Cisco NSO Datacenter Core Function Pack (CFP) Solution Guide

First Published: 2020-12-17

Last Modified: 2021-09-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Solution Overview** 1

About Cisco NSO and CFPs 1

About Cisco Network Services Orchestrator 1

Layered Services Architecture 2

About NSO Core Function Packs 3

About the Cisco NSO DC-SDN Core Function Pack 3

About the Cisco NSO DC-Transport Core Function Pack 4

Additional NSO Documentation and Resources 7

CHAPTER 2 **Use Case: Datacenter CFP** 9

Telco Cloud Deployment Using NSO 9

CHAPTER 3 **Use Case: Cross-Domain Orchestration Using SR/MPLS Handoff** 11

Cross-Domain Orchestration Using SR/MPLS Handoff 11

CHAPTER 4 **Use Case: Brownfield Support** 15

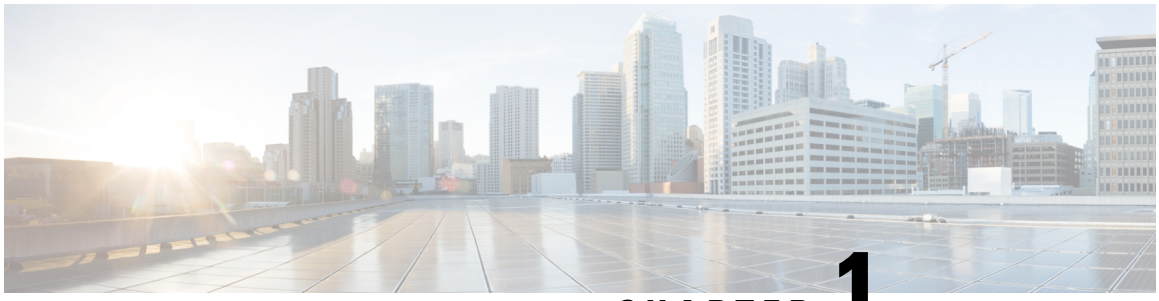
Brownfield Configuration 15

CHAPTER 5 **Use Case: SPAN Monitoring** 17

SPAN Monitoring 17

CHAPTER 6 **Use Case: IP SLA Monitoring Policies** 19

IP SLA Monitoring Policies 19



CHAPTER 1

Solution Overview

- About Cisco NSO and CFPs, on page 1
- About Cisco Network Services Orchestrator, on page 1
- About NSO Core Function Packs, on page 3
- About the Cisco NSO DC-SDN Core Function Pack, on page 3
- About the Cisco NSO DC-Transport Core Function Pack, on page 4
- Additional NSO Documentation and Resources, on page 7

About Cisco NSO and CFPs

Cisco Network Services Orchestrator (NSO) core function packs (CFPs) extend the NSO core platform to address specific use cases.

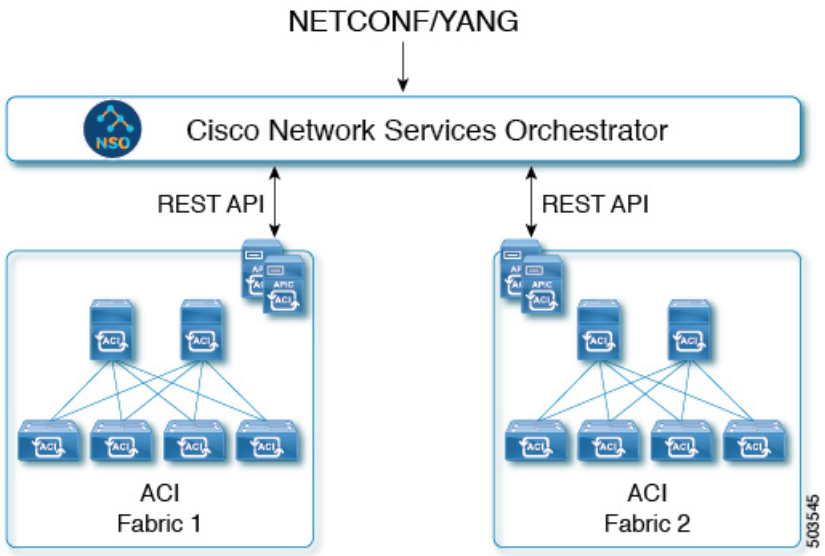
About Cisco Network Services Orchestrator

Cisco Network Services Orchestrator (NSO) provides a robust bridge linking network automation and orchestration tools with the underlying physical and virtual infrastructure.

