ı' ı' ı'ı'
CISCO
The bridge to possible

Data-Center Cross-Domain Orchestration with Cisco NSO Core Function Pack

Contents

Introduction

Service-provider networks are going through a revolutionary shift due to advancements in 5G, and Communication Service Providers (CSP)s are constantly looking to automate their operations to meet the increased demand. Automation is not easy when we try to accomplish a cross-domain task because the domain-specific automation tools are not always capable of performing cross-domain automation. Hence, there is a need for a tool that can act as a single, unified solution for a given domain as well as for cross-domain automation needs. In this paper we will discuss the cross-domain automation capabilities of Cisco® Network Service Orchestrator (NSO), a well-known automation tool for Service Provider (SP) networks.

Example use-case: Cross-domain orchestration across data-center and transport networks for 5G

With 5G, communication service providers need to install data centers closer to end customers to meet the low-latency requirements of time-sensitive applications. With the increased number of Data Centers (DCs), there is a need for an automation solution that can seamlessly integrate with both the data-center and transport parts of CSP networks. The automation solution should be able to onboard applications in DC, provision cross-domain connections between DC and Transport networks and enable the network as a whole to grant on-demand resources for application traffic. The automation solution capable of doing this will take control of the complete application deployment lifecycle.
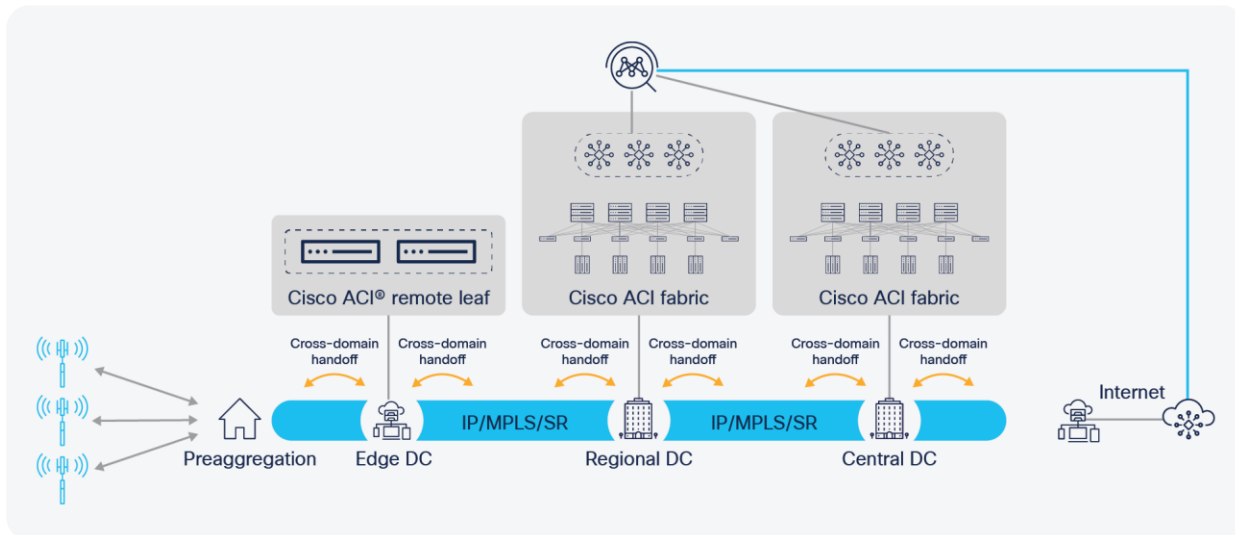

Figure 1.
Telecom data centers and cross-domain handoffs between data-center and transport networks

