# Table of Contents

Lab Overview - HOL-1940-01-NET - Getting Started with VeloCloud by VMware.......2  
Lab Guidance .................................................................................................................. 3  
Module 1 - Overview of SD-WAN (15 minutes).............................................................. 9  
  Introduction......................................................................................................................... 10  
  Overview of SD-WAN........................................................................................................ 11  
  Conclusion......................................................................................................................... 17  
Module 2 - Key Components and Architecture (15 minutes)...................................... 18  
  Introduction to NSX-SD WAN by VeloCloud............................................................... 19  
  VMware NSX SD-WAN by VeloCloud Key components and Architecture............... 20  
  Conclusion......................................................................................................................... 29  
Module 3 - Features and Product Tour (60 minutes)....................................................... 30  
  Introduction......................................................................................................................... 31  
  Hands-on Labs Interactive Simulation: Features and Product Tour....................... 32  
  Conclusion......................................................................................................................... 33  
Module 4 - Advanced Topics (30 minutes).................................................................. 34  
  Introduction......................................................................................................................... 35  
  Zero Touch Provisioning.................................................................................................. 36  
  Conclusion......................................................................................................................... 69  
Module 5 - Troubleshooting and diagnostics (30 minutes).......................................... 70  
  Introduction......................................................................................................................... 71  
  Monitoring and Troubleshooting.................................................................................... 72  
  Conclusion......................................................................................................................... 94
Lab Overview - HOL-1940-01-NET - Getting Started with VeloCloud by VMware
Lab Guidance

Note: It may take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

Explore VMware NSX SD-WAN by VeloCloud including the key components and architecture. Review options for troubleshooting and diagnostics.

Lab Module List:

- **Module 1 - Overview of SD-WAN** (15 minutes) (Basic)
- **Module 2 - Key Components and Architecture** (15 minutes) (Basic)
- **Module 3 - Features and Product Tour** (60 minutes) (Basic)
- **Module 4 - Advanced Topics** (30 minutes) (Advanced)
- **Module 5 - Troubleshooting and diagnostics** (30 minutes) (Advanced)

Lab Captains:

- Module 1 - Mostafa Magdy, Sr. SE, Canada / Rohan Naggi, Sr. TPM, USA
- Module 2 - Mostafa Magdy, Sr. SE, Canada / Rohan Naggi, Sr. TPM, USA
- Module 3 - Rohan Naggi, Sr. TPM, USA / Mostafa Magdy, Sr. SE, Canada
- Module 4 - Rohan Naggi, Sr. TPM, USA / Mostafa Magdy, Sr. SE, Canada
- Module 5 - Rohan Naggi, Sr. TPM, USA / Mostafa Magdy, Sr. SE, Canada

This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

Location of the Main Console

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.

2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.

3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ key

1. Click on the "@ key"

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Overview of SD-WAN (15 minutes)
Introduction

In this module, we will talk about Software-Defined WAN and why the technology is important for modern business requirements.

This Module contains the following lessons:

- [Lesson 1: Defining Software-Defined WAN]
- [Lesson 2: Common business use cases for SD-WAN]
- [Lesson 3: SD-WAN Features]
- [Lesson 4: What SD-WAN is not]
- [Lesson 5: VMware NSX SD-WAN by Velocloud AT-a-Glance]
Overview of SD-WAN

SD-WAN offers compelling advantages for distributed organizations with critical branch operations, including the benefits of business agility, improved application performance, and lower cost of bandwidth. In this module, we will try to highlight those advantages and how enterprises can benefit from them.

Defining Software-Defined WAN

SD-WAN uses software and cloud-based technologies to simplify delivery of WAN services to branch offices. Software-based virtualization enables network abstraction that results in simplification of network operations. SD-WAN enables IT and business managers to deploy Internet-based connectivity (with its benefits of ubiquity, high bandwidth and low cost) easily, quickly and with quality, reliability and security.

SD-WAN Benefits

SD-WAN provides a wide range of benefits for distributed organizations, including:

1. **Business agility.** Rapid deployment of WAN services (such as bandwidth and firewall) to distributed branch operations without the need to send IT personnel on-site. Bandwidth can be easily added (with additional circuits) or reduced as business requirements evolve.
2. **Internet economics.** Internet connectivity (including cable, DSL and ethernet) is widely available, quick to deploy, and a fraction of the cost of equivalent MPLS circuits. SD-WAN provides the benefits of reliable, secure WAN service at Internet price points.
3. **Optimized cloud architecture.** SD-WAN eliminates the backhaul penalties of traditional MPLS networks and leverages the Internet to provide secure, high-performance connections from the branch to cloud. With SD-WAN, remote users will see significant improvements in their experience when using the cloud/SaaS-based applications.

SD-WAN Considerations

If you’re an IT or business manager, consider the following criteria when evaluating SD-WAN deployments:

1. **Ease of adoption and management.** A key benefit of SD-WAN is that it makes deploying WAN services at the branch fast and simple. SD-WAN solutions must be straightforward to deploy, and they leverage centralized provisioning to eliminate the need for trained personnel to visit remote sites.
2. **Ability to migrate to hybrid WAN.** The majority of distributed organizations already have MPLS deployed to the branch offices. Organizations should be able to seamlessly deploy SD-WAN solutions (Internet circuits) without changing the
existing MPLS network. Those organizations can over time, migrate traffic growth toward cost-effective Internet bandwidth.

3. **Automation - traffic steering.** SD-WAN gives organizations the ability to prioritize traffic. The key is providing managers with easy-to-use tools for setting priorities and with features that automatically changes traffic flows according to current network conditions.

**Common business use cases for SD-WAN**

Businesses need to be close to their customers at the branches and to support the organization’s growth. Enterprises grow by adding more branches to serve customers where they are, and every branch is growing bigger to be the hub of multiple services for the customers. Both types of growth require enterprises to be agile, to expand current network infrastructure and be able to provision more services per branch. SD-WAN solutions include features to eliminate the bottlenecks of hardware-based static architectures:

- Improving Business Agility with a Software-Defined Solution
- Driving IT Efficiency with Automation and Cloud Management
- Enabling the Migration to Cloud Services and Applications
- Reducing Overall Costs and Helping IT Budget Management

**SD-WAN Features**

In a nutshell, SD-WAN

- **Virtualizes the network**: SD-WAN as a network overlay enables application traffic to be carried independently of the underlying physical or transport layer, offering a transport-independent overlay. Multiple links, even from different service providers, constitute a unified pool of resources, often referred to as a virtual WAN.
- **Enables a secure overlay**: SD-WAN provides a secure overlay that is independent of the underlying transport components. SD-WAN devices are authenticated before they participate in the overlay.
- **Simplifies services delivery**: SD-WAN programmability does not just cover connectivity policy, it also extends to the insertion of network services, whether on the branch customer premise equipment (CPE), in the cloud or in regional and enterprise data centers.
- **Provides interoperability**: SD-WAN provides the ability to incrementally add resources and interoperate with existing devices and circuits. This capability follows directly from the separation and abstraction of the control plane from the data plane.
- **Leverages cost effective hardware**: SD-WAN improves cost effectiveness and flexibility by leveraging commercially available hardware and network appliances.
or servers. The separation of the control plane from the data plane enables the use of standard hardware for the data plane.