NSO provides a single, network-wide interface to all network devices and services, using a single-state model and configuration database. YANG models describe all NSO configuration, including device and service configurations. NSO includes a rich set of northbound software interfaces and APIs that allow straightforward northbound integration. An extensible southbound device abstraction layer allows NSO to work with multiple technology domains.

The following figure shows how NSO abstracts the configuration of Cisco ACI fabrics, allowing configuration based on YANG models.

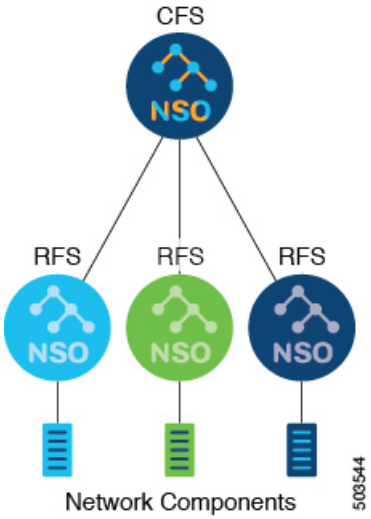
Figure 1: NSO translates models to underlying APIs



Layered Services Architecture

Cisco NSO uses a Layered Services Architecture (LSA), in which a service is implemented in an upper-layer customer-facing (CFS) service and one or more lower-level resource-facing services (RFS) that interact with network components.

Figure 2: NSO Layered Services Architecture



The LSA architecture provides these benefits:

- High scalability
- Automation across lower node domains and boundaries
- Improved performance through parallel service execution

- Allows rolling, granular upgrades and isolated testing

About NSO Core Function Packs

A Core Function Pack (CFP) is a ready-made add-on software package for NSO that is intended for a specific use case or a set of closely related use cases. Because the CFP is use-case driven instead of being general purpose, it can simplify configuration of the network function, exposing only the settings necessary for the application. The CFP can automate other areas of the configuration, it can validate the resulting configuration, and it can roll back the configuration if needed.

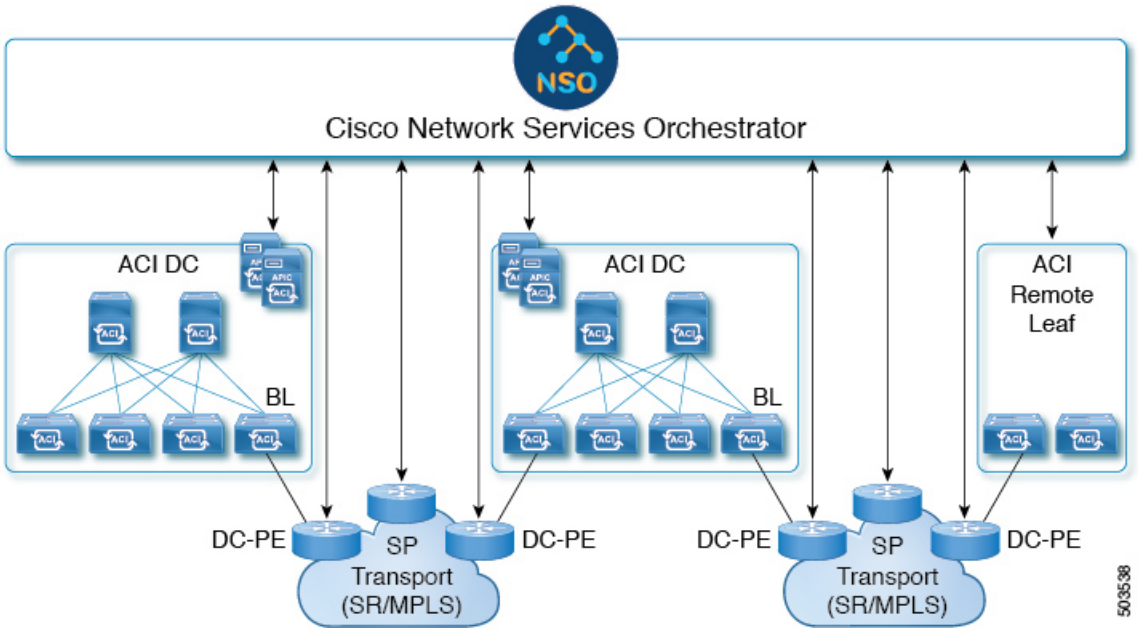
A CFP can comprise a bundle of packages, including device drivers, templates, and other CFPs. A CFP is a released software package, fully supported by Cisco TAC.

About the Cisco NSO DC-SDN Core Function Pack

The Cisco NSO Data Center - Software Defined Networking (DC-SDN) CFP focuses on the provisioning of datacenter fabrics and domains connecting to datacenter fabrics. For example, this CFP allows you to provision an ACI fabric without the need to understand the details of the ACI-specific configuration model. The CFP provides the following functionality:

- Provisioning and management of multiple ACI fabrics, Multi-Pod, and Remote Leaf (RL) networks
- Telco datacenter (DC) provisioning, including DC handoff provisioning for both IP and segment routing (SR/MPLS) handoffs to the transport domain
- Multi-domain orchestration across the DC and transport domains

Figure 3: Cisco NSO DC-SDN application topology



Cisco NSO DC-SDN Core Function Pack Use Cases

The NSO DC-SDN CFP provides a single interface for many management and provisioning scenarios, including the following:

- A single tool to automate and orchestrate the provisioning of multiple data centers
- A single tool to manage data centers and transport networks
- A tool to perform cross-domain orchestration between a data center and a transport network
- The DC-SDN CFP, when combined with other CFPs, can be used to perform end-to-end service provisioning across data centers, transport networks, Network Functions Virtualization Infrastructure (NFVI) servers, and other domains

In this solution document, we will focus on the cross-domain orchestration between a data center and a transport network.

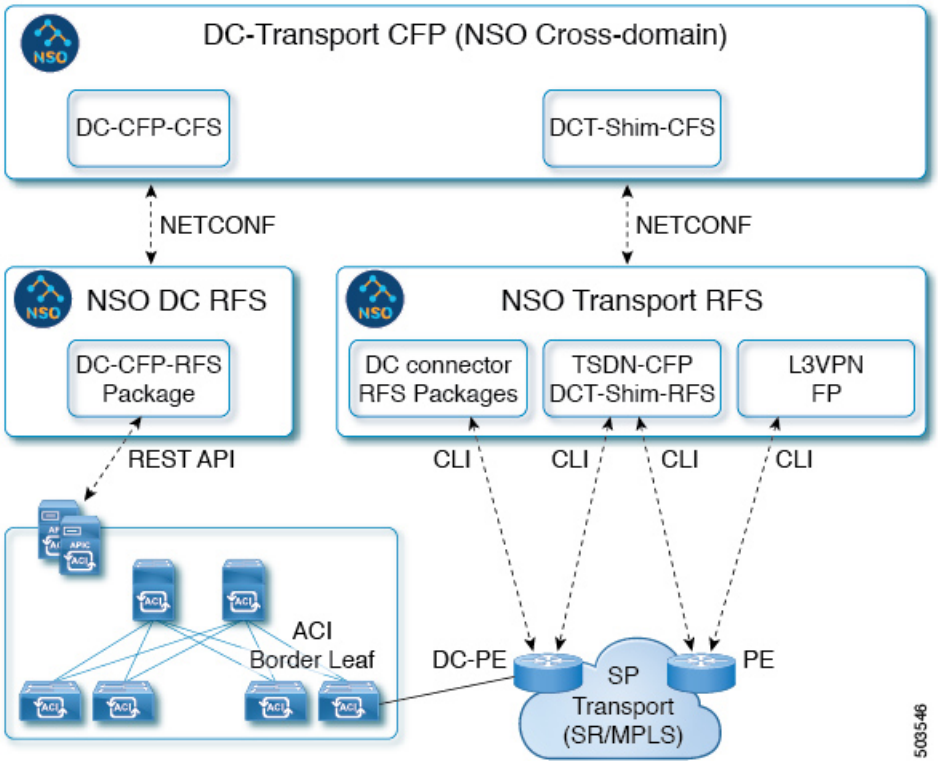
About the Cisco NSO DC-Transport Core Function Pack

The Cisco NSO DC-Transport CFP, a component of the NSO DC-SDN CFP, provides multi-domain orchestration across the datacenter (DC) domain and the service provider (SP) domain. The DC-Transport package extends the DC-SDN CFP to allow NSO to configure the domain edge devices:

- The border leaf (BL) switches that serve as the datacenter edge facing the transport network
- The provider edge (DC-PE) routers that serve as the transport network edge facing the datacenter

In the DC-SDN solution, three NSO instances are used in a Layered Services Architecture (LSA), as shown in the following figure:

Figure 4: NSO instances for cross-domain orchestration



- A customer-facing cross-domain "upper NSO" with the DC-Transport CFP provides the top-level orchestration for the two resource-facing "lower NSO" instances.
- A Datacenter NSO with the DC CFP provisions the APIC controllers of the ACI datacenter.
- A Transport NSO provisions the PE routers of the SP transport network, using three installed function packages:
  - The DC-Connector CFP to provision the handoff to the DC-PE router
  - The TSDN CFP to configure the segment routing in the transport network
  - The L3VPN function pack to provision the VPN services

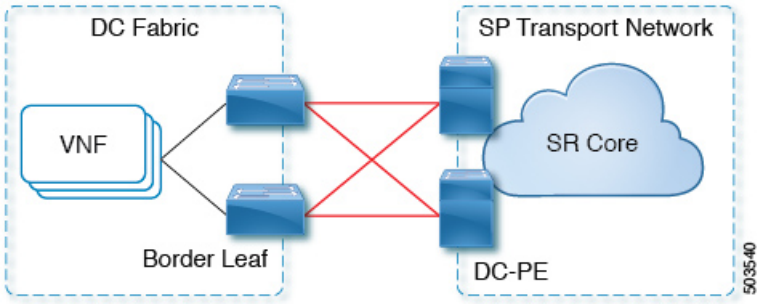
This solution is capable of managing multiple ACI datacenters and multiple DC-PE devices through the single top-level NSO.

Cross-Domain Connection

The DC and SP domains can be directly connected, as shown in Figure 5: Direct connection of DC to SP network, on page 6, or connected remotely.

Note Although the following figure shows the recommended connection using two BL switches and two DC_PE routers, you can also connect with one BL to one DC-PE or with two BLs to one DC-PE.

Figure 5: Direct connection of DC to SP network



The following figures show a remote connection between domains, using either the IP handoff method or the segment routing (SR/MPLS) handoff method.

Figure 6: IP handoff of DC to SP network

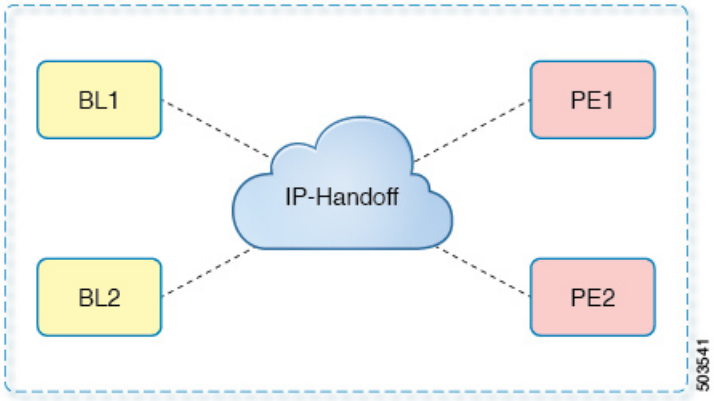
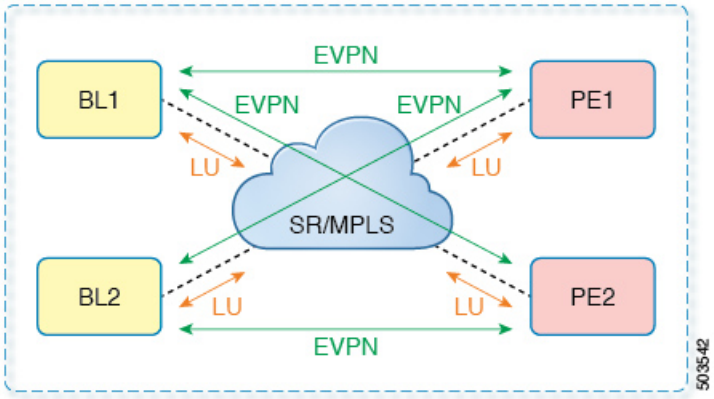


Figure 7: SR/MPLS handoff of DC to SP network



Additional NSO Documentation and Resources

Cisco NSO DC-SDN CFP Documentation

The following documents are available for the NSO DC-SDN CFP:

- *Data Center – Software Defined Networking - Core Function Pack User Guide*
- *Data Center – Software Defined Networking - Core Function Pack Installation Guide*
- *Cisco DC-Transport YANG Models*

These documents are bundled with the NSO software. To download the documents, go to the Cisco Software Download page and search for Network Services Orchestrator 5.x (or later).

