CONFIGURATION GUIDE



RUCKUS SmartZone Data Plane (vSZ-D/SZ100-D/SZ144-D) Configuration Guide

# **Copyright, Trademark and Proprietary Rights Information**

© 2022 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

# **Export Restrictions**

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

# Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

# **Limitation of Liability**

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

# **Trademarks**

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

Preface	5
Contacting RUCKUS Customer Services and Support	5
What Support Do I Need?	
Open a Case	5
Self-Service Resources	6
Document Feedback	6
RUCKUS Product Documentation Resources	6
Online Training Resources	
Document Conventions	
Notes, Cautions, and Safety Warnings	7
Command Syntax Conventions	
About This Guide	
New In This Document	
SmartLicense Overview	
SmartZone Data Plane Features	11
Virtual SmartZone Data Plane and SmartZone 100 Data Plane Overview	
Features and Benefits	
Tunneled WLANs and Flexible Traffic Redirection	
Architecture and Deployment Flexibility	
IPv6 Address Support	
vSZ-D/SZ100-D/SZ144-D DP Group	
DHCP Server and NAT Service on vSZ-D/SZ100-D/SZ144-D	
DHCP/NAT	
Configuring License Bandwidth	
Configuring the DHCP/NAT License Assignment	19
L3 Roaming	
Editing L3 Roaming for a vSZ-D/SZ100-D/SZ144-D	
Lawful Intercept	
Enabling Flexi VPN	
Enabling Tunnel Encryption	25
Network Architecture	27
Communication Workflow	29
NAT Deployment Topologies	
AP Behind NAT and vSZ-D/SZ100-D/SZ144-D Behind NAT	
vSZ and vSZ-D/SZ100-D/SZ144-D at Data Center Behind NAT	
vSZ-D/SZ100-D/SZ144-D at Access Site with NAT	
vSZ-D/SZ100-D/SZ144-D Behind NAT	
DHCP Relay with NAT	
DHCP Option 82 and Bridge Profile	
Configuring the vSZ Controller to Prepare for Network Segmentation	
Configuring the DHCP/NAT License Assignment	
Creating Profile-based DHCP	
Configuring Global Settings	

Configuring DHCP Pool Settings	
Creating Profile-based NAT	
Configuring NAT Global Settings	
Configuring NAT Pool Setting	
Creating an AP Group	
Creating WLAN for Network Segmentation	
Creating Network Segmentation Profile on the vSZ Controller	47
Hardware Requirements	
Important Notes About Hardware Requirements	
Supported Modes of Operation	
vSZ-D with DirectI/O	54
vSZ-D with Hypervisor vSwitch Installed	
vSZ-D and vSZ with Hypervisor vSwitch Installed	
Recommended NICs and Operation Modes	57
Hypervisor Configuration	
Supported Hypervisors	
General Configuration	
VMware Specific Configuration	59
KVM Specific Configuration	
Hypervisor Detail	
СРИ Туре	
Memory Allocation	
Disk Configuration	
NIC Configuration in Direct IO Mode	
NIC Configuration in vSwitch Mode	
Adding a PCI Device to a VM on Virt-Manager	
NIC Card Setting	
Deployment of vSZ	75
Deploy vSZ-D with 40GB NIC on ESXi Server	
Deploy vSZ-D with 40GB NIC on ESXi Server	
Deploy vSZ-D with 40GB NIC on Linux Server	
Deploy vSZ-D with 40GB NIC on Linux Server	
Upgrade Procedure	
Upgrade Procedure	
Data Plane Performance Recommendations	

# Preface

•	Contacting RUCKUS Customer Services and Support	5
	Document Feedback	
•	RUCKUS Product Documentation Resources	6
•	Online Training Resources	. 6
•	Document Conventions	7
•	Command Syntax Conventions	7

# **Contacting RUCKUS Customer Services and Support**

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

# What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the Open a Case section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the Self-Service Resources section.

# **Open a Case**

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <a href="https://support.ruckuswireless.com/contact-us">https://support.ruckuswireless.com/contact-us</a> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

# **Self-Service Resources**

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes-https://support.ruckuswireless.com/#products\_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/ case\_management.

# **Document Feedback**

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

# **RUCKUS Product Documentation Resources**

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

# **Online Training Resources**

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

# **Document Conventions**

The following table lists the text conventions that are used throughout this guide.

#### TABLE 1 Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<pre>device(config)# interface ethernet 1/1/6</pre>
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs.</b>
italics	Publication titles	Refer to the RUCKUS Small Cell Release Notes for more information.

# Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

### NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

### ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



## CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



#### DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

# **Command Syntax Conventions**

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{x   y   z}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
	Repeat the previous element, for example, member[member].
١	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

# **About This Guide**

•	New In This Document	9
•	SmartLicense Overview	9

# **New In This Document**

### TABLE 2 Key Features and Enhancements in SmartZone 6.1.1 (December 2022)

Feature	Description	Location
NIC Driver support	<b>Updated</b> : Removed the NIC model supported fields for VMXNET3/virtIO and Virtio.	Recommended NICs and Operation Modes on page 57
Upgrade Procedu	Controller and vSZ-D/SZ100-D/SZ144-D Firmware Compatibility Matrix	Upgrade Procedure on page 113

# **SmartLicense Overview**

This guide is intended for use by those responsible for managing the RUCKUS Wireless network controller. Therefore, it assumes basic working knowledge of the RUCKUS wireless network controller and Access Point (AP) products.

The controller (SmartZone) currently includes a licensing feature that stores proprietary license files. As part of this feature, the new license feature implementation uses *Flexera* licensing to handle license management.

The controller uses a Flexera license server as the primary license source and periodically retrieves the license from the server for any updates. The manual upload of a binary license file from the local machine is also supported.

In addition displaying all assigned license entitlements on the user interface, the user interface provides a method to set the Local License Server (LLS) address, and allows you to manually retrieve license data from the license server from the controller. The user interface enforces the system upgrade process by checking the availability of supported licenses.

The SmartZone (controller) user interface provides information about licensing and the licenses you are currently using to determine when you may require more licenses (or fewer licenses) over time.

For the purposes of this document, the following assumptions are made:

- You have already deployed your SmartZone system.
- You have purchased a license or are using the 90-day trial license.

# **SmartZone Data Plane Features**

# Virtual SmartZone Data Plane and SmartZone 100 Data Plane Overview

The RUCKUS Virtual SmartZone controller platform is the industry's most scalable Wi-Fi controller platform that enables service providers and enterprises to leverage virtualization technologies to deploy superior Wi-Fi management systems.

With the introduction of the Virtual Data Plane (vSZ-D) in SZ 3.2 release and SZ100-D in 5.1, the SmartZone platform launched sophisticated data plane capabilities. This is truly differentiated and distinguished offering that provides compelling business benefits for varied deployment scenarios.

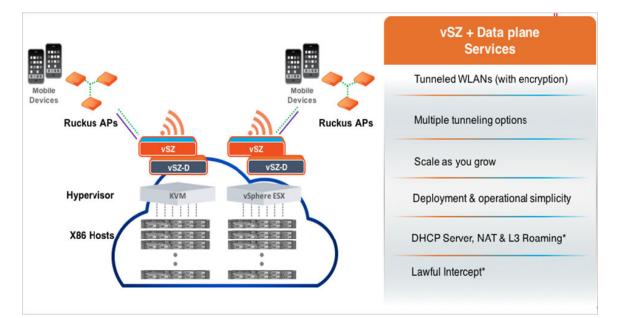


FIGURE 1 vSZ-D/SZ100-D/SZ144-D Services

# **Features and Benefits**

•	Tunneled WLANs and Flexible Traffic Redirection	. 14
•	Architecture and Deployment Flexibility	. 15
	IPv6 Address Support	
	vSZ-D/SZ100-D/SZ144-D DP Group	
	DHCP Server and NAT Service on vSZ-D/SZ100-D/SZ144-D	
•	L3 Roaming	. 21
	Lawful Intercept	
	Enabling Flexi VPN	
	Enabling Tunnel Encryption	

vSZ-D is a virtualized service to segregate and securely tunnel user data traffic.

### NOTE

You can create a maximum of 2047 multicast groups on vSZ-D/SZ100-D/SZ144-D.

Some of the key use cases for the vSZ-D/SZ100-D/SZ144-D are:

### FIGURE 2 Use cases

- Tunneling of user data traffic
- Guest traffic encryption & security
- POS data traffic tunneling for PCI compliance
- ✓ VoIP traffic tunneling
- ✓ Seamless roaming/mobility across L2 subnets
- Flat network topology Avoid costly network reconfiguration (ex: VLAN tagging at AP Ethernet ports, avoid VLAN clashes)

### **Traffic handling**

- Improved network & operational management with distributed or centralized tunneled WLANs
- ✓ Data aggregation with support for forwarding data over multiple tunnel types towards network
- gateways, router

NFV aligned future proof architecture

Scalable and NFV aligned true separation of control plane and data plane functions

#### TABLE 3 Feature and Benefits

Feature	Benefit
Secure data plane tunneling	Manages the creation of aggregated user data streams through secure tunnel
Multiple Hypervisor Support	Supports the most widely deployed VMware and KVM hypervisors, applicable only to vSZ-D.
Dynamic data plane scaling	Supports 1Gbps, 10Gbps or even higher throughput capacities to support all types of enterprise and carrier deployments that can be dynamically tuned without needing software updates

Tunneled WLANs and Flexible Traffic Redirection

### TABLE 3 Feature and Benefits (continued)

Feature	Benefit
Seamless integration with vSZ controller	• Simple integration and management with vSZ controller clustering architecture enables support for multiple vSZ-D/SZ100-D/SZ144-D instances
	• vSZ + Data Plane services
	<ul> <li>20 vSZ-D/SZ100-D/SZ144-D instances per vSZ instance</li> <li>80 vSZ-D/SZ100-D/SZ144-D instances per vSZ cluster of 4 instances</li> </ul>
	Workaround:
	<ul> <li>If CALEA/Flexi-VPN/L3 Roaming/Network Segmentation is enabled, user shall not be able to approve more than 40 DPs.</li> <li>If CALEA/Flexi-VPN/L3 Roaming/Network Segmentation is not enabled and the user adds more than 40 DPs, then CALEA/Flexi- VPN/L3 Roaming/Network Segmentation setting shall be greyed out.</li> </ul>
	• The controller runs in Active/Active (3+1) mode for extremely high availability.
	• Each vSZ-D runs as an independent virtual machine instance that is managed by the controller.
	<ul> <li>With vSZ-D/SZ100-D/SZ144-D DP Group enabled, it is possible to support a distributed vSZ-D/SZ100-D/SZ144-D instance on a per vSZ Zone basis.</li> </ul>
Superior data plane functions	Encrypted tunnel aggregation from all types of WLANs (Captive portal, 802.1x, HS2.0), VLANs, DHCP Relay, DHCP Server, NAT, L3 Roaming, Lawful Intercept, IPv6 Support and NAT traversal between AP and vSZ-D/SZ100-D/SZ144-D.
Scalable Deployment Architectures	Provides the ability to service distributed and centralized network configurations
Deployment and operational simplicity	Simple integration and management with vSZ-E and vSZ-H installations
Site level QoS and policy control	Service policy management and data stream (will be supported in a later release)

# **Tunneled WLANs and Flexible Traffic Redirection**

Many WiFi deployments have requirements to support tunneled WLANs for guest isolation and encryption, POS data security, VoIP traffic management, and seamless roaming across L2 subnets. One of the most deployed and easily managed way to meet these requirements is to enable a flat network topology by tunneling traffic to a controller.

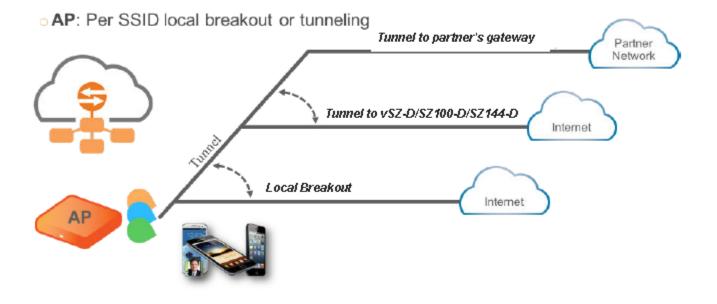
With the vSZ-D/SZ100-D/SZ144-D, it is now possible to support tunneled WLANs on RUCKUS APs that are managed by a vSZ controller. In addition, both the RUCKUS APs and the vSZ-D/SZ100-D/SZ144-D support encryption capabilities on tunnels for data protection. This is especially important when tunneling guest traffic and in use cases where the service provider or enterprise operator does not have control on the backhaul links.

### NOTE

SZ100 and SZ144 controllers are not supported with external DPs (vSZ-D/SZ100-D/SZ144-D).

FIGURE 3 Traffic redirection flexibility with the Virtual SmartZone platform

- Controller or vSZ-D/SZ100-D/SZ144-D: Aggregate user data and tunneling
- AP: Per SSID local breakout of tunneling

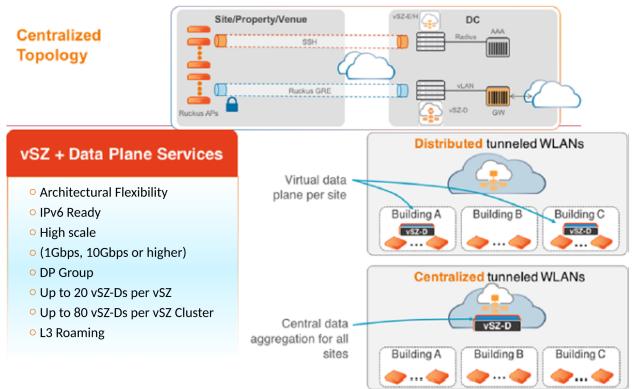


# **Architecture and Deployment Flexibility**

Existing architectures for supporting tunneled WLANs involve tunneling data back into controllers. This results in architectures where a complete controller needs to be deployed on each site or all the tunneled WLAN traffic being backhauled into a centralized data center. This also results in dependencies on choices for controller platforms with different capacity profiles, which increase the capital and operating expenses of the entire solution without actually solving the real problem.

With the vSZ-D/SZ100-D/SZ144-D, it is now possible to deploy the same software either on-premise (on cheaper COTS hardware) when needed, as well as deploy it at the data center (on higher end COTS hardware) and the entire Wi-Fi management controller by the vSZ controller.

### FIGURE 4 Unmatched architecture flexibility



# **IPv6 Address Support**

The vSZ-D/SZ100-D/SZ144-D supports IPv6 addresses for the data plane interface. The vSZ-D/SZ100-D/SZ144-D also supports client IPv6 addresses for DHCP Relay only.

## NOTE

vSZ-D/SZ100-D/SZ144-D does not support IPv6 addresses for northbound soft-GRE tunnels.

