VMware SD-WAN: Deploy and Manage

Lecture Manual

VMware® Education Services
VMware, Inc.
www.vmware.com/education

VMware SD-WAN: Deploy and Manage

Lecture Manual

VMware SD-WAN™

Part Number EDU-EN-SDWANDM4-LEC (01-APR-2022)

Copyright © 2022 VMware, Inc. All rights reserved. This manual and its accompanying materials are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware vSphere® 2015, VMware vSphere®, VMware vCloud®, VMware vCenter Server®, VMware vSphere® vApp(s)™, VMware View®, VMware Horizon® View™, VMware Verify™, VMware Secure Access™, VMware SD-WAN™ by VeloCloud®, VMware SD-WAN™ by VeloCloud® – WFH Pro Subscription, VMware SD-WAN™ by VeloCloud® – WFH Subscription, VMware SD-WAN™, VMware SD-WAN™ for AWS GovCloud (US), VMware SD-WAN™ on AWS GovCloud (US), VMware SASE PoP™, VMware SASE™, VMware Horizon® 7, VMware Horizon® 7, VMware Horizon® 7 on VMware Cloud™ on AWS, VMware Edge Network Intelligence™, VMware Customer Connect™, VMware Cloud Web Security™, VMware Cloud Web Security™ Standard, VMware Cloud Web Security™ Advanced, VMware NSX®, VMware Lab Connect™, VMware Go™, and VMware ESXi™ are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

The training material is provided “as is,” and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This material is designed to be used for reference purposes in conjunction with a training course.

The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended. These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted, or modified without the express written approval of VMware, Inc.

www.vmware.com/education

Contents

Module 1 Course Introduction 1

1-2 Course Introduction 1
1-3 Importance 1
1-4 Learner Objectives (1) 2
1-5 Learner Objectives (2) 2
1-6 Course Outline 3
1-7 Typographical Conventions 4
1-8 References 5
1-9 VMware Online Resources 6
1-10 VMware Learning Overview 7
1-11 VMware Certification Overview 8
1-12 VMware Credentials Overview 9

Module 2 Introduction to the VMware SD-WAN Solution 11

2-2 Importance 11
2-3 Module Lessons 11
2-4 Lesson 1: Reviewing Traditional WAN Technology 12
2-5 Learner Objectives 12
2-6 Introduction to WAN Technology 13
2-7 WAN Topologies 14
2-8 WAN Connection Types 15
2-9 Popular WAN Technologies 16
2-10 Virtual Private Networks 17
2-11 Disadvantages of Traditional WANs 18
2-12 Review of Learner Objectives 19
2-13 Lesson 2: Introduction to VMware SASE 20
2-14 Learner Objectives 20

2-15 Modern Security and Performance Challenges 21
2-16 About SASE 22
2-17 VMware SASE 23
2-18 Components of the VMware SASE Solution 24
2-19 SASE Use Cases 25
2-20 VMware SASE PoP 26
2-21 Review of Learner Objectives 27
2-22 Lesson 3: Introduction to the VMware SD-WAN Solution 28
2-23 Learner Objectives 28
2-24 About SD-WAN Solutions 29
2-25 VMware SD-WAN Capabilities 30
2-26 VMware SD-WAN Benefits 31
2-27 VMware Dynamic Multipath Optimization 32
2-28 Review of Learner Objectives 33
2-29 Key Points 34

Module 3 VMware SD-WAN Components and Architecture 35

3-2 Importance 35
3-3 Module Lessons 35
3-4 Lesson 1: VMware SD-WAN Edge 36
3-5 Learner Objectives 36
3-6 About VMware SD-WAN Edge 37
3-7 Advanced Features of VMware SD-WAN Edge 38
3-8 VeloCloud Multipath Protocol 39
3-9 About the Underlay Network 40
3-10 About the Overlay Network 41
3-11 About VMware SD-WAN Hubs 42
3-12 Use Cases for VMware SD-WAN Hubs 43
3-13 High Availability Design Options for Branches 44
3-14 High Availability Design Options for Data Centers and Hubs 45
3-15 Versions of VMware SD-WAN Edge 46
3-16 Subscription Options 47
3-17 VMware SD-WAN Edge Software Features 48
3-18 Physical Connectivity Options 51
3-19 Review of Learner Objectives 52
3-20 Lesson 2: VMware SD-WAN Orchestrator 53
3-21 Learner Objectives 53

3-22 About VMware SD-WAN Orchestrator 54
3-23 Functions of VMware SD-WAN Orchestrator 55
3-24 VMware SD-WAN Orchestrator Placement 56
3-25 Supported Web Browsers 57
3-26 Review of Learner Objectives 58
3-27 Lesson 3: VMware SD-WAN Gateway 59
3-28 Learner Objectives 59
3-29 About VMware SD-WAN Gateway 60
3-30 Cloud-Hosted Gateways 61
3-31 Gateway Proximity and Assignment 62
3-32 Connecting to SaaS, IaaS, and Non-SD-WAN Destinations 63
3-33 Gateways as Controllers 64
3-34 Gateways as Hubs 65
3-35 Gateways as Route Reflectors 66
3-36 Types of Gateways 67
3-37 Advantages of Cloud-Hosted Gateways 68
3-38 Partner Gateways 69
3-39 Review of Learner Objectives 70
3-40 Lesson 4: VMware SD-WAN Component Interactions 71
3-41 Learner Objectives 71
3-42 VMware SD-WAN Planes 72
3-43 VMware SD-WAN Management Path 73
3-44 VMware SD-WAN Control Path 74
3-45 VMware SD-WAN Data Path 75
3-46 Review of Learner Objectives 76
3-47 Key Points 77

Module 4 Using VMware SD-WAN Orchestrator 79

4-2 Importance 79
4-3 Module Lessons 79
4-4 Lesson 1: VMware SD-WAN Orchestrator Portal Walk-Through 80
4-5 Learner Objectives 80
4-6 VMware SD-WAN Orchestrator Capabilities 81
4-7 VMware SD-WAN Orchestrator Portal Layout 82
4-8 Navigating the VMware SD-WAN Orchestrator Header (1) 83
4-9 Navigating the VMware SD-WAN Orchestrator Header (2) 84
4-10 Navigating the Monitor Menu 85

4-11 Navigating the Configure Menu 86
4-12 Navigating the Test & Troubleshoot Menu 87
4-13 Navigating the Administration Menu 88
4-14 Lab 1: Understanding the Lab Environment 89
4-15 Lab 2: Exploring VMware SD-WAN Orchestrator 90
4-16 Review of Learner Objectives 91
4-17 Lesson 2: Installing Edge Hardware 92
4-18 Learner Objectives 92
4-19 VMware SD-WAN Edge Hardware Appliance Placement 93
4-20 Front Panel Status Indicators 94
4-21 Edge Installation Best Practices 95
4-22 Powering the Edge 96
4-23 Establishing Internet Connectivity 97
4-24 Connecting LAN Devices 98
4-25 Review of Learner Objectives 99
4-26 Lesson 3: Commissioning an Edge Appliance 100
4-27 Learner Objectives 100
4-28 Commissioning an Edge Appliance 101
4-29 Provisioning an Edge Appliance 102
4-30 Activating an Edge Appliance 103
4-31 Comparing Edge Activation Methods 104
4-32 About Zero-Touch Activation 105
4-33 Lab 3: Zero-Touch Provisioning 106
4-34 Review of Learner Objectives 107
4-35 Key Points 108

Module 5 Configuring VMware SD-WAN 109
5-2 Importance 109
5-3 Module Lessons 109
5-4 Lesson 1: Basic Network Configuration 110
5-5 Learner Objectives 110
5-6 VMware SD-WAN Configuration Workflow 111
5-7 Configuring the Basic Network (1) 112
5-8 Configuring the Basic Network (2) 113
5-9 Segmentation in LAN and WAN Networks 114
5-10 Segmentation in VMware SD-WAN 115
5-11 VMware SD-WAN Segmentation Use Cases 116

5-12 Types of Segments in VMware SD-WAN 117
5-13 VMware SD-WAN Segmentation Topology 118
5-14 Configuring Segmentation for an Enterprise 119
5-15 Lab 4: Configuring Segmentation 120
5-16 Review of Learner Objectives 121
5-17 Lesson 2: Configuring Network Services 122
5-18 Learner Objectives 122
5-19 Configurable Network Services 123
5-20 Configuring Network Services 124
5-21 Configuring Non-SD-WAN Destinations 125
5-22 Non-SD-WAN Destination Configuration Workflow 126
5-23 Non-SD-WAN Destinations Through VMware SD-WAN Gateway 127
5-24 Configuring Access to Non-SD-WAN Destinations from a Gateway 129
5-25 Non-SD-WAN Destinations Through VMware SD-WAN Edge 130
5-26 Configuring Access to Non-SD-WAN Destinations from an Edge (1) 132
5-27 Configuring Access to Non-SD-WAN Destinations from an Edge (2) 133
5-28 About DNS Services 134
5-29 Configuring DNS Services 135
5-30 About Authentication Services 136
5-31 About Cloud Security Services 137
5-32 Configuring a Cloud Security Provider (1) 138
5-33 Configuring a Cloud Security Provider (2) 139
5-34 Configuring a Cloud Security Provider (3) 140
5-35 Configuring Cloud Security Services for Profiles 141
5-36 About the Edge Clustering Service 142
5-37 About Cluster Scores 143
5-38 About Auto Rebalance 144
5-39 Configuring an Edge Cluster 145
5-40 Review of Learner Objectives 146
5-41 Lesson 3: Configuring Profiles 147
5-42 Learner Objectives 147
5-43 About Profiles in VMware SD-WAN 148
5-44 Workflow for Creating a New Profile 149
5-45 Creating a New Profile 150
5-46 Configuring a Profile Device 151
5-47 Segment-Aware Configuration 152

5-48 Common Configuration 153
5-49 Configuring VLANs for Profiles 154
5-50 Edge Interface Settings 155
5-51 About Business Policies 156
5-52 About Business Policy Rules 157
5-53 Creating a New Business Policy Rule 158
5-54 Configuring the Source and the Destination 159
5-55 Selecting an Application for the Rule 160
5-56 Configuring the Action for the Rule 161
5-57 About the Firewall Tab 162
5-58 Stateful Versus Stateless Firewalls 163
5-59 Benefits of Stateful Firewalls 164
5-60 Creating a Firewall Rule 165
5-61 Network and Flood Protection 166
5-62 Controlling Edge Access 168
5-63 Lab 5: Configuring Profiles 169
5-64 Review of Learner Objectives 170
5-65 Key Points 171

Module 6 Site Configuration and Traffic Management 173

6-2 Importance 173
6-3 Module Lessons 173
6-4 Lesson 1: Site Configuration 174
6-5 Learner Objectives 174
6-6 General Workflow of Site Configuration 175
6-7 Configuring the Data Center Hub 176
6-8 Connecting the Edge to the Internet 177
6-9 Activating the Data Center Edge 178
6-10 Configuring the Private MPLS WAN Link 179
6-11 Adding a User-Defined WAN Overlay 180
6-12 Configuring a Route to Local Networks 181
6-13 Configuring Branch Sites 182
6-14 Enabling Tunnels Between Sites (1) 183
6-15 Enabling Tunnels Between Sites (2) 184
6-16 Overlay Flow Control 185
6-17 Lab 6: Configuring and Verifying Overlay Tunnels 186
6-18 Lab 7: Configuring Overlays for Cloud VPN 187

6-19 Review of Learner Objectives 188
6-20 Lesson 2: Routing in VMware SD-WAN 189
6-21 Learner Objectives 189
6-22 Routing in VMware SD-WAN 190
6-23 About Static Routing 191
6-24 Static Routes to Non-SD-WAN Destinations 192
6-25 About Route Redistribution 193
6-26 About OSPF 194
6-27 Configuring OSPF 195
6-28 About BGP 196
6-29 Configuring BGP in VMware SD-WAN 197
6-30 Configuring BGP from an Edge to the Underlay Neighbors 198
6-31 BGP Advanced Configuration 199
6-32 About Bidirectional Forwarding Detection 200
6-33 Advantages of Bidirectional Forwarding Detection 201
6-34 Bidirectional Forwarding Detection in VMware SD-WAN 202
6-35 Review of Learner Objectives 203
6-36 Lesson 3: Dynamic Multipath Optimization 204
6-37 Learner Objectives 204
6-38 About Dynamic Multipath Optimization 205
6-39 Features of Dynamic Multipath Optimization 206
6-40 About Link Steering 207
6-41 Link Steering Modes 208
6-42 Quality of Service and Class of Service 210
6-43 Overlay QoS-CoS Mapping 211
6-44 Configuring Priority and Service Class (1) 212
6-45 Configure Priority and Service Class (2) 213
6-46 On-Demand Remediation 214
6-47 Bandwidth Aggregation 215
6-48 Lab 8: Dynamic Multipath Optimization 216
6-49 Review of Learner Objectives 217
6-50 Key Points 218

Module 7 Monitoring, Testing, and Troubleshooting VMware SD-WAN ... 219

7-2 Importance 219
7-3 Module Lessons 219
7-4 Lesson 1: Monitoring VMware SD-WAN 220

7-5 Learner Objectives 220
7-6 Monitoring VMware SD-WAN 221
7-7 About Network Overview 222
7-8 Monitoring VMware SD-WAN Edge Appliances (1) 223
7-9 Monitoring VMware SD-WAN Appliances (2) 224
7-10 Monitoring Alerts 225
7-11 Configuring Alerts 226
7-12 Monitoring Events 227
7-13 About Auto Rollback 228
7-14 Monitoring Reports 229
7-15 Review of Learner Objectives 230
7-16 Lesson 2: Troubleshooting VMware SD-WAN 231
7-17 Learner Objectives 231
7-18 Test & Troubleshoot Features 232
7-19 About Remote Diagnostics 233
7-20 Viewing Diagnostics Information 234
7-21 Running Diagnostics Tests 235
7-22 Basic Troubleshooting 236
7-23 About Remote Actions 237
7-24 About Diagnostic Bundles 238
7-25 Requesting PCAP Bundles 239
7-26 Requesting Diagnostic Bundles 240
7-27 Review of Learner Objectives 241
7-28 Key Points 242

Module 1

Course Introduction

1-2 Course Introduction

1-3 Importance

The secure access service edge (SASE) platform offers an integrated solution framework for network and security services. SASE services are located in the cloud to deliver increased network intelligence, protection, and performance.

As a part of VMware SASE, VMware SD-WAN paves the way for the convergence of networking and security. With the current trends of cloud computing and remote working, organizations worldwide must reevaluate their existing enterprise networking and security architectures. By combining the principles of Cloud Delivered, Assured Application Performance, and Cloud-On-Ramp, VMware SD-WAN solves the problem of secure connectivity for enterprises.

1-4 Learner Objectives (1)

- Describe the advantages of using SD-WAN over traditional branch networking
- Discuss the VMware SASE architecture
- Describe the VMware SD-WAN traffic patterns, network flows, and software-defined networking approach
- Identify the core features of VMware SD-WAN and discuss how they improve operational automation
- List the names and functions of key VMware SD-WAN architecture components
- Illustrate the interactions between the VMware SD-WAN Edge, Orchestrator, and Gateway components
- Describe the process of activating a VMware SD-WAN Edge appliance

1-5 Learner Objectives (2)

- Describe the significance of VMware SD-WAN profiles
- Compare and contrast the function of overlays and underlays
- Summarize the procedure for configuring Dynamic Multipath Optimization
- Discuss the VMware SD-WAN platform deployment models
- Outline the best practices for deploying and managing VMware SD-WAN
- List the technologies used to monitor key performance indicators in VMware SD-WAN Orchestrator

1-6 Course Outline

1. Course Introduction
2. Introduction to the VMware SD-WAN Solution
3. VMware SD-WAN Components and Architecture
4. Using VMware SD-WAN Orchestrator
5. Configuring VMware SD-WAN
6. Site Configuration and Traffic Management
7. Monitoring, Testing, and Troubleshooting VMware SD-WAN

1-7 Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Use and Examples
`Monospace`	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: • Run the `esxtop` command. • ... found in the `/var/log/messages` file.
`Monospace Bold`	Identifies user inputs: • Enter **`ipconfig /release`**.
Boldface	Identifies user interface controls: • Click the **Configuration** tab.
Italic	Identifies book titles: • *vSphere Virtual Machine Administration*
< >	Indicates placeholder variables: • <ESXi_host_name> • ... the `Settings/<Your_Name>.txt` file

1-8 References

Title	Location
VMware SD-WAN Administration Guide	https://docs.vmware.com/en/VMware-SD-WAN/index.html
Dynamic Multipath Optimization	http://wan.velocloud.com/rs/098-RBR-178/images/sdwan-678-dynamic-multipath-optimization-wp-1119.pdf
VMware SD-WAN Delivers Automated Network Segmentation for the Enterprise	https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-589-automated-network-segmentation-wp-1220.pdf
"VMware SD-WAN Edge Platform Specifications"	https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf
VMware knowledge base article 2828742	https://kb.vmware.com/s/article/2828742

1-9 VMware Online Resources

Documentation for VMware SASE: https://docs.vmware.com/en/VMware-SASE/index.html

Documentation for VMware SD-WAN: https://docs.vmware.com/en/VMware-SD-WAN/index.html

VMware Communities: https://communities.vmware.com

- Start a discussion.
- Access the knowledge base.
- Access documentation, technical papers, and compatibility guides.
- Access communities.
- Access user groups.

VMware Support: http://www.vmware.com/support

VMware Hands-on Labs: http://hol.vmware.com

VMware Learning: http://www.vmware.com/learning

- Access course catalog.
- Access worldwide course schedule.

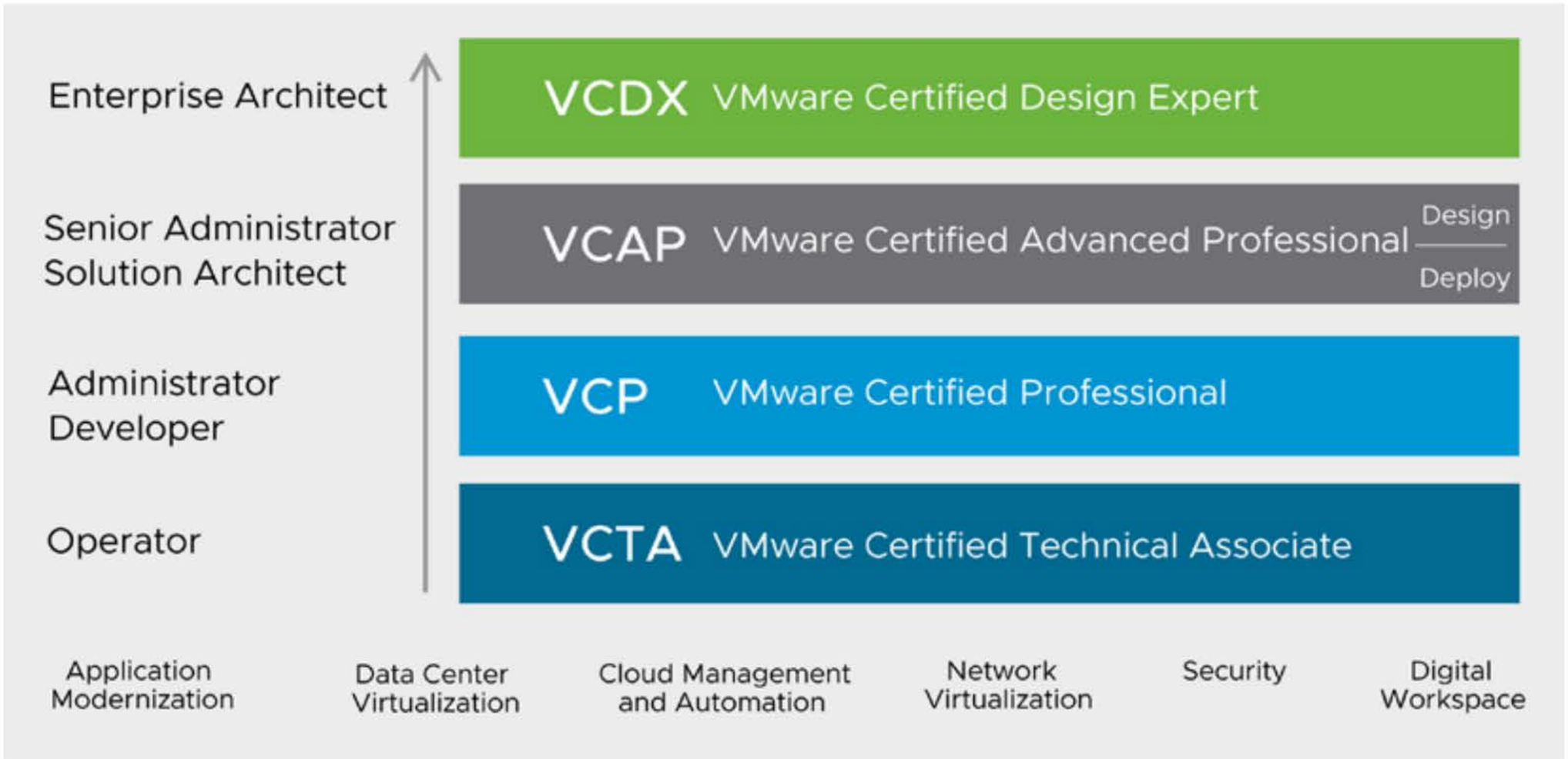
1-10 VMware Learning Overview

You can access the following Education Services:

- VMware Learning Paths:
  - Help you find the course that you need based on the product, your role, and your level of experience
  - Can be accessed at https://vmware.com/learning
- VMware Customer Connect Learning, which is the official source of digital training, includes the following options:
  - On Demand Courses: Self-paced learning that combines lecture modules with hands-on practice labs
  - VMware Lab Connect: Self-paced, technical lab environment where you can practice skills learned during instructor-led training
  - Certification Exam Prep: Comprehensive video-based reviews of exam topics and objectives to help you take your certification exam
- For more information, see https://vmware.com/learning/connect-learning.

1-11 VMware Certification Overview

VMware certifications validate your expertise and recognize your technical knowledge and skills with VMware technology.



VMware certification sets the standards for IT professionals who work with VMware technology. Certifications are grouped into technology tracks. Each track offers one or more levels of certification (up to four levels).

For the complete list of certifications and details about how to attain these certifications, see https://vmware.com/certification.

1-12 VMware Credentials Overview

VMware badges are digital emblems of skills and achievements. Career certifications align to job roles and validate expertise across a solution domain. Certifications can cover multiple products in the same certification.

Specialist certifications and skills badges align to products and verticals and show expanded expertise.

Digital badges have the following features:

- Easy to share in social media (LinkedIn, Twitter, Facebook, blogs, and so on)
- Validate and verify achievement
- Contain metadata with skill tags and accomplishments
- Based on Mozilla's Open Badges standard

For the complete list of digital badges, see http://www.pearsonvue.com/vmware/badging.

Module 2

Introduction to the VMware SD-WAN Solution

2-2 Importance

To understand the challenges that VMware SD-WAN solves, you must understand its function and its purpose.

2-3 Module Lessons

1. Reviewing Traditional WAN Technology
2. Introduction to VMware SASE
3. Introduction to the VMware SD-WAN Solution

2-4 Lesson 1: Reviewing Traditional WAN Technology

2-5 Learner Objectives

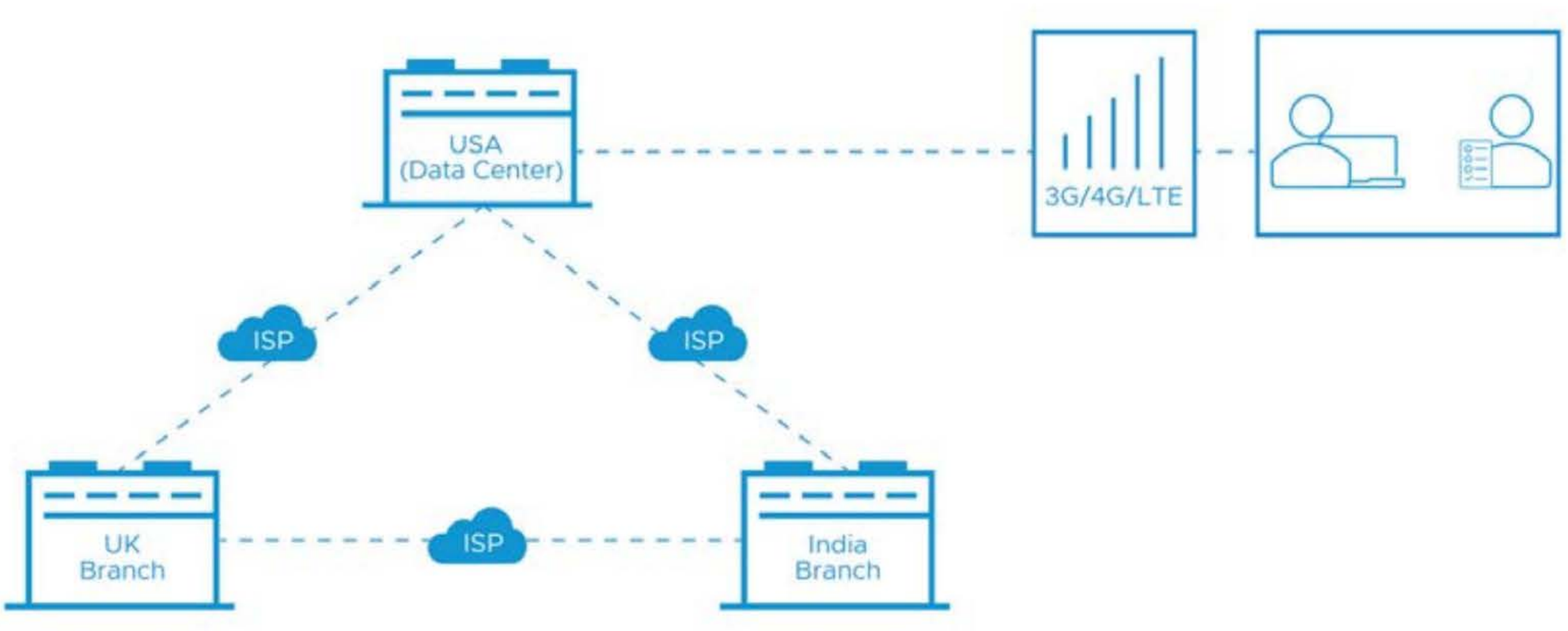
- Define the terminologies used in relation to traditional WAN technology
- Review the traditional WAN technologies and available options
- Recognize the disadvantages of traditional WAN technologies

2-6 Introduction to WAN Technology

A WAN connects two or more networks that are geographically dispersed. WANs use infrastructure provided by telcos, satellites systems, network providers, and so on. You manage a LAN infrastructure, whereas you typically lease a WAN infrastructure from a service provider.

WANs are usually required to establish remote connectivity in the following instances:

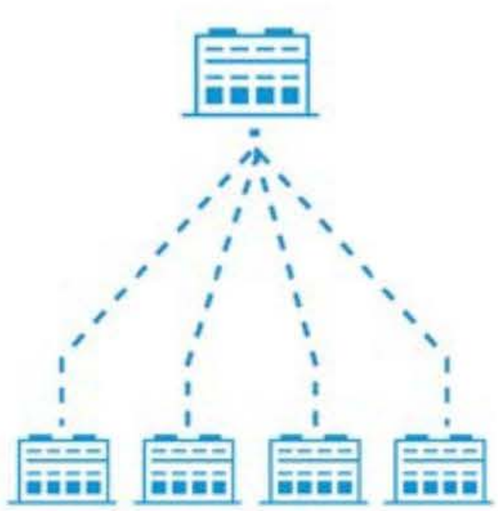
- Between central and branch offices
- Between different organizations
- Between remote employees and corporate networks and resources



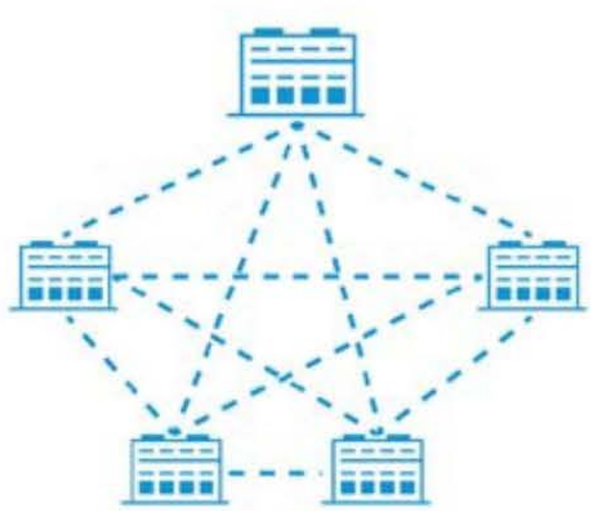
2-7 WAN Topologies

WANs supports the following network topologies:

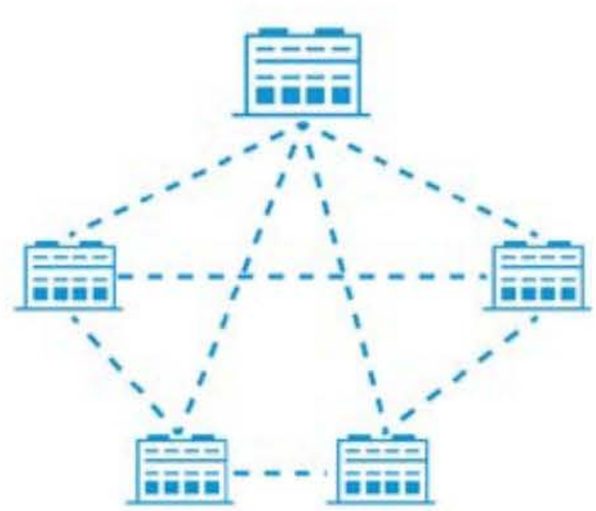
- Hub-and-spoke topology
- Full-mesh topology
- Partial-mesh topology



Hub-and-Spoke Topology



Full-Mesh Topology



Partial-Mesh Topology

2-8 WAN Connection Types

The following types of connections are available in traditional WANs:

- Leased lines
- Packet switching
- Circuit switching

The following types of connections are available in traditional WANs:

- Leased lines:
  - Leased lines are dedicated circuits between two or more geographically separate sites.
  - A leased line is a private circuit provided by the ISP.
- Packet switching:
  - Packet switching uses a digital network to transfer data in the form of packets.
  - It is cheaper than circuit switching and leased lines.
  - It is also more efficient, more scalable, and easier to implement than circuit switching.
  - Most modern computer communications use packet switching.
- Circuit switching:
  - Circuit switching is a method in which two devices establish a dedicated physical circuit for communication.
  - The devices create the circuit as needed before the communication occurs.
  - Full bandwidth is guaranteed between the two devices, and the connection remains intact during the communication session.
  - Analog telephone networks are classic examples of circuit switching.

2-9 Popular WAN Technologies

You can use the following technologies to set up WAN connections:

- Metropolitan area network
- Multiprotocol Label Switching
- Cellular networks (3G, 4G, LTE)
- (Asymmetric) digital subscriber line
- Cable Internet

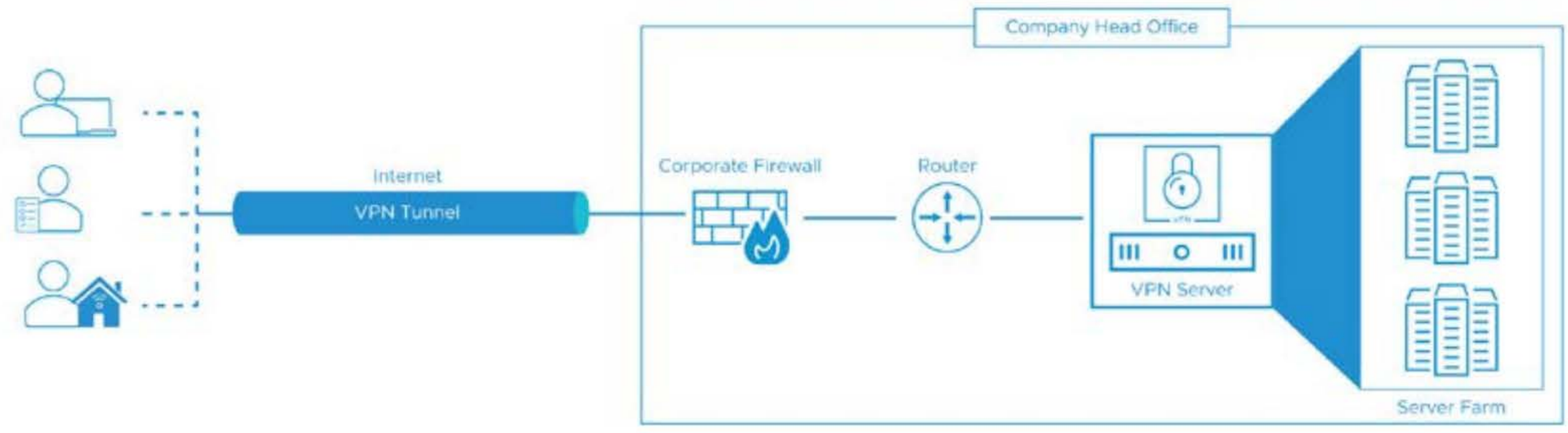
The following examples are some of the many options available for setting up WAN connections:

- Metropolitan area network (MAN):
  - Provides point-to-point or multipoint connectivity services over a metropolitan area
  - Replaces low-speed WAN technologies
- Multiprotocol Label Switching (MPLS):
  - Uses labels instead of source and destination addresses
  - Performs direct routing of IPv4 and IPv6 and tunneling of other protocols
  - Supports various WAN options, such as digital subscriber line, Asynchronous Transfer Mode, and so on
- Cellular networks:
  - Enables wireless Internet access for end-user devices
  - Provides access at any time, regardless of the user's location
- (Asymmetric) digital subscriber line:
  - Transfers digital data over telephone lines
  - Enables phone lines to transfer both voice and digital data simultaneously
- Broadband cable Internet:
  - Uses the same infrastructure as cable television
  - Shares the bandwidth between the subscribers, which makes it cheaper and more readily available for home Internet users

2-10 Virtual Private Networks

A VPN provides a highly secure connection between the user device and the remote network. For example, an employee can connect to the resources and network of the company using a VPN.

A VPN makes the device appear as if it is locally connected to the corporate network even though the device is geographically remote. In WAN connections, by comparison, the remote LANs see each other as remote networks.



VPNs also provide the following benefits:

- Reduced cost
- Scalability
- Security
- Flexibility with Internet connections

2-11 Disadvantages of Traditional WANs

Modern application designs have the following requirements:

- Continuous access to resources
- Portable access from any location
- Evolving cloud technologies

Traditional WANs have many unfavorable aspects:

- Decentralized configuration
- Manual configuration and management
- Minimal flexibility
- Inefficient use of resources

2-12 Review of Learner Objectives

- Define the terminologies used in relation to traditional WAN technology
- Review the traditional WAN technologies and available options
- Recognize the disadvantages of traditional WAN technologies

2-13 Lesson 2: Introduction to VMware SASE

2-14 Learner Objectives

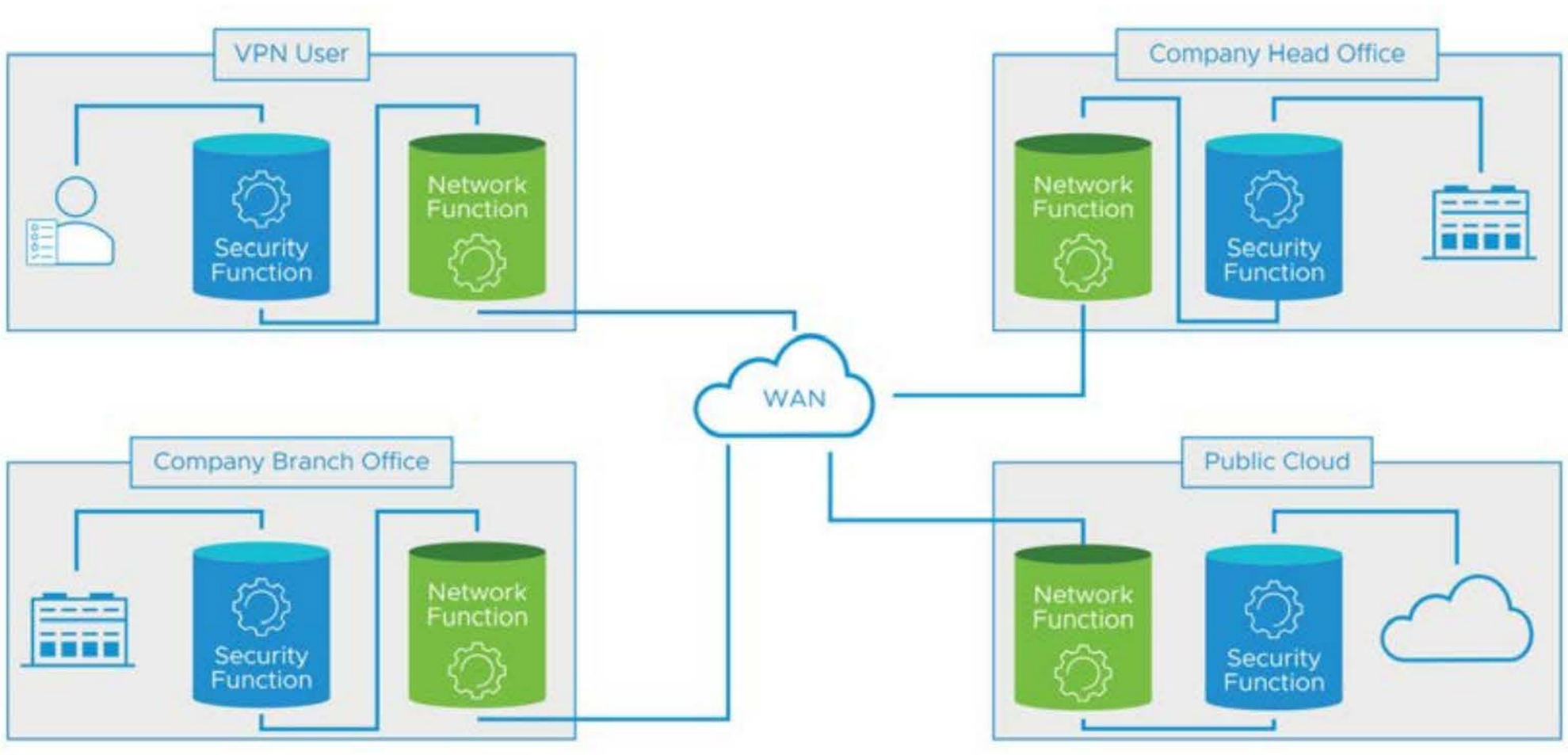
- Identify the need for SASE
- List the components of VMware SASE
- Describe VMware SASE PoP

Technet24

2-15 Modern Security and Performance Challenges

Modern IT users require the ability to access services such as Microsoft Office 365, Amazon Web Services, VPNs, and so on from any location and at any time. This requirement poses new expectations for increased security and performance.

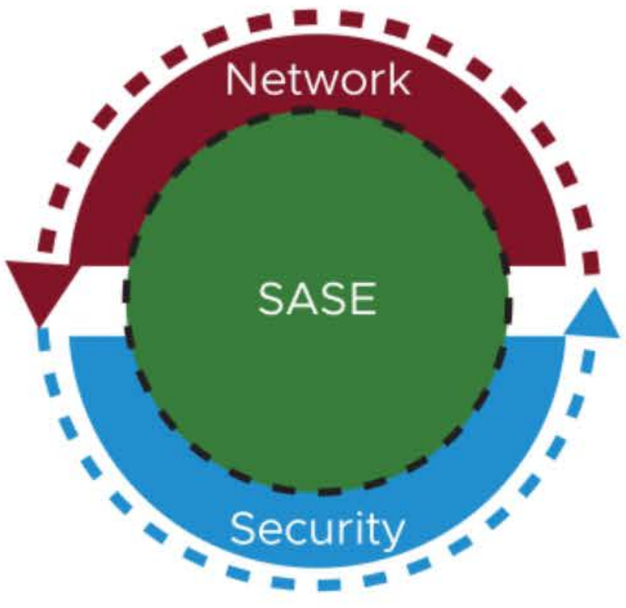
Networking and security functions traditionally operate independently from each other, which makes configuration complicated and outdated. As a result of outdated designs, the applications can experience degraded performance and compromised security.



2-16 About SASE

Secure access service edge (SASE) offers an integrated solution framework for network and security services. SASE integrates network and security functions into a single service for cloud-based applications, which simplifies configuration. It also improves application performance by more efficiently utilizing the network bandwidth with enhanced security.

SASE services are located in the cloud to deliver increased network intelligence, protection, and performance.



Technet24

2-17 VMware SASE

The VMware SASE solution integrates WAN and security services into a cloud-delivered service model. As a result, organizations can connect users to applications from any location.

VMware SASE offers the following benefits:

- Simple configuration
- Flexibility
- Agility
- Scalability for enterprises of all sizes
- High performance
- Enhanced security
- VMware Edge Network Intelligence machine learning

2-18 Components of the VMware SASE Solution

The SASE solution offered by VMware includes the following components:

- Software-defined wide-area network (SD-WAN)
- Secure access with Zero Trust Network Access
- Cloud web security:
  - Secure web gateway
  - Cloud access security broker
  - Data loss prevention
  - Remote browser isolation
- Cloud firewall:
  - Intrusion detection system
  - Intrusion prevention system
  - Firewall as a service

The SASE solution offered by VMware includes the following components:

- A software-defined wide-area network (SD-WAN) removes direct dependency of networking services from traditional WAN infrastructures. As a result, application traffic flows independently from underlying WAN connections.
- Zero Trust Network Access (ZTNA) provides security through a trust-no-one approach. In contrast to network-centric security, ZTNA security is based on identity, location, and context.
- A secure web gateway enforces policy-based controls for accessing the web while protecting against malware.
- A cloud access security broker ensures that all endpoints comply with enterprise cloud security policies.
- Data loss prevention refers to processes and tools that protect against the loss or misuse of sensitive data.
- Remote browser isolation creates a remote, virtual network location while browsing the web, which prevents malware or viruses from entering the user's device or network.
- An intrusion detection system reports and flags cybersecurity threats by analyzing network traffic and inspecting packets.
- An intrusion prevention system reports and proactively blocks malicious activities by analyzing network packets.
- Firewall as a service secures network traffic through centralized enterprise policies as a cloud-based service.

Technet24

2-19 SASE Use Cases

SASE is the ideal solution for several use cases:

- Remote work
- Cloud migration
- Branch connectivity

2-20 VMware SASE PoP

VMware SASE uses point-of-presence (PoP) locations that are unique to the VMware SASE platform. These cloud devices are strategically deployed and highly available.

VMware SASE PoP devices are used by all VMware SASE services, including VMware SD-WAN, VMware Cloud Web Security, and VMware Secure Access.

VMware SASE PoP locations provide the closest and most optimized hand-off traffic to application tenant locations. These horizontally scalable cloud devices offer the added benefit of real-time monitoring, dynamic traffic steering, and link remediation.

Technet24

2-21 Review of Learner Objectives

- Identify the need for SASE
- List the components of VMware SASE
- Describe VMware SASE PoP

2-22 Lesson 3: Introduction to the VMware SD-WAN Solution

2-23 Learner Objectives

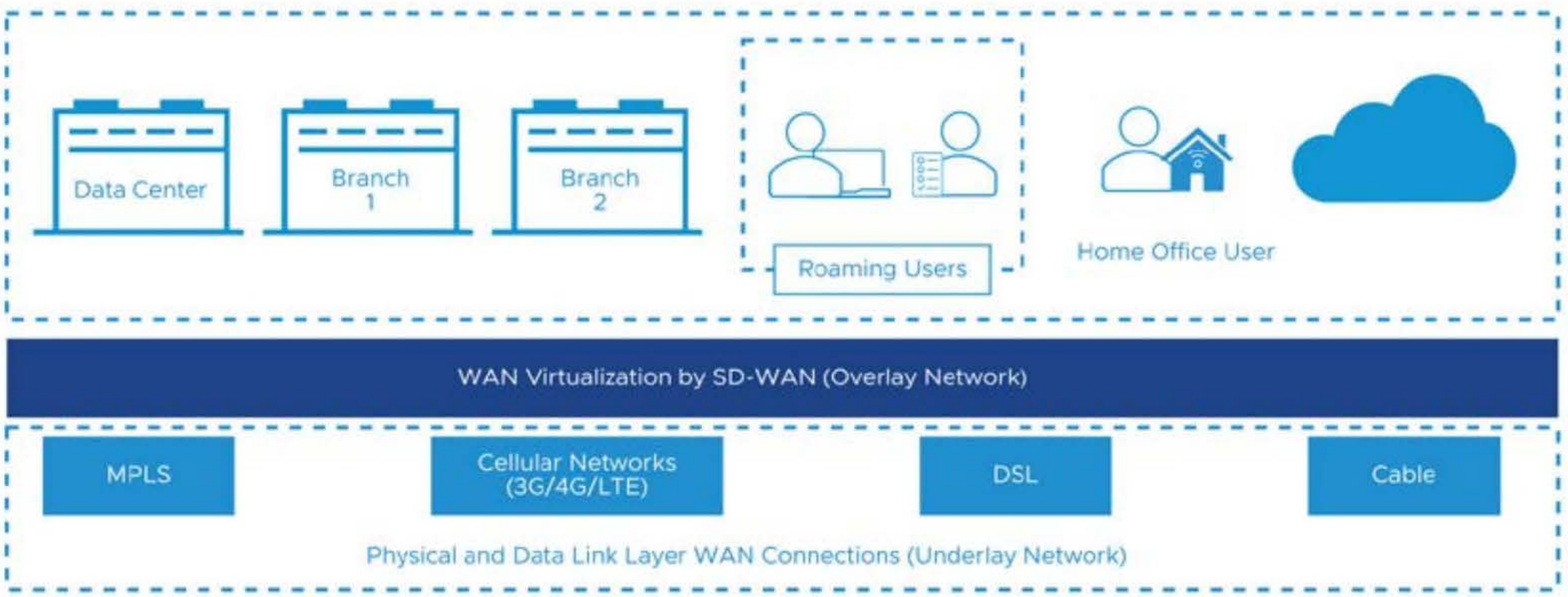
- Describe the function of an SD-WAN
- Identify the capabilities and benefits of the VMware SD-WAN solution

Technet24

2-24 About SD-WAN Solutions

An SD-WAN does not replace the physical connection used in a traditional WAN. Instead, an SD-WAN creates a virtualized network overlay by decoupling network software services from the underlying hardware.

SD-WANs offer enhanced control, flexibility, performance, security, and scalability. They are well suited for modern data traffic patterns between branch offices, remote users, cloud services, and data centers.



SD-WANs do not replace the physical connections provided by ISPs, such as frame relay, leased lines, and so on. SD-WANs create virtualized network overlays by decoupling network software services from underlying hardware. SD-WANs also have the benefit of ease of deployment, central management and control, and assured application performance.

2-25 VMware SD-WAN Capabilities

The VMware SD-WAN solution offers several important capabilities:

- Automation and orchestration
- Performance and reliability
- Cloud network
- Virtual services

The VMware SD-WAN solution offers the following capabilities:

- Automation and orchestration:
  - Provides automated zero-touch branch deployment
  - Allows users to monitor the network and applications in real time
- Performance and reliability:
  - Achieves higher performance for critical applications by aggregating bandwidth (of broadband, 4G LTE, MPLS, and so on) without affecting the overall cost
  - Provides packet steering and on-demand remediation
- Cloud network:
  - Manages the transfer of data and provides direct access to cloud and on-premises resources
  - Creates a distributed network deployed by VMware and ISPs to support optimal connectivity to cloud and enterprise data centers
  - Enables access to cloud applications, infrastructure as a service (IaaS), and software as a service (SaaS)
- Virtual services:
  - Consolidates multiple virtualized network functions into a single appliance
  - Enables the elimination of multiple appliances that host single functions

Technet24

2-26 VMware SD-WAN Benefits

VMware SD-WAN provides several benefits:

- Simplified WAN management:
  - Centralized SD-WAN management
  - Zero-touch deployment
  - Separation of network services from a physical WAN connection
- Assured application performance, with stronger and more granular control over traffic
- Managed on-ramp to the cloud:
  - Supports the migration of applications to the cloud
  - Provides the same performance, simplification, and security benefits as cloud-based applications

2-27 VMware Dynamic Multipath Optimization

Dynamic Multipath Optimization is an advanced traffic-management feature. It provides the following functions:

- Continuous link monitoring
- Dynamic per-packet steering
- On-demand remediation

The VMware SD-WAN solution also provides a response time that is 10 times faster than other SD-WAN solution providers.

Speed Comparison: 50 MB File Transferred over Dual 20 Mbps Links

Packet Loss	Without VMware SD-WAN	With VMware SD-WAN
No loss	22 seconds	12 seconds
2% packet loss	134 seconds	13 seconds

Dynamic Multipath Optimization provides the following functionalities:

- Continuous link monitoring drives automation and optimization.
- Dynamic per-packet steering provides sub-second steering without session drops as well as aggregated bandwidth for single flows.
- On-demand remediation provides protection against concurrent degradation of multiple links and enables single-link performance.

Technet24

2-28 Review of Learner Objectives

- Describe the function of an SD-WAN
- Identify the capabilities and benefits of the VMware SD-WAN solution

2-29 Key Points

- Traditional WANs cannot efficiently service the requirements of modern traffic patterns, such as cloud-bound and work-from-anywhere traffic.
- SD-WAN technology uses virtualized network overlays to make efficient use of traditional WANs and their underlying hardware.
- VMware SASE is a framework that offers security and network functions as a single service.

Questions?

Technet24

Module 3

VMware SD-WAN Components and Architecture

3-2 Importance

VMware SD-WAN is a complex technology. To understand its functionality, you must understand its components as well as their interactions and architecture.

3-3 Module Lessons

1. VMware SD-WAN Edge
2. VMware SD-WAN Orchestrator
3. VMware SD-WAN Gateway
4. VMware SD-WAN Component Interactions

3-4 Lesson 1: VMware SD-WAN Edge

3-5 Learner Objectives

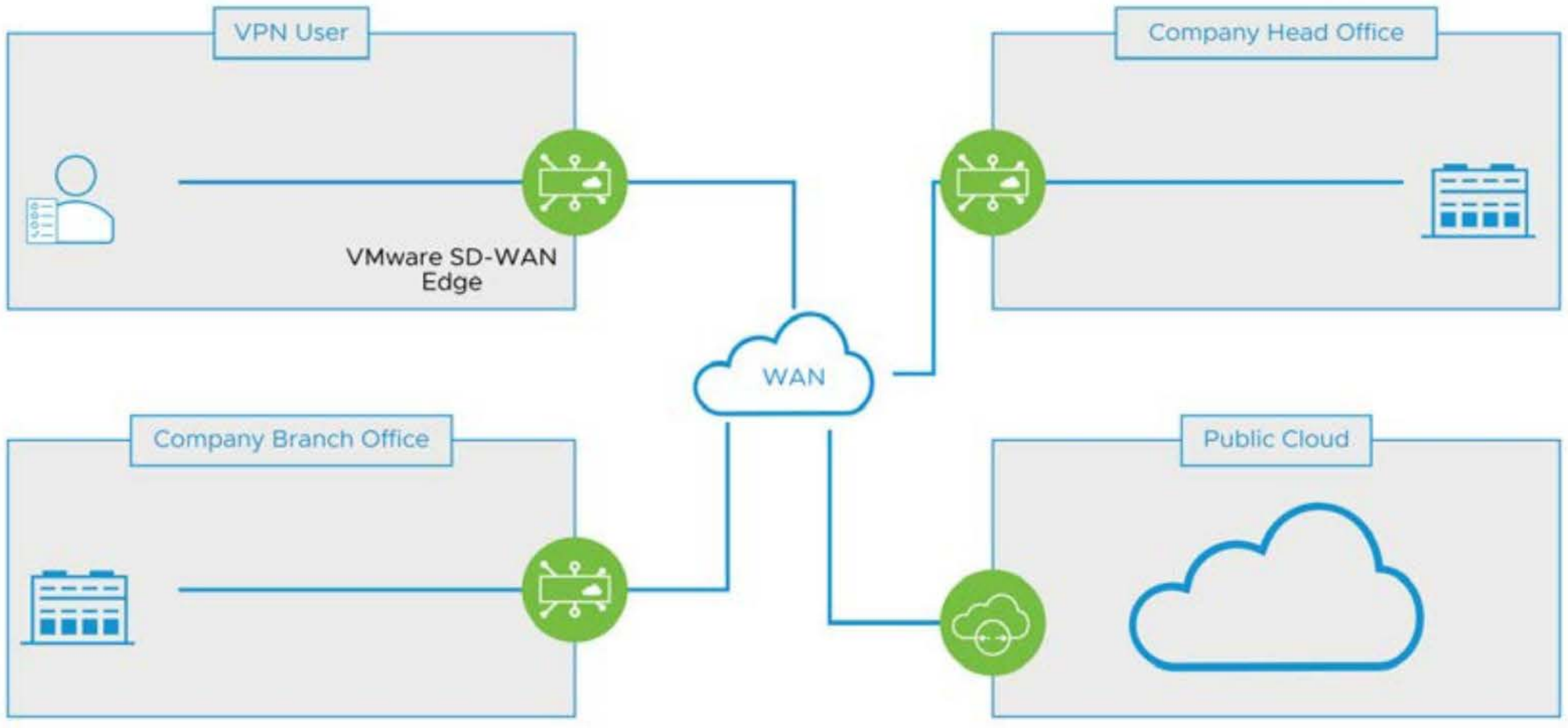
- Identify the role of VMware SD-WAN Edge appliances
- Describe the functions of underlay and overlay networks
- List the use cases for deploying edges as hubs
- Identify the features of VMware SD-WAN Edge

Technet24

3-6 About VMware SD-WAN Edge

VMware SD-WAN Edge is an enterprise-class appliance that establishes a secure virtual network between the data center, branches, cloud, and remote users. This secure virtual network is known as an overlay network.

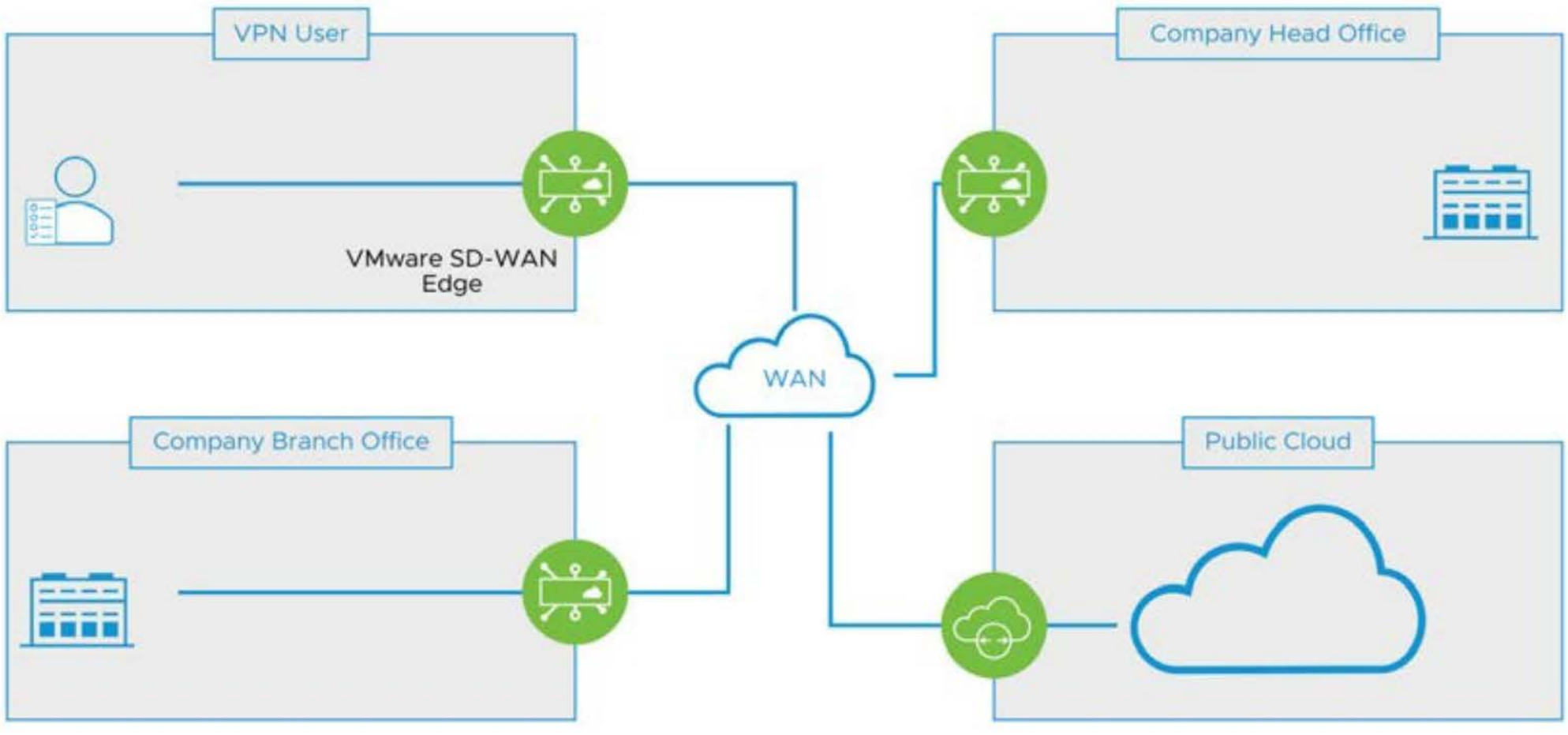
The purpose of the overlay network is to provide an optimized connection to private, public, and hybrid applications as well as to the compute and virtualized services.



3-7 Advanced Features of VMware SD-WAN Edge

VMware SD-WAN Edge aggregates multiple broadband links (for example, cable, DSL, and 4G-LTE) at the branch office and sends the traffic to VMware SD-WAN Gateway. You can deploy VMware SD-WAN Edge appliances at the customer premises, such as data centers, branches, or home offices, as well as through infrastructure-as-a-service (IaaS) platforms, such as Amazon Web Services or Microsoft Azure.

Edges receive all policies and configurations from VMware SD-WAN Orchestrator. They classify traffic with a deep-packet application recognition engine and then apply policies based on real-time link quality. VMware SD-WAN Edge makes traffic-steering decisions locally.



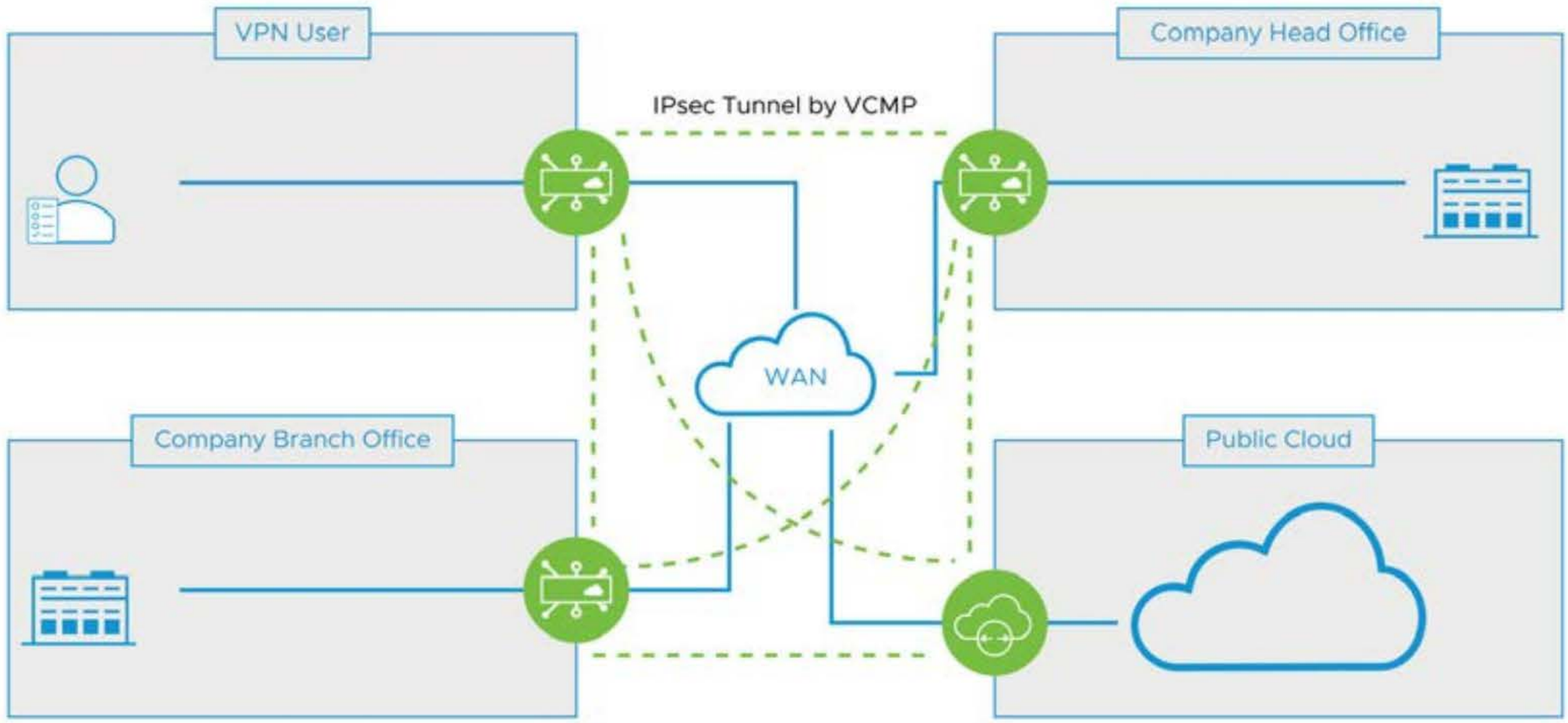
VMware SD-WAN Edge aggregates multiple broadband links, including cable, digital subscriber line, and 4G-LTE.

Technet24

3-8 VeloCloud Multipath Protocol

VMware SD-WAN uses VeloCloud Multipath Protocol (VCMP) to create VCMP tunnels over any kind of transport. These VCMP tunnels can be created from edge-to-edge, edge-to-hub, or edge-to-gateway connections.

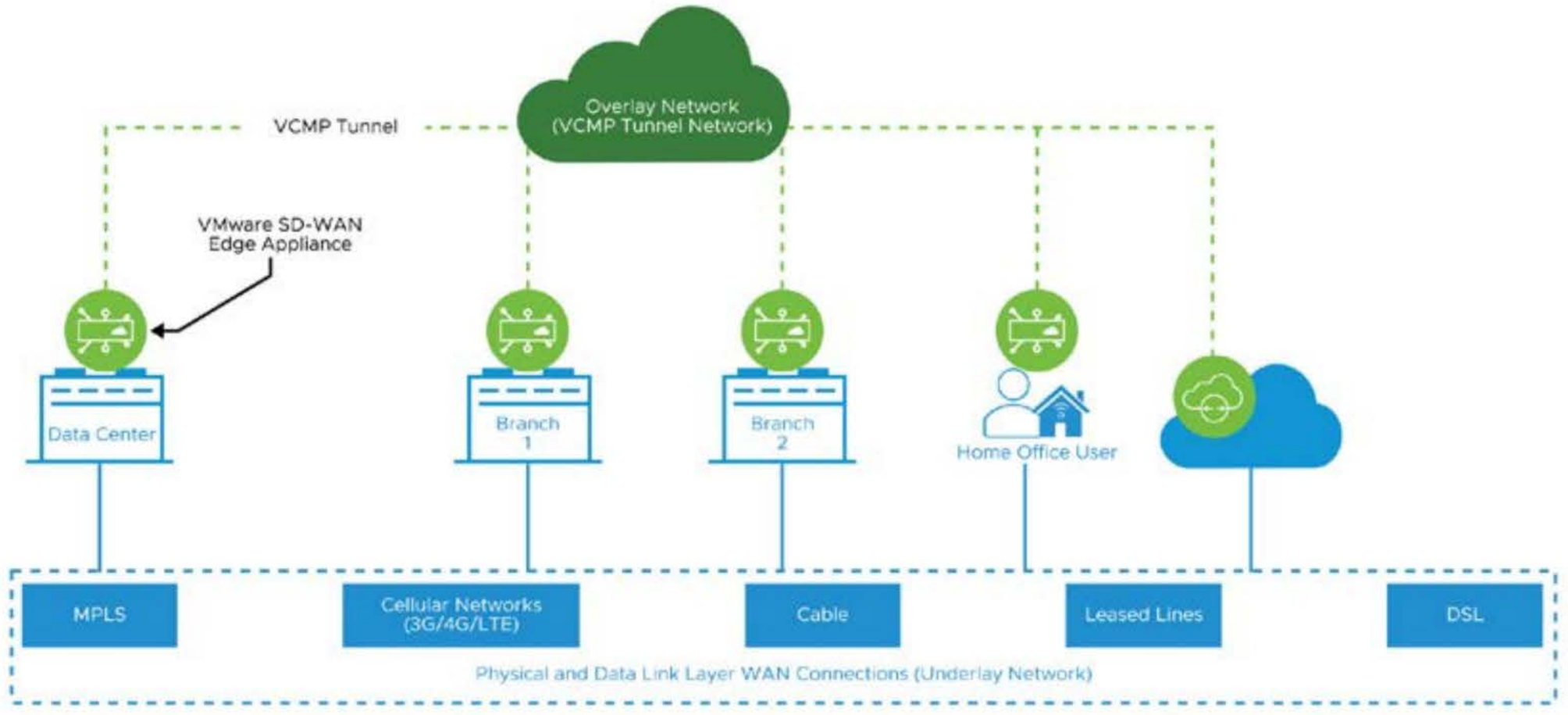
VCMP tunnels provide an abstraction layer from the underlying transport. If necessary, the VCMP traffic can be encrypted using an Internet Protocol Security (IPsec) tunnel.



VCMP uses the Internet Assigned Numbers Authority (IANA) registered UDP port 2426.

3-9 About the Underlay Network

The WAN infrastructure provided by a service provider is known as the underlay network. The WAN connections function at the physical and data link layers of the Open Systems Interconnection (OSI) model. An SD-WAN decouples the network software services from the underlying hardware to create a virtual WAN connection.

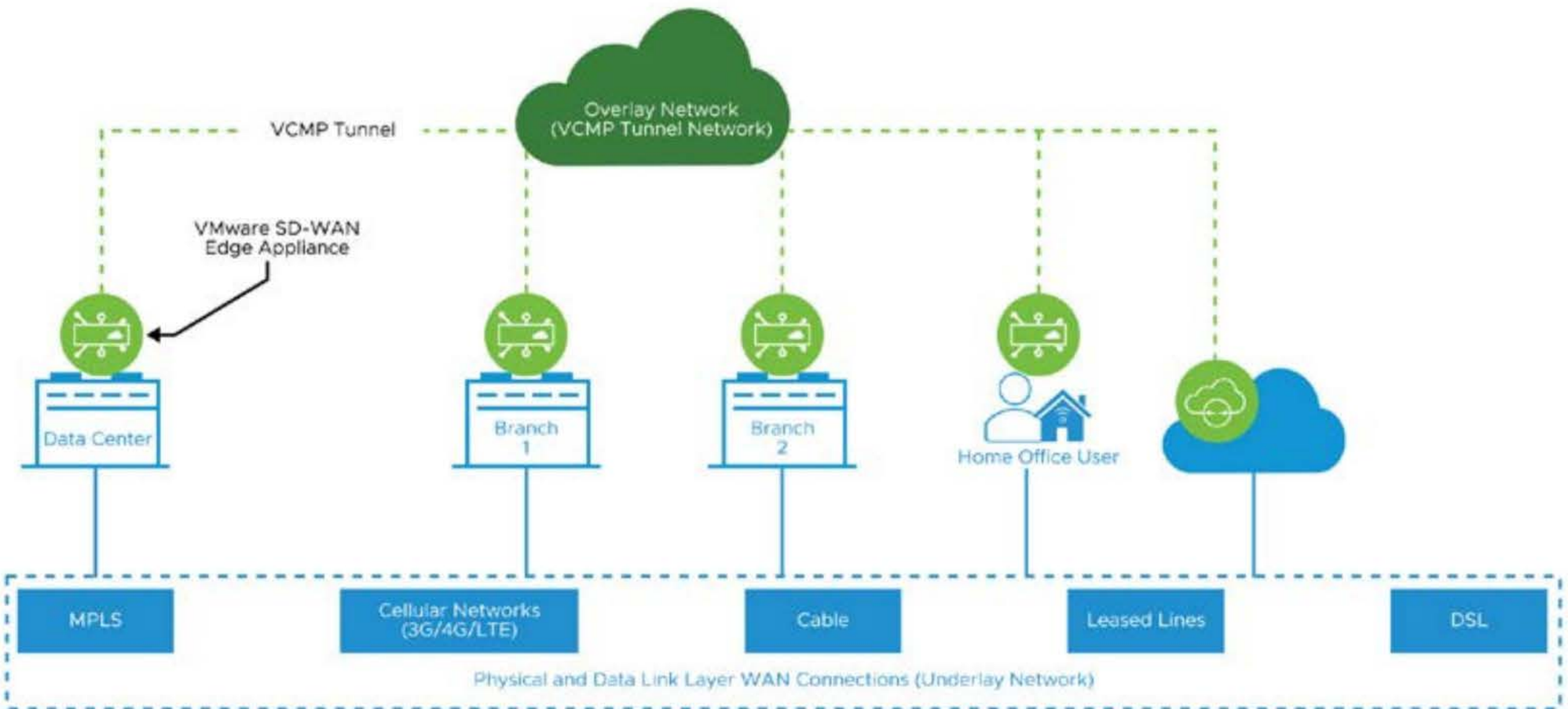


Technet24

3-10 About the Overlay Network

VMware SD-WAN virtualizes the WAN connection provided by service providers. It creates an overlay network with the help of VMware SD-WAN Edge. The overlay network determines all routing and traffic-management decisions.

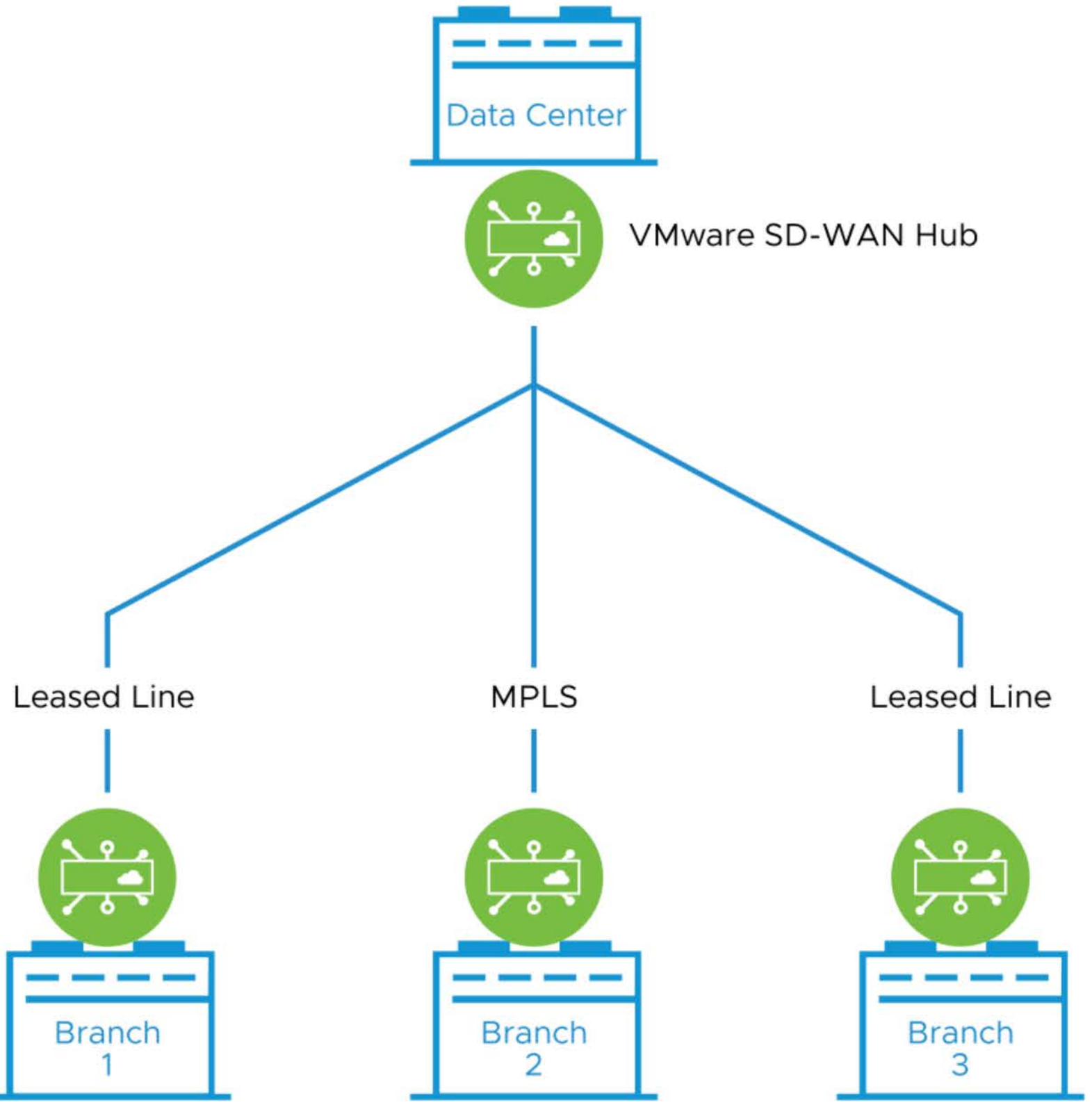
The overlay network uses the underlay network as a medium for transporting data. If the overlay network breaks and communication is interrupted, the SD-WAN reverts to the underlay network.



3-11 About VMware SD-WAN Hubs

A large-capacity edge device can be deployed as a VMware SD-WAN hub. Hubs terminate the traffic coming from VMware SD-WAN Edge devices deployed at branch offices or from VMware SD-WAN Gateway instances.

For each of the branch offices, an interface on the hub device is connected to a WAN link.

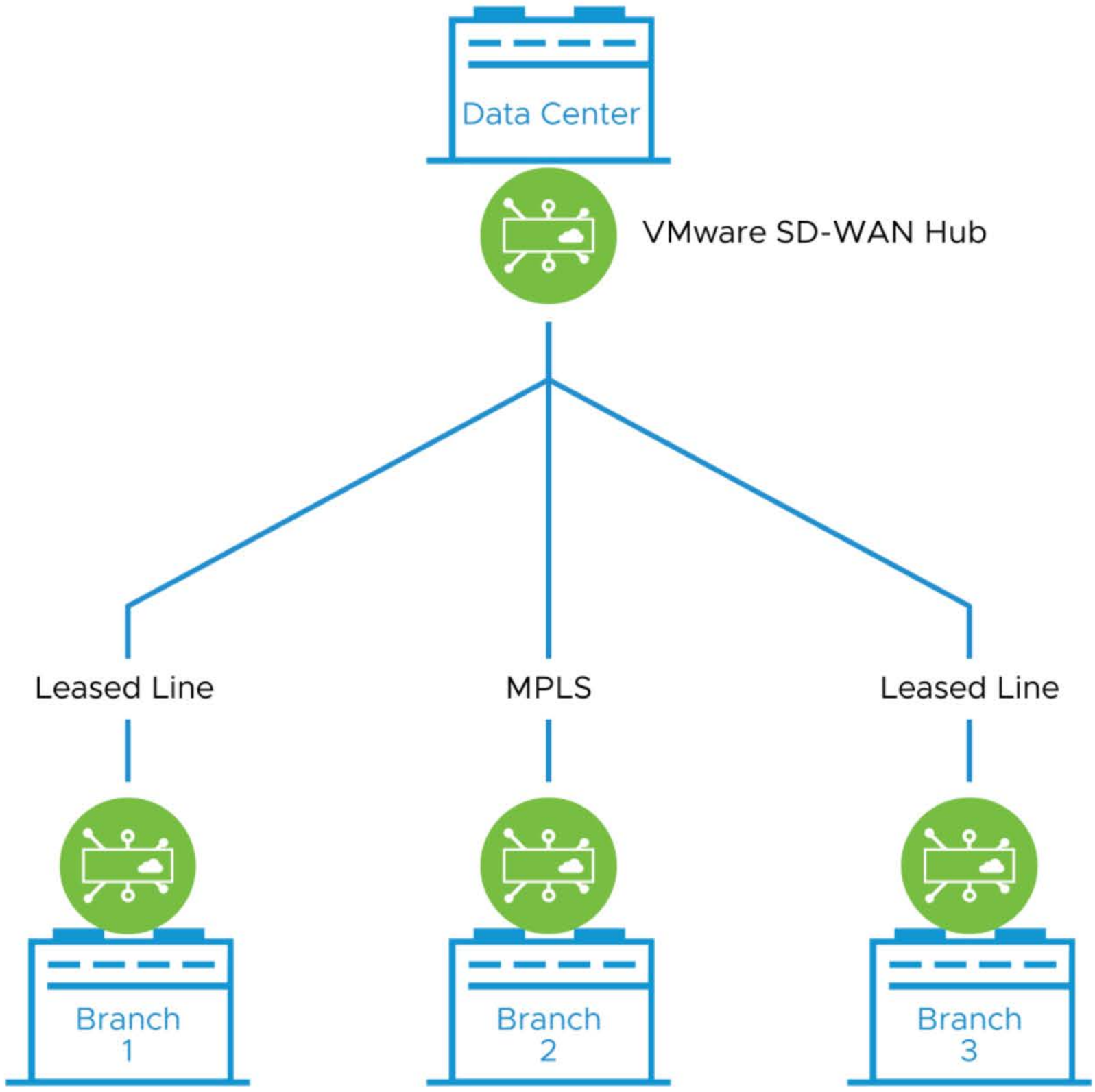


Technet24

3-12 Use Cases for VMware SD-WAN Hubs

You can use VMware SD-WAN hubs for the following purposes:

- Establish branch-to-data-center connectivity to access data center resources and applications
- Use hubs for Internet backhaul
- Establish branch-to-branch connectivity when a direct branch-to-branch VPN is not available



3-13 High Availability Design Options for Branches

Standard high availability:

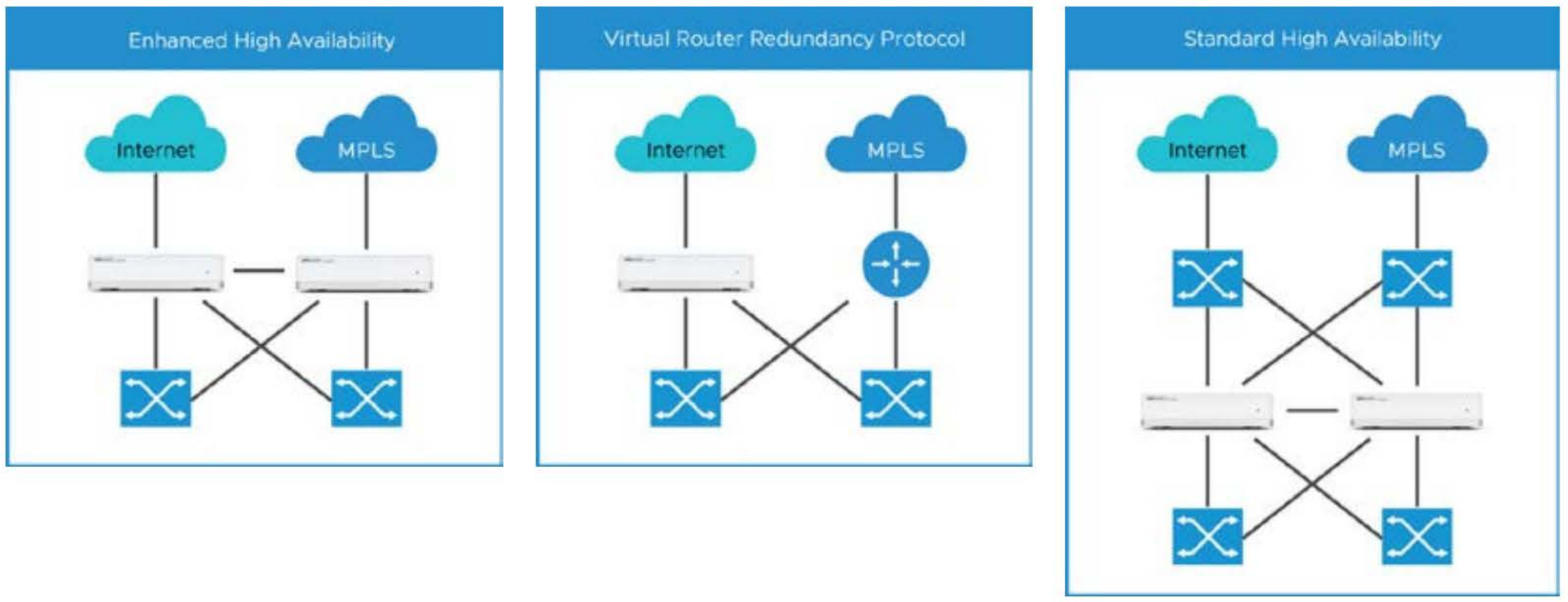
- Hardware redundancy
- Upstream switch requirement
- Standby unit syncs to the active unit

Enhanced high availability:

- Same benefits as standard high availability
- Upstream L2 switch elimination
- Both edge and link failure can trigger high availability failover

Virtual Router Redundancy Protocol (VRRP):

- Edge is the primary VRRP
- Failover to Multiprotocol Label Switching (MPLS) customer equipment router
- Often used during migrations



Technet24

3-14 High Availability Design Options for Data Centers and Hubs

Standard and enhanced high availability:

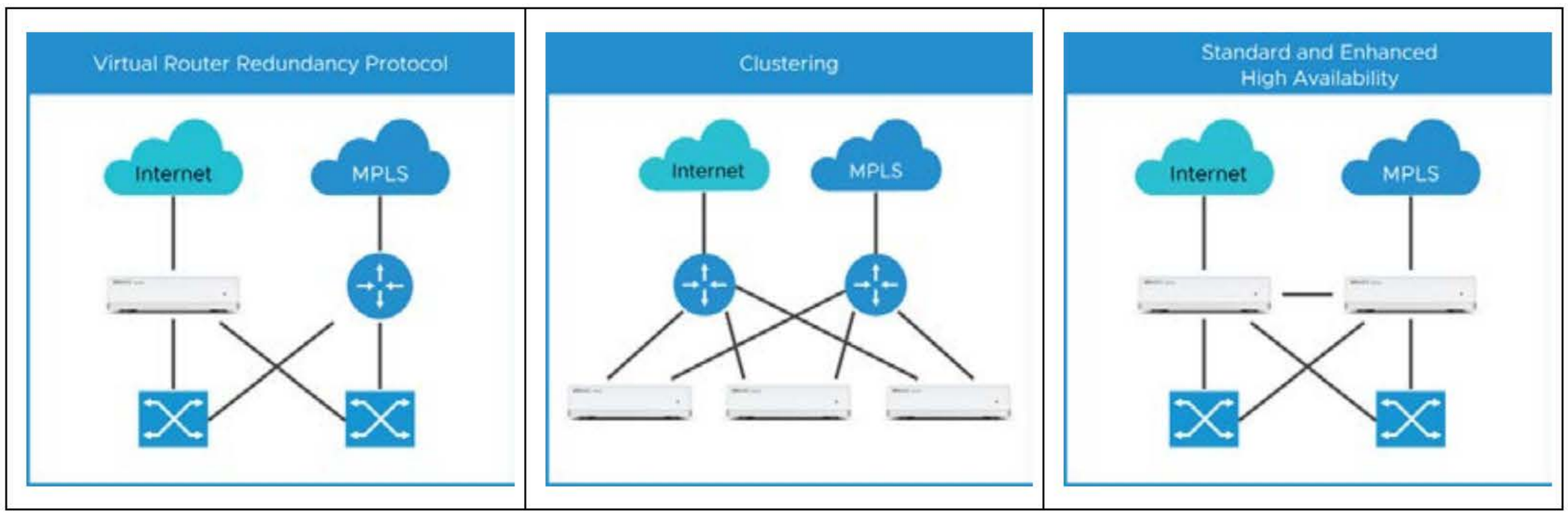
- Hardware redundancy
- Standby unit syncs to the active unit

VRRP:

- Edge is the primary VRRP
- Failover to MPLS customer equipment router
- Often used during migrations

Clustering:

- Data center scale-out and redundancy option
- All edge devices are active
- Border Gateway Protocol is used to synchronize control plane



3-15 Versions of VMware SD-WAN Edge

VMware SD-WAN Edge is available both as hardware-based devices and as software-based appliances.

Physical VMware SD-WAN Edge devices are available in multiple form factors based on the scale of the infrastructure:

- Small branch
- Medium branch
- Large branch or data center

As a software-based appliance, VMware SD-WAN Edge is available in the following options:

- Virtual appliance
- Cloud marketplace

Small Branch

Medium Branch

Large Branch or Data Center

The image in the slide is not an exhaustive representation of the hardware models available.

You can install a virtual edge on a kernel-based virtual machine (KVM) or ESXi hypervisor. See the chapter about virtual VMware SD-WAN Edge deployment in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

Technet24

3-16 Subscription Options

VMware SD-WAN software is available in several subscription editions, with different features available for a wide variety of use cases. The different subscription editions are as follows:

- Standard
- Enterprise
- Premium

VMware SD-WAN is also licensed by bandwidth tier. For more information about the VMware SD-WAN subscription editions, see "VMware SD-WAN Edge Platform Specifications" at https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-712-edge-platform-spec-ds-1020.pdf.

3-17 VMware SD-WAN Edge Software Features

VMware SD-WAN Edge software offers a wide variety of features:

- Support for software as a service (SaaS) and IaaS
- Authentication, authorization, and accounting
- High availability
- Link and bandwidth aggregation
- Zero-touch provisioning
- Dynamic Multipath Optimization
- Routing
- Multitenancy
- Deployment flexibility
- Quality of service
- Remote troubleshooting
- Wide range of security features
- Port security
- VLAN tagging
- WAN overlay support
- Network services
- Support for APIs
- Monitoring

Technet24

VMware SD-WAN Edge software offers the following features:

- Support for software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) models:
  - Improved performance for cloud apps
  - Support for well-known IaaS (Amazon Web Services, Microsoft Azure, Google Cloud Platform)
  - VMware Cloud Web Security (including Check Point, Zscaler, Palo Alto Networks, Netskope, Menlo Security, Websense, and OpenDNS)
- Authentication, authorization, and accounting: RADIUS, local authentication and authorization, multitenant three-tier role-based access control (RBAC) architecture, auditing, roles, and privileges
- High availability: Disaster recovery for VMware SD-WAN Orchestrator, WAN multilinking, VMware SD-WAN Edge clustering
- Dynamic Multipath Optimization: Application and network condition-aware sub-second steering, jitter and packet loss correction, fast intelligent routing, intelligent gateway selection, link aggregation, TCP flow optimization, unidirectional link measurements, bandwidth detection
- Routing: Open Shortest Path First Protocol, Border Gate Protocol, static routes, connected networks, ICMP probes and responders, overlay flow control, per-packet application-aware steering, route filtering, route redistribution
- Multitenancy: VMware SD-WAN Controller, VMware SD-WAN Gateway, VMware SD-WAN Orchestrator
- Deployment flexibility: No pre-staging, no CLI, group policies, consolidated ICOM and end-customer dashboard, Virtual Network Function form factor, multitenant stateless headend, transport group for business policy abstraction, application-aware service insertion on premises or in the cloud, Return Merchandise Authorization workflow, customized application maps
- Configuration and monitoring: REST API, SDK (Java and Python), Syslog, Simple Network Management Protocol (SNMP), NetFlow, application usage, device identification, live mode, zero-touch activation
- Network services: IPv4, DNS, DHCP client, DHCP server, DHCP relay, network address translation (NAT)
- Quality of service (QoS): Shaping, policing, per-flow queueing, tunnel shaper, multisource inbound QoS, rate-limiter, Console Operating System (COS) aware, outer and inner Differentiated Services Code Point tagging, smart defaults, Multiprotocol Label Switching COS

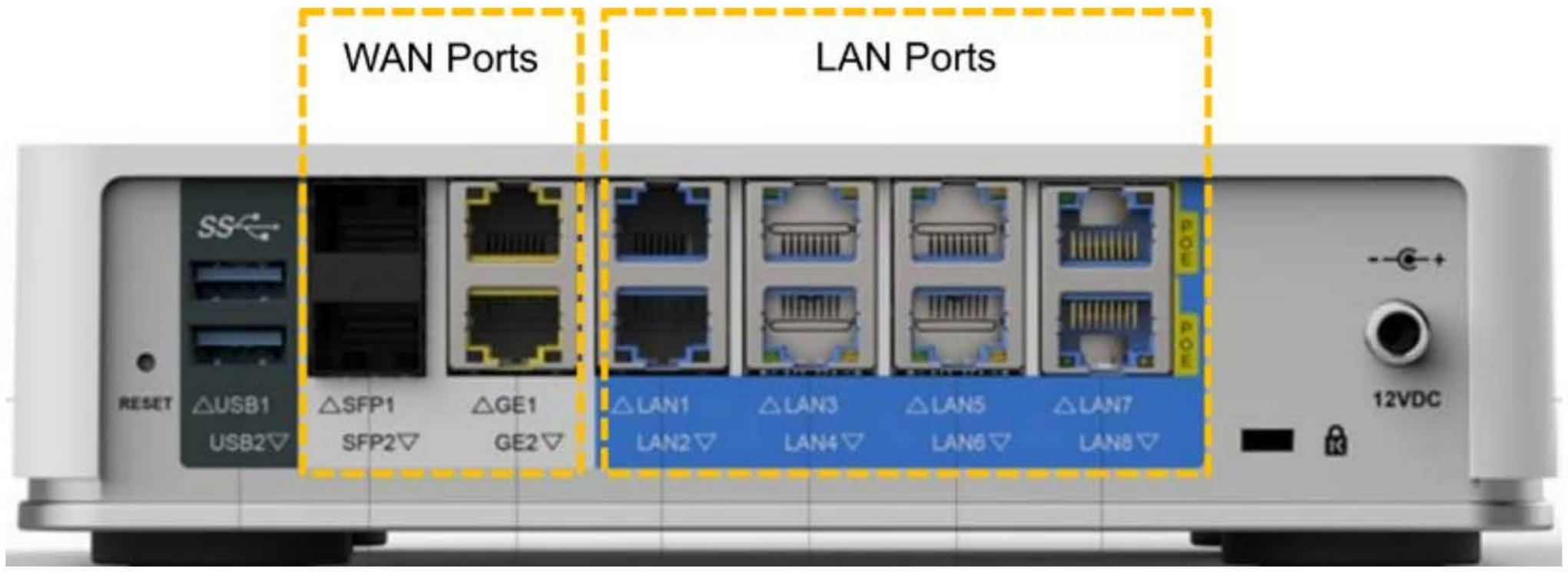
- Remote troubleshooting: Live mode, alerts, events, remote diagnostics (such as DNS test, ping test, flush active flows, list active flows, paths, VPN tests, packet capture, and so on), PKI infrastructure with certificate management workflows, diagnostic bundles
- Security features: AES256/128, SHA1/SHA2, IKEv2, VPN-client-compliant IPsec, public key infrastructure, segmentation, TLS1.2, Simple Certificate Enrollment Protocol, firewall L2-7, 1:1 NAT, port forwarding, dynamic branch to branch, MAC-filtering security service
- Port security
- VLAN tagging: 802.1Q, 802.1ad, QinQ (0x8100), QinQ (0x9100), native
- WAN overlay support:
  - Public, private, or hybrid transport
  - Cloud and on-premises availability
- Traffic monitoring: SNMP, NetFlow, live mode, and so on

Technet24

3-18 Physical Connectivity Options

Physical VMware SD-WAN Edge appliances provide several connectivity options:

- RJ-45 (1G): LAN and WAN connectivity
- SFP+ module: LAN and WAN Connectivity
- Integrated Wi-Fi
- USB Ports: 3G, 4G, and LTE connectivity



Connectivity options vary from model to model.

3-19 Review of Learner Objectives

- Identify the role of VMware SD-WAN Edge appliances
- Describe the functions of underlay and overlay networks
- List the use cases for deploying edges as hubs
- Identify the features of VMware SD-WAN Edge

Technet24

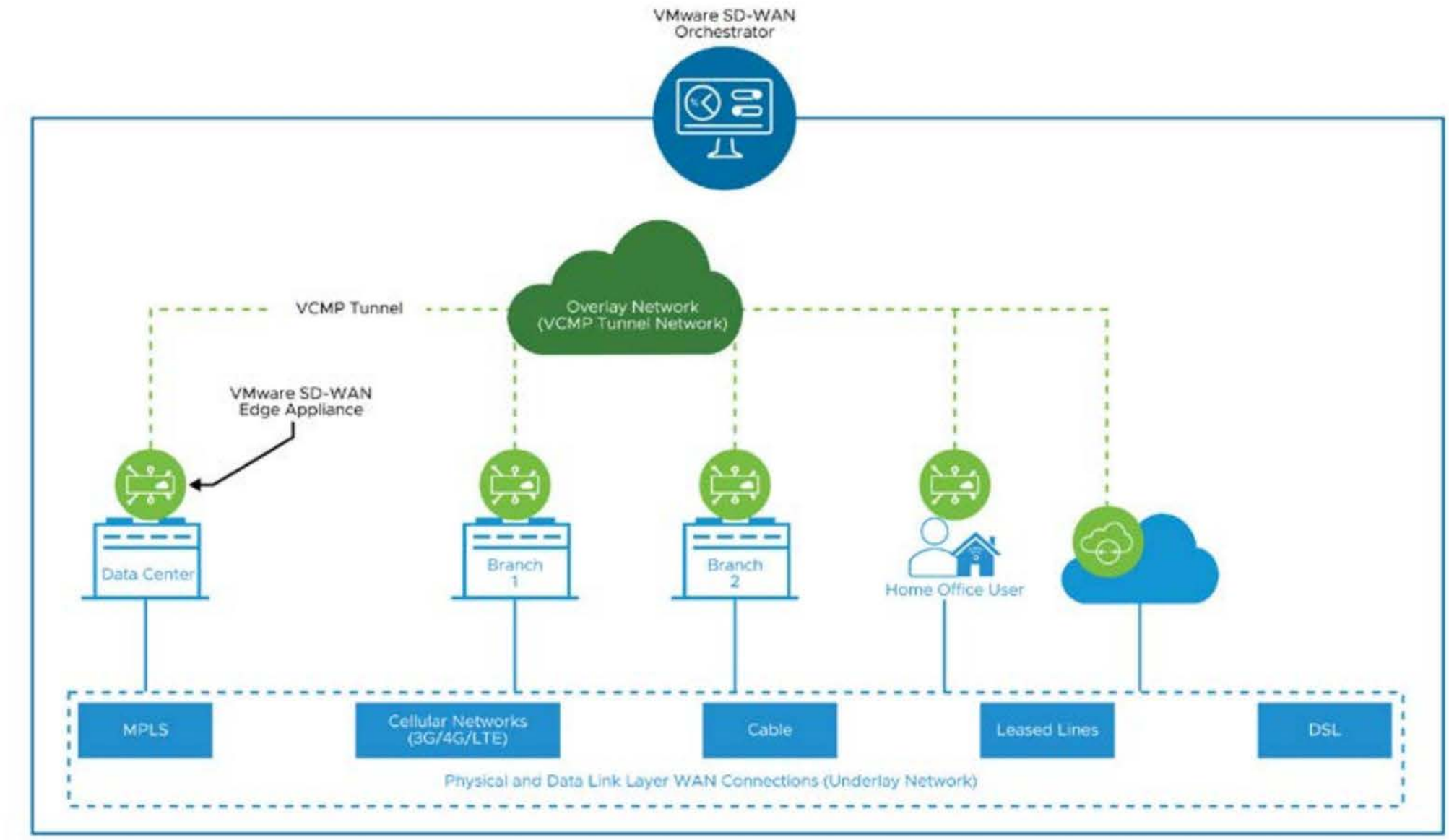
3-20 Lesson 2: VMware SD-WAN Orchestrator

3-21 Learner Objectives

- Identify the functions of VMware SD-WAN Orchestrator
- Describe the deployment models of VMware SD-WAN Orchestrator

3-22 About VMware SD-WAN Orchestrator

VMware SD-WAN Orchestrator is a web-based GUI that provides centralized management, configuration, and monitoring of the VMware SD-WAN infrastructure. The orchestrator also offers a wide array of APIs to provide management troubleshooting as well as operations support system (OSS) and business support system (BSS) integration.



VMware SD-WAN Orchestrator is the central management component of the VMware SD-WAN infrastructure. You must deploy VMware SD-WAN Orchestrator for every VMware SD-WAN solution.

Technet24

3-23 Functions of VMware SD-WAN Orchestrator

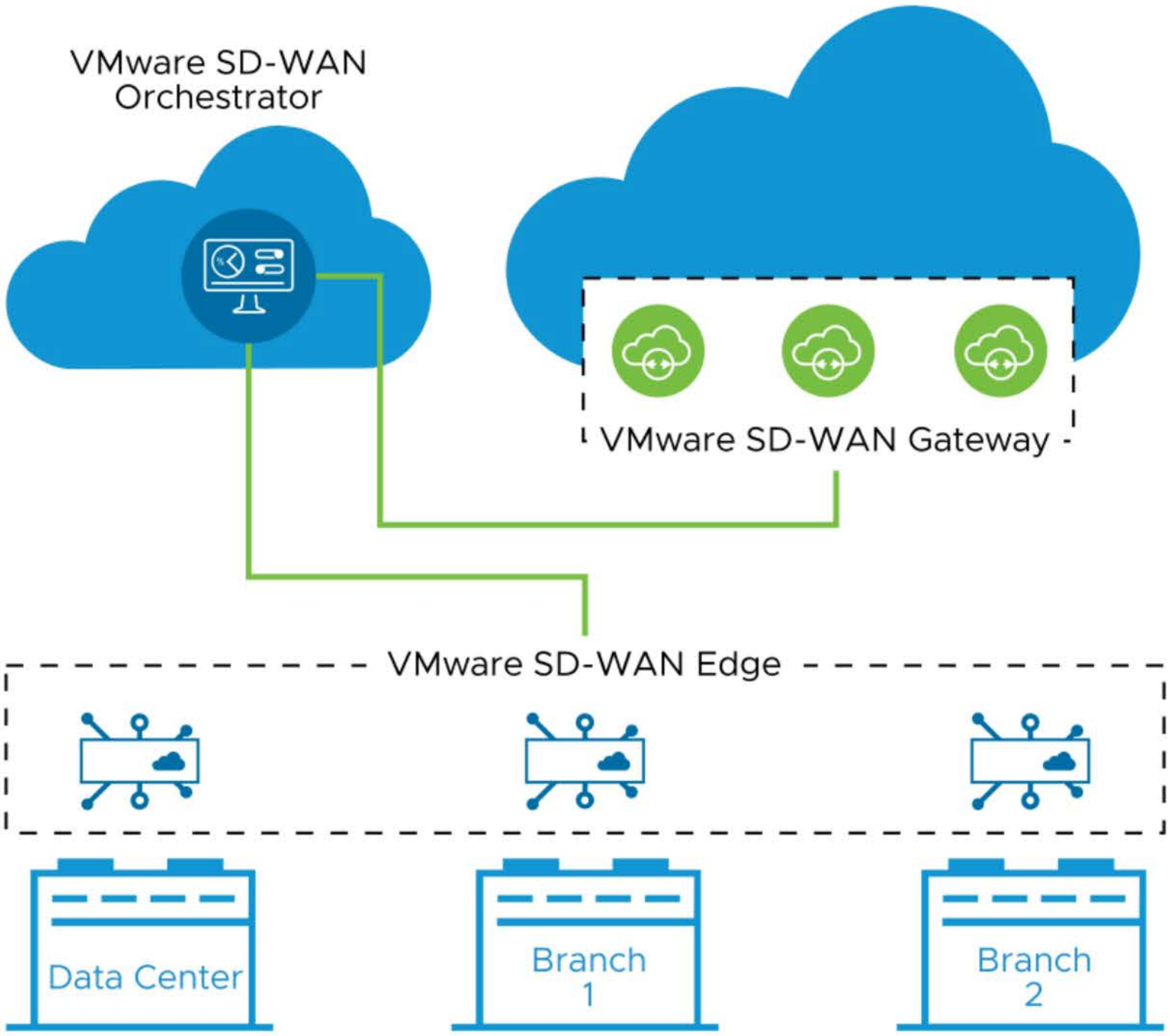
VMware SD-WAN Orchestrator has the following functions:

- Activating and provisioning VMware SD-WAN Edge appliances
- Monitoring link and flow statistics, application statistics, and link status
- Monitoring business compliance for customers and network engineers
- Accessing remote diagnostics, packet captures, and troubleshooting issues

3-24 VMware SD-WAN Orchestrator Placement

VMware SD-WAN Orchestrator is commonly deployed in a hosted cloud environment. VMware maintains and operates cloud-delivered orchestrators that service provider partners and end users can then access.

Service providers and organizations can also host VMware SD-WAN Orchestrator on-premises.



When deployed through the cloud, VMware SD-WAN Orchestrator can be distributed globally. It also offers a service level agreement (SLA) of 99.99 percent availability per month.

Technet24

3-25 Supported Web Browsers

VMware SD-WAN Orchestrator supports several Internet browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

Use Google Chrome or Mozilla Firefox for the best user experience.

3-26 Review of Learner Objectives

- Identify the functions of VMware SD-WAN Orchestrator
- Describe the deployment models of VMware SD-WAN Orchestrator

Technet24

3-27 Lesson 3: VMware SD-WAN Gateway

3-28 Learner Objectives

- List the various functions of VMware SD-WAN Gateway
- List the types of VMware SD-WAN Gateway instances
- Describe the advantages of VMware SD-WAN Gateway

3-29 About VMware SD-WAN Gateway

VMware SD-WAN Gateway is one of the most important components of the VMware SD-WAN infrastructure. VMware SD-WAN Gateway instances are cloud-delivered, multitenant components of the VMware SD-WAN solution.

VMware SD-WAN Gateway can act as a controller, a hub, or a route propagator. It can also perform the following functions:

- Connect VMware SD-WAN to SaaS or IaaS
- Connect VMware SD-WAN to a non-SD-WAN destination

Technet24

3-30 Cloud-Hosted Gateways

VMware SD-WAN Gateway is offered as a managed service. The gateways are deployed by VMware and its partners at points of presence (PoPs) and cloud data centers around the world.

Cloud-hosted gateways have some of the following advantages:

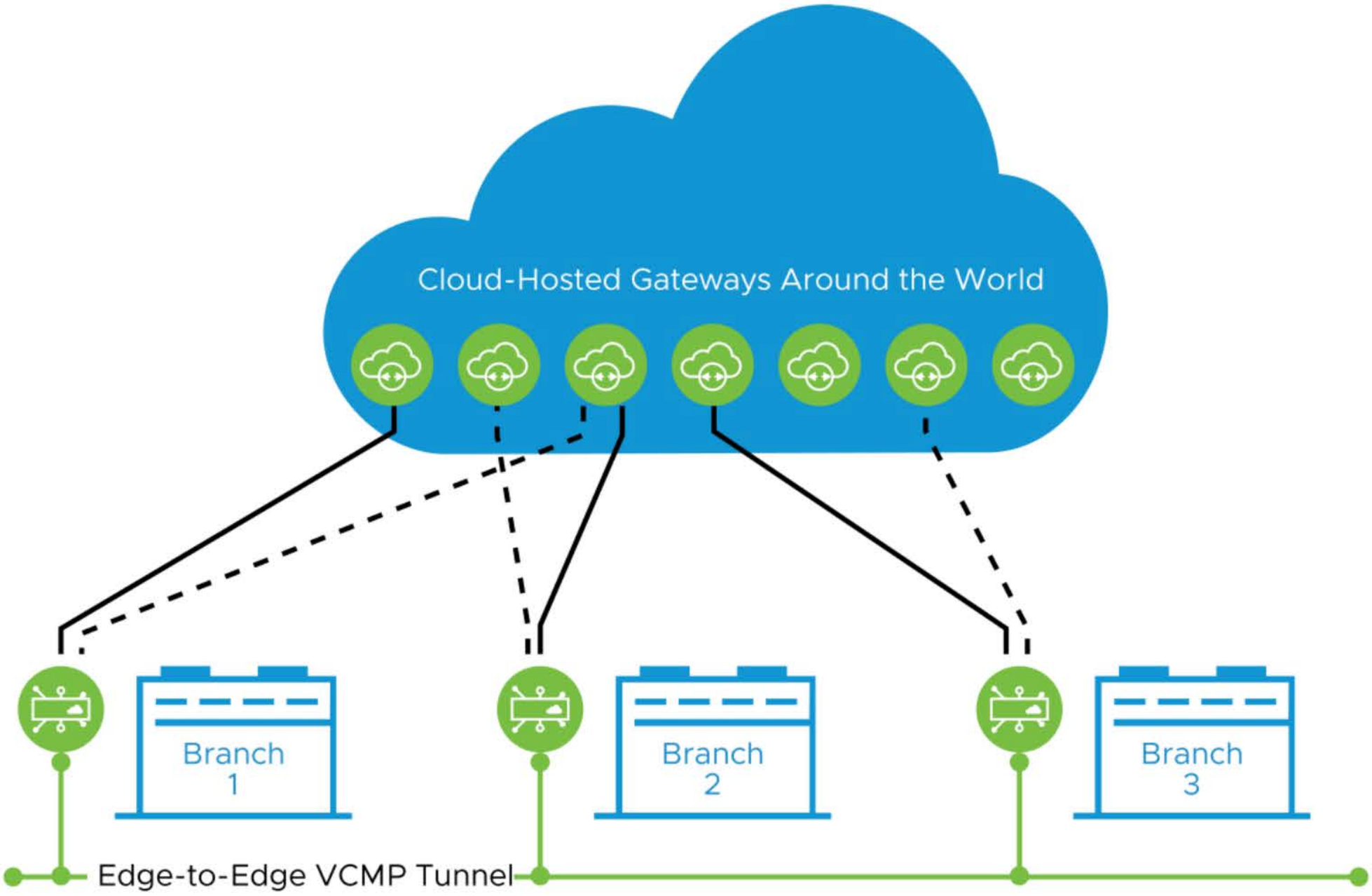
- Over 30 regions available globally
- Service level agreements with 99.99 percent reliability
- Over 2,000 gateways available
- Instant failover to other gateways for certain traffic types

3-31 Gateway Proximity and Assignment

Instances of VMware SD-WAN Gateway are strategically positioned close to major cloud service providers. The proximity of a gateway to the VMware SD-WAN Edge location determines how it is assigned.

When an edge powers on, its WAN IP address determines its location by default.

The orchestrator queries the MaxMind database to determine the location and then calculates and assigns the closest gateway for the edge. You can change the assignment of the gateway manually.



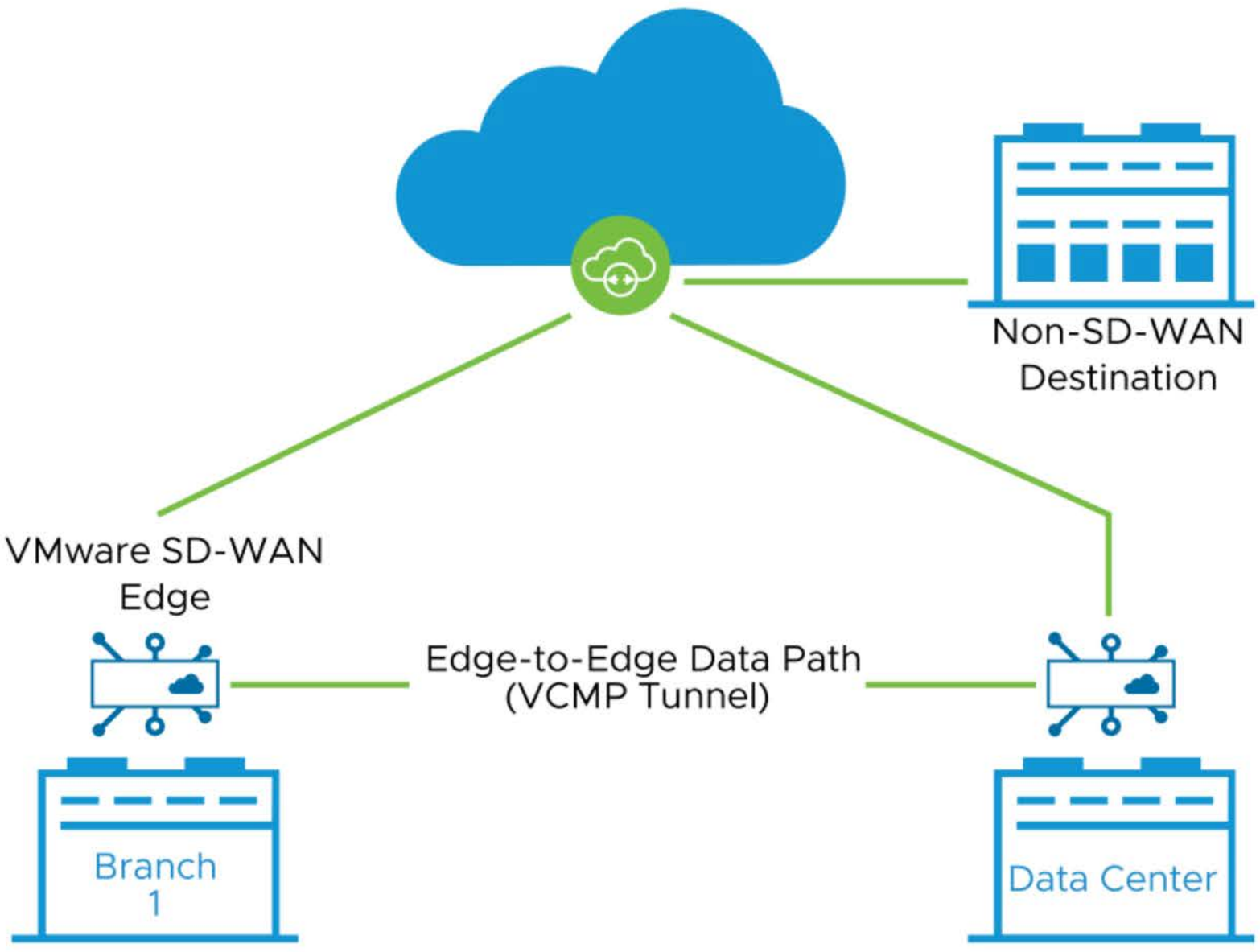
Technet24

3-32 Connecting to SaaS, IaaS, and Non-SD-WAN Destinations

VMware SD-WAN Gateway instances serve as the tunnel ends for VMware SD-WAN Edge appliances. The gateways establish a secure and optimized communication channel between VMware SD-WAN Edge and the SaaS or IaaS application in the cloud. A secure overlay tunnel is created between the edges and gateways.

At the data plane, VMware SD-WAN Gateway provides the following functions:

- Hand off traffic to SaaS or IaaS applications
- Hand off traffic to a non-SD-WAN destination
- Integrate with service providers

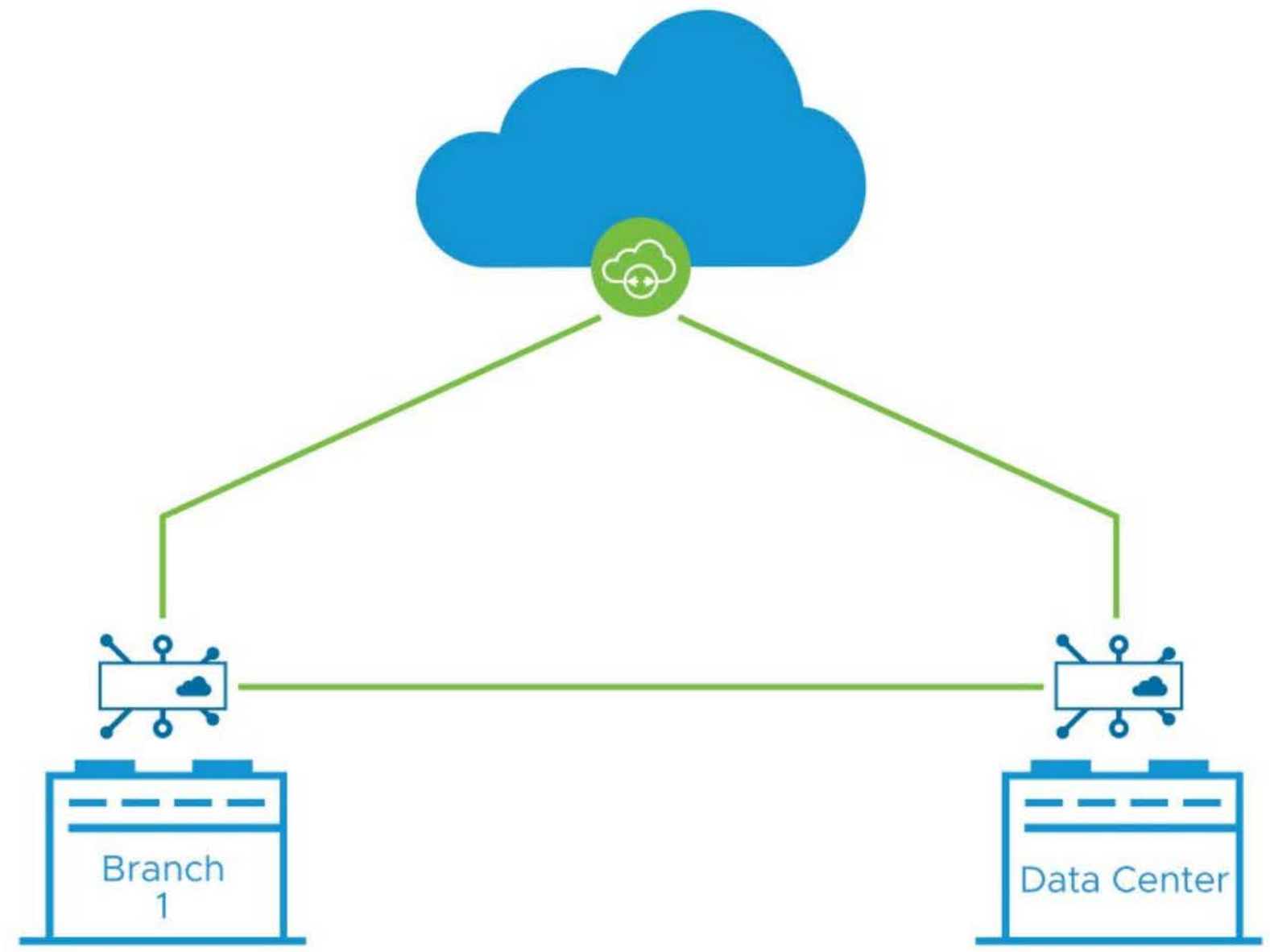


3-33 Gateways as Controllers

In addition to the data plane, VMware SD-WAN Gateway software functions at the control plane through a process called the controller. The controller receives its policy information from VMware SD-WAN Edge and carries out the functions that the edge specifies.

As a controller, VMware SD-WAN Gateway performs the following functions:

- Discovers and resolves the WAN IP address
- Detects the link bandwidth
- Receives and distributes routing information
- Updates the routing information to the edges
- Runs bandwidth tests

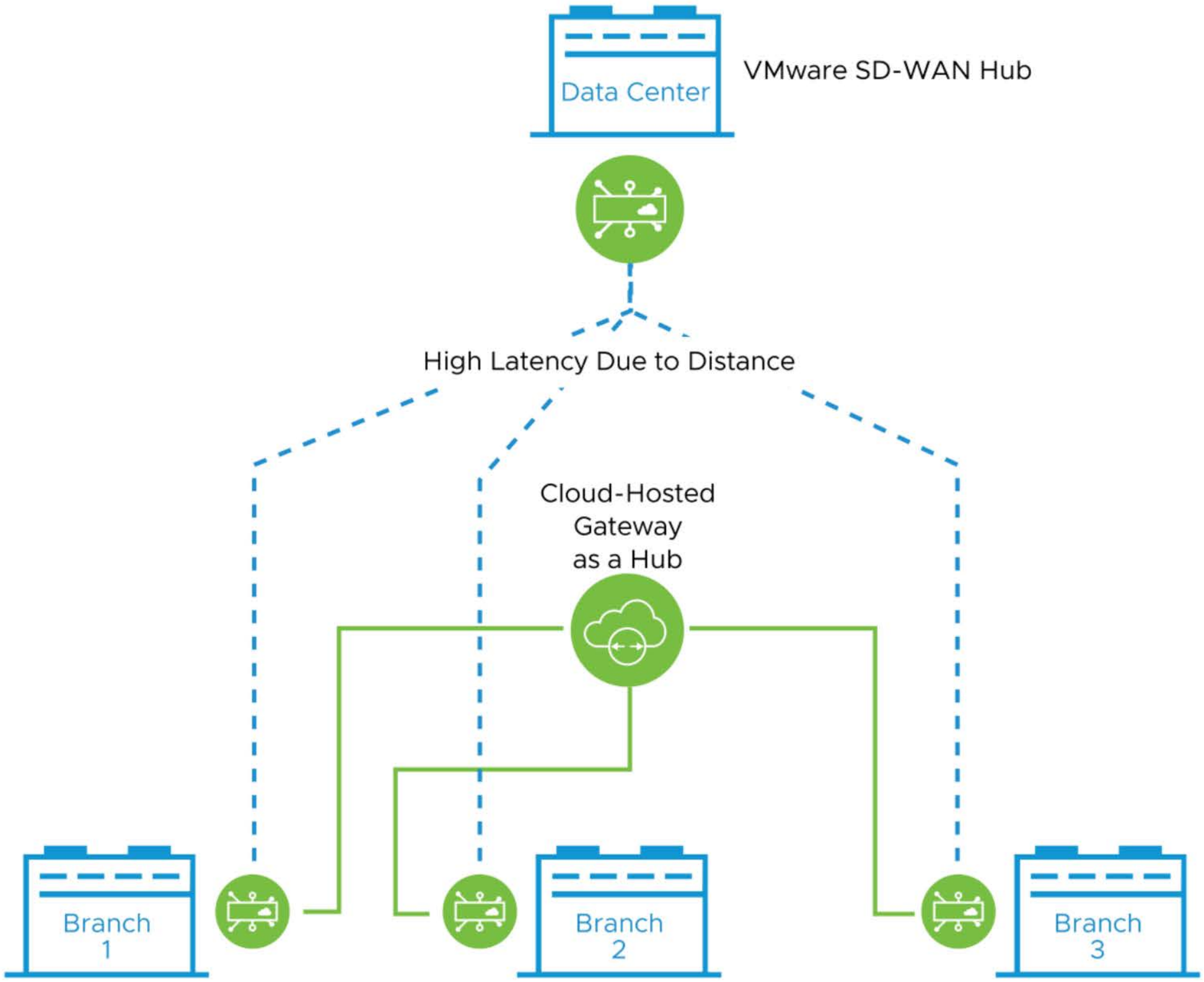


Technet24

3-34 Gateways as Hubs

The function of a hub is to terminate the traffic coming from VMware SD-WAN Edge devices deployed at branch offices or from VMware SD-WAN Gateway instances. VMware SD-WAN Gateway also runs a process that allows it to function as a hub.

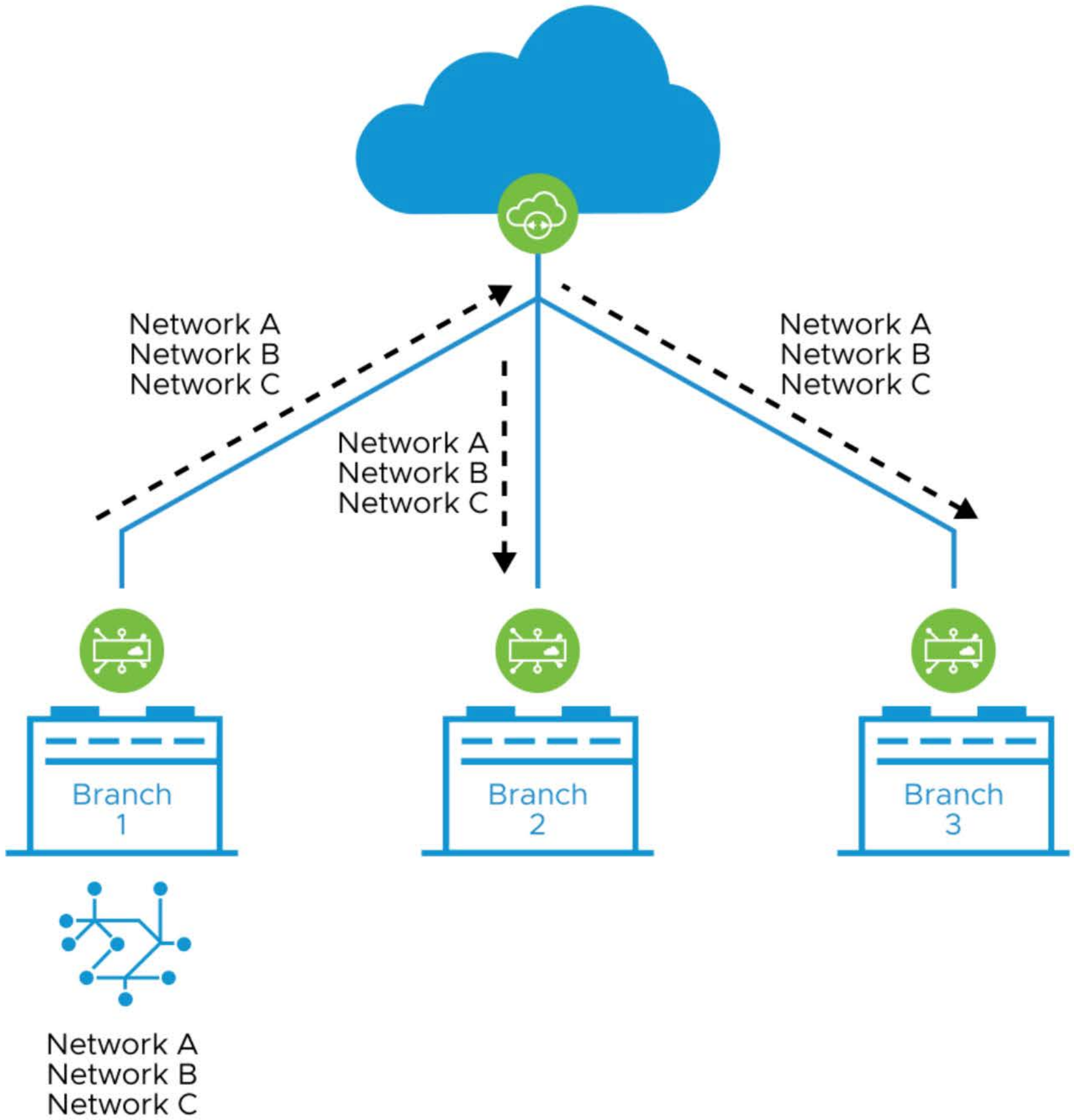
If for any reason the edge device cannot be used as hub, you can use a cloud-hosted gateway as a hub. For example, a large distance between the data center and the branch office can introduce noticeable latency in the traffic. In that case, using a cloud-hosted gateway as a hub might be more efficient.



3-35 Gateways as Route Reflectors

VMware SD-WAN Gateway can function as a route reflector between VMware SD-WAN Edge applications.

The edges send the local routing information to the gateway. The gateway, functioning as a route reflector, propagates the routing information and any subsequent updates to other VMware SD-WAN Edge appliances that belong to the enterprise.

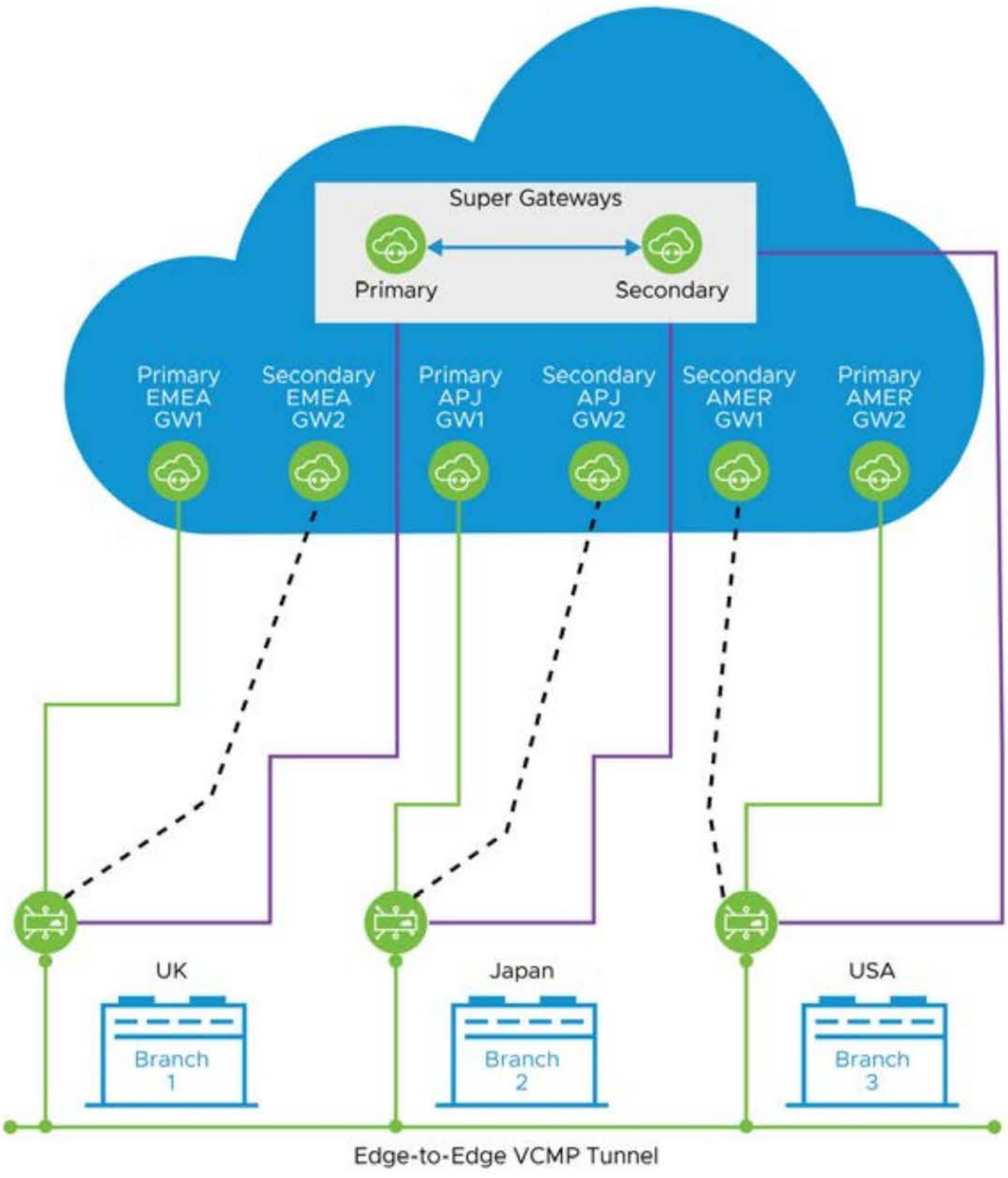


Technet24

3-36 Types of Gateways

A VMware SD-WAN Gateway instance can be assigned to an edge appliance as either a primary, secondary, or super gateway:

- Primary gateways are used to route all cloud-bound traffic. If the primary gateway becomes inoperative, all cloud traffic bypasses the primary gateway and directly uses the edge WAN link.
- Secondary gateways are used by the VPN traffic if the following conditions are met:
  - The primary gateway is not available.
  - The secondary gateway is common between the edges.
- Super gateways are required for communication between the edges if they do not share a primary or secondary gateway.



3-37 Advantages of Cloud-Hosted Gateways

In addition to performance, a cloud-hosted gateway delivers several other capabilities and benefits:

- Creates an instant global footprint
- Provides horizontal scalability
- Enables high availability for control plane functions
- Uses upstream peering at the PoPs
- Incorporates inherent network redundancy and failover
- Eliminates the need for custom endpoints close to business-critical SaaS and IaaS services
- Offers scheduled upgrades, data redundancy, disaster recovery, and global rapid-response teams
- Provides aggregated connectivity to IaaS and non-SD-WAN destinations

Technet24

3-38 Partner Gateways

VMware SD-WAN Gateway can be deployed as a partner gateway that is on-premises and managed in a service provider network.

A partner gateway provides access to the service provider's infrastructure and services.

3-39 Review of Learner Objectives

- List the various functions of VMware SD-WAN Gateway
- List the types of VMware SD-WAN Gateway instances
- Describe the advantages of VMware SD-WAN Gateway

Technet24

3-40 Lesson 4: VMware SD-WAN Component Interactions

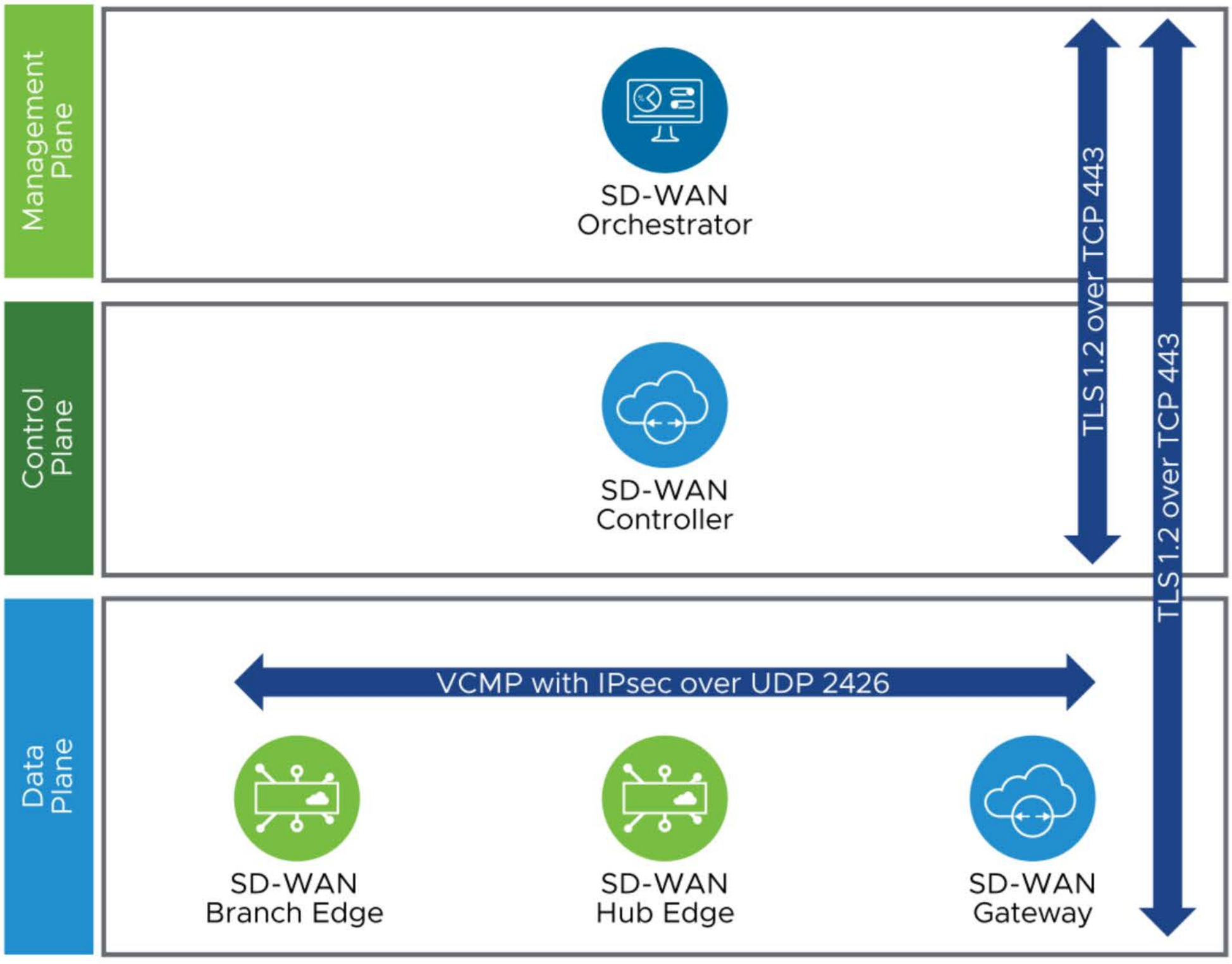
3-41 Learner Objectives

- List and describe the different VMware SD-WAN planes and their associated components
- Explain how the components of the different planes interact

3-42 VMware SD-WAN Planes

VMware SD-WAN Orchestrator, VMware SD-WAN Gateway, and VMware SD-WAN Edge work at different planes depending on how they function and interact:

- Management plane (VMware SD-WAN Orchestrator)
- Control plane (VMware SD-WAN Gateway)
- Data plane (gateways, edges, and hubs)



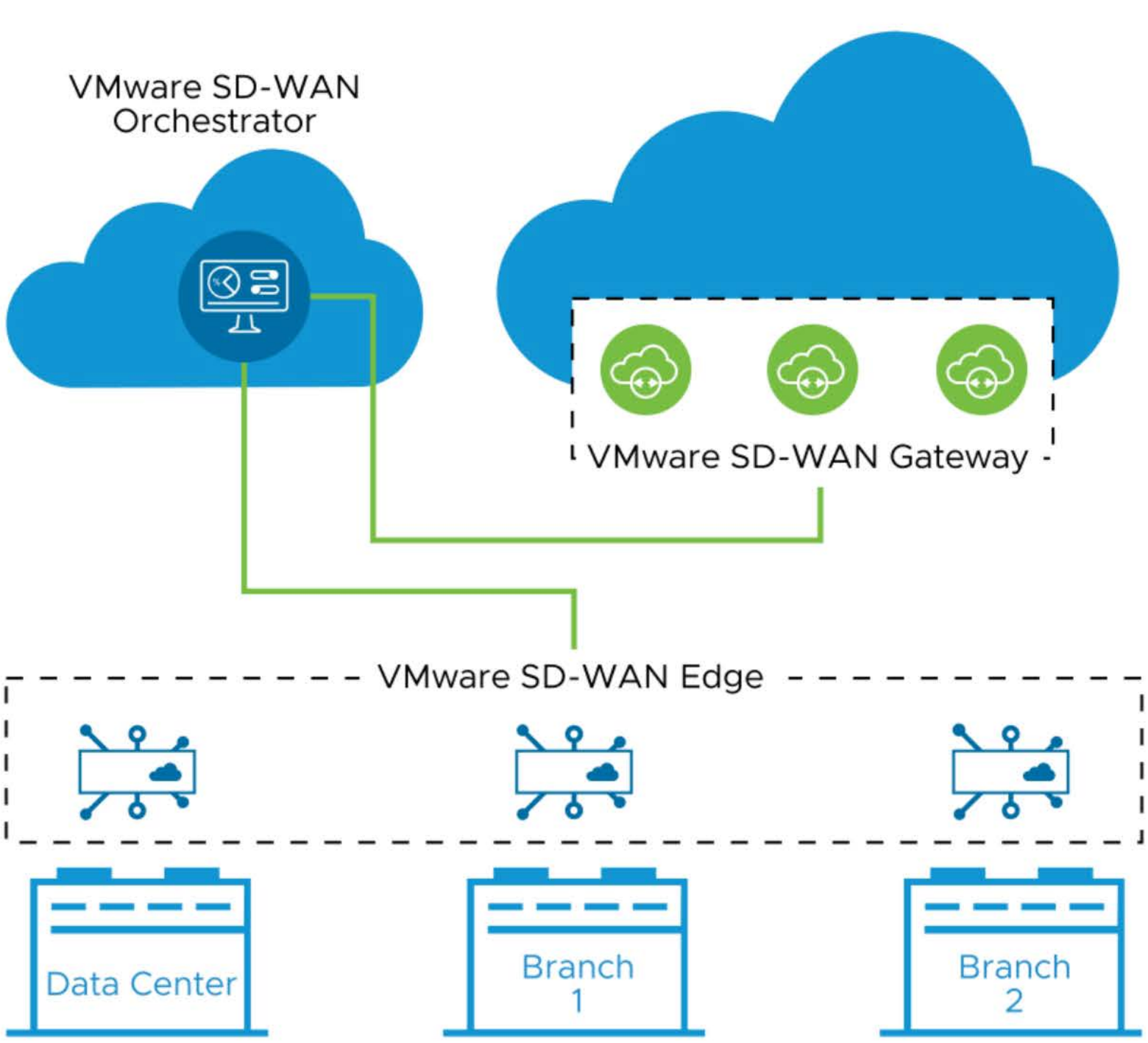
Technet24

3-43 VMware SD-WAN Management Path

VMware SD-WAN Orchestrator operates at the management plane as the single point for all configuration, management, monitoring, and troubleshooting options. VMware SD-WAN Orchestrator is responsible for the management of VMware SD-WAN Gateway and VMware SD-WAN Edge.

The orchestrator sends all configuration and management instructions to the edges and gateways.

On initial activation, the edges and gateways initiate the first management traffic toward the orchestrator.

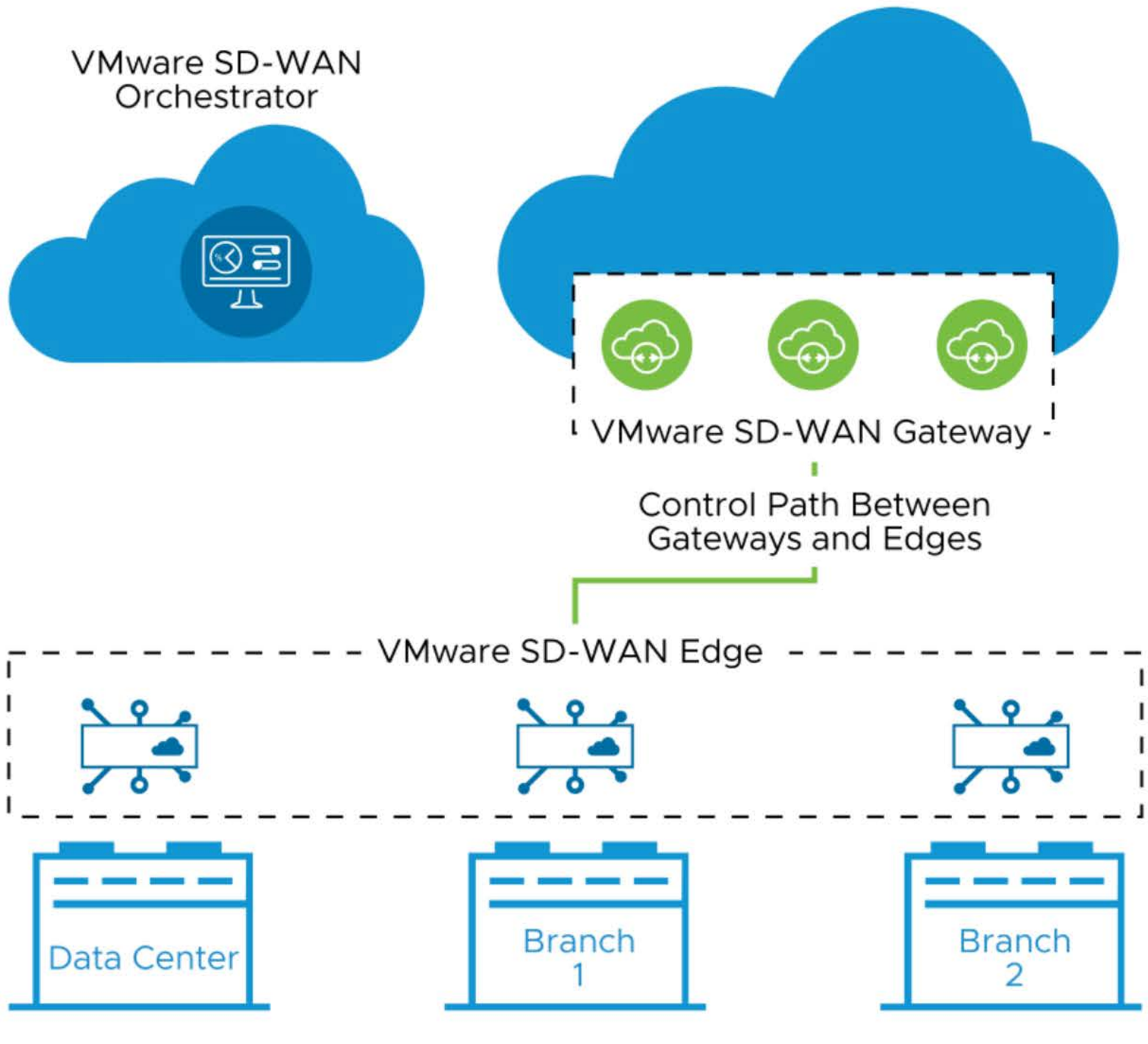


VMware SD-WAN Edge and VMware SD-WAN Gateway send heartbeat packets to VMware SD-WAN Orchestrator every 30 seconds. After missing four consecutive heartbeat packets, VMware SD-WAN Orchestrator assumes the edge or gateway is offline. VMware SD-WAN Edge also sends the flow and link statistics every five minutes to the orchestrator.

3-44 VMware SD-WAN Control Path

VMware SD-WAN Gateway operates at the control plane through the controller process that runs in each gateway's software. This controller process establishes a control path between the gateways, edges, and hubs.

VMware SD-WAN Orchestrator distributes the user-defined configuration to the VMware SD-WAN Edge appliances. The edges store the configuration locally and then update the controller.



The controller performs the following functions:

- Propagates the routing information between the edges
- Detects IP addresses, bandwidth, and other WAN characteristics
- Acts as a route reflector
- Stores the routing table locally on VMware SD-WAN Edge appliances for forwarding decisions

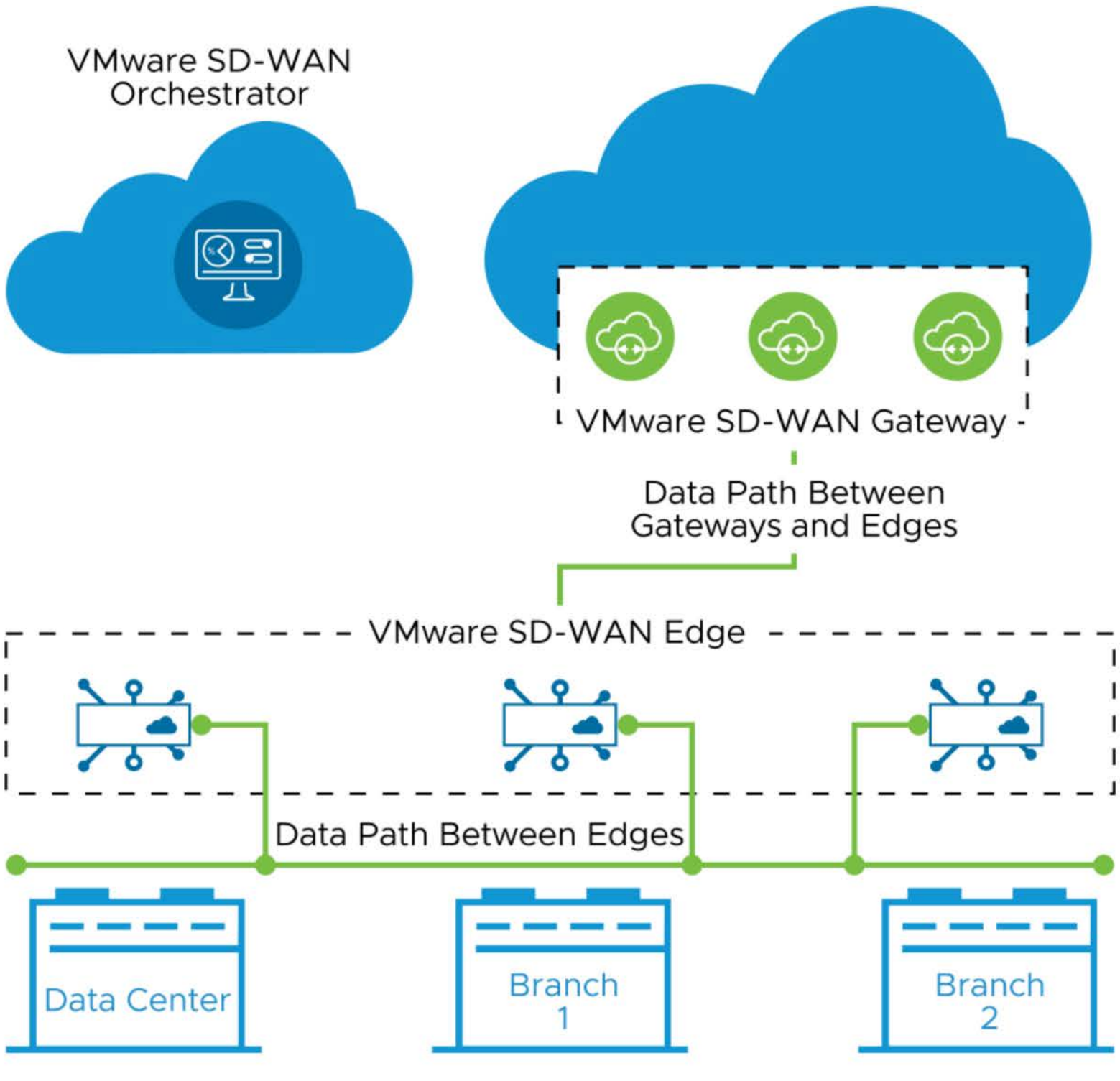
The VMware SD-WAN controller establishes a VCMP tunnel from the VMware SD-WAN Edge appliances to the assigned gateways. These control plane communications are encrypted using IPsec.

Technet24

3-45 VMware SD-WAN Data Path

The data plane is where user data traffic flows between VMware SD-WAN Edge and VMware SD-WAN Gateway.

Data plane traffic is encapsulated using VCMP and secured using IPsec encryption.



The local routing table entries of VMware SD-WAN Edge appliances determine the branch-to-branch flow of traffic. If VMware SD-WAN Edge loses connectivity to the management or control plane, it does not impact packet forwarding for established SD-WAN peers and prefixes. However, the operator cannot make configuration changes on VMware SD-WAN Edge while the edges are disconnected from the management and control planes.

3-46 Review of Learner Objectives

- List and describe the different VMware SD-WAN planes and their associated components
- Explain how the components of the different planes interact

Technet24

3-47 Key Points

- You can deploy VMWare SD-WAN Edge appliances as hubs at the data center sites.
- A tunnel created by VCMP is secured using IPsec protocol.
- You use VMware SD-WAN Orchestrator to manage VMware SD-WAN Gateway and VMware SD-WAN Edge.
- VMware SD-WAN Gateway instances can serve various roles, such as route reflectors, hubs, and controllers.

Questions?

Technet24

Module 4

Using VMware SD-WAN Orchestrator

4-2 Importance

VMware SD-WAN Orchestrator constitutes the management plane of the VMware SD-WAN solution. The establishment of a centralized management plane gives IT managers the ability to control and manage their networks with greater ease, agility, and programmability.

4-3 Module Lessons

1. VMware SD-WAN Orchestrator Portal Walk-Through
2. Installing Edge Hardware
3. Commissioning an Edge Appliance

4-4 Lesson 1: VMware SD-WAN Orchestrator Portal Walk-Through

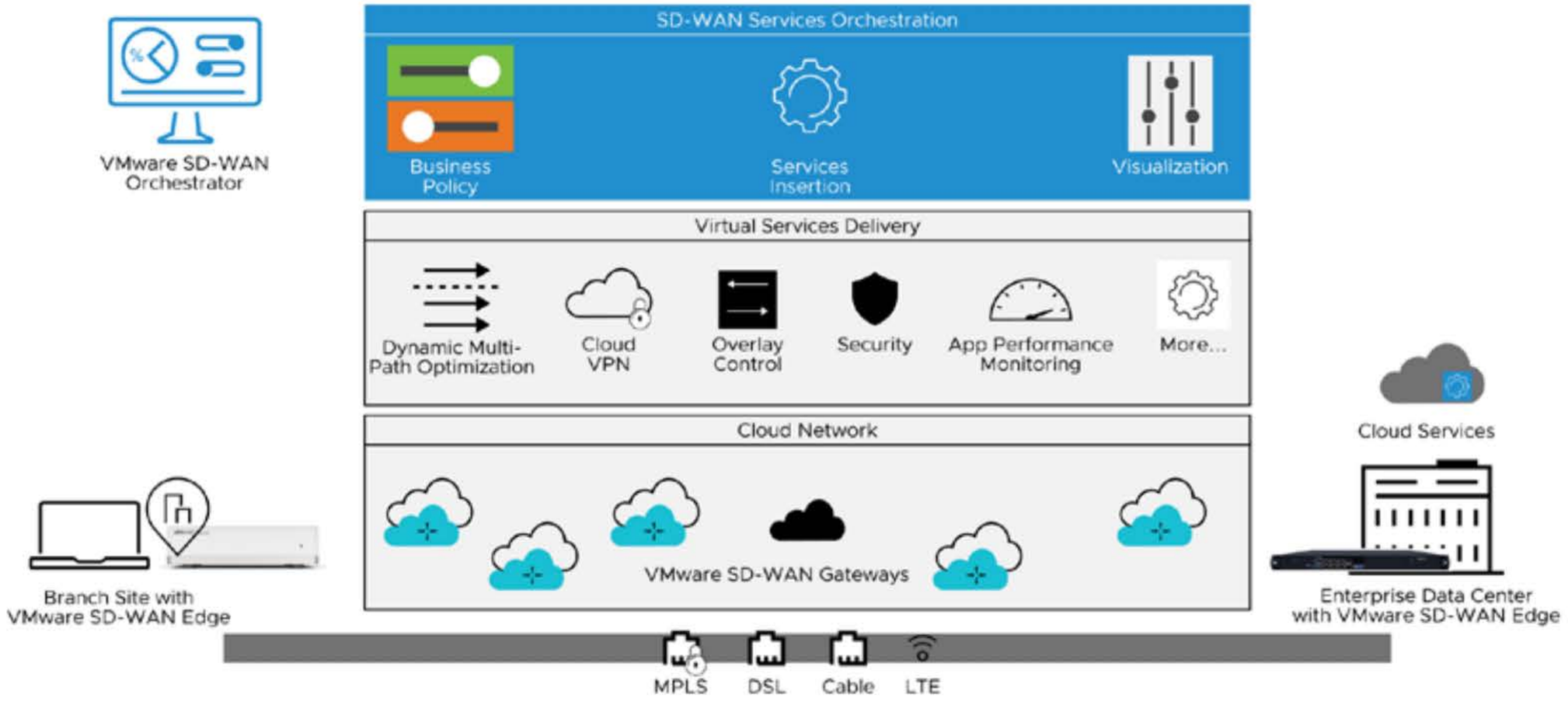
4-5 Learner Objectives

- Explain the primary functions of VMware SD-WAN Orchestrator
- Demonstrate how to navigate the menus of the VMware SD-WAN Orchestrator portal

Technet24

4-6 VMware SD-WAN Orchestrator Capabilities

The orchestration layer is where administrators configure, manage, and troubleshoot their SD-WAN network.



VMware SD-WAN Orchestrator provides centralized enterprise-wide element configuration and management. It also provides one-click provisioning of virtual services across edge appliances, in enterprise service hubs, and in the cloud.

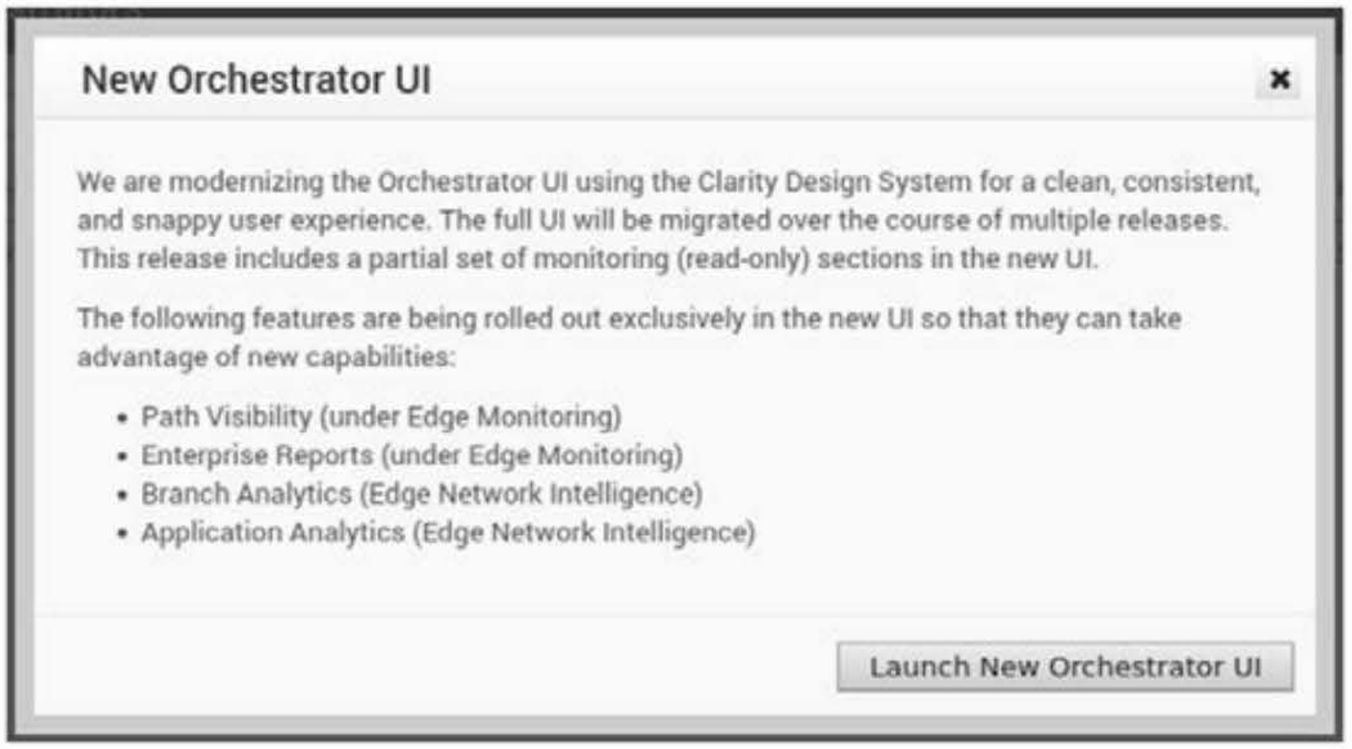
4-7 VMware SD-WAN Orchestrator Portal Layout

The VMware SD-WAN Orchestrator portal contains menu options in the navigation pane on the left and in the header along the top.

Technet24

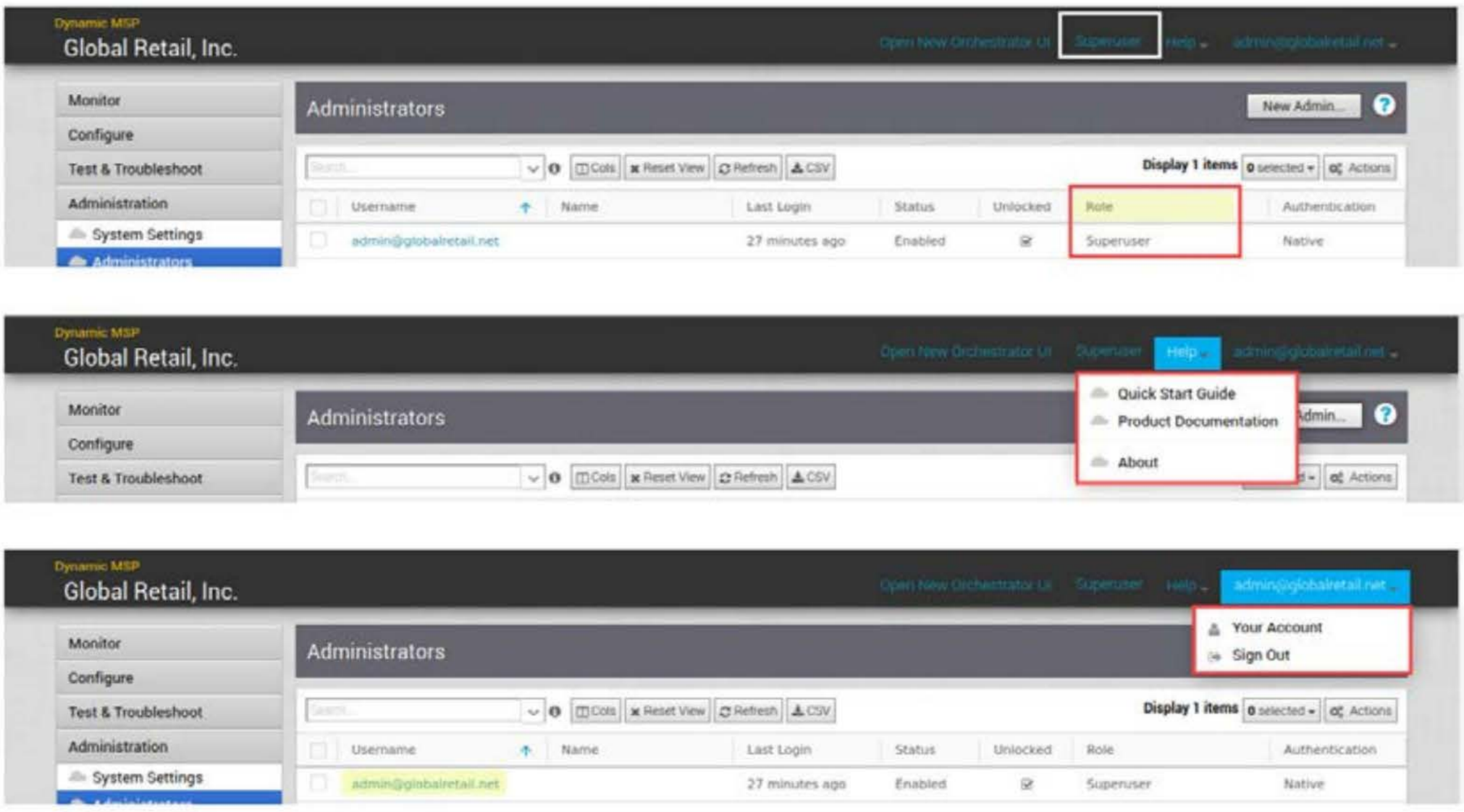
4-8 Navigating the VMware SD-WAN Orchestrator Header (1)

You launch the new orchestrator user interface by clicking **Open New Orchestrator UI** in the header.



4-9 Navigating the VMware SD-WAN Orchestrator Header (2)

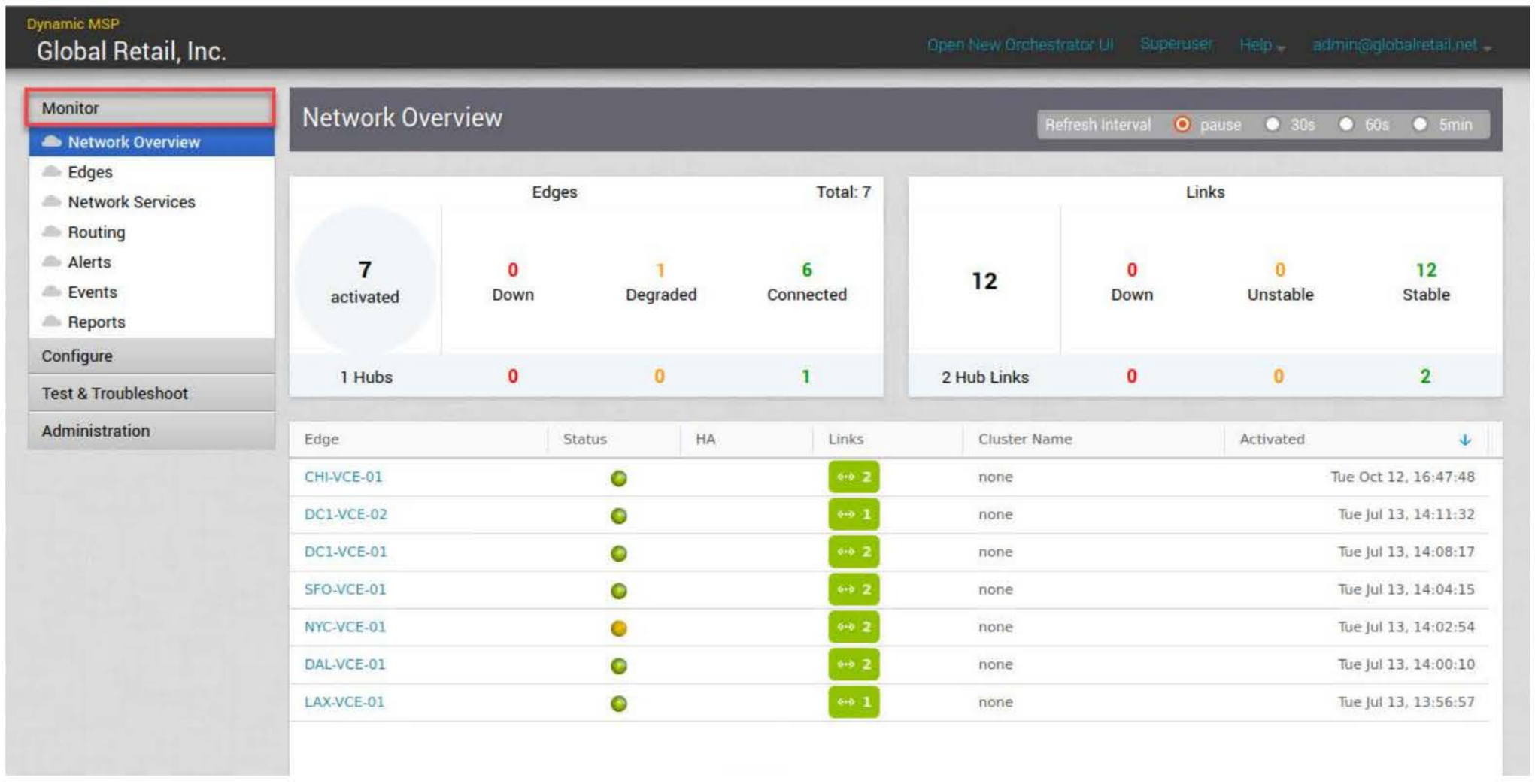
The privileges you logged in with, such as Superuser, are displayed on the orchestrator portal header. You can also access documentation and administrator functions from the drop-down menus.



Technet24

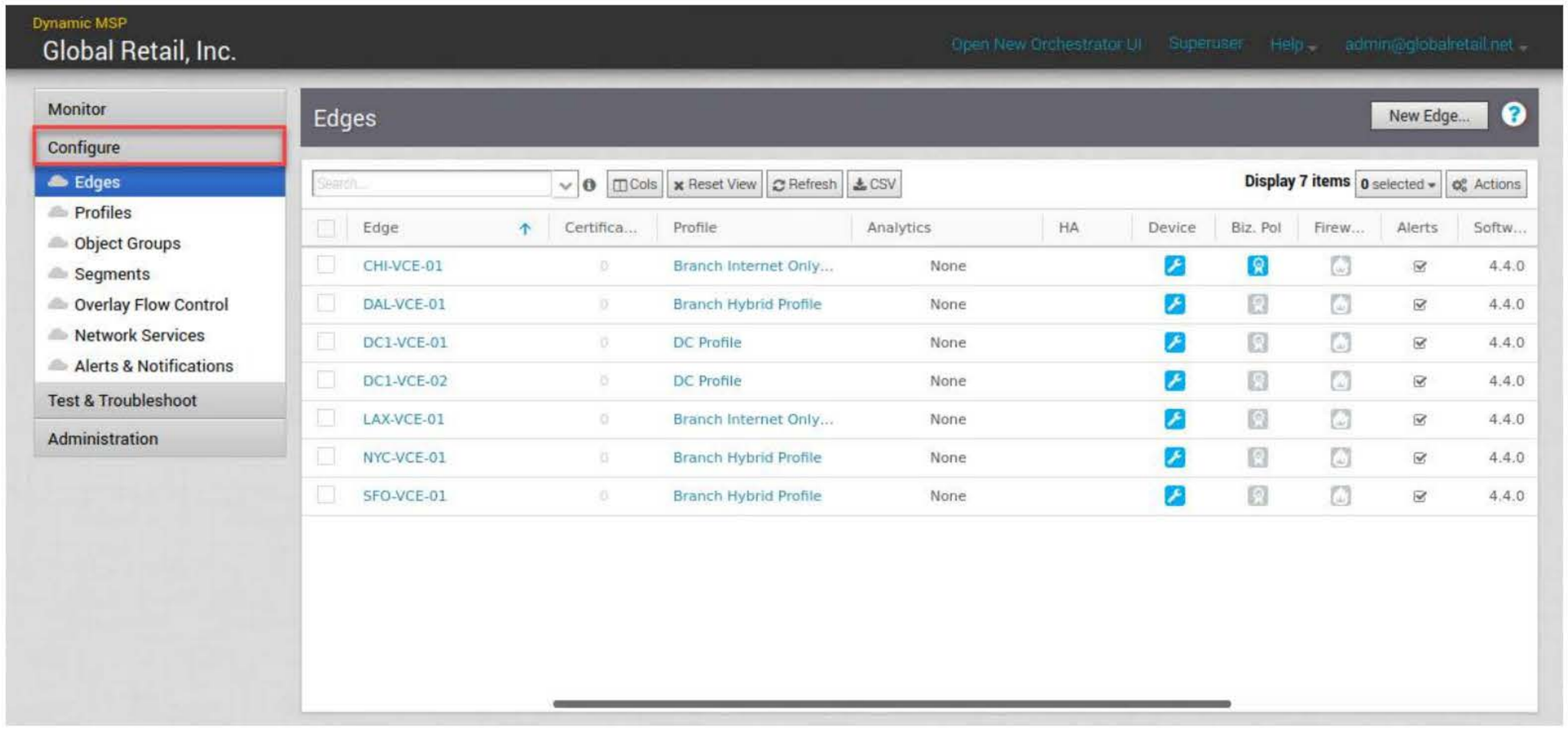
4-10 Navigating the Monitor Menu

The Monitor menu provides monitoring, alerting, and reporting functions for all aspects of VMware SD-WAN, including details of routing and networking services.



4-11 Navigating the Configure Menu

The Configure menu provides access to essential network configuration functions, such as establishing profiles, setting up segments, defining global routing preferences, and defining additional networking services.

