
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

SD-WAN+SDA Interworking Task Walkthrough

CCIE Enterprise Infrastructure

Peter Palúch, CCIE #23527, CCIE Enterprise Infrastructure EPM
@Peter_Paluch

BRKCRT-3101

Agenda

- SDA/SD-WAN in the context of CCIE Enterprise Infrastructure exam
- SD-WAN In a Nutshell
- SDA In a Nutshell
- SDA and SD-WAN Interworking Considerations
- Sample Task and Demo
- Concluding Remarks

SDx Technologies in CCIE Ent Infra Exam

- CCIE Enterprise Infrastructure exam blueprint includes two SDN technologies highly relevant for today's enterprise segment
  - Software Defined WAN (SD-WAN)
  - Software Defined Access (SDA)
- The total weight of SDx technologies on the exam score is 25%
- We acknowledge that these technologies are still new to many
  - Current exams in production focus on fundamental functionality
  - As the level of familiarity with these technologies will eventually grow, so will the sophistication level of the SDx exam tasks, too

SD-WAN In A Nutshell

Management plane
vManage

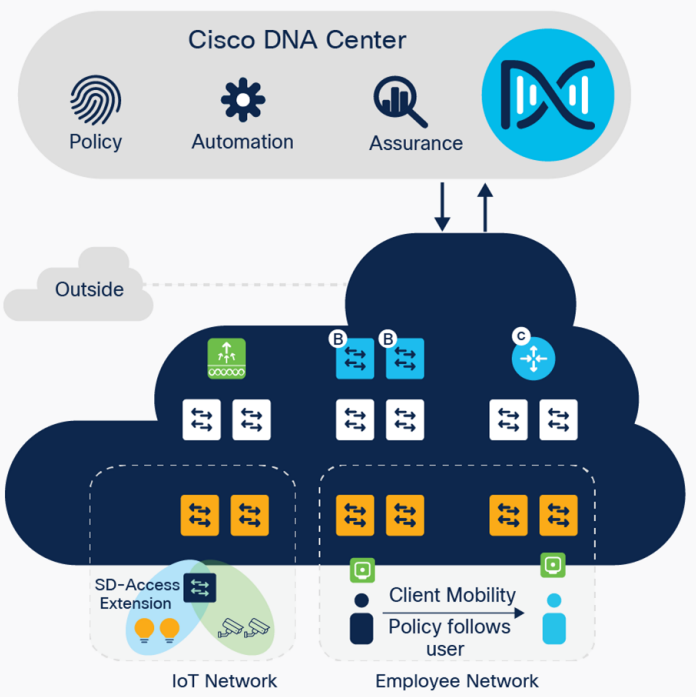
Orchestration plane
vBond

Control plane
vSmart

Data plane
vEdge/cEdge

- SD-WAN is a controller-based WAN solution with centralized management
  - Virtualizes the underlay into multiple user defined VPNs
  - Provides rich toolset for routing and data policies, application aware routing, arbitrary topologies, service chaining and other goodies
  - Uses IPsec and MPLS-derived encapsulation to protect and carry VPN traffic
  - On edge routers, individual VPNs behave effectively as VRFs

SDA In A Nutshell



- SDA is a controller-based solution replacing the traditional access/distribution/core architecture in enterprise networks
  - Virtualizes the underlay into multiple user defined VNs
  - Based on LISP in control plane and VXLAN in data plane to provide VLAN-like services over the routed fabric including client mobility
  - Uses VRFs for macrosegmentation, SGTs for microsegmentation
  - On border nodes, individual VNs behave effectively as VRFs

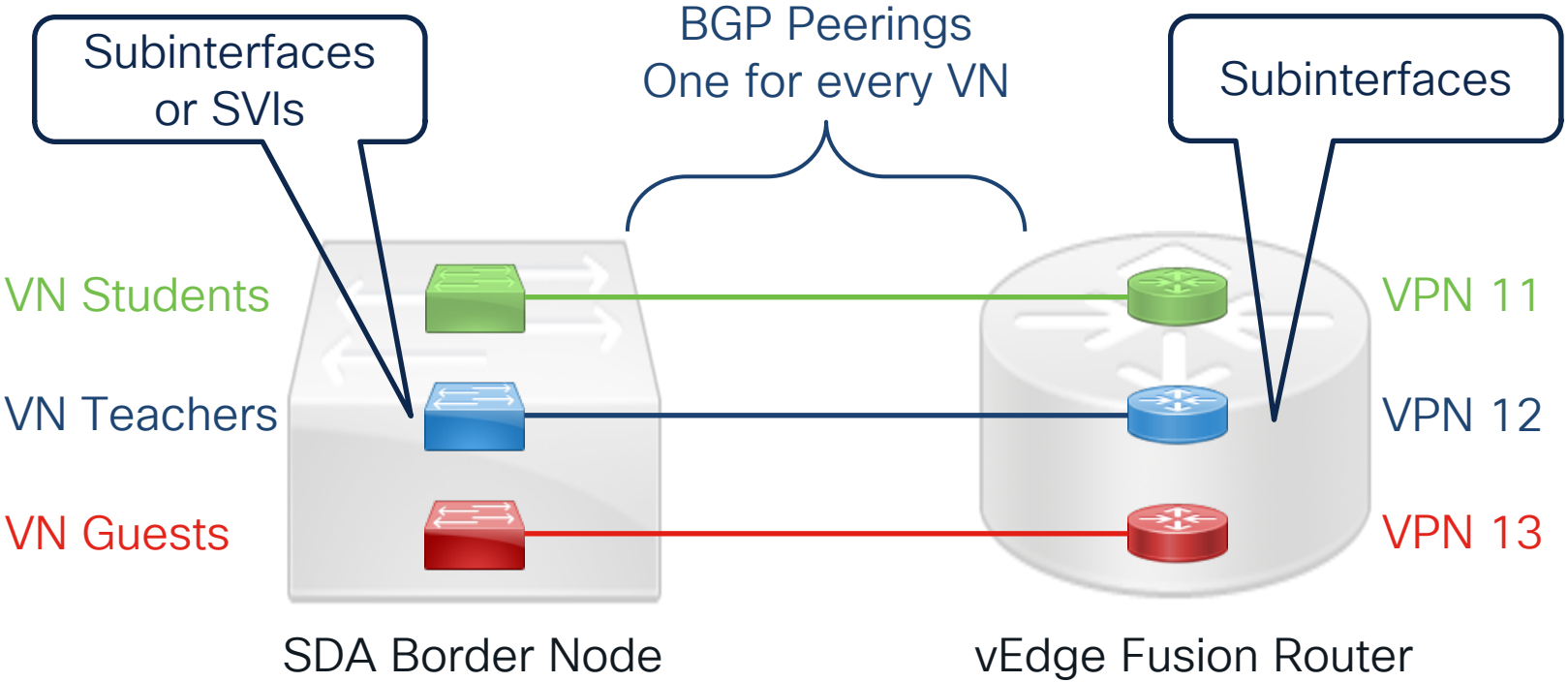
Interworking SDA and SD-WAN (1)