With the growing variety of applications, it is important for CSPs to prepare networks to identify and treat network traffic distinctly. For example, real-time analysis and feedback-based application traffic cannot be treated like normal browsing traffic within the transport network. 5G network slicing is precisely trying to address this challenge. With the help of NSO, we can orchestrate the end-to-end transport network slice for a particular kind of traffic by leveraging segment routing On-Demand Tunnelling (ODN) in the transport domain.
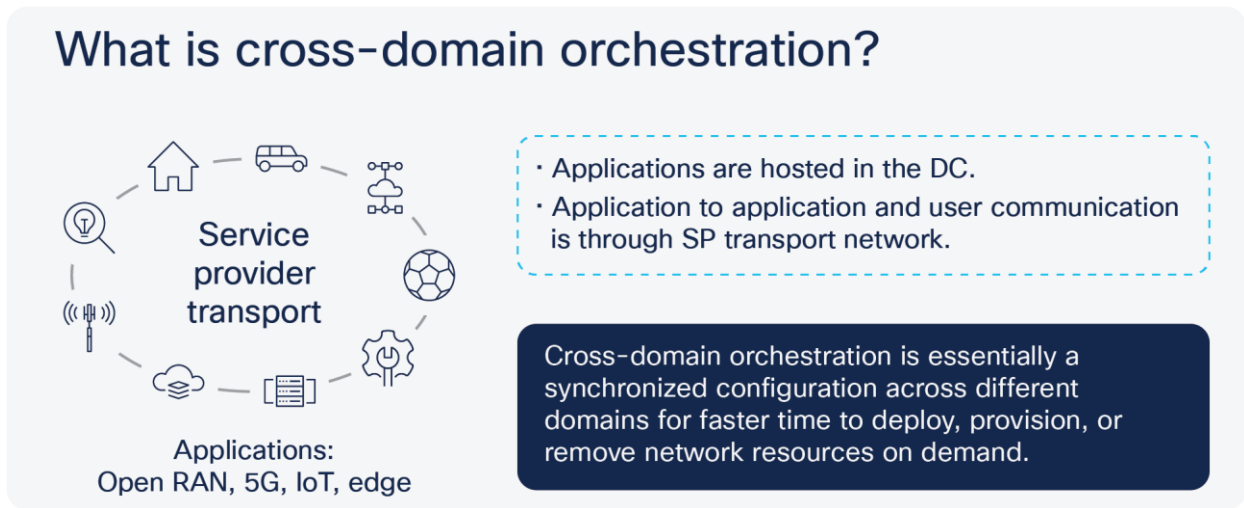

Figure 2.
Applications in a 5G network

The idea of unifying domains is not easy. The orchestrator tool should be able to work between different domains and present a uniform experience to the user by abstracting domain-specific elements. NSO evolves through the domain boundaries and takes care of the complete application deployment and network configuration lifecycle. The NSO DC-Transport Core Function Pack (CFP) can automate application onboarding in the data-center fabric and provision the handoff connection between data-center and transport networks. All this provisioning and decommissioning can be performed with NSO by just a single click in customer OSS/BSS environments.
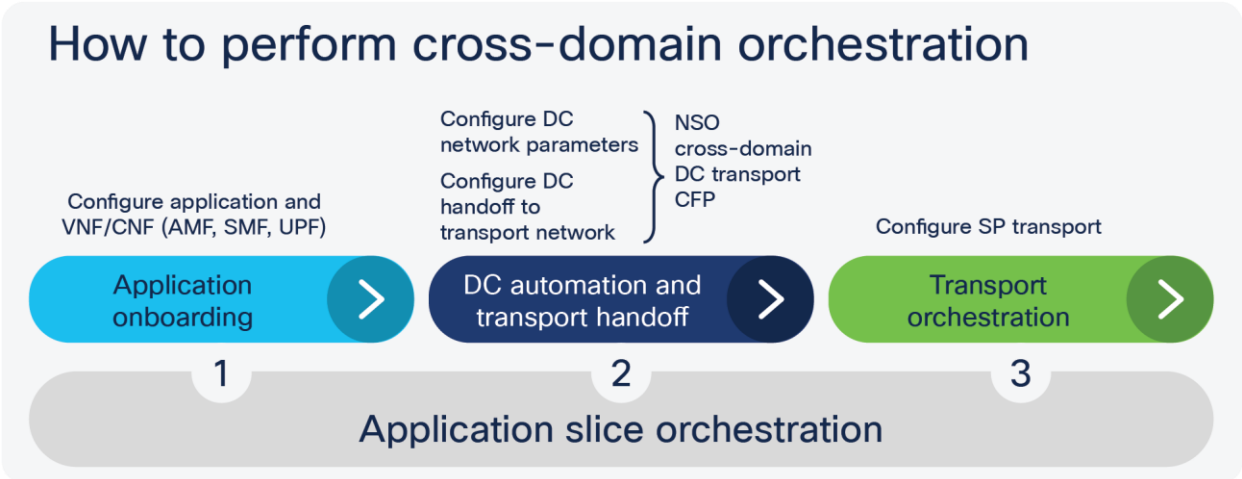
Figure 3.
Cross-domain automation lifecycle