- **Supports automation with business policy framework**: SD-WAN enables the abstraction of configuration into business-level policy definitions that span multiple data plane components and also remain stable over time, even as the network changes. The control plane provides the programming flexibility and centralization over a diverse and distributed data plane. Enterprises can expect application awareness and smart defaults to provide further abstraction from the detailed transport level details. Policy definitions can refer to users & groups, the applications they should use, and what level of service they should receive.

- **Monitors usage and performance**: SD-WAN provides consolidated monitoring and visibility across the variety of physical transports and service providers, as well as across all remote sites. This monitoring capability offers business-level visibility, such as application usage and network resource utilization. SD-WAN adds detailed performance monitoring across all components of the data plane.

- **Supports interoperable and open networking**: SD-WAN further improves agility, cost effectiveness and incremental migration via its approach of open networking, interoperability, and evolving standards.

- **Enables managed services**: Many enterprises, even the largest, outsource the management of their branch networks and WAN to either managed IT providers or to their network service providers. Additionally, some cloud application providers, such as Unified Communications as a Service (UCaaS) providers provision and manage the circuits needed for accessing their applications.

More information on the above topics will be discussed later in the coming modules. You can also refer to the whitepapers and reports section on the VeloCloud website.

**What SD-WAN is not**

SD-WAN is a comprehensive solution comprised of many components. It does not include traditional WAN optimization.

- It is not just multi-link WAN bonding with path control.
- It is not just the last mile solution with a cloud gateway to provide caching and acceleration techniques to applications.
- It is not multilayer integration of packet and optical networks in a telco backbone.
- It is not private, dark-fiber networking that avoids telco services.
NSX SD-WAN by VeloCloud At-a-Glance

**Company Background**

- Acquired by VMware in 2017
- 2,000+ Customers
- 70,000+ Sites
- World’s Two Largest Enterprise SD-WAN Deployments
- Powers Global Tier 1 & Tier 2 Service Providers
- Global Footprint:
  - 24x7x365 Worldwide Support
  - 70+ Countries
- Robust Partner Ecosystem:

NSX SD-WAN by VeloCloud enables enterprises to securely support application growth, network agility, and simplified branch implementations. At the same time NSX SD-WAN delivers high-performance, reliable branch access to cloud services, private data centers, and SaaS-based enterprise applications. SD-WAN technology is ideal for customers looking for flexibility in network connectivity options that can augment MPLS. SD-WAN can provide a cost-effective, agile, and scalable fabric for the digital era, and improve overall TCO for branch connectivity.
The VMware Advantage

Connecting Everything, from Data Center to Edge

Why is VMware® well positioned to deliver on this new way of networking and security behind the idea of an enterprise cloud network?

6 years ago, VMware® set out to redefine networking in the data center. As a result, VMware has become the leading provider of Network Virtualization/SDN to the enterprise.

While VMware® had solved our customer needs as it's related to data center networking, many of our customers were looking to gain the same controls and capabilities in the public cloud.

NSX SD-WAN by VeloCloud targets Enterprises in every vertical industry with an initial focus on retail, manufacturing, healthcare, and services companies with 15 or more branch locations. NSX SD-WAN also tightly integrates with Service Provider network by placing SD-WAN components in SP network. The key advantage to SP (Service Provider) is the Multi-Tenancy aspect of the solution along with last mile protection for the user traffic. NSX SD-WAN by VeloCloud offers an easy to deploy solution which is provisioned through a cloud-based configuration and monitoring portal. NSX SD-WAN by VeloCloud is delivered through a combination of distributed gateways located in the cloud which are connected to edge devices located in each branch office.

NSX SD-WAN by VeloCloud offers the unique ability for Enterprises to keep their existing WAN. NSX SD-WAN by VeloCloud interoperates with the existing WAN while providing the ability for the Enterprise to add additional, reliable capacity via other links such as one or more Internet, cellular, private or other links. NSX SD-WAN by VeloCloud provides a smooth migration strategy allowing Enterprises to begin with a small number of users (as low as a single user or more) with the ability to scale to hundreds of thousands of users at their own pace.

The following challenges are addressed:
1. Security
2. Mobile device proliferation (BYOD: beyond bring your own device)
3. SaaS adoption by rogue users, shadow IT and sanctioned IT
4. Broadband Internet growth compared to traditional leased line (scale and geography)
5. Application demands by business operations (revenue and competitive)
Conclusion

This concludes our first chapter on the Overview of SD-WAN. In this module, you learned about SD-WAN and the business benefits it can help provide your company. In the next modules, we will focus more on NSX SD-WAN by VeloCloud.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on NSX SD-WAN by VeloCloud, try one of these:

- Click on this link
- Or go to https://tinyurl.com/yd7q2xs7

Proceed to any module below which interests you most.

- **Module 1 - Overview of SD-WAN** (15 minutes) (Basic)
- **Module 2 - Key Components and Architecture** (15 minutes) (Basic)
- **Module 3 - Features and Product Tour** (60 minutes) (Basic)
- **Module 4 - Advanced Topics** (30 minutes) (Advanced)
- **Module 5 - Troubleshooting and diagnostics** (30 minutes) (Advanced)

How to End Lab

To end your lab click on the END button.
Module 2 - Key Components and Architecture (15 minutes)
Introduction to NSX-SD WAN by VeloCloud

NSX SD-WAN is the first solution to provide all three elements needed to achieve an enterprise grade, Cloud-Delivered SD-WAN:

- Network connection to cloud and enterprise applications
- Software-defined control and automation
- Virtual services delivery

This Module contains the following lessons:

- [Lesson 1: NSX SD-WAN Advantages](#)
- [Lesson 2: Architecture](#)
- [Lesson 3: Solution Components](#)
- [Lesson 4: Core Features](#)
VMware NSX SD-WAN by VeloCloud

Key components and Architecture

In this lesson, we will introduce the NSX-SD WAN Solution in more detail. We will discuss the value, components and architecture of the solution of adopting NSX SD-WAN by VeloCloud solution:

- Increases acceleration to cloud application adoption (O365, SFDC, AWS, etc) with flexible traffic policies
- A fraction of the cost of an MPLS network
- Transport independent, whether private, public, even LTE
- We can improve your real time voice & video applications
- You'll have full management & visibility of your entire WAN
- Simplicity of zero-touch branch deployments
- Link remediation and correction
- Multi-tier / Multi-tenant

VMware NSX SD-WAN by VeloCloud is the only SD-WAN solution supporting data plane services in the cloud, in addition to on-premise deployments; enabling policy-based access to cloud and data center applications. NSX SD-WAN leverages the economics of the cloud to offer a SaaS like subscription price model to ease adoption and pay as you grow.
NSX SD-WAN solution is a logical overlay network:

- That can encompass any WAN transport, whether private, public, even LTE
- Independent of any service provider
- Between any two SD-WAN nodes
- These nodes are deployed at branches and datacenters in what we call SD-WAN Edges
- These can be appliances or virtual software appliances running on any x86 server
- This overlay is also extended to any cloud POP or datacenter with the cloud Gateways
- These are multi-tenant virtual appliances

The first benefit is SIMPLIFYING the management of WAN’s (Wide Area Networking) especially as IT wants the flexibility to use multiple circuits all while simplifying configuration and ongoing management. This starts with deployment also known as zero-touch branch deployments.

The second unique benefit of our approach is to assure the performance of critical applications.

- Over any transport, including Internet
- Means can fully leverage economical bandwidth for significant cost reductions

Finally, we support the migration of apps to the cloud.
• The NSX SD-WAN solution provides all the same performance, simplification and security benefits to the doorstep of cloud applications

Architecture Overview

NSX SD-WAN is a comprehensive platform for Enterprises and Service Providers.

Enterprise Deployment

Enterprise Deployments – Over-The-Top

In an Enterprise deployment model with branch edges creating overlay tunnels to gateway and hub devices. Simplified and secure VPN tunnels are established from branch to gateway and from branch to hub devices. Also supported are dynamic branch to branch links.
NSX SD-WAN supports tight integration with Service Provider network topologies. Gateways are usually found in Service Provider MPLS networks supporting multi-tenancy.

Component Overview

The NSX SD-WAN solution has three main components:
**Edge (VCE)** - highlight location flexibility (cloud, dc, branch), form factor flexibility

**Orchestrator (VCO)** - Virtual, Multi-tenant, highlight simplicity and no CLI, enables fast ramp of IT teams, less need for skilled resources, monitoring and troubleshooting are key, API Integration (eg AT&T leverages APIs)

**Gateway (VCG)** - Virtual, Multi-tenant with functions on data plane and control plane, VCG has global presence with partnerships with major service providers. Supports both cloud and on-premise model.

**NSX SD-WAN Edge**

The NSX SD-WAN Edge is deployed on-premises and optimizes traffic between customer branch, data center and/or cloud locations.

The NSX SD-WAN Edge is a compact, thin edge device that is zero-touch provisioned from the cloud for secure, optimized connectivity to applications and data. The NSX SD-WAN Edge is also available as a VNF (virtual network function) for instantiation on a virtual CPE platform. The NSX SD-WAN Edge with Dynamic Multi-Path Optimization (DMPO) and Deep Application Recognition (DAR) aggregates multiple links (e.g. Private, Cable, DSL, 4GLTE) and steers traffic over the optimal links in a dynamic fashion. These edges can be instantiated from AWS/Azure cloud.
NSX SD-WAN Orchestrator

The NSX SD-WAN Orchestrator is the centralized management portal that is used for configuration, monitoring, testing and troubleshooting the NSX SD-WAN. The cloud based NSX SD-WAN Orchestrator is used to provision network-wide business policy, enable services insertion, perform real-time monitoring and analyze application performance.

- Zero-touch provisioning
- Group business-level policies
- Automatic link profiling

The NSX SD-WAN Orchestrator is the centralized management portal that is used for configuration, monitoring, testing and troubleshooting the NSX SD-WAN. The cloud based NSX SD-WAN Orchestrator is used to provision network-wide business policy, enable services insertion, perform real-time monitoring and analyze application performance.

NSX SD-WAN Cloud Gateway

The NSX SD-WAN Gateway optimizes traffic between customer branch and data center locations and cloud (SaaS, IaaS) sites. NSX SD-WAN Gateways can also be used to extend SD-WAN connectivity from branches to legacy datacenters that do not have NSX SD-WAN Edge. The NSX SD-WAN Gateway also performs control plane as a route reflector for the SD-WAN overlay.

The NSX SD-WAN Edge can also optionally connect to the system of global NSX SD-WAN Gateways to provide performance, security and visibility for cloud services (SaaS, IaaS, B2B Internet). This system of NSX SD-WAN Gateways is deployed globally at top-tier cloud data centers to provide scalable and on-demand cloud network services.

Core Features

There are seven core features that are central to the NSX SD-WAN platform.
Core Feature #1: Zero-Touch Deployment

Zero-Touch Deployment
NSX SD-WAN Edge appliances automatically authenticate, connect, and receive configuration instructions once they are connected to the Internet in a zero-touch deployment. Deliver highly available deployment with NSX SD-WAN Edge redundancy protocol. Integrate with the existing network with support for OSPF routing protocol and benefit from dynamic learning and automation.

Core Feature #2: Dynamic Path Selection

Dynamic Path Selection
NSX SD-WAN Dynamic Multipath Optimization™ comprises of automatic link monitoring, auto-detection of provider and auto-configuration of link characteristics, routing and QOS settings.

Core Feature #3: Link Steering & Remediation

Link Steering and Remediation
On-demand, Per-packet link steering is performed automatically based on the measured performance metric, intelligent application learning, business priority of the application, and link cost. Delivers sub-second blackout and brownout protection to improve application availability. Remediates link degradation through forward error correction, activating jitter buffering and synthetic packet production.
Core Feature #4: Cloud VPN

Cloud VPN

One-click site-to-site cloud VPN is a VPNC-compliant IPSec VPN to connect NSX SD-WAN and non-NSX SD-WAN sites while delivering real-time status and health of VPN sites. Establish dynamic edge-to-edge communication for all types of branches based on service level objectives and application performance. Deliver secure connectivity across all branches with PKI scalable key management. New branches join the VPN network automatically with access to all resources in other branches, enterprise datacenters, and 3rd party datacenters, like Amazon AWS.