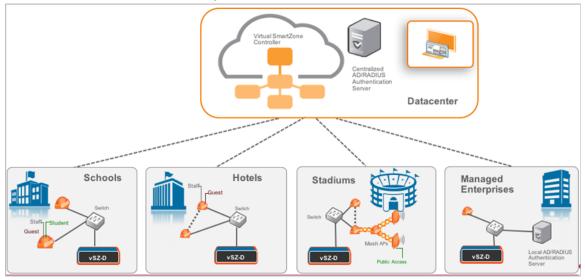
# vSZ-D/SZ100-D/SZ144-D DP Group

It is now possible to dedicate vSZ-D/SZ100-D/SZ144-D instance on a per distributed site basis.

This is especially useful for managed service providers and ISPs who manage remote distributed sites through a central or regional data center. In this architecture, the vSZ is in the provider's data center managing APs across all remote distributed sites.

On sites where there is a need for tunneling, they can introduce the vSZ-D/SZ100-D/SZ144-D and bind them to that particular site so that all APs on that site shall tunnel traffic locally to the vSZ-D/SZ100-D/SZ144-D DP Group on that site.

#### FIGURE 5 vSZ-D/SZ100-D/SZ144-D DP Group



# DHCP Server and NAT Service on vSZ-D/SZ100-D/SZ144-D

Highly scalable and optimized DHCP Server on vSZ-D/SZ100-D/SZ144-D is designed from the ground up for WiFi networks. It also introduces NAT capability.

#### NOTE

DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

#### NOTE

DHCP Server and NAT service configuration is supported using AP and web user interface. Refer to Administrator Guide for configuring DHCP server and NAT service on the web interface.

### **DHCP** Server

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D/SZ100-D/SZ144-D provides high scale IP assignment and management with minimal impact on forwarding latency. DHCP Server supports 63 pools with profile support.

#### NOTE

The DHCP service can scale for a maximum of 101K IP leases per data plane. You can incrementally add-on license on a per-group basis of two DPs.

### **NAT Service**

With NAT service enabled, all the WiFi client traffic is NATed by vSZ-D/SZ100-D/SZ144-D before being forwarded to the core network. Each vSZ-D/ SZ100-D/SZ144-D supports up to 16 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

### NOTE

Only single subnet is supported.

### NOTE

The NAT service scales a maximum of 2 million sessions/ flows per Data Plane. You can incrementally add-on license on a per-Data Plane basis.

# **DHCP/NAT**

DHCP/NAT functionality on SZ-managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server/NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery you can choose appropriate user profile for DHCP and NAT services on vSZ-D/SZ100-D/SZ144-D.

## **AP-based DHCP/NAT**

In highly distributed environments, particularly those with only a few APs per site, the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

Three general DHCP scenarios are supported:

- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients via NAT.
- Enterprise (>12): For Enterprise sites, an additional on site vSZ-D/SZ100-D/SZ144-D will be deployed at the remote site which will assume the responsibilities of performing DHCP/NAT functions. Therefore, DHCP/NAT service will not be running on any APs (they will serve clients only), while the DHCP/NAT services are provided by the onsite vSZ-D/SZ100-D/SZ144-D.

## **Profile-based DHCP**

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D/SZ100-D/SZ144-D provides high scale IP assignment and management with minimal impact on forwarding latency. DHCP Server supports 440K IP addresses and 64 pools with profile support.

### NOTE

DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

## **Profile-based NAT**

With NAT service enabled, all the WiFi client traffic is NATed by the vSZ-D/SZ100-D/SZ144-D before being forwarded to the core network. Each vSZ-D/SZ100-D/SZ144-D supports up to 990K ports and 16 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

# **Configuring License Bandwidth**

You can assign a license bandwidth for a data plane provided it is already approved. Each data plane can be configured with only one bandwidth license. Only vSZ-D support License Bandwidth.

1. Go to Administration > Administration > Licenses.

2. Select the License Bandwidth Configuration tab.

The License Bandwidth Configuration page appears.

FIGURE 6 License Bandwidth Configuration

Installed Licenses	License Servers	DP Bandwidth License Configuration	DP DHCP/NAT Licenses Assignment	URL Filtering License	s
* DP		* Bandwidth			
		No data available		✓ Cancel     ✓	
DP 🔺			DP Type	Bandwidth	
ANI-vDP-Upgrad	e		External-Virtual	1Gbps	
anu-127			External-Virtual	1Gbps	
					2 records « 1 »
V OK X Car	ncel				

- 3. Select a DP from the Data Plane table, the **DP** name is automatically displayed.
- 4. From the **Bandwidth** drop-down menu, select one of the following bandwidth license:
  - 1Gbps (default)
  - 10Gbps for customers using 10G NIC card
  - Unlimited for customers using 40G NIC card.
- 5. Click **OK**. The data plane with the assigned license bandwidth is displayed.
- 6. Click OK.

The message Submitting form appears, and the data plane is assigned a bandwidth.

You have successfully assigned a license bandwidth to the data plane.

# **Configuring the DHCP/NAT License Assignment**

## **Creating DHCP License Assignment**

Licensing needs to be created on a per SZ Controller Cluster basis. The default license, **CAPACITY-DP-SVDS-DEFAULT**, supports 1K DHCP address leases.

To create the DHCP License assignment:

- 1. Go to Administration > Administration > Licenses.
- 2. Select the DP DHCP/NAT Licenses Assignment tab.

DHCP Server and NAT Service on vSZ-D/SZ100-D/SZ144-D

3. From the DHCP License area, click Create. The DHCP License form appears.

FIGURE 7 DHCP License Assignment

# **DHCP** License

License Usage:	Total: 1 / Consumed: 0 / Available: 1	
* Primary Data Plane:	DP-THO-vdp-UPGRADE	•
Secondary Data Plane:	DP-THO-vdp-UPGRADE-2	*
* [?] License Count:	1 x 1000 IP Leases	
IP Leases:	1000	
Description:		

- License Usage: Lists the details of license consumption and availability.
- **Primary Data Plane**: Select the primary data plane from the drop-down. To remove the Data Plane from the DHCP license assignment, select **Clear**.
- Secondary Data Plane: Select the secondary data plane from the drop-down. To remove the Data Plane from the DHCP license assignment, select Clear.

OK

Cancel

- License Count: Enter the number of license. Range: 1 through 101.
- IP Leases: Lists the number of IPs assigned.
- Description: Enter a short description about the license assignment.
- 4. Click OK.

You have created the DHCP license assignment.

### NOTE

To edit or remove the license assignment on the data plane, select the assignment from the list and click Configure or Delete respectively.

## **Creating NAT License Assignment**

Licensing needs to be created on a per SZ Controller Cluster basis. The default license, CAPACITY-DP-SNAT-DEFAULT, supports 100K NAT sessions.

To create the NAT License assignment:

1. Go to Administration > Administration > Licenses.

x

- -

- 2. Select the DP DHCP/NAT Licenses Assignment tab.
- 3. From the NAT License area, click Create. The NAT License form appears.

FIGURE 8 NAT License Assignment

NAT License			2	×
License Usage:	Total: 1 / Consumed: 0 / Ava	ailable: 1		
* Data Plane:	DP-THO-vdp-UPGRADE		<b>•</b>	
* [?] License Count:	1	x 100000 Sessions/Fl	ows	
NAT Sessions/Flows:	100000			
Description:				
		OK	Cancel	

- License Usage: Lists the details of license consumption and availability.
- Data Plane: Select the data plane from the drop-down. To remove the Data Plane from the NAT license assignment, select Clear.
- License Count: Enter the number of license for the data plane. Range: 1 through 20.
- NAT Sessions/Flows: Lists the number of NAT sessions/flows.
- Description: Enter a short description about the license assignment.
- 4. Click OK.

You have created the NAT license assignment.

#### NOTE

To edit or remove the license assignment on the data plane, select the assignment from the list and click Configure or Delete respectively.

# L3 Roaming

RUCKUS vSZ and vSZ-D/SZ100-D/SZ144-D architecture now supports L3 Roaming without the need for additional mobility controllers.

The key use cases for L3 Roaming are well-understood,. Typically, a large WLAN network where APs are separated on different VLAN segments and there is a need for IP address preservation and potentially session persistence. Most common deployments are large campus networks designed with multiple switches and VLANs and there is a need to support L3 Roaming.

### Features and Benefits L3 Roaming

On vSZ-D/SZ100-D/SZ144-D, RUCKUS Wi-Fi can now support L3 Roaming with IP Address preservation. Below is the high level use case that describes the feature functions. A large network that is broken up into various campuses and there is a need to support L3 Roaming. Below figure depicts 2 campuses, which are L2 separated but need L3 Roaming.

The APs in campus A setup a tunneled WLAN to the vSZ-D (Using DP Group) and APs in building B setup a tunneled WLAN to the vSZ-D in their building.

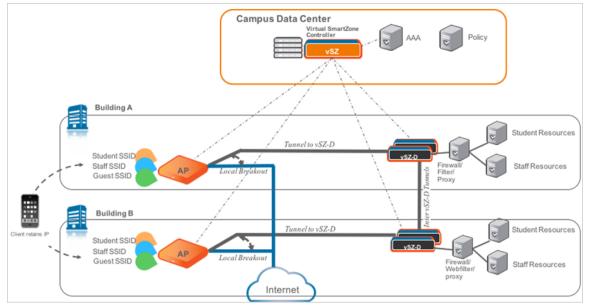
Each vSZ-D/SZ100-D/SZ144-D in the building can be configured to run a DHCP Server and NAT the traffic or be setup as a DHCP Relay. When a client roams from an AP in building A to an AP in building B, the vSZ-D/SZ100-D/SZ144-D in building B detects the roaming event and forwards the traffic (or assigns the same IP back to the client) to the vSZ-D in building A (home vSZ-D/SZ100-D/SZ144-D or anchor vSZ-D/SZ100-D/SZ144-D) to ensure that service to the client is not interrupted.

One additional unique benefit of this architecture over other L3 Roaming solutions is that with this architecture, the roamer client can still have access to his home network resources (this is similar to mobile roaming on 3G/4G networks).

### NOTE

Traffic between inter vSZ-D/SZ100-D/SZ144-D tunnels in Figure 9 can be encrypted by enabling tunnel encryption. Refer to Enabling Tunnel Encryption on page 25 for more information.

### FIGURE 9 Usage of L3 roaming



# Editing L3 Roaming for a vSZ-D/SZ100-D/SZ144-D

For L3 roaming to work without session break, the data planes between which the roaming happens must both be enabled with the L3 Roaming feature.

### NOTE

If the IP address of the UE changes, then the session breaks.

1. Go to Network > Data and Control Plane.

### 2. Select L3 Roaming.

The Enabling L3 Roaming page is displayed.

FIGURE 10 Enabling L3 Roaming

🖀 🛃 Monitor 🏭 Network	Security	🗱 Services	Administration	*	search menu	× Q	
DP Group Flexi-VPN L3 Roaming		Edit L3 Roa	ming				
L3 Roaming 🔞		DP:	ANI-vDP-Upgrade@A0:36	:9F:F4:1B:52			
		Version:	6.1.0.0.875				
Configure Cleared by Selected		* Activate:	Disable	~			
DP 🔺	Version	* Roaming Criteria:	UE Subnet	$\sim$			
		+ Create Delete					
anu-127@A0:36:9F:F4:1B:50							
⑦ Refresh ♥ OK ♥ Cancel		UE Subnet		ок	Ca	ncel	

3. Click **Configure** to edit the L3 roaming settings.

The Edit L3 Roaming page is displayed.

- 4. From Activate, you can enable the feature for the DP by selecting Enable or Disable from the drop-down menu.
- 5. From the **Roaming Criteria** list, select one of the following options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
- 6. Click OK.

You have successfully enabled L3 roaming, and also set the roaming criteria based on which DPs would connect within the network.

You have enabled L3 roaming in the selected vSZ-D/SZ100-D/SZ144-D.

# Lawful Intercept

An important carrier class feature that is being introduced on the vSZ-D/SZ100-D/SZ144-D is to support Lawful Intercept requirements.

These are slowly becoming mandatory and stringent on SP-WiFi deployments where Service Providers need to meet the CALEA standard requirements.

RUCKUS vSZ-D/SZ100-D/SZ144-D now supports the ability to identify a device that has a LI warrant issued against it and mirror the client data traffic to a LIG (Lawful Intercept Gateway) that is hosted in the SP's data center over L2oGRE.

The figure below illustrates the high level architecture that is supported for Lawful Intercept capabilities. It aslo depicts an architecture where smaller sites (with lesser number of APs) that do not need data tunneling to vSZ-D/SZ100-D/SZ144-D (depicted as Multi-AP and Single AP sites) but need Lawful Intercept. On the other side is a large enterprise site with large number of APs and need tunneling (depicted as Enterprise site with vSZ-D/SZ100-D/SZ144-D on premise) with Lawful intercept.

### NOTE

As mentioned in this document, the flexibility of the RUCKUS vSZ/vSZ-D architecture is that WiFi service providers can deploy the vSZ-D/ SZ100-D/SZ144-D only on premises where there is a need (typically larger venues) for tunneling. The RUCKUS architecture simply involves spinning up a vSZ-D/SZ100-D/SZ144-D instance at the central data center and designate that vSZ-D/SZ100-D/SZ144-D instance as a CALEA mirroring agent. All of this configuration is centrally managed through the vSZ. Once the network is setup appropriately, when a client device with a matching MAC address that has a warrant is detected on any of the access sites, the APs (or the vSZ-D/SZ100-D/SZ144-D) will mirror the packets to the vSZ-D (CALEA Mirroring agent) in the DC which will then forward the traffic to the LIG (Lawful Intercept Gateway) either in the DC or SP DC.

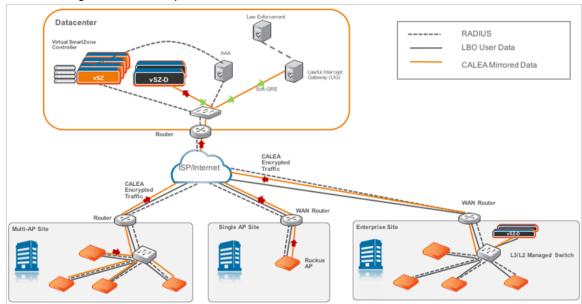


FIGURE 11 Usage of Lawful Intercept

# **Enabling Flexi VPN**

You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

1. Select Network > Data and Control Plane.

### 2. Select Flexi-VPN.

The Flexi-VPN status page is displayed.

### FIGURE 12 Enabling Flexi-VPN

*	Monitor	🏦 Network	Security	C Services	Administration	*	search menu V C	۲. Netw	rork > Data and Control Plane	> Flexi-VPN
DP Group	Flexi-VPN	L3 Roaming								
Flexi-V	PN 🕐									
										C 🕈
WLAN			Zone		DP Group (Source)		Flexi-VPN Profile (Destination	n)		
									No data «	1 »

### NOTE

The Flexi-VPN option is available only if the Access-VLAN ID is configured in manual mode, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options, and Tunnel NAT are disabled.

### NOTE

Flexi-VPN is activated when a Flexi-VPN profile is assigned to a WLAN.

### NOTE

A maximum of 1024 WLAN IDs can be applied to a Flexi-VPN profile. Flexi-VPN supports IPv4 addressing formats and RUCKUS GRE tunnel protocol. It does not support IPv6 addressing formats.

The following record table indicates that the Flexi-VPN profile is successfully applied to the WLAN:

- WLAN: displays the name of the WLAN
- Zone: displays the name of the zone
- DP Group: displays the name of the source data plane from which tunneled traffic starts
- Flexi-VPN Profile: displays the name of the destination data plane to where the tunneled traffic terminates

# **Enabling Tunnel Encryption**

You can use the tunnel encryption feature to encrypt data for a private network, through a public network. This feature is available in vSZ-H and vSZ-E.

1. Go to Services > Tunnels and Ports.

2. Select the Tunnel Encryption(DP) tab.

The Tunnel Encryption (DP) page appears.

FIGURE 13 Tunnel Encryption (DP)

<b>#</b>	Monitor	🚠 Net	twork 🏾 🛡	Security	Ø\$ Se	rvices	💄 Admini	stration 🔺	search menu	~ <b>Q</b>	Services > Tunnels&Ports > Tunnel Encryption(DP)
Ruckus GF	RE SoftGRE	IPsec	Ethernet Port	DiffServ	CALEA	Tunnel En	cryption(DP)	Multicast Forwarding	Split Tunnel	Bond Port	
OFF	Enable Tunnel Encry	ption									
C Refr	resh 🗸 OK	X Cancel									

- 3. Select the Enable Tunnel Encryption check-box.
- 4. Click OK.

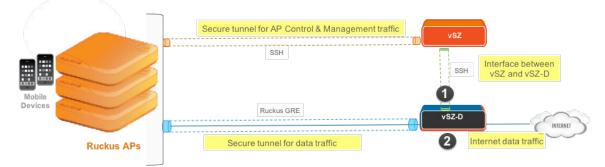
You have successfully enabled tunnel encryption.

# **Network Architecture**

vSZ-D/SZ100-D/SZ144-D requires at least two physical interfaces: one for control/management and another for data plane.

The control/management interface is used for communication with the vSZ controller, as well as the command line interface. The data plane interface is used to tunnel user data traffic from the APs.

## FIGURE 14 vSZ-D logical interfaces



The access layer (southbound) is used to tunnel traffic to and from managed APs. The following connections exist on the access layer.

- 1. AP to and from vSZ-D/SZ100-D/SZ144-D: Data plane, secured by RUCKUS GRE tunnel.
- 2. vSZ to and from vSZ-D/SZ100-D/SZ144-D: Control plane, for vSZ to manage vSZ-D/SZ100-D/SZ144-D
- 3. AP to and from vSZ: Control plane, for vSZ to manage the AP

The core layer (northbound) is used by vSZ-D/SZ100-D/SZ144-D to forward traffic to and from the core network.

# **Communication Workflow**

The figure below captures a high level end-to-end communication flow between RUCKUS APs, vSZ and vSZ-D/SZ100-D/SZ144-D.

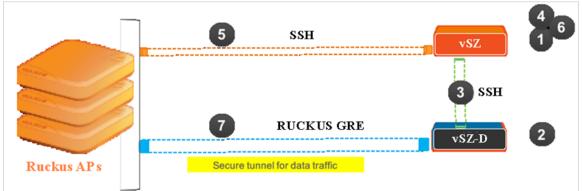


FIGURE 15 Communication workflow between RUCKUS APs, vSZ, and vSZ-D/SZ100-D/SZ144-D

The following are the steps seen in the above figure.

1. Update the vSZ controller to the latest release or perform a fresh install of the vSZ controller with the latest release

### NOTE

If you are upgrading the vSZ controller and the vSZ-D/SZ100-D/SZ144-D, RUCKUS recommends the update of vSZ controller before the update of vSZ-D/SZ100-D/SZ144-D

- 2. Install vSZ-D/SZ100-D/SZ144-D and point it to the vSZ-E or vSZ-H controller by using the following options:
  - Set vSZ-E or vSZ-H control interface IP address or FQDN or configure the controller IP address via DHCP option 43.
  - For vSZ-E or vSZ-H configured with three (3) IP interfaces, the IP address to use is the vSZ control interface IP address.
- 3. The vSZ-D/SZ100-D/SZ144-D management interface connects with the vSZ-E or vSZ-H controller control interface
- 4. The vSZ-E or vSZ-H controller administrator approves the vSZ-D/SZ100-D/SZ144-D connection request
- 5. The vSZ informs the AP of the vSZ-D/SZ100-D/SZ144-D data interface
- 6. The vSZ-D/SZ100-D/SZ144-D is displayed as active and managed on vSZ-E or vSZ-H
- 7. AP establishes a RUCKUS GRE tunnel with the vSZ-D/SZ100-D/SZ144-D data interface when a tunnelling WLAN is configured

Figure 15 depicts logical network architecture. In real-world deployments, there may be network routers, gateways, firewalls and other devices; these typical network devices are not shown in the figure to focus on the vSZ-D/SZ100-D/SZ144-D interfaces and communication protocol aspects between the various entities.

It is also important to note that support for distributed or centralized deployment topologies introduce NAT routers/gateway devices. The communication interfaces between RUCKUS APs, vSZ and vSZ-D/SZ100-D/SZ144-D are designed to support NAT traversal so as to support such NAT Deployment Topologies on page 31.

# **NAT Deployment Topologies**

vSZ-D/SZ100-D/SZ144-D supports several deployment topologies.

# AP Behind NAT and vSZ-D/SZ100-D/SZ144-D Behind NAT

When an AP is behind NAT, it is assumed that AP is sitting in the private world and wants to talk to vSZ-D/SZ100-D/SZ144-D in the public world through NAT. The AP obtains its private IP address and communicate with the vSZ-D/SZ100-D/SZ144-D through NAT. During communication with vSZ-D/SZ100-D/SZ144-D, the NAT router will intercept the packet and change the source IP address (which is the AP IP address) to a public IP address and add a new source port number before forwarding the packet to vSZ-D/SZ100-D/SZ144-D. vSZ-D/SZ100-D/SZ144-D, in this case, is insensitive to the NAT router's operation. When the packet comes back from vSZ-D/SZ100-D/SZ144-D to the AP, the NAT router will intercept the packet and translate the destination IP address and port number back to the appropriate (original) AP IP address and port number.

When vSZ-D/SZ100-D/SZ144-D is behind NAT, it is assumed that vSZ-D/SZ100-D/SZ144-D is sitting in the private world and wants to talk to the AP in the public world through NAT. In this case, it is needed to setup the NAT IP (public IP) and a port number pair in vSZ-D/SZ100-D/SZ144-D "setup" process. vSZ picks up this public address and the associated port number and informs the AP that this is the vSZ-D/SZ100-D/SZ144-D address/port (public-IP, port) pair to connect to.

It is also needed to configure the NAT device and enter the port mapping, basically, (public-IP, port) <-> (private-IP, 23233) into NAT's rule table. Thus, when NAT receives the packet bound for vSZ-D/SZ100-D/SZ144-D (sent to public-IP/port) from the AP, it will translate it to (private-IP, 23233) based on the rule table before sending it to vSZ-D/SZ100-D/SZ144-D, and conversely, for packet from vSZ-D/SZ100-D/SZ144-D, NAT router will look at the srcIP/srcPort (IP, 23233), and convert it to public IP address or port based on the rule table before sending it to AP.

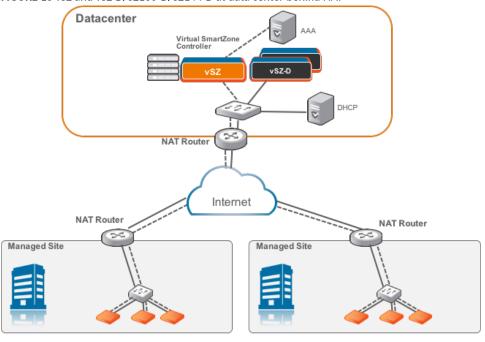
### NOTE

Both TCP and UDP protocols on port 23233 need to be forwarded as both are used (TCP is used for tunnel establishment and UDP for client data)

# vSZ and vSZ-D/SZ100-D/SZ144-D at Data Center Behind NAT

In this deployment topology, vSZ-D/SZ100-D/SZ144-D and vSZ are co-located at the data center behind NAT, while Ruckus APs are on the access network behind NAT.

vSZ-D/SZ100-D/SZ144-D at Access Site with NAT

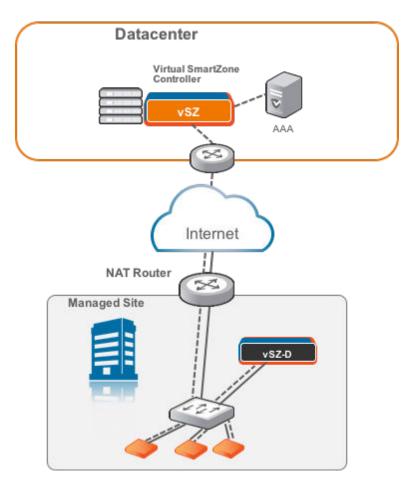


### FIGURE 16 vSZ and vSZ-D/SZ100-D/SZ144-D at data center behind NAT

# vSZ-D/SZ100-D/SZ144-D at Access Site with NAT

In this deployment topology, vSZ is at the data center and vSZ-D/SZ100-D/SZ144-D is co-located with the Ruckus APs on the access network. In this scenario, there are NAT routers between vSZ and vSZ-D/SZ100-D/SZ144-D/Ruckus APs.

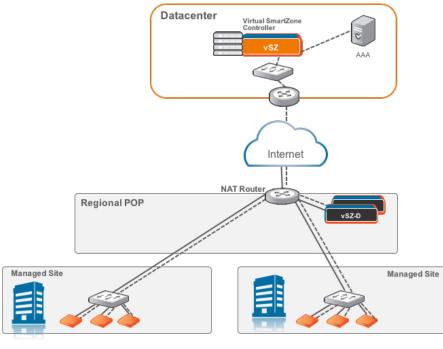
FIGURE 17 vSZ-D/SZ100-D/SZ144-D at access site with a NAT router



# vSZ-D/SZ100-D/SZ144-D Behind NAT

In this deployment topology, vSZ is at the data center and vSZ-D/SZ100-D/SZ144-D is in a distributed site but not co-located with the Ruckus APs within the access network. There are NAT routers between vSZ and vSZ-D/SZ100-D/SZ144-D, and between vSZ-D/SZ100-D/SZ144-D and Ruckus APs. The vSZ-D/SZ100-D/SZ144-D port to communicate with vSZ control plane is port 22.

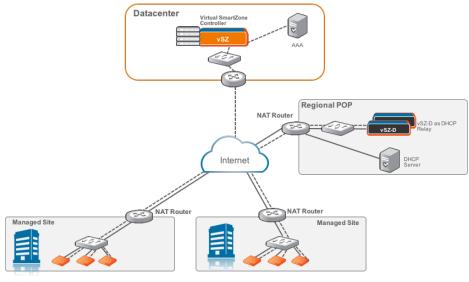
### FIGURE 18 vSZ-D/SZ100-D/SZ144-D behind a NAT router



# **DHCP Relay with NAT**

Similar to the vSZ-D/SZ100-D/SZ144-D Behind NAT, in this deployment topology, vSZ is at the data center and vSZ-D/SZ100-D/SZ144-D is in a distributed site but not co-located with the Ruckus APs within the access network. There are NAT routers between vSZ and vSZ-D/SZ100-D/SZ144-D, and between vSZ-D/SZ100-D/SZ144-D and Ruckus APs. However, in this topology, the DHCP server assigning client IP addresses is on its own separate subnet. vSZ-D/SZ100-D/SZ144-D provides the DHCP relay function to support such a network configuration.

#### FIGURE 19 DHCP relay with a NAT router



# **DHCP Option 82 and Bridge Profile**

If you are enabling the DHCP Option 82 in WLAN configuration in the controller vSZ, it means that the AP is going to put DHCP Option 82 in the DHCP server and will send it to vSZ-D/SZ100-D/SZ144-D. This is in the format IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC. If you want to give the users the option to choose what needs to be included in DHCP Option 82, you would need to create a *Bridge Service Profile* in the vSZ controller web interface. Follow the steps to create a *Bridge Service Profile*.

- Go to vSZ controller web interface > Services > Tunnels & Ports > Core Network Tunnel > Bridge.
- Click on Create.
- Enter the bridge forwarding profile information
  - In the **Name** field, type a name for the bridge forwarding profile.
  - In the **Description** field, type a short description for the profile.
  - Ensure the Enabled DHCP Relay option is selected.
  - Enter the DHCP server IP addresses. Select the Send DHCP requests to both servers simultaneously option, if you want to send the request to both the servers.
  - Enable **DHCP Option 82** and choose the sub options based on your requirement or of the user. This will be taken care by vSZ-D/ SZ100-D/SZ144-D during DHCP packet relay to the DHCP server.

FIGURE 20 Creating Bridge Profile

# Create Bridge Forwarding Profile

* Name:			
Description:			
DHCP Relay			▼
Enabled DHCP Relay	,		
* DHCP Server 1:			
DHCP Server 2:	198.10.10.5	ON O Send DHCP requests to both servers simultaneously	
DHCP Option 82:			
	ON OSubopt-1 with format	IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC	$\sim$
	ON O Subopt-2 with format	Client-MAC-hex 🗸	
	ON O Subopt-150 with VLAN	-ID	
	Subopt-151 with forma	at Area-Name 🗸	

OK Cancel

- Go to vSZ controller web interface > Network > Wireless > Wireless LANs.
- Click on **Create** to add the following new WLAN configuration:
  - Access Network as Tunnel WLAN traffic through Ruckus GRE
  - Core Network as Bridge
  - Authentication Options > Methodas Open
  - Encryption Options > Methodas None
  - Forwarding Policy as Factory Default . Choose the forwarding policy as the bridge profile.
- Click **OK** to complete and save the configuration.

#### FIGURE 21 Creating a WLAN Configuration

Conoral Options		
General Options		Ψ.
* Name		
* SSID		
Description	c	
* Zone	: Z dpsktest V	
* WLAN Group	No data available	
WLAN Usage		v
	Z Tunnel WLAN traffic through Ruckus GRE	
	Bridge C L2oGRE	
* Authentication Type	:      O Standard usage (For most regular	
	Hotspot 2.0 Access Hotspot 2.0 Secure WeChat Onboarding (OSEN)	
Authentication Optio	ns	
* Method	:      Open O 802.1x EAP MAC Address	
Encryption Options		Ψ.
* Method	: _ WPA2 _ WPA-Mixed _ WEP-64 (40 bits) _ WEP-128 (104 bits)	
Accounting Service		
Accounting Serv	vice: Use the controller as proxy Disable   Create	
Forwarding Profile		Ŧ
* Forwarding Policy	Factory Default	

# **Configuring the vSZ Controller to Prepare for Network Segmentation**

•	Configuring the DHCP/NAT License Assignment	39
•	Creating Profile-based DHCP	39
	Configuring Global Settings	
	Configuring DHCP Pool Settings	
	Creating Profile-based NAT	
	Configuring NAT Global Settings	
	Configuring NAT Pool Setting	
	Creating an AP Group	
	Creating WLAN for Network Segmentation	
	creating white intervent segmentation	

### **Configuring the DHCP/NAT License Assignment**

License assignment specifies the capability of each Data Plane, which has the ability to assign IPs by DHCP feature and translate packets by NAT feature. Though these features already exist, starting 5.0, customers must purchase license to enable these features.

#### NOTE

This feature is supported only on virtual platform.

## **Creating Profile-based DHCP**

DHCP profile can be applied to vSZ-D and the vSZ-D server can assign IP to the UE based on the profile rule. Different pools with the same subnet can be created without overlapping IP range.

#### NOTE

DHCP supports only access-side network.

- Configuring Global Settings on page 39
- Configuring DHCP Pool Settings on page 40

# **Configuring Global Settings**

To configure Profile-based DHCP Global settings:

- 1. Go to Services > DHCP & NAT > DHCP Profiles (DP).
- 2. Click Create, the Create DHCP Profile page appears.

- 3. Configure the following:
  - **Profile Name**: Type a name for the DHCP profile you want to create. AP supports 32 bytes.
  - **Description**: Type a description of the settings you want to create.
  - **Domain Name**: Type the domain name address.
  - **Primary DNS Server**: Type the primary domain name server address.
  - Secondary DNS Server: Type the secondary domain name server address.
  - Lease Time: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
  - DHCP Option43 Space: Click Create, the Create DHCP Option43 Space form appears. Configure the following:
    - **Space Name**: Type a name for Option43 space.
    - **Description**: Type a description for Option43 space.
    - Under Option43 Sub Option, click Create and configure the following:
      - Sub Option Name: Type a sub option name.
      - > **Type**: Select the required option from the drop-down.
      - > Code: Enter a code. Range: 1 through 254.
      - > ClickOK, you have created Option43 Sub Option.
    - Click **OK**, you have created Option43 Space.
  - Hosts: Click Create, the Create Host Configuration form appears. Configure the following:
    - General Options
      - **Host**: Type a name for the host settings that you want to create.
      - > Description: Type a description for the host settings that you want to create.
    - Policy Options
      - > Mac Address: Type the MAC address of the DHCP host.
    - Assigning Options
      - > Broadcast Address: Type the broadcast IP address.
      - > Fixed Address: Type the fixed IP address of the host.
      - > Gateway: Type the gateway IP address.
      - > DNS Server: Type the IP address of the DNS server.
      - Domain Name: Type the domain name.
      - Host Name: Type the host name.
      - > Lease Time: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
  - Click **OK**, you have created DHCP Host configuration.
- 4. Click OK.

You have created DHCP Profile settings.

# **Configuring DHCP Pool Settings**

To configure DHCP pool settings:

- 1. Go to Services > DHCP & NAT > DHCP Profiles (DP).
- 2. Select the DHCP profile from the list for which you want to configure the pool settings.
- 3. Select the **Pools** tab page.

- 4. Click Create and configure the following:
  - General Options
    - **Pool Name**: Type a name for the pool configuration.
    - **Description**: Type a description for the pool configuration.
  - Policy Options
    - Policy type: Select VNI type for Network Segmentation.
  - Assigning Options
    - Subnet: Type the IP address.
    - Subnet Mask: Type the network address.
    - Broadcast Address: Type the broadcast IP address.
    - **Pool Range**: Type the address range for the pool.
    - **Exclude Pool**: Type the address range that must be excluded.
    - Primary Gateway: Type the primary gateway IP address.
    - Secondary Gateway: Type the secondary gateway IP address.
    - Primary DNS Server: Type the IP address of the primary DNS server.
    - Secondary DNS Server: Type the IP address of the secondary DNS server.
    - Domain Name: Type the domain name.
    - Host Name: Type the host name.
    - Lease Time: Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
  - Option43 Value
    - Click Create, the Create Option43 value form appears. Configure the following:
      - > Choose the Space Name or click Create to configure Option 43 Space Name.
      - > Enter a **Description**.
    - Click **OK**, you have configured Option43 value.
- 5. Click OK.

You have created DHCP pool configuration.

# **Creating Profile-based NAT**

A NAT Profile could be applied to a vSZ-D. The NAT server settings work independently. You must configure the following settings to create a NAT profile:

#### NOTE

NAT does not support multiple public subnet/VLAN.

- Configuring NAT Global Settings on page 41
- Configuring NAT Pool Setting on page 42

# **Configuring NAT Global Settings**

To create a NAT global setting:

- 1. Go to Services > DHCP & NAT > NAT Profiles (DP).
- 2. Click **Create**, the Create NAT Profile page appears.

- 3. Configure the following:
  - Profile Name: Type a name for the NAT profile that you want to create. AP supports 32 bytes.
  - **Description**: Type a description for the profile that you want to create.
  - Subnet: Type the IP address.
  - Policy type : Select VNI type for Network Segmentation.
  - **Prefix**: Type a prefix value. Maximum range: 31.
  - **Gateway**: Type the gateway IP address.
- 4. Click OK.

You have created a NAT Profile.

# **Configuring NAT Pool Setting**

To configure NAT pool settings

- 1. Go to Services > DHCP & NAT > NAT Profiles (DP).
- 2. Select the NAT profile from the list and click the **Pools** tab.
- 3. Click Create, the Create Pool Configuration page appears.
- 4. Configure the following:
  - General Options
    - **Pool Name**: Type a name for the NAT pool settings that you want to create.
    - **Description**: Type a description for the pool settings that you want to create.
  - Policy Options:
    - Policy Type: Select VNI type for Network Segmentation.
  - Translation Options
    - Port Range: Type the port range. Range: 10000 through 65534. For example: 10000-20000.
    - Public Address Range: Type the public address range.

Note: This public address must not be duplicated with the other public address in the same subnet, which includes applied NAT Profile and vSZ-D's Access and Core Interface Address.

5. Click OK.

You have created a NAT pool setting.

## **Creating an AP Group**

Creating an AP group means creating a configuration profile that defines channels, radio settings, ethernet ports and network segmentation groups and other configurable for all members of the group or for all APs of a specific model in the group.

Follow these steps to create an AP group.

- 1. On the main menu, click Network > Access Point
  - The Access Point page is displayed.

*	🛃 Monitor 🛛 🎄 Netwo	ork 🛡 Security	🕫 Services	👗 Adm	inistration	★ s	earch menu	~ <b>Q</b>	Network >	Wireless > .	Access Points
	Access Points 1000	1000 0 0		VIEW	MODE: List	Group Mesh	Map Zone				Â
	+ 🖊 🗋 🗙 More 🗸 😂 🛠	Configure Move De	lete More V						search table	Q	C 7 ¢
_	- D System	MAC Address 🔺	AP Name	Status	Alarm	IP Address	Total Traffic (1hr)	Clients	Latency (2.4G)	Latency (5G)	Latency (6)
ORGANIZATION	= D Christopher	00:35:35:00:1F:FE	Sim-61	Online	0	35.35.1.62	N/A	0	0	0	0
ANIZ	+ Z MDU1-Demo	00:35:35:00:20:84	Sim-62	Online	0	35.35.1.63	N/A	0	0	0	0
ORG	+ Z MDU2-Demo	00:35:35:00:21:0A	Sim-63	Online	0	35.35.1.64	N/A	0	0	0	0
	+ D Commscope + D Jeff	00:35:35:00:21:90	Sim-64	Online	0	35.35.1.65	N/A	0	0	0	0
	+ D Nipun	00:35:35:00:22:16	Sim-65	Online	0	35.35.1.66	N/A	0	0	0	0
	– D Sushma	00:35:35:00:22:9C	Sim-66	Online	0	35.35.1.67	N/A	0	0	0	0
	+ Z Sushma-MDU	00:35:35:00:23:22	Sim-67	Online	0	35.35.1.68	N/A	0	0	0	0
	+ Z RuckusWireless + Z Staging Zone	00:35:35:00:23:A8	Sim-68	Online	0	35.35.1.69	N/A	0	0	0	0
	0000000 20110	00:35:35:00:24:2E	Sim-69	Online	0	35.35.1.70	N/A	0	0	0	0
		00:35:35:00:24:B4	Sim-70	Online	0	35.35.1.71	N/A	0	0	0	0
									-		•

#### FIGURE 22 Access Point

From the System tree hierarchy, select the location (for example: System, Domain, Zone) and click 主. The following figure appears. 2.

Croate Group		
Create Group		2
* Name: Description: Type: Ozone (in) AP Group		
Parent Group: zone1		
Configuration General Options	~	^
Location: Override (example: Starbucks)		Ŀ.
Location Additional CA IICA)		1
ок	Cancel	

Enter the details as explained in the following table. 3.

#### NOTE

You can also edit the configuration of default AP group by selecting the default group and clicking the 💌 icon.

- 4. Click OK.
- Select the AP's that will be used in the Network Segmentation and move them into the created AP Group(s). 5.

#### NOTE

You can also edit, clone or delete an AP Group by selecting the options Configure  $\mathbb{Z}$ , Clone  $\mathbb{Z}$  or Delete  $\mathbb{Z}$  respectively, from the Access Points page.

## **Creating WLAN for Network Segmentation**

- Go to the Network> Wireless Lans> System.
- Click Create .

General Options		▼
* Name:		
* SSID:		
Description:		
* WLAN Group:	default v	
Authentication Options		▼
Authentication Type:	Standard usage (For most regular wireless O Hotspot (WISPr) O Guest Access O Web Authentication networks)	
	O Hotspot 2.0 Access O Hotspot 2.0 Onboarding O WeChat	
Method:	Open      B02.1X EAP      MAC Address      B02.1X EAP & MAC	
Encryption Options		
Method:	WPA2 WPA3 WPA2/WPA3-Mixed OWE WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None	
	Encryption methods other than WPA3 and OWE will not be supported on Wi-Fi 6E devices.	
Data Plane Options		▼
[?] Access Netw	rork: OFF Tunnel WLAN traffic through Ruckus GRE	

**Create WLAN Configuration** 

- Enter the "Name" and SSID in general options.
- Select WPA2 in encryption options.
  - Select "External" in Dynamic DPSK.

Encryption Options		▼
Method:	WPA2 WPA3 WPA2/WPA3-Mixed OWE WPA-Mixed WEP-64 (40 bits) WEP-128 (104 bits) None	
	Encryption methods other than WPA3 and OWE will not be supported on Wi-Fi 6E devices.	
Algorithm:	● AES ○ AUTO○ AES-GCMP-256	
802.11w MFP:	Disabled      Capable      Required	
Dynamic PSK:	O Disable O Internal 🖲 External	

- In Data plane options, Enable "Access network".
- Enable NAT.
- Enable DHCP.
- Enter GRE tunnel profile with "Ruckus GRE".

a Plane Options	
[?] Access Network: ON O Tunnel WLAN traffic through Ruckus GRE	
* GRE Tunnel Profile: Default Tunnel Profile	
Current WLAN Tunnel selected type: Ruckus GRE	
[?] Flexi-VPN Profile: Disable	
Split Tunnel Profile: Disable 🗸 🕂	
RADIUS based DHCP/NAT: OFF NAT	
OFF DHCP	
RADIUS NAT/DHCP conflicts the option 82 of the core side, please choose one to use.	

• Enable Authentication Service .

ata Plane Options		V
[?] Access Network	ON O Tunnel WLAN traffic through Ruckus GRE	
GRE Tunnel Profile	Default Tunnel Profile V	
	Current WLAN Tunnel selected type: Ruckus GRE	
Core Network	Bridge      L20GRE	
[7] DP DHCP/NAT	ON ONAT	
	ON O DHCP	
Split Tunnel Profile	Disable 🗸 🕂 🖉	
RADIUS based DHCP/NAT	OFF NAT	
	OFF DHCP	
	RADIUS NAT/DHCP conflicts the option 82 of the core side, please choose one to use.	
uthentication & Accounting	Service	
• [?] Authentication Service	Use the controller as proxy	
Accounting Service:	OFF Use the controller as proxy	
	Disable 🗸 🕂 🖉	

#### NOTE

WLAN will not be displayed, if any of the above conditions are not met.

For Authentication and Accounting from SmartZone.

#### NOTE

Refer to RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide, 6.0.0 (Part Number: 800-72580-001 Rev A) and navigate to Services and Profiles > Working with Tunnels and Ports.

# **Creating Network Segmentation Profile on the vSZ Controller**

Network Segmentation was designed specifically to target Multi Dwelling Unit (MDU) deployments. Network Segmentation is currently using external Dynamic Pre shared Key (DPSK) to place a single tenant and their devices into their own individual VXLAN (iLAN).

Data Plane (DP) will play the role of Home DP or Partner DP. Each DP plays the home DP role and has its own VXLAN Network Identifier (VNI) range. Home DP facilitates MDU UE, connect with each other based on the same VNI number.

Steps for the creation of Segmentation:

- Go to Services> Hotspots & Portals > Network Segmentation> Network Segmentation Profiles
- Click Create.

FIGURE 24 Edit Network Segmentation Groups in SmartZone User Interface

#### **Create Network Segmentation**

General Options							
* Name: test							
Type: 🔘 Wired + W	ïreless 🔵 Wireless						
Data Plane							
+ Add Configure De	elete						
Data Plane 🔺	VNI Range	DHCP Profile	DHCP Pool	NAT Profile	NAT Pool		
						Start	Canc

- Enter a Network Segmentation Profile name in the Name field.
- Click "Add".

FIGURE 25 Create Data plane Relation

### Create Data Plane Relation

#### - [Data Plane] This field is required

* Data Plane:	vdp-1	· · · ·	,
VNI Range:	[1-16777215] ex.1, 2 or 1-2	2000	
* NAT Profile:			
* NAT Pool:			

- Select the Data Plane details
- Enter the VNI range; ensure your VNI range is large enough to accommodate all units in the property. Each unit gets its own unique VNI.
- Select/Create DHCP Profile and Pool.
- Select/Create NAT Profile and Pool.
- Click "OK".
- "Select AP Group(s) that will be used for Network Segmentation , refer to the figure below.

#### NOTE

This step is not applicable for Wireless group.

#### FIGURE 26 Add AP Group

#### **Create Network Segmentation**

All APs within the selected AP groups will be part of the network segmentation.

AP groups presented here are from the zones which Select Ethernet Profile: No data available		1		
Select AP Groups (Domain-Zone-AP Group)		Selected AP Groups (Domain-Zone-AP Group)		
Type a keyword to find a group	Q		Q	
- D System		Administration Domain-test-default		

- Create/Select an ethernet profile with enabled Network Segmentation and select AP Model's port to apply.
- Click "Next".
- Select the SSID (wireless) for Network Segmentation.

