A close up of a sign

Description automatically generated

**“TAF”**

**Edge DC Network Build Document**

Table of Contents

[1. Document Control 3](#_Toc89396591)

[1.1 Version Control 4](#_Toc1932042257)

[1.2 References 4](#_Toc1161089182)

[1.3 Index 4](#_Toc125704537)

[1.4 Signoff 6](#_Toc256682515)

[2. Introduction 6](#_Toc409375016)

[2.1 Objectives 7](#_Toc1304700692)

[2.2 In-Scope 7](#_Toc1860540097)

[2.3 Out of Scope 7](#_Toc2131786765)

[3. Network DC Build Details 7](#_Toc979377036)

[3.1 HLD Overview 8](#_Toc1532028202)

[3.2 LLD Overview 8](#_Toc999255032)

[4. Rack Layout and Patch Matrix 8](#_Toc288097483)

[4.1 Rack Layout 9](#_Toc699807503)

[4.2 Patch Matrix or Cable Maps 9](#_Toc829774711)

[5. Device Inventory and IP-VLAN Allocation 9](#_Toc628989749)

[5.1 Fabric devices inventory details 10](#_Toc1834141663)

[5.2 IP and VLAN allocation 10](#_Toc1009946543)

[6. VANCE DC Network Design 11](#_Toc1175172514)

[6.1 Physical Network Diagram 12](#_Toc1159149382)

[6.1.1 Spine and Compute leaf 12](#_Toc2115989488)

[6.1.2 Spine and Service Leafs 13](#_Toc1957295907)

[6.1.3 Spine and Border Leafs 15](#_Toc264483478)

[6.1.4 CMO and FMO Border Leaf 15](#_Toc1692703248)

[6.1.5 CMO and FMO Network Integration (Layer 3) 16](#_Toc1237854474)

[6.1.6 Out Of Band (OOB) Design 17](#_Toc1530549606)

[6.1.7 Cisco VPC Configuration & Best Practices 18](#_Toc1000051988)

[6.2 Logical Network Diagram 19](#_Toc1815658330)

[6.2.1 DC1 Underlay 19](#_Toc1408372547)

[6.2.2 DC1 Overlay 20](#_Toc1811743618)

[6.2.3 DC2 Underlay 21](#_Toc2142018910)

[6.2.4 DC2 Overlay 23](#_Toc2015327355)

[7. NDFC (Nexus Dashboard Fabric Controller) 24](#_Toc1668596482)

[7.1 Overview 25](#_Toc1948964052)

[8. Device Hardening 25](#_Toc980455791)

[8.1 AAA- Authentication, Authorization and Accounting 26](#_Toc1512183521)

[8.1.1 Authentication 26](#_Toc669588075)

[8.1.2 Authorization 26](#_Toc1253741844)

[8.1.3 Accounting 27](#_Toc809290326)

[8.1.4 SSH Parameters 27](#_Toc654576513)

[8.1.5 Line Parameters 27](#_Toc1000807647)

[9. Device Management and Monitoring 28](#_Toc676603232)

[9.1 Network Device Monitoring and Management configuration details per location 29](#_Toc966266341)

[9.2 Monitoring 29](#_Toc844463882)

[9.3 Login Banner 29](#_Toc1979361371)

[9.4 Configuration Backup 30](#_Toc76255977)

[9.5 CMDB Additions 30](#_Toc1048993904)

[9.6 Vendor Account Manager Contacts 30](#_Toc1340565820)

[10. NSX-T Overlay Network Management 30](#_Toc434099644)

# Document Control

## Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 1.2 | Jan 31, 2023 | Ajay Yelduri | Release Version |
| 1.1 | Jan 19, 2023 | Ajay Yelduri | Review Comments updated |
| 1.0 | June 20, 2022 | David Powell | Initial Draft Version |
| 1.3 | April 12, 2023 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## References

This document should be read in conjunction with the following reference documents that have been submitted with the Infosys proposal.

|  |  |
| --- | --- |
| S. No | Document Name |
| 1 | HLD Vance Approved |
| 2 | NAFTA\_EDC-Vance-Network-LLD-v0.6 |
|  |  |
|  |  |
|  |  |

## Index

|  |  |
| --- | --- |
| Term | Explanation / Definition |
| ADC | Application Delivery Controllers |
| ASR | Aggregated Service Router |
| bpps | billion packets per second |
| BGP | Border Gateway Protocol |
| CPU | Central Processing Unit |
| DC | Datacenter |
| DCI | Datacenter Interconnect |
| DNS | Domain Name System |
| DR | Disaster Recovery |
| EPG | Endpoint Groups |
| FPR | Firepower |
| FTD | Firepower Threat Defense |
| FW | Firewall |
| Gbps | Gigabits per second |
| GE | Gigabit Ethernet |
| GRE | Generic Routing Encapsulation |
| GTM | Global Traffic Manager |
| GUI | Graphical User Interface |
| HA | High Availability |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IPSec | Internet Protocol security |
| ISR | Integrated Service Router |
| LAN | Local Area Network |
| LTM | Local Traffic Manager |
| Mbps | Megabits per second |
| MPLS | Multi-Protocol Label Switching |
| NTP | Network Time Protocol |
| OOB | Out of Band Management |
| OSPF | Open Shortest Path First |
| OTV | Overlay Transport Virtualization |
| QSFP | Quad Small Form-Factor Pluggable |
| RBAC | Role Based Access Controls |
| Term | **Explanation / Definition** |
| RU | Rack Unit |
| SAN | Storage Area Network |
| SDWAN | Software Defined Wide Area Network |
| SFP | Small Form-Factor Pluggable |
| DAIMLER | Siemens Gamesa Renewable Energy |
| SIEM | Security Information and Event Management |
| SNAT | Source Network Address Translation |
| SNMP | Simple Network Management Protocol |
| SSL | Secure Socket Layer |
| Tbps | Terabits per second |
| TSL | Transport Layer Security |
| URL | Uniform Resource Locator |
| vCMP | Virtual Cluster Multiprocessing |
| vPC | Virtual Port-Channel |
| VIP | Virtual IP |
| VLAN | Virtual Local Area Network |
| VM | Virtual Machine |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| ZPA | Zscaler Private access |
| bpps | billion packets per second |
| mpps | million packets per second |
| MMF | Multi-Mode fiber |
| SMF | Single-Mode fiber |