Core Feature #5: Multi-Tenancy

All the VMware NSX SD-WAN by Velocloud components, Orchestrator and the Gateways, are multi-tenant in nature.
Core Feature #6: Segmentation

Segmentation is essential for isolating different types of traffic while maintaining specific business policies, such as segmenting PCI traffic from corporate traffic and guest Internet traffic. Customers can enable the creation of separate and unique topologies and rules for each segment, and the segments are carried forward the entire network seamlessly.

Core Feature #7: Virtual Network Function

Virtual Network Function

Support virtual network function services to run on NSX SD-WAN Edge hardware, NSX SD-WAN Gateway, in the cloud of the service provider, or at the specific enterprise regional hub with service chaining support.

NSX SD-WAN core features will be discussed in greater detail in the next module.
Conclusion

In this module, we've taken a closer look on the overall architecture of NSX SD-WAN. We've also identified the major components along with the key features that differentiate NSX SD-WAN versus any other solution in the market.

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on [NSX SD-WAN by VeloCloud], try one of these:

- Click on this link
- Or go to https://tinyurl.com/yd7q2xs7

Proceed to any module below which interests you most.

- **Module 1 - Overview of SD-WAN** (15 minutes) (Basic)
- **Module 2 - Key Components and Architecture** (15 minutes) (Basic)
- **Module 3 - Features and Product Tour** (60 minutes) (Basic)
- **Module 4 - Advanced Topics** (30 minutes) (Advanced)
- **Module 5 - Troubleshooting and diagnostics** (30 minutes) (Advanced)

How to End Lab

To end your lab click on the END button.
Module 3 - Features and Product Tour (60 minutes)
Introduction

In this module, we will take product tour and check-out some of the most useful features of NSX SD-WAN Orchestrator.
Hands-on Labs Interactive Simulation: Features and Product Tour

This part of the lab is presented as a Hands-on Labs Interactive Simulation. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

1. Click here to open the interactive simulation. It will open in a new browser window or tab.
2. When finished, click the “Return to the lab” link to continue with this lab.

The lab continues to run in the background. If the lab goes into standby mode, you can resume it after completing the module.
Conclusion

In this module, we've taken a closer look on the overall architecture of NSX SD-WAN. We've also identified the major components along with the key features that differentiate NSX SD-WAN versus any other solution in the market.

You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on [NSX SD-WAN by VeloCloud], try one of these:

- Click on this [link](https://tinyurl.com/yd7q2xs7)
- Or go to [https://tinyurl.com/yd7q2xs7](https://tinyurl.com/yd7q2xs7)

Proceed to any module below which interests you most.

- **Module 1 - Overview of SD-WAN** (15 minutes) (Basic)
- **Module 2 - Key Components and Architecture** (15 minutes) (Basic)
- **Module 3 - Features and Product Tour** (60 minutes) (Basic)
- **Module 4 - Advanced Topics** (30 minutes) (Advanced)
- **Module 5 - Troubleshooting and diagnostics** (30 minutes) (Advanced)

How to End Lab

To end your lab click on the **END** button.
Module 4 - Advanced Topics (30 minutes)
Introduction

Zero Touch Provisioning

Zero Touch Provisioning is a feature that allows us to easily deploy and scale across hundreds of sites. This feature simplifies the entire process of edge activation.

Zero-touch provisioning of a NSX SD-WAN Edge is accomplished via the VeloCloud Orchestrator. With the Orchestrator, sites can be brought online in matter of few minutes in a true zero touch fashion. NSX SD-WAN Edges automatically authenticate, connect, and receive configuration instructions from the Orchestrator.

The Orchestrator supports both push and pull activation options for secure on-boarding. With these options, technical personnel do not have to be sent to remote customer sites for installation and activation.

This Module contains the following lessons:

- [Activation for Branch Site] [In this lesson we will walkthrough the process of activating a new branch site]
- [Configuring LAN side of the Edge Device] [In this lesson we will configure the network access for the edge device]
Zero Touch Provisioning

In this module we will be working on two main tasks:

1. Activation for a new Branch site.
2. Configuring LAN side of the Edge Device.

Activation for a new Branch site

Provision a new VeloCloud Edge

Before starting the lab, let us understand the NSX SD-WAN Zero Touch Provisioning feature

The current lab focuses on the Pull Activation process. In this Pull Activation model, the Edge device is shipped to the customer site with a factory-default image. Prior to activation, the Edge contains no configuration or credentials to connect to the enterprise network.

Two simple steps for the Activation of Edge device: (A) Provisioning & (B) Activation

Provisioning: On the Orchestrator, the Enterprise administrator (operator) creates a new Edge in the customer account. At this time, an activation key is generated which can be emailed to the person installing the device.
**Activation**: The person (remote admin) installing the device will receive both an activation email as well as instructions to complete the installation. Part of these instructions is to connect power and Internet links to the device. The installer next connects to a temporary wireless network the Edge emits or connects to one of the wired LAN ports and opens the activation email and clicks on the activation link. At this time, the Edge will phone home to the Orchestrator and bind itself to the correct enterprise and profile context. At this point the Edge downloads all relevant policies, updates and settings and makes these effective.

By the end of the lab, the Virtual Edge device status from the Orchestrator will show as Activated. All the WAN link information will get auto-populated with the activation process.

In this lab exercise, Virtual edge is used for activation.

- Orchestrator is hosted and managed by NSX SD-WAN. End user will use the Orchestrator (VCO) for Provisioning the Branch Site
- An un-activated Edge device (Virtual Edge) is used for Activation
- Edge device has two WAN Internet links. DHCP based IP on WAN side
- Client machine to access the local UI of the edge device

VeloCloud Orchestrator (VMware NSX SD-WAN Orchestrator), also referred to as VCO in the lab
The following information will be used to configure the virtual edge in the lab.

- Site name = **Chicago branch Site**
- Profile = **Branch OSPF profile**
- DHCP Based dual WAN links
- LAN IP address=**192.168.6.x/24**
- Chicago Branch site is with virtual edge device and a client machine (linux based)

*With the successful activation, ISP name, IP address, interface and the bandwidth for each of the WAN links will be auto discovered. This is done by the Edge device running a WAN bandwidth test with the SD-WAN Gateway component.*

**Provisioning and Activating an new Branch site**

In this exercise, End user will activate a Branch site. Branch site has a Virtual Edge with 2 internet links connected. Internet links have DHCP based WAN addresses. Once the edge device is activated successfully, all the WAN information is auto-discovered and pre-populated.
Read before you start

For this lab exercise, Activation process requires access to email client and server. As we don't have access to email, end user will access the Orchestrator from the client machine to access the Activation link. Client machine is connected to the LAN side of the edge device.

**Provisioning the Site**

Provisioning the Site starts with logging on to the Orchestrator as an Enterprise administrator and creating the site.
1. Double click on the Chrome browser to access the Orchestrator (VCO)
1. Click on VCO bookmark
2. Click on Advanced
1. Click on "Proceed to vco.velocloud.org" to continue

   ![Image of VeloCloud Orchestration login page]

   - Enter the Login name and Password
     
     Login= admin@globalretail.net
     
     Password= VMware1!
     
   - Click on Sign in to continue

You are now logged in as the "Super User" for the Enterprise "Global Retail". As a Super User, you are able to add and configure new edge devices.

Please Read:
For security reasons, the lab does not have access to the internet. There will be no Map view displayed. It might show as Loading Map view. Ignore the screen without the Map and continue with the lab exercise.

Screen shot with Map view is provided for your reference.
Monitoring Interface

1. The interface shows customer name "Global Retail, Inc" along with a total of 5 Sites with a geographical map and a list view.
2. Under Monitor-> Edges, you'll see a summary view for all the sites managed by VCO.
3. Details on each managed edge can be found here.
4. Each site statistics can be accessed separately by clicking on the site name.

Profiles provide a composite of the configurations created in Networks and Network Services. It also adds configuration for Business Policy and Firewall rules. Profiles have four tab pages: Profile Overview, Device, Business Policy, and Firewall.
Provisioning a New Edge

For this step, Enterprise administrator will create a new Branch Site and assign the model and profile or the edge device.

1. Name=Chicago Branch Site,
2. Model=Virtual Edge (from the drop down, select the Virtual Edge)
3. Profile=Branch OSPF Profile (from the drop down menu, select the profile)
5. Set Location: For this lab exercise, manually enter the location
   1. Type: Chicago
   2. Click Search
   3. Click OK
6. Click on **Create**

The site is created and the status for the site is "Pending". Activation Key is generated and this Activation key is sent to the remote user an link in the email.

Remote user (non IT person) needs to have access to the Edge device (physical or virtual).

1. Click on "**Send Activation Email**" to send the email to the remote administrator.
Sending Activation Email

1. Click **Send**

The Remote admin, as part of the activation process, will power on the device and follow the simple instructions specified in the email to activate the site.

**Activate Site:**

After provisioning the site, we need to activate the site. In this step, Activation link is sent over email to the remote admin who has access to the edge device.

In a real world scenario, Enterprise administrator / Super User provisions the site and emails the activation link to the remote user. Edge device is drop shipped to the remote location. As a next step, remote admin will connect his/her laptop to the edge device using Wireless or Wired connection and click on the activation link provided in the email.
As the lab environment does not have access to email server/client, our workaround is to access the activation link from the client machine. Client machine in this case is already connected to Edge device and has access to VCO.

For this lab, the client machine (Chicago Client machine) should be accessed from VNC viewer UI.

Minimize the Orchestrator browser window.

VNC Viewer UI can be accessed by going back to the windows desktop.

1. Double click on the "Chicago Client" connection to open up the client machine. This will give us access to the Edge device and VCO to complete the activation process.
VNC Viewer Client
1. Click on the **web browser** icon in the launcher.

![Web browser icon](image)

From the web browser,

1. Click on the bookmark to access VCO.
2. Sign in using the saved credentials. Click on Sign in

NSX SD-WAN Orchestrator (VCO) is being accessed from the client machine as a workaround to email. In the live deployment scenario, remote user will click on the email link and access the local User Interface (UI) for the edge device.
Chicago Branch Site Interface
- After the remote user logs in, check on the status for the Chicago Site. Hover over the Chicago site status, it will show as "pending activation".

1. Click on **Configure -> Edges**
2. Click on **Chicago Branch Site**

### Chicago Branch Site Activation
3. Click on "Send Activation Email" button

![Send Activation Email dialog box]

4. Access the highlighted url from the client. Click on the Link (Activation Link)

Clicking on the link will show case the local UI for the Edge device.

Local UI opens up in a new browser tab. All the information related to activation like Orchestrator IP Address, Activation key gets auto-populated. End user does not have to type in all of this information.
Client Activation

As this is a lab environment, Certificate Error should be ignored.

1. Click on **Advanced**
2. Click the **Ignore checkbox** for Certificate Error.
3. Click **Activate**

*You might have to wait for approximately 15-30 seconds for the activation process to complete.*

Real World Tip: Make sure in the field "Internet Status" is connected. Activation process will fail if the internet status is not connected.
• The Activation process starts. The Edge device calls home to Orchestrator over the internet link, identities (security tokens) are exchanged, and the activation process is successful.

Close the local UI and the Orchestrator browser page from the client machine.
Also, please go ahead and close or minimize the VNC viewer UI.

Next Step is to Verify the Status for the Chicago Site.
Verifying the Site Status

- After closing the VNC Viewer UI, return to the Google browser where we are in Orchestrator.

1. Click on **Monitor->Edges**
2. Confirm the **Chicago Branch Site** shows the Active (green status)
Chicago Site Link Status

As the lab environment have limited or no internet access, you might not see the WAN ISP link names getting auto populated. You will see the IP addresses for the WAN ISP Links.

Hover the mouse cursor over the 2 Links field

1. Click on the **Chicago Branch Site**
### Chicago Site WAN details

![Chicago Branch Site](image)

As this is a lab environment with no or limited internet access, lab pod might not auto resolve the ISP names. End user in the lab environment will only see the IP address for the links and not the ISP names.

ISP names will not auto populate in lab environment.

All the WAN link related information is auto-populated for the end user. End user does not have to provide ISP IP address, Interface details, or Bandwidth as part of the activation process.

Also, the current statistics related to WAN throughput are provided. You will notice the Throughput numbers keep changing.

*This is done by the Edge device running WAN bandwidth tests with the SD-WAN Gateway component.*

This concludes the Activation lab.

### Configuring LAN side of the Edge device

This lab will help you understand how to configure the edge device.

In this exercise, we will configure the LAN side for the edge device. Client machines which are part of the LAN subnet will use the Edge device to get Internet connectivity.

For this lab, you will configure the LAN subnet and also enable the Edge device to be the DHCP server for LAN subnet.

<table>
<thead>
<tr>
<th>Links</th>
<th>Cloud Status</th>
<th>VPN Status</th>
<th>Interface (WAN Type)</th>
<th>Throughput</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verizon Wireless</td>
<td><img src="image" alt="status" /></td>
<td><img src="image" alt="status" /></td>
<td>GE3 (Ethernet)</td>
<td>2.83 kbps</td>
<td>192.52 Mbps</td>
</tr>
<tr>
<td>Time Warner Cable</td>
<td><img src="image" alt="status" /></td>
<td><img src="image" alt="status" /></td>
<td>GE4 (Ethernet)</td>
<td>43.55 kbps</td>
<td>193.96 Mbps</td>
</tr>
</tbody>
</table>
Configuration can also be performed on a unactivated edge device. When the edge device gets activated, Orchestrator will push the configuration to the edge device.