FIGURE 27 Select SSID(wireless) for Network Segmentation

#### **Create Network Segmentation**

Select one SSID to be used for the network segmentation.

WLANs	ction in this Network Segmentation.				
				search table	Q 2 0
Name 🔺	SSID	Zone Name	Domain Name		
test	test	test	Administration Dor	nain	
test2	test2	test	Administration Dor	nain	
test3	test3	test	Administration Dor	nain	

- Click "Next".
- Select WLANs (wireless) for Network Segmentation.

#### FIGURE 28 Select WLANs (wireless) for Network Segmentation

#### Create Network Segmentation

Select WLANs from different zones to be part of the network segmentation.

Select Wlans (Domain-Zone-WLAN-SSID)	0	Selected Wlans (Domain-Zone-WLAN-SSID)	c	
	•	Administration Domain-test-test		
		Q.		Administration Domain-test-test-test

- Select "Next".
- Review the details entered.

#### **Create Network Segmentation**

Review the configurations.

Start 🔶 AP Gro	up(wired) 🔶 Sele	ect SSID(wireless) →	Select WLANs(wire)	ess) → Review			
Name:	: test						
Type:	WIRED+WIRELESS						
Data Plane:	Data Plane 🔺	VNI Range	DHCP Profile	DHCP Pool	NAT Profile	NAT Pool	
	charley-MDU	5-50	test	test	test	test	
AP Groups:	AP Group		Zone Name		Domain Name		
	default		test		Administration D	omain	
Ethernet Profile:	: test						
Wlans:	WLAN	SSID		Zone Name	Don	nain Name	
	A	8 × +8		A = +A		estata a na serie a	
				I	Back	ок	Cance

- Click "OK".
- The Network Segmentation Profile is created.

# **Hardware Requirements**

•	Important Notes About Hardware Requirements	
•	Supported Modes of Operation	

vSZ-D supports auto scaling, which means the number of CPU cores can be expanded without needing a software update. Ruckus has tested from three to six CPU core allocations for the vSZ-D.

#### NOTE

The minimum memory and CPU requirements for vSZ have changed in this release. You may need to upgrade your infrastructure before upgrading. Please read carefully. This is the minimum requirement recommended. Refer to the Release Notes or the vSZ Getting Started Guide.

The following table lists the minimum hardware requirements recommended for running an instance of vSZ-D.

#### TABLE 4 vSZ-D hardware requirements

Hardware Component	Requirement	
Hypervisor support required by Management Interface	VMWare ESXi 6.7 and later OR KVM (CentOS 7.4 64bit)	
Processor	Intel Xeon E55xx and above. Recent Intel E5-2xxx chips are recommended	
CPU cores	<ul> <li>Minimum 3 to 6 cores per instance dedicated for data plane processing.</li> <li>DirectIO mode for best data plane performance.</li> <li>NOTE         Actual throughput numbers will vary depending on infrastructure and traffic type.     </li> <li>vSwitch mode for flexibility</li> </ul>	
Memory	Minimum 6 Gb memory per instance	
Disk space	10GB per instance	
Ethernet interfaces	2	
NICs that support Intel DPDK requiredby Data Interface	<ul> <li>Intel NICs igb, ixgbe, i40en</li> <li>I350</li> <li>82599, 82599EB, 82599ES, X520, X710, XL710</li> </ul>	

### **Important Notes About Hardware Requirements**

- If you change the number of CPU cores, you must reboot vSZ-D for the changes to take effect.
- The first core is always shared between Linux and NPE. Other cores are dedicated to NPE.
- vSZ-D requires two interfaces and these interfaces must be deployed on different subnets.
- The management interface of the vSZ-D can be any model as long as the NIC is supported by the hypervisor.
- The data interface needs to be Intel DPDK based.

# **Supported Modes of Operation**

vSZ-D supports two modes of operation: direct IO mode and vSwitch mode.

For best performance, Ruckus recommends using the direct IO mode. SR-IOV mode is unsupported. Refer to the table below for mode of operation

#### NOTE

NICs assigned to direct IO cannot be shared. Moreover, VMware features such as vMotion, DRS, and HA are unsupported.

The hardware configuration for a single vSZ-D instance specified in the guide will scale to handle 10K tunnels (10K APs) and up to 10Gbps of throughput (unencrypted) with appropriate underlying Intel NIC cards (10G interfaces) in directIO mode of operation. This aligns with the number of Ruckus AP that a vSZ controller supports. Refer to the dimensioning table below.

#### TABLE 5 Hardware Dimensioning

Number of vSZ Instances	Number of vSZ-D Instances	Number of Ruckus APs	Number of Tunnels on vSZ-D	Maximum Throughput (Unencrypted)	Notes
1	1	10000	10000	10 Gbps	It is recommended to have 10G NICS on the vSZ-D considering the high number of Ruckus APs.
1	2	10000	5000 (10K maximum in case of failover)	10 Gbps	Tunnels are load- balanced towards the vSZ-D by the vSZ. This is useful when data plane redundancy is required. It is recommended to have 10G NICS on the vSZ-D considering the high number of Ruckus APs.
2	2	10000	5000 (10K maximum)	10 Gbps	Tunnels are load- balanced towards the vSZ-D by the vSZ. Each vSZ-Dmim tunnels.
2	4	10000	2500 (10K maximum)	10 Gbps	Tunnels are load- balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
3	6	20000	3300 (10K maximum)	10 Gbps	Tunnels are load- balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
4	8	30000	3750 (10K maximum)	10 Gbps	Tunnels are load- balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.

#### TABLE 6 Mode of Operation

Hypervisor	Number of CPUs	Memory (GB)	Hard Disk (GB)	Number of Tunnels	Tunnel Bandwidth (Intel NIC-10 G) (Unencrypted)	Packet Size (Bytes)
Vmware (DirectIO)	3	6	10	1000	17.6 Gbps	1400
Vmware (DirectIO)	6*	6	10	10000	6.3 Gbps	Random
Vmware (DirectIO)	3	6	10	10000	4.5 Gbps	Random

#### NOTE

Refer to the Data Plane Performance Recommendations on page 117 chapter for encryption and vSwitch impacts.

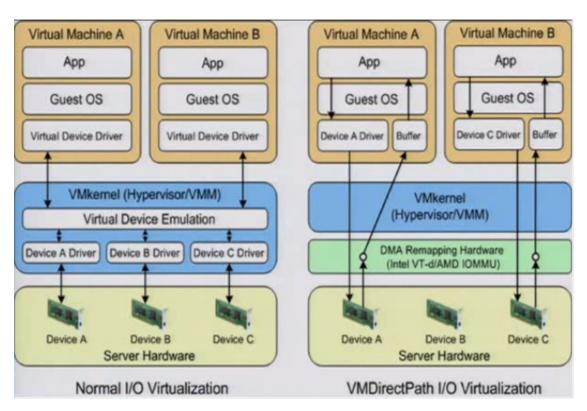
#### NOTE

\* vSZ-D needs to increase the CPUs to 6 for sustaining the 10GB line rate in random-byte traffic when the encryption is enabled. Encrypted requires 6 cores and unencrypted requires 3 cores

**Direct IO Mode** 

# Network Mode

vSwitch Mode



The figure below depicts a sample configuration in DirectIO mode. This is the recommended deployment model for the vSZ-D for best performance benefits. In this setup, cores as well as the NICs are dedicated to the vSZ-D VM only for best performance.

#### NOTE

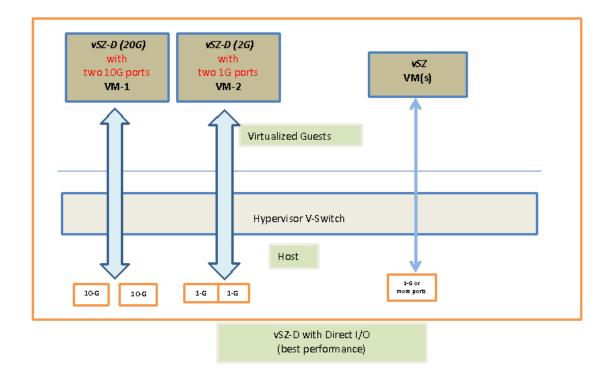
In this setup, the vSZ-D data plane interfaces directly with the DPDK NIC, completely bypassing the vSwitch

### vSZ-D with Directl/O

#### NOTE

The figure below depicts multiple virtual data plane instances for reference purposes only.

It also depicts a vSZ controller instance running as a separate VM. These VMs can be running on the same underlying host or potentially different hosts.

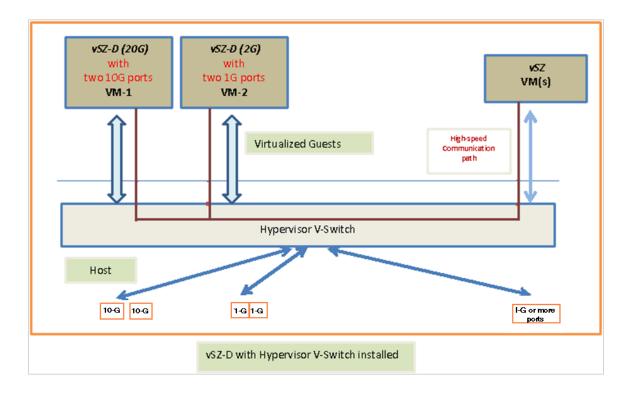


### vSZ-D with Hypervisor vSwitch Installed

The figure below depicts a sample setup via the vSwitch.

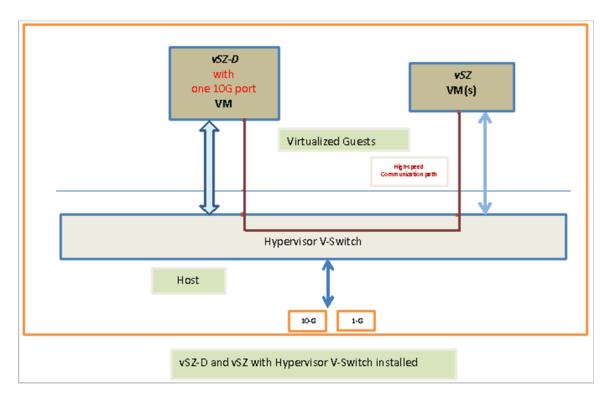
#### NOTE

The figure below depicts multiple virtual data plane instances for reference. It also depicts a vSZ controller instance running as a separate VM.



### vSZ-D and vSZ with Hypervisor vSwitch Installed

The figure below depicts an architecture where vSZ and vSZ-D are running on the same underlying host.



# **Recommended NICs and Operation Modes**

The following table lists the modes of operation and network interface cards (NICs) that have been tested by Ruckus. Other NICs that support Intel DPDK architectures may or may not work.

#### TABLE 7 Recommended NICs and operation modes

Interface	Mode	Supported NIC Driver		NIC Model
Control / management	vSwitch	E1000		1350
				Broadcom BCM5720
Data	Direct IO	1GB	igb	1350
		10GB	ixgbe	82599EB
				82599
				82599ES
				X520
			i40en	X710
		40GB	i40en	XL710
	vSwitch	VMware	VMXNET3/virtIO	
		KVM	Virtio	

# **Hypervisor Configuration**

•	Supported Hypervisors	. 59
•	General Configuration	. 59
•	VMware Specific Configuration	. 59
•	KVM Specific Configuration	. 64

This section covers hypervisor-specific configurations that Ruckus recommends and other settings that you may need to fine tune.

# **Supported Hypervisors**

Unlike the vSZ controller, vSZ-D can only be installed on specific versions of VMware and KVM.

The tables below list the hypervisors and versions on which vSZ and vSZ-D can and cannot be installed.

#### **TABLE 8** vSZ and vSZ-D supported hypervisors

	vSZ	vSZ-D
VMware 5.1	Supported from 2.5	
VMware 5.5 and later	Supported from 3.0	Supported from 3.2
KVM CentOS 6.5 64-bit	Supported from 2.5	
KVM CentOS 7.0 64-bit	Supported from 3.0	Supported from 3.2
Hyper-V	Supported from 3.2	
Azure	Supported from 3.2	
GCE	Supported from 3.2	

### **General Configuration**

Ruckus offers the following general configuration recommendations.

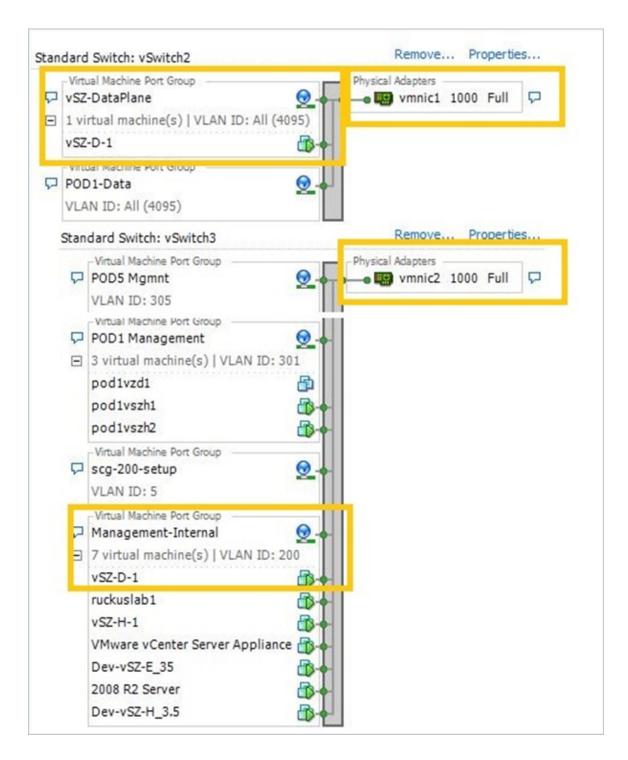
TABLE 9 General vSZ-D configuration recommendations

Component	Minimum Recommendation
Recommended reserved memory	Minimum 6144MB
Recommended number of CPU cores	Minimum three CPU cores. For improved performance in a large-scale deployment, allocate six CPU cores.
Configuration via DirectIO or through vSwitch	To enable passthrough on NIC devices, configure DirectIO mode in ESXi in <b>Advanced Settings</b> .

## **VMware Specific Configuration**

If you are installing vSZ-D on VMware, read these VMware specific configuration recommendations from Ruckus.

Deploy vSZ-D on a machine that has at least two physical NICs. Alternatively, deploy to two vSwitch instances with dedicated physical NICs.



• When deploying an instance of vSZ-D using an OVA file, you must assign the management and data interfaces to two different network groups (vSwitch) on different subnets.

Deploy OVF Template		
Network Mapping What networks should the	deployed template use?	
Source OVF Template Details End User License Agreement	Map the networks used in this OVF	template to networks in your inventory
Name and Location	Source Networks	DestinationNetworks
<u>Disk Format</u>	VM Network	VM Network
Network Mapping Ready to Complete	data-network	Private TestBed
	Description: The data-network network	
Help		< Back Next > Cancel

• Enable **Promiscuous** mode in vSwitch Config.

🕢 vSwitch1 Properties		x
General Security Traffic Shaping NI	Teaming	
Policy Exceptions		1
Promiscuous Mode:	Arrest	
MAC Address Changes:	Accept Accept	
Forged Transmits:	Accept	<u> </u>
	ОК	Cancel Help

• In vSwitch Config, enable VLAN ID for All.

💋 VM xaui0 Properties		×
General Security Traffic Sha	aping NIC Teaming	
Port Group Properties		1
Network Label:	VM xaui0	
VLAN ID (Optional):	All (4095)	<b>•</b>
	OK	Cancel Help

• After the vSZ-D instance is ready, modify the number of CPU cores (if needed) before powering on vSZ-D.

🕢 vDP 740 - Virtual Machine Proper	ies		
Hardware Options Resources			Virtual Machine Version: 8
Show All Devices	Add Remove	Number of virtual sockets:	3 💌
Hardware	Summary	Number of cores per socket:	1 💌
Memory	6144 MB	Total number of cores:	
CPUs	3	Total number of cores:	3
Video card VMCI device SCSI controller 0 Hard disk 1	Video card Restricted LSI Logic SAS Virtual Disk	Changing the number of virtual OS is installed might make your unstable.	
Hard disk 1 Network adapter 1 Network adapter 2	VM Network Private Test Bed	The virtual CPU configuration sp might violate the license of the g	
Help		(	DK Cancel

• For advanced CPU and memory resource configuration recommendations, refer to the vSphere Resource Management Guide, which is available on the VMware website.

# **KVM Specific Configuration**

If you are installing a KVM on VMware, read these KVM specific configuration recommendations from Ruckus.

### **Hypervisor Detail**

You can view the details of the hypervisor.

8	💿 vSZ-D_KVM	I Virtual Machine	
File	Virtual Machine	View Send Key	
	Overview Performance Processor Memory Boot Options IDE Disk 1 NIC :3c:8c:bd NIC :1d:92:39 Mouse Input Display VNC Sound: ich6 Serial 1 Video Cirrus Controller USB Controller pci Controller IDE	Basic Details         Name:       vSz-D_KVM         UUID:       4fd89fdc-0f1c-59a4-1066-62f75e4a35cc         Status:       ■ Running         Description:	
	Add Hardware		Cancel Apply

### **CPU Type**

When selecting the CPU model, make sure you select one that is higher than Intel Core 2 Duo. On Linux, you can this information in /proc/ cpuinfo.

### Hypervisor Configuration

KVM Specific Configuration

8	vsz-D_KVM Virt	ual Machine
File	Virtual Machine View	v Send Key
	1   > 💷 🖸	
	Overview Performance Processor Memory Boot Options IDE Disk 1 NIC :3c:8c:bd NIC :1d:92:39 Mouse Input Display VNC Sound: ich6 Serial 1 Video Cirrus Controller USB Controller IDE	CPUs Logical host CPUs: 8 Current allocation: 4 : Maximum allocation: 4 : Configuration Model: Haswell Copy host CPU configuration COpy host CPU configuration COPy Features Topology Pinning Copy localhost CPU configuration as the CPU info for VM host
	Add Hardware	Cancel Apply

### **Memory Allocation**

You must allocate a minimum of 6G (6144 MByte) memory for vSZ-D.

8	😣 🚍 🐵 vSZ-D_KVM Virtual Machine		
File	Virtual Machine Vie	w Send Key	
	1 🕨 🔟 🙋	Ψ         1         1           Δ         0         0	
	Overview Performance Processor Memory Boot Options IDE Disk 1 NIC :3c:8c:bd NIC :1d:92:39 Mouse Input Display VNC Sound: ich6 Serial 1 Video Cirrus Controller USB Controller IDE	Memory Total host memory: 32055 MB Current allocation: 6144  MB Maximum allocation: 6144  MB	
	Add Hardware	Cancel Apply	

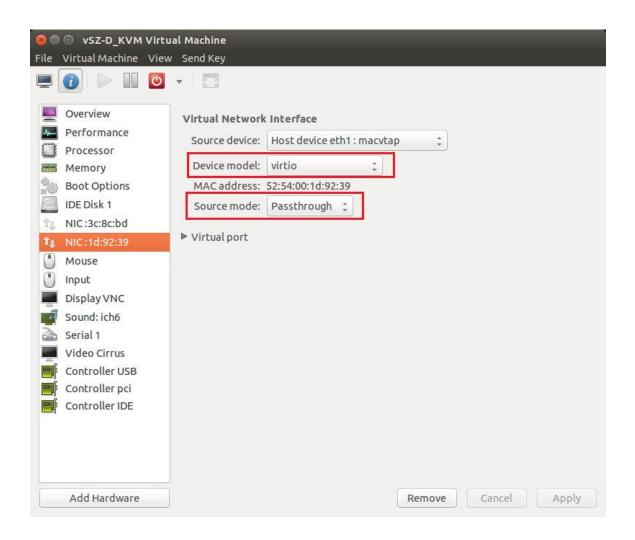
### **Disk Configuration**

Ruckus recommends using Virtio as the disk bus and qcow2 as the storage format.

### Hypervisor Configuration

KVM Specific Configuration

😣 🗐 🗉 vsz-D_KVM Vir	rtual Machine
<u>F</u> ile Virtual <u>M</u> achine <u>V</u> i	ew Send <u>K</u> ey
OverviewPerformanceProcessorMemoryBoot OptionsIDE Disk 1NIC :3c:8c:bdNIC :1d:92:39MouseInputDisplay VNCSound: ich6Serial 1Video CirrusController USBController pciController IDE	<pre>Virtual Disk Target device: IDE Disk 1 Source path: /home/ruckus/vSZ-D image/vdp-3.2.0.0.577.qcow2 Storage size: 1.19 GB Rgadonly: Shareable: Shareable: Disk bus: Virtio Disk bus: Virtio Disk bus: Virtio Serial number: Storage format: qcow2 Performance options Pio Tuning Tip: 'source' refers to information seen from the host OS, while 'target' refers to information seen from the guest OS</pre>
A <u>d</u> d Hardware	<u>R</u> emove <u>C</u> ancel <u>Apply</u>



### **NIC Configuration in Direct IO Mode**

#### NOTE

Only the data interface needs to be configured to direct PCI passthrough. The management interface should always be configured to e1000 as the NIC driver.

Before adding a PCI device to the KVM, you need to complete the following steps:

- 1. Enable VT-d (for Intel processors) in the motherboard BIOS. Intel's VT-d ("Intel Virtualization Technology for Directed I/O") is available on most i7 family processors.
- 2. Add kernel boot parameters via GRUB to enable IOMMU (see figure below). To enable IOMMU in the kernel of Intel processors, pass **intel\_iommu=on** boot parameter on Linux. For more information, read this tutorial.
- 3. After configuring the boot parameter, reset the computer.

You can add kernel boot parameters during boot time.

- For Debian or Ubuntu:
  - a. Edit GRUB config template at /etc/default/grub.
  - b. Add a kernel parameter as "name=value" in GRUB\_CMDLINE\_LINUX\_DEFAULT variable.

\$ sudo -e /etc/default/grub

GRUB\_CMDLINE\_LINUX\_DEFAULT="..... intel\_iommu=on"

c. Then run the following command to generate the GRUB config file.

\$ sudo update-grub

If the command "update-grub" is not found, you can install it as follows:

\$ sudo apt-get install grub2-common

- For Fedora
  - a. Edit GRUB config template at /etc/default/grub.
  - b. Add a kernel parameter as "name=value" in GRUB\_CMDLINE\_LINUX variable.

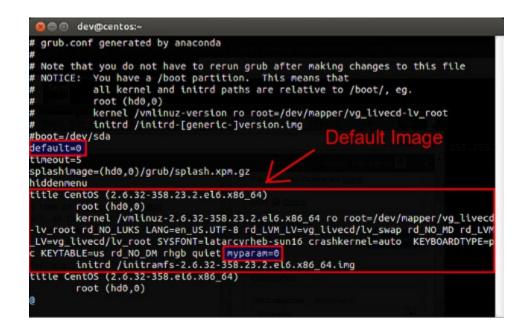
\$ sudo -e /etc/default/grub
GRUB CMDLINE LINUX="..... intel iommu=on"

c. Then run the following command to generate the GRUB config file.

\$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg

- For CentOS
  - a. Edit GRUB config template at /boot/grub.conf.
  - In the config file, look for the entry "default=N" at the top of the config file indicates which entry is the default image.
     On the next line, add a kernel parameter as "name=value" in kernel /vmlinuz- variable.

kernel /vmlinuz-".... intel\_iommu=on"



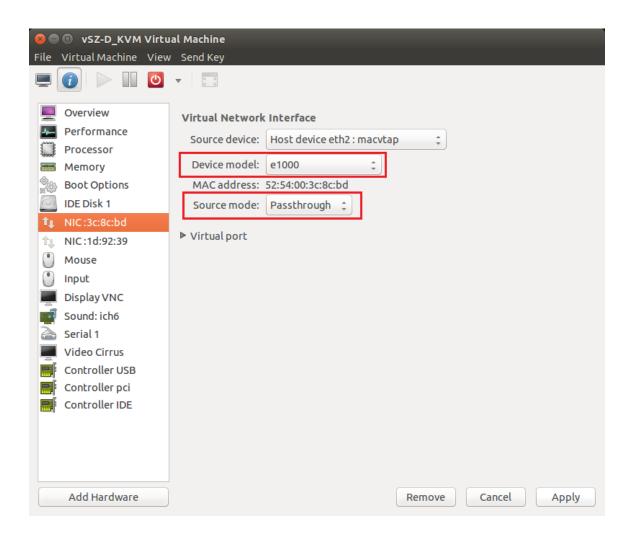
### NIC Configuration in vSwitch Mode

#### NOTE

Configure only two ports for vSZ-D/.

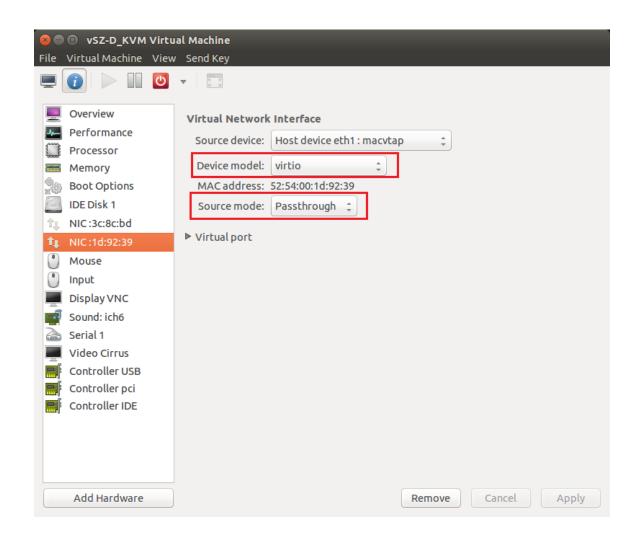
For the management interface, use the following settings:

- Device model: e1000
- Source mode: Either Bridge or Passthrough if you are using macvtap for the device type.



For the data interface, use the following settings:

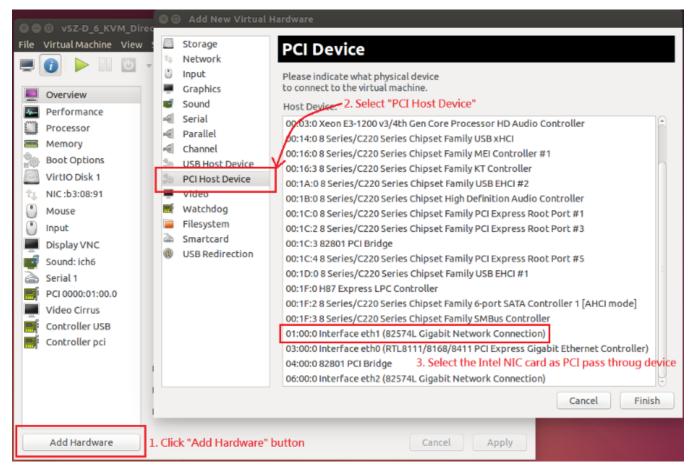
- Device model: e1000
- Source mode: Passthrough if you are using macvtap for the device type. Only the passthrough mode can allow UE traffic to pass through the VM NIC.



### Adding a PCI Device to a VM on Virt-Manager

To assign a PCI device to a guest VM on virt-manager. :

- 1. From the VNC Viewer and click Add Hardware > PCI Host Device.
- 2. Choose a PCI device to assign from the PCI device list, and click Finish.



3. Power on the guest and the host PCI device would be visible in the guest VM.

## **NIC Card Setting**

You must use only two ports.

	Management Interface	Data Interface
KVM w/ vSwitch	e1000	virtio
KVM w/ pci passthrough	e1000	1G: igb
		10G:ixgbe
VMware w/ vSwitch	e1000	VMXNET3
	e1000e	
VMware w/ pci passthrough	e1000	1G:igb
	e1000e	10G:ixgbe

# **Deployment of vSZ**

•	Deploy vSZ-D with 40GB NIC on ESXi Server	. 75
•	Deploy vSZ-D with 40GB NIC on Linux Server	90

## Deploy vSZ-D with 40GB NIC on ESXi Server

### Deploy vSZ-D with 40GB NIC on ESXi Server

#### Hardware Requirement and Prerequisite

The following are the hardware and prerequisite for deploying vSZ-D on ESXi 6.7

#### Hardware Requirement

- 1. DELL Inc. PowerEdge R530
- 2. ESXi Server License 6.7
- 3. Broadcom NetXtreme BCM5720 Gigabit Ethernet NIC
- 4. Intel Ethernet XL710 for 40GbE QSFP+
- 5. CPU minimum 4 cores
- 6. vSphere ESXi Server 6.7 or later
- 7. 1 or 2 vNICs
- 8. 8 GB memory
- 9. 128 GB Hard disk

#### Prerequisite

- A hypervisor on ESXi to install vSZ-D. Recommended version is ESXi 6.7 and later.
- Download the vSZ-D package (.OVA file) from Ruckus support .
- The IP addresses, netmask, gateway, DNS, DHCP and NAT support for vSZ-D.
- Before you power on vSZ-D, ensure that the networking is configured on ESXi.
- Recommended to use static network addresses that are assigned to vSZ-D during setup.

#### NOTE

Due to different servers and NIC, the deployment procedure mentioned in this section is for reference.

#### Topology

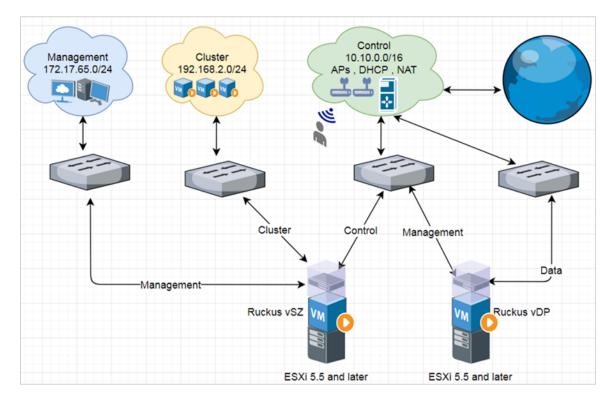
The network topologies for vSZ-D deployment on ESXi 6.7 server.

The following are basic topologies for setting up vSZ-D. Based on your requirement you can choose any of the alternatives between one IP domain to three separate domains for deployment.

The below topology shows the different IP addresses for the domains.

**Deployment of vSZ** Deploy vSZ-D with 40GB NIC on ESXi Server

#### FIGURE 29 Three different IP addresses setup



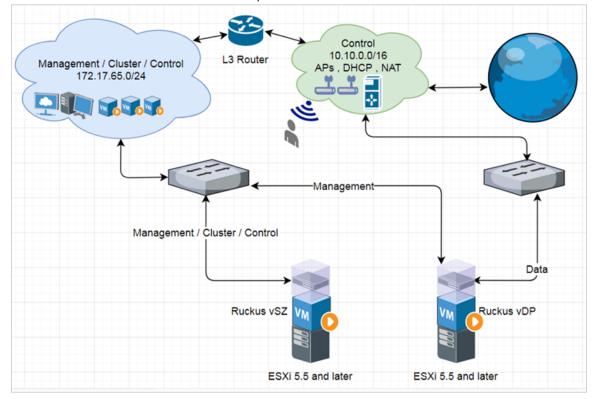
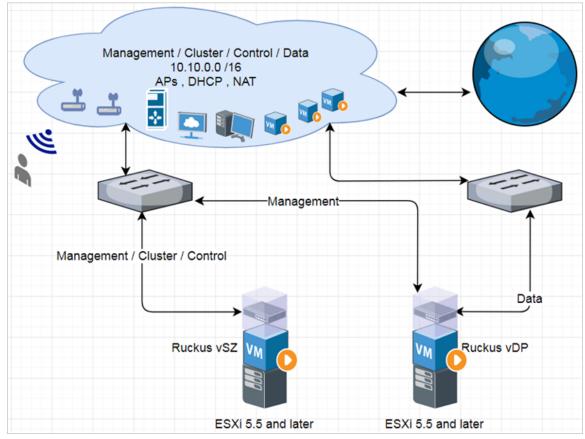


FIGURE 30 Two different domain IP addresses setup

The below topology shows the same IP addresses for the all the interfaces.

**Deployment of vSZ** Deploy vSZ-D with 40GB NIC on ESXi Server

#### FIGURE 31 The same IP addresses setup



#### **Deployment Procedure**

The following are basic instructions for setting up the controller on the ESXi server.

VMware ESXi 6.7 is installed and working.

For this deployment two different IP address domains are considered for controller interfaces. Refer to Topology on page 75

1. Login to the server through vSphere client tool as seen below.

FIGURE 32 Login to vSphere

💋 VMware vSphere Client		X
vmware VMware vSphere Client	ļ	2
only through the vSphe	oduced in vSphere 5.5 and beyond are available ere Web Client. The traditional vSphere Client will pporting the same feature set as vSphere 5.0.	
name.	ost, enter the IP address or host er the IP address or name of a	_
IP address / Name:	172.17.65.43	
User name:	root	
Password:	*****	
	Use Windows session credentials Login C	lose

The vSphere Client management page appears as shown in the following figure.

FIGURE 33 vSphere Client management page



2. Navigate to Configuration > Advanced Settings > Edit.

The DirectPath I/O Configuration page appears.



3. Select XL710 40GbE QSFP+ ports and reboot vSphere server.

4. Download the controller (.ova file) from Ruckus support .

#### NOTE

You must deploy the controller directly from the .ova file. Copying an instance of the controller from another controller template might not function properly.

#### FIGURE 34 Deploy the file

🕜 Deploy OVF Templat	e 📃 🗌 其 X
Source Select the source	location.
Source OVF Template Detais Name and Location Disk Format Ready to Complete	Deploy from a file or URL D:\Brocade Report\\VDP\Vdp-5.0.0.0.372.ova To Browse. Enter a URL to download and instal the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
	< Back Next > Cancel

- 5. Click Browse, to select the source location and upload the .ova file.
- 6. Click Next.

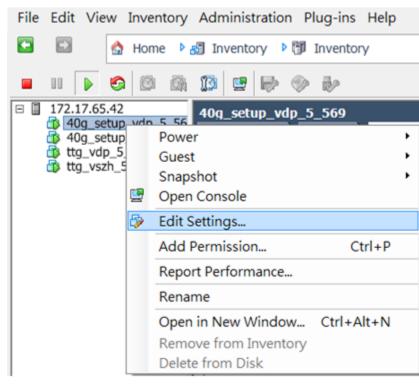
7. Enter the vSZ datastore name and choose the disk format as seen below.

FIGURE 35 Choose the disk format

🕝 Deploy OVF Templat	e					_ 🗆 🗙
<b>Disk Format</b> In which format de	o you want to store the v	irtual disks?				
Source OVF Template Detais End User License Agreer Name and Location Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB): C Thick Provision Lazy C Thick Provision Eage C Thin Provision					
4 III >				< Back	Next >	Cancel
			_	S DOCK	NCAL >	

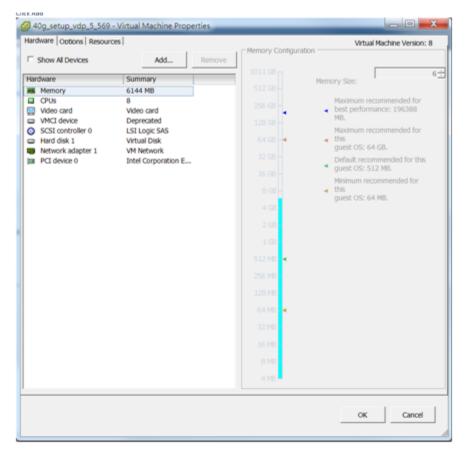
8. Click Next.

9. From the controller, right-click the VM and select **Edit Settings**.



The Virtual Machine Properties dialog opens.

10. Select the destination network for each network source and click Add as shown in the following image.



11. For 40Gb throughput performance , select total number of CPU cores to 8.

🕜 40g_setup_vdp_5_569 - V	irtual Machine Prope	rties			-	_ D X
Hardware Options Resources	]				Virtual N	Nachine Version: 8
Show All Devices	Add	Remove	Number of virtual socke		8 <b>•</b>	
Hardware	Summary					
Memory	6144 MB		Total number of cores:		8	
CPUs	8		Changing the number of the	ber of vir	tual CPUs a	after the quest OS
📃 Video card	Video card		is installed might ma			
VMCI device	Deprecated			,		
SCSI controller 0	LSI Logic SAS		The virtual CDU cor	-four stic	n an affed	on this page
Hard disk 1	Virtual Disk		The virtual CPU cor might violate the lic			
Network adapter 1	VM Network		might violate the lic	Jense or (	une guest o	
PCI device 0	Intel Corporation E					

#### 12. Select 6GB memory size.

ardware Options Resour	ces		Virtual Machine Version: 8
Show All Devices	Add	Remove	Configuration
ardware	Summary	1011 GB	Memory Size:
Memory	6144 MB	512 GB	
CPUs Video card	8 Video card	256 GB	B Maximum recommended for best performance: 196388 MB.
VMCI device SCSI controller 0	Deprecated LSI Logic SAS	128 GB	B Maximum recommended for
Hard disk 1	Virtual Disk	64 GB	
Network adapter 1 PCI device 0	VM Network Intel Corporation E	32 GB	B − Default recommended for this guest OS: 512 MB.

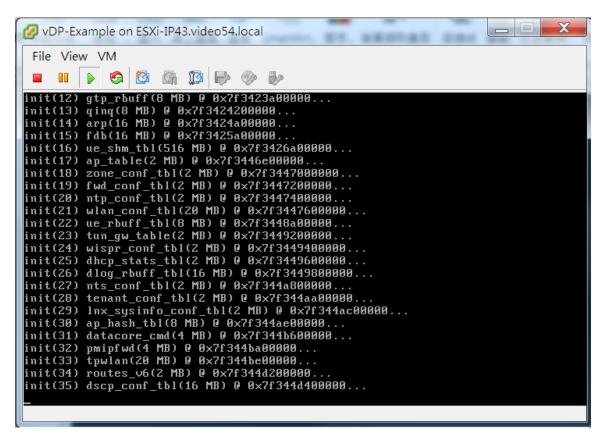
- 13. Click **OK** to start the deployment.
- 14. The deployment progress is displayed. On successful deployment, by default the controller now supports two network interfaces for management and data.

#### vSZ-D/SZ100-D/SZ144-D Connect to vSZ Using CLI

Follow the below procedures for vSZ-D/SZ100-D/SZ144-D to connect to vSZ.

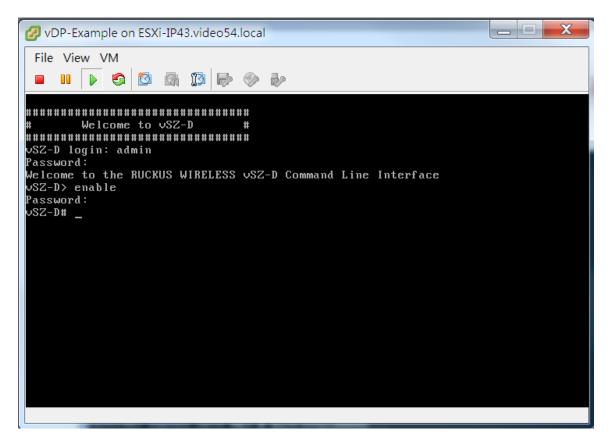
Open a CLI console window to run the deployed vSZ-D/SZ100-D/SZ144-D.

FIGURE 36 Run vSZ-D/SZ100-D/SZ144-D on the console



1. At the login prompt, login using **administrator** credentials of username and password. At the > prompt, enter the **enable (en)** command and the admin password to change the mode to Privileged-exec mode.

#### FIGURE 37 Login and Privileged mode



2. Run the **setup** command to configure the IP address for management and data interface. It is recommended to add a new host if you have multiple hosts for various configurations

FIGURE 38 Execute the setup command



Deploy vSZ-D with 40GB NIC on ESXi Server

3. Choose the IP address setup (IPv4 only or IPv4 and IPv6) for Management and Data interface by either selecting manual or DHCP. On defining the IP setup the process of vSZ-D/SZ100-D/SZ144-D connecting to vSZ controller starts.

FIGURE 39 Management interface

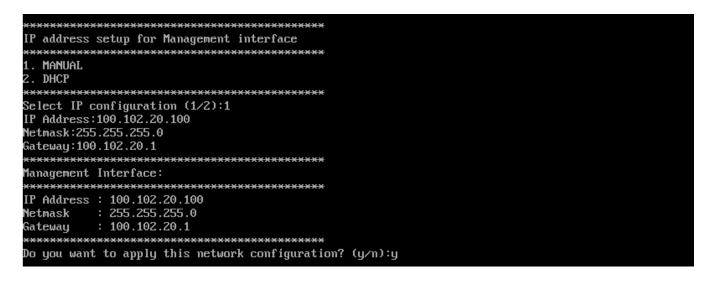


FIGURE 40 Data interface



4. Enter the DNS setting and select Enter to skip the NAT IP setting.

FIGURE 41 DNS setting

```
Primary DNS:8.8.8.8
Secondary DNS:8.8.4.4
Apply networking configuration ...
Save network configuration !
Data Interface external NAT IP:_
```

5. Enter vSZ control interface IP address. Follow the set of sequences as seen below for the vSZ-D/SZ100-D/SZ144-D to connect to vSZ controller. This changes the mode for vSZ-D/SZ100-D/SZ144-D as well as for vSZ.

FIGURE 42 vSZ control IP address

```
Please input vSZ Control address:10.10.234.1
Do you want to connect vSZ (address:10.10.234.1) (y/n):y
Apply vSZ address ...
Save vSZ address
```

FIGURE 43 Connecting to vSZ

```
Please enter the new password for the local user "admin".....
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Please enter CLI enable password that provides advance command.....
New password:
Retype:
CLI enable password saved.
Setup vSZ-D Done !!
Exit setup.
vDP-Example# _
```

6. Exit from CLI console.

7. To view and approve the vSZ-D/SZ100-D/SZ144-D, login to the web interface. Navigate to **Clusters** > **Data planes**. Select the vSZ-D/SZ100-D/SZ144-D and click on **Approve**. On approval the status is greyed.

#### FIGURE 44 Approve the vSZ-D/SZ100-D/SZ144-D

Data Planes									
🖉 Configure	✓ Approve	<u> Î</u> Delete	L Download				search table		Q 2
Name 🔺	DP T	prove the da	ata plane ress	Data IP	Management/Co	Model	Serial Number	Firmware	Manage
vDP-Example	External	-Virt 00	):0C:29:81:D1:46	10.10.239.235	172.17.65.235	vSZ-D	972M3WP03B	5.0.0.372	vSZ-EXa

#### FIGURE 45 Approved status

Data Plane	es								
🖉 Configure	e 🗸 Appro	ove <u>व</u> Delete	L Download			5	search table	Q	C
nagement/Co	Model	Serial Number	Firmware	Managed By	DP Status	Registration State	Uptime	Last Seer	n On
.17.65.235	vSZ-D	972M3WP03B	5.0.0.372	vSZ-EXample	Managed	Approved	27m 37s	2018/02/	

You have successfully added the vSZ-D/SZ100-D/SZ144-D image to the vSZ controller.

#### NOTE

Once the vSZ-D is registered and managed by the vSZ controller, the CLI login credentials will be the same as the vSZ superadmin. The CLI **enable password** remains the admin password set during vSZ-D configuration.

# **Deploy vSZ-D with 40GB NIC on Linux Server**

### Deploy vSZ-D with 40GB NIC on Linux Server

#### Hardware Requirement and Prerequisite

The following are the hardware and prerequisite for deploying vSZ-D on LINUX CentOS 7.

#### Hardware Requirement

- 1. DELL Inc. PowerEdge R320
- 2. Linux CentOS 7
- 3. Broadcom NetXtreme BCM5720 Gigabit Ethernet 2 Ports
- 4. Intel Ethernet 10G 2P X520

#### Prerequisite

- A Linux host enabled KVM which to install vSZ-D VM. Prefer CentOS 7 and later.
- Download the vSZ-D package (.qcow2 file) from Ruckus support .

- The IP addresses, netmask, gateway, DNS, DHCP and NAT support for vSZ-D.
- Two network interfaces to support vSZ-D.
- Before you power on vSZ-D, ensure that the networking is configured on LINUX.
- Recommended to use static network addresses that are assigned to vSZ-D during setup.
- Using CentOS 7, install KVM package with the yum command.

```
root@localhost ruckusvnc]# yum -y install qemu-kvm qemu-img virt-manager virt-viewer virt-install
libvirt libvirt-phthon libvirt-client
```

• Ensure KVM is active and running the following command

[root@localhost ruckusvnc]# systemctl status libvirtd

• Edit the following commands and file.

```
sudo yum install grub2-common
```

```
gedit /etc/default/grub
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet
intel_iommu=on"
GRUB_DISABLE_RECOVERY="true"
```

sudo grub2-mkconfig -o /boot/grub2/grub.cfg

Reboot Linux host.

#### NOTE

Due to different servers and NIC, the deployment procedure mentioned in this section is for reference.

#### Topology

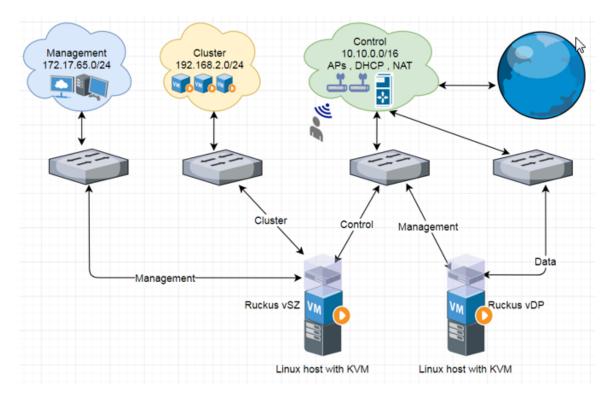
The network topologies for vSZ-D deployment on LINUX CentOS 7.

The following are basic topologies for setting up vSZ-D. Based on your requirement you can choose any of the alternatives between one IP domain to three separate domains for deployment.

The below topology shows the different IP addresses for the domains.

**Deployment of vSZ** Deploy vSZ-D with 40GB NIC on Linux Server

#### FIGURE 46 Three different IP addresses setup



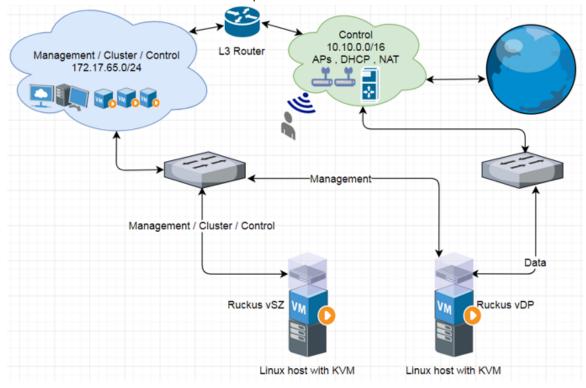
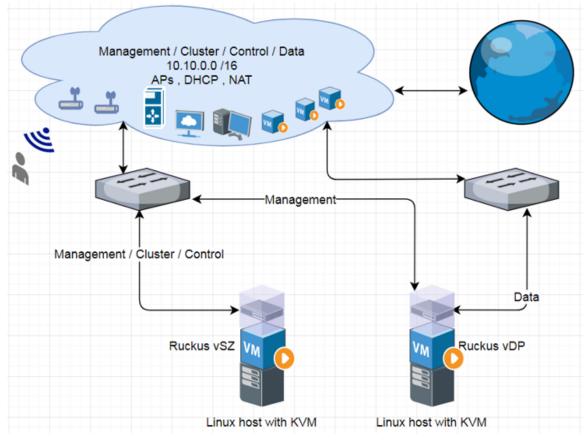


FIGURE 47 Two different domain IP addresses setup

The below topology shows the same IP addresses for the all the interfaces.

**Deployment of vSZ** Deploy vSZ-D with 40GB NIC on Linux Server

#### FIGURE 48 The same IP addresses setup



#### **Deployment Procedure**

The following are basic instructions for setting up vSZ-D on LINUX KVM.

LINUX CentOS 7 KVM Package is installed and working.

For this deployment two different IP address domains are considered for Data Plane interfaces. Refer to Topology on page 91.

1. Download the Data Plane package (.qcow2 file) from Ruckus support .

2. From the VNC Viewer, click **System Tools** > **Virtual Machine Manager** to open the Virtual Machine Manager tool. The Data Plane status must appear Running as shown in the following figure.

Applications Places     Favorites     Accessories   Documentation   Graphics   Merret   Office   Software   Office   Sound & Video   Sundry   System Tools   Utilities   Other     System Monitor	172.17.65.34:5904 (lo	ocalhost.localdomain:4 (ruckusvnc)) - VNC Viewer		x
Accessories   Accessories   Documentation   Graphics   Settings   Internet   Software   Office   Sound & Video   Sundry   Startup Applications   System Tools   Vetilities   System Monitor	S Applications - Place	es 👻 🚺 Machine Manager 👻	Thu 16:01 🗖 🖤	00
	Accessories Documentation Graphics Internet Office Sound & Video Sundry System Tools Utilities	Boxes         Settings         Software         Software         Software Update         Software Update         System Log         System Monitor	File Edit View Help	
Activities Overview	Activities Overview			

FIGURE 49 Virtual Machine Manager

**Deployment of vSZ** Deploy vSZ-D with 40GB NIC on Linux Server

- 3. Create a new VM.
  - a) Click File and select New Virtual Machine as shown in the following figure.

#### FIGURE 50 Creating a Virtual Machine

	Virtual Machin	e Manag	jer	- 1	×
File Edit View	Help				
Add Connection		-			
New Virtual Mach	iine		÷	CDU	
Close	Ctrl+W		*	CPU usage	
Quit	Ctrl+Q				~~
Running					]

b) In the New VM dialog box, choose the disk format option as shown in the following figure.

#### FIGURE 51 Disk Format

New VM
Create a new virtual machine Step 1 of 4
Connection: QEMU/KVM
Choose how you would like to install the operating system
<ul> <li>Local install media (ISO image or CDROM)</li> </ul>
<ul> <li>Network Install (HTTP, FTP, or NFS)</li> </ul>
O Network Boot (PXE)
<ul> <li>Import existing disk image</li> </ul>
Cancel Back Forward

#### c) Click Forward.

d) Choose destination storage path and storage volume. Click Browse Local as show in the following figure.

#### FIGURE 52 Storage Volume

	Choose Storag	e Volun	ne			×
22%     default Filesystem Directory     Size:     38.50 GiB Free / 11.48 GiB In Use Location: /var/lib/libvirt/images       or     Downloads						
0% Filesystem Directory	Volumes 💠 🥲 🗵				2	
	Volumes	~	Size	Format	Used By	
	ubuntu16.04.qcow2		15.00 GiB	qcow2	ubuntu16.04	
			Browsel		Choose Volu	
+ 🖻 💥 📀			Browse L	ocal Car	Choose Volu	me

e) Select the Data Plane file and click **Open** as shown in the following figure.

#### FIGURE 53 Data Plane File

Applications Places	Virtual Machine Manager		Mon 20:34 • 🔥 📢
Cancel	Name vdp-5.0.0.0.376.qcow2	c	Q Open
Home			C2
Documents N	ame	▼ Size	Modified
Downloads	ubuntu-16.04-desktop-amd64.iso	1.5 G	8 15 Jan
Lowintoads	vdp=5.0.0.0.376.qcow2	950.0	MB 15:41
Music	vscg-5.0.0.0.376.qcow2	3.1 G	B 20:34
Pictures			
Videos			
Other Locations			

f) To select the storage path, click **Browse** as shown in the following figure.

#### FIGURE 54 Storage Path

	New VM	×
	ate a new virtual machine	
Provide the	existing storage path:	
/home/re	uckusvnc/Downloads/vdp-5.0.0.0. Browse	
Choose an o	perating system type and version	
OS type:	Generic	
Version:	Generic	
version.	Generic	
	Cancel Back Forward	

- g) Click Forward.
- h) Enter the Memory (RAM) and CPUs setting as shown in the following figure.

#### NOTE

Memory (RAM) must be 6GB and CPUs must be 8 cores.

#### FIGURE 55 Memory and CPU Settings

	New VM	×					
C	Create a new virtual machine Step 3 of 4						
c	hoose Memory and CPU settings						
	Memory (RAM): 6144 - + MiB						
	Up to 98082 MiB available on the host						
	CPUs: 8 – +						
l	Up to 24 available						
	Cancel Back Forwa	rd					

#### i) Click Forward.

j) To confirm the installation process, click **Finish** as shown in the following figure.

#### NOTE

The sequence for Network interfaces must first be Management and the Data.

FIGURE 56 Installation Confirmation

New VM ×					
Create a new virtual machine Step 4 of 4					
Ready to begin the installation					
Name: 40G-vDP-Example					
OS: Generic					
Install: Import existing OS image					
Memory: 6144 MiB					
CPUs: 8					
Storage:c/Downloads/vdp-5.0.0.0.594.qcow2					
Customize configuration before install					
▶ Network selection					
Cancel Back Finish					

4. 4. Add another NIC as Data Plane needs two interfaces; Management and Data. From the VNC Viewer and click Add Hardware > PCI Host Device > PCI Device to add another NIC as shown in the following figure.

#### FIGURE 57 Adding NIC

💠 Applications Places Virtual Machine Manager		
vDP-Example on QEMU/KVM _		×
File Virtual Machine View Send Key		
		¢
Source Basic Details		
Performance Name: vDP-Example		
CPUs UUID: 268ca1bf-ae63-4784-9275-4ee682d0a243		
Memory Status: Shutoff		
Boot Options Title:		
VITO Disk I		
NIC :ae:b2:28 Description:		
Mouse		
🛋 Keyboard		
Display Spice		
Sound: Icne		
Serial 1		
Channel spice		
Video GAL		
Conducter 03B		
Controller PCI		
Controller VirtIO Serial		
W USB Redirector 1		
Add Hardware Cancel A	pply	

#### 5. Select PCI Host Device > PCI Device and click Finish to add another NIC as shown in the following figure.

#### FIGURE 58 PCI Host Device

		Add New Virtual Hardware			
9	Storage	PCI Device			
2	Controller				
٥	Network	Host Device:			
0	Input	prporation C610/X99 series chipset PCI Express Root Port #3			
2	Graphics	prporation C610/X99 series chipset PCI Express Root Port #4			
	Sound	prporation C610/X99 series chipset PCI Express Root Port #5			
4	Serial	prporation C610/X99 series chipset USB Enhanced Host Controller #1			
-	Parallel	rporation C610/X99 series chipset LPC Controller			
-	Console	prporation C610/X99 series chipset 6-Port SATA Controller [AHCI mode]			
-	Channel	ic / Symbios Logic MegaRAID SAS-3 3008 [Fury]			
ŝ	USB Host Device	om Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em1)			
¢₿	PCI Host Device	om Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em2)			
2	Video	om Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em3)			
	Watchdog	om Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em4)			
	Filesystem	rporation Ethernet Controller XL710 for 40GbE QSFP+ (Interface p2p1)			
à	Smartcard	rporation Ethernet Controller XL710 for 40GbE QSFP+ (Interface p2p2)			
	USB Redirection	s Technology Corp. SH7758 PCIe Switch [PS]			
۵	TPM	s Technology Corp. SH7758 PCIe Switch [PS]			
ŝ	RNG	s Technology Corp. SH7758 PCIe-PCI Bridge [PPB]			
ŝ	Panic Notifier	Electronics Systems Ltd. G200eR2			
		Cancel Finish			

6. Select the NIC and choose the **Device model** to update the management interface associate as shown in the following figure.

FIGURE 59 Management Interface

40G-vDP-Example on QEMU/KVM								×
<	Begin Installation	🥚 Cancel Installati	ion					
	Overview	Virtual Network Int	terface					
	CPUs	Network source:	Host device e	em1: macvta	ap 🖣	•		
	Memory					_		
33	Boot Options		Source mode:	Bridge		•	J	
	IDE Disk 1		A In most config for host to gu					
3	NIC :81:2d:bd		-	connection c				
$\diamond$	Mouse	Device model:	e1000		•			
-	Display Spice	MAC address:	52:54:00:81:2	d:bd				
	Sound: ich6							
2	Console	<ul> <li>Virtual port</li> </ul>						
	Channel spice							
	PCI 0:4:0.1							
-	Video QXL							
	Controller USB							
۲	USB Redirector 1							
۲	USB Redirector 2							
	Add Hardware					Remove	Cancel	Apply
	Add HardWare					Remove	Cancer	ubbra

7. From PCI, select the ROM BAR check box to define the Data IP domain as shown in the following figure.

FIGURE 60 Data IP Domain

40G-vDP-Example on QEMU/KVM							
1	Begin Installation	Cancel Installation					
	IDE Disk 1 NIC :81:2d:bd Mouse Display Spice	Physical PCI Device Device: 0000:04:00:1 Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+ ROM BAR: ☑					
	Add Hardware	Remove Cancel Apply	,				

8. Define the CPU Configuration. Select the Copy host CPU configuration check box as shown in the following figure.

FIGURE 61 CPU Configuration

	40G-vDP-Example on QEMU/KVM							×	
<b>«</b>	Begin Installation	Cancel In	stallation						
	Overview	CPUs							
	CPUs	Logical hos	t CPUs:	24					
-	Memory	Current allo	ocation:	8	-	+			
33	Boot Options			-					
	IDE Disk 1	Maximum a	llocation:	8		+			
9	NIC :81:2d:bd	Configuration	n						
Ò	Mouse	Copy ho	ost CPU co	nfigurati	on				
	Display Spice	▼Topology				-			
	Sound: ich6	1 27	ally set CP	U topolo	gy				
e	Console	Sockets:	8	- +					
	Channel spice								
	PCI 0:4:0.1	Cores:	1	- +					
	Video QXL	Threads:	1	- +					
	Controller USB USB Redirector 1								
	USB Redirector 2								
	OSB Redirector 2								
	Add Hardware							Cancel	Apply

9. Define the IDE Disk Configuration. Choose the **Disk bus** option as shown in the following figure.

FIGURE 62 IDE Disk Configuration

40G-vDP-Example on QEMU/KVM					×
Ľ	Begin Installation	🥚 Cancel Installat	ion		
	Overview	Virtual Disk			
Ō	CPUs	Source path: /ho	ome/ruckusvnc/Download	ds/vdp-5.0.0.0.594.qcow	2
-	Memory	Device type: IDE			
33	Boot Options	Storage size: 10.	.00 GiB		
-	IDE Disk 1	Readonly:			
9	NIC :81:2d:bd	Shareable: 📃			
ð	Mouse	▼ Advanced optio	ons		
-	Display Spice	Disk bus:	VirtlO	•	
J	Sound: ich6	Serial number:			
2	Console			_	
2	Channel spice	Storage format:	qcow2		
	PCI 0:4:0.1	Performance op	ptions		
	Video QXL				
	Controller USB				
¢	USB Redirector 1				
1	USB Redirector 2				
	Add Hardware			Remove	Cancel Apply