In a core function pack, we get prebuilt, productized services integrated with NSO to reduce implementation time and cost for CSP. This helps improve time to market for the CSP.
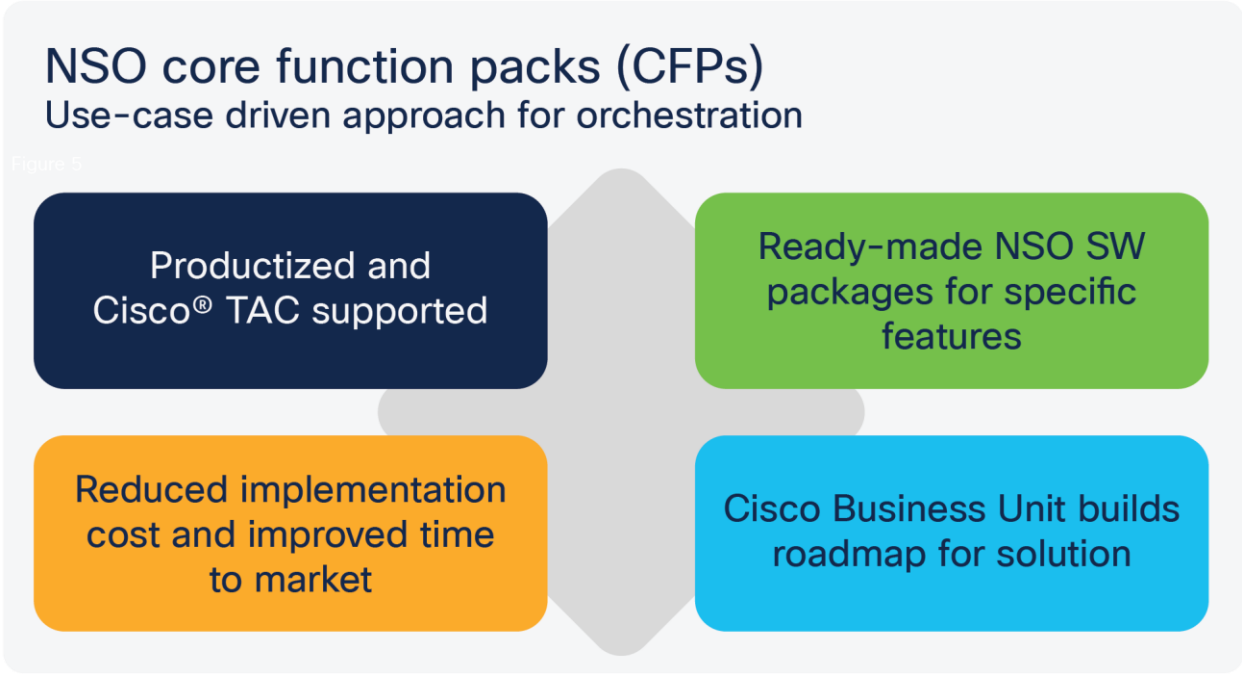

Figure 4.
Cross-domain Core Function Pack (CFP) benefits

NSO cross-domain orchestration architecture

For cross-domain orchestrations, using NSO's Layered Service Architecture (LSA) is recommended. In this architecture we have two layers of NSO implementations: CFS (customer-facing services) and RFS (resource-facing services). CFS is the node that provides interfaces to interact with OSS/BSS systems; it translates instructions with the help of device-specific Network Element Driver (NED) packages to push changes finally to the RFS node. The RFS node is the one interacting with end devices, such as routers, servers, etc. This architecture provides nearly unlimited horizontal scale for NSO deployments and gives us the liberty to use different domain-specific RFS nodes with the same parent CFS, which is the unifying point for the different domains, thus making the cross-domain orchestration possible. For example, in order to perform cross-domain orchestration possible between DC and Transport networks one CFS NSO node can be connected to RFS node in DC and to the RFS node in Transport.
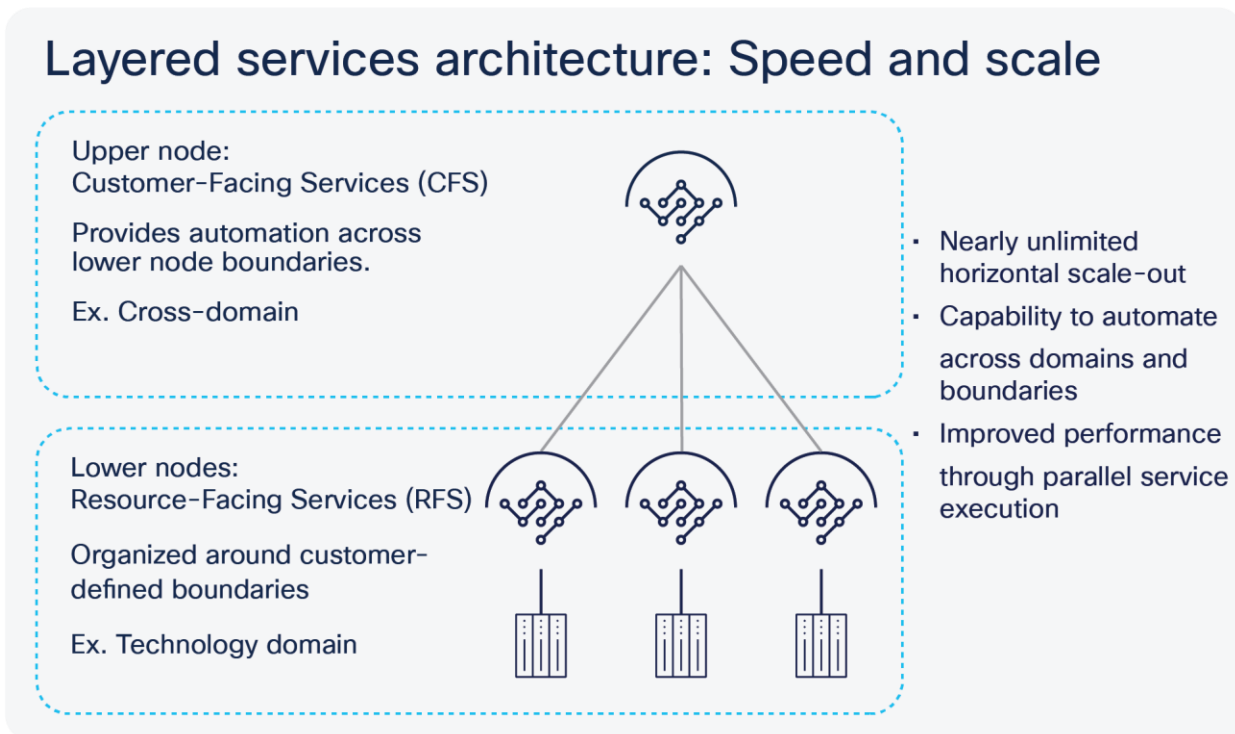

Figure 5.
NSO layered-service architecture

DC-transport cross-domain orchestration feature details

Device specific Network element Driver or NED packages used with NSO makes it capable of connecting and automating services on different devices, for example if we need to automate IOS-XR based device we need IOS-XR based NED package, if we want to automate NXOS based device NXOS based NED package is needed. Network administrators can automate almost everything in the data center and transport networks using the NED packages provided by NSO. However, using NEDs to create service packages may take some time, domain-specific core function packs such as the DC-Transport Core Function Pack provide prebuilt service packages, hence reducing the time it takes to create the entire NSO service package. We can configure many features in Cisco ACI® and the transport network with the help of the DC-Transport CFP. The overall capabilities of CFPs can be described in three steps, described below:

1. Using the NSO CFP, we can configure ACI constructs such as tenants, ports and port policies, contracts, QoS, service chaining, etc.
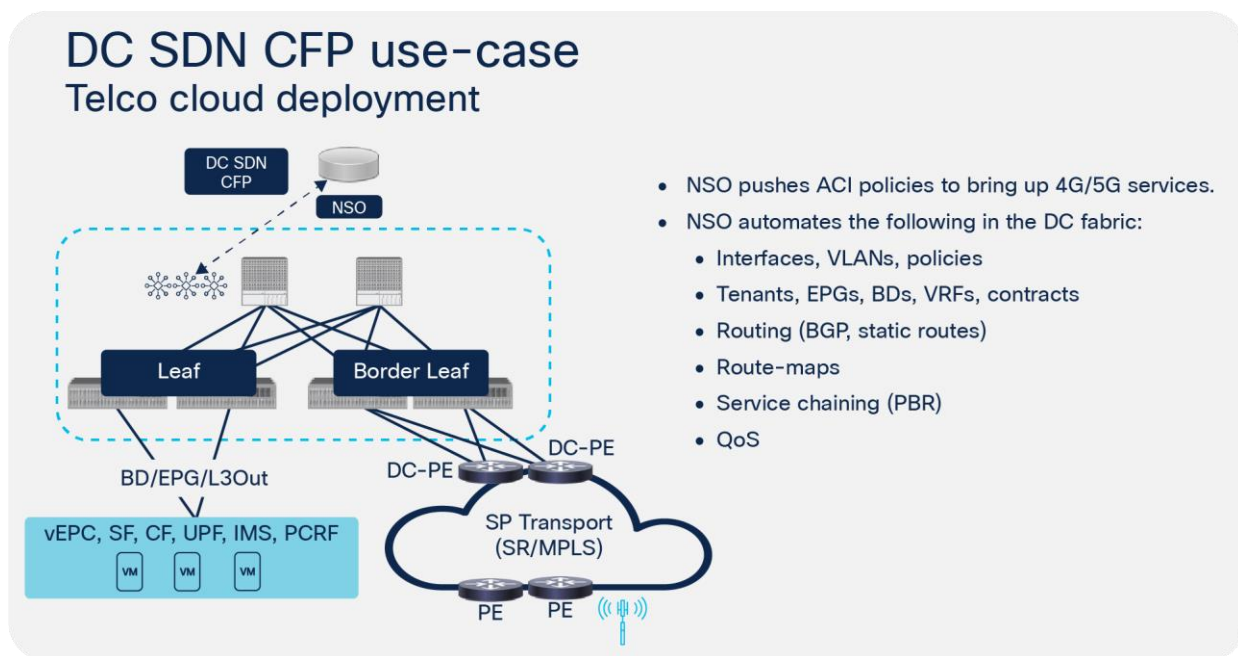

Figure 6.
Configuring of ACI constructs by NSO

2. It also automates the handoff configuration between the ACI fabric and the transport network. The figures below illustrate handoff features between the ACI and transport networks that can be automated with the help of NSO CFP.