## Signoff

|  |  |  |
| --- | --- | --- |
| **Name** | **Position** | **Date** |
| 1.0 |  |  |
|  |  |  |
|  |  |  |

# Introduction

## Objectives

The purpose of this document is to outline the comprehensive design and analysis of MBUSI’s business and technical goals, including a logical and physical component of the network. This document will also help measure the success of the implementation and evolving the network design as new application requirements arise.

## In-Scope

The following items will be considered “In-scope for this document: Rack Layout, Inventory, Physical and Logical design, IP Plan Details and NDFC Management Details.

## Out of Scope

* Any design and configuration details of the existing infrastructure components.
* Any industry or regulatory compliance related activities / audits.
* Any devices not in LLD or HLD.
* Service Level Management of MBUSI 3rd Parties (or) Vendors.

# Network DC Build Details

## Overview of High-level Design

The purpose of the document is to provide a reference architecture standards, guidelines, and deployment patterns to be followed for implementation of Enterprise private Cloud Platform as part of Edge Datacenters for Future Mode of Operations (FMO) model under Daimler’s TAF program.

Please refer to the network section of the HLD



## Overview of Low-level Design

The objective of this document is to provide a Low-Level Design (LLD), which is based on information gathered during information gathering phase/workshops and High-Level design (HLD) for the target state FMO Edge DCs



# Rack Layout and Patch Matrix

## Data Center Hosting

Vance Edge infrastructure consists of two separate datacenter rooms separated by approximately 700m distance, each in a different building. DC rooms are considered as primary F3G and secondary (standby), marked C8.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| US | Tuscaloosa | VANCE | Plant ID - 138  Physical ID - USA0144 | DC1 [DC138001] | DC2 [DC138002] | VA1 & VA2 |

## Rack Layout

The rack elevation details of VANCE DC1 & DC2 FMO network devices are available under the sheet “RACKS\_LAYOUT\_DC1“and “RACKS\_LAYOUT\_DC2“of the workbooks

## Patch Matrix or Cable Maps

The Patch Matrix or Cable Maps of VANCE FMO network devices are available on the respective sheets of the workbook at

# Device Inventory and IP-VLAN Allocation

## Fabric devices inventory details

Below information provides the inventory of the fabric devices of FMO VANCE DC1 & 2

**FMO VANCE DC1:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | DC1 Hostname | Purpose | IP | Serial Number |
| N9K-C9332C | SPN-MAIN-VA1-001 | Spine leaf 01 | 10.34.80.4 | FLM253302LA |
| N9K-C9332C | SPN-MAIN-VA1-002 | Spine leaf 02 | 10.34.80.5 | FLM253302J5 |
| N9K-C93180YC-FX3 | SWS-MAIN-VA1-003 | Service & BGW leaf 01 | 10.34.80.12 | FD0260905YP |
| N9K-C93180YC-FX3 | SWS-MAIN-VA1-004 | Service &  BGW leaf 02 | 10.34.80.13 | FD0260905YW |
| N9K-C93180YC-FX3 | SWB-MAIN-VA1-001 | Border leaf 01 | 10.34.80.6 | FDO260225EL |
| N9K-C93180YC-FX3 | SWB-MAIN-VA1-002 | Border leaf 02 | 10.34.80.7 | FDO26030HUS |
| N9K-C93240YC-FX2 | SWA-MAIN-VA1-001 | Compute leaf 01 | 10.34.80.10 | FDO26020EYY |
| N9K-C93240YC-FX2 | SWA-MAIN-VA1-002 | Compute leaf 02 | 10.34.80.11 | FDO26020EY3 |
| C9300-48T | SWC-ADM--VAN1-001 | OOB Switch 01 | 10.34.80.1 | FJC26121AAN  FJC2615129E |

**FMO VANCE DC2:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | DC2 Hostname | Purpose | IP | Serial Number |
| N9K-C9332C | SPN-MAIN-VA2-001 | Spine leaf 01 | 10.34.84.4 | FLM253302HF |
| N9K-C9332C | SPN-MAIN-VA2-002 | Spine leaf 02 | 10.34.84.5 | FLM253303TQ |
| N9K-C93180YC-FX3 | SWS-MAIN-VA2-003 | Service & BGW leaf 01 | 10.34.84.12 | FD02609062C |
| N9K-C93180YC-FX3 | SWS-MAIN-VA2-004 | Service & BGW leaf 02 | 10.34.84.13 | FD0260905Z7 |
| N9K-C93180YC-FX3 | SWB-MAIN-VA2-001 | Border leaf 01 | 10.34.84.6 | FDO260225EQ |
| N9K-C93180YC-FX3 | SWB-MAIN-VA2-002 | Border leaf 02 | 10.34.84.7 | FDO2602252G |
| N9K-C93240YC-FX2 | SWA-MAIN-VA2-001 | Compute leaf 01 | 10.34.84.10 | FDO26020EYT |
| N9K-C93240YC-FX2 | SWA-MAIN-VA2-002 | Compute leaf 02 | 10.34.84.11 | FDO26020EKA |
| C9300-48T | SWC-ADM--VAN2-001 | OOB Switch 01 | 10.34.84.1 | FJC261512KK  FJC261512H4 |

## IP and VLAN allocation

The IP Plan outlines the details of IP Blocks, VLANs allocated of the entire Network Infrastructure. Network infrastructure includes the VxLAN Fabric (Spine and Leaf Architecture), an out of band Admin Fabric, Security devices, Compute, Storage & backups. Below is a link to the reference document showing all the specified details at



Below is the short summary of the same

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Allocated IP Block | | | | | |
| Network Address | **Subnet Mask** | **Host Address Range** | **Number of hosts** | **Broadcast Address** | **Purpose** |
|  |  |  |  |  |  |
| 10.34.64.0/20 | 255.255.240.0 | 10.34.64.1 - 10.34.79.254 | 4096 | 10.34.79.255 | Private Pool for DC Infra Routable Ips |
| 10.34.80.0/21 | 255.255.240.0 | 10.34.80.1 - 10.34.87.254 | 2048 | 10.34.87.255 | Private Pool for DC OOB MGMT Routable Ips |
| 192.168.0.0/20 | 255.255.240.0 | 192.168.0.1 - 192.168.15.254 | 4096 | 192.168.15.255 | Private Non-Routable IP Pool |
|  |  |  |  |  |  |
| L3 VNI BLOCK FOR VAN - 10000 - 29999  L2 VNI BLOCK FOR VAN - 30000 - 39999 | | | | **Overlay Network VLAN Range (L2VNI) - 1000 to 2999** | |
| **VRF VLAN Range (L3VNI) - 3000 to 3499** | |
| **Network/Security Mgmt. - 3500 to 3599** | |
| **Compute/Storage Mgmt. iLO - 3600 to 3699** | |
| **Transit Networks - 3700 to 3799** | |
| **Other Requirements (Migration, CMO<->FMO) - 700 to 849** | |

# VANCE DC Network Design

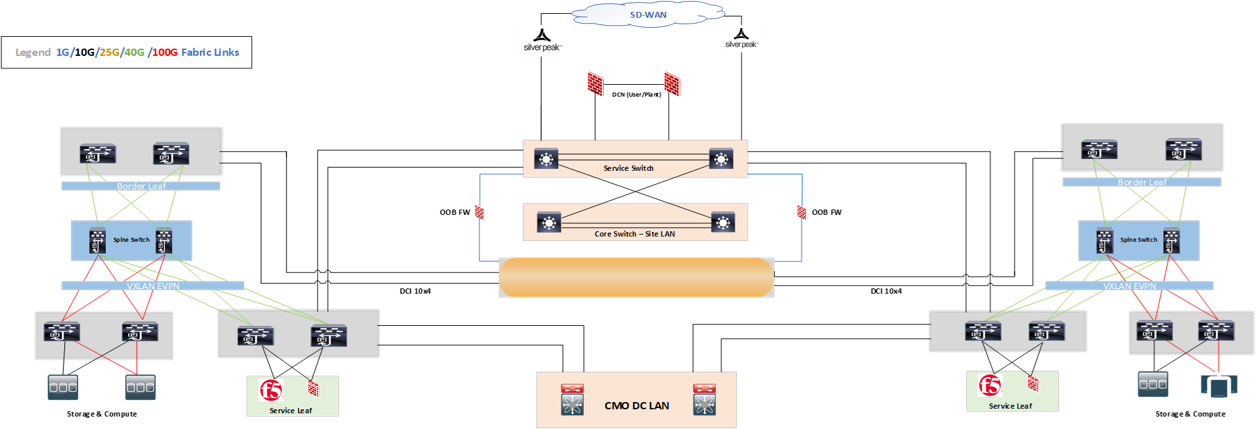
## Physical Network Diagram

This diagram describes how the physical connectivity between the network devices within DC and between the DC’s

The DC Network in an EDC includes the EVPN VXLAN fabric, Internal & External firewall’s, out of band network fabric. The VXLAN Fabric (Spine and Leaf Architecture) constructs the switching and routing infrastructure providing connectivity and integration of services to private cloud and other components hosted inside the DC. Internal or Infra PoD firewalls integrated with the VXLAN fabric provides security to the management components of individual stacks such as SDI and OpenStack. The Workloads hosted on the SDI stack are protected by NSX Distributed firewalls. The External or Internet Firewalls restricts the inbound and outbound access of the Internet. The Business partner firewalls secures the partner’s connection to applications or servers hosted in the DC.

Vance DC is planned to deploy an environment that support automation, orchestration, security, and management. This new deployment is planned to be installed in a “greenfield” approach with the new infrastructure being stood up under this design and connected to the existing environment. Some compute workloads will be selected and moved to the new environment. The interconnectivity required for this movement has already been established. Any new required features will be tested and stabilized. Post stabilization workload migration will be performed.

The new design will be comprised of Spine-Leaf data center physical underlay design with a VxLAN overlay providing L2/L3 DC connectivity. Cisco hardware to provide the physical underlay and use NSX-T in the VCF environment to provide SDN capabilities into the virtual hosts and guests. This will deliver segmentation and firewall capability within the hosting environment.



The below sections highlight the physical connections between Spine and each category of leaf.

### Spine and Compute leaf

Each Compute leaf switch will connect to both Spine Switches with redundant 100G links.

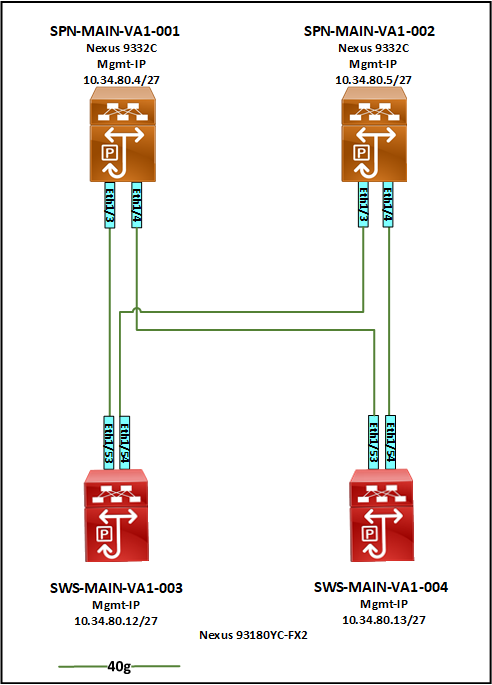


|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Source Device** | | | | **Destination Device** | | | |
| **Source Device name** | **Port** | **SFP Optics** | **Connector** | **Destination Device name** | **Port** | **SFP Optics** | **Connector** |
| SPN-MAIN-VAN1-001 | 1 | QSFP-100-SRBD | MM-LC | SWA-MAIN-VA1-001 | 59 | QSFP-100-SRBD | MM-LC |
| SPN-MAIN-VAN1-001 | 2 | QSFP-100-SRBD | MM-LC | SWA-MAIN-VA1-002 | 59 | QSFP-100-SRBD | MM-LC |
| SPN-MAIN-VAN1-002 | 1 | QSFP-100-SRBD | MM-LC | SWA-MAIN-VA1-001 | 60 | QSFP-100-SRBD | MM-LC |
| SPN-MAIN-VAN1-002 | 2 | QSFP-100-SRBD | MM-LC | SWA-MAIN-VA1-002 | 60 | QSFP-100-SRBD | MM-LC |

**Figure 12 Spine and Compute Leaf**

### Spine and Service Leafs

Each Service leaf switch will connect to both Spine Switches with redundant 40G links.



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Source Device** | | | | **Destination Device** | | | |
| **Source Device name** | **Port** | **SFP Optics** | **Connector** | **Destination Device name** | **Port** | **SFP Optics** | **Connector** |
| SPN-MAIN-VAN1-003 | 3 | QSFP-40-SR-BD | MM-LC | SWS-MAIN-VA1-001 | 53 | QSFP-40-SR-BD | MM-LC |
| SPN-MAIN-VAN1-003 | 4 | QSFP-40-SR-BD | MM-LC | SWS-MAIN-VA1-002 | 53 | QSFP-40-SR-BD | MM-LC |
| SPN-MAIN-VAN1-004 | 3 | QSFP-40-SR-BD | MM-LC | SWS-MAIN-VA1-001 | 54 | QSFP-40-SR-BD | MM-LC |
| SPN-MAIN-VAN1-004 | 4 | QSFP-40-SR-BD | MM-LC | SWS-MAIN-VA1-002 | 54 | QSFP-40-SR-BD | MM-LC |

**Figure 15: Spine and Service Service Leaf**

### Spine and Border Leafs



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Source Device** | | | | **Destination Device** | | | |
| **Source Device name** | **Port** | **SFP Optics** | **Connector** | **Destination Device name** | **Port** | **SFP Optics** | **Connector** |
| SPN-MAIN-VAN1-001 | 31 | QSFP-40-SR-BD | MM-LC | SWB-MAIN-VA1-001 | 53 | QSFP-40-SR-BD | MM-LC |
| SPN-MAIN-VAN1-001 | 32 | QSFP-40-SR-BD | MM-LC | SWB-MAIN-VA1-002 | 54 | QSFP-40-SR-BD | MM-LC |
| SPN-MAIN-VAN1-002 | 31 | QSFP-40-SR-BD | MM-LC | SWB-MAIN-VA1-001 | 53 | QSFP-40-SR-BD | MM-LC |
| SPN-MAIN-VAN1-002 | 32 | QSFP-40-SR-BD | MM-LC | SWB-MAIN-VA1-002 | 54 | QSFP-40-SR-BD | MM-LC |

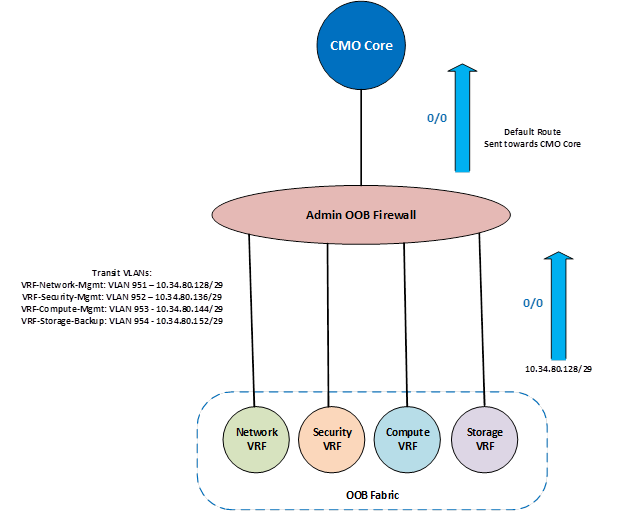
### CMO and FMO Network Integration (Layer 3)

Each CMO border switch will connect to FMO Service leaf switches using redundant 10G links. These links will be configured as Layer 3 links and used for routing the traffic towards CMO environment & other external connectivity depending on CMO

### Out Of Band (OOB) Design

To support the isolation/segmentation between each network segments Network, Storage, Compute & Security Managements, we have created the VRFs corresponding to each network on OOB Switches and pointed their default gateway to the OOB security firewall where the actual inter-vrf routing will take place along with the firewall rules in-place to provide the segmentation. Identical setup is made in VA1 & VA2. Below is the VLAN/IP information pertaining to the OOB setup along with logical network diagram of the same.

* The infrastructure devices require a back-door entry into the network during datacenter outages or disaster recovery
* Out of band network in EL will have dedicated network switches of Cisco C9300-48T-A deployed
* All the network and security devices will have connectivity to the out of band switches and firewalls either through the management interface or a dedicated VRF assigned for the out of band connectivity.
* The admin firewalls have a connection to both EL1 and EL2 admin leaf’s.
* The OOB fabric is connected to the WAN Edge.
* The Border Leaf’s, Services Leaf’s, Main Spines, Access leaf’s, Internet Leaf’s, DMZ leaf’s, F5 Load Balancers, infra firewalls, BPC firewalls, Internet firewalls and DCN firewall are connected to the OOB Core switches on from the management port.



## Logical Network Diagram

### DC1 Underlay

The main function of the underlay network in the VXLAN EVPN fabric is to ensure the reachability of VTEPs (Virtual Tunnel End Points) and BGP peering addresses. IS-IS is the chosen underlay protocol is chosen for fast convergence in the event of node failures.

IS-IS, similar to OSPF is an IGP routing protocol which is configured to establish communication between Spine and Leaf switches. This protocol uses CLNS (Connectionless Network Service) and is independent of IP which is well suited for routed interfaces or ports. IS-IS has faster reconvergence and calculates SPF only in case of topology change (not link change). The IS-IS protocol attributes/parameters for the underlay network are as below.



**IS-IS Autonomous System - UNDERLAY**

**Area ID - 49.(AFI).0001**

**IS-TYPE - L2**

**NET Format**

[](https://www.cisco.com/c/dam/en/us/td/i/100001-200000/120001-130000/127001-128000/127420.ps/_jcr_content/renditions/127420.jpg)

|  |  |  |  |
| --- | --- | --- | --- |
| ISIS Net | | Device | |
| 49.0001.1720.3000.0001.00 | | SPN-MAIN-VA1-001 | |
| 49.0001.1720.3000.0002.00 | | SPN-MAIN-VA1-002 | |
| 49.0001.1720.3000.0003.00 | | SWA-MAIN-VA1-001 | |
| 49.0001.1720.3000.0004.00 | | SWA-MAIN-VA1-002 | |
| 49.0001.1720.3000.0005.00 | | SWB-MAIN-VA1-001 | |
| 49.0001.1720.3000.0006.00 | | SWB-MAIN-VA1-002 | |
| 49.0001.1720.3000.0009.00 | | SWS-MAIN-VA1-003 | |
| 49.0001.1720.3000.0010.00 | | SWS-MAIN-VA1-004 | |
| **Level Type** | **System ID** | | **Device** | |
| 2 | 0001.1720.3000 01 | | SPN-MAIN-VA1-001 | |
| 2 | 0001.1720.3000 02 | | SPN-MAIN-VA1-002 | |
| 2 | 0001.1720.3000 03 | | SWA-MAIN-VA1-001 | |
| 2 | 0001.1720.3000 04 | | SWA-MAIN-VA1-002 | |
| 2 | 0001.1720.3000 05 | | SWB-MAIN-VA1-001 | |
| 2 | 0001.1720.3000 06 | | SWB-MAIN-VA1-002 | |
| 2 | 0001.1720.3000 09 | | SWS-MAIN-VA1-003 | |
| 2 | 0001.1720.3000 10 | | SWS-MAIN-VA1-004 | |

### DC1 Overlay

The overlay for the MBUS switching fabric is VXLAN and BGP and it uses EVPN as the address family/control plane for communicating end host MAC and IP Addresses.

An overlay is a dynamic tunnel which transports frames between two endpoints. Here endpoint (VTEP) refers to a ToR Switch or known as a leaf switch. The VTEP functionality is enabled on all the leaf switches in the VXLAN EVPN Fabric and on border leaf switches. VXLAN is an overlay technology which performs a MAC in IP/UDP encapsulation which allows layer 2 segments to be stretched over an IP network. The encapsulation and decapsulation of VXLAN headers are handled by VTEPs. VXLAN has all the benefits of layer 3 topologies including Layer-3 ECMP which efficiently spreads traffic across multiple available paths.

The below diagram represents the Overlay Network of the MBUSI Datacenter.





### DC2 Underlay

The main function of the underlay network in the VXLAN EVPN fabric is to ensure the reachability of VTEPs (Virtual Tunnel End Points) and BGP peering addresses. IS-IS is the chosen underlay protocol is chosen for fast convergence in the event of node failures.

IS-IS, like OSPF is an IGP routing protocol which is configured to establish communication between Spine and Leaf switches. This protocol uses CLNS (Connectionless Network Service) and is independent of IP which is well suited for routed interfaces or ports. IS-IS has faster reconvergence and calculates SPF only in case of topology change (not link change). The IS-IS protocol attributes/parameters for the underlay network are as below.

**IS-IS Autonomous System - UNDERLAY**

**Area ID - 49.(AFI).0001**

**IS-TYPE - L2**

**NET Format**

[](https://www.cisco.com/c/dam/en/us/td/i/100001-200000/120001-130000/127001-128000/127420.ps/_jcr_content/renditions/127420.jpg)

|  |  |  |  |
| --- | --- | --- | --- |
| ISIS Net | | Device | |
| 49.0001.1720.3100.0001.00 | | SPN-MAIN-VA2-001 | |
| 49.0001.1720.3100.0002.00 | | SPN-MAIN-VA2-002 | |
| 49.0001.1720.3100.0003.00 | | SWA-MAIN-VA2-001 | |
| 49.0001.1720.3100.0004.00 | | SWA-MAIN-VA2-002 | |
| 49.0001.1720.3100.0005.00 | | SWB-MAIN-VA2-001 | |
| 49.0001.1720.3100.0006.00 | | SWB-MAIN-VA2-002 | |
| 49.0001.1720.3100.0009.00 | | SWS-MAIN-VA2-003 | |
| 49.0001.1720.3100.0010.00 | | SWS-MAIN-VA2-004 | |
| **Level Type** | **System ID** | | **Device** | |
| 2 | 0001.1720.3100 01 | | SPN-MAIN-VA2-001 | |
| 2 | 0001.1720.3100 02 | | SPN-MAIN-VA2-002 | |
| 2 | 0001.1720.3100 03 | | SWA-MAIN-VA2-001 | |
| 2 | 0001.1720.3100 04 | | SWA-MAIN-VA2-002 | |
| 2 | 0001.1720.3100 05 | | SWB-MAIN-VA2-001 | |
| 2 | 0001.1720.3100 06 | | SWB-MAIN-VA2-002 | |
| 2 | 0001.1720.3100 09 | | SWS-MAIN-VA2-003 | |
| 2 | 0001.1720.3100 10 | | SWS-MAIN-VA2-004 | |



### DC2 Overlay

The overlay for the MBUSI switching fabric is VXLAN and BGP and it uses EVPN as the address family/control plane for communicating end host MAC and IP Addresses.

An overlay is a dynamic tunnel which transport frames between two endpoints. Here endpoint (VTEP) refers to a ToR Switch or known as a leaf switch. The VTEP functionality is enabled on all the leaf switches in the VXLAN EVPN Fabric and on border leaf switches. VXLAN is an overlay technology which performs a MAC in IP/UDP encapsulation which allows layer 2 segments to be stretched over an IP network. The encapsulation and decapsulation of VXLAN headers are handled by VTEPs. VXLAN has all the benefits of layer 3 topologies including Layer-3 ECMP which efficiently spreads traffic across multiple available paths.

The below diagram represents the Overlay Network of the MBUSI Datacenter.





# NDFC (Nexus Dashboard Fabric Controller)

## Overview

It provides end-to-end automation for data centers that are distributed in multiple locations and either on-premises or in a public cloud, reducing the complexities.

The Management IP address <https://10.46.37.69/appcenter/cisco/ndfc/ui/dashboard>

Cluster Name S138NLNEX00A

The detailed walkthrough of the NDFC device is available at



# Device Hardening

Local AAA Solution as per Edge DCs will be used as authentication server for all DC network devices and firewalls. Radius protocol will be used for authenticating all administrative users.

|  |  |
| --- | --- |
| **Configuration Parameter** | **Preference** |
| Server Name |  |
| Secret Radius Key | <secret key> |
| Server name | ppp |
| Protocol | ip |
| Role | Read Only |

## AAA- Authentication, Authorization and Accounting

Cisco ISE is being used as the AAA server supporting the TACACS protocol. Cisco ISE will intern integrate with AD servers for the central user-database. The local password store will be used for authentication when the AAA Server is unavailable.

Below are the AD Groups/Service accounts being leveraged for the day-to-day operations and/or full life cycle management of any network devices in Vance1 & 2.

"DTPD\_DC\_EDC-NWT-RW" AD group for Vance Build Engineers to manage the devices

“DTPD\_DC\_EDGE-NDFC-RW" Service account for management of the devices through NDFC

“DTPD\_DC\_s\_MONNWTRW” AD account for the Backup of network devices using the SolarWinds

### Authentication

The authentication configurations and locations where the list is applicable are as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Facility** | **List Name** | **Description** | **Group Order** | **Applied** |
| Login | default | Default Login Authentication List | FDC-Tacacs, Local | <default list> |
| Login | Vty method | Login Method for VTY Lines | FDC-Tacacs, Local | VTY Lines 0 to 15 |
| Login | Con method | Login Method for Console Ports | FDC-Tacacs, Local | VTY Lines 0 to 15 |

### Authorization

The authorization configurations and locations where the list is applicable are as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Facility** | **List Name** | **Description** | **Group Order** | **Applied** |
| Exec | Default | Default Exec Shell Authorisation | AAA Server,  Local DB | <default list> |
| Commands 0 | Default | Command Authorisation for Level 15 | AAA Server,  , Local DB,  If-Authenticated | <default list> |
| Commands 1 | Default | Command Authorisation for Level 15 | AAA Server,  , Local DB,  If-Authenticated | <default list> |
| Commands 15 | Default | Command Authorisation for Level 15 | AAA Server,  , Local DB,  If-Authenticated | <default list> |

In addition to the above AAA Authorization lists, Console Authorization is enabled where available.

### Accounting

The accounting configurations and locations where the list is applicable are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Facility** | **Description** | **Mode** | **Group Order** |
| Exec | Exec shell accounting | Start-stop | AAA Server |
| Level 0 Commands | All standard level commands | Stop Only | AAA Server |
| Level 15 Commands | All Exec level commands | Stop Only | AAA Server |

Devices permit many methods of administrative access.

The available administrative access methods are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Method** | **Description** | **Enabled** | **Permitted Hosts** |
| Console | Basic out of band access | Y | N/A |
| SSH Version 2 | Encrypted in band administrative access, Secure Shell Version 2 | Y | XX.XX.XX.XX/24 |
| XX.XX.XX.XX/24 |

### SSH Parameters

The configuration parameters used for the SSH service is as follows

|  |  |  |  |
| --- | --- | --- | --- |
| **RSA Keypair** | Default | **Modulus Size** | Default |
| **Versions Enabled** | 2 | **Authentication Retries** | 3 |
| **Timeout** | 10 Seconds |  |  |

### Line Parameters

The configuration for administrative management lines present on devices is as follows:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Line** | **Authentication Group** | **Authorisation Group** | **Synchronous Logging** | **Timeout** | **Administrative Protocols** | |
| **In** | **Out** |
| Console | Default | Default | Yes | 15 Minutes | N/A | None |
| VTY 0 to 15 | Default | Default | Yes | 15 Minutes | SSH | None |

# Device Management and Monitoring

## Network Device Monitoring and Management configuration details per location

|  |  |  |
| --- | --- | --- |
| Function | Local v/s Remote | Data Center  Vance |
| SNMP | Solarwinds | 53.219.64.134 & .153 (Master Polling Engines) - More Pollers mentioned below |
| SNMP TRAP | Solarwinds | 53.219.64.134 & .153 (Master Polling Engines) - More Pollers mentioned below |
| SYSLOG |  |  |
| NTP | Remote | 53.35.131.20 & 53.35.134.20 |
| AAA | Cisco ISE - Remote | 10.46.34.197 & 10.46.34.199 |

## Monitoring

SolarWinds is used as NMS for Vance DC1 and DC2 in NDC1 Data Center for querying the networks devices using the SNMPv3 protocol by using the module called NPM (Network Performance Monitor). SolarWinds management plane is available at <https://ndc-solarwinds.app.corpintra.net/>

ServiceNow is used as CMDB to query the network devices using SNMPv3 protocol in Vance1 & 2 data centers. Below is a short summary of protocols, version, usernames and more that are being leveraged.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NMS | SNMP Version | UserName | Auth Protocol | Privacy Protocol |
| ServiceNow | V3 | americas-servicenow-ro | SHA1 | AES128 |
| Solarwinds | V3 | americas-solarwinds-ro | SHA1 | AES128 |

## Login Banner

The following message will be displayed to users prior to obtaining any form of access to the system via SSH:

*\*\*\*W A R N I N G\*\*\**

*THIS IS A PRIVATE COMPUTER SYSTEM.*

*This computer system including all related equipment, network devices,*

*are provided only for authorized use.*

*All computer systems may be monitored for all lawful purposes, including*

*those activities that are authorized for management of the system.*

*All information including personal information, stored or sent over this*

*system may be monitored.*

*Uses of this system, authorized or unauthorized, constitutes consent to*

*monitoring of this system.*

*Unauthorized use may subject you to criminal prosecution.*

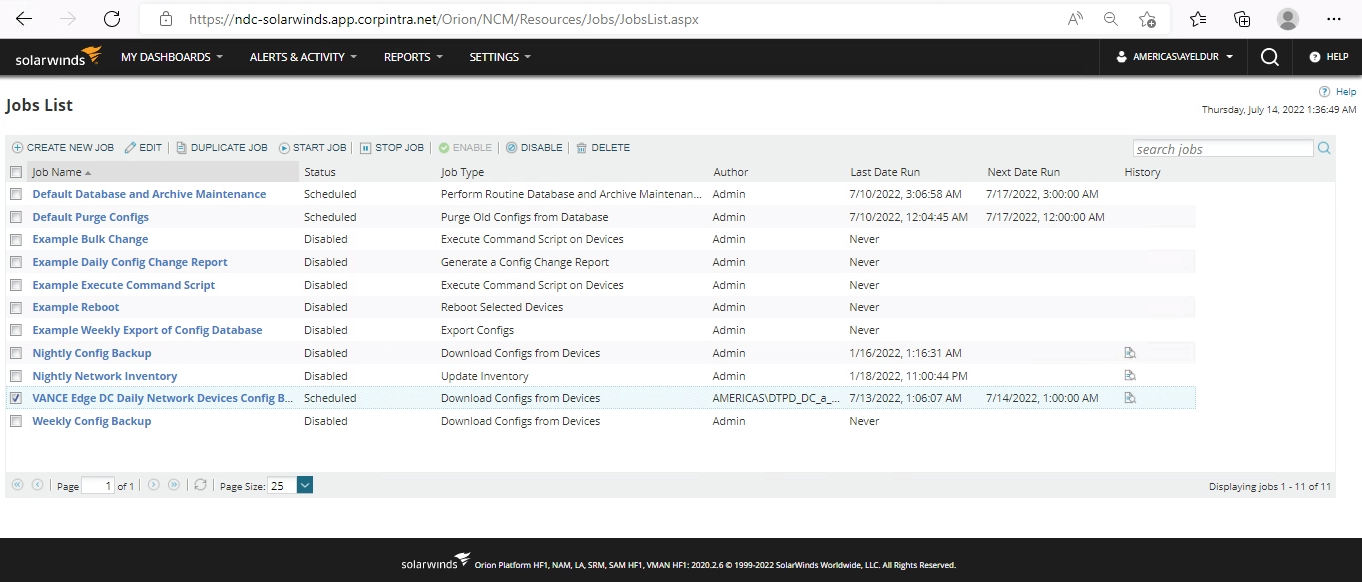
*WARNING: Unauthorized access to this system is forbidden and will be*

*prosecuted by law.*

*By accessing this system, you agree that your actions may be monitored.*

## Configuration Backup

Daily network configuration backups for Network devices will be done through NDFC as well as through Network Configuration Manager (NCM) feature of the SolarWinds under the Jobs section of My Dashboards -> Network Configuration as shown below.



Configuration Backup details:

**Schedule –** Backups happen every day at 1:00 AM EST

**Location of the files** - <Installdir>\SolarWinds\NCM\Config-Archive on the Solarwinds polling engines

**Purging** – Weekly on Sunday at 1:00 AM EST

## CMDB Additions

ServiceNow is being leveraged for the Configuration Management Database. You can find the respective information at <https://everest.service-now.com/sp/?id=kb_article_view&sys_kb_id=1b3e663987245d54e70832a80cbb359a>

## Vendor Account Manager Contacts

**Cisco System, Inc.**

**Tommy Cooksey**

**Global Account Manager**

**301 752 2646**

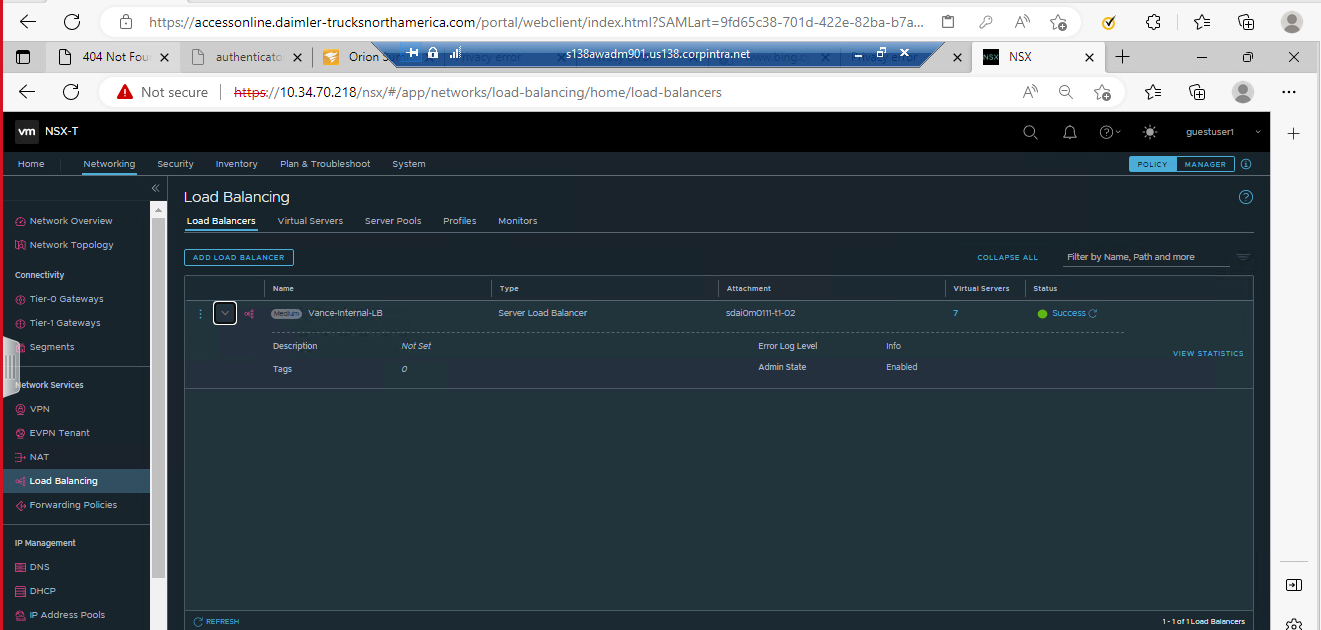
# NSX-T Overlay Network Management

The Compute overlay network is managed by NSX-T SDN solution, which provides the tenant creations, Distributed firewall and more. NSX-T Overlay is integrated with network using Tier-0 router with BGP routing to import/export the network routes.

We only manage network segment creation & some load balancing configurations as part of day-to-day work. Sample network segment & LB component creation is shown in the screenshot below.

The Management IP address <https://10.34.70.218/login.jsp?idp=local>

accessonline.daimler-trucksnorthamerica.com/portal/webclient/index.html?SAMLart=OObOb9bb-1c5e-4101-b7c5-e228b1778d28#/desktop 
links 
IP calc 
Office Microsoft SARF Word 
access 
SolarWinds Orion X 
SolarWinds Orion X 
Not secure 
NSX-T 
Home 
Networking 
Security 
Inventory 
Plan & Troubleshoot 
System 
Excel Microsoft 365 My OneNote 
VMware Horizon 
sl 38awadm901. usl corpintra.net 
Metadata Proxies 
Segments 
Segments 
Segment Profiles 
ADO SEGMENT 
Segn 
guestuserl 
Filte' by Name. Peth end more 
O 
@ Network Overview 
Network 
Tier-O Gateways 
Tier-I Gateways 
Segmen ts 
Q VPN 
EVPN Tenant 
NAT 
Forwarding Policies 
DNS 
Edge Bridge Profiles 
sdaomom-t1-011 Tierl 
Segment needs to have either Subnets or 'v'?N defined. or both. 
Adm State 
L2 VPN this go to 
VPN Note tut L2 to mrk. 
EXPAND ALL 
S ubnets 
Gateway CDR 
CDR e.g. 
SET DHCP CONFIG 
0) 
VPN ID 
e 
[3 
1 - 9 of 9 
3:46 PM 
12/6/2022 



# Bill of Material:

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Category** | **Device Type** | **DC1** | **DC2** |
| Spine | N9K-C9332C | 2 | 2 |
| Access | N9K-C93240YC-FX2 | 2 | 2 |
| Service | N9K-C93180YC-FX3 | 2 | 2 |
| OOB | C9300-48T-A | 1 | 1 |
| Border Leaf | N9K-C93180YC-FX3 | 2 | 2 |