With Edge device being the DHCP server for LAN subnet 192.168.6.x/24, Chicago Client machine will get the new IP address from Subnet 192.168.6.x

- Site Name = **Chicago Branch Site**
- Branch site in this case is **Activated**
- Client machine name is **Chicago Client** machine. This machine is accessed using VNC UI
- LAN side Subnet is **192.168.6.x/24**

**Topology**
Configure the Edge Device

- From the Windows desktop, click on the Internet browser (in this case, google chrome) to access VCO.

Please Read: If you are already logged onto the Orchestrator, you can ignore the steps on clicking on the web browser and logging on to the orchestrator. You can start by clicking on Configuring the edge.

1. Click on the bookmark for VCO
2. Type the below credentials:
   
   Login = admin@globalretail.net
   Password = VMware1!
3. Click Sign In

**Configuring Edge**

1. Click on **Configure**
2. Click on **Chicago Branch Site**

1. Click on the **Device** tab
Configuring VLAN

Scroll down on the device tab to access the VLAN configuration.
1. Click on **Edit** to configure the LAN Subnet

![VLAN Configuration Screen]

1. Enter the Edge LAN IP address as **192.168.6.1**
2. Click on the network address, it will be auto-filled
3. Click on "Update VLAN" button

GE1 and GE2 are part of VLAN1 (LAN Segment)

Depending on your enterprise network, you will configure the DHCP client address range, lease time, and other DHCP Options.

Optional Step: Optional Step: You could put the Management interface in the same subnet as the LAN subnet.

How to put the management IP address in the same subnet as LAN segment (VLAN1)?

By clicking on "**Enable Edge Override**" and changing the management IP to **192.168.6.2**.
Save Changes

- Click on **Save Changes**

You could also use Monitor->Events to check for the events between the orchestrator and the edge device

**Verification Step**

- In this step, End user will verify by connecting the machine on the LAN segment of the edge device. Expected result is to have the client machine get the IP address from the edge device in the subnet 192.168.6.x/24
• Let us access the client machine from the Windows desktop. Minimize the browser window

• Click on the VNC Viewer.

• Double click on the **Chicago Client** VNC session to get the CLI Access for the client machine.
• This machine is pre-wired and connected to the GE1 interface of the edge device.
1. Click on the terminal window to access the CLI (Command line interface).

- As the client machine is a Linux machine, end user will have to execute "Service networking restart" cli. This way client machine will restart networking and get the IP address from DHCP Server.

DHCP Server is the Edge Device (Chicago Branch Site)
Type in "service networking restart" and press Enter to restart the networking on the Linux machine.

```
.service networking restart
```

If for some reason the prompt return back immediately, re-execute the cli.

```
Service networking restart
```

**Confirm Network Configuration**

```
root@x-chi-client:/# (netstat -rn
Kernel IP routing table
 Destination Gateway Genmask Flags MSS Window Irtt Iface
 0.0.0.0 192.168.6.1 0.0.0.0 UG 0 0 0 eth1
 0.0.0.0 192.168.6.1 0.0.0.0 UG 0 0 0 eth2
50.50.50.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
192.168.6.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
root@x-chi-client:/#
```

After executing the service networking cli, now check for the IP address assignment on the client machine.

Type:

```
netstat -rn
```

Expected result should be that the Default gateway should be **192.168.6.1 (edge device)** and GE1 on the client machine should be part of **192.168.6.x subnet**.

```
root@x-chi-client:/# ifconfig eth1
eth1 Link encap:Ethernet HWaddr 00:ba:be:32:4e:e6
inet addr:192.168.6.18 Pbrcast:192.168.6.255 Mask:255.255.255.0
inet6 addr: fe80::2ba:beff:fe32:4ee6/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3322 errors:0 dropped:0 overruns:0 frame:0
TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:167314 (167.3 KB) TX bytes:39005 (39.0 KB)
```

• Also check the interface IP address by executing

```
ifconfig eth1
```

Verify that the command shows the Client IP Address **192.168.6.18/24**.
This IP address got assigned by the DHCP Server. In this case the DHCP server is the Edge device.

```
root@x-chi-client:/# ping 192.168.6.1
PING 192.168.6.1 (192.168.6.1) 50(64) bytes of data.
64 bytes from 192.168.6.1: icmp_seq=1 ttl=64 time=0.239 ms
64 bytes from 192.168.6.1: icmp_seq=2 ttl=64 time=0.195 ms
64 bytes from 192.168.6.1: icmp_seq=3 ttl=64 time=0.180 ms
64 bytes from 192.168.6.1: icmp_seq=4 ttl=64 time=0.150 ms
--- 192.168.6.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 300ms
rtt min/avg/max/mdev = 0.159/0.193/0.239/0.033 ms
root@x-chi-client:/#
```

Initiate a ping to the gateway. In this case the gateway for subnet 192.168.6.x is the DHCP Server (edge device).

**Exit VNC**

Close the VNC UI and open the Chrome browser tab with orchestrator. Orchestrator can be accessed from the windows taskbar.
Verify configuration change in the UI

1. Click on **Monitor**
2. Click on **Events**
3. Verify you can see the new IP configured on the edge with IP address **192.168.6.18** (in this case the Linux machine = Chicago Client machine)

This Concludes the 2nd lab exercise.
Conclusion

In this module we have successfully provisioned a new branch site using Zero Touch Provisioning and we have also configured the network access for the edge device and verified connectivity.

You’ve finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on [NSX SD-WAN by VeloCloud], try one of these:

- Click on this link
- Or go to https://tinyurl.com/yd7q2xs7

Proceed to any module below which interests you most.

- **Module 1 - Overview of SD-WAN** (15 minutes) (Basic)
- **Module 2 - Key Components and Architecture** (15 minutes) (Basic)
- **Module 3 - Features and Product Tour** (60 minutes) (Basic)
- **Module 4 - Advanced Topics** (30 minutes) (Advanced)
- **Module 5 - Troubleshooting and diagnostics** (30 minutes) (Advanced)

How to End Lab

To end your lab click on the **END** button.
Module 5 - Troubleshooting and diagnostics (30 minutes)
Introduction

VMware NSX SD-WAN Orchestrator (VCO) is an essential component of the SD-WAN solution where enterprise administrators can configure, monitor and troubleshoot the entire SD-WAN Network.