- In networks utilizing SDA and SD-WAN, interworking these technologies involves the cooperation of SDA border nodes and SD-WAN vEdge/cEdge routers
- SDA provides two types of handoff to external networks
  - Layer 3 Handoff: Every VN is terminated at the border node, traffic is decapsulated from VXLAN and is further routed and forwarded natively within the VRF associated with the VN
  - Layer 2 Handoff: The traffic from corresponding VNs is decapsulated from VXLAN at the border node and is further switched and forwarded natively, extending the Layer2 domain of the corresponding VNs
- In this session, we will discuss Layer 3 Handoff only

Interworking SDA and SD-WAN (2)

- Every SD-WAN VPN acts like a VRF on its vEdge termination point
  - cEdges use VRFs directly
- Every SDA VN is a VRF on its termination point
- In principle, L3 interworking between SDA and SD-WAN boils down to interconnecting VRFs on an SDA border node with VPN interfaces on a vEdge (or VRF interfaces on a cEdge)
  - Depending on the design and needs, it may be 1:1 mapping between VNs and VPNs, or multiple VNs can map into a single VPN
  - The vEdge/cEdge router acts as a fusion router
  - Route exchange is accomplished by BGP

Interworking SDA and SD-WAN (3)



Interworking SDA and SD-WAN (4)

- Cisco DNA Center v1.3 supports configuring SDA Border Nodes for Layer 3 Handoff but does not support creating the counterpart configuration on vEdge / cEdge routers
- This results into a rather specific workflow:
  - Configure Layer 3 Handoff in DNA Center for the required VNs
  - Inspect the resulting configuration of each Border Node and take note of
    - Handoff SVIs and their IP addresses for every VN
    - Preconfigured BGP neighbors for every VN
  - Configure vEdges in corresponding VPNs with appropriately matching VLAN IDs, addresses and BGP peerings

Sample CCIE Ent Infra Lab Task

- *Create additional SD-WAN VPNs to carry the SDA VN traffic*
  - *VPN ID 11 for Students VN*
  - *VPN ID 12 for Teachers VN*
  - *VPN ID 13 for Guests VN*
- *On Branch #1 vEdge, for each of these VPNs:*
  - *Create a new subinterface on the interface toward the SDA border switch. Align the VLAN ID and IP address on the subinterface with the configuration generated by DNA Center on the border switches for the appropriate VN.*
  - *Peer the vEdge and the SDA border switch using iBGP. Ensure full reachability between all locations of the same VPN.*

Demo

Concluding Remarks

- To those familiar with RFC 4364 Inter-AS VPN Option A, the SDA/SD-WAN interworking is essentially the same thing
- The SVI numbers, IP addresses and BGP peering addresses on SDA border nodes generated by DNA Center…
  - … depend on the order of actions
  - … may be different every time the configuration procedure is repeated
- By far, the most often used routing protocol on the SDA/SD-WAN boundary is eBGP
  - There are gotchas with multi-homed sites and possible routing loops
  - Remember to propagate the AS_PATH BGP attribute into OMP

Further Reading – SDA

- Cisco SD-Access Solution Design Guide (CVD)
- Software-Defined Access for Distributed Campus Deployment Guide
- Software-Defined Access Medium and Large Site Fabric Provisioning
- Software-Defined Access Macro Segmentation Deployment Guide
- the ascii construct (blog by Aninda Chatterjee)

Further reading – SD-WAN

- Cisco SD-WAN End-to-End Deployment Guide
- Cisco SD-WAN Design Guide
- Cisco Extended Enterprise SD-WAN Design Guide
- SD-WAN docs at Design Zone for Branch, WAN, and Internet Edge

Certification Resources

- Expert Certifications Homepage
- CCIE Enterprise Infrastructure Certification and Training
- CCIE Enterprise Infrastructure Exam Topics
- Enterprise Certifications Community
- Certification Tracking System
- Continuing Education Portal

Continue your education

- Demos in the Cisco campus
- Meet the engineer 1:1 meetings
- Walk-in labs
- Related sessions

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive