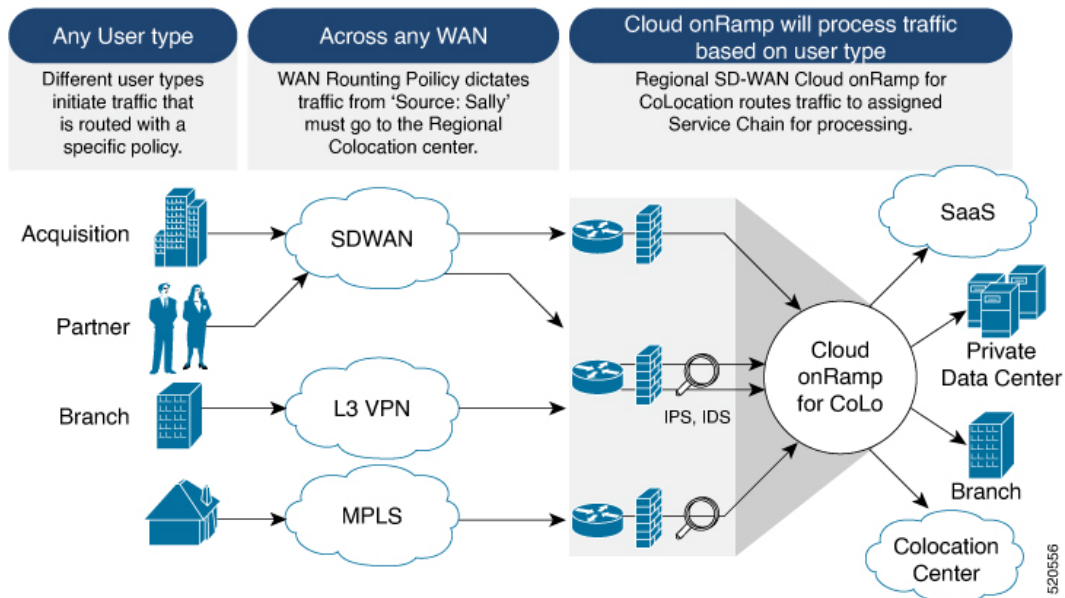
The architects are turning to Software-Defined WAN (SD-WAN) fabric to take advantage of inexpensive broadband Internet services and to route intelligently a trusted SaaS cloud-bound traffic directly from remote branches.

With the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution built specifically for colocation facilities, the solution routes the traffic to the best-permissible path from branches and remote workers to where all applications are hosted. The solution also allows distributed enterprises to have an alternative to enabling direct internet access at the branch and enhance their connectivity to infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) providers.

The solution provides enterprises with multiple distributed branch offices that are clustered around major cities or spread over several countries the ability to regionalize the routing services in colocation facilities. Reason being, these facilities are physically closer to the branches and can host the cloud resources that the enterprise needs to access. So, essentially by distributing a virtual Cisco Catalyst SD-WAN over a regional architecture of colocation centers, the processing power is brought to the cloud edge.

The following image shows how you can aggregate the access to the multicloud applications from multiple branches to regional colocation facilities.

Figure 1: Cisco Catalyst SD-WAN Cloud OnRamp for Colocation



The solution can serve four specific types of enterprises:

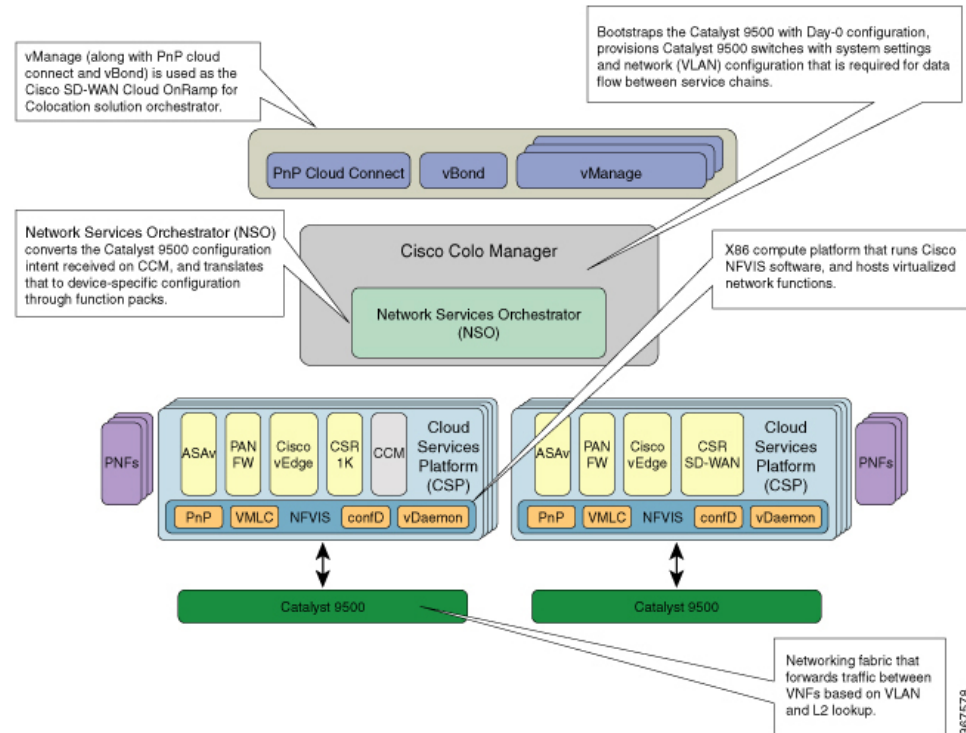
- Multinational companies that cannot use direct internet connections to the cloud and SaaS platforms due to security restrictions and privacy regulations.
- Partners and vendors without Cisco Catalyst SD-WAN but still need connectivity to their customers. They do not want to install Cisco Catalyst SD-WAN routing appliances in their site.
- Global organizations with geographically distributed branch offices that require high bandwidth, optimum application performance, and granular security.
- Remote access that need secure VPN connections to an enterprise over inexpensive direct internet links.

The Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution can be hosted within certain colocation facilities by a colocation IaaS provider. You can select the colocation provider that meets your needs in a region on a regional basis as long as it supports the necessary components.

Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Components

The Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution can be deployed in multiple colocations. A colocation is a stack of compute and networking fabric that brings up multiple virtual networking functions and multiple service chains on them. This stack connects branch users, endpoints to a hybrid cloud or data center. Cisco vManage is used as the orchestrator to provision the devices in a colocation. Each colocation does not have visibility of other colocations in the same site or across sites.

The following image shows the components of Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution.

Figure 2: Cisco Catalyst SD-WAN Cloud OnRamp for Colocation Solution Architectural Overview

- **Cisco Cloud Services Platform, CSP-5444 and CSP-5456**—Cloud Services Platform (CSP) is an x86 Linux hardware platform that runs NFVIS software. It is used as the compute platform for hosting the virtual network functions in the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution. Multiple CSP systems can be used in a Cisco Catalyst SD-WAN Cloud OnRamp for Colocation deployment.

Cisco Network Function Virtualization Infrastructure Software—The Cisco Network Function Virtualization Infrastructure Software (NFVIS) software is used as the base virtualization infrastructure software running on the x86 compute platform. The Cisco NFVIS software provides VM lifecycle management, VM service chaining, VM image management, platform management, PNP for bootstrapping a device, AAA features, and syslog server. See the NFVIS Functionality Changes for SD-WAN Cloud OnRamp for Colocation in [NFVIS documentation](#).

- **Virtual Network Functions** —The Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution supports both Cisco-developed and third-party Virtual Network Functions (VNFs). The following table includes the validated VNFs and their versions:

Table 1: Validated Virtual Network Functions

| Virtual Network Functions | Version |
|-------------------------------------|-------------------------------------|
| Cisco CSR1000V | 17.1.1, 17.2, 17.3 |
| Cisco Catalyst 8000V | 17.4.1a |
| Cisco IOS XE Catalyst SD-WAN Device | 16.12.1, 16.12.2r, 17.2.1r, 17.3.1a |
| Cisco ASAv | 9.12.2, 9.13.1, 9.15.1 |
| CheckPoint | R80.30, R80.40 |

| Virtual Network Functions | Version |
|---------------------------|--------------------------------|
| Cisco FTDv/NGFW | 6.4.0.1, 6.5.0-115 |
| Cisco vEdge Cloud Router | 19.2.1, 20.1.1, 20.3.1, 20.4.1 |
| Palo Alto Firewall (PAFW) | 9.0.0 |
| Fortinet Firewall | 6.0.2 |

To validate third-party VNFs on the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, you can use the Cisco certification program. For more information about validating third-party VNFs, see <https://developer.cisco.com/site/nfv/#the-ecosystem-program>.

- **Physical Network Functions**—A Physical Network Function (PNF) is a physical device that is dedicated to provide a specific network function as part of a colocation service chain such as a router or a firewall. The following are the validated PNFs and their versions:

Table 2: Validated Physical Network Functions

| Physical Network Functions | Version |
|------------------------------|---------------------------|
| Cisco FTD Model: FPR-9300 | 6.4.0.1, 6.5 |
| Cisco ASR 1000 Series | 16.12.1, 17.1, 17.2, 17.3 |

- **Network Fabric**—Forwards traffic between the VNFs in a service chain by using a L2 and VLAN-based lookup. The last VNF can forward traffic to the network fabric either through L2 or L3 forwarding. The network fabric can include either of the following:
 - Cisco Catalyst 9500-40X switch: Supports 40 10G ports and two 40G ports, which is used as the network fabric
 - Cisco Catalyst 9500-48Y4C switch: Supports 48 1G/10G/25G ports and four 40G/100G ports, which is used as the network fabric.
- **Management Network**—A separate management network connects the NFVIS software running on the CSP systems, the virtual network functions, and the switches in fabric. This management network is also used for transferring files and images into and out of the systems. The Out of Band management switch configures the management network. The IP addresses assigned to the CSP devices, Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches are acquired by the management network pool through DHCP configuration. The orchestrator manages VNF management IP addresses and assigns through the VNF Day-0 configuration file.
- **Virtual Network Function Network Connectivity**—A VNF can be connected to the physical network by using either Single Root IO Virtualization (SR-IOV) or through a software virtual switch. A VNF can have one or more virtual network interfaces (VNICs), which can be directly or indirectly connected to the physical network interfaces. A physical network interface can be connected to a software virtual switch and one or more VNFs can share the virtual switch. The Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution manages the creation of virtual switch instances and the virtual NIC membership to create connectivity. By default, all the physical interfaces and the management interface in the CSP system are available for use by VNFs.

In Cisco Catalyst SD-WAN Cloud OnRamp for Colocation deployments, SR-IOV interfaces are configured in Virtual Ethernet Port Aggregator (VEPA) mode. In this mode, the NIC sends all the traffic that is received from the VNFs to the external Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. The Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C transfers the traffic that is based on the L2 MAC address and VLAN. It can send the traffic back to the CSP or to an external connected network. The Catalyst 9500 switch ports that are connected to the CSP interfaces are configured in VEPA mode. When a VLAN is configured on a VNF VNIC, the VLAN must be configured on the connected port on Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches.

A VNF using a SR-IOV interface and a VNF using the software switch can be service chained through the external switch fabric.

- **Physical Network Function Network Connectivity**— A PNF can be connected to the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switch ports, which are the free data ports available from the right side.
- **Service Chains** —In Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution deployment, the traffic between the VNFs is service chained externally through Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C. The service chaining requirement provides service chaining functionality to the traffic across VNFs running either on a single CSP or across multiple CSP systems in a cluster. The service chaining is based on the source and destination endpoints in the service chain and is not based on the provider application. In Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution, L2 (VLAN, destination MAC address) based service chaining has been used.
- **Cisco Colocation Manager** —The Cisco Colocation Manager (CCM) component is a software stack that manages the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C switches. In this solution, Cisco Colocation Manager is hosted on NFVIS software in a docker container. The CSP devices host Cisco Colocation Manager along with PNFs and VNFs as shown in the solution architectural overview

A single CCM instance per cluster is brought up in one of the CSP devices after activating a cluster. The CCM software accepts the Cisco Catalyst 9500-40X or Cisco Catalyst 9500-48Y4C configuration and monitors them. See [Configure Cloud OnRamp for Colocation Devices from vManage](#) for more information.
- **Orchestration through Cisco vManage** —Cisco vManage server is used for orchestrating the Cisco Catalyst SD-WAN Cloud OnRamp for Colocation solution. For more information, see the [Cisco SD-WAN Configuration Guides](#).