1. **Orchestrator Monitoring** includes: Site monitoring like Link statistics, Link Quality score card (QoE), Application level analytics, Business priority, Network service monitoring and more. Different type of alerts and how to check them along with events.

2. Built in **Troubleshooting Tools**: included tools are ping, traceroute, list path, routing table list and many more.

QoE: Quality of Experience (QoE) rating for WAN links

The QoE screen shows the *VeloCloud Quality Score* (VQS) for each of the links and rates them on a scale from 0 through 10 on how well the links perform to carry a certain type of traffic (Voice in the default case)

This Module contains the following lessons:

- [Lesson 1: Monitoring tabs](#) [Understand the Monitoring Capabilities]
- [Lesson 2: Troubleshooting](#) [Built-in Troubleshooting Tools available from the Orchestrator]
Monitoring and Troubleshooting

In this portion of the lab user will understand the Monitoring capabilities and the Built-in troubleshooting Tools available from the Orchestrator

NSX SD-WAN Orchestrator Monitoring

As we move forward in understanding the concept, there will be series of mini labs to be executed

Monitoring Labs

In this section, we’ve identified a couple of exercises that highlight some of the monitoring features available in the orchestrator

Lab 1: Identify the Map View and the List View.

Lab 2: Identify how many transport links are in use, determine the ISP (Service Provider) info & software version being run by Dallas Site.

Lab 3: How to find details on the WAN links analytic like current statistics?

Lab 4: How to view details on the WAN performance parameters like link Latency, Jitter, and Packet loss?

Lab 5: Understand on how to check the score card for Voice and Video applications.

Lab 6: How to check on the real time update and identify Avg Throughput along with traffic type (TCP or UDP)?

Lab 7: Walk through the Application tab.

Troubleshooting Labs

Lab 1: Use of Remote Action to reboot an edge device

Lab 2: Use of Remote Diagnostics tools

Monitoring

Monitoring section will focus on
1. Site & Link Monitoring
2. QoE
3. Application Tab
4. Transport Tab
5. Business Policy

Other Monitoring capabilities exist like Syslog, SNMP, Netflow and API integration. These topics are advanced topics and are not covered in this lab.

Some of the lab exercise cannot be simulated in the lab environment like going back 30 days and checking the statistics, introducing % loss on the link and more, generating real application traffic and checking on the application list. To compensate these real lab challenges, screen shots are provided from live deployment testbed. Use it for your reference and to understand the concept.

**Site/Link Monitoring**

Double click on the browser

The browser should direct you to the VeloCloud Orchestrator, to be referred in the rest of the document as VCO.
A bookmark has been saved in case the browser doesn't automatically redirect you.

1. Login using:
   Username: admin@globalretail.net
   Password: VMware1!

2. Click Sign In

Main monitoring interface

1. When a user logs into the Enterprise portal of VCO, under Monitor, a list of the most important components that require admin attention are listed.
2. The VeloCloud map shows a global overview of all managed branch locations.
3. Edge: Shows a list of the sites managed by VCO
4. Status: Shows the link health.
5. Links: Shows the number of transport links associated with the branch site

This lab will help us understand:

- How to Identify different site status
- How many WAN links are connected to the site and their status
- What software version the site is running
• Zoom in for Map View (this section might not work in a lab environment as the access to the internet is blocked)

Question: Using the Map view, are you able to identify those 3 sites in California region and their status

On your student lab pod if you don't see the Map view, Do not try to execute the lab of Zooming the map, use this as a reference.

Student pod might see an error message instead of Google Map view.

As this is a lab environment, Internet access is blocked for security reasons.

In the next release of lab version, we will provide you with the workaround. This lab exercise is for your understanding and can be leveraged in the live deployment.

**Identify Sites/ Links geographically on the map**
Either use the Zoom + sign or click on the "3" to get the details.

If you don't see the Map view and are getting an error message, or the map view always shows loading maps, Do not execute this lab exercise but instead use it for your understanding.

SFO, SJC, DC1 Sites and the status for all these sites are Green(Up and Running).

**Transport links**

Are you able to identify how many transport links, ISPs (Service Providers) info & software version being run by Dallas Site?

Answer: Hover over the links next to Dallas Branch Site. Dallas Site is with single Internet link provided by Comcast ISP. Software version running is 3.1 release.

This allows administrators to ascertain the state of the network in a single glance.
Wan link analytics

When looking at the details of the edge, one of the first items that will stand out is the inventory of transport links. All of the information you see in the Link Status section is automatically populated when an edge is activated.

The system will discover the Service Provider as well as the bandwidth of the link, including the physical port that this capacity is connected to on the edge device.

For this lab, Use the LAX Site. LAX site is with single internet connection.

1. Click on the LAX Branch Site from the list view (Monitor->Edges)

Link throughput
• Initial Throughput numbers are 0. Give it few seconds and end user will start noticing the Current statistics for the WAN Link.

The system will auto discover the Service Provider as well as the bandwidth of the link, including the physical port that this capacity is connected to on the edge device. This way no one has to provide all these information during the activation stage.

**WAN performance**

Question: How to get the details on the WAN performance parameters link Latency, Jitter, Packet loss?

There are real time measurements available that characterize the links, latency, jitter and packet loss behavior.

1. Click on the blue arrow to get the details on the WAN performance parameters like Latency, Jitter, %Packet loss.
This is a critical component to understand what the links are capable of transporting and what the impact of these conditions are on applications.

**Quality of Experience**

Another way to determine the link quality is to look at the Quality of Experience (QoE) rating.

![Screenshot of VeloCloud/NSX Quality Score](image)

Screenshot is for reference only. This screenshot is taken from a live deployment in order to understand QoE.

Screenshot shows yellow and red color legend with problem either related to Latency, Jitter or Packet loss. As you hover over sections of the timeline, you can see what the system detected and what techniques have been employed to protect application traffic.

The screenshot shows the VeloCloud/NSX Quality Score (VQS) for each of the links and rates them on a scale from 0 through 10 on how well the links perform to carry a certain type of traffic (Voice in the default case).

It will show the score before SD-WAN services applied and the top bar shows the quality observed by end users after SD-WAN services were applied.

At a minimum, the solution can steer around brown-out conditions on an individual link. The solution is also capable of enabling packet duplication in order to mitigate effects of packet-loss on all of the available links. In addition, de-jitter buffering can normalize the effects of jitter on VOIP calls. All of the steering and mitigation techniques are dynamically enabled on a per-application basis.
Steering of flows is done on a per-packet basis, insuring sessions are preserved while protecting the quality of the session towards the end-users.

Current and Historical insight into link properties are available, as well as usage

**Quality of Experience, QOE**

The NSX SD-WAN by VeloCloud Quality of Experience (QoE) tab shows the Quality Score (VQS) for different applications. The VQS rates an application's quality of experience that a network can deliver for a period of time.