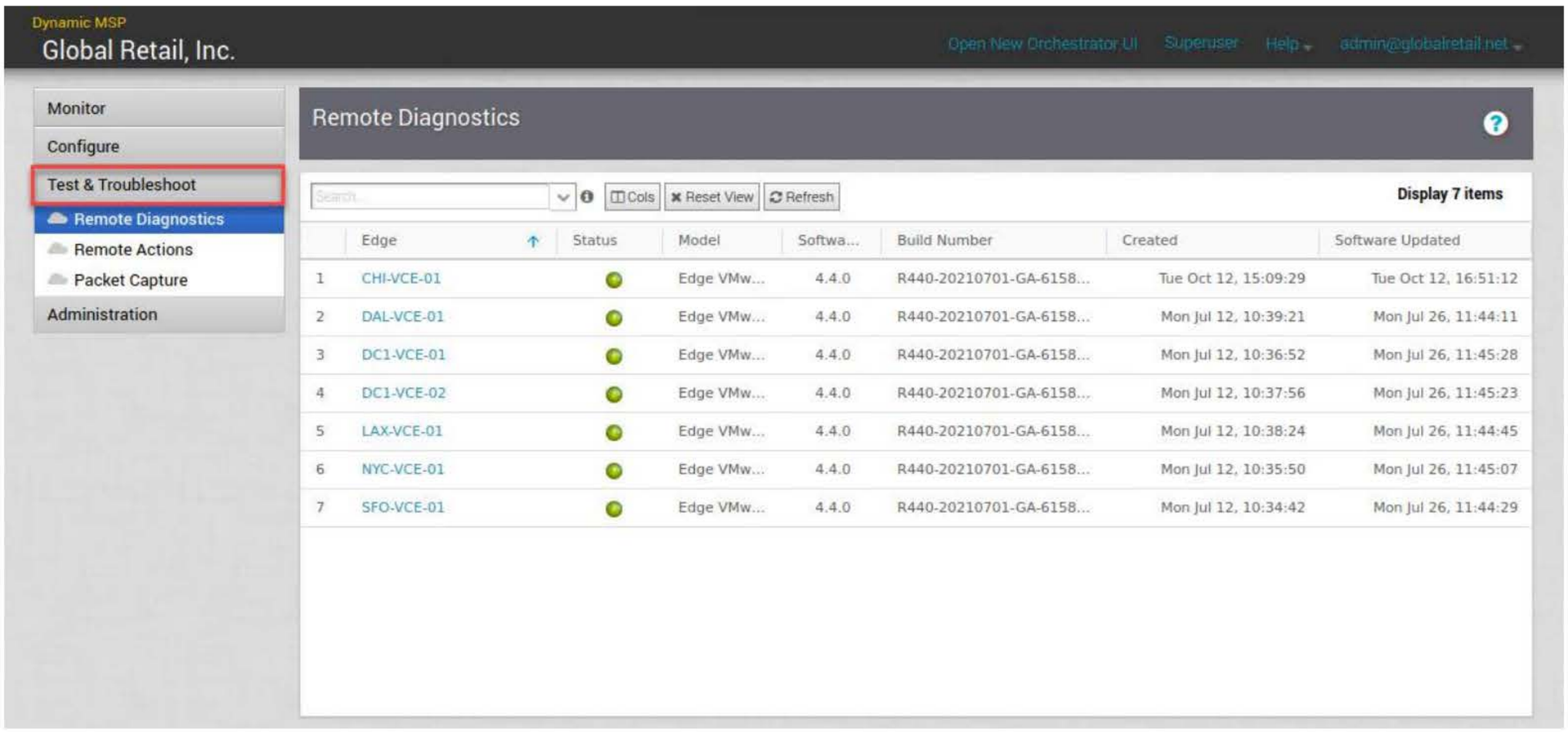


Technet24

4-12 Navigating the Test & Troubleshoot Menu

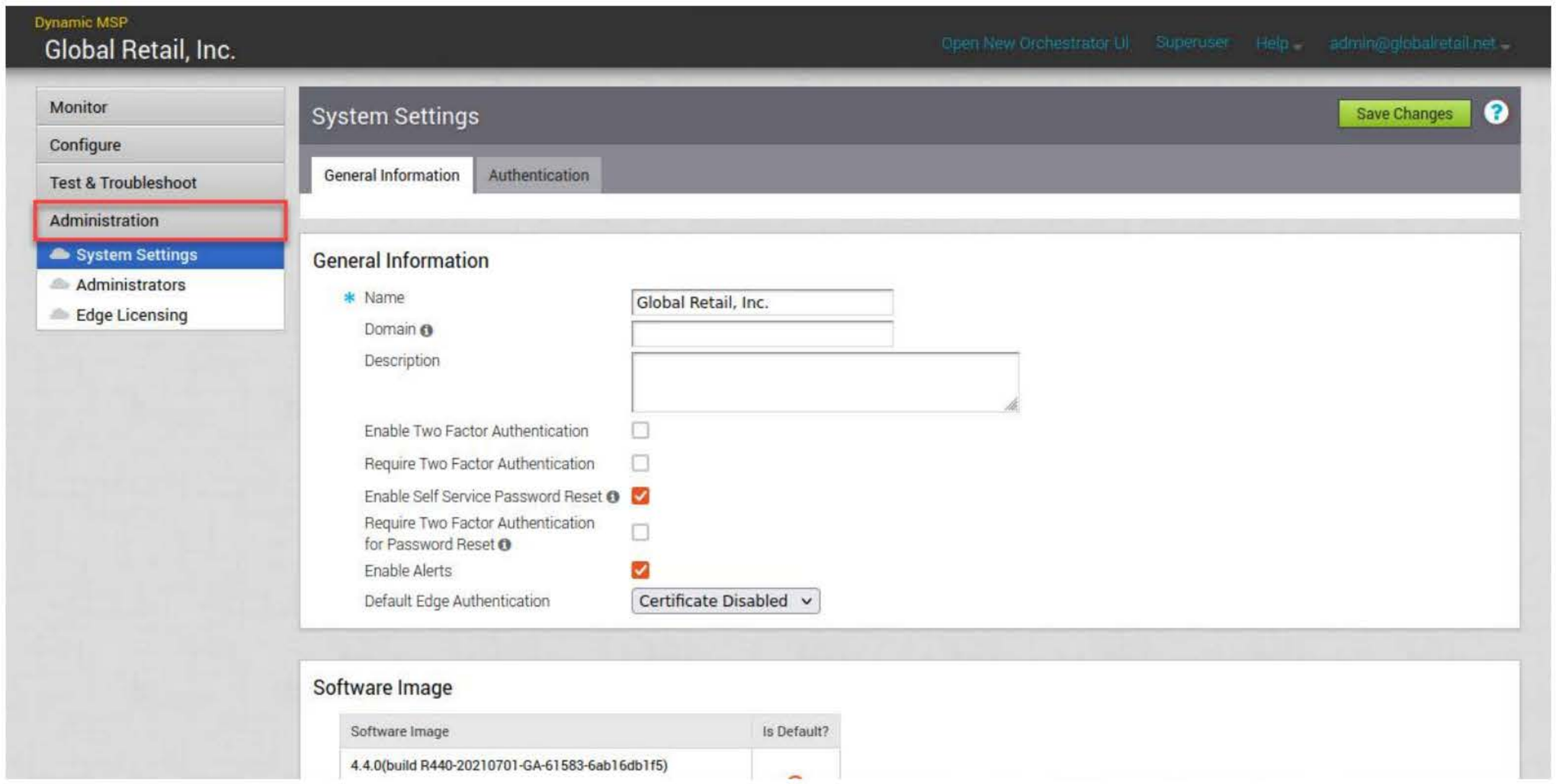
The Test & Troubleshoot menu provides access to several functions:

- Remote diagnostics, such as ping, traceroute, and listing flows
- Remote actions, such as rebooting edge appliances
- Packet captures



4-13 Navigating the Administration Menu

The Administration menu provides access to common administrator functions, such as setting up administrator access and managing edge licensing.



Technet24

4-14 Lab 1: Understanding the Lab Environment

Review the following information to understand the lab design:

- Reviewing the Lab Topology
- Data Center Site
- VMware SD-WAN Edge at the Chicago Site

4-15 Lab 2: Exploring VMware SD-WAN Orchestrator

Configure new accounts in VMware SD-WAN Orchestrator:

1. Access VMware SD-WAN Orchestrator
2. Create and Configure a Read-Only Account
3. Create and Configure a Read-Write Account
4. Create and Configure a Customer Support Account
5. Validate the Newly Created Accounts

Technet24

4-16 Review of Learner Objectives

- Explain the primary functions of VMware SD-WAN Orchestrator
- Demonstrate how to navigate the menus of the VMware SD-WAN Orchestrator portal

4-17 Lesson 2: Installing Edge Hardware

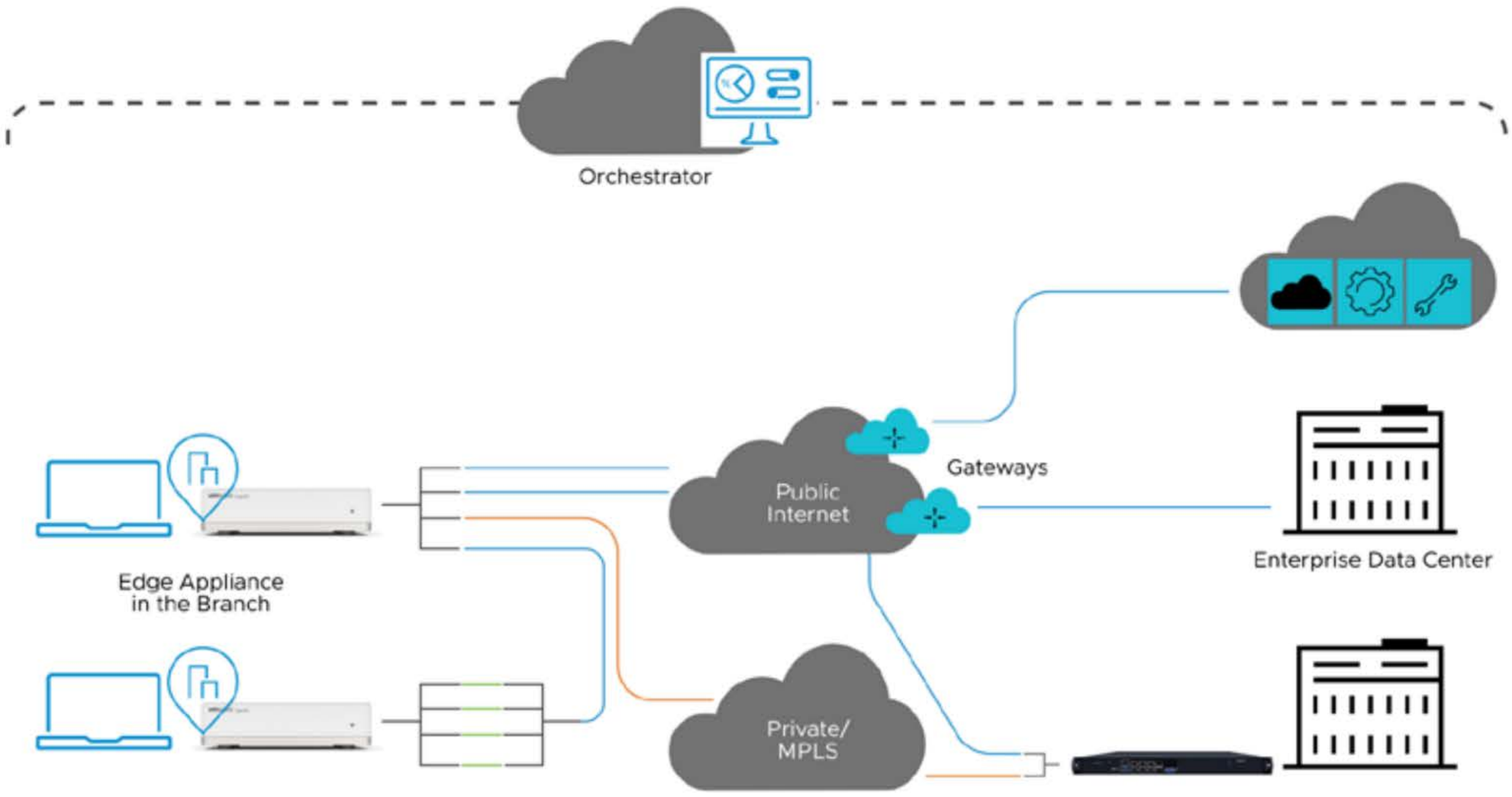
4-18 Learner Objectives

- Recognize the VMware SD-WAN Edge hardware appliance ports
- Identify the different states of the status LEDs on an edge hardware appliance
- Describe the installation sequence of VMware SD-WAN Edge hardware appliances

Technet24

4-19 VMware SD-WAN Edge Hardware Appliance Placement

The VMware SD-WAN Edge hardware appliance is designed to be deployed in branch locations without the help of trained network engineers.



4-20 Front Panel Status Indicators

The front panel LED reflects the current operational status of the VMware SD-WAN Edge hardware appliance.

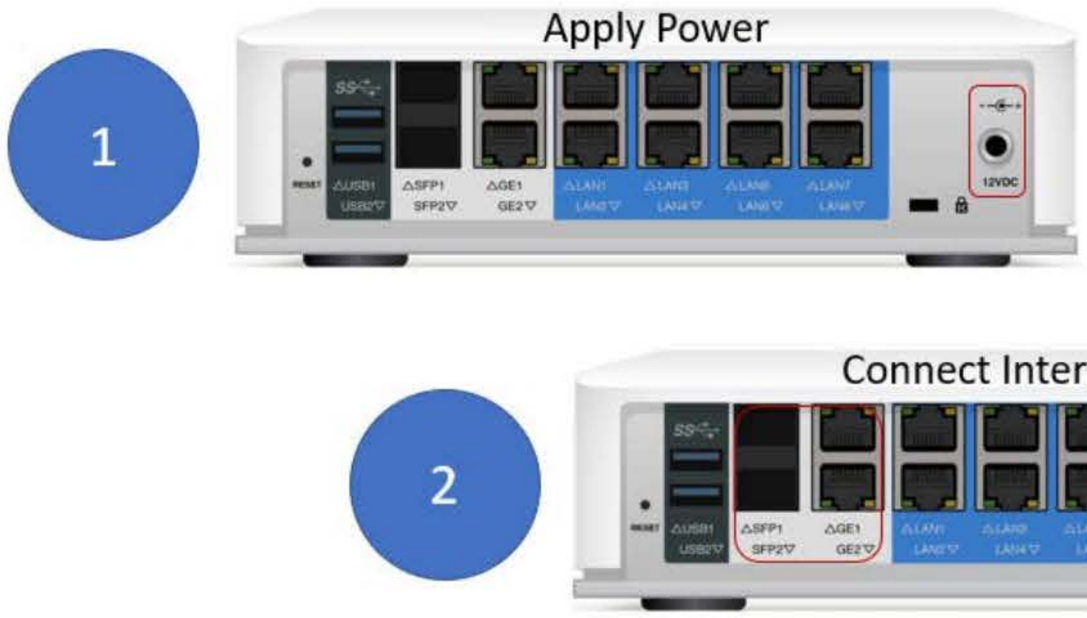
LED Color	System Status
White	Initial power-on and boot sequence
Red	No active Internet connection
Yellow	Connected to the Internet, device has not been activated
Green	Device has been activated
Flashing blue	System reset or software reset in progress
Flashing white	Edge software initialization (bootup) in progress

For more information about the front LED status light on VMware SD-WAN Edge appliances, see VMware knowledge base article 2828742 at https://kb.vmware.com/s/article/2828742.

Technet24

4-21 Edge Installation Best Practices

The edge hardware appliance yields the best results if you follow the recommended installation sequence.



4-22 Powering the Edge

You must power the edge hardware appliance from a secure AC power source, preferably fed by an Uninterruptible Power Supply (UPS). The status LED on the front of the appliance illuminates when you connect the power.

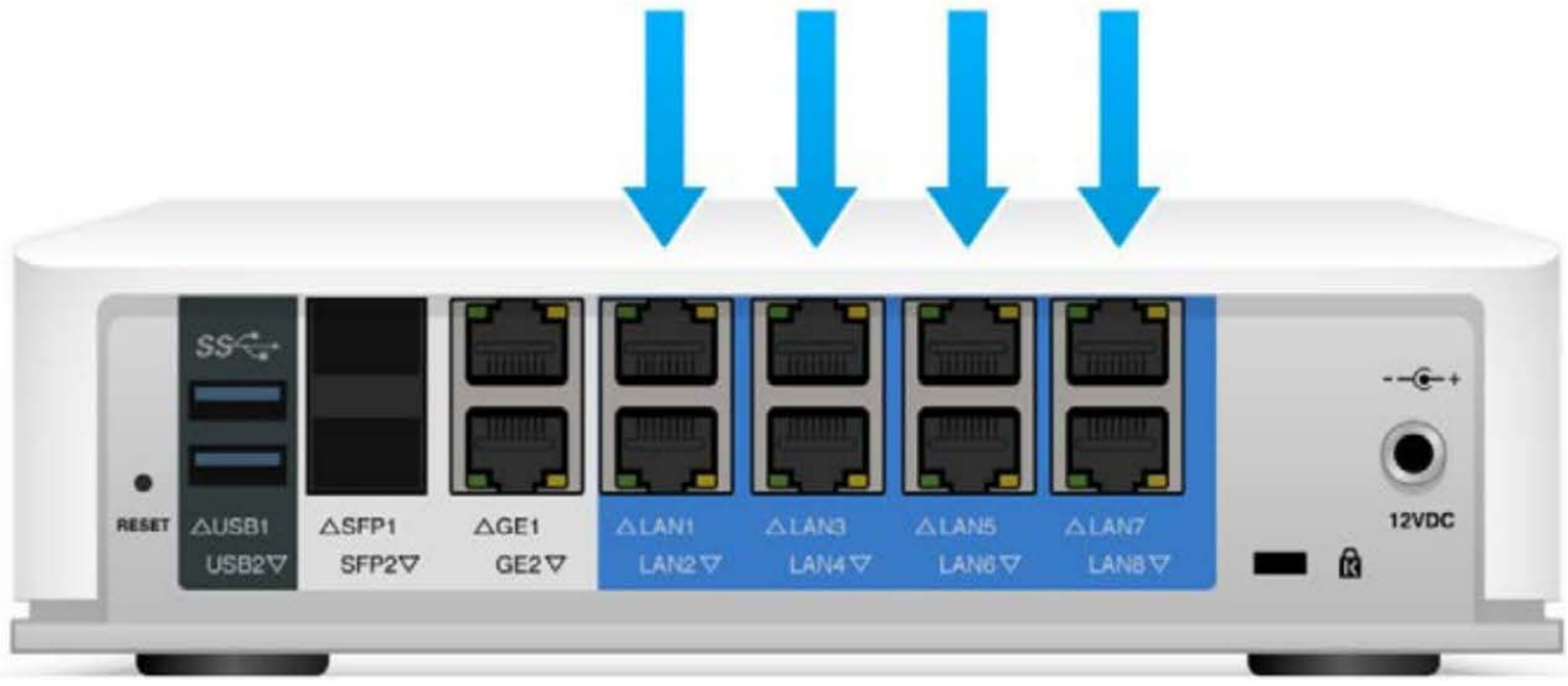
Technet24

4-23 Establishing Internet Connectivity

You connect the appropriate cable from your ISP demarcation point to one of the WAN ports on the edge hardware appliance. It is a best practice to use the lowest port for Internet connectivity.

4-24 Connecting LAN Devices

You connect LAN devices to the edge ports labeled LANx. You can also establish local connectivity through Wi-Fi.



Technet24

4-25 Review of Learner Objectives

- Recognize the VMware SD-WAN Edge hardware appliance ports
- Identify the different states of the status LEDs on an edge hardware appliance
- Describe the installation sequence of VMware SD-WAN Edge hardware appliances

4-26 Lesson 3: Commissioning an Edge Appliance

4-27 Learner Objectives

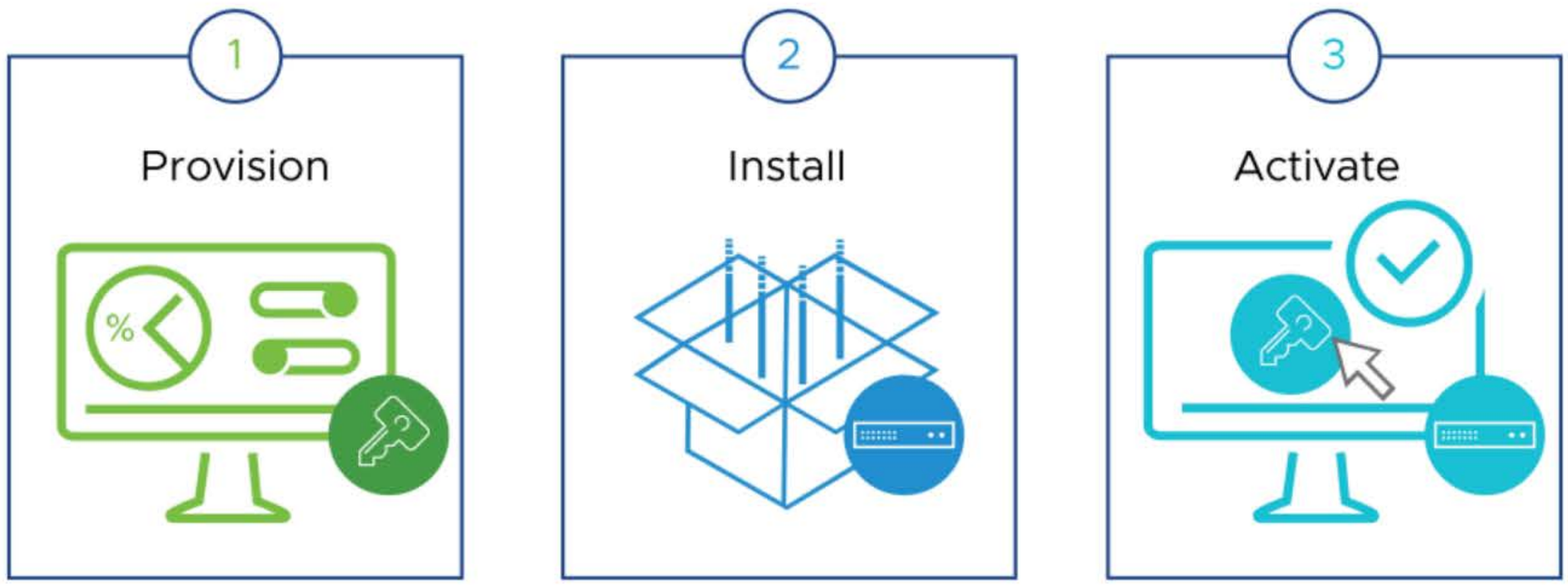
- List the steps required to commission an edge appliance onto the network
- Describe the process of provisioning an edge appliance
- Differentiate between provisioning and activating an edge appliance
- Discuss the methods of activating an edge appliance

Technet24

4-28 Commissioning an Edge Appliance

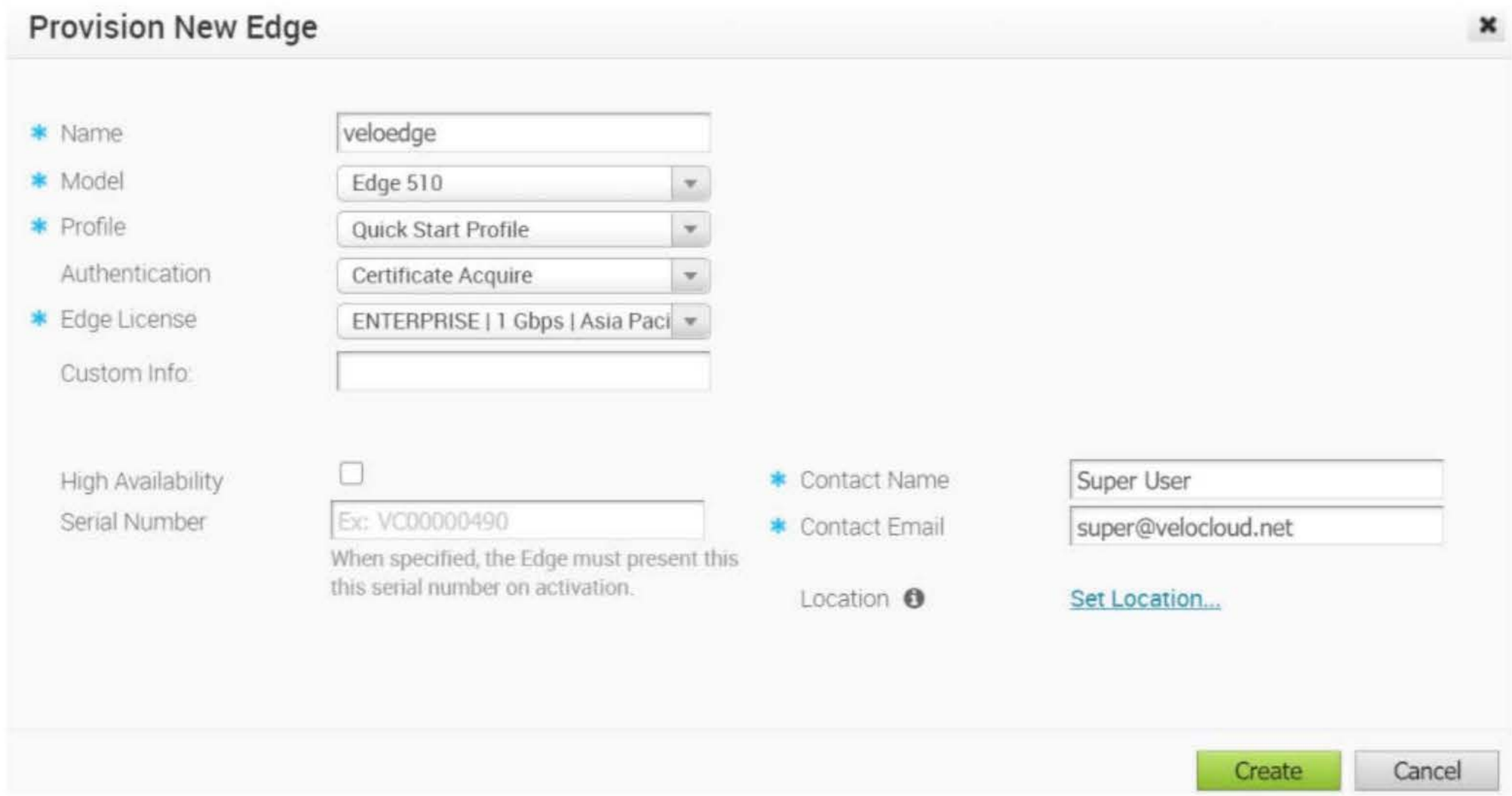
To commission an edge appliance onto the network:

1. Provision the edge.
   a.. Select the edge in the VMware SD-WAN Orchestrator portal.
   b.. Specify a configuration file for the edge.
2. Install the edge.
   a.. Unbox the edge hardware.
   b.. Connect the power.
   c.. Establish Internet connectivity.
3. Activate the edge.
   a.. Follow the email instructions.
   b.. Download the edge configuration to the device.



4-29 Provisioning an Edge Appliance

Select **Configure** > **Edges** > **New Edge** in the orchestrator portal to access the Provision New Edge dialog box, which is where you enter the details of a new edge.



Technet24

4-30 Activating an Edge Appliance

You can activate an edge appliance in multiple ways:

- Zero-touch activation:
  - A branch administrator powers on the edge and connects it to the Internet.
  - The edge retrieves a configuration with no user intervention.
- Email activation:
  - The edge is shipped to the branch location with a factory-default configuration.
  - The enterprise network administrator sends an email with activation instructions to the designated branch administrator.
  - The branch administrator follows the email instructions to activate the edge.

4-31 Comparing Edge Activation Methods

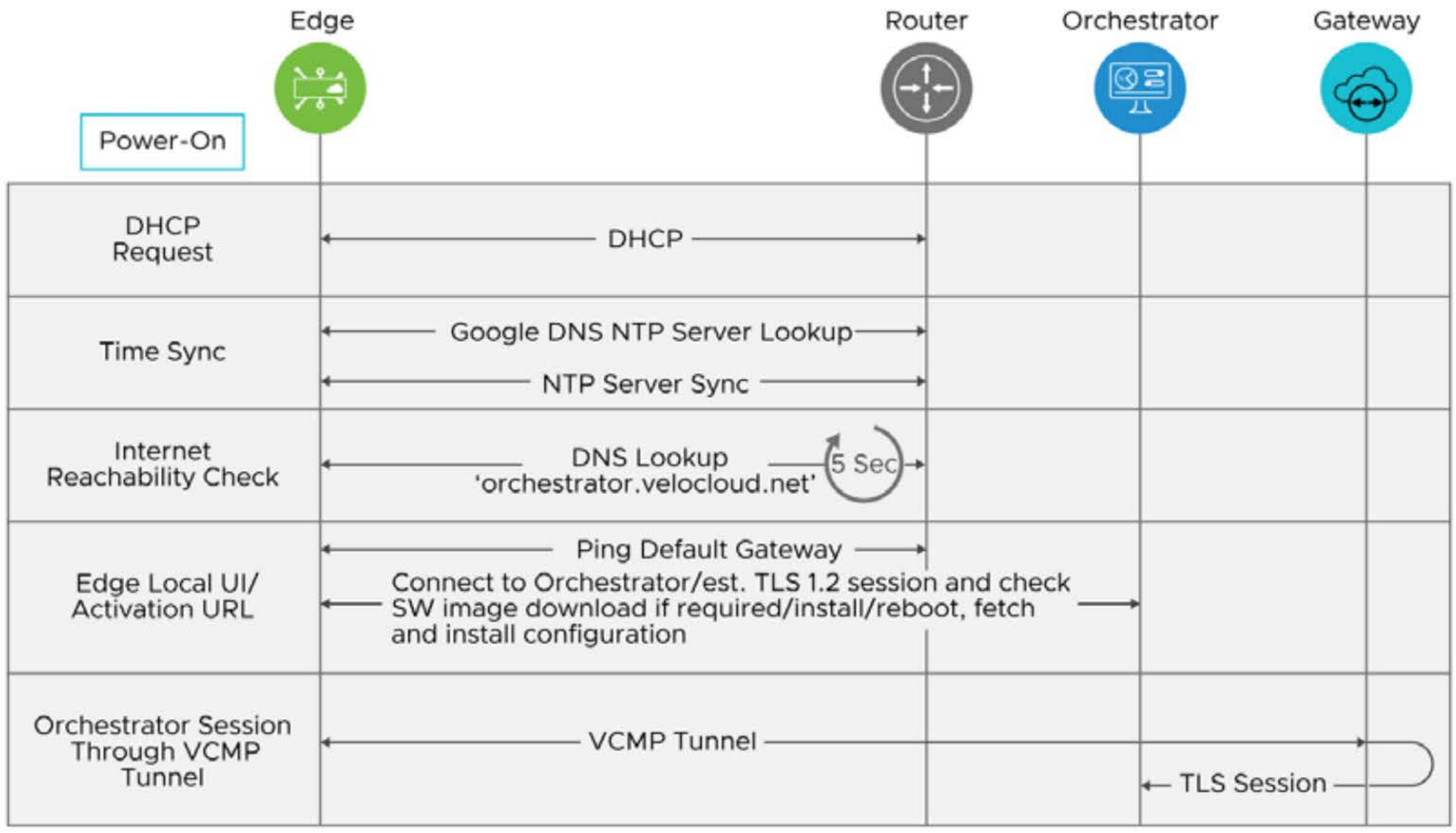
When choosing between zero-touch activation and email activation, you must decide which method best suits the size and circumstances of your organization.

Activity	Zero-Touch Activation (Data Center Activation)	Email Activation (Branch Office Activation)
No On-Site IT Staff Is Required During Activation	✓	✓
No Pre-Staging Is Required	✓	✓
No Security Risk if the Box Is Lost in Transit	✓	✓
Manual Device Configuration Errors Are Minimized	✓	✓
Designated Person Is Required to Click the Activation URL On-Site		✓
Laptop, Tablet, or Phone Is Required to Activate the Edge		✓

Technet24

4-32 About Zero-Touch Activation

During zero-touch activation, the VMware SD-WAN Edge appliance communicates with the VMware SD-WAN router, the orchestrator, and the gateway using various protocols.



The diagram depicts the communication stages between the edge, the router, VMware SD-WAN Orchestrator, and VMware SD-WAN Gateway during zero-touch activation.

4-33 Lab 3: Zero-Touch Provisioning

Configure the VMware SD-WAN Edge appliance:

1. Provision a New Branch
2. Activate a New Branch
3. Configure the LAN Interface of an Edge Appliance
4. Verify Network Connectivity

Technet24

4-34 Review of Learner Objectives

- List the steps required to commission an edge appliance onto the network
- Describe the process of provisioning an edge appliance
- Differentiate between provisioning and activating an edge appliance
- Discuss the methods of activating an edge appliance

4-35 Key Points

- VMware SD-WAN Orchestrator is a single application that administrators can use to configure and monitor the VMware SD-WAN network.
- A centralized management plane gives IT managers the ability to control and manage their networks with greater ease, agility, and programmability.
- The VMware SD-WAN hardware appliance is designed to be deployed quickly by non-technical branch employees.
- Provisioning an edge appliance takes place in VMware SD-WAN Orchestrator.
- You can activate an edge appliance with zero-touch activation or email link activation.

Questions?

Technet24

Module 5

Configuring VMware SD-WAN

5-2 Importance

VMware SD-WAN is a complex solution. To ensure that the infrastructure functions properly, you must account for a wide variety of features and configurations.

5-3 Module Lessons

1. Basic Network Configuration
2. Configuring Network Services
3. Configuring Profiles

5-4 Lesson 1: Basic Network Configuration

5-5 Learner Objectives

- Explain the basic network configuration of the VMware SD-WAN environment
- Describe segmentation in the VMware SD-WAN environment

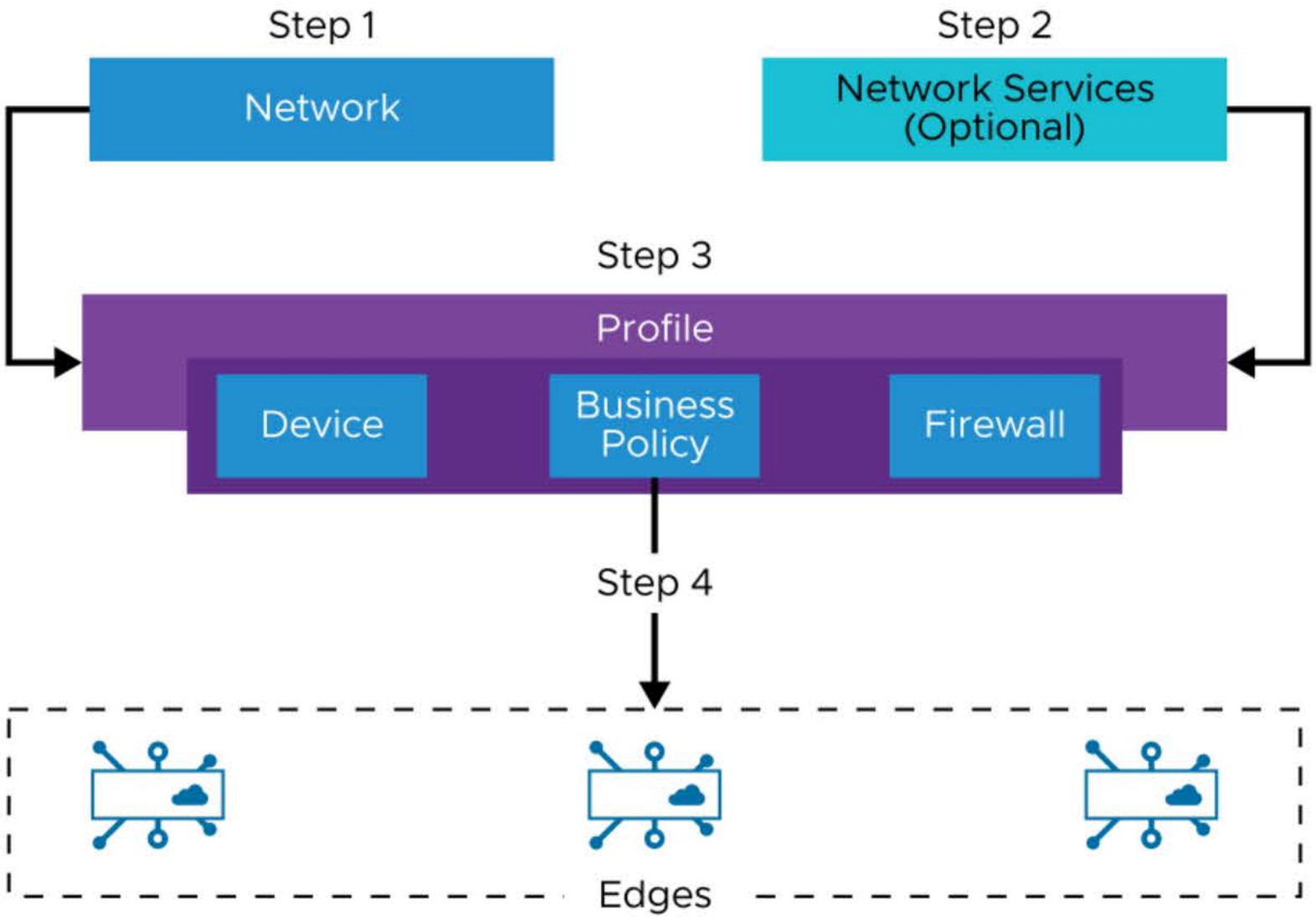
Technet24

5-6 VMware SD-WAN Configuration Workflow

The VMware SD-WAN service has four core configurations that constitute a hierarchical relationship.

The workflow for configuring VMware SD-WAN is as follows:

1. Configure the basic network.
2. Configure optional network services.
3. Create a profile.
4. Provision and activate edges.



Configuration includes the following details:

- Basic network configuration includes settings such as IP address, VLAN, segmentation, and so on.
- Optional network services that you can configure include DNS, authentication, cloud VPN services, and so on.
- Profile creation is the most important step. Most of the VMware SD-WAN configuration and management is done through profiles. You add the basic network settings and optional network services that you configured in the previous steps to the profile.
- You provision edges in VMware SD-WAN Orchestrator and activate the edges with email activation or zero-touch provisioning.

5-7 Configuring the Basic Network (1)

The first step of the VMware SD-WAN configuration workflow is the basic network configuration. This configuration includes IP addressing, VLANs, virtual routing and forwarding (VRF), segmentation, and so on.

Networks are standard configurations that define network address spaces and VLAN assignments for edges. You can configure the following network types:

- Corporate or trusted network: Overlapping or non-overlapping addresses
- Guest or untrusted network: Overlapping addresses only

The following details describe the differences between overlapping and non-overlapping addresses:

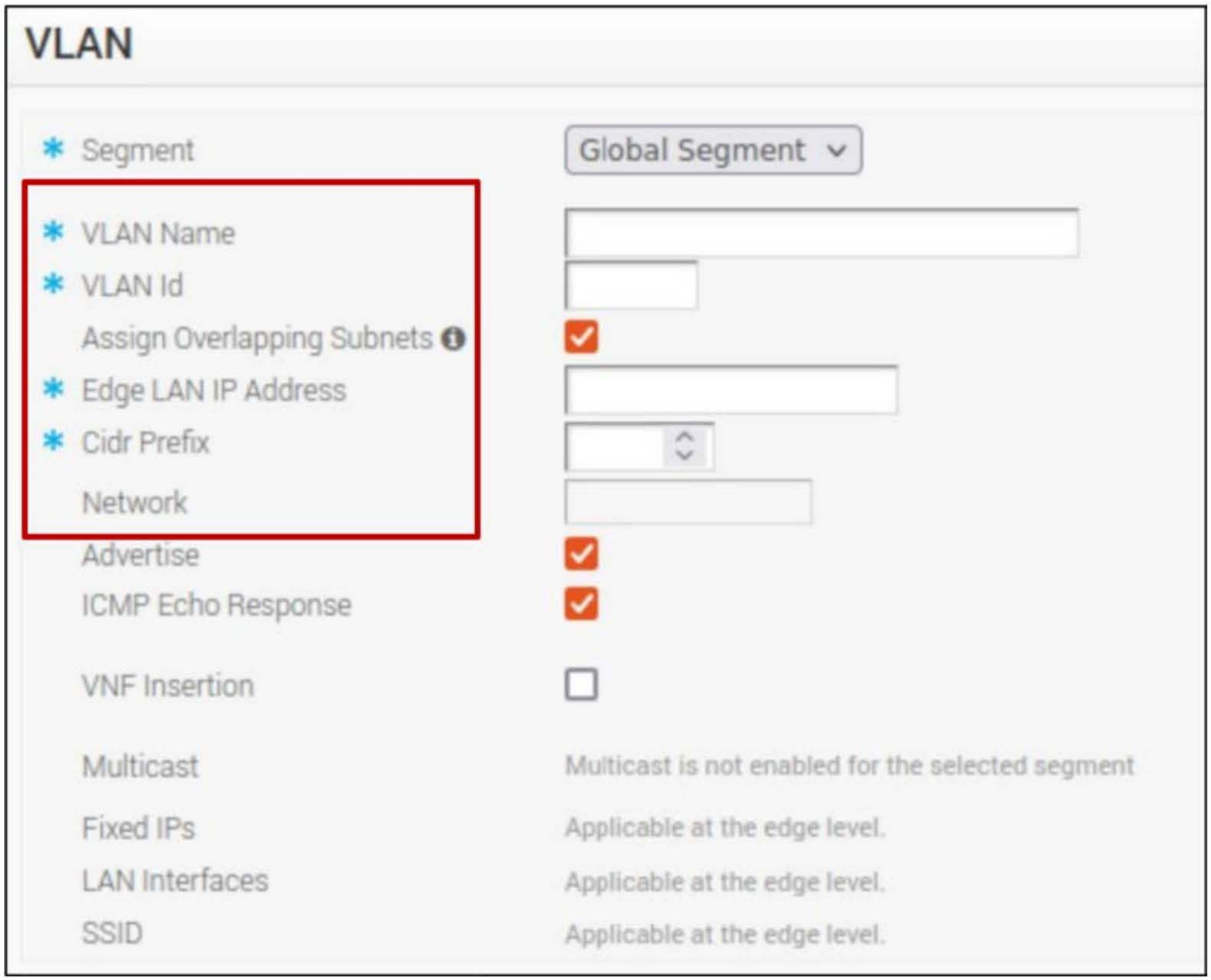
- Overlapping addresses:
  - All edges that use the network have the same address space.
  - Overlapping addresses are associated with non-VPN configurations.
- Non-overlapping addresses:
  - An address space is divided into blocks of an equal number of addresses.
  - Non-overlapping addresses are associated with VPN configurations.
  - Address blocks are assigned to edges that use the network so that each edge has a unique set of addresses.
  - Non-overlapping addresses are required for edge-to-edge and edge-to-non-SD-WAN-destination VPN communication.

When using non-overlapping addresses, VMware SD-WAN Orchestrator automatically allocates the blocks of addresses to the edges. This allocation is based on the maximum number of edges that might use the network configuration.

Technet24

5-8 Configuring the Basic Network (2)

You configure the VLAN, overlapping subnets, and other basic network settings at the profile level. You can also override the configuration at the edge level.



You manage the LAN IP addressing from the assigned profile of the edge. When you select the Assign Overlapping Subnets check box, the edge inherits the values for the LAN IP address, Classless Inter-Domain Routing (CIDR) prefix, and DHCP as read-only. The network address is automatically set based on the subnet mask and CIDR value.

5-9 Segmentation in LAN and WAN Networks

Segmentation refers to the division of the network into logical sub-networks called segments. Segmentation provides network isolation for management and security reasons.

Administrators deploy VLANs at layer 2 and VRFs at layer 3 to achieve segmentation within a campus and over a WAN, respectively. Modern networks also deploy VXLANs to achieve segmentation.

Technet24

5-10 Segmentation in VMware SD-WAN

As cloud traffic evolves and the demands of remote work increase, VLANs and VRFs are no longer adequate. Segmentation must be able to meet the following modern requirements:

- Applications can be accessed by diverse groups of employees, supply chain partners, customers, and so on.
- Application data is only seen by those who need to see it.
- Money transactions and card data are isolated and secure.
- Internet of things (IoT) traffic does not impact critical application traffic.
- Different traffic types require isolation and security.
- Traffic prioritization must be enabled based on traffic class.
- Quality of service (QoS) must be implemented to optimize application performance and user experience.

5-11 VMware SD-WAN Segmentation Use Cases

Segmentation in VMware SD-WAN environments include some of the following use cases:

- Line-of-business separation: Engineering, HR, sales, and so on
- User data separation: Guests, payment cards industry (PCI), employee versus corporate traffic
- Separation of enterprises with overlapping IP addresses in different VRFs
- Separation of traffic between tenants in multitenant environments
- Segmentation of VPNs for connecting off-network sites

VMware SD-WAN enables end-to-end segmentation. The edge device attaches a segment ID to the packet and forwards it to the hub and cloud gateway. This segmentation enables network service isolation from the edge to the cloud and the data center. As a result, you can group prefixes into a unique routing table, making the business policy segment aware.

Technet24

5-12 Types of Segments in VMware SD-WAN

You can configure VMware SD-WAN segments as either regular, cardholder data environment (CDE), or private:

- Regular: Caters to general traffic
- CDE: Manages traffic flows that require PCI functionality and must use VMware PCI certification
- Private: Addresses end-user privacy

If the segment is configured for regular traffic, then it does not require any special configuration.

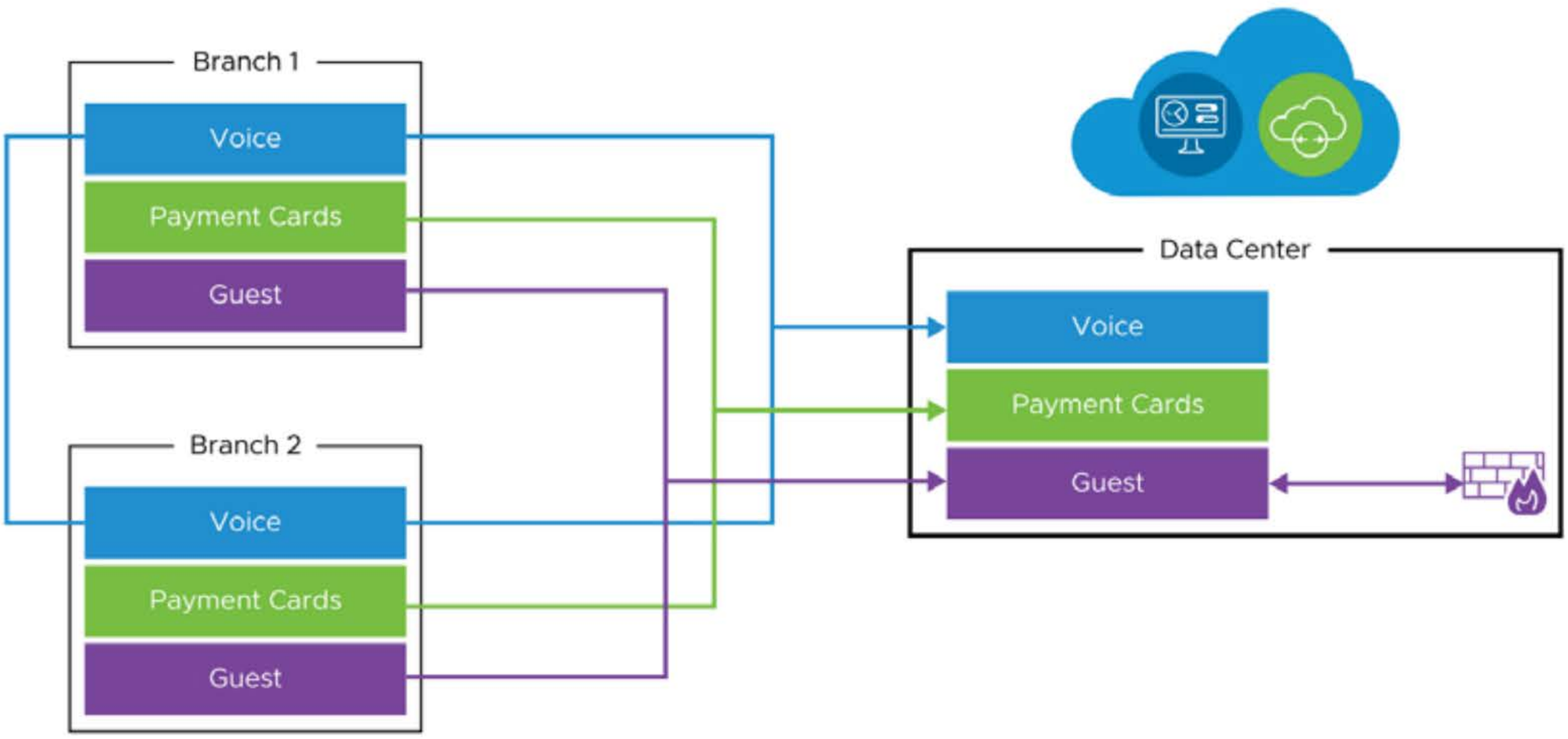
If the segment is configured as cardholder data environment (CDE), then the orchestrator and the controller become aware of the payment cards industry (PCI) segment and are in the PCI scope. Gateways (marked as non-CDE gateways) do not transmit PCI traffic and are out of the PCI scope.

If the segment is configured as private, then the segment does not perform the following actions:

- Upload user traffic statistics to VMware SD-WAN Orchestrator
- Allow users to view traffic in remote diagnostics
- Allow traffic to be sent as Internet multipath

5-13 VMware SD-WAN Segmentation Topology

The topology in the diagram demonstrates a common enterprise segmentation scenario. Two branches communicate with one data center, and each branch has three segmentations for the customer: voice, guest, and PCI.



The topology in the diagram demonstrates a common enterprise segmentation scenario. Two branches communicate with one data center, and each branch has voice, guest, and PCI segmentations:

- Different branches can subscribe to different segments.
- VMware SD-WAN Edge instances send internal routes learned over Interior Gateway Protocol (IGP) or Border Gateway Protocol (BGP) to the controller.
- Edges receive routes from other edges in the same segment as the controller.
- VMware SD-WAN Edge does not receive routes about segments to which it does not subscribe.
- By default, each segment does not have routes from other segments.
- Voice traffic between two branches routes directly between them.
- Guest traffic between two branches routes to the data center and reverses direction at the firewall.
- PCI traffic transfers directly to the PCI network in the data center.

For more information about how traffic for each segment is managed, see “VMware SD-WAN topology” in *VMware SD-WAN Delivers Automated Network Segmentation for the Enterprise* at https://sase.vmware.com/content/dam/digitalmarketing/vmware-sase/pdfs/sdwan-589-automated-network-segmentation-wp-1220.pdf.

Technet24

5-14 Configuring Segmentation for an Enterprise

You configure segmentation in VMware SD-WAN Orchestrator.

To configure segmentation for an enterprise:

1. Select **Configure** > **Segments** from the navigation pane on the left.

   The Segments page for the selected enterprise appears.

2. Click the plus sign (+) icon to create a new segment.

3. Provide the requested information.

You must specify the following information when you create a new segment:

- Segment Name:
  - Specify the name for a specific segment of traffic.
  - Global Segment is the default segment for any traffic that is not explicitly assigned to a specific segment.
- Service VLAN:
  - Specify the identifier for the VLAN configured for that segment.
  - For example, if voice traffic must be handled over VLAN 101, enter **101** under Service VLAN.

5-15 Lab 4: Configuring Segmentation

Configure segments and firewall rules:

1. Configure a Cardholder Data Environment Segment
2. Configure a Guest Segment
3. Configure a CDE Segment Firewall Rule
4. Test the CDE Segment Firewall Rule
5. Test the Guest Segment with No Firewall Rule
6. Reconnect the Edge to the Corporate VLAN

Technet24

5-16 Review of Learner Objectives

- Explain the basic network configuration of the VMware SD-WAN environment
- Describe segmentation in the VMware SD-WAN environment

5-17 Lesson 2: Configuring Network Services

5-18 Learner Objectives

- List the configurable network services
- Demonstrate how to configure some of the optional network services

Technet24

5-19 Configurable Network Services

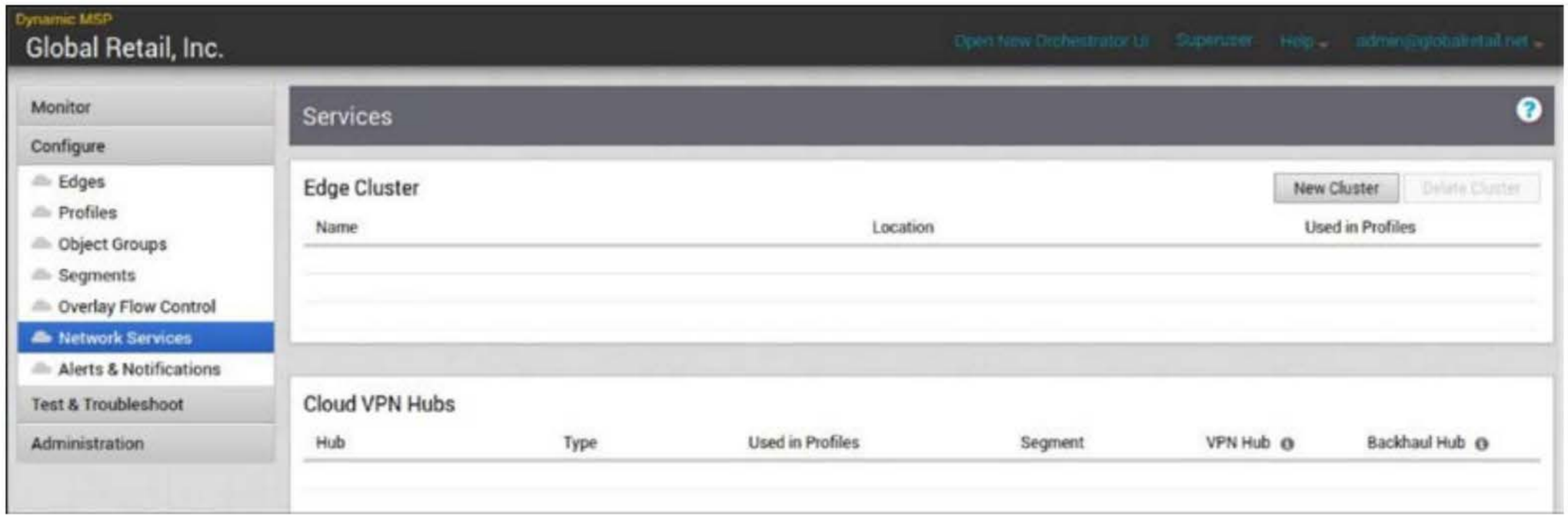
As an enterprise user, VMware SD-WAN Orchestrator allows you to configure multiple network services:

- Edge clusters
- Cloud VPN hubs
- Non-SD-WAN destinations through VMware SD-WAN Gateway
- Non-SD-WAN destinations through VMware SD-WAN Edge
- Cloud security service (CSS)
- Virtual network functions (VNFs)
- VNF licenses
- DNS services
- Netflow settings
- Private network names
- Authentication services
- Infrastructure-as-a-service (IaaS) subscriptions

All the services listed in the slide are optional.

5-20 Configuring Network Services

You can configure network services in the VMware SD-WAN Orchestrator portal by logging in as Customer and selecting **Configure** > **Network Services**. The configurable network services appear in the pane on the right.



Technet24

5-21 Configuring Non-SD-WAN Destinations

You can connect non-SD-WAN destinations to a VMware network. A secure Internet Protocol Security (IPsec) tunnel is created between a VMware SD-WAN site and a VPN gateway of the network provider.

You can define and configure a data center as a non-SD-WAN destination and establish connectivity with VMware SD-WAN Gateway or VMware SD-WAN Edge.

5-22 Non-SD-WAN Destination Configuration Workflow

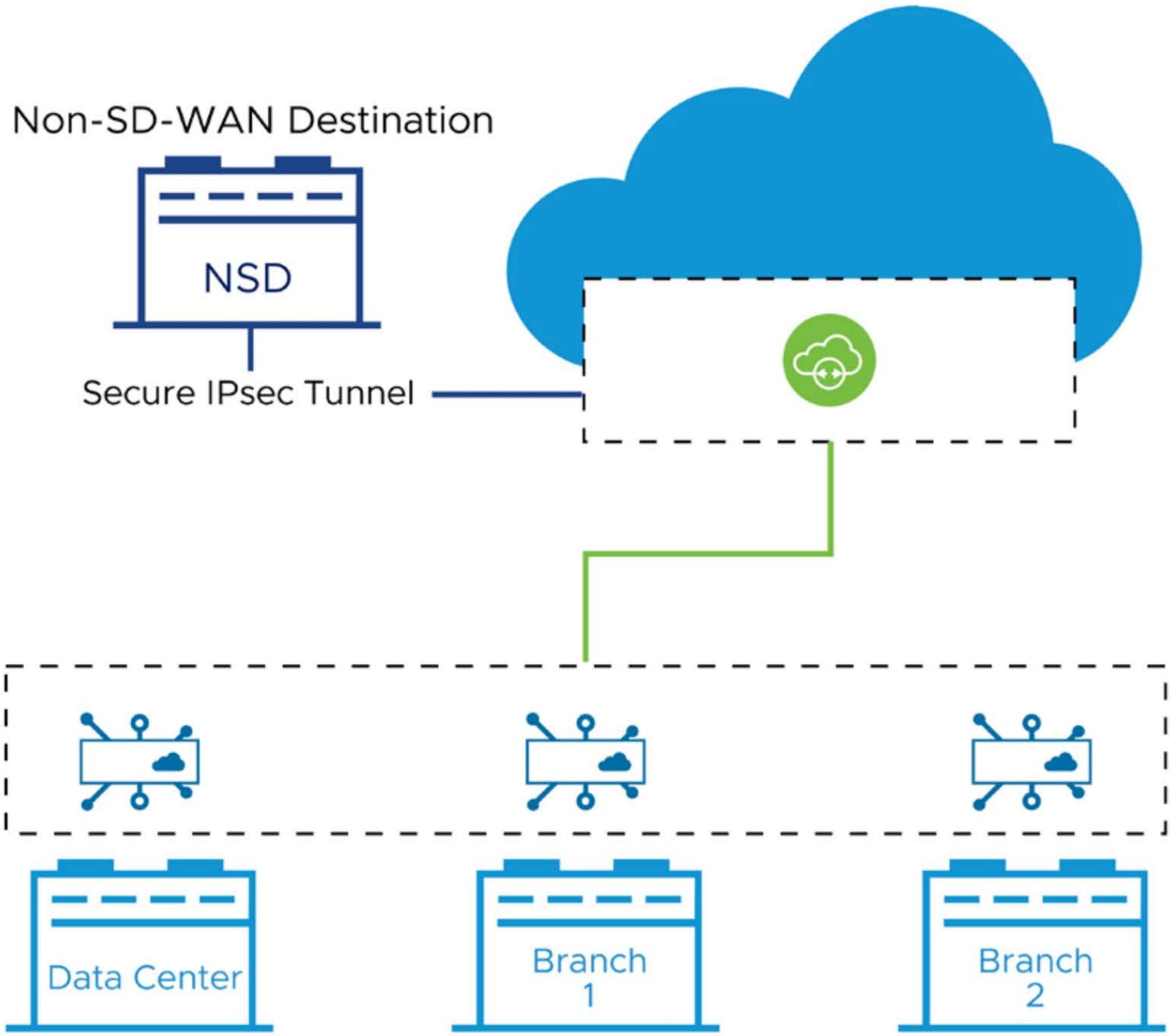
The general workflow for configuring a non-SD-WAN destination is as follows:

1. Configure a non-SD-WAN destination network service.
2. Associate a non-SD-WAN destination network service to a profile or edge.
3. Configure tunnel parameters:
    a.. WAN link selection
    b.. Per-tunnel credentials
4. Configure a business policy.