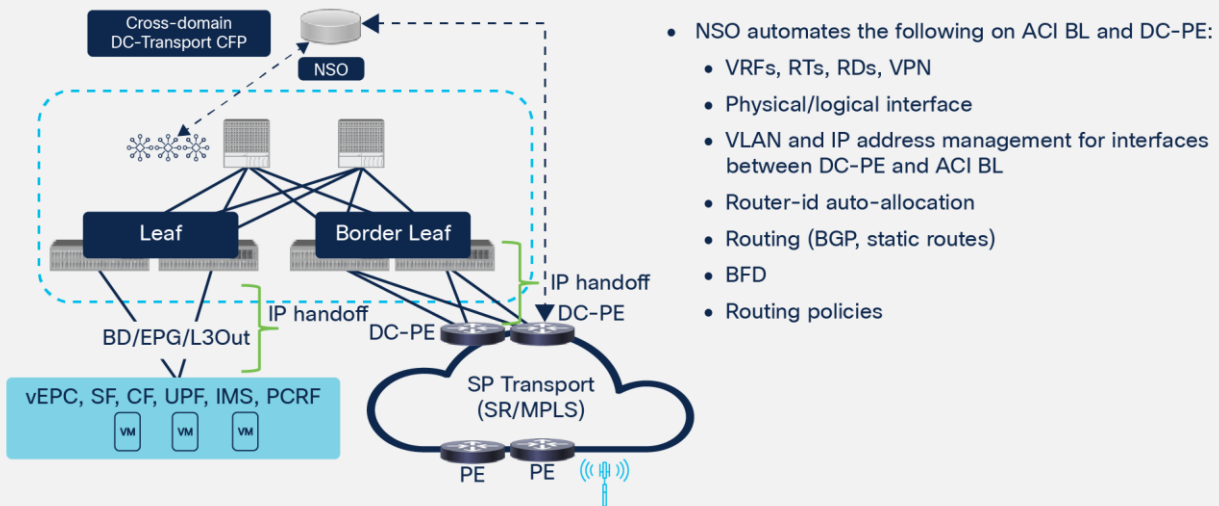

Cross-domain core function pack (IP handoff)

- NSO automates the following on ACI BL and DC-PE:
  - VRFs, RTs, RDs, VPN
  - Physical/logical interface
  - VLAN and IP address management for interfaces between DC-PE and ACI BL
  - Router-id auto-allocation
  - Routing (BGP, static routes)
  - BFD
  - Routing policies

Figure 7.
Configuring ACI IP handoff with NSO

Cross-domain core function pack (SR handoff)

- NSO will automate following configurations on ACI BL and DC-PE:
  - Configuration and management of VLAN and IP addresses for underlay BGP-LU, EVPN loopback, transport loopback, RD, RT, VLAN, SID, and Router-id
  - MPLS QoS policies
  - BGP EVPN and labeled unicast sessions
  - Single- and multi-hop BFD
  - Routing policies such as BGP color community
  - SR/MPLS QoS policies
- RT translation from EVPN to L3VPN on DC-PE
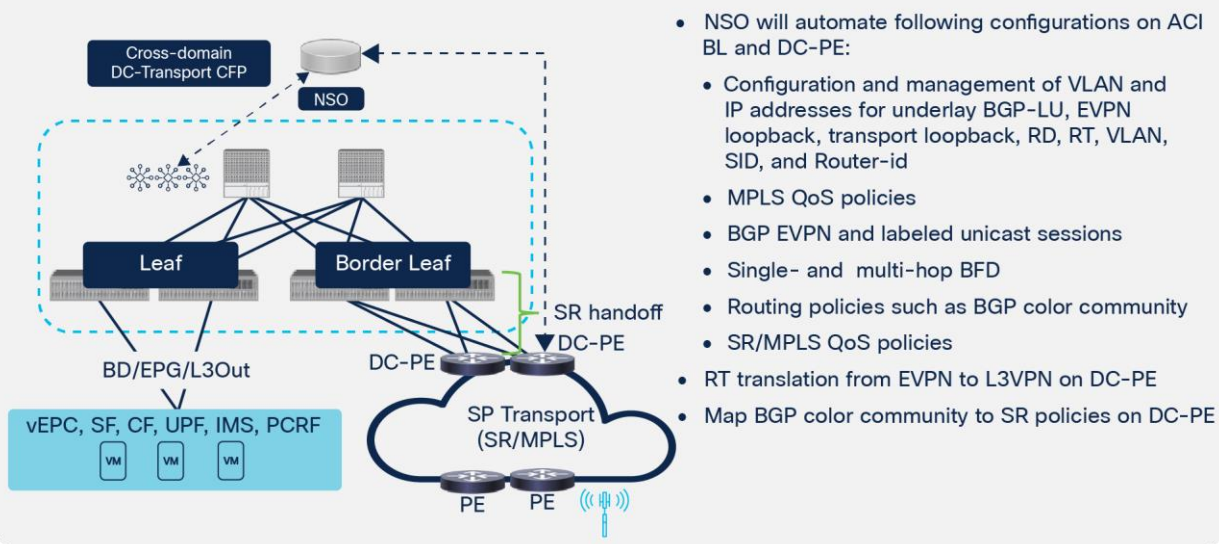- Map BGP color community to SR policies on DC-PE

Figure 8.
Configuring ACI SR-MPLS-type handoff with NSO

3. 5G network slicing in transport by segment-routing ODN. 5G network slicing can be achieved by sending BGP community attributes from ACI that can be used by the segment routing process in transport to trigger ODN tunnels to ensure the resources required for the intended traffic.
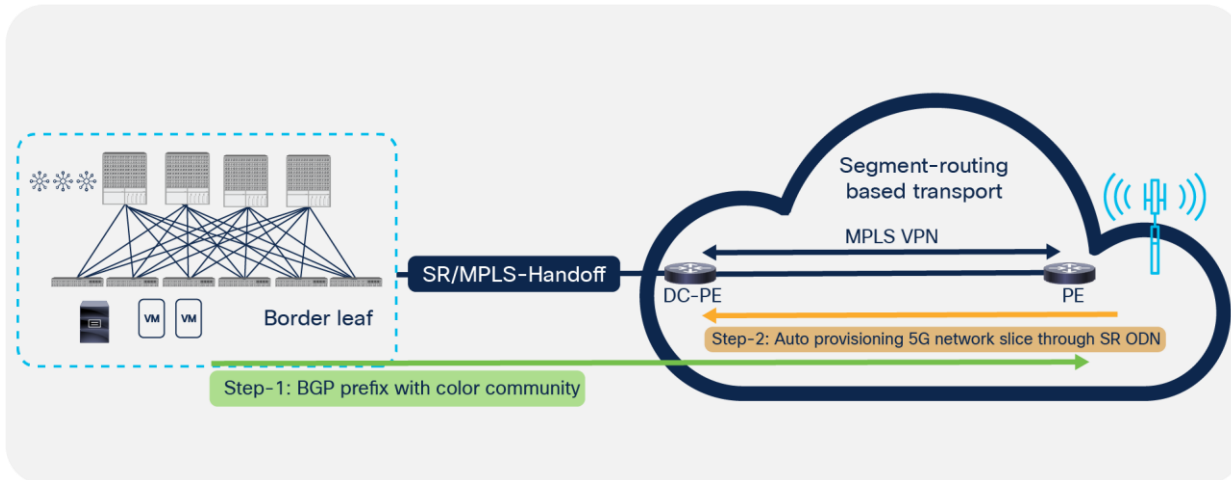

Figure 9.
5G network slicing orchestrated by NSO

Conclusion

NSO CFP not only addresses a very important issue for automation, but it also comes with many salient benefits in operations; for example, a transport engineer does not have to be highly skilled in DC technologies to bring up an application in DC. Overall, NSO CFP can be a very helpful tool to achieve end-to-end automation for service providers.

References

https://www.cisco.com/c/en/us/td/docs/dcn/nso/dc-sdn/cfp/cisco-nso-datacenter-cfp-solution-guide.pdf

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-744107.html

Printed in USA

C11-3157550-00   10/22