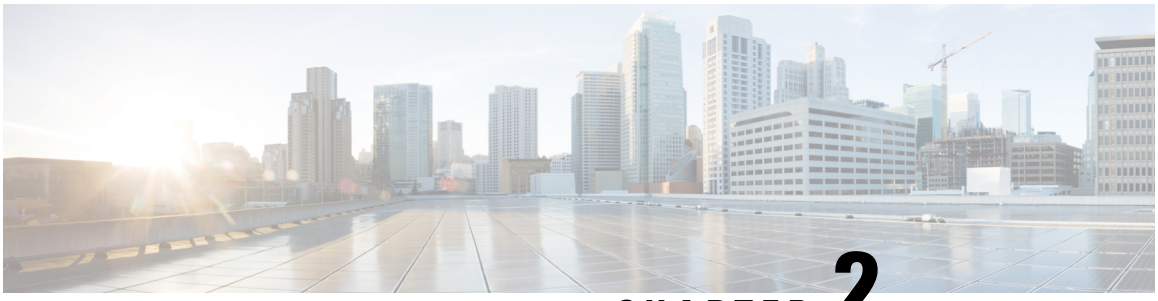
Cisco NSO General Documentation

For information about Cisco Network Services Orchestrator (NSO), go to http://cisco.com/go/nso or to the Cisco NSO documentation page.

You can find NSO tutorials, labs, and developer information on Cisco DevNet at https://developer.cisco.com/docs/nso/.

Cisco ACI Documentation

For detailed information about deploying, configuring, and using the Cisco ACI components and fabric, see the *Cisco Application Policy Infrastructure Controller (APIC)* documentation page. The ACI documentation includes technical references, troubleshooting guides, and white papers.



CHAPTER 2

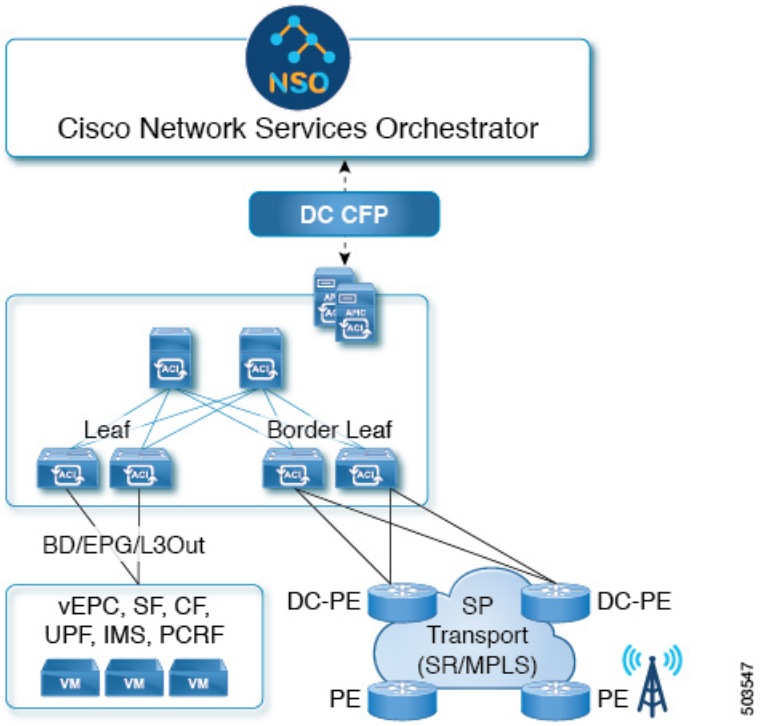
Use Case: Datacenter CFP

- Telco Cloud Deployment Using NSO, on page 9

Telco Cloud Deployment Using NSO

NSO, using the datacenter (DC) CFP, can provision the datacenter for a telco cloud, pushing policies for 4G/5G services such as those shown in the following figure. In the DC CFP use case, NSO pushes ACI policies to bring up 4G/5G services in the telco datacenter.

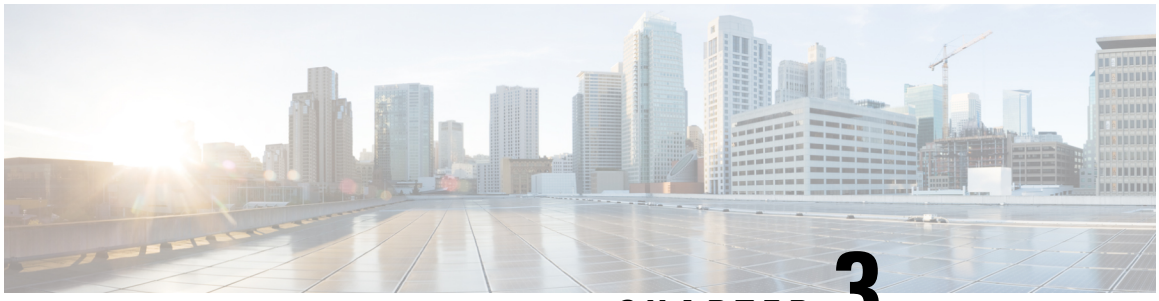
Figure 8: NSO for telco cloud deployment



NSO will automate the deployment and configuration of the following policies in the ACI fabric:

- Interfaces and VLANs
- Tenants, endpoint groups (EPGs), bridge domains (BDs), VRFs, and contracts

- Routing, including BGP and static routes
- Route maps
- Service chaining, including policy-based routing (PBR)
- Quality of Service (QoS)



CHAPTER 3

Use Case: Cross-Domain Orchestration Using SR/MPLS Handoff

• Cross-Domain Orchestration Using SR/MPLS Handoff, on page 11

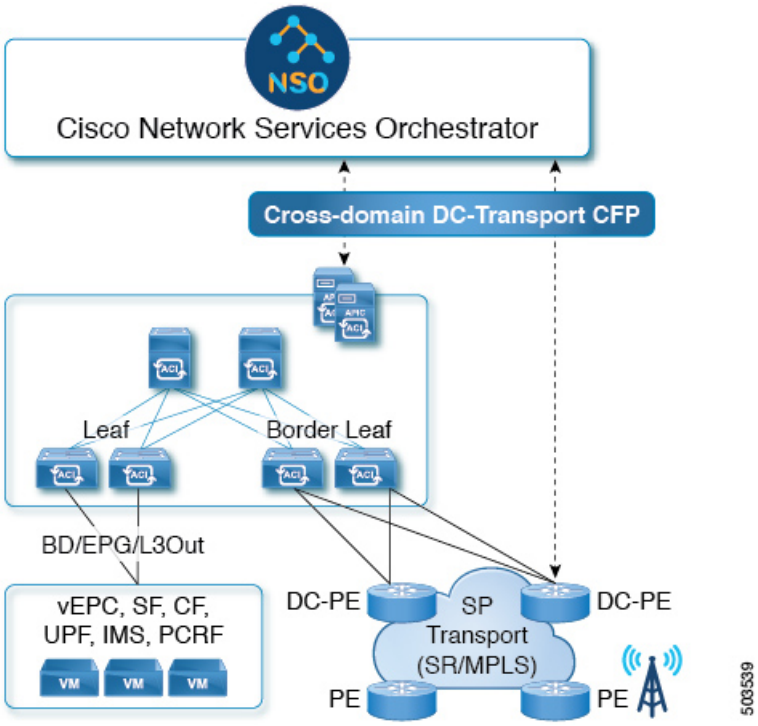
Cross-Domain Orchestration Using SR/MPLS Handoff

In this solution example, we use NSO with the DC-Transport CFP to orchestrate cross-domain transport between the datacenter domain and the service provider (SP) transport domain of a telco network.

The DC-Transport CFP, which is part of the DC-SDN CFP bundle, facilitates the provisioning of the cross-domain transport, enabling automation, scale, and consistent policy between domains.

In this example, shown in the following figure, the handoff to the SP transport network is a segment routing (SR/MPLS) handoff.

Figure 9: Telco ACI datacenter and transport network



You can also provision SR/MPLS handoff for ACI distributed DC solutions such as ACI Remote Leaf, Multi-Site, and Multi-Pod topologies.

Automated Configuration

To provision the cross-domain connection, you will need to provide resource pools, such as the IP subnet, router IDs, and VLAN pools. Using the DC-Transport CFP, NSO will then automate the configuration of the following policies and settings for the ACI border leaf switches and the DC-PE routers:

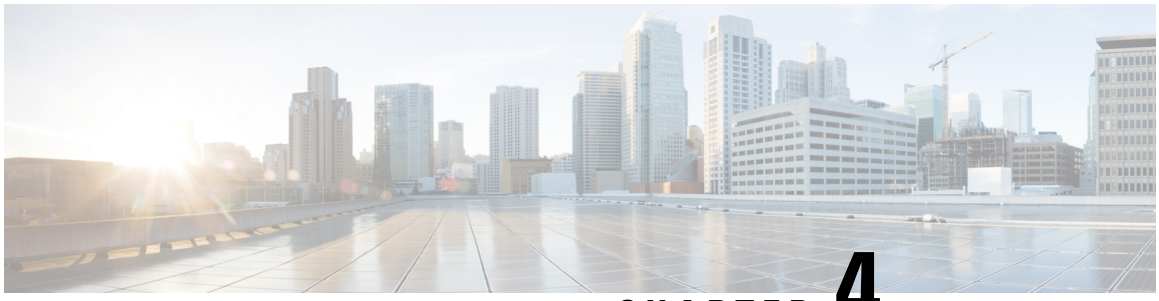
- VLAN and IP addresses for the underlay BGP-LU, EVPN loopback, transport loopback, RD, RT, VLAN, SID, and Router-ID
    - If resource pools are provided, NSO can also manage these resources during operation, including automatic allocation and removal as needed.
- MPLS QoS policies
- BGP EVPN and labeled unicast session
- Single and Multi-hop BFD
- Routing policies such as BGP color community
- SR/MPLS QOS policies

NSO will also configure Route Target (RT) translation from EVPN to L3VPN on the DC-PE routers, and it will map BGP color-community and prefixes to SR policies on the DC-PE routers.

Software Requirements

The following table lists the minimum software requirements for this solution.

Service	Software Version
IP Handoff	APIC Release 4.2(x)
SR/MPLS Handoff	APIC Release 5.0(x)
IOS XR	Release 7.0.2
SR-TE CFP	Release 1.1



CHAPTER 4

Use Case: Brownfield Support

- Brownfield Configuration, on page 15

Brownfield Configuration

Beginning with the Cisco NSO DC-SDN Core Function Pack (CFP) Release 1.1, NSO DC-SDN CFP can import the preexisting (brownfield) configuration of the controlled devices, such as an APIC, by executing a `sync-from` operation. You can then modify the imported configurable entities (objects, policies, or services) of the device's configuration, or you can create new entities.

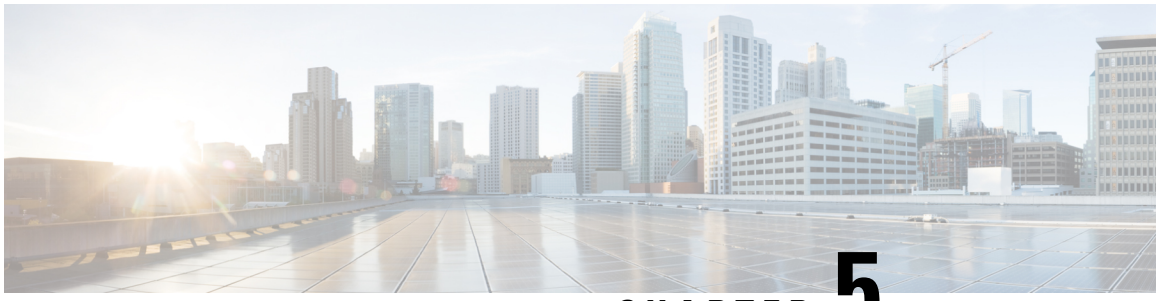
Configurable entities created using NSO are "owned" by NSO and can be deleted by NSO. Preexisting configurable entities imported by NSO are not owned by NSO. When you use NSO to delete an entity not owned by NSO, the configuration of the entity merely reverts to its state before any modification by NSO. For example, if you use NSO to modify an EPG in an imported brownfield configuration, and then you delete that EPG, the configuration of the EPG reverts to its configuration before it was imported into NSO.

You can have NSO take ownership of an imported entity through a special "reconcile" operation.

Brownfield configuration actions that you can perform using NSO include the following:

- Create a new EPG, BD, L3Out, contract, service graph, or VRF within an existing Tenant and VRF.
- Add ports into an existing L3Out. Create a regular L3 Port, vPC, PC, SVI, or sub-interface.
- Add ports into an existing EPG. Ports could be regular L2 ports, vPC, or PC.
- Configure a new vPC, PC, regular L2/L3 port on an existing switch.
- Use an existing contract, service graph into existing EPG, L3Outs.
- Add new ports into existing configured SPAN (Access and ERSPAN) sessions (both source and destination).
- Create a new L3Out with existing route-map configuration.
- Add a new subnet/External EPG into existing L3Out.
- Add a new next-hop into existing static route.
- Add a new static route into existing L3Out.
- Add a route-map into existing L3Out.

- Add a new BGP neighbor into existing L3Out.
- Add a new BGP LU and BGP EVPN neighbor into existing SR/MPLS L3Out.
- Add a new interface into SR-MPLS Infra L3Out for BGP-LU.
- Add new subnets, export policy, import policy into existing SR-MPLS VRF L3Out.
- Perform autocompletion in the CLI for the following entities: BFD Policy, L3Out name, PBR policy, Filter.
- Add a route-map policy and add/delete/modify match/set rules into route-map.
- Modify and use an existing BFD policy.
- Add new node into existing L3Out node profile.
- Add new interfaces into existing L3Out interface profile.
- Add new interface profiles into existing node profile of L3Out. (This is required for IPv6 since both v4 and v6 cannot be enabled in a single interface profile).
- Simplify APIC-Port service to ensure user is only asked for ports required to be configured and not the whole path.
- Use existing Physical domain, external domain, AEP and VLAN pool for new ports to be configured from NSO.
- Use a VLAN pool that's configured in dynamic VLAN allocation mode.
- Configure a new contract into an existing external EPG.
- Configure a new VPC on a leaf that's already configured with vPC domain and have preconfigured vPCs.
- Add a new next-hop and tracking into existing PBR policy.
- Use an existing PBR tracking policy into a new PBR policy configuration.
- Add a new line into existing filter.
- Add a new filter into existing contract.
- Add a new service device and its interface into existing device group.
- Configure a static EP for ERSPAN.



CHAPTER 5

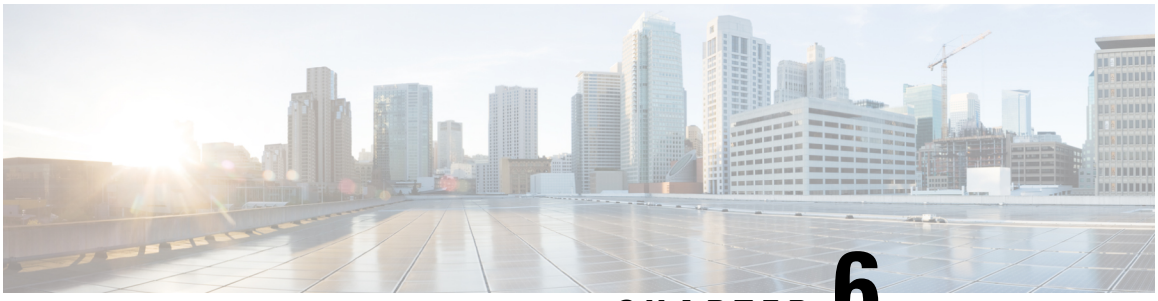
Use Case: SPAN Monitoring

- SPAN Monitoring, on page 17

SPAN Monitoring

Switched Port Analyzer (SPAN) is a troubleshooting utility that copies traffic from one or more ports, VLANs, or endpoint groups and sends the copied traffic to one or more destinations for analysis by a network analyzer. You can use SPAN to perform detailed troubleshooting or to take a sample of traffic from a particular application host for proactive monitoring and analysis.

Beginning with the Cisco NSO DC-SDN Core Function Pack (CFP) Release 1.1, you can use NSO to configure SPAN on a tenant (tenant SPAN) or on a switch. When configuring SPAN on a switch, you can configure SPAN as a fabric policy (fabric SPAN) or an access policy (access SPAN).



CHAPTER 6

Use Case: IP SLA Monitoring Policies

• IP SLA Monitoring Policies, on page 19

IP SLA Monitoring Policies

An IP Service Level Agreement (IP SLA) is a method for using active traffic monitoring — the generation of traffic in a continuous, reliable, and predictable manner — for measuring network performance. Using an IP SLA monitoring policy, you can track network performance and take actions such as permitting, dropping, or bypassing a service device based on service chaining or Policy-Based Redirect (PBR) requirements.

Beginning with the Cisco NSO DC-SDN Core Function Pack (CFP) Release 1.1, you can use NSO to configure IP SLA for L1/L2 and L3 PBR cases. Once defined, an IP SLA monitoring policy can be applied to a PBR policy to define actions (permit, drop, bypass) based on the liveliness of a service device.