Technet24

5-23 Non-SD-WAN Destinations Through VMware SD-WAN Gateway

VMware supports many non-SD-WAN destinations through VMware SD-WAN Gateway. Connecting to a non-SD-WAN-destination through a gateway provides protections from unstable links between the edge and the gateway, offering a higher-quality experience.



VMware supports the following non-SD-WAN-destination configurations through VMware SD-WAN Gateway:

- AWS VPN Gateway
- Check Point
- Cisco ASA
- Cisco ISR
- Generic IKEv1 Router (route-based VPN)
- Generic IKEv2 Router (route-based VPN)
- Palo Alto Networks
- Microsoft Azure Virtual Hub
- SonicWALL
- Zscaler
- Generic Firewall (policy-based VPN)

Technet24

5-24 Configuring Access to Non-SD-WAN Destinations from a Gateway

You use the VMware SD-WAN Orchestrator portal to configure non-SD-WAN destinations through gateways.

To configure access to a non-SD-WAN destination using VMware SD-WAN Gateway:

1. In the VMware SD-WAN Orchestrator portal, select **Configure** > **Network Services** from the navigation pane on the left.

   The Services pane appears on the right.
2. Under Non SD-WAN Destinations via Gateway, click **New**.

   The New Non SD-WAN Destination via Gateway dialog box appears.
3. In the **Name** text box, enter the name of the new non-SD-WAN destination.
4. From the **Type** drop-down menu, select the gateway type for your environment.

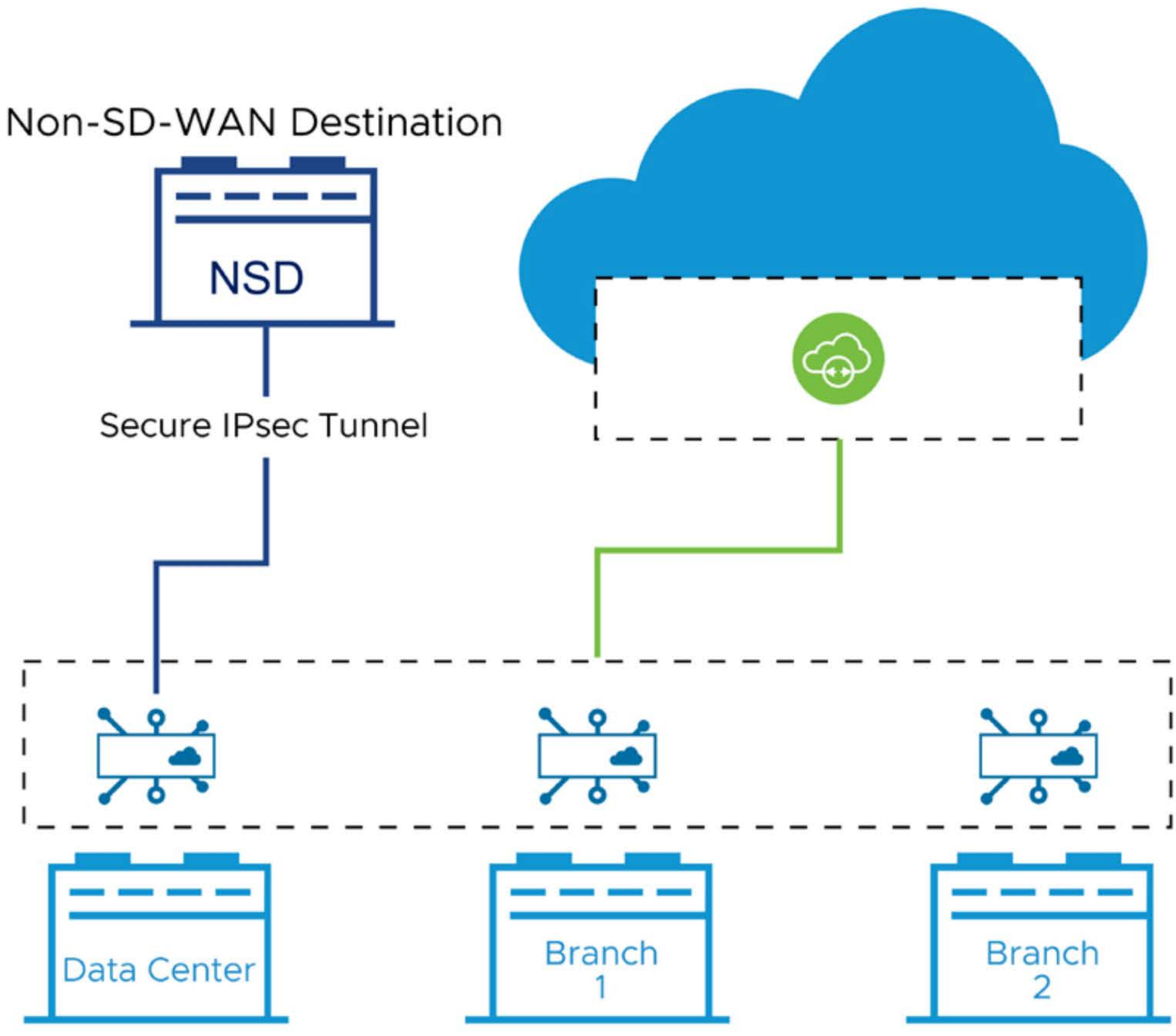
   In the screenshot, **Cisco ASA** is selected.
5. Enter the IP address in the **Primary VPN Gateway** text box and click **Next**.
6. Enter the requested information and click **Save Changes**.

5-25 Non-SD-WAN Destinations Through VMware SD-WAN Edge

You can enable a VMware SD-WAN Edge appliance to establish an IPsec tunnel directly to a non-SD-WAN destination. This direct tunnel connects a VMware network to an external network. This connection is achieved by creating a secure IPsec tunnel between a VMware entity and a VPN gateway at the network provider.

VMware supports the following non-SD-WAN destination configurations through VMware SD-WAN Edge:

- Generic IKEv1 Router
- Generic IKEv2 Router
- Microsoft Azure Virtual WAN



Technet24

External networks that can connect to a VMware network through a VMware SD-WAN Edge IPsec tunnel include the following examples:

- Zscaler
- Cloud Security Service
- Microsoft Azure
- Amazon AWS
- Partner data centers

5-26 Configuring Access to Non-SD-WAN Destinations from an Edge (1)

You also use the VMware SD-WAN Orchestrator portal to configure non-SD-WAN destinations through VMware SD-WAN Edge.

To configure access to a non-SD-WAN destination using VMware SD-WAN Edge:

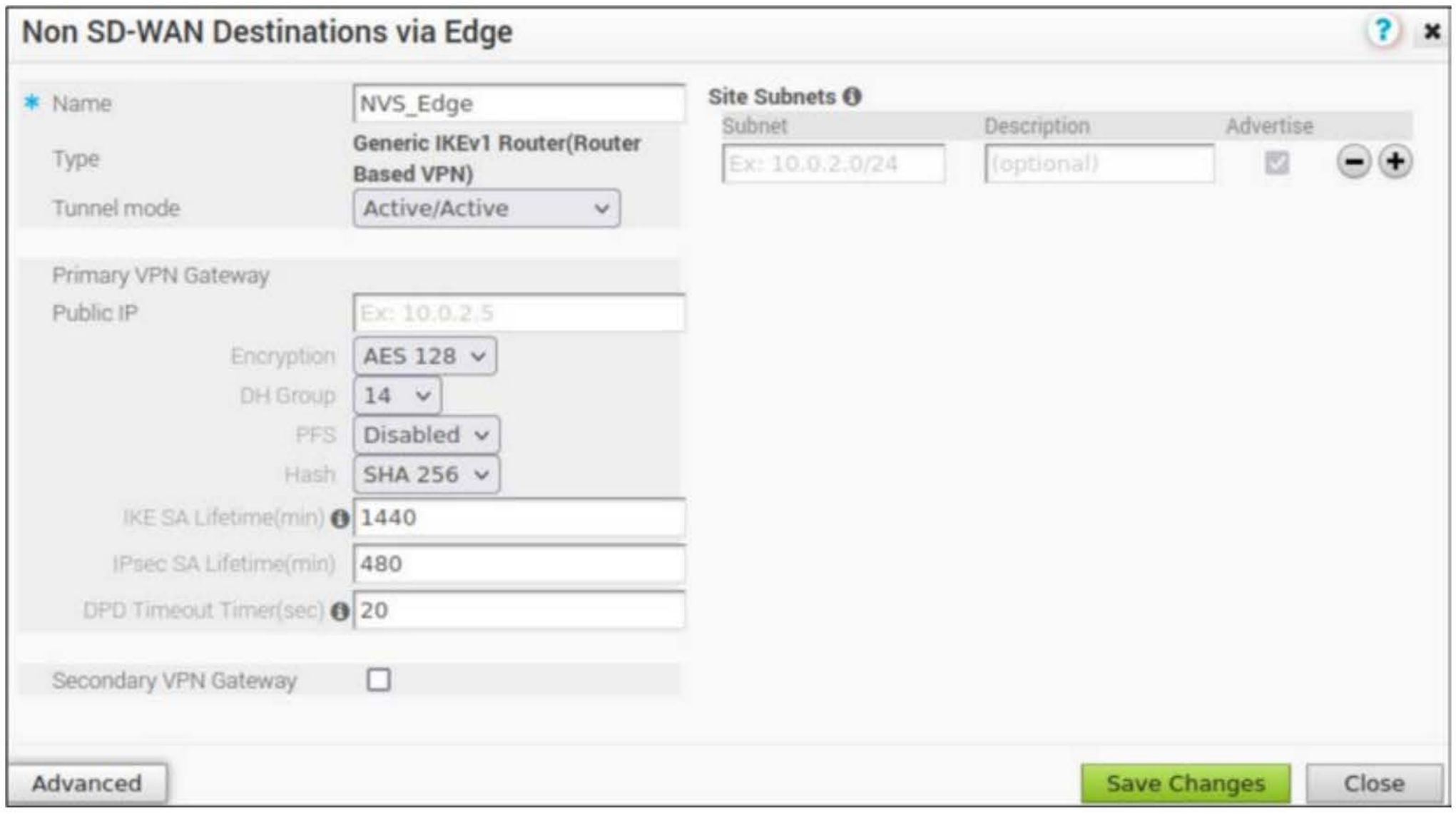
1. From the navigation panel in the SD-WAN Orchestrator, select **Configure** > **Network Services**.

   The Services pane appears on the right.
2. Under Non SD-WAN Destinations via Edge, click **New**.

   The New Non SD-WAN Destinations via Edge dialog box appears.
3. In the **Service Name** text box, enter the name of the non-SD-WAN Destination.
4. From the **Service Type** drop-down menu, select one of the available options and click **Next**.
5. Provide the requested information and click **Save Changes**.

Technet24

5-27 Configuring Access to Non-SD-WAN Destinations from an Edge (2)



See the chapter about configuring network services in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

5-28 About DNS Services

You can configure public and private DNS services in VMware SD-WAN Orchestrator. You can also specify both a primary server and a backup server. The service is preconfigured to use Google and OpenDNS servers.

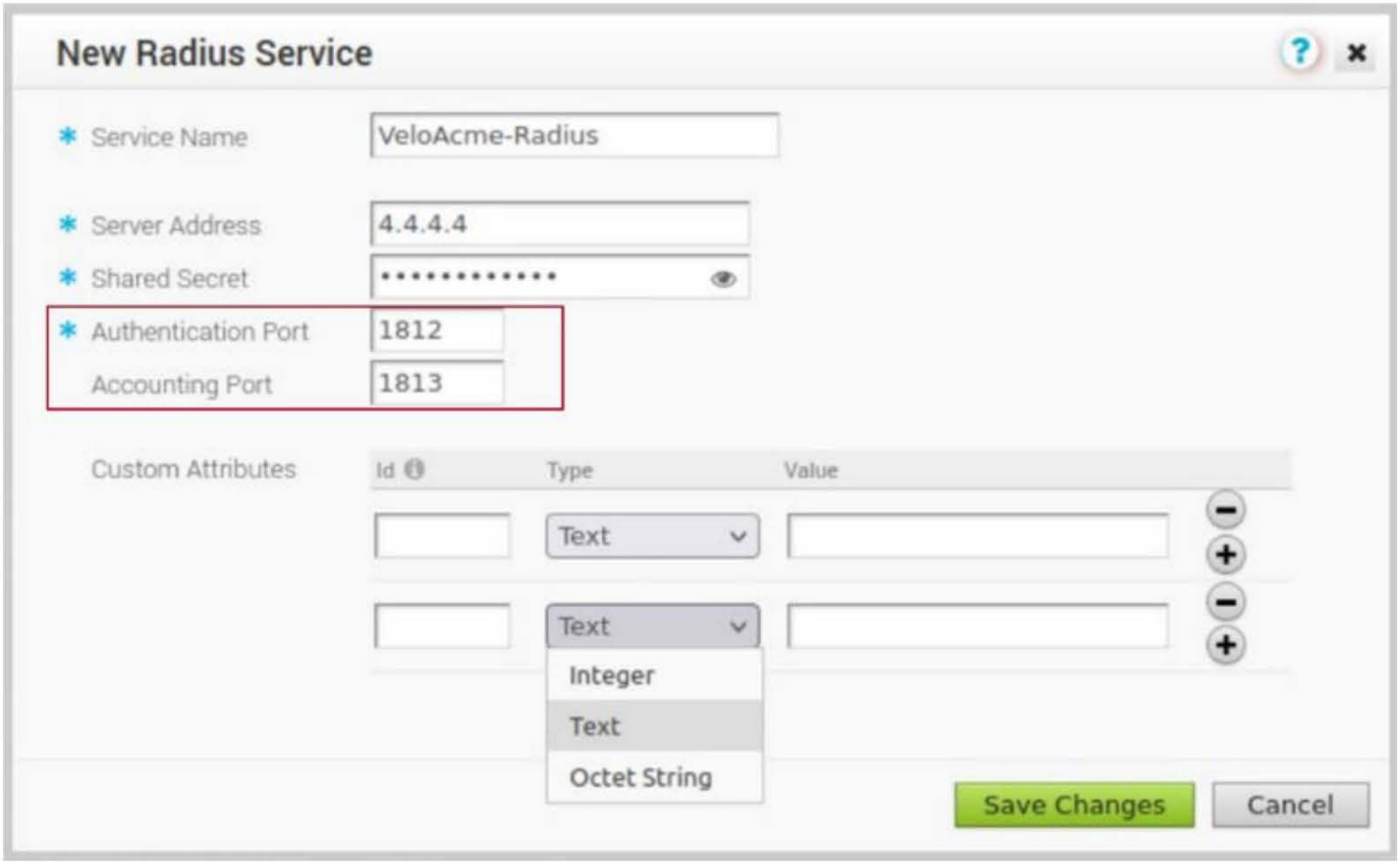
Technet24

5-29 Configuring DNS Services

You can configure the public and private DNS servers with primary and backup servers. The private DNS can also be configured with private domains.

5-30 About Authentication Services

Authentication and accounting are optional but important services used to restrict access to resources. You can create a network service that specifies the IP address and ports for the service.



Technet24

5-31 About Cloud Security Services

A CSS protects enterprise branches or data centers through firewalls, URL filtering, and so on. The tunnel between VMware SD-WAN Edge and CSS sites ensures that the flow of traffic remains secure.

A branch edge can also establish a direct tunnel to the cloud service point of presence (PoP). This option offers several advantages:

- Simplifying configuration
- Offloading non-enterprise traffic to the Internet, conserving SD-WAN bandwidth
- Protecting against malicious traffic by redirecting Internet traffic to a CSS

Currently, the connectivity from a branch edge to a cloud service or a non-SD-WAN destination is established through VMware SD-WAN Gateway. In this model, the gateway aggregates traffic from multiple branch edges and securely forwards the traffic to the non-SD-WAN-destination.

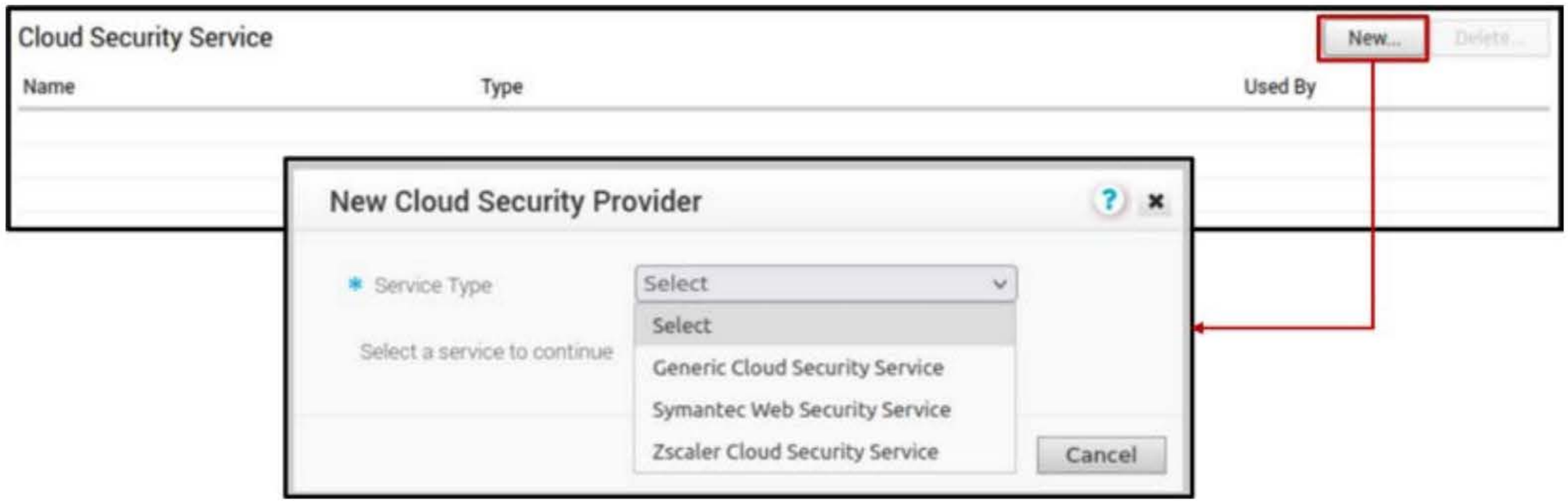
5-32 Configuring a Cloud Security Provider (1)

The secure tunnel between VMware SD-WAN Edge and CSS sites ensures a secure flow of traffic.

To configure a cloud security provider:

1. In VMware SD-WAN Orchestrator, select **Configure** > **Network Services**.
2. Click **New**.

   The New Cloud Security Provider dialog box appears.
3. Select one of the available options from the **Service Type** drop-down menu.



Technet24

5-33 Configuring a Cloud Security Provider (2)

The following services are available when you configure a new cloud security provider:

- Generic Cloud Security Service
- Symantec Web Security Service
- Zscaler Cloud Security Service

See the chapter about configuring cloud security providers in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

5-34 Configuring a Cloud Security Provider (3)

Successfully configured cloud security providers appear under Cloud Security Service in the orchestrator.

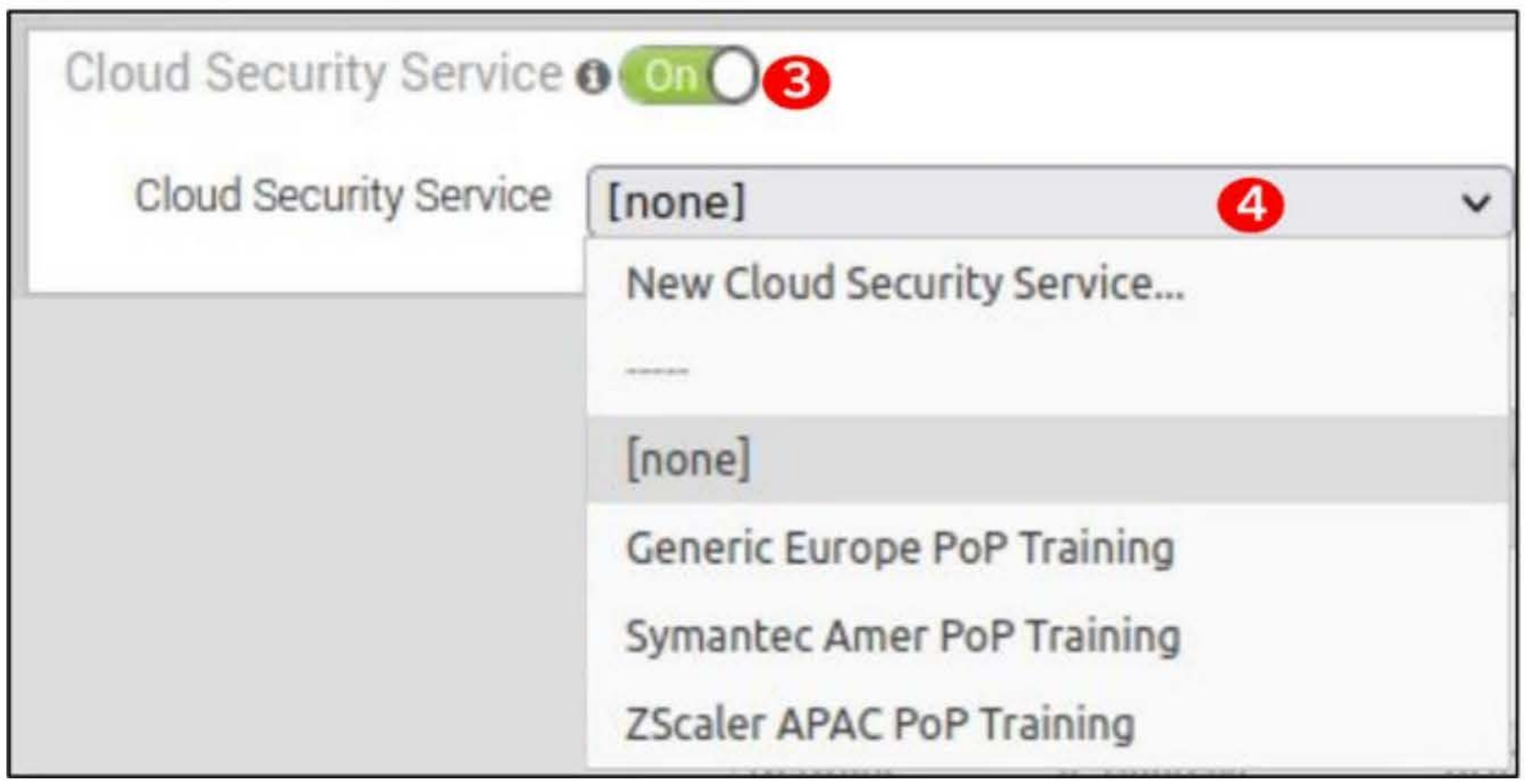
Technet24

5-35 Configuring Cloud Security Services for Profiles

A CSS protects both enterprise branches and data centers. The security services available include firewalls, URL filtering, VPN, and so on.

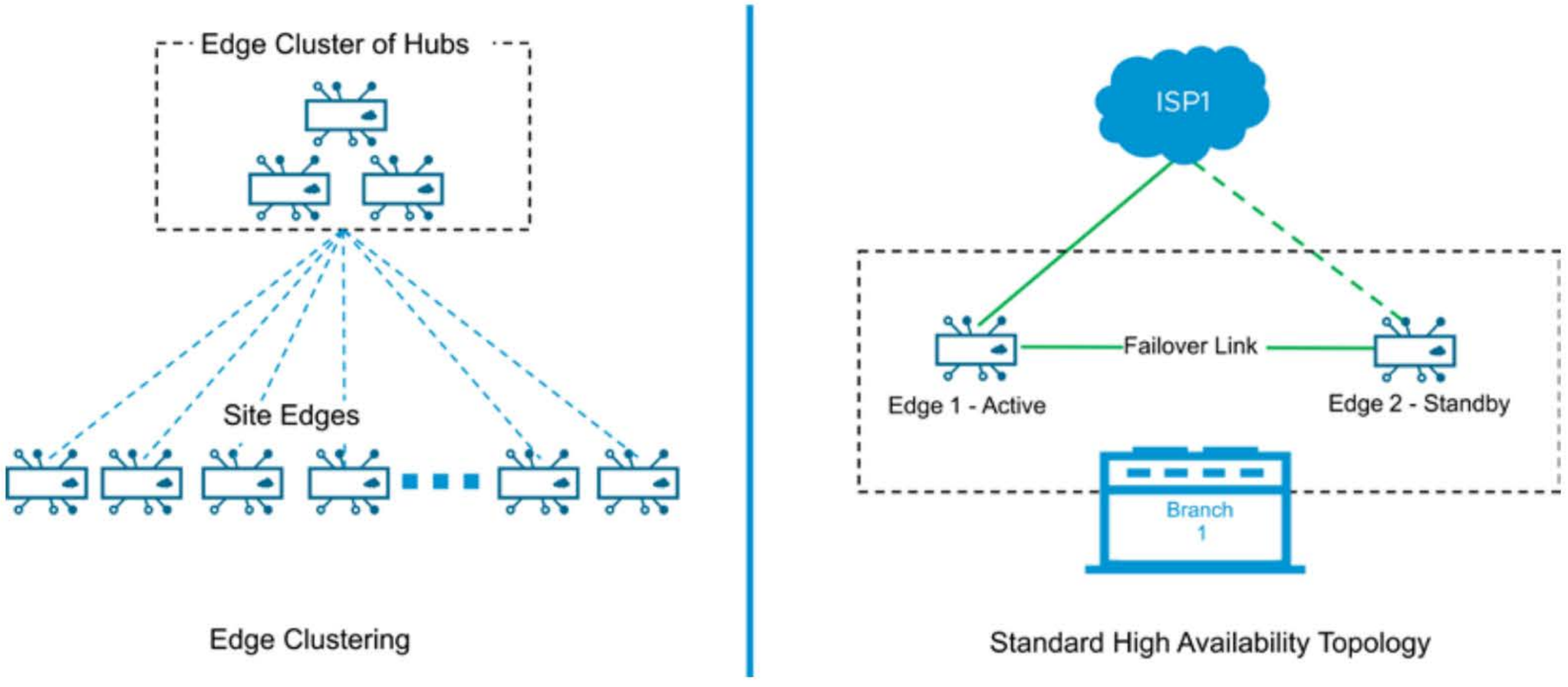
To configure a CSS for a profile:

1. In VMware SD-WAN Orchestrator, select **Configure** > **Profiles**.
2. Click the **Device** tab in the right pane.
3. To enable the service, turn on the **Cloud Security Service** toggle.
4. From the **Cloud Security Service** drop-down menu, select one of the configured cloud security providers.
5. Click **Save Changes**.



5-36 About the Edge Clustering Service

For hub locations, active-standby edge high availability may be insufficient. Edge clustering allows for active-active high availability, as well as load distribution among multiple devices for enhanced scale. Clustering also simplifies management because all members of a cluster are treated as a common entity.



The diagram demonstrates the difference between edge clustering and edge high availability configurations.

Edge clustering addresses the issue of SD-WAN hub scale. By creating a logical cluster of edges, edge clustering can easily and dynamically expand the tunnel capacity of the hub. Edge clustering also provides resilience through the active-active high availability topology that a cluster of VMware SD-WAN Edge appliances provides. A cluster is functionally treated as an individual hub from the perspective of other edges.

The hubs in a cluster can consist of either physical or virtual edges. If they are virtual, they can exist on a single hypervisor or across multiple hypervisors. Typically, edge clusters are deployed as hubs in data centers.

Technet24

5-37 About Cluster Scores

A cluster score is a mathematical calculation of the utilization of resources. The utilization factors measured in a cluster score are as follows:

- CPU usage
- Memory usage
- Tunnel capacity

An integer-based cluster score (1 to 100) is calculated from these factors. For example, you can determine the cluster score of an Edge 2000 using the following calculations:

- CPU usage: 20 percent
- Memory usage: 30 percent
- Connected tunnels: 600 / (capacity of 6,000) = 10 percent
- Cluster score: (20 + 30 + 10) / 3 = 20

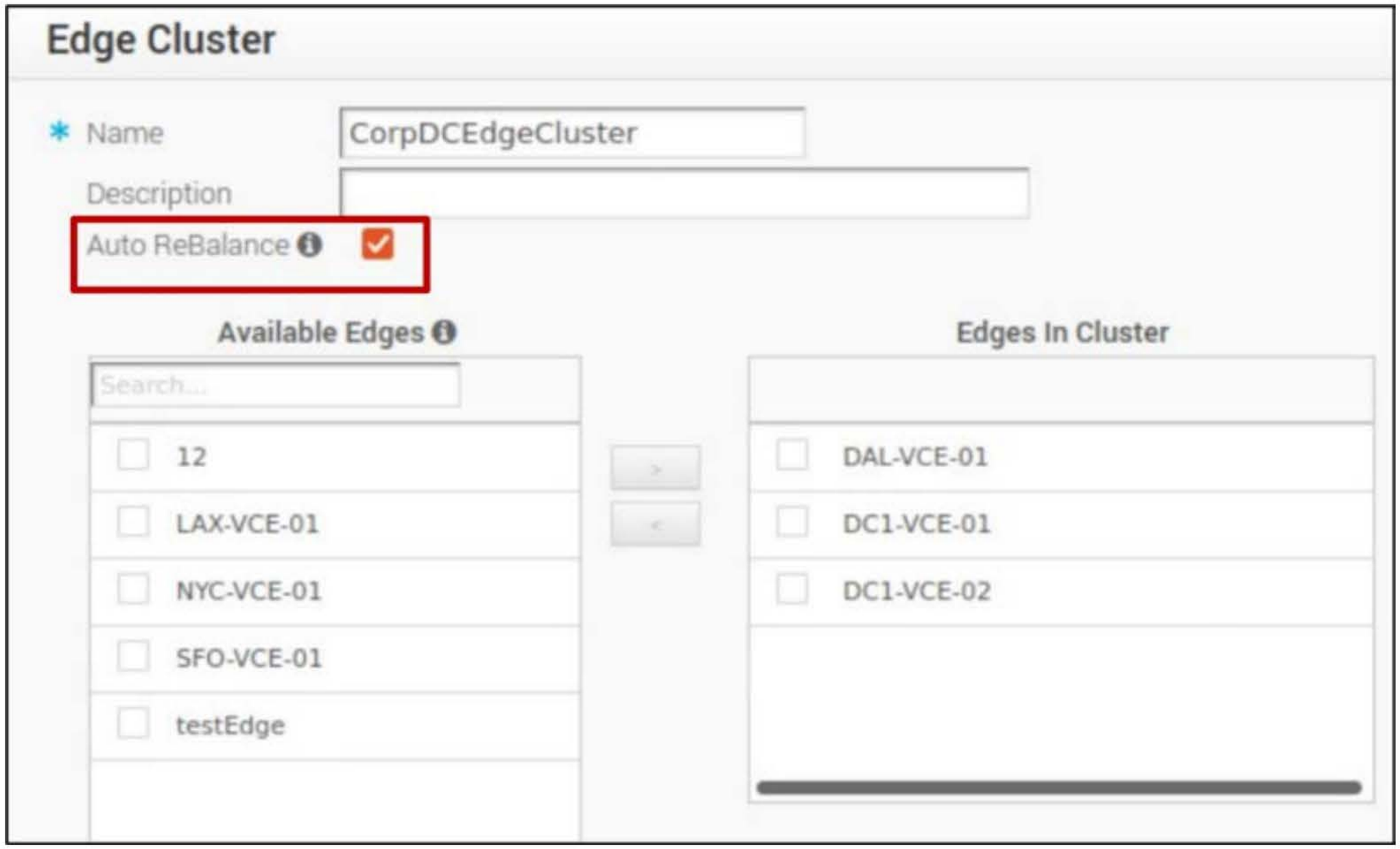
A cluster score greater than 70 is considered over capacity.

5-38 About Auto Rebalance

Auto Rebalance ensures that the resources of a hub are utilized evenly.

You use the cluster score of a hub to perform Auto Rebalance in the following situations:

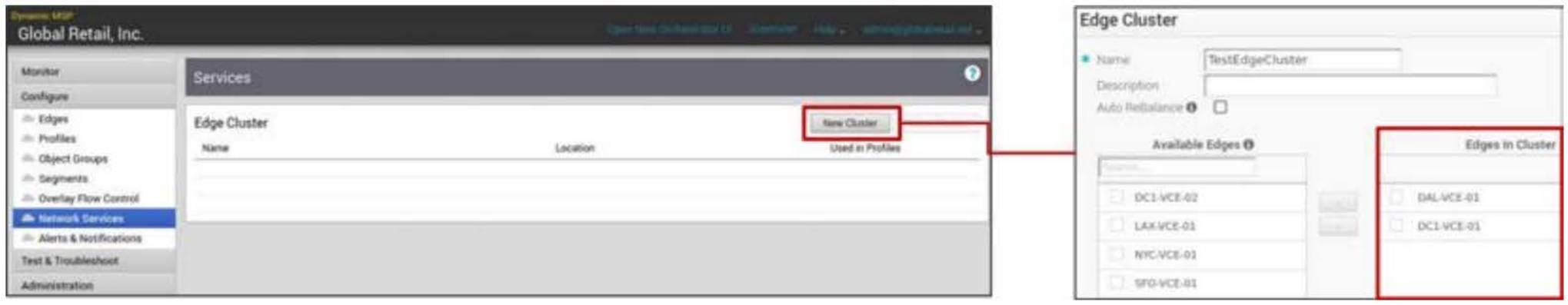
- If Auto Rebalance is deactivated and a hub exceeds a cluster score of 70 (but not 70 percent tunnel capacity), then no action is taken.
- If Auto Rebalance is enabled and one or more hubs exceed a cluster score of 70, the gateway reassigns one edge per minute to the hub with the lowest cluster score until all hubs are below 70 or no more reassignments are possible.



Technet24

5-39 Configuring an Edge Cluster

You can configure edge clusters in VMware SD-WAN Orchestrator. You can select which edges you want to add to each cluster.



To configure a new edge cluster in VMware SD-WAN Orchestrator:

1. Select **Configure** > **Network Services**.
2. Click **New Cluster** in the Edge Cluster pane.
3. In the Edge Cluster dialog box, enter the name and description in the appropriate text boxes.
4. Select the **Auto Rebalance** check box if needed.

   This feature is not enabled by default.
5. Under Available Edges, select the check box for the desired edge.
6. Click the right arrow to move the selected edge to the Edges In Cluster column.
7. Click **Save**.

5-40 Review of Learner Objectives

- List the configurable network services
- Demonstrate how to configure some of the optional network services

Technet24

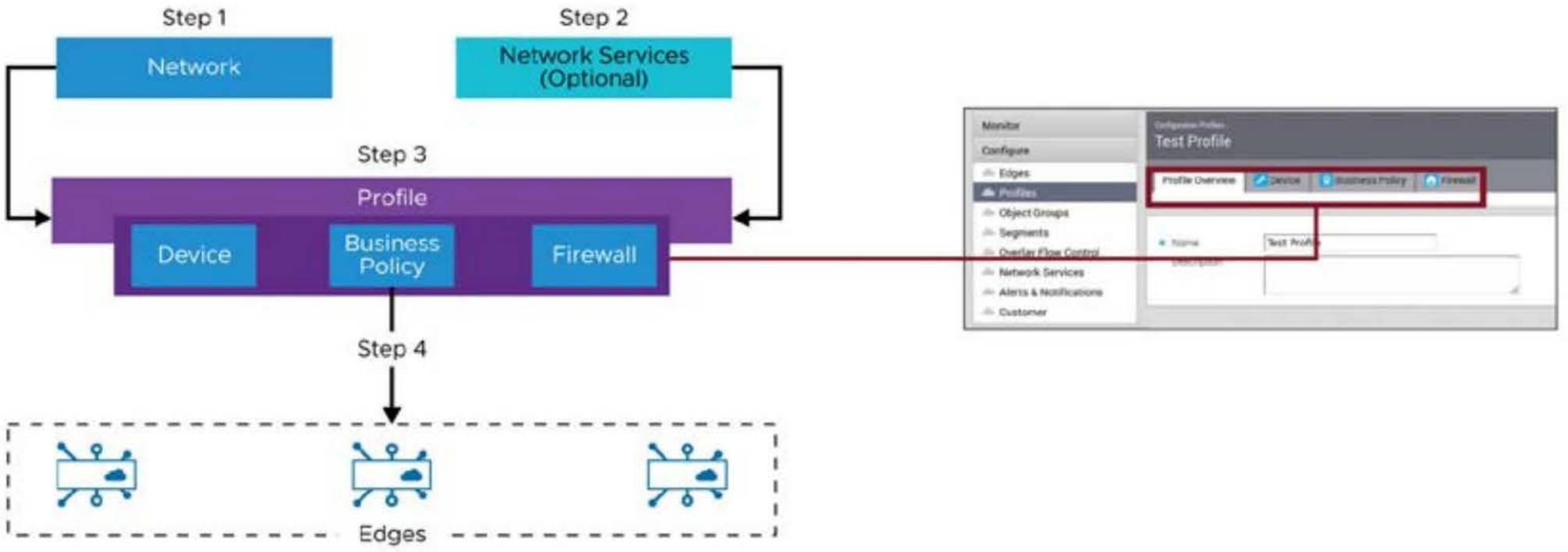
5-41 Lesson 3: Configuring Profiles

5-42 Learner Objectives

- Describe how to create a profile in VMware SD-WAN
- Demonstrate how to configure a profile device
- Demonstrate how to configure a business policy rule
- Demonstrate how to configure the interfaces of an edge device
- Differentiate between stateful and stateless firewalls
- Demonstrate how to configure a firewall rule

5-43 About Profiles in VMware SD-WAN

A profile in VMware SD-WAN defines a template configuration that can be applied to multiple edges. It also defines the settings for the LAN, Internet, wireless LAN, and WAN edge interfaces.



Profiles can also provide settings for Wi-Fi radio, Simple Network Management Protocol (SNMP), Netflow, business policies, and firewall configuration.

Using profiles, you can define a standard configuration for one or more VMware SD-WAN Edge devices. Profiles can also define rules and configurations for business policies and firewall settings.

Technet24

5-44 Workflow for Creating a New Profile

Creating a new profile involves the following tasks:

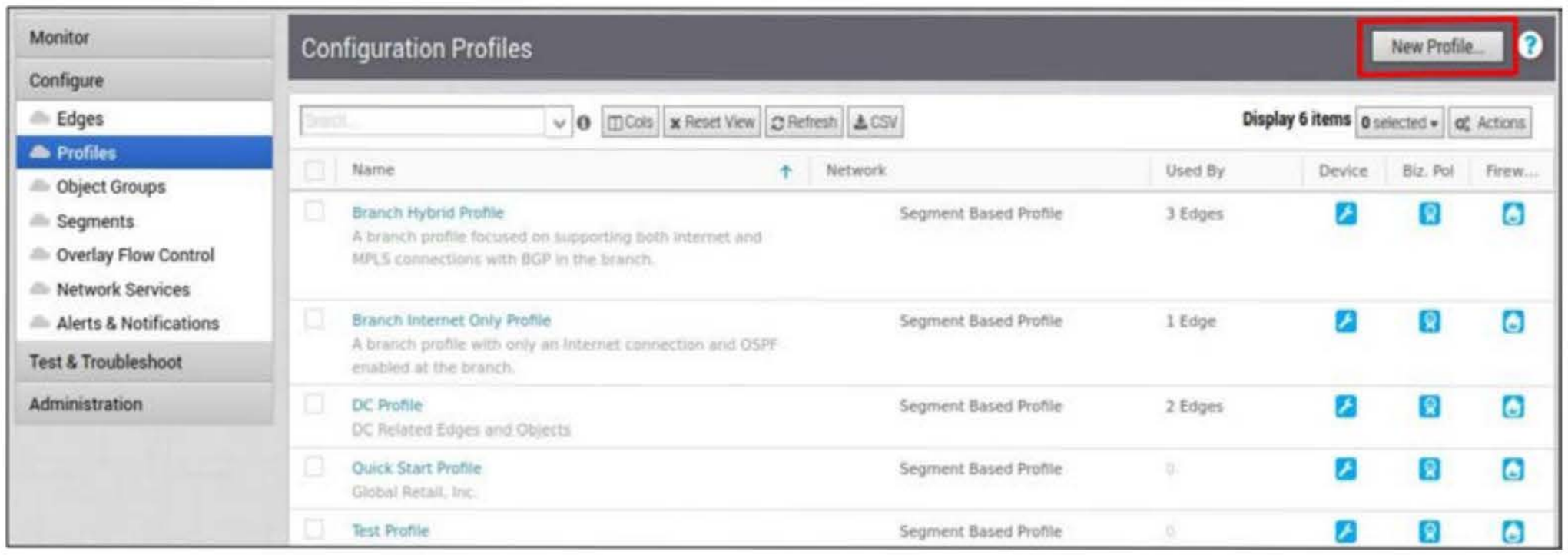
1. Create a profile.
2. Configure a device.
3. Configure Cloud VPN for the profile.
4. Configure a business policy for the profile.
5. Configure a firewall for the profile.

5-45 Creating a New Profile

You use VMware SD-WAN Orchestrator to create new profiles.

To create a new profile:

1. Select **Configure** > **Profiles**.
2. Under Configuration Profiles, click **New Profile**.



Technet24

5-46 Configuring a Profile Device

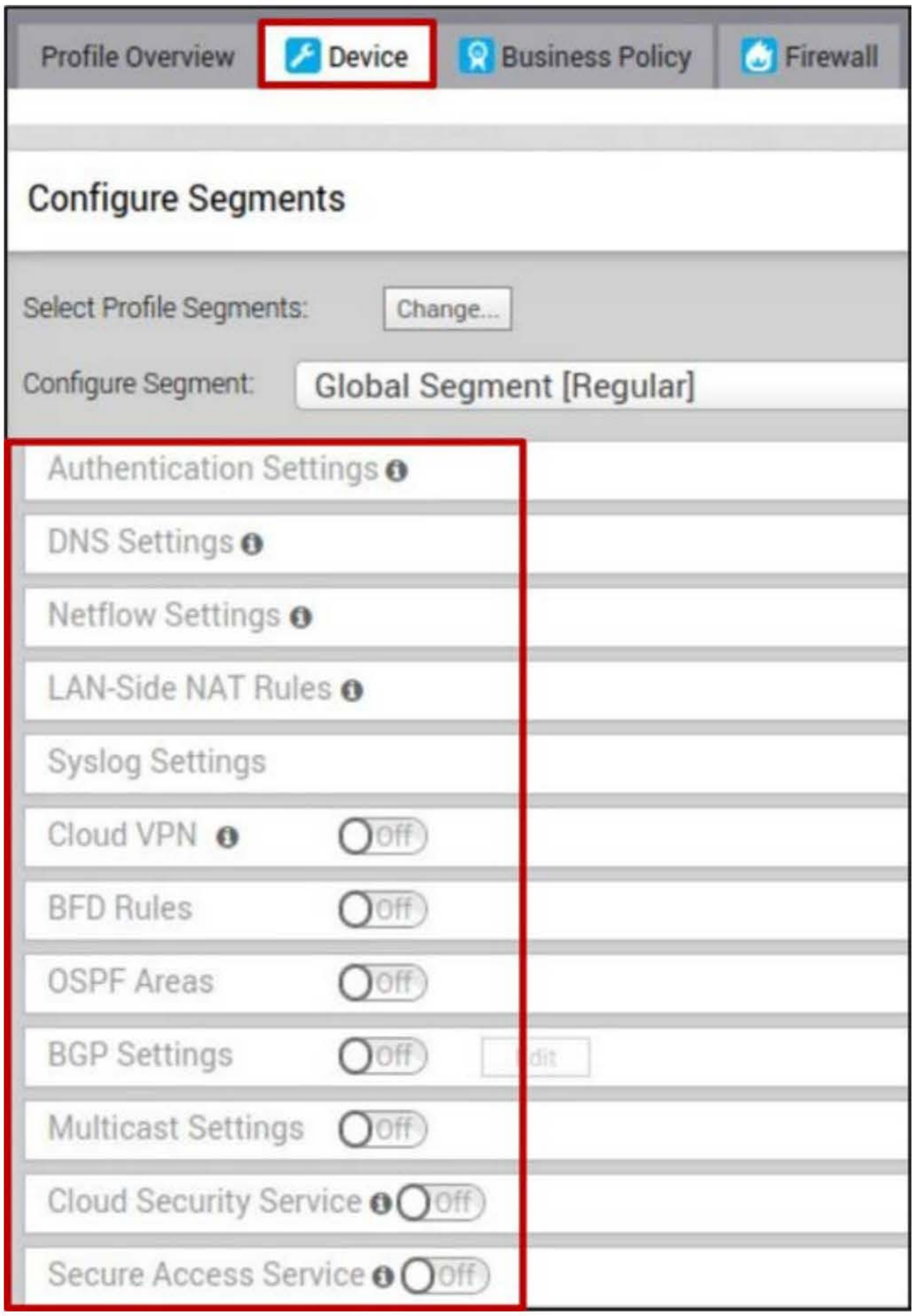
Device configuration allows you to assign segments to a profile and configure which interfaces are associated with it. The following types of device configurations are available:

- Segment-aware configurations
- Common configurations

5-47 Segment-Aware Configuration

Segment-aware configuration in VMware SD-WAN Orchestrator includes the following settings and options:

- Authentication Settings
- DNS Settings
- Netflow Settings
- LAN-Side NAT Rules
- Syslog Settings
- Cloud VPN
- BFD Rules
- OSPF Areas
- BGP Settings
- Multicast Settings
- Cloud Security Service
- Secure Access Service

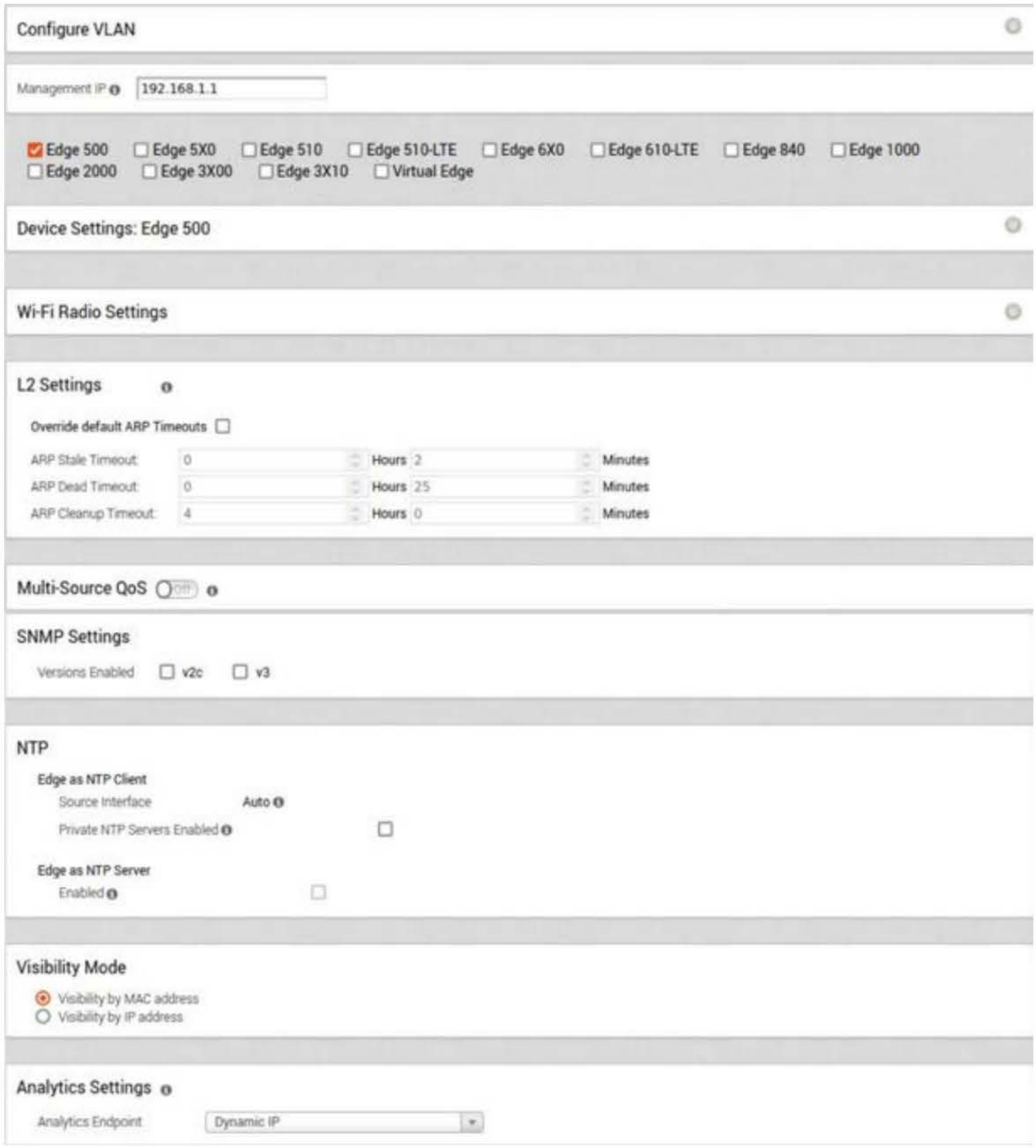


Technet24

5-48 Common Configuration

Common configuration refers to the settings and features that apply to multiple segments:

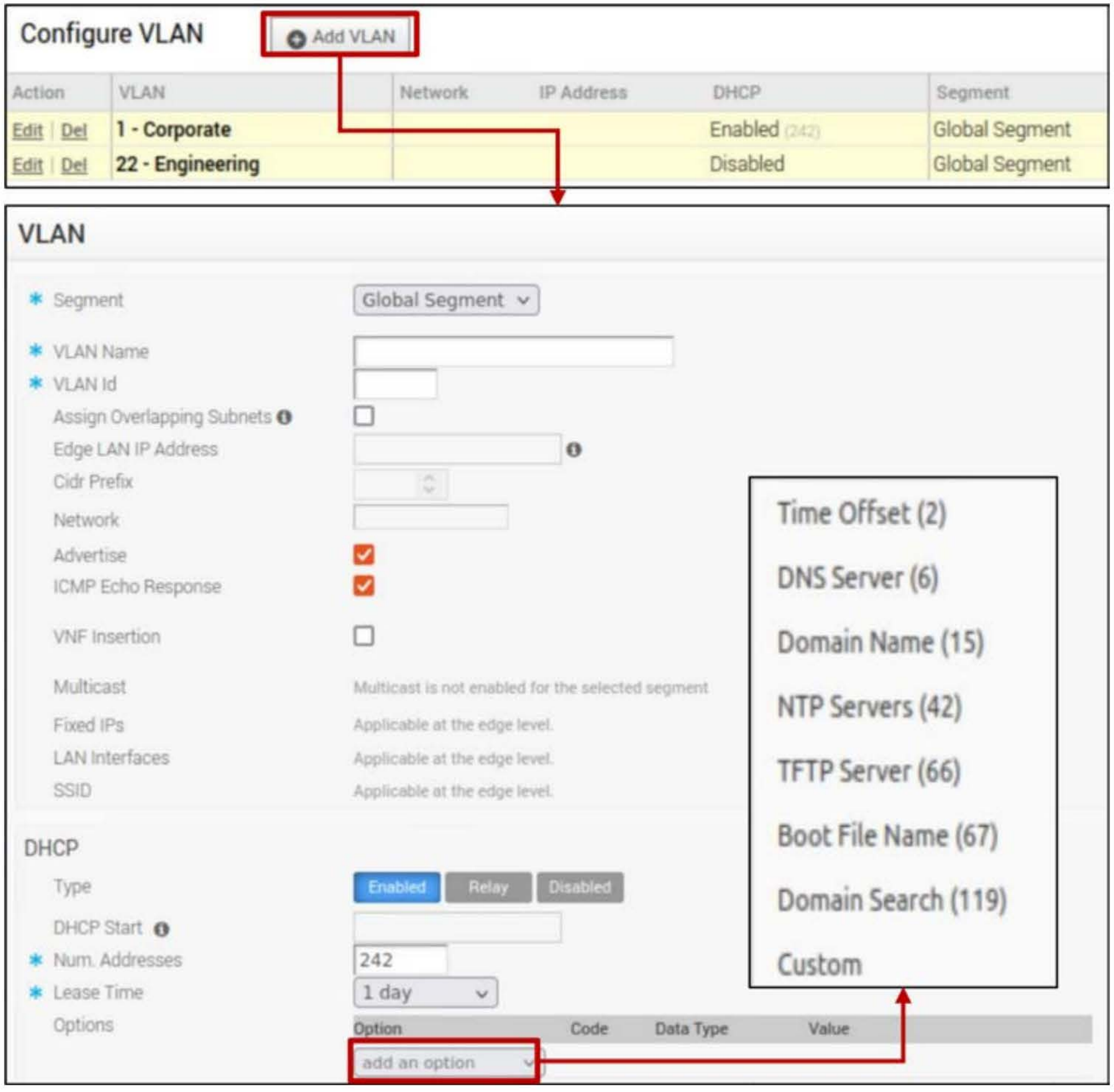
- VLAN
- Management IP
- Device Settings
- Wi-Fi Radio Settings
- L2 Settings
- Multi-Source QoS
- SNMP Settings
- NTP
- Visibility Mode
- Analytics Settings



5-49 Configuring VLANs for Profiles

VLANs are a part of the common configuration of a profile device. You can add a new VLAN or update the existing VLAN settings.

You can also enable DHCP for the VLAN. Several options can be added to the DHCP configuration, such as DNS, NTP, TFTP Server, and so on.



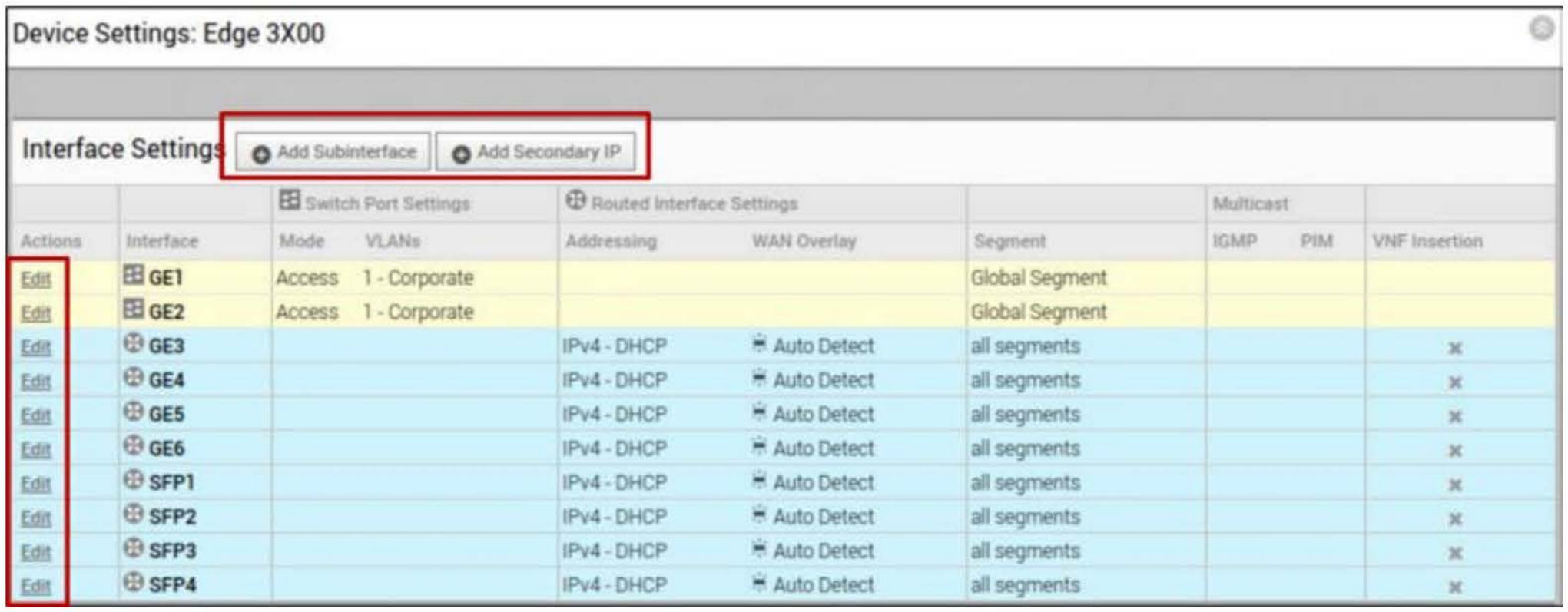
You can configure VLANs at either the profile or edge level. Edges automatically inherit the VLAN configurations from profiles, but you can override these configurations at the edge level.

See the chapter about configuring VLANs for profiles in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

Technet24

5-50 Edge Interface Settings

You can configure device-specific settings for the VMware SD-WAN Edge appliance for each profile.

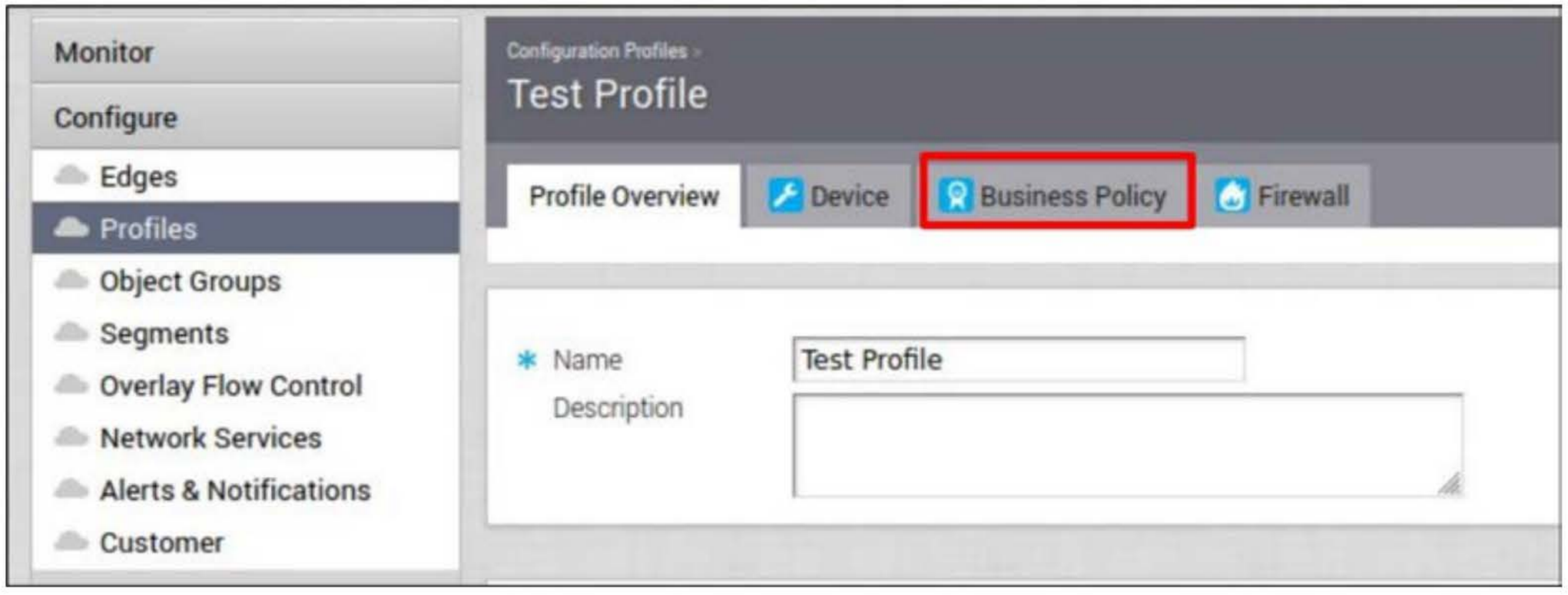


The image shows the interface settings available for the Edge 3X00.

5-51 About Business Policies

Business policies allow the QoS feature to handle data traffic efficiently. You can configure business policy rules at the profile and edge levels to manage the forwarding of traffic direct to the network or across the overlay. The business policy creates its rules from parameters such as source IP address or port, destination IP address or port, domain name, address, port group, and so on.

You configure business policy rules in the **Business Policy** tab of the Configuration Profiles pane in VMware SD-WAN Orchestrator. Operators, partners, and administrators of all levels can create a business policy.

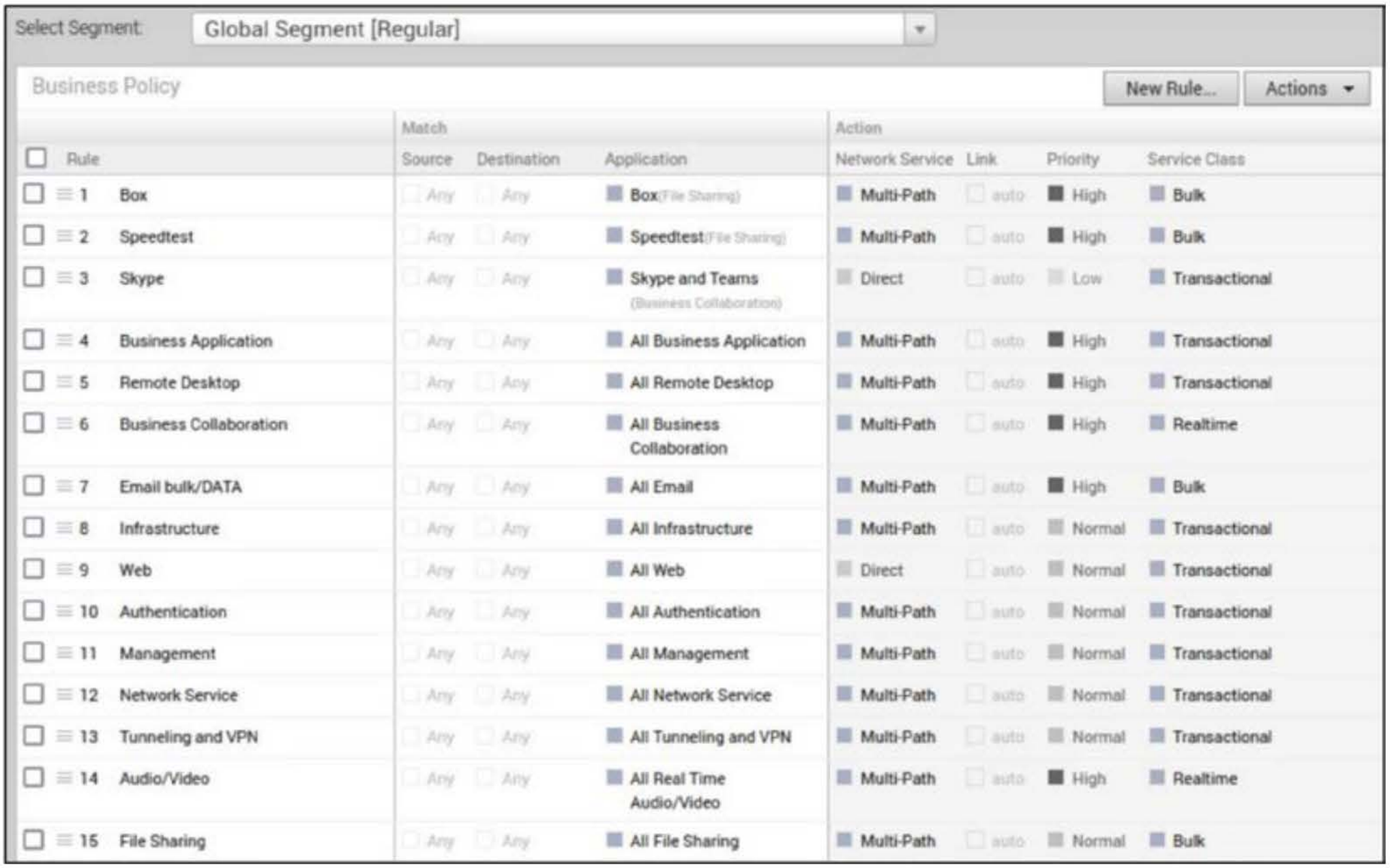


Technet24

5-52 About Business Policy Rules

Business policy rules appear in the VMware SD-WAN profile in order of highest precedence. VMware SD-WAN manages network traffic by matching the characteristics of the traffic to the rule with the highest precedence.

Some rules are available by default. You can create new rules or customize existing ones.



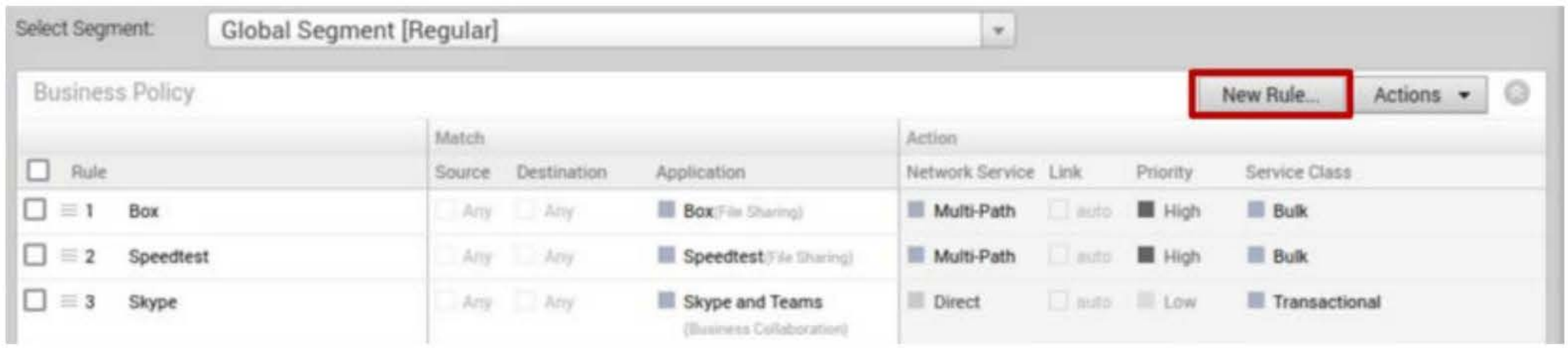
Business policy rules are segment aware. All segments that are available for configuration are listed in the **Select Segment** drop-down menu

When you choose a segment to configure from the **Configure Segment** drop-down menu, the settings and options associated with that segment appear in the Configure Segments area. Global Segment [Regular] is the default segment.

You can move configured rules up or down in the list of rules to establish precedence. Click and hold the lines next to the numeric value at the left side of the rule, and then drag the rule up or down. If you point to the right side of a rule, you can click the minus (-) sign next to the rule to remove it from the list or the plus (+) sign to add a new rule.

5-53 Creating a New Business Policy Rule

To create a new business policy rule, select **Configure** > **Profiles** > **Business Policy** and click **New Rule**.

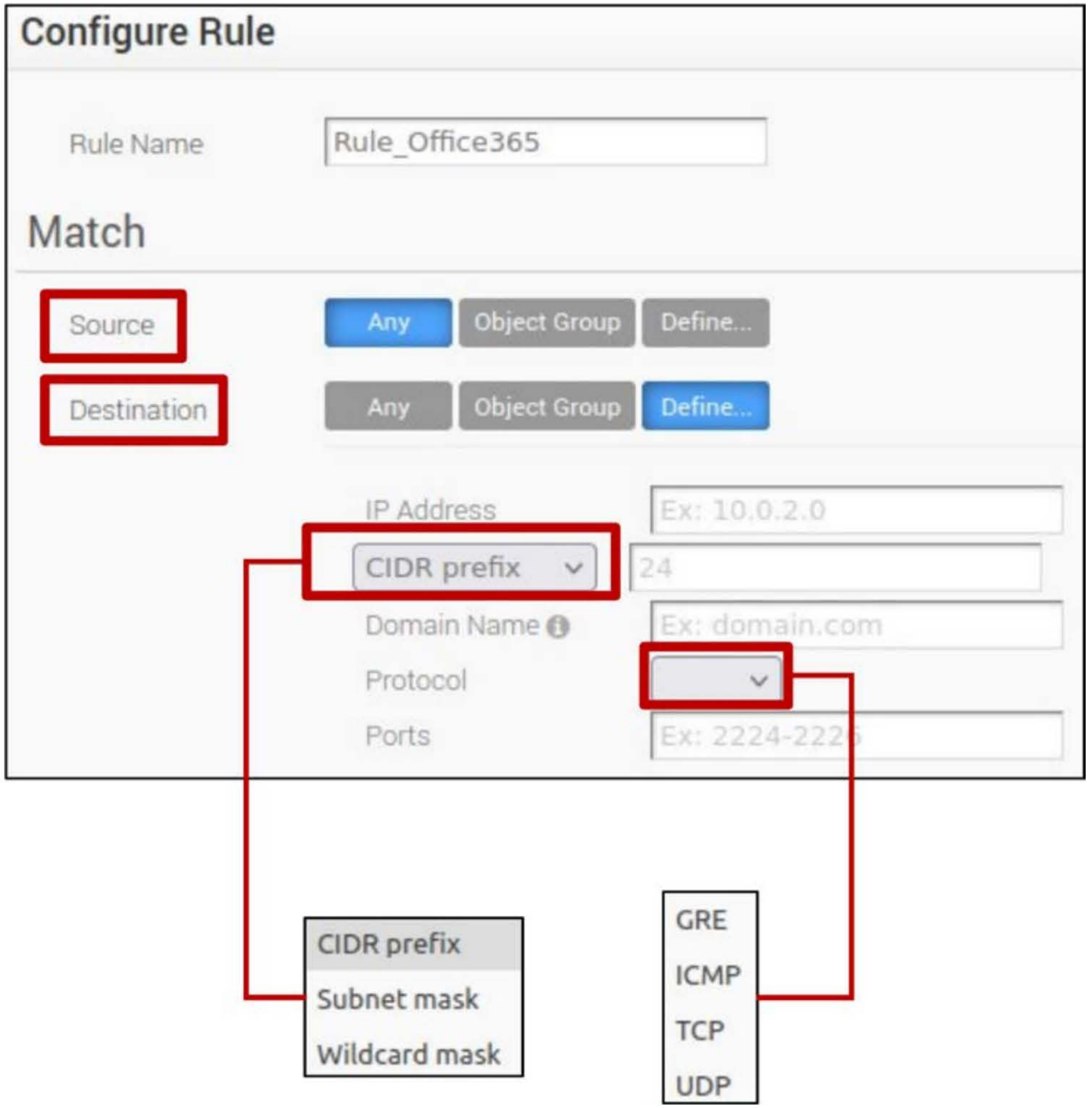


Technet24

5-54 Configuring the Source and the Destination

The following source and destination types are available:

- Any: Any source or destination device processing the traffic data.
- Object Group: An object group consists of a range of IP addresses or port numbers.
- Define: This option lets you make specific adjustments to the source or destination. You can define the network, host, or protocol.



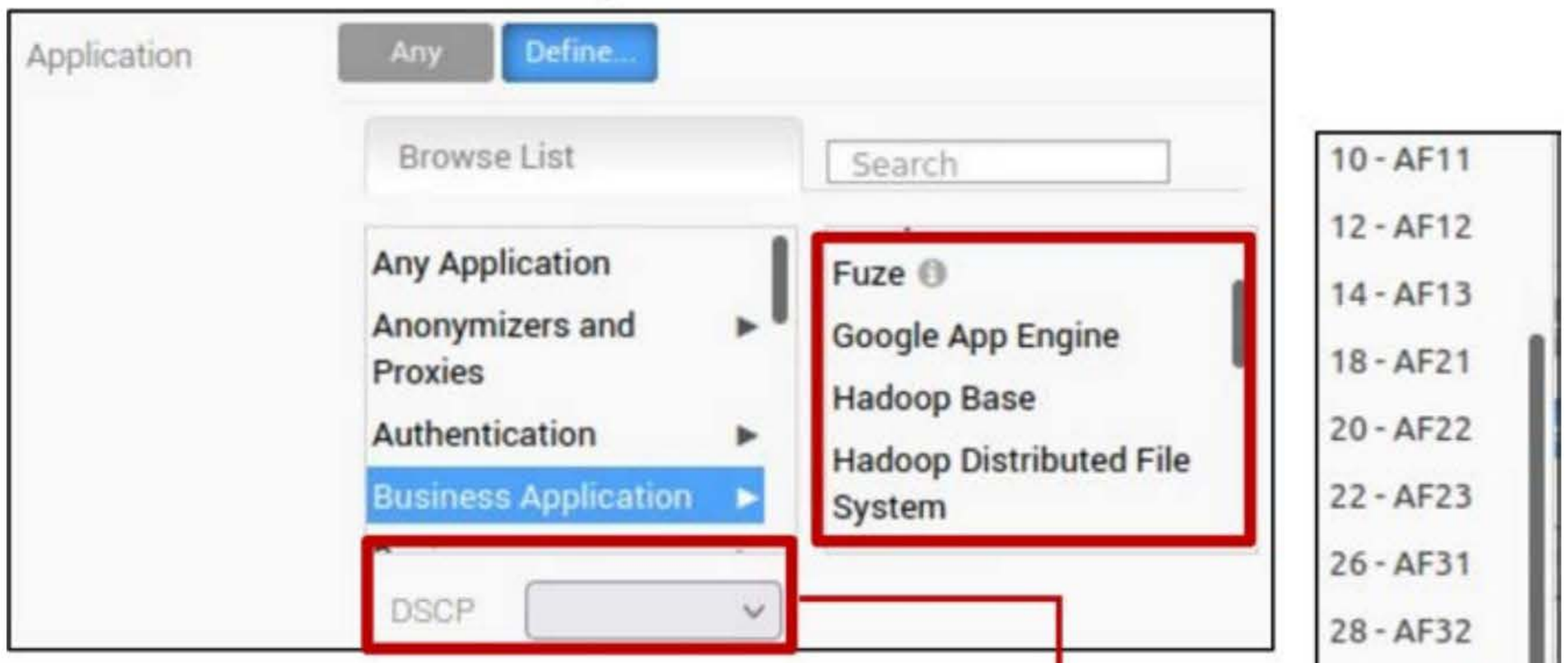
5-55 Selecting an Application for the Rule

After defining the source and the destination, you must define the application whose traffic must be managed.

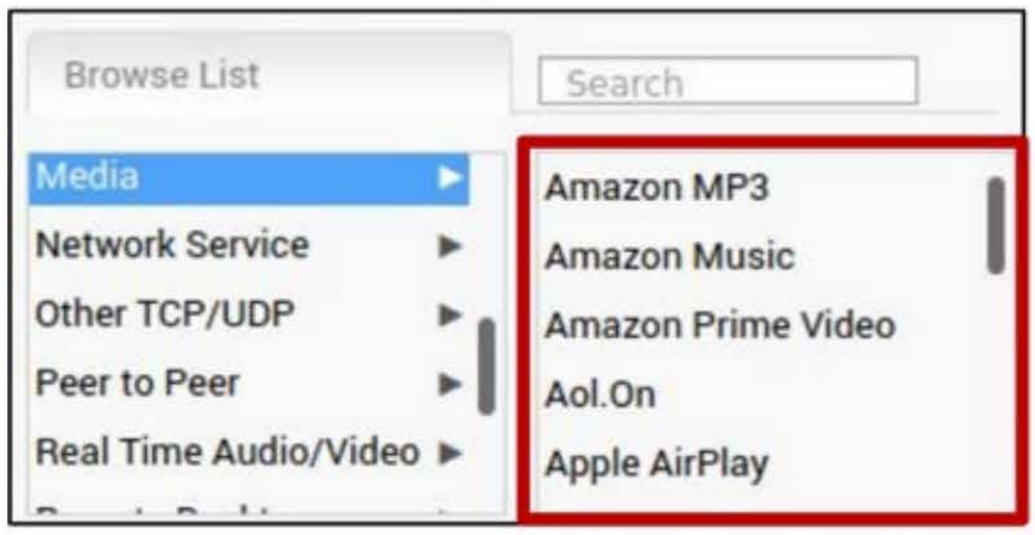
You can select different applications from a variety of categories, for example, **Business Application**, **Media**, or **Business Collaboration**.

You can also configure the class of service from the **DSCP** drop-down menu.

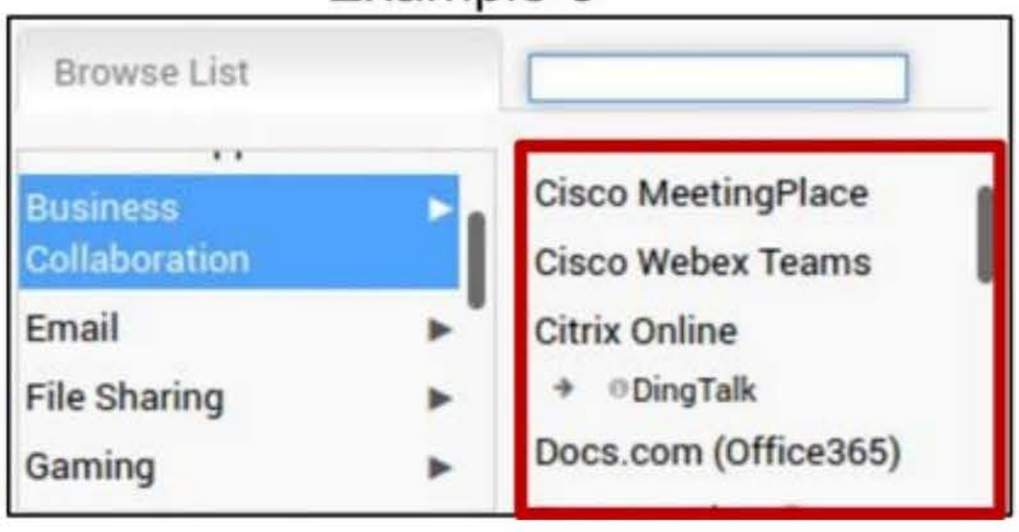
Example 1



Example 2



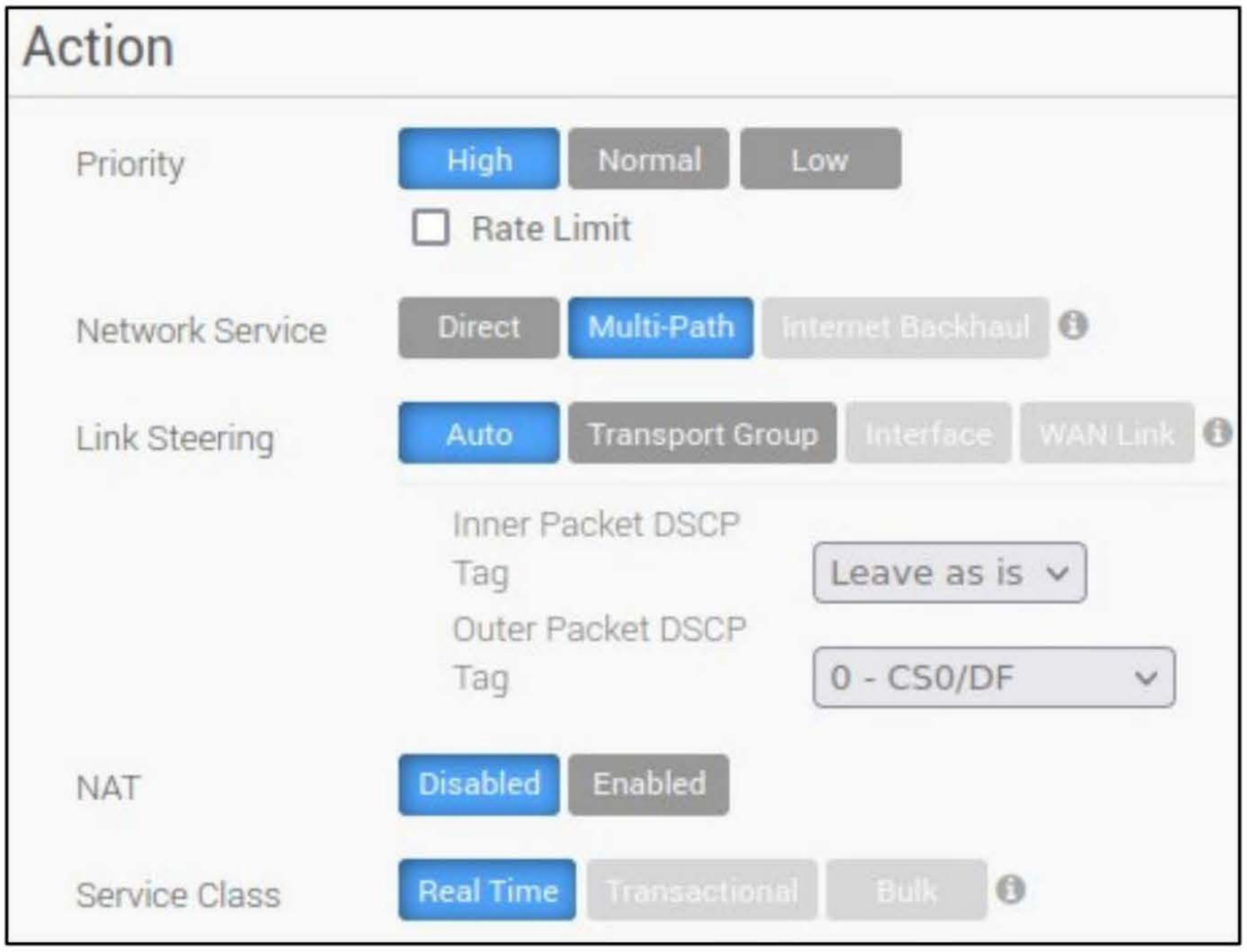
Example 3



Technet24

5-56 Configuring the Action for the Rule

As the final step of configuring a business policy rule, you must specify what action the rule takes based on the source, destination, and applications that you defined previously.



Consider the following details when you select the Network Service:

- Direct: This option bypasses the gateway to send traffic directly to destination.
- Multi-Path: This option sends the traffic from one VMware SD-WAN Edge application to another.
- Internet Backhaul: This option is only applicable if the destination is the Internet.

For more information about configuring actions, see the chapter about configuring business policies in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

5-57 About the Firewall Tab

VMware SD-WAN Orchestrator supports the configuration of stateful and stateless firewalls for profiles and edges.

To enable a firewall:

1 Select **Configure** > **Profiles** > **Firewall**.

2 Turn on the **Firewall Status** toggle.

3 (Optional) Turn on the **Stateful Firewall** toggle.

Technet24

5-58 Stateful Versus Stateless Firewalls

Stateful firewalls provide several features that stateless firewalls lack:

- Directional control of traffic movement
- Session awareness
- Enforcement of symmetric traffic routing
- Rechecked rules after a configuration change

The following examples demonstrate the differences between stateful and stateless firewalls:

- Directional control of traffic movement:
  - A stateful firewall can allow hosts on VLAN 1 to initiate a TCP session with hosts on VLAN 2 but deny the reverse.
  - A stateless firewall translates into a simple access lists, which does not allow for this kind of granular control.
- Session awareness:
  - As a part of a TCP three-way handshake, a stateful firewall does not allow a SYN-ACK packet or an ACK packet to initiate a new session. The session must start with a SYN, and all other packets in the TCP session must also follow the protocol correctly or the firewall drops them.
  - A stateless firewall has no concept of a session. Instead, it only filters packets on an individual, packet-by-packet basis.
- Enforcement of symmetric traffic routing:
  - Asymmetric routing commonly occurs in a network where traffic enters through one hub but exits through another.
  - With a stateful firewall, such traffic would be dropped.
  - With a stateless firewall, third-party routing allows the packet to reach its destination.
- Rechecked rules after a configuration change: If an existing flow has already been accepted, and you configure the stateful firewall to now drop those packets, the firewall rechecks the flow against the new rule set and then drops it.

5-59 Benefits of Stateful Firewalls

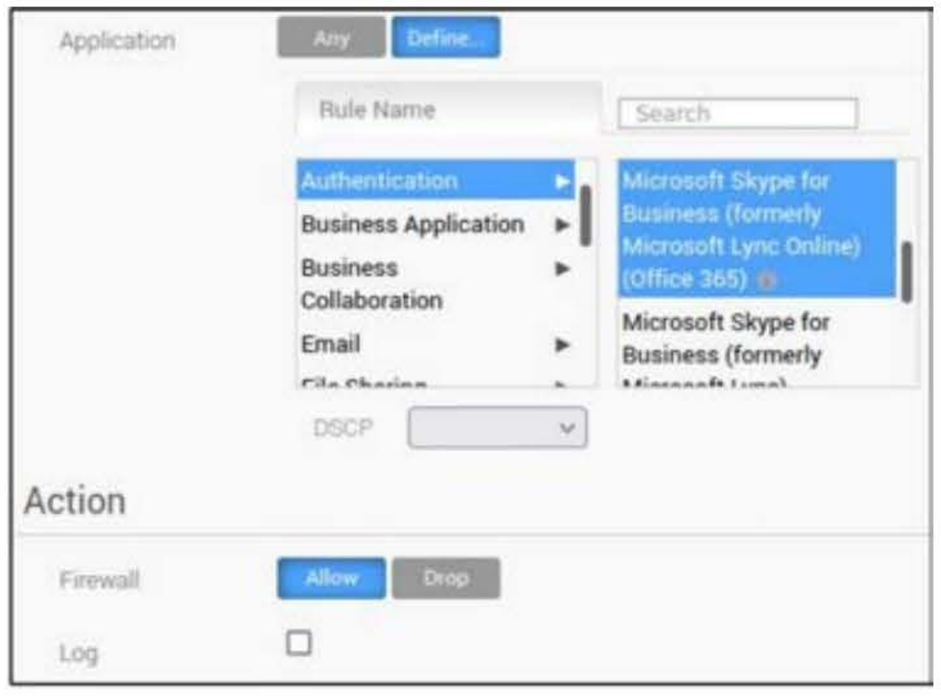
Stateful firewalls provide several benefits:

- Prevention of attacks, such as denial of service (DoS) and spoofing
- Robust logging
- Improved network security

Technet24

5-60 Creating a Firewall Rule

Creating a firewall rule requires you to define a source, a destination, and an application to monitor. The firewall then takes a specified action based on these parameters.



5-61 Network and Flood Protection

VMware SD-WAN can detect and protect against various attacks to combat exploits at all stages of their execution. You can configure Network & Flood Protection Settings at the profile and edge levels to protect against the following types of attacks:

- DoS attacks
- TCP-based attacks
- ICMP-based attacks
- IP-based attacks

Technet24

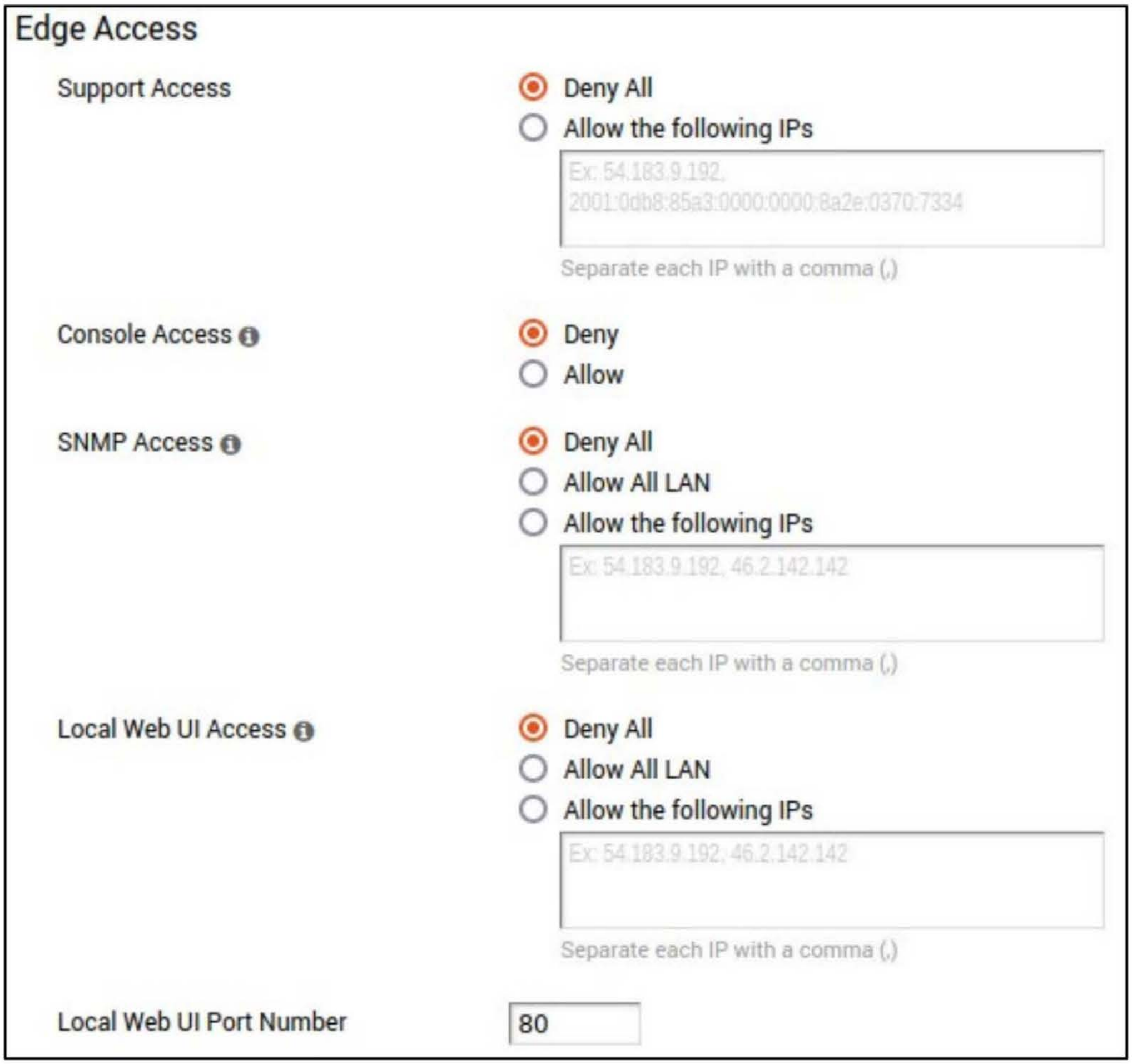
You can configure Network & Flood Protection Settings to protect against the following types of attacks:

- Denial-of-Service (DoS) attack:
  - This type of network security attack overwhelms the targeted device with a tremendous amount of illegitimate traffic.
  - The target becomes so preoccupied processing the bogus traffic that legitimate traffic cannot be processed.
- Invalid TCP Flags:
  - This type of attack occurs when the TCP packet has an invalid or bad flag settings, which causes the device to crash.
  - VMware SD-WAN can prevent invalid TCP flag attacks by filtering the packets out.
- TCP LAND:
  - A TCP LAND attack is a type of DoS attack at TCP/IP layer 4.
  - The source IP address and the port are the same as the destination IP address and port.
  - As a result, the device processes the packet in an infinite loop.
  - The CPU of the device becomes indefinitely consumed, causing the target device to crash or freeze.
- ICMP Ping of Death:
  - In this type of attack, the attacker sends large ping packets to the target device.
  - Attackers might craft ping packets that are larger than the maximum size of 65,535 bytes.
  - The fragmentation and reassembly of this type of large packets can result in buffer overflow, ultimately causing the system to crash, freeze, or reboot.
- IP Unknown Protocol:
  - IP packets with a protocol ID number of 143 or greater can cause the end device to crash.
  - VMware SD-WAN prevents these attacks by blocking such packets.

5-62 Controlling Edge Access

You configure the settings under Edge Access to secure the VMware SD-WAN Edge device against unauthorized users.

For security reasons, Support Access, Console Access, SNMP Access, and Local Web UI Access are disabled by default.



Technet24

5-63 Lab 5: Configuring Profiles

Create a new profile and apply restrictions to the profile:

1. Create a New Configuration Profile
2. Apply a Profile Restriction
3. Create a New Edge
4. Change the Profile Assigned to the Edge

5-64 Review of Learner Objectives

- Describe how to create a profile in VMware SD-WAN
- Demonstrate how to configure a profile device
- Demonstrate how to configure a business policy rule
- Demonstrate how to configure the interfaces of an edge device
- Differentiate between stateful and stateless firewalls
- Demonstrate how to configure a firewall rule

Technet24

5-65 Key Points

- Segmentation in VMware SD-WAN separates the traffic coming from different business verticals.
- A profile is a configuration template that can be applied to multiple edges. You can override the configuration at the edge level.
- Firewalls can be used to block or allow traffic based on source, destination, application, or protocol.

Questions?

Module 6

Site Configuration and Traffic Management

6-2 Importance

Site configuration is a one-time process that must be planned well in advance. Efficient traffic management can improve application and system performance as well as enhance the user experience. Class of service, routes, and link steering are just a few methods of managing traffic more efficiently.

6-3 Module Lessons

1. Site Configuration
2. Routing in VMware SD-WAN
3. Dynamic Multipath Optimization

6-4 Lesson 1: Site Configuration

6-5 Learner Objectives

- Explain the general steps required for site configuration
- Describe the configuration of a hub
- Enable tunnels between the branch sites and the data center

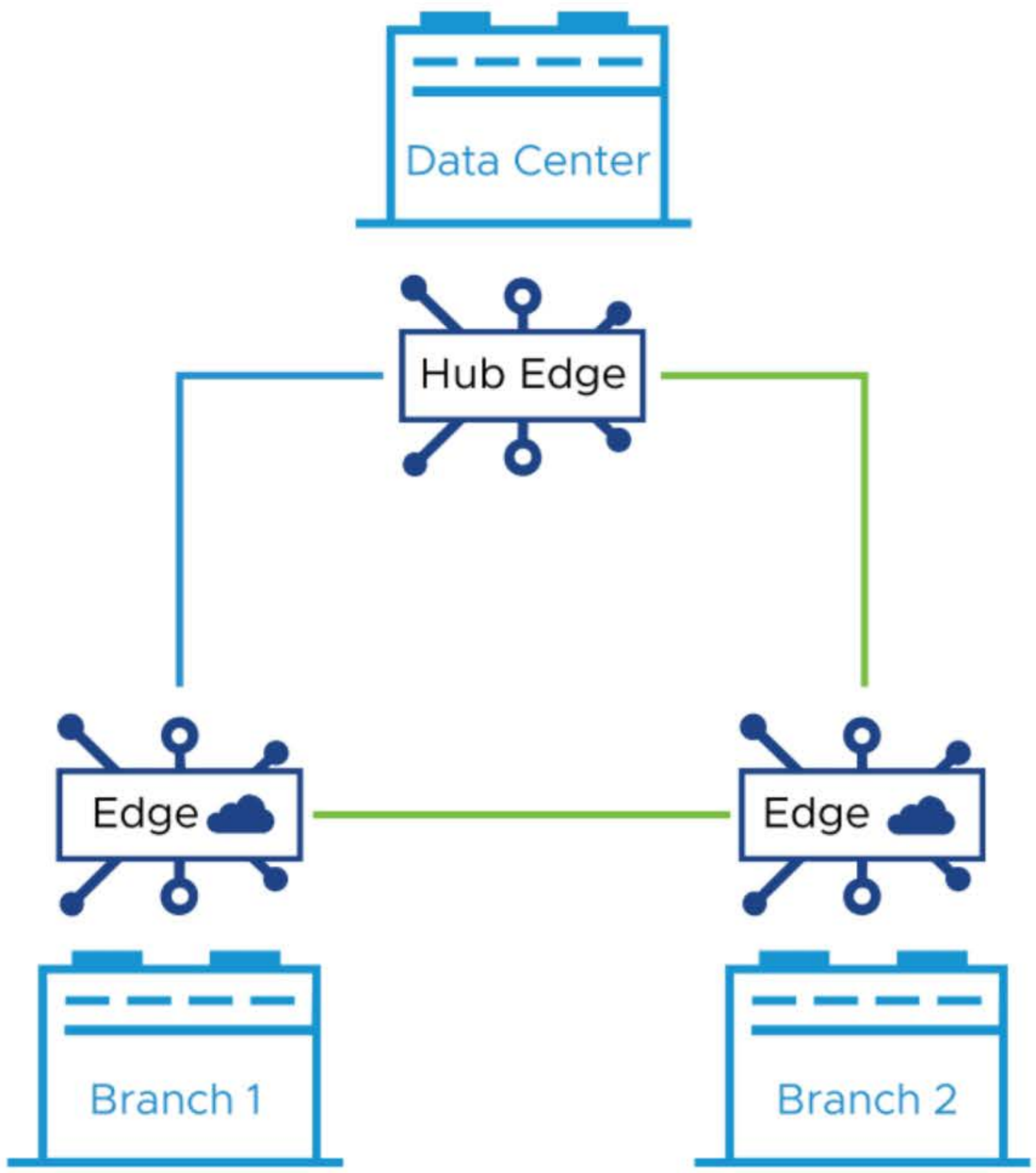
Technet24

6-6 General Workflow of Site Configuration

Consider a scenario in which two branch sites are connected to a data center site.

The general workflow of configuring VMware SD-WAN Edge in a two-arm configuration is as follows:

1. Configure and activate a data center hub.
2. Configure and activate Branch 1.
3. Enable a tunnel between Branch 1 and the data center.
4. Configure and activate Branch 2.
5. Enable a tunnel between Branch 2 and the data center.
6. Enable a tunnel between the Branch 1 and Branch 2 edges.



6-7 Configuring the Data Center Hub

The first step to configuring a data center hub is to connect the VMware SD-WAN Edge appliance to the Internet:

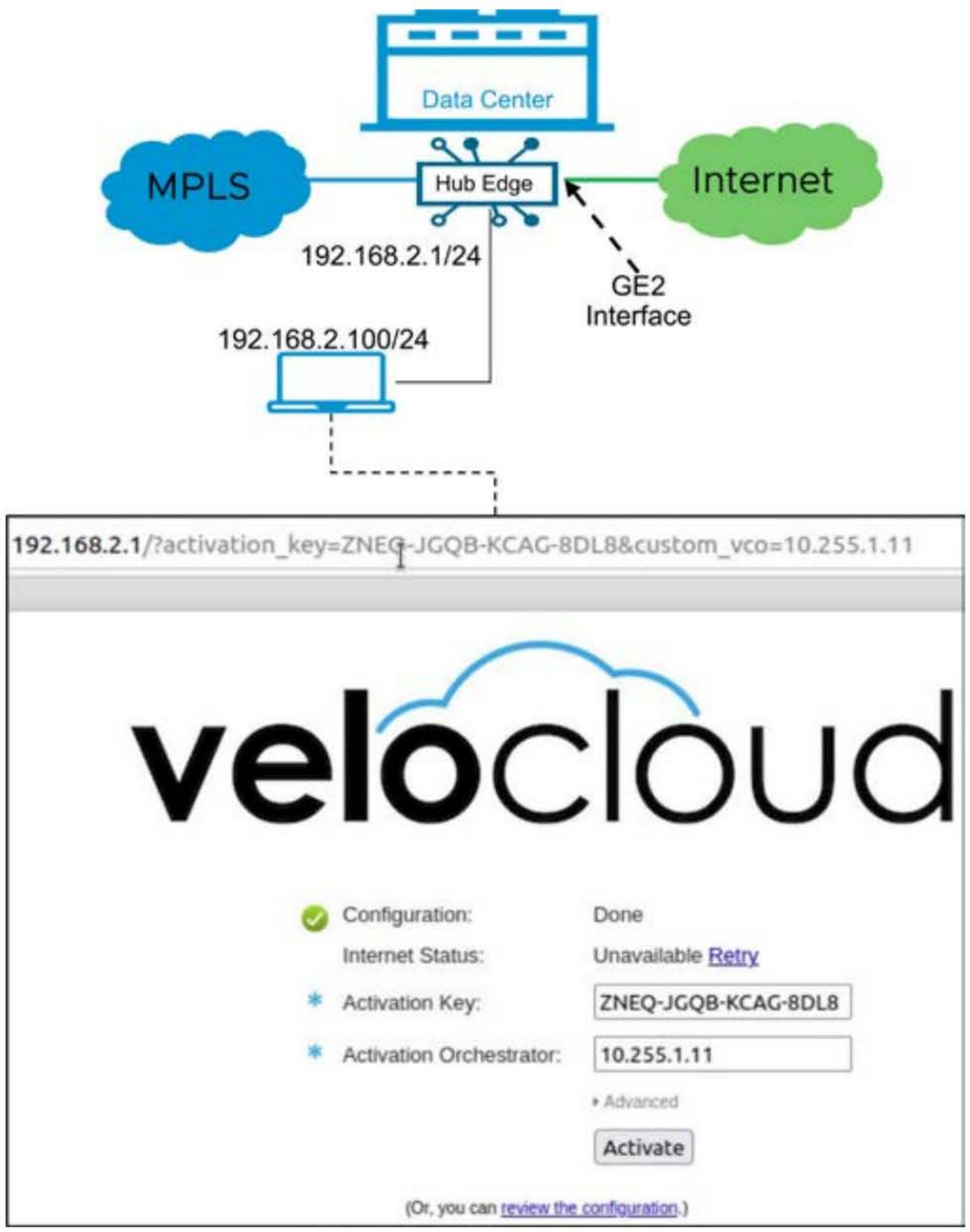
1. Configure a PC with a static IP of 192.168.2.100/24 and a gateway with an IP address of 192.168.2.1

   These IP addresses are the default LAN settings for accessing a VMware SD-WAN Edge appliance.

2. Connect the PC to the VMware SD-WAN Edge LAN interface
3. From the PC, go to http://192.168.2.1

   This URL is the local web interface of the edge appliance.

4. Click the **Device Configuration** link to review the configuration and to configure the GE2 interface

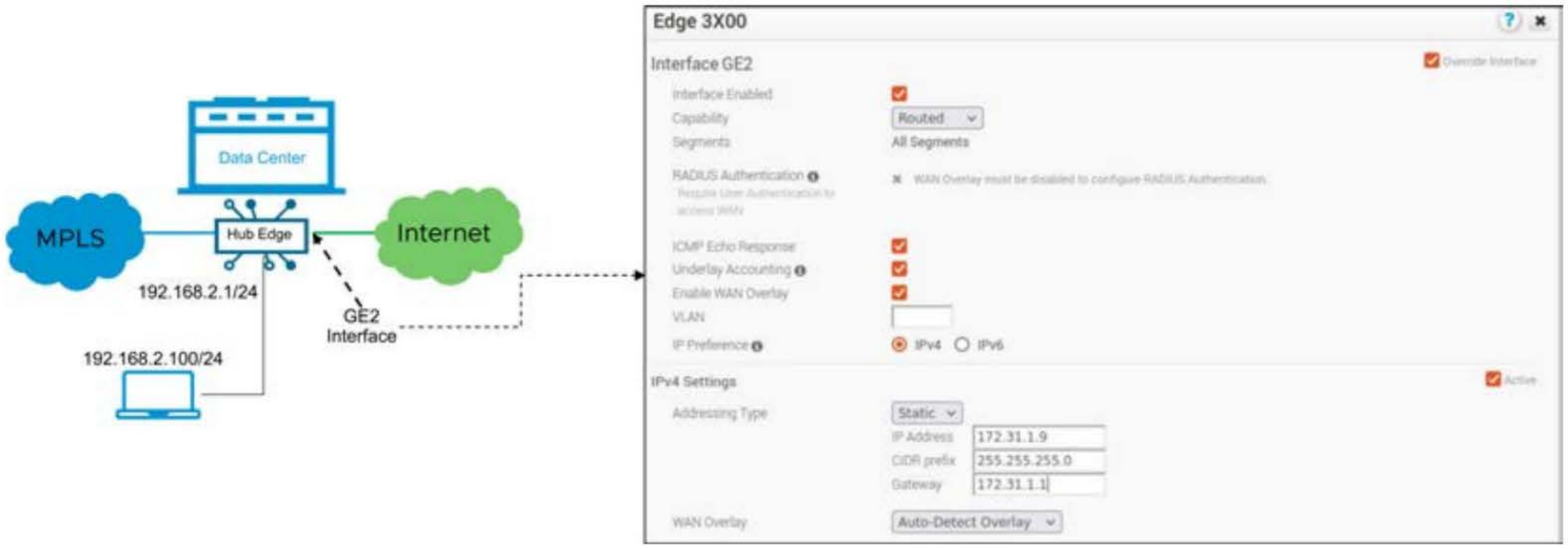


The IP values in the slide are for reference only.

Technet24

6-8 Connecting the Edge to the Internet

From VMware SD-WAN Orchestrator, you configure an interface, such as GE2, with a static WAN IP address and default gateway so that it can reach the Internet.

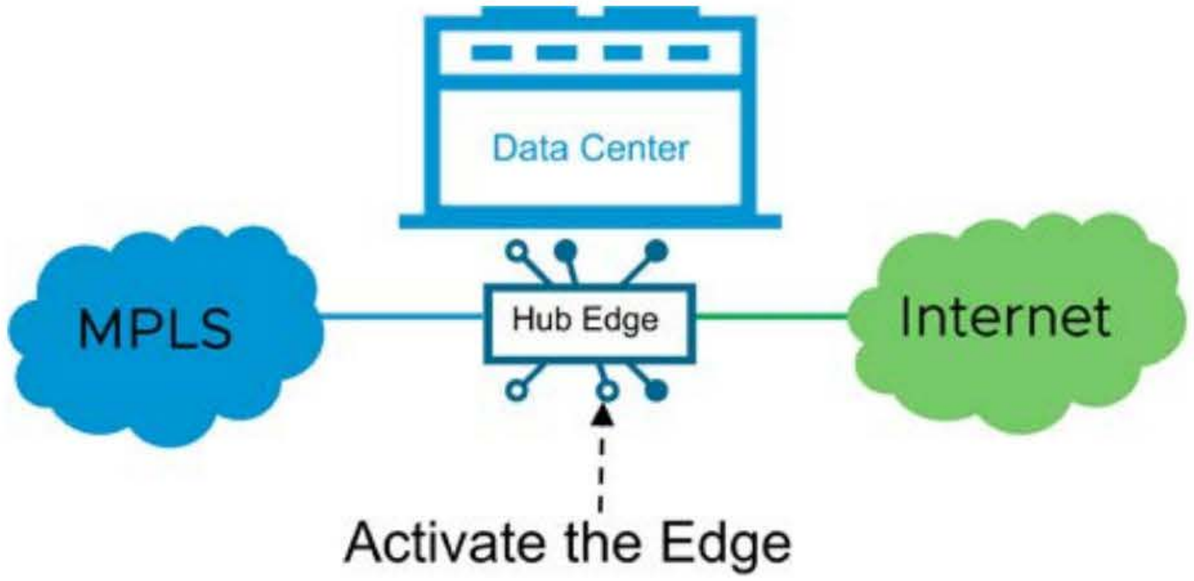


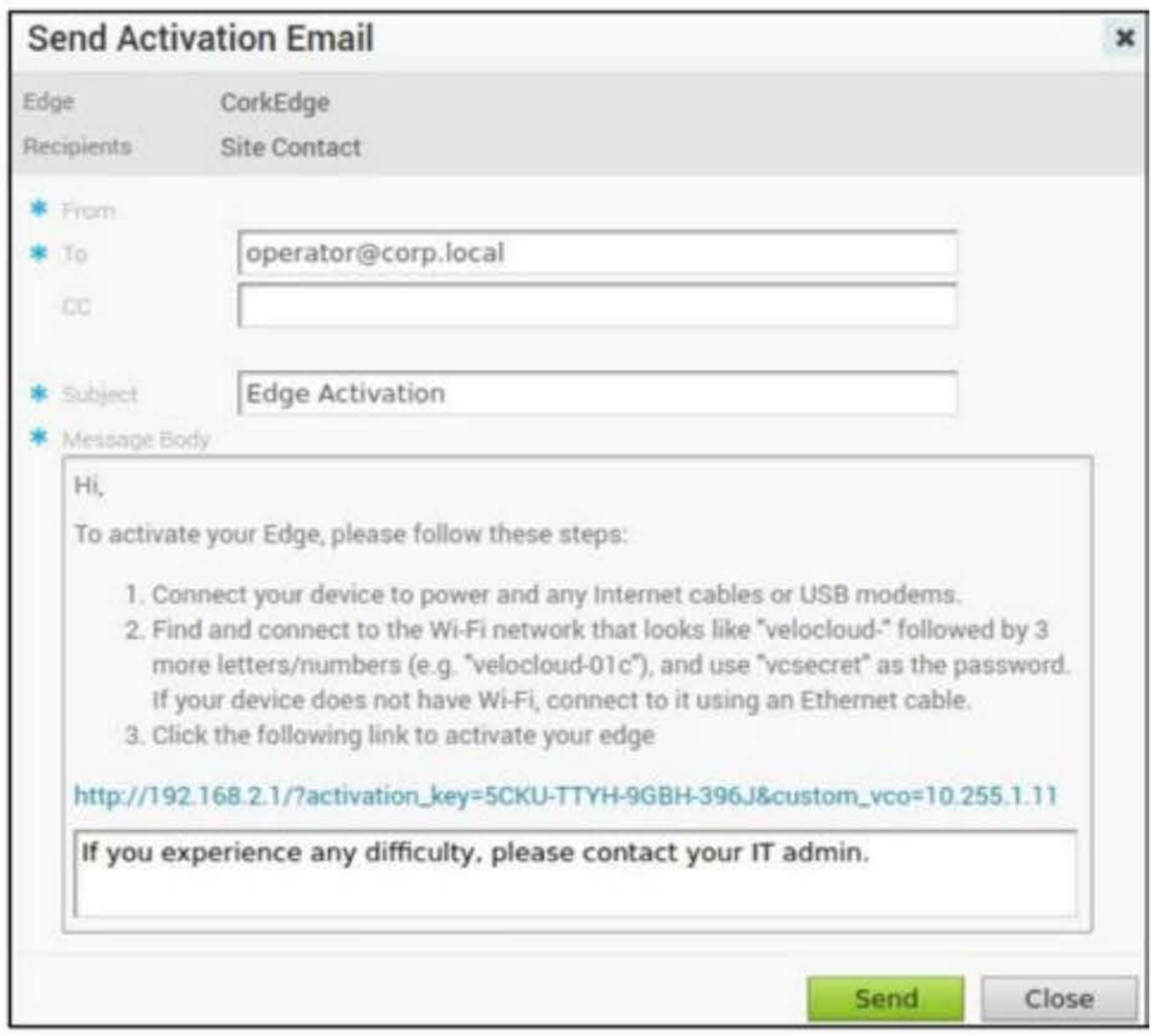
6-9 Activating the Data Center Edge

After configuring the data center edge, the next step is to activate it.

To activate the edge from VMware SD-WAN Orchestrator:

1. Select **Configure** > **Edges** from the navigation pane on the left.
2. On the Edges page, select **New Edge**.
3. Specify the correct model and the profile.
4. Follow the normal activation process.





Screenshot of Activation Email

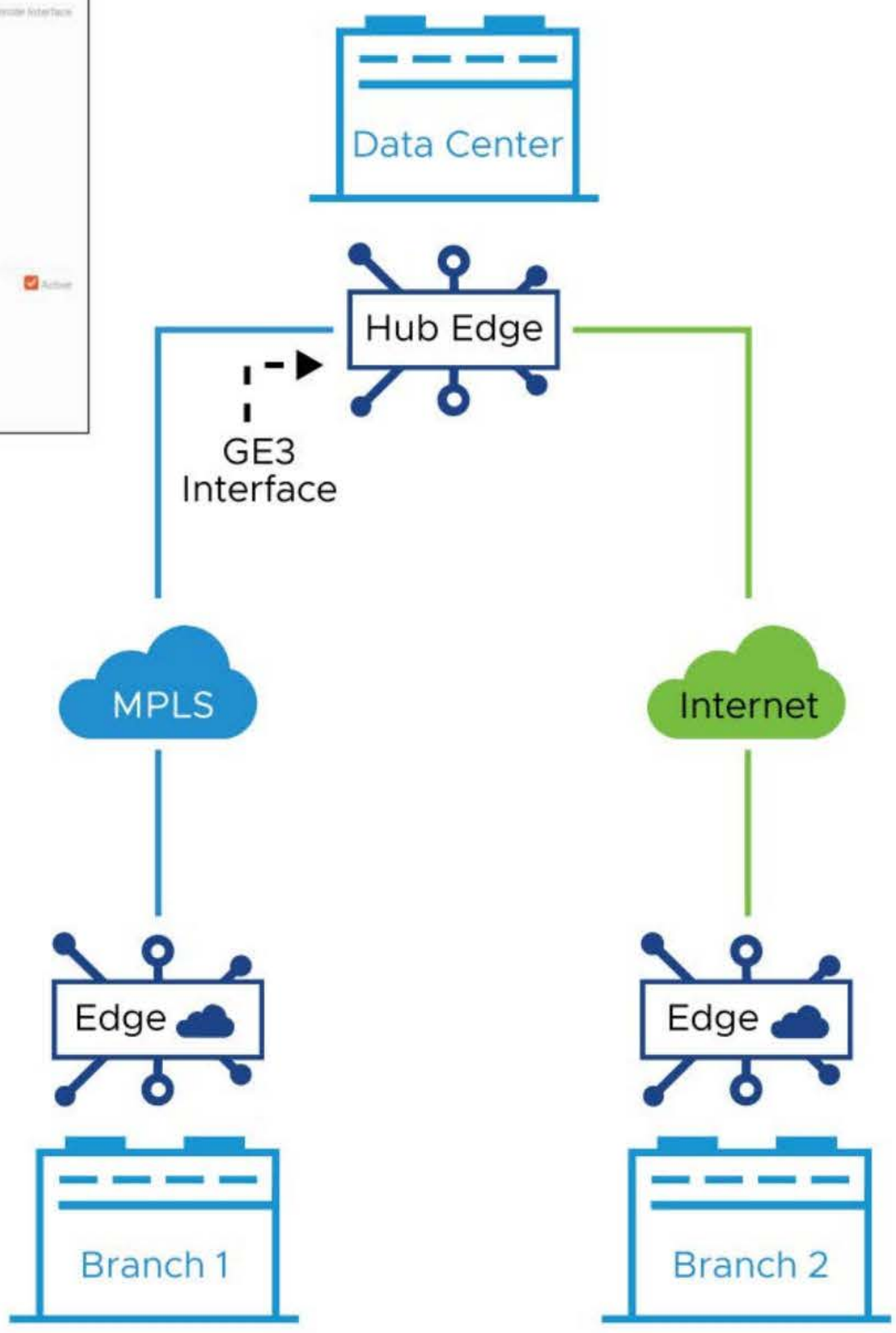
If you already have the email feature set up, an activation email will be sent to that email address. Otherwise, you can go to the device setting page to get the activation URL.

Technet24

6-10 Configuring the Private MPLS WAN Link

You can configure the private Multiprotocol Label Switching (MPLS) edge WAN interface directly from VMware SD-WAN Orchestrator.

From the **WAN Overlay** drop-down menu, select **User Defined Overlay** to define a WAN link manually in the next step.

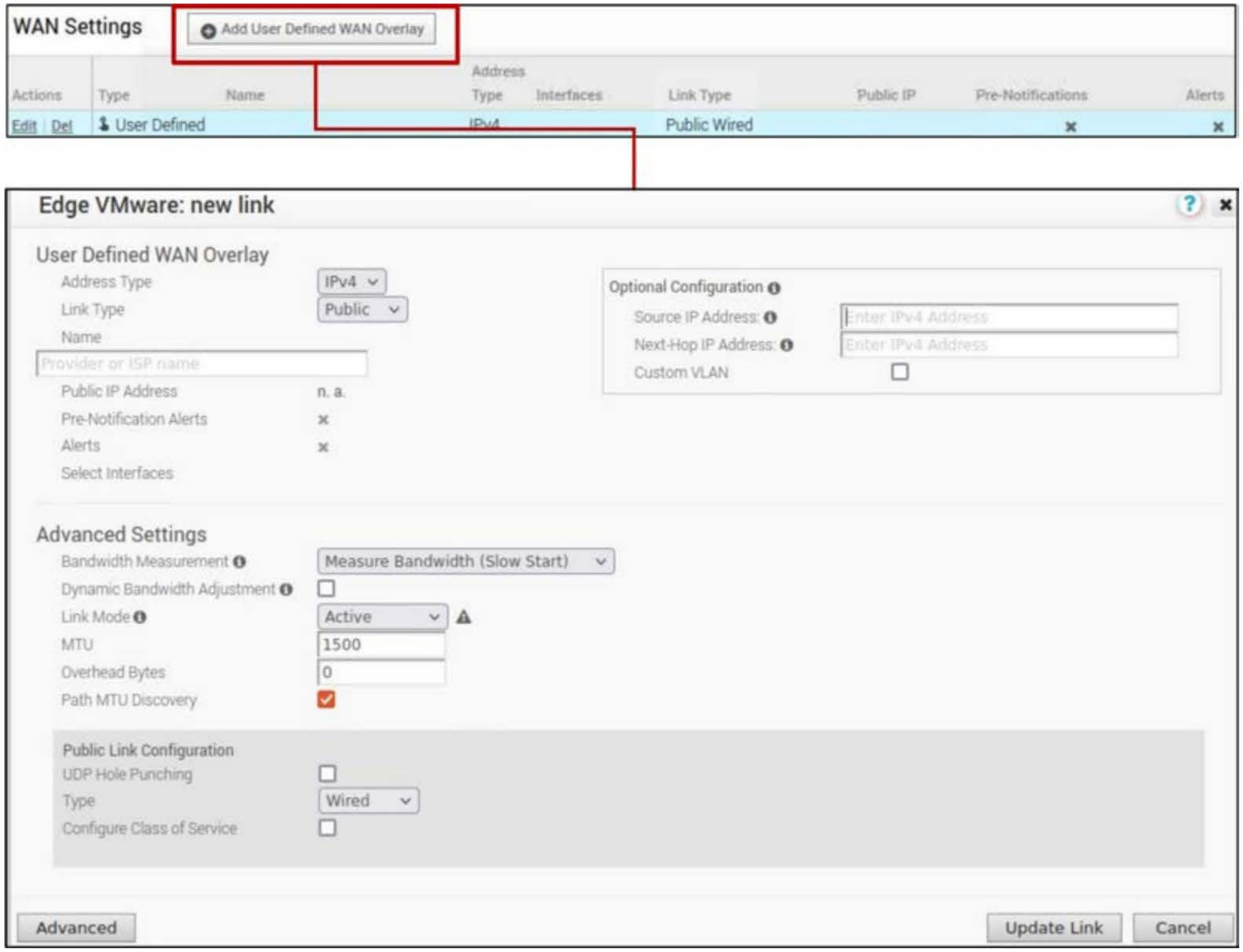


For example, on the GE3 interface, you configure 172.31.2.1/24 as the static IP and 172.31.2.2 as the default gateway.

6-11 Adding a User-Defined WAN Overlay

To add a user-defined WAN overlay for an interface:

1. Under WAN Settings, click the **Add User Defined WAN Overlay** button.
2. Define the WAN overlay for the MPLS path.
   a.. From the **Link Type** drop-down menu, select **Private**.
   b.. Next to Select Interfaces, select the **GE3** check box.
   c.. Enter **`172.31.2.2`** in the **Next-Hop IP Address** text box.



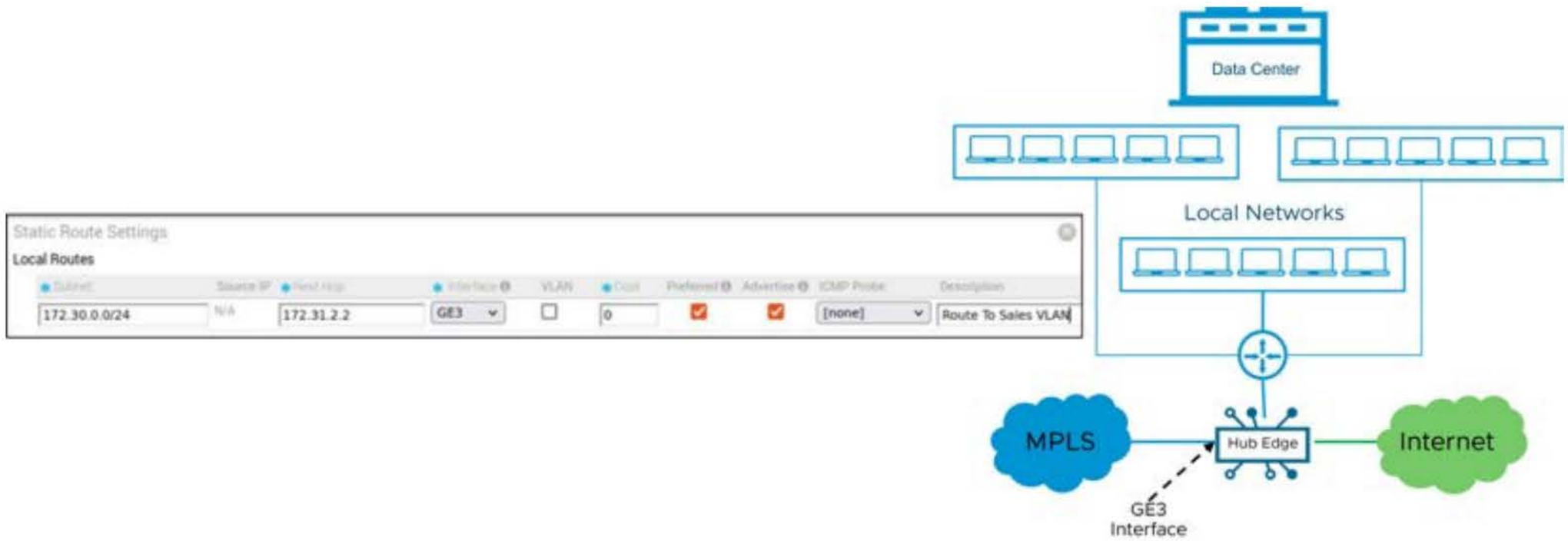
In the slide, the GE3 interface is used for reference.

Technet24

6-12 Configuring a Route to Local Networks

You add a static route to the 172.30.0.0/24 subnet. You must specify which interface to use for routing to the next hop.

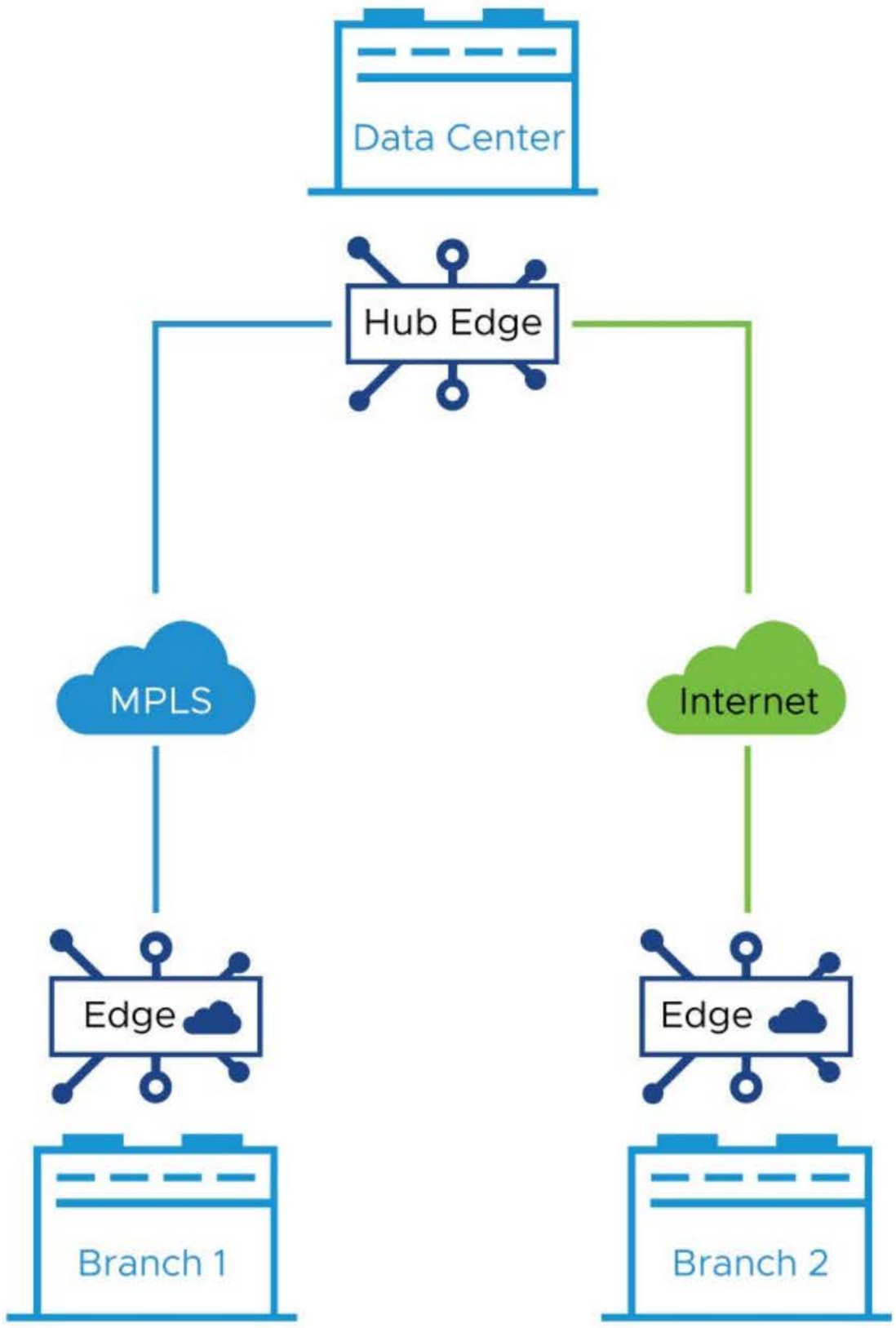
You must select the **Advertise** check box so that other VMware SD-WAN Edge appliances can learn about this subnet behind a layer 3 switch or routers.



In the slide, the GE3 interface is used for reference.

6-13 Configuring Branch Sites

Branch site configuration is similar to data center configuration. You can configure the private MPLS WAN link or establish a public network to the data center and other branch sites.

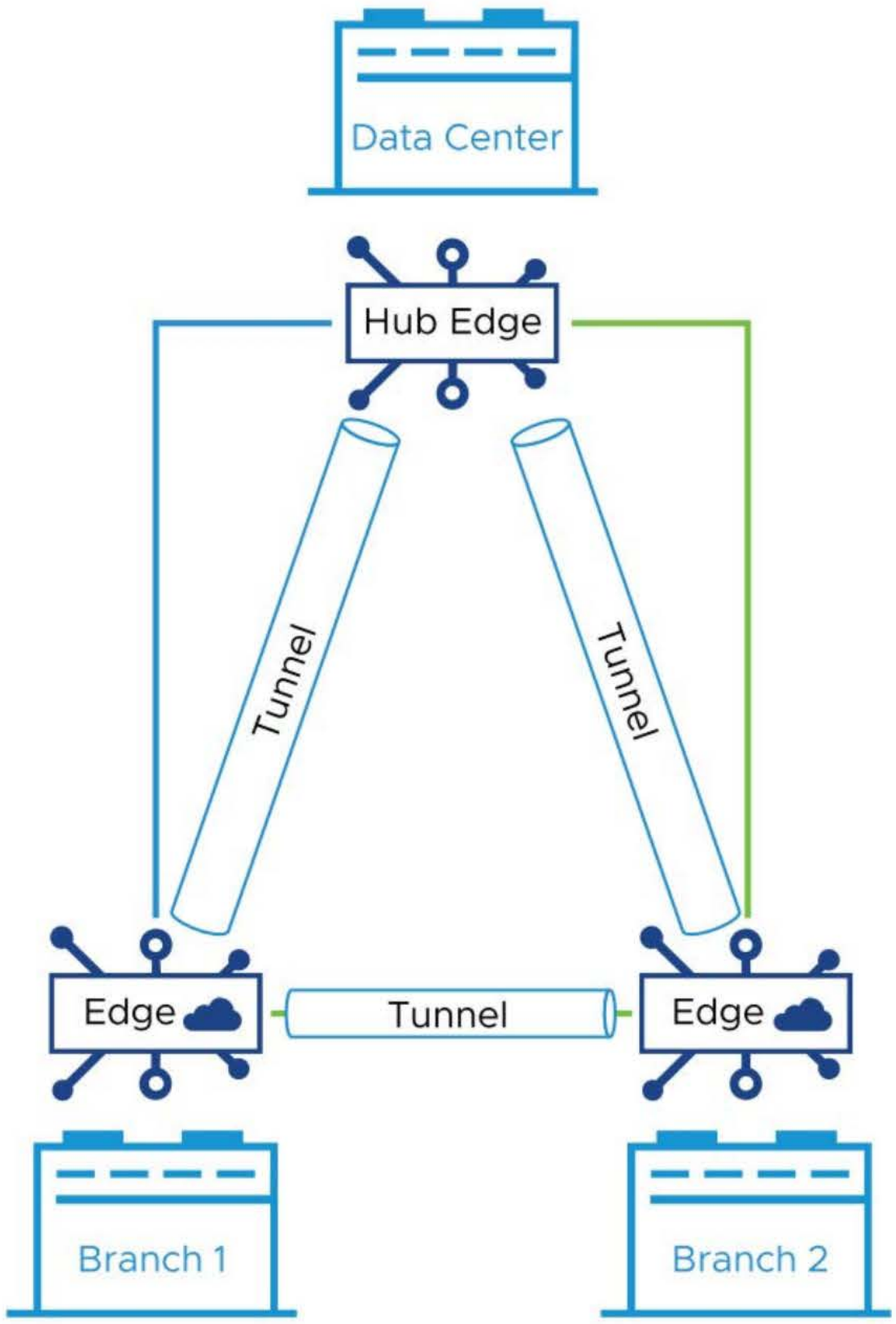


See the chapter about site configurations in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

Technet24

6-14 Enabling Tunnels Between Sites (1)

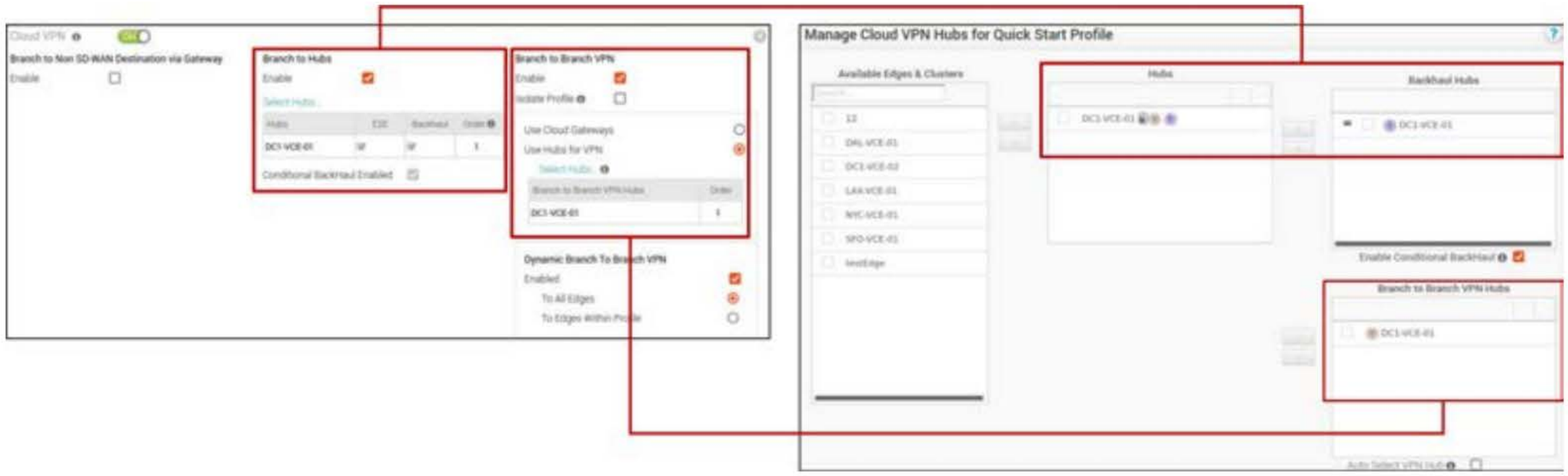
The next step in the site configuration process is to build the overlay tunnel between the sites. To do so, you must enable Cloud VPN from the branch to the hub.



6-15 Enabling Tunnels Between Sites (2)

To enable tunnels between sites from VMware SD-WAN Orchestrator:

1. Select **Configure** > **Profiles** in the navigation pane.
2. Select **Quick Start VPN Profile** and click the **Device** tab.
3. Turn on the **Cloud VPN** toggle.
4. Under Branch to Hubs, select the **Enable** check box.
5. Under Branch to Branch VPN, select the **Enable** check box.
6. Under Branch to Branch VPN, click **Use Hubs for VPN**.



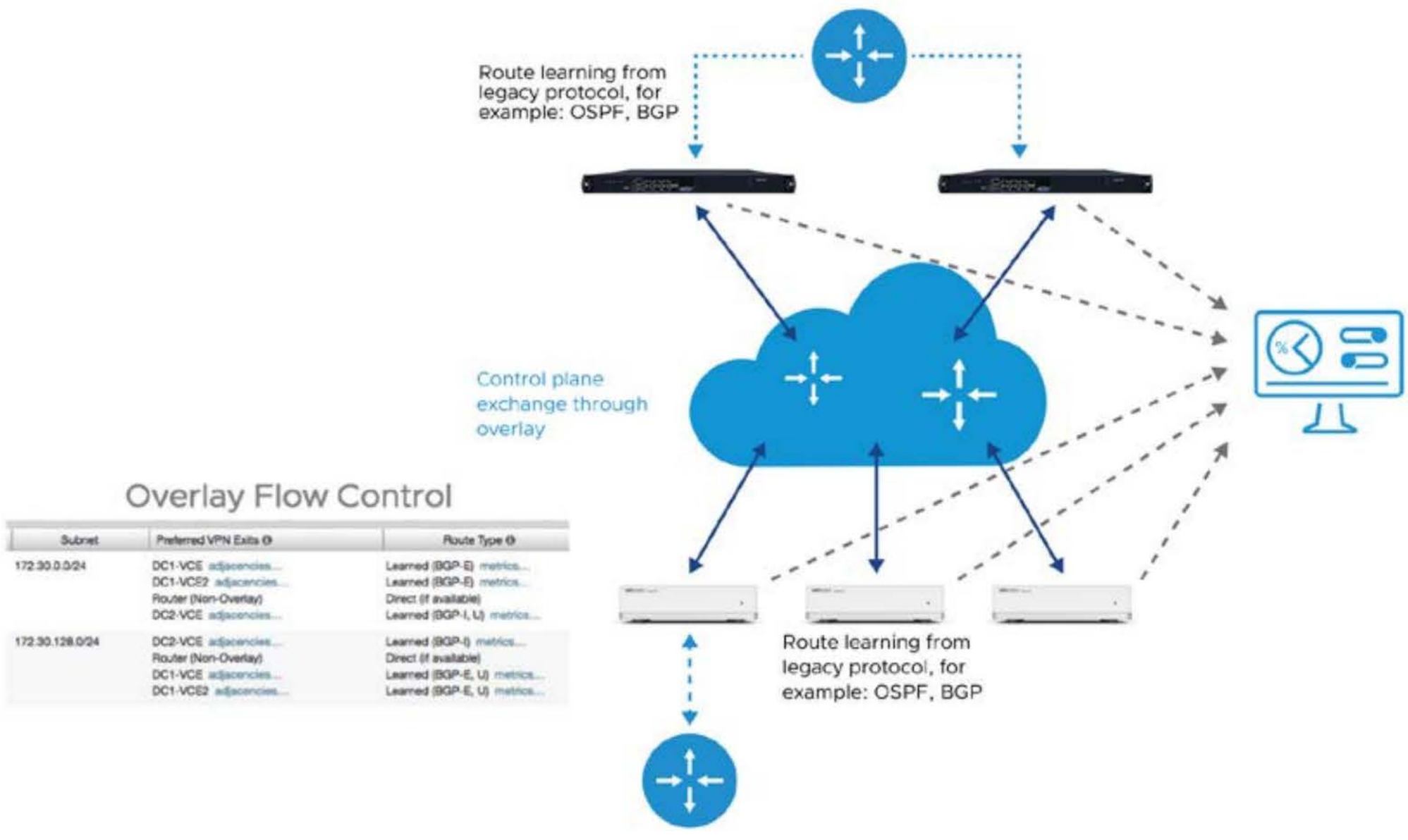
Technet24

6-16 Overlay Flow Control

The Overlay Flow Control section of VMware SD-WAN Orchestrator displays all the routes and their origins.

It provides the following information:

- Aggregated view of all routes
- Where each route is learned



Overlay Flow Control

Subnet	Preferred VPN Exits	Route Type
172.30.0.0/24	DC1-VCE adjacencies... DC1-VCE2 adjacencies... Router (Non-Overlay) DC2-VCE adjacencies...	Learned (BGP-E) metrics... Learned (BGP-E) metrics... Direct (if available) Learned (BGP-I, U) metrics...
172.30.128.0/24	DC2-VCE adjacencies... Router (Non-Overlay) DC1-VCE adjacencies... DC1-VCE2 adjacencies...	Learned (BGP-I) metrics... Direct (if available) Learned (BGP-E, U) metrics... Learned (BGP-E, U) metrics...

6-17 Lab 6: Configuring and Verifying Overlay Tunnels

Understand the configuration of user-defined and auto-defined overlay tunnels:

1. Configure an Auto-Detected Overlay
2. Verify the Auto-Detected Overlay
3. Verify the User-Defined Overlay

Technet24

6-18 Lab 7: Configuring Overlays for Cloud VPN

Configure overlays and VPNs to establish secure data paths between the branch sites and the data center:

1. Explore the OFC Table and Enable Cloud VPN for Internet-Only Profiles
2. Enable Cloud VPN for Branch Hybrid Profile
3. Change the Device Role from Edge to Hub
4. Enable Hub-Spoke Topology for Branch Hybrid Profile
5. Enable Branch to Branch VPN with Gateways
6. Verify the Path for Branch to Branch VPN
7. Enable Branch to Branch VPN with Hubs

6-19 Review of Learner Objectives

- Explain the general steps required for site configuration
- Describe the configuration of a hub
- Enable tunnels between the branch sites and the data center

Technet24

6-20 Lesson 2: Routing in VMware SD-WAN

6-21 Learner Objectives

- List the routing options available in a VMware SD-WAN environment
- Describe the configuration of static routes, Open Shortest Path First Protocol, and Border Gateway Protocol
- Describe the advantages of Bidirectional Forwarding Detection

6-22 Routing in VMware SD-WAN

VMware SD-WAN provides the following options for routing:

- Static routing
- Open Shortest Path First (OSPF) protocol
- Border Gateway Protocol (BGP)

VMware SD-WAN Edge learns routes from adjacent routers through OSPF and BGP. The gateway controller acts like a route reflector and sends the learned routes to other VMware SD-WAN Edge appliances.

Technet24

6-23 About Static Routing

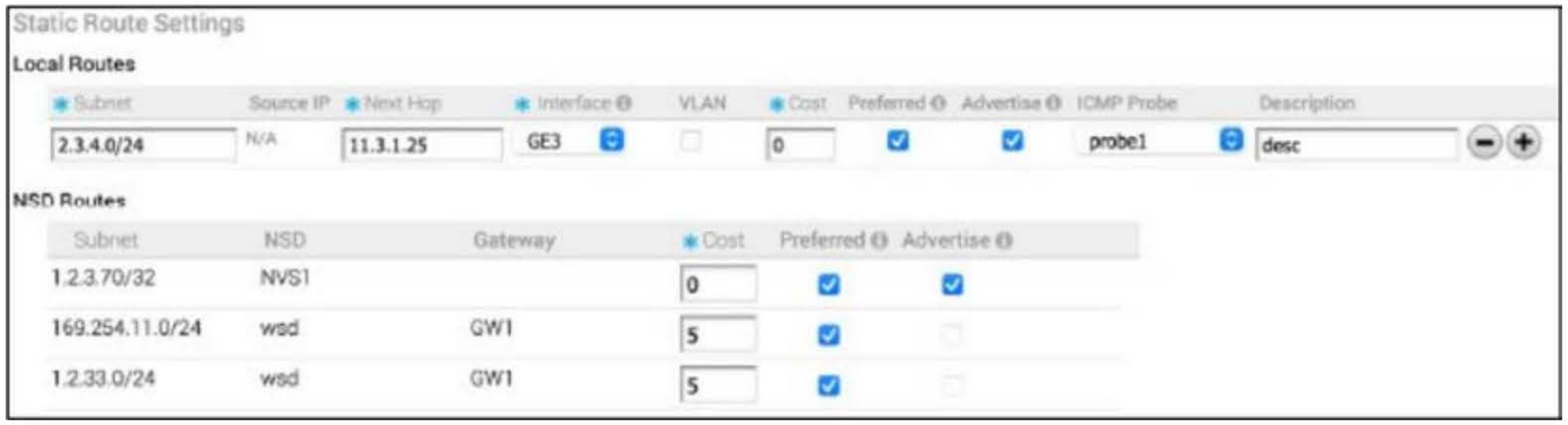
Static routes are useful for specific instances in which routes are needed for existing network-attached devices, such as printers. You have the option to control the advertisement, preferred flag, and cost for the route.

You can configure static routes in VMware SD-WAN Orchestrator by selecting **Edges** > **Device Settings** > **Static Routes** in the navigation pane.

6-24 Static Routes to Non-SD-WAN Destinations

You can configure static routes to non-SD-WAN destinations (NSDs) on the Network Services page of VMware SD-WAN Orchestrator. You can enable an edge or gateway to establish IPsec tunnels directly to an NSD.

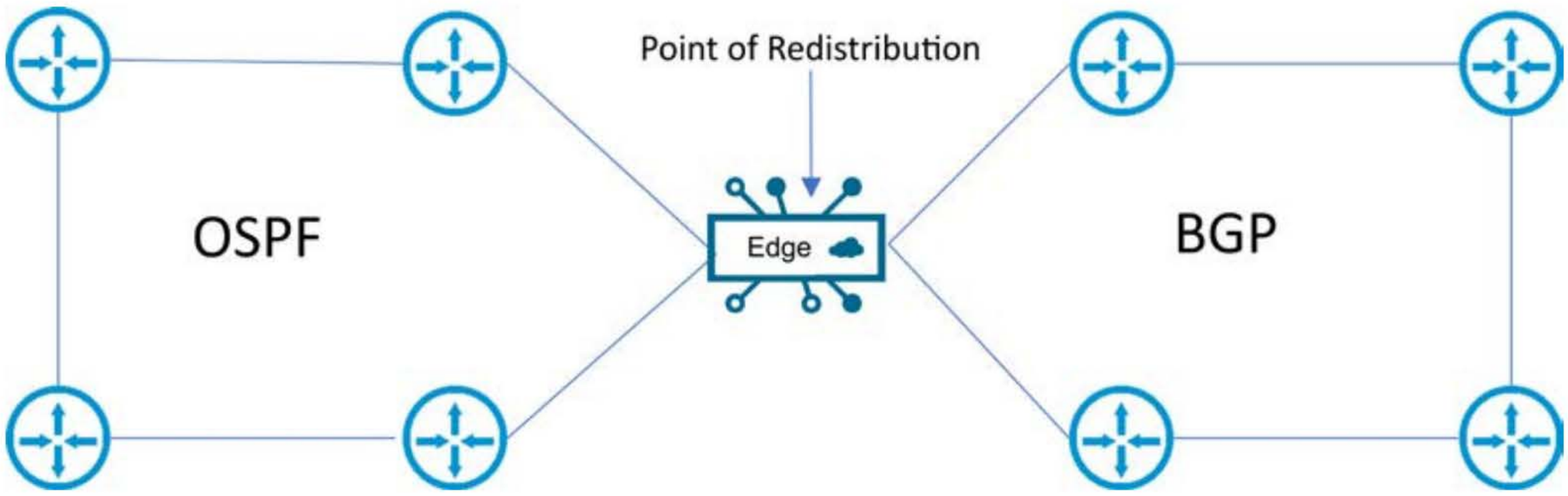
The static subnets of the NSDs configured on the Network Services page appear automatically on the Device Settings page.



Technet24

6-25 About Route Redistribution

You can independently enable OSPF and BGP. You can redistribute routes from OSPF to BGP or vice versa, or you can redistribute routes from both simultaneously.

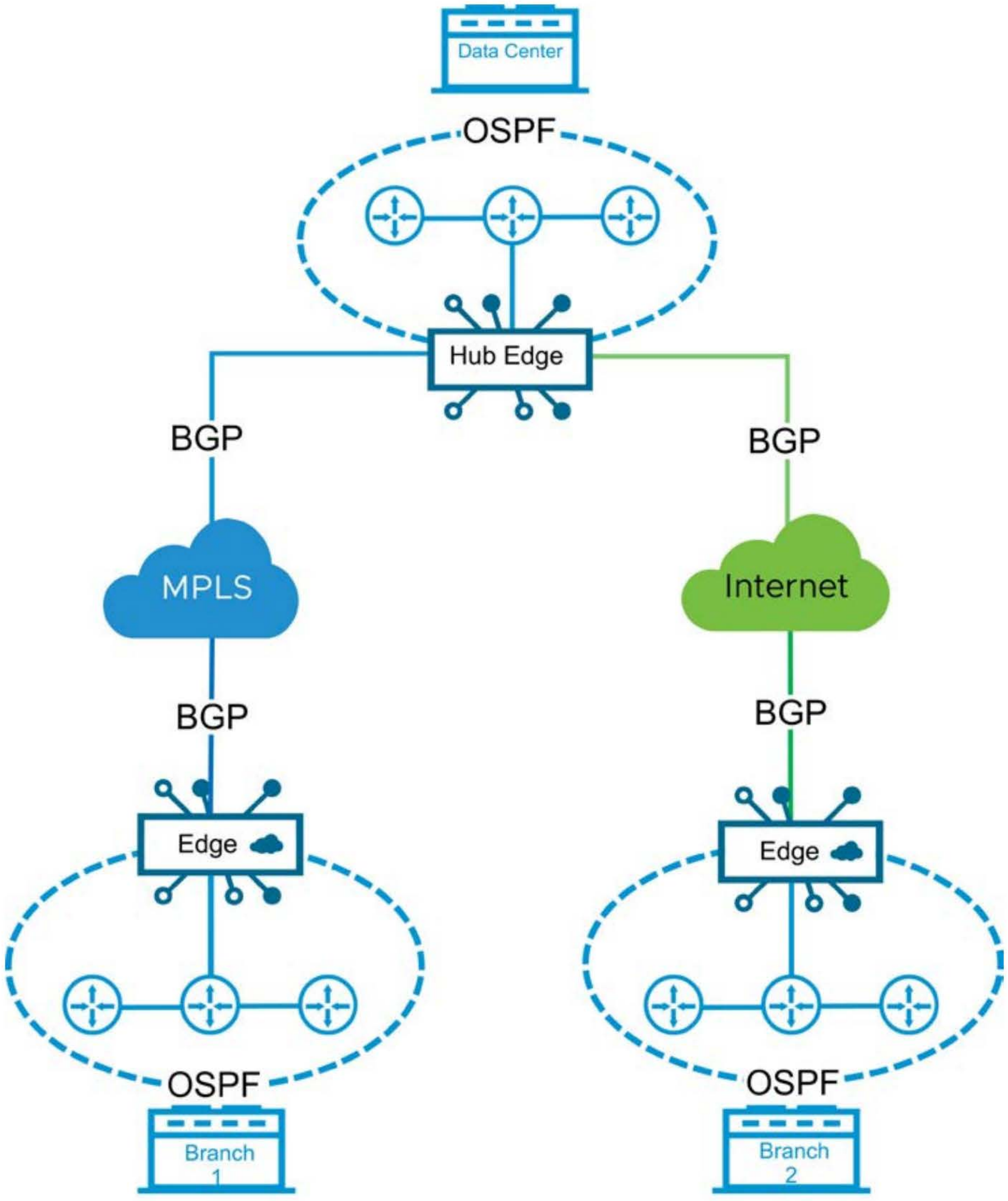


See the chapter on configuring OSPF and BGP redistribution in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

6-26 About OSPF

OSPF is a dynamic routing protocol that can be enabled only on a LAN interface. The LAN interface must be configured as a passive interface. The edge advertises only the prefix associated with that LAN switch port.

For full OSPF functionality, you must use it in routed interfaces.



Technet24

6-27 Configuring OSPF

To configure OSPF for VPN profiles in VMware SD-WAN Orchestrator, select **Configure** > **Profile** in the navigation pane. Locate the section called OSPF Areas.

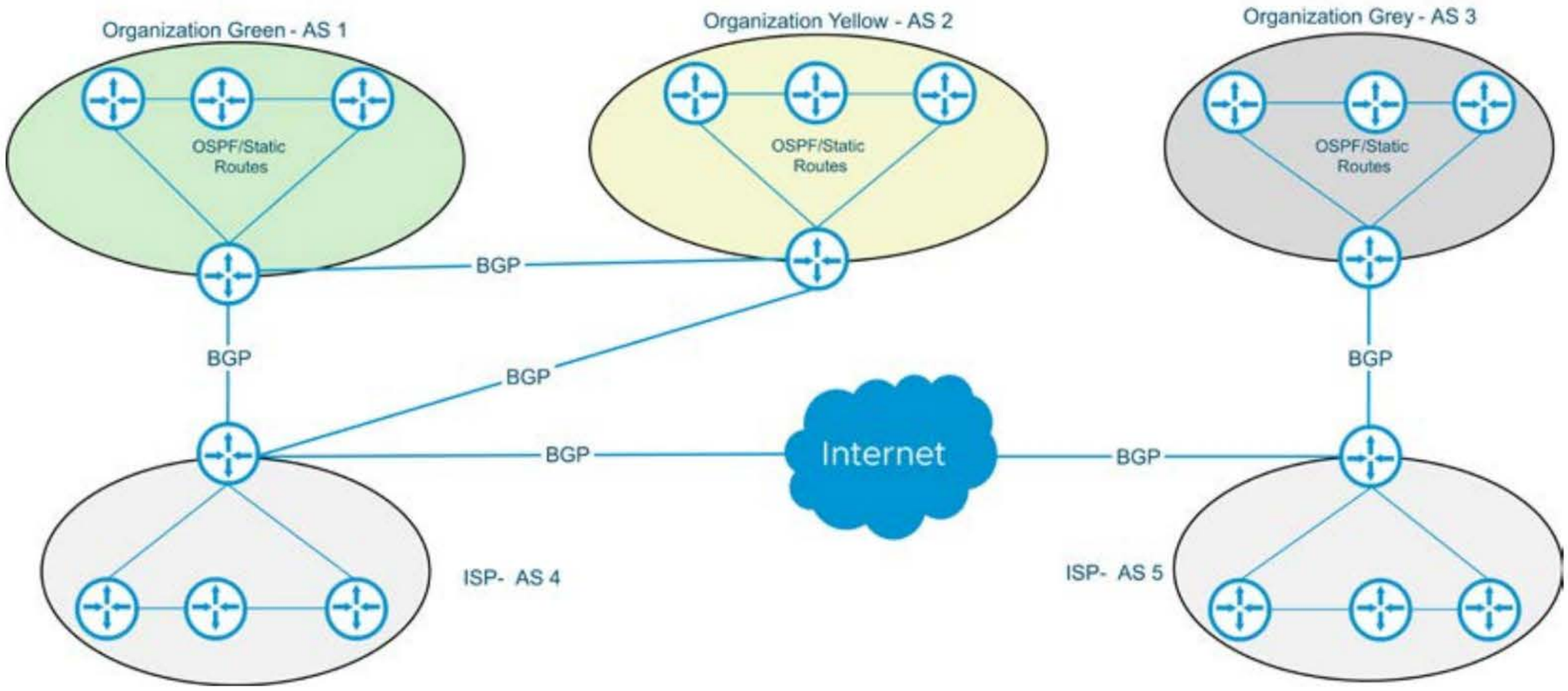
You configure the following settings under OSPF Areas in VMware SD-WAN Orchestrator:

- Redistribution Settings:
  - Route redistribution allows networks to use a routing protocol to dynamically route traffic based on information learned from a different routing protocol.
  - For example, advertising routes between BGP and OSPF, and vice versa.
- Default Route:
  - Default Route is the route used for unknown destinations.
  - From the **Default Route** drop-down menu, choose an OSPF route type (E1 or E2) to be used for default route.
- Advertise:
  - From the **Advertise** drop-down menu, select either **Always** or **Conditional**.
  - Selecting **Always** instructs the default route to be advertised at all times.
  - Selecting **Conditional** redistributes the default route only when the edge learns from the overlay or underlay networks.
- Overlay Prefixes: You must select the **Overlay Prefixes** check box to use the conditional default route.

See the section about enabling OSPF in *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

6-28 About BGP

BGP is an exterior gateway routing protocol used to route the packets between autonomous systems. BGP is the most widely used protocol on the Internet to exchange networks.



An autonomous system is the scope of a computer network that is controlled under a single administrative domain.

Technet24

6-29 Configuring BGP in VMware SD-WAN

In VMware SD-WAN, you can configure BGP on a per-segment basis at either the profile level or the edge level.

You can perform the following actions when configuring BGP:

- Establish connections between an edge to the underlay neighbors
- Configure BGP over IPsec from an edge to the non-SD-WAN neighbors
- Configure BGP over IPsec from gateways

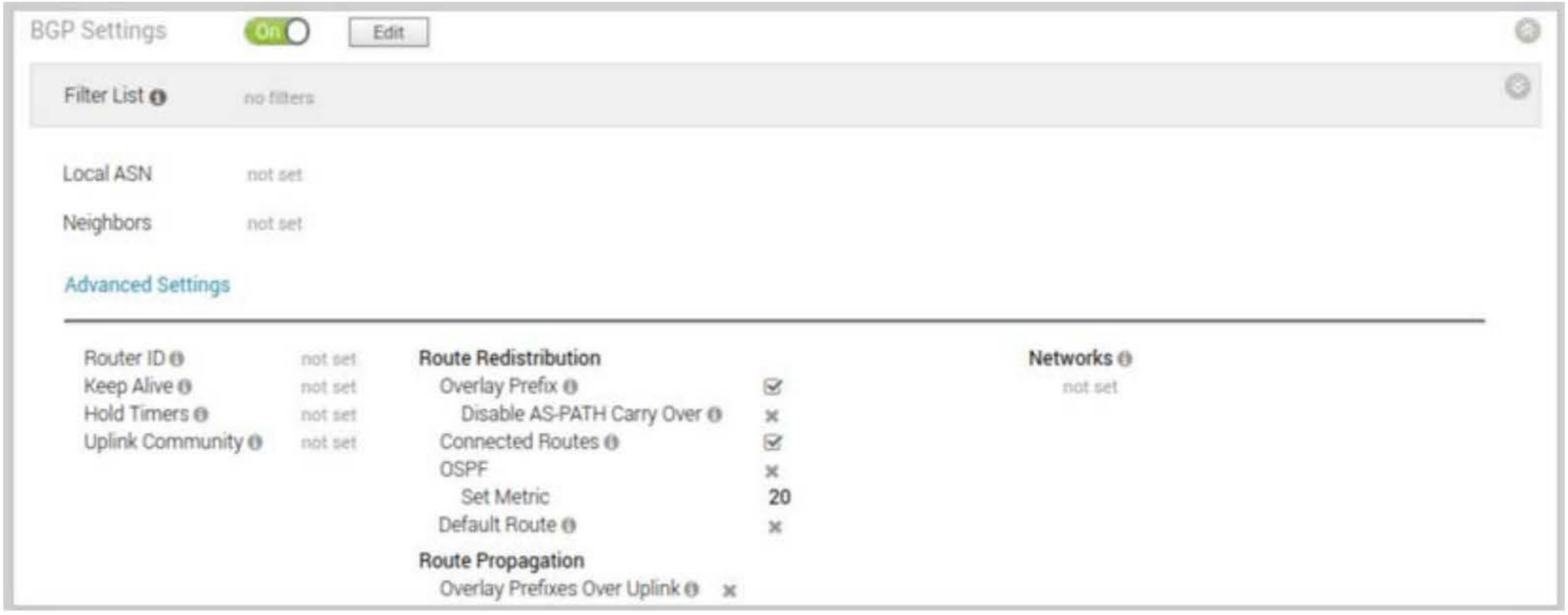
VMware supports 4-byte autonomous system number (ASN) BGP in the following instances:

- As the ASN of VMware SD-WAN Edge instances
- As the peer to a neighbor with 4-byte ASN
- As 4-byte ASNs in route advertisements

6-30 Configuring BGP from an Edge to the Underlay Neighbors

To configure BGP from an edge to its underlay neighbors in VMware SD-WAN Orchestrator:

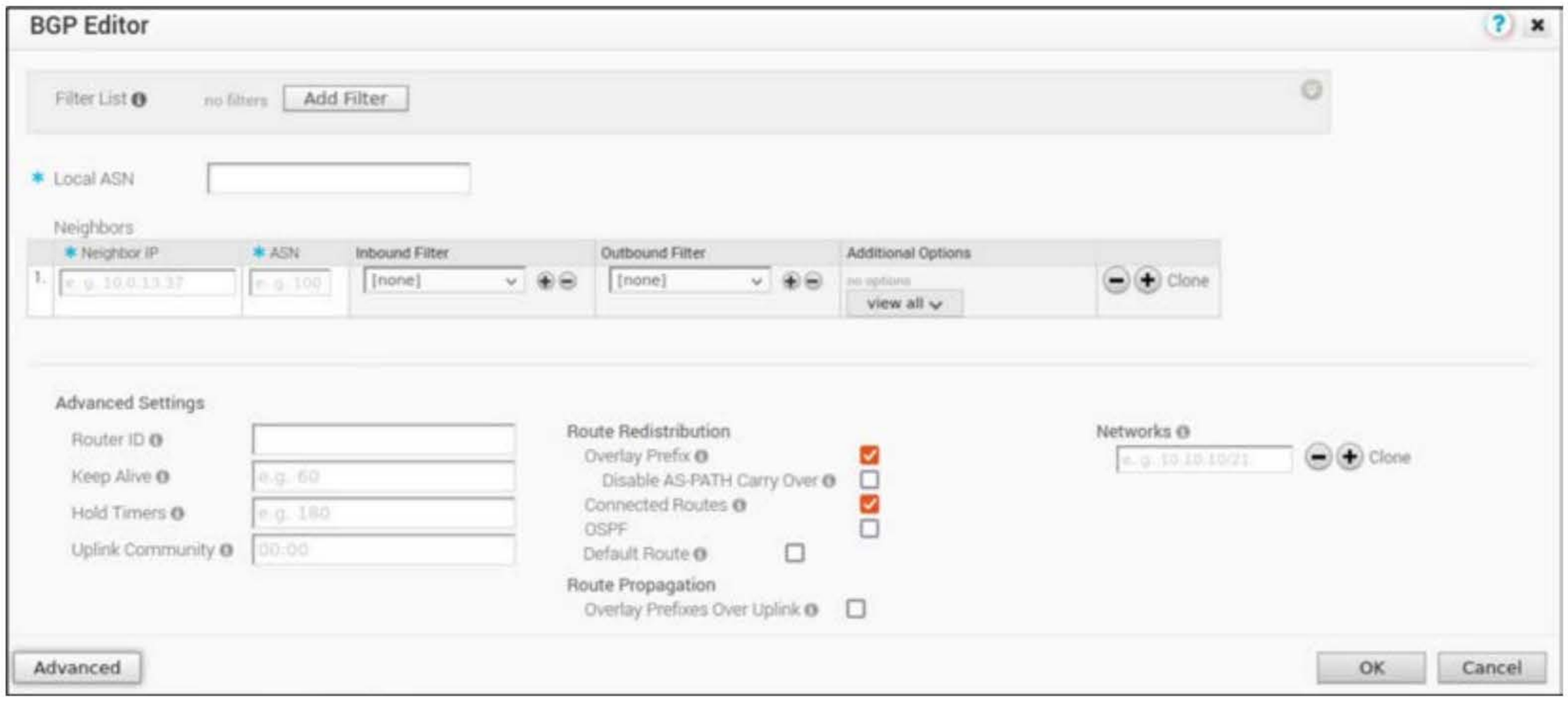
1. Select **Configure** > **Profiles** in the navigation portal.
2. Click the **Device** icon for a profile, or select a profile and click the **Device** tab.
3. Scroll down to BGP Settings.
4. Turn on the **BGP Settings** toggle and click **Edit**.



Technet24

6-31 BGP Advanced Configuration

You can configure advanced settings in the BGP Editor window, including filters, router ID, timers, route redistribution, and so on.



For more information about configuring BGP over IPsec from edges and gateways, see *VMware SD-WAN Administration Guide* at https://docs.vmware.com/en/VMware-SD-WAN/index.html.

6-32 About Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) is a simple Hello protocol. A pair of systems transmits BFD packets periodically over each path between the two. If one system stops receiving BFD packets for long enough, the protocol assumes that the neighboring system has failed.

BGP and OSPF detect route failures using their own mechanisms. These routing protocols have higher keepalive timers, which result in longer periods of time in which to detect the route failures.

BFD detects route failures between two connected entities faster and with lower overhead.

Technet24

6-33 Advantages of Bidirectional Forwarding Detection

Implementing BFD with existing routing protocols affords the following advantages:

- Faster route failure detection with low re-convergence time
- Lower overhead in route failure detection
- More uniform rate of route failure detection across routing protocols

6-34 Bidirectional Forwarding Detection in VMware SD-WAN

BFD can operate in two modes: asynchronous mode and demand mode. VMware SD-WAN only supports asynchronous mode.

In asynchronous mode, the systems periodically send BFD control packets to other systems. If several packets in a row are not received by one system, then the entire session is considered disconnected.

VMware SD-WAN supports BFD for the following routing protocols:

- BGP on VMware SD-WAN Edge appliances and partner gateways
- OSPF on VMware SD-WAN Edge appliances

Technet24

6-35 Review of Learner Objectives

- List the routing options available in a VMware SD-WAN environment
- Describe the configuration of static routes, Open Shortest Path First Protocol, and Border Gateway Protocol
- Describe the advantages of Bidirectional Forwarding Detection

6-36 Lesson 3: Dynamic Multipath Optimization

6-37 Learner Objectives

- List the functions of Dynamic Multipath Optimization
- Define link steering and explain its advantages
- Describe quality of service and class of service as implemented in VMware SD-WAN infrastructures

Technet24

6-38 About Dynamic Multipath Optimization

Dynamic Multipath Optimization (DMPO) is an advanced traffic-management feature. DMPO is used between all VMware SD-WAN components that process and forward data traffic, such as VMware SD-WAN Edge and VMware SD-WAN Gateway.

For branch-to-branch or branch-to-hub connectivity, VMware SD-WAN Edge appliances establish DMPO tunnels between one another. For connectivity to cloud applications, each edge appliance establishes DMPO tunnels with one or more VMware SD-WAN Gateway instances.

6-39 Features of Dynamic Multipath Optimization

DMPO is a collection of techniques utilized by the VMware SD-WAN overlay to provide the following features:

- Automatic link monitoring
- On-demand remediation
- Load balancing and dynamic link steering

Technet24

6-40 About Link Steering

VMware SD-WAN can perform application-aware, per-packet steering based on business policies and real-time link conditions.

During its lifetime, a traffic flow can be steered into one or more DMPO tunnels with no impact to the flow, even in the middle of communication.

Application steering can also improve data security. For example, in a payment card industry (PCI) environment, traffic must travel over PCI-certified cloud gateways. If it becomes nonfunctional and no other link is available, VMware SD-WAN stops transmitting to avoid potentially exposing sensitive information.

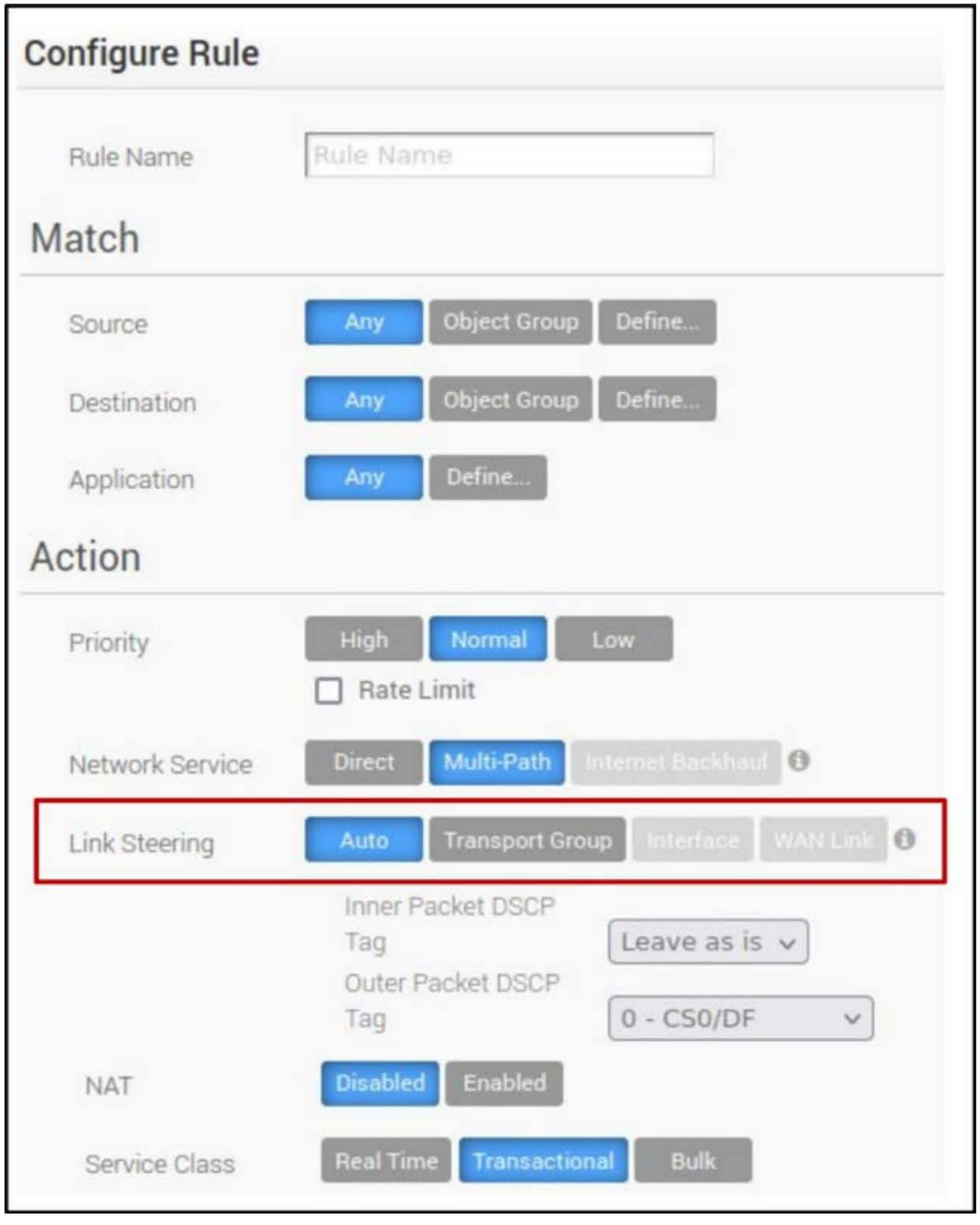
DMPO identifies traffic using layer 2 to layer 7 attributes, for example, VLAN, IP address, protocol, and applications.

The business policy contains preconfigured smart defaults that specify the default steering behavior and priority of more than 3,000 applications. Customers can immediately use the dynamic packet steering and application-aware prioritization without having to define policies.

6-41 Link Steering Modes

The following link steering modes are available in the Business Policy section of VMware SD-WAN Orchestrator:

- Auto (Default Mode)
- Transport Group
- Interface
- WAN Link



Technet24

The following link steering modes are available in the business policy:

- Auto (Default Mode): Dynamic Multipath Optimization (DMPO) automatically picks the best links based on the application type and automatically enables on-demand remediation when necessary.
- Transport Group:
  - DMPO uses the concept of a transport group to abstract the underlying WAN carriers and interfaces from the business policy configuration.
  - Transport groups are the WAN links grouped into one of the following categories: Public Wired, Public Wireless, or Private Wired.
  - These three categories help group similar WAN connections together.
- Interface:
  - You can apply a link steering policy to the interface, such as GE2, GE3, and so on.
  - IT administrators must be fully aware of how the VMware SD-WAN Edge appliance is connected to be able to specify which interface to use.
- WAN Link:
  - The WAN interface is connected to a WAN carrier.
  - A WAN interface is specific to the location of the VMware SD-WAN Edge appliance.
  - DMPO automatically detects the WAN carrier by performing a GeoIP lookup.
  - The IT administrator can also specify the WAN carrier.

For more information about link steering, see *Dynamic Multipath Optimization* at http://wan.velocloud.com/rs/098-RBR-178/images/sdwan-678-dynamic-multipath-optimization-wp-1119.pdf.

6-42 Quality of Service and Class of Service

You can configure DMPO to prioritize traffic based on quality of service (QoS) and class of service (CoS).

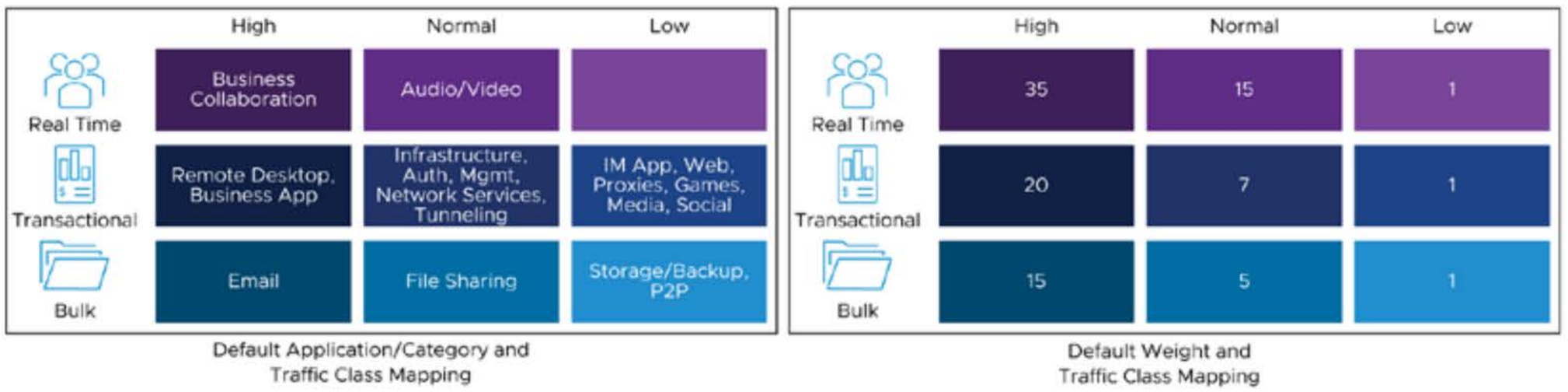
Traffic classes can help optimize link steering decisions.

The VMware SD-WAN Management Protocol header is added to the packet before leaving the VMware SD-WAN Edge appliance. On the receiving end, the gateway or the edge removes all tunnel headers. The original user data passes to the next hop router, which can be another L3 switch or a router in the enterprise scenario.

Technet24

6-43 Overlay QoS-CoS Mapping

A combination of priority and service class defines the class of traffic. The priority value categories are High, Normal, and Low, while the service class categories are Real Time, Transactional, and Bulk. This results in a total of nine traffic classes.

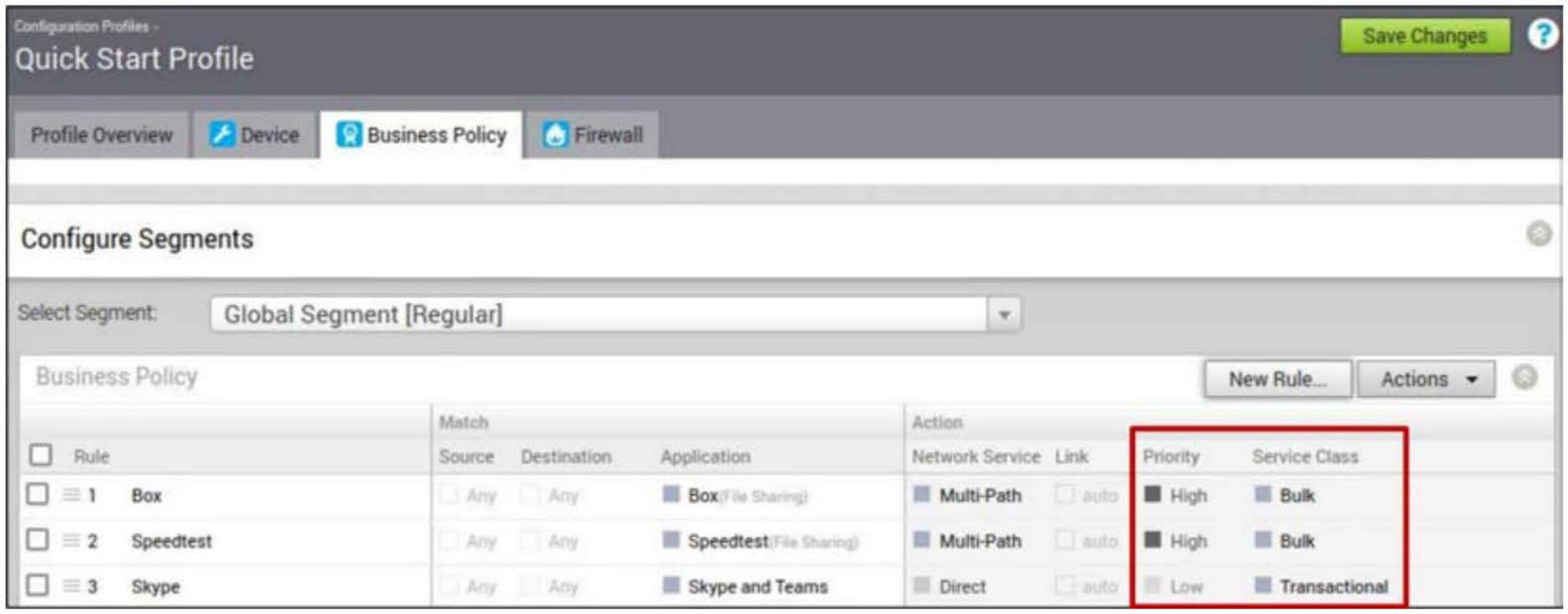


The application or category and the scheduler weight can be mapped to these traffic classes. The business policy contains preconfigured smart defaults that map more than 3,000 applications to traffic classes.

Customers can immediately use application-aware QoS without having to define a policy. They can also define policies for their own custom applications. Each traffic class is assigned a default weight in the scheduler. These parameters can be changed in the business policy.

6-44 Configuring Priority and Service Class (1)

You can configure the priority and the service class of traffic under the Business Policy tab of a profile in VMware SD-WAN Orchestrator. You can also view the existing configuration.



Technet24

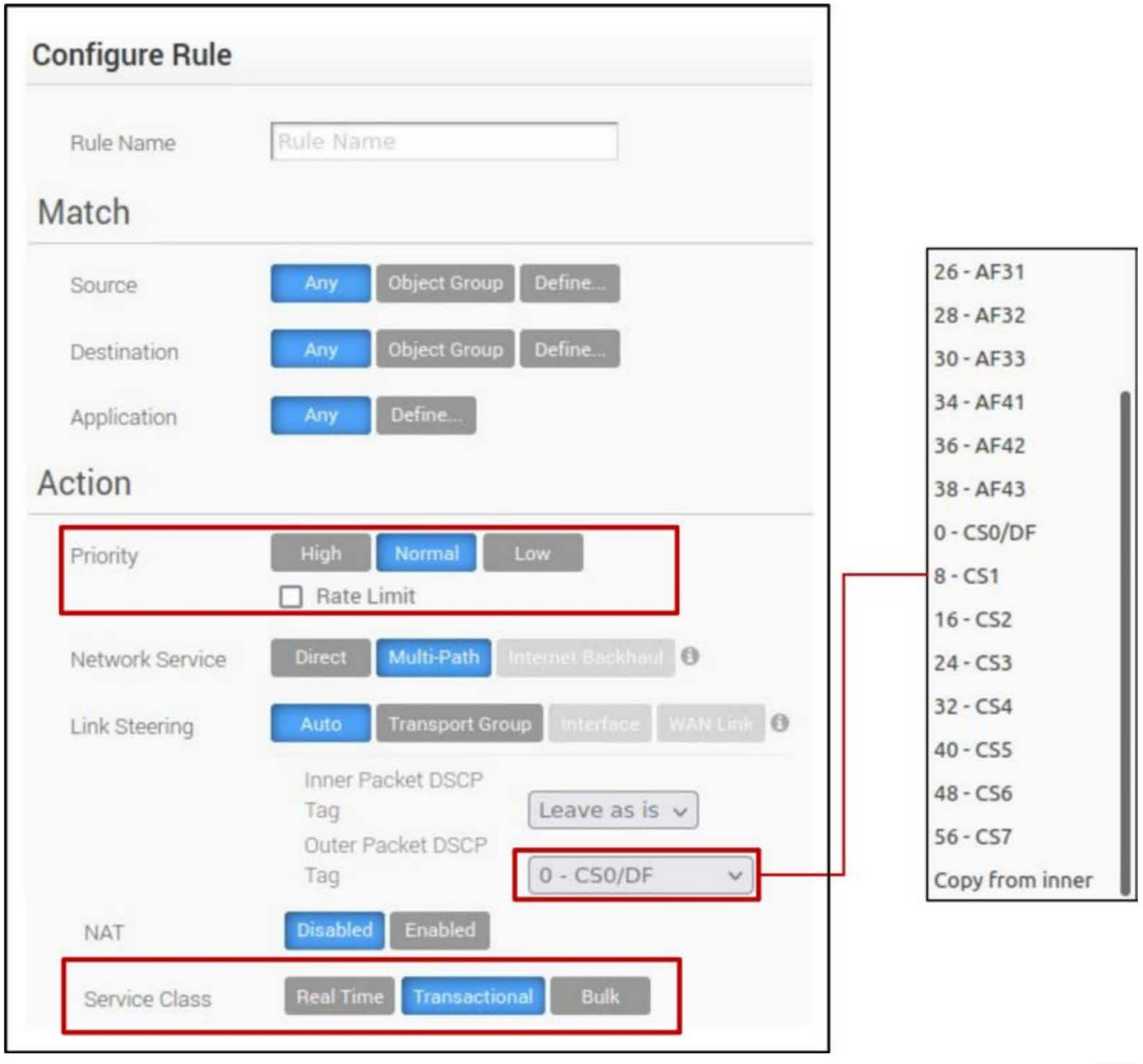
6-45 Configure Priority and Service Class (2)

To configure the priority and the service class of traffic:

1. Select **Configure** > **Profiles** in the navigation pane on the left.
2. Click the **Business Policy** tab.
3. Click **New Rule**.

   The Configure Rule dialog box appears.
4. Under Action, select the required categories next to Priority and Service Class.

You can also select the Differentiated Services Code Point (DSCP) tag for the traffic.



6-46 On-Demand Remediation

On-demand remediation facilitates error correction and jitter correction when multiple links have faults or only a single link is available.

DMPO can enable error correction when the WAN links have issues. The type of error correction used depends on the type of applications and the type of errors.

DMPO enables a jitter buffer for real-time applications when the WAN links experience jitter.

On-demand remediation reduces error correction and jitter correction:

- Error correction: Real-time applications such as voice and video flows can benefit from Forward Error Correction (FEC) when there is packet loss. DMPO automatically enables FEC on single or multiple links. When multiple links exist, DMPO selects up to two of the best links at any given time for FEC. Duplicated packets are discarded and out-of-order packets are reordered at the receiving end before being delivered to the final destination.
- Jitter correction: TCP applications such as file transfer benefit from Negative Acknowledgement (NACK). Upon detection of a missing packet, the receiving DMPO endpoint instructs the sending DMPO endpoint to retransmit the missing packet. Doing so protects the end applications from detecting packet loss and, as a result, maximizes the TCP window and delivers high TCP throughput even during lossy conditions.

Technet24

6-47 Bandwidth Aggregation

DMPO can perform per-packet load balancing. Per-packet load balancing utilizes the available links to deliver all packets of a single flow to the destination. Based on real-time WAN performance, DMPO selects the paths that the flow can use.

DMPO also performs packet resequencing to ensure that no out-of-order packets are introduced as a result of per-packet load balancing.

6-48 Lab 8: Dynamic Multipath Optimization

Configure business policies that enable deep application recognition and link steering:

1. Ping the Data Center Server from the Chicago Client
2. Run iPerf on Port 5001
3. List the Active Flows
4. Configure a Preferred Option Business Policy
5. Run iPerf on Port 8080
6. Verify That Traffic Follows the Preferred Route

Technet24

6-49 Review of Learner Objectives

- List the functions of Dynamic Multipath Optimization
- Define link steering and explain its advantages
- Describe quality of service and class of service as implemented in VMware SD-WAN infrastructures

6-50 Key Points

- You can configure static routes, OSPF, and BGP for dynamic routing in VMware SD-WAN.
- Bidirectional forwarding is faster at detecting the liveliness of a device than the built-in mechanisms of OSPF and BGP.
- Traffic flow can be steered onto one or more DMPO tunnels, in the middle of the communication, with no impact to the flow.
- Nine different traffic classes are available in VMware SD-WAN, determined by a combination of the priority value and the service class category.

Questions?

Technet24

Module 7

Monitoring, Testing, and Troubleshooting VMware SD-WAN

7-2 Importance

The VMware SD-WAN infrastructure spans multiple sites that are geographically remote. VMware SD-WAN manages all communication between the sites and to the cloud services. As a result, monitoring, testing, and troubleshooting the connections and configurations of the VMware SD-WAN infrastructure are critically important.

7-3 Module Lessons

1. Monitoring VMware SD-WAN
2. Troubleshooting VMware SD-WAN

7-4 Lesson 1: Monitoring VMware SD-WAN

7-5 Learner Objectives

- Identify the tools available to monitor the VMware SD-WAN infrastructure
- Describe the functions of the various VMware SD-WAN monitoring tools

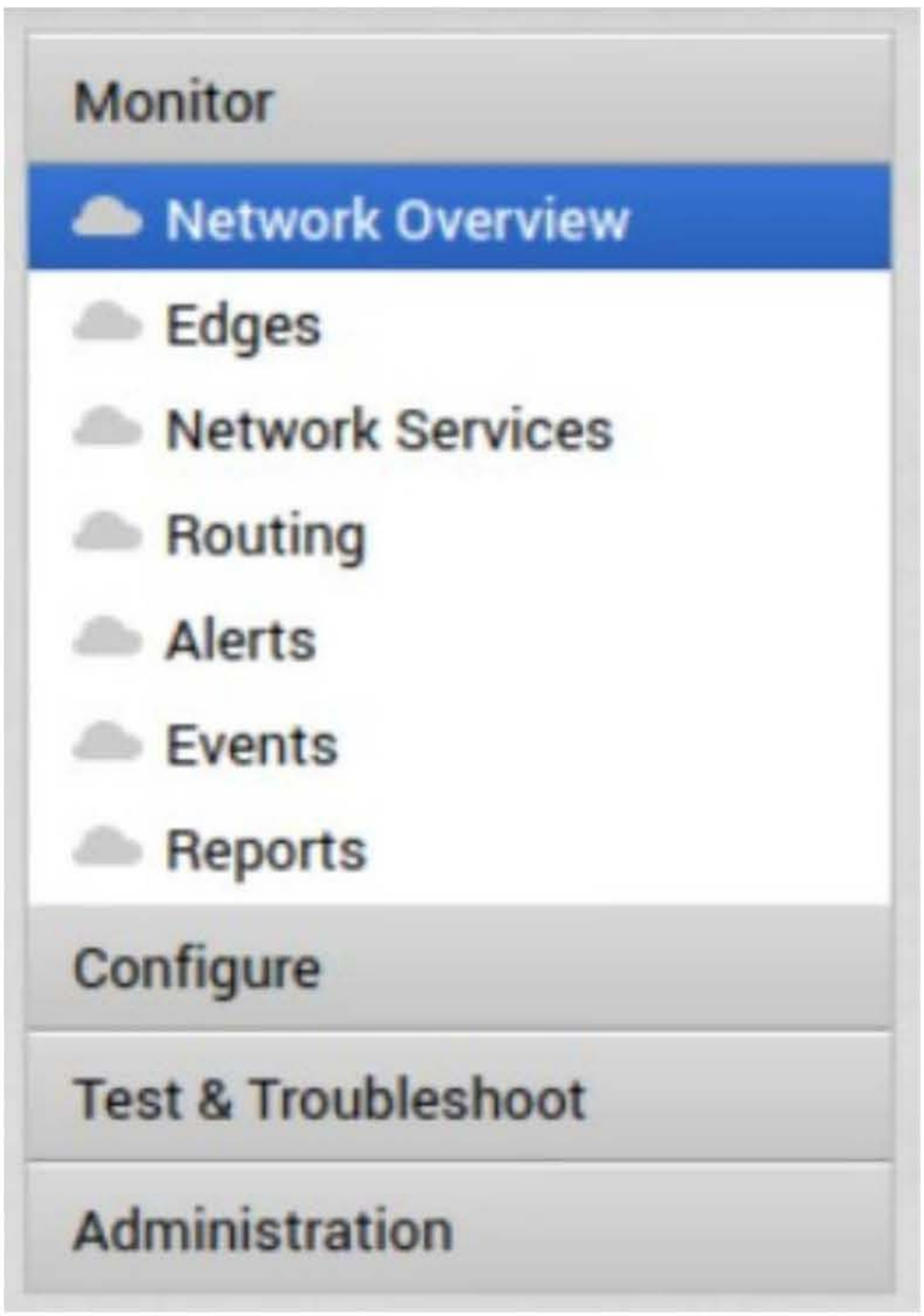
Technet24

7-6 Monitoring VMware SD-WAN

VMware SD-WAN Orchestrator provides an interface with which to monitor VMware SD-WAN. Monitoring functionality is accessible in the Monitor area of the navigation pane.

The following monitoring capabilities are displayed under Monitor in the navigation pane:

- Network Overview
- Edges
- Network Services
- Routing
- Alerts
- Events
- Reports

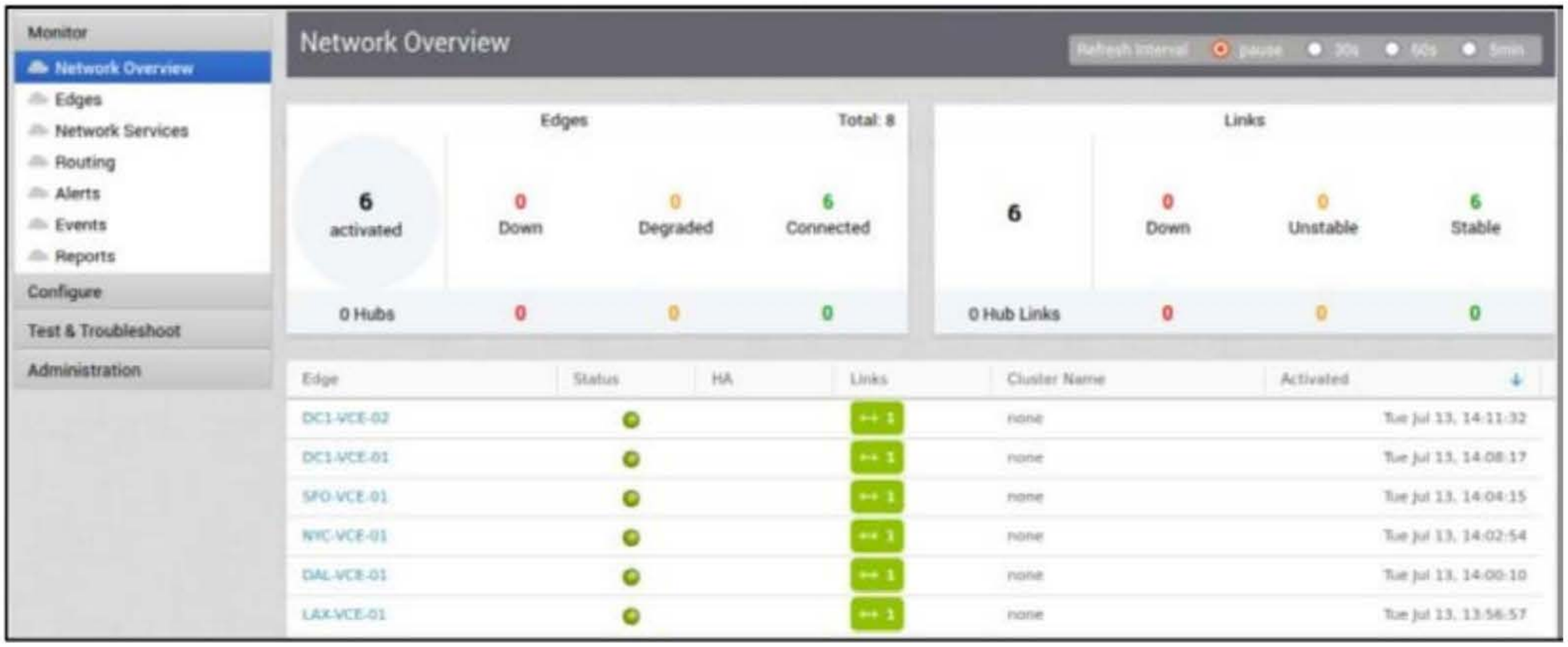


7-7 About Network Overview

On the Network Overview page, you can monitor the VMware SD-WAN networks by checking the status summary for each edge and link. The page provides a visual overview of the VMware SD-WAN Edge devices, non-SD-WAN destinations, profiles, and segments.

The Network Overview page includes the following information about the edges and links:

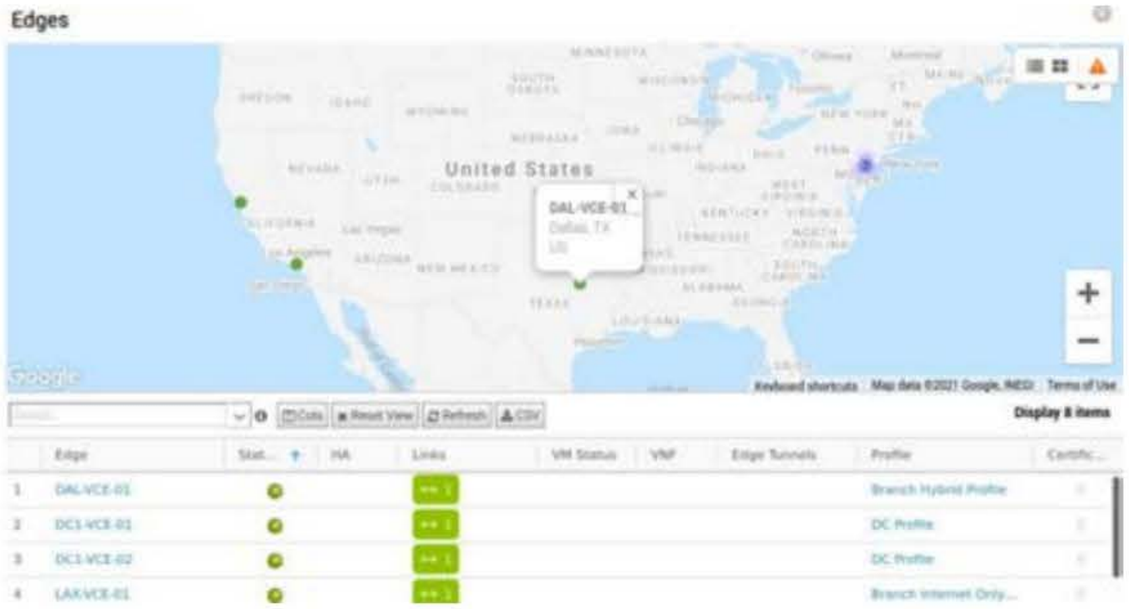
- Total number of edges
- Total number of edge hubs
- Total number of links
- Total number of hub links
- Number of edges and edge hubs marked as Connected, Degraded, or Down
- Number of links and hub links marked as Stable, Unstable, or Down



Technet24

7-8 Monitoring VMware SD-WAN Edge Appliances (1)

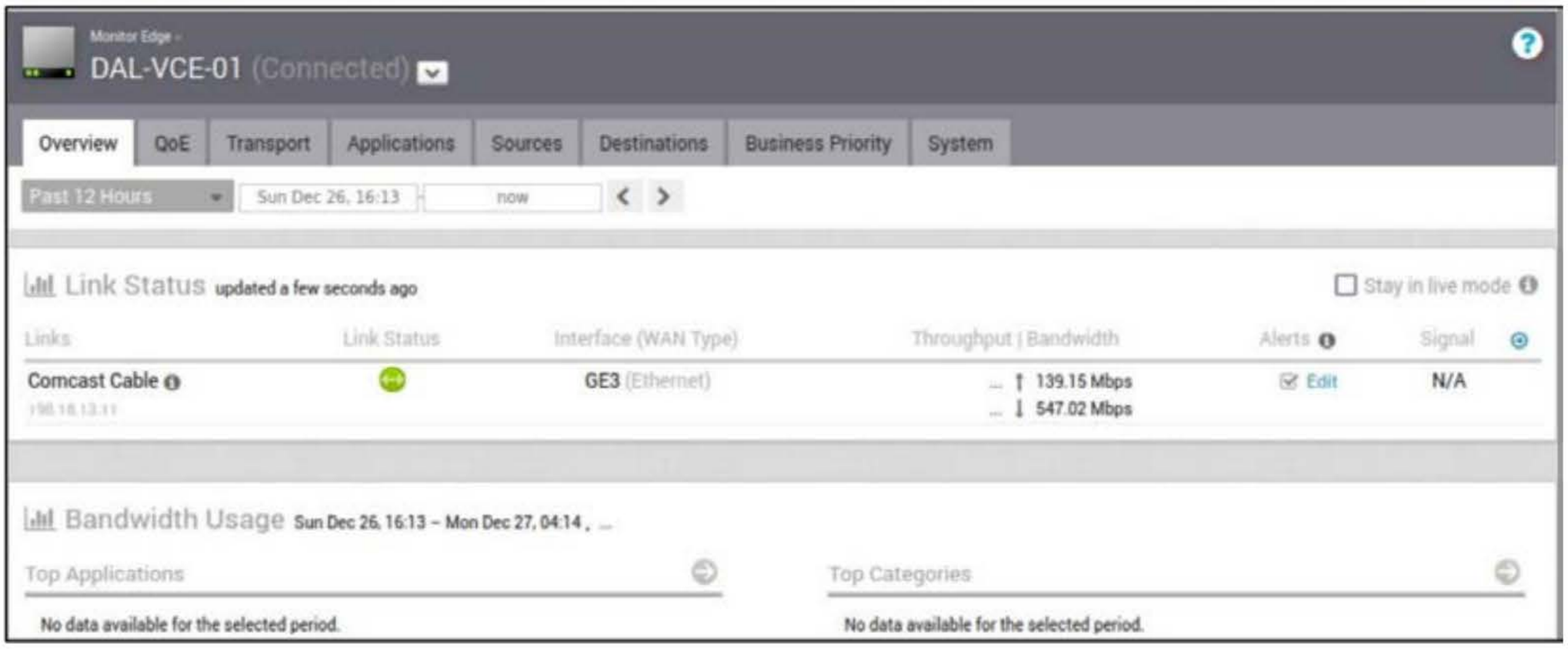
You can monitor the status of individual edges by selecting **Monitor** > **Edges** in the navigation pane. You can view the location of each edge on the map.



7-9 Monitoring VMware SD-WAN Appliances (2)

You can also view the following details of each VMware SD-WAN Edge appliance:

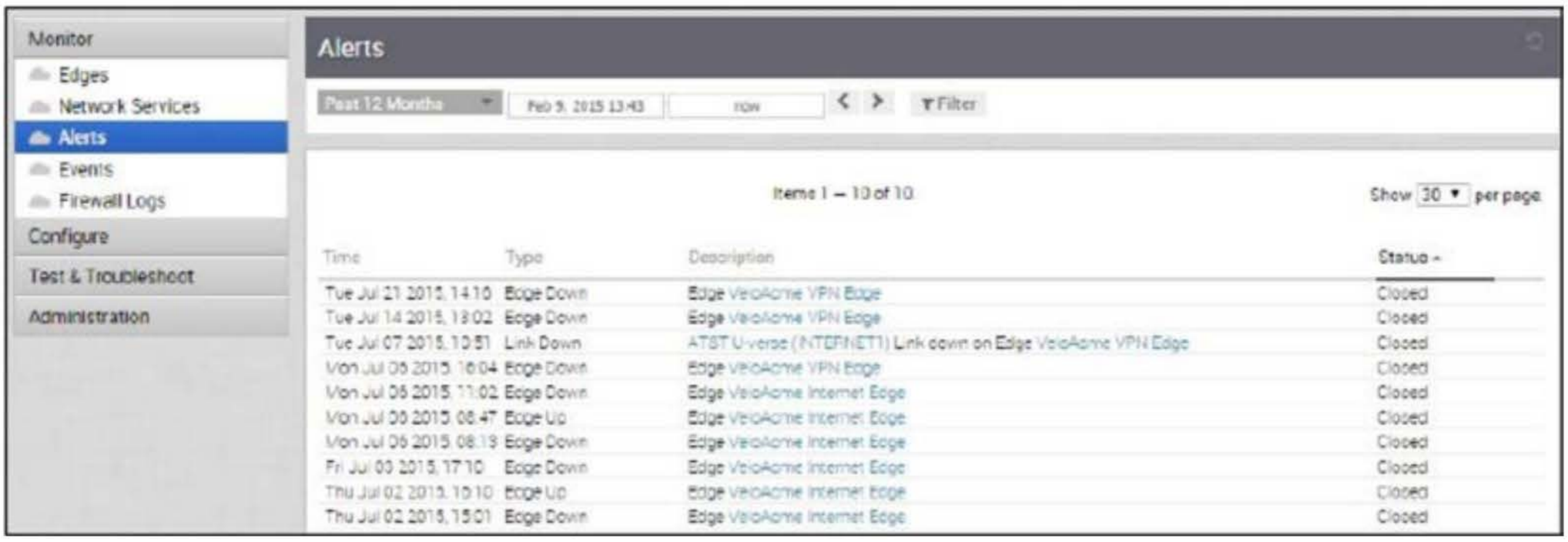
- WAN links
- Top applications used by the edges
- Usage data
- Traffic destinations
- Business priority of network traffic
- System information



Technet24

7-10 Monitoring Alerts

The Alerts function notifies one or more enterprise administrators when a problem occurs. An alert can be sent when edges, WAN links, or VPN tunnels experience an issue or when an edge high availability failover occurs. You can view alerts by selecting **Monitor** > **Alerts** in the navigation pane.

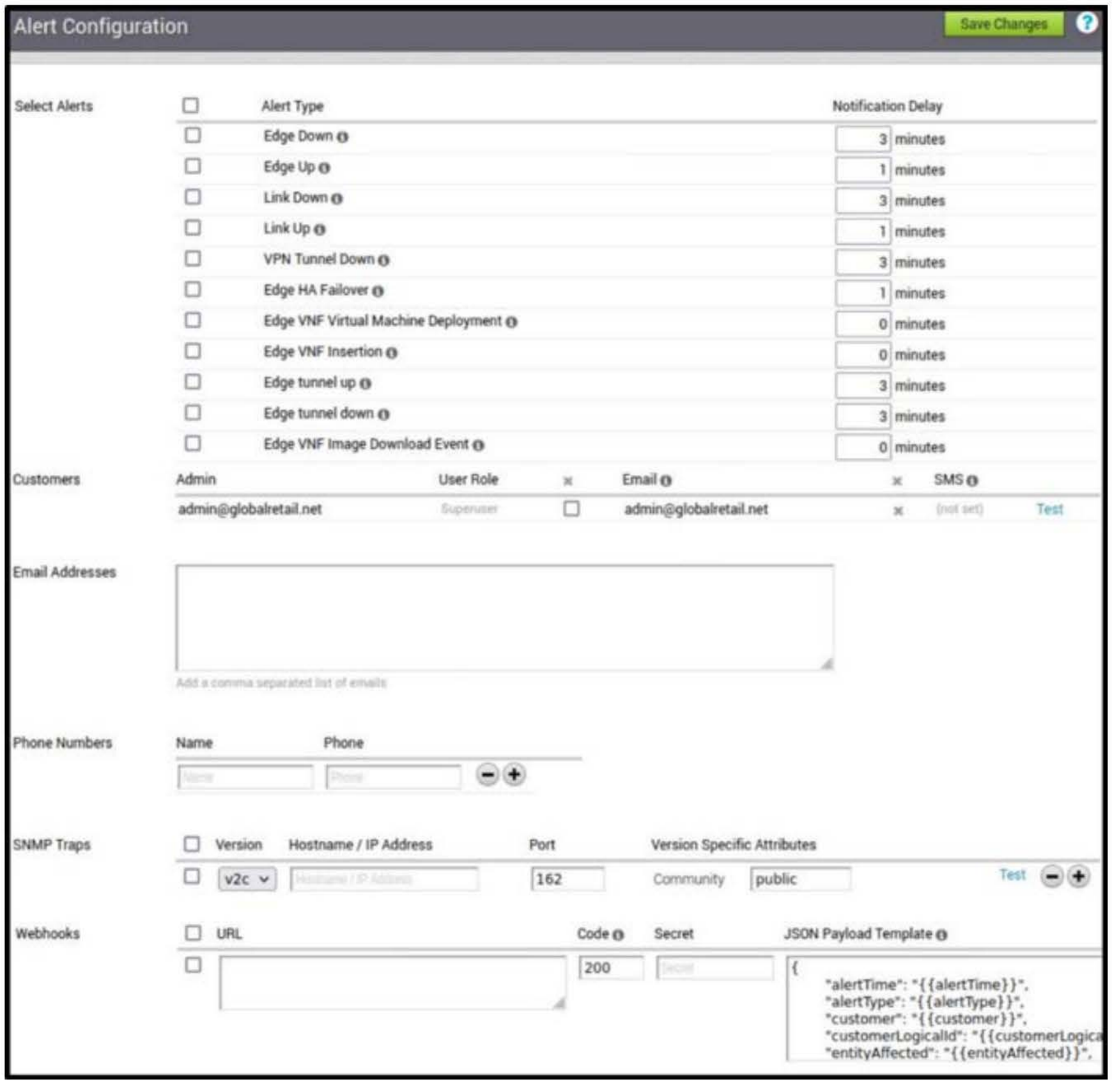


7-11 Configuring Alerts

You can configure alerts in VMware SD-WAN Orchestrator by selecting **Configure** > **Alerts & Notifications** in the navigation pane. Under Select Alerts, you select the events for which the alerts must be sent. You then enter the notification delay time (in minutes).

You can configure the following information when you create an alert:

- SMS settings
- Email addresses
- Phone numbers
- Simple Network Management Protocol (SNMP) traps
- Webhooks



Webhooks deliver data to other applications. They are triggered by certain events through HTTP POST.

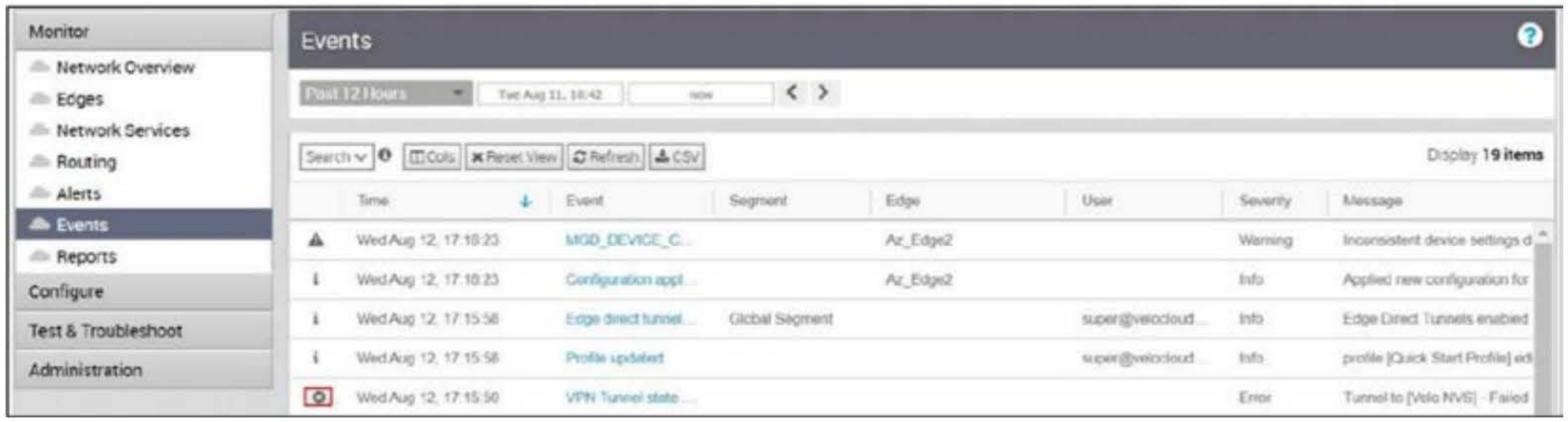
Technet24

7-12 Monitoring Events

You can see the events generated by VMware SD-WAN Orchestrator on the Events page.

The Events feature is useful for obtaining the following information:

- Audit trail of user activity
- Historical record of activity at a given site
- Record of outages and significant network events
- Analysis of degraded ISP performance



7-13 About Auto Rollback

If an edge appliance disconnects from VMware SD-WAN Orchestrator as the result of a configuration change, the edge rolls back to the last known configuration. This event also generates an alert to the administrator that the edge is down. The orchestrator logs this event as a bad configuration.

For standalone edges, the rollback time is 5 to 6 minutes. For edges with high availability, the rollback time is 10 to 12 minutes.

The rollback takes place only for edge-level device settings. If the bad configuration originates from a profile that causes multiple edges to go offline from the orchestrator, the edges will log a bad configuration and roll back individually to the last known good configuration. The profile configuration does not roll back automatically, so the administrator is responsible for fixing the profile.

Technet24

7-14 Monitoring Reports

The Reports page in VMware SD-WAN Orchestrator allows you to generate reports about the overall network summary. You can also generate reports about VMware SD-WAN traffic and transport distribution.

Consider the following information about the reports available in VMware SD-WAN Orchestrator:

- The reports provide descriptive analytics. You cannot use them for troubleshooting purposes.
- You can only generate a report for a 14-day period of activity and for a maximum of 600 edges.
- You can download the report as a PDF:
  - This report provides an overall summary of the traffic and transport distribution, represented as a pie chart.
  - It also provides a list of the top 10 applications according to traffic and transport type.

7-15 Review of Learner Objectives

- Identify the tools available to monitor the VMware SD-WAN infrastructure
- Describe the functions of the various VMware SD-WAN monitoring tools

Technet24

7-16 Lesson 2: Troubleshooting VMware SD-WAN

7-17 Learner Objectives

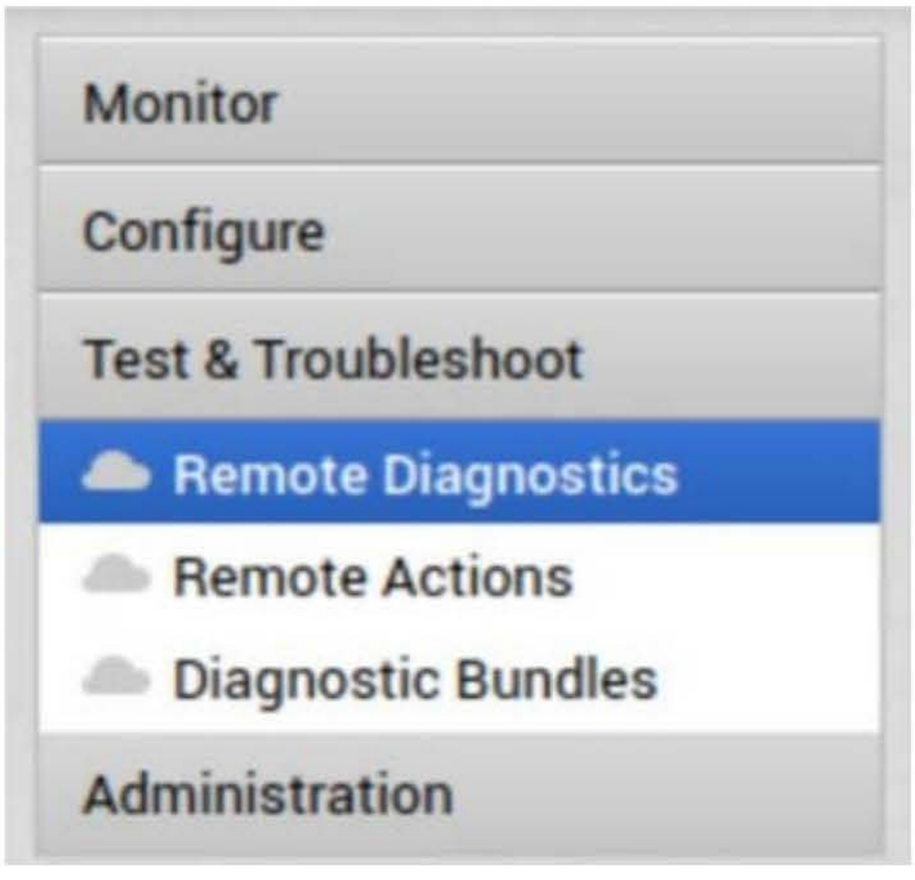
- Identify the functions available to test VMware SD-WAN configurations
- Explain how to perform a health check of VMware SD-WAN
- Describe the troubleshooting functions provided by VMware SD-WAN Orchestrator

7-18 Test & Troubleshoot Features

VMware SD-WAN Orchestrator provides several testing and troubleshooting features.

In the navigation pane, select **Test & Troubleshoot** to access the following options:

- Remote Diagnostics
- Remote Actions
- Diagnostic Bundles



Technet24

7-19 About Remote Diagnostics

From the Remote Diagnostics page, administrators can perform the following actions:

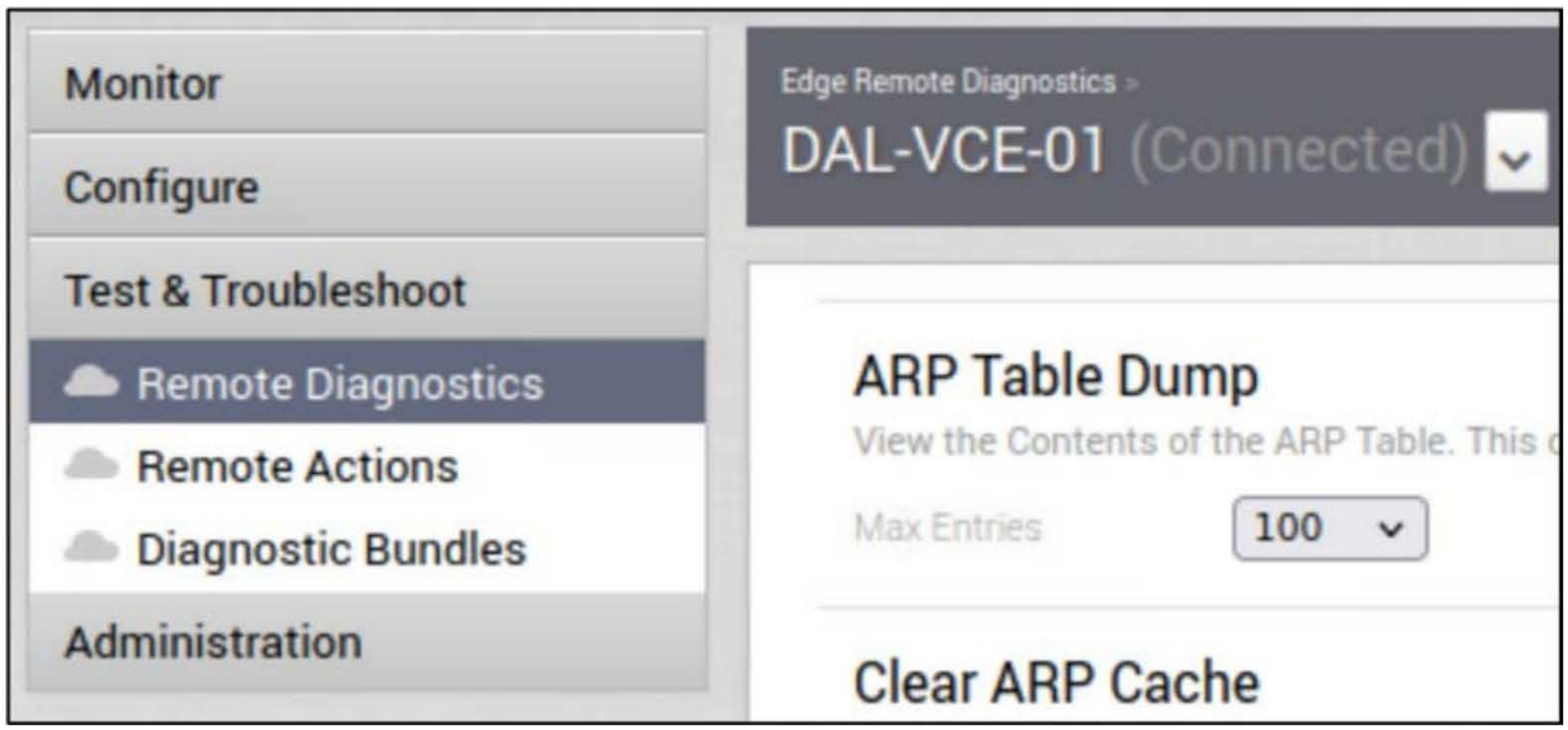
- View diagnostic information
- Run tests
- Perform troubleshooting

7-20 Viewing Diagnostics Information

The Remote Diagnostics page provides information required to investigate, troubleshoot, and perform health checks on the VMware SD-WAN Edge appliances.

The following information is available on the Remote Diagnostics page:

- Address Resolution Protocol (ARP) table
- High availability information
- Interface status
- Active flows
- Network address translation (NAT) table
- Network Time Protocol (NTP) information



Technet24

7-21 Running Diagnostics Tests

The Remote Diagnostics page also provides various tests that you can run to check the configuration and health of edge appliances:

- DNS test
- Ping test
- Traceroute
- VPN test
- WAN link bandwidth test

7-22 Basic Troubleshooting

You can perform some basic troubleshooting functions from the Remote Diagnostics page:

- Clear the ARP cache
- Restart the DNS and DHCP services
- Reset small form-factor pluggable (SFP) firmware configuration
- Troubleshoot Bidirectional Forwarding Detection (BFD)
- Troubleshoot the Border Gateway Protocol (BGP)
- Troubleshoot the Open Shortest Path First (OSPF) Protocol

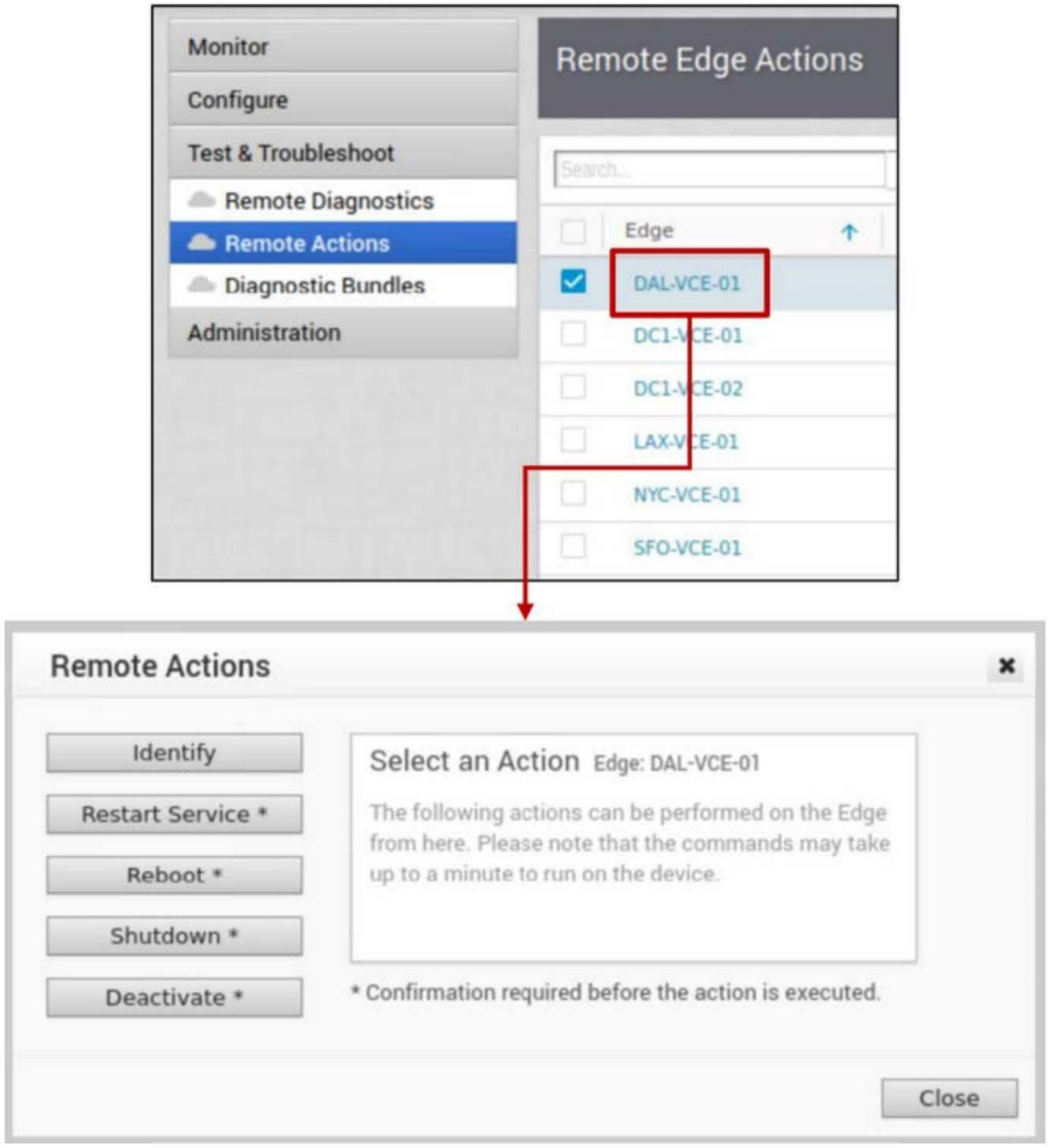
Technet24

7-23 About Remote Actions

VMware SD-WAN Orchestrator allows users to perform certain actions on edges remotely. You can perform remote actions only on edge appliances that are marked as Connected.

From the Remote Actions page, you can perform the following actions:

- Identify
- Restart Service
- Reboot
- Shutdown
- Deactivate



7-24 About Diagnostic Bundles

The Diagnostic Bundles page allows you to collect network packet data, configuration files, and log files as consolidated zip files. These bundles are useful for debugging purposes.

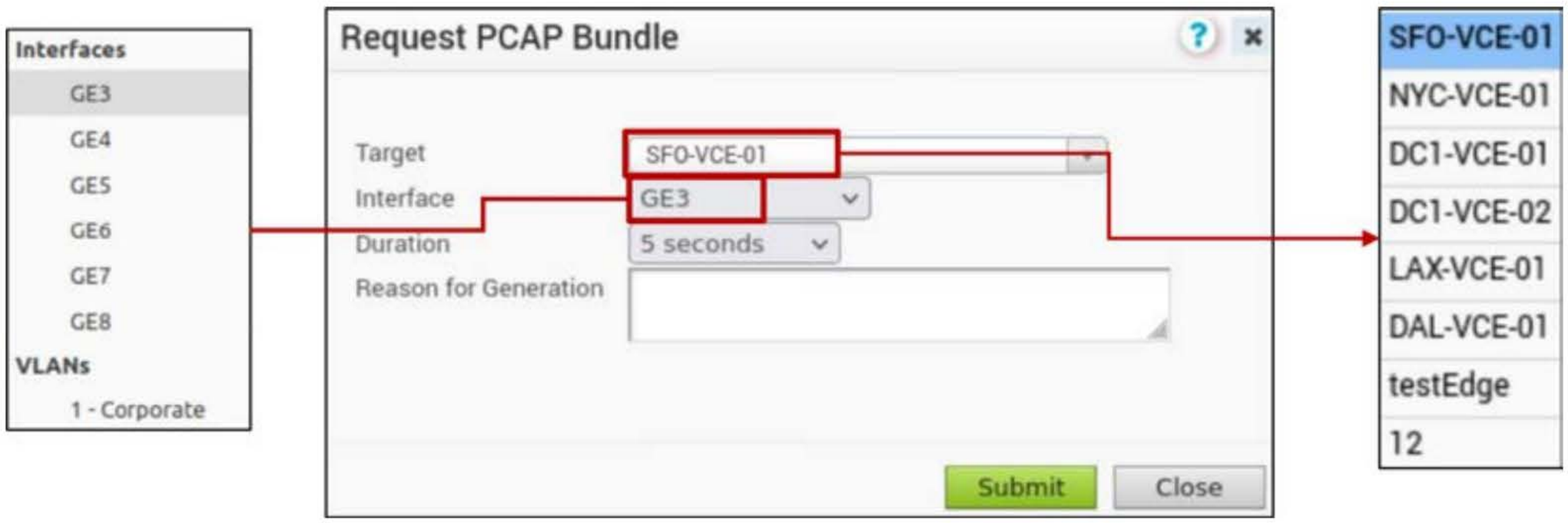
You can download the following types of bundles:

- Packet Capture (PCAP) bundles:
  - The PCAP bundle is a collection of the network packet data.
  - Operators, standard administrators, and customer support users can request PCAP bundles.
- Diagnostic bundles:
  - The diagnostic bundle is a collection of all the configuration and log files from a specific edge.
  - Only operators can request diagnostic bundles.

Technet24

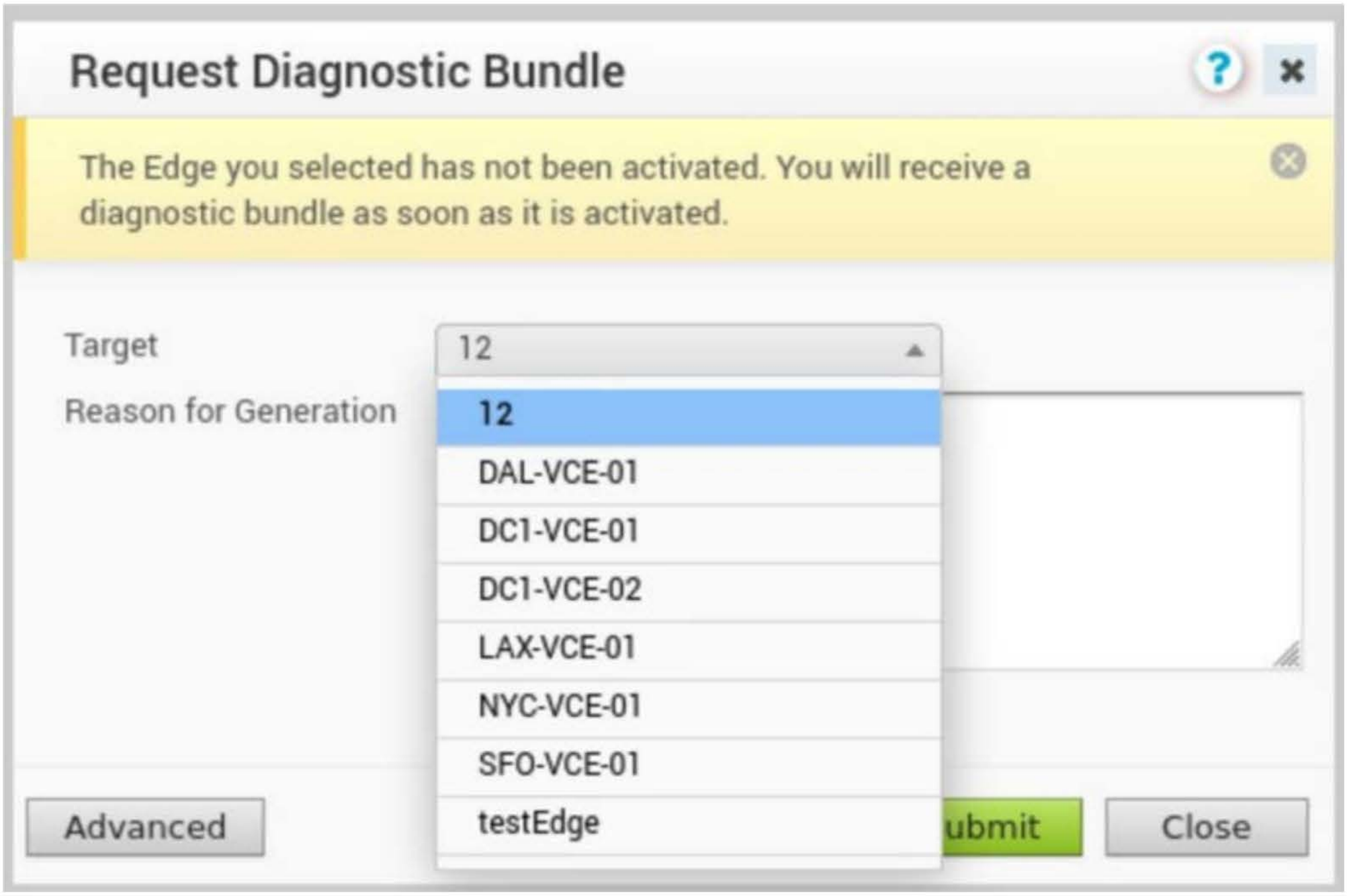
7-25 Requesting PCAP Bundles

When you request a PCAP bundle, you must select the name of the target edge, the interface of the target edge, and the duration of the capture.



7-26 Requesting Diagnostic Bundles

When you request a diagnostic bundle, you select the name of the desired edge from the **Target** drop-down menu.



Technet24

7-27 Review of Learner Objectives

- Identify the functions available to test VMware SD-WAN configurations
- Explain how to perform a health check of VMware SD-WAN
- Describe the troubleshooting functions provided by VMware SD-WAN Orchestrator

7-28 Key Points

- A VMware SD-WAN Edge appliance can roll back to its last known configuration if a configuration change results in a disconnection.
- You can configure alerts to notify administrators or operators about an event by SMS and email.
- You can perform basic health checks, configuration tests, and troubleshooting tests in VMware SD-WAN Orchestrator.

Questions?

Technet24