In this section we will demonstrate how to check the score card for Voice and Video application.

For this lab, LAX Branch site will be used. If you are already in the LAX branch site, click on it. If not follow the steps to access LAX Branch Site.
1. Click **Monitor->Edges**
2. Click on the **LAX Branch Site**.

1. Click on the **QoE Tab**
2. Use the drop down for Traffic type. Select **Voice**.

There are three different traffic types that you can monitor (Voice, Video, and Transactional) in the **QoE** tab. You can hover over a WAN network link, or the aggregate link provided by the NSX SD-WAN by VeloCloud to display a summary of Latency, Jitter, and Packet Loss.

In a real deployment environment, you will not see all green. There will be patches with Red/yellow. Red/yellow patches indicate issues with the WAN links (%loss, latency or Jitter).

**Transport**

Let's move over to the **Transport** visibility where administrators can seek to better understand the utilization of the individual links. Administrators can place an Edge in live mode in which it will stream real time updates to the VCO.

This is a tool that is valuable for troubleshooting and identifying network utilization pattern breakouts.
Screenshot captured for reference from a live deployment network

**Throughput**

In the coming section we will identify Avg Throughput along with traffic type (TCP or UDP) in real time.

In this lab exercise, you will put the edge device in live troubleshooting mode to check on:
1. Average Throughput for the live traffic on the WAN link.
2. TCP/UDP Traffic

From the Orchestrator UI, Click on the LAX Branch Site.

**Transport Tab**
1. Click on the **Transport Tab**

1. Click on the drop down menu to select the **Average Throughput**

**Live Monitoring**

1. Click **Start Live Monitoring** button to view the current statistics
TCP/UDP details

- Enable the check box for **TCP/UDP Details**

This will help user view the current statistics and also give details on TCP/UDP.
This tool that is valuable for troubleshooting and identifying network utilization pattern breakouts.

**Stop Monitoring**

- Suspend the Live troubleshooting tool by clicking on the "Stop Live Monitoring"

**Applications Tab**

Let's investigate why there is a sizable volume of Youtube traffic on the branch network and eroding bandwidth?

This can be answered from the Application Tab.

The Edges are also responsible for detecting the applications that are being used and have awareness of what the networking requirements are for each application.

To answer the question on who is using Youtube traffic. The Top Applications infographics will show which devices are using Youtube and to which domains the flows are being sent.

Administrators can now see all of the devices that are sending Youtube traffic as an application filter is carried to the Source tab.
The embedded Deep Application Recognition (DAR) engine can detect 2500+ applications.

Capturing 30 days of data is not possible in a lab environment. This Screen shot is for your reference only and for your understanding it has been captured from a live deployment environment.

1. **Click Application Tab from Monitor-> Edge**

2. **Click the drop down** menu and change the time period.

Screen captured is for your reference. This screen has been captured from a live network. This view is not possible to simulate in lab environment.

Screen shot shows that in past 30 days, edge device has recognized and seen 456+ applications
Lab 4.1 Walkthrough Application tab

- As this is a lab environment, you will not see list of applications under application. This lab walkthrough is to understand when and how to use the Application tab.

Clicking on any of the application will provide you with deeper level details on which devices are using that application.

Source and Destination Tabs

With the source and destination tab, Administrators can now see all of the devices that are sending specific traffic and to which destination. End user can also use filters to get more details, one such example is captured in below screen shot for Youtube traffic.
Administrators can now see all of the devices that are sending Youtube traffic as an application filter is carried to the Source tab.

No lab is to be performed for Source and Destination Tab. Screen captured is for your reference and has been captured from a live deployment.

**Troubleshooting**

In this portion of the module, we will focus on the embedded diagnostic tool.

The NSX SD-WAN by VeloCloud Orchestrator Test & Troubleshoot functionality provides tools to test the status of the VeloCloud service, perform Edge actions, and gather Packet Capture information for an individual Edge. You can access these features under the **Test & Troubleshoot** section of the orchestrator.
The SD-WAN solution has also a series of embedded diagnostics tools to remotely troubleshoot connectivity as well as client issues. Most common diagnostic activities can now be performed without participation of an on-site technician.

**Use of Remote Action**

How does an Enterprise administrator reboot a remote edge device without sending an IT person to remote location?

From the Orchestrator, Test & Troubleshoot-> Remote Actions-> Select the edge and perform the remote action.

1. Click on Test & Troubleshoot to access a wide range of tools
2. Click on Remote Action
3. Click on the LAX Branch Site
Reboot Edge

1. Click on **Reboot**

1. Reboot the device, **Click to Continue Yes**
2. Click **Close**
1. Click on **Monitor**

2. Click on **Events** to check on the status of reboot

### Remote Diagnostics

There are many embedded tools for Remote diagnostics like List path, list routing table, ping, traceroute and more. These tools will help troubleshoot without sending an IT staff to remote location.

From the Orchestrator, Click on Test and Troubleshoot to access wide range of tools.

*No CLI is required for the remote edge device.*

![Remote Diagnostics interface](image)

1. Click on **Test & Troubleshoot**

2. Click on **Remote Diagnostics**

3. Click on **Dallas Branch Site**
Dallas Branch Site

• Perform a simple *System health test*

• Click on Run for the System Health test result

**Conclusion**

This lab module focus for you was to understand different monitoring capabilities along with available troubleshooting tools available through the Orchestrator.
Conclusion

In this module, we learned about some of the many Monitoring capabilities and Built-in troubleshooting tools available out of the box from the VCO.

You have finished Module 5

Congratulations on completing Module 5.

If you are looking for additional information on [NSX SD-WAN by VeloCloud], try one of these:

- Click on this link
- Or go to https://tinyurl.com/yd7q2xs7

Proceed to any module below which interests you most.

- Module 1 - Overview of SD-WAN (15 minutes) (Basic)
- Module 2 - Key Components and Architecture (15 minutes) (Basic)
- Module 3 - Features and Product Tour (60 minutes) (Basic)
- Module 4 - Advanced Topics (30 minutes) (Advanced)
- Module 5 - Troubleshooting and diagnostics (30 minutes) (Advanced)

How to End Lab

To end your lab click on the END button.

Instructions (Not to copied into actual HOL manual)

- The additional information is optional but recommended per the module topic. Use the 3 methods to offer easy access now and later to your material. After copying the QRC code in as a picture resize by dragging the corners to reduce the overall size.
- Place a hyperlink for each module pointing to the beginning of each module in the manual. Instructions can be found in the Lab Guide.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1940-01-NET

Version: 20181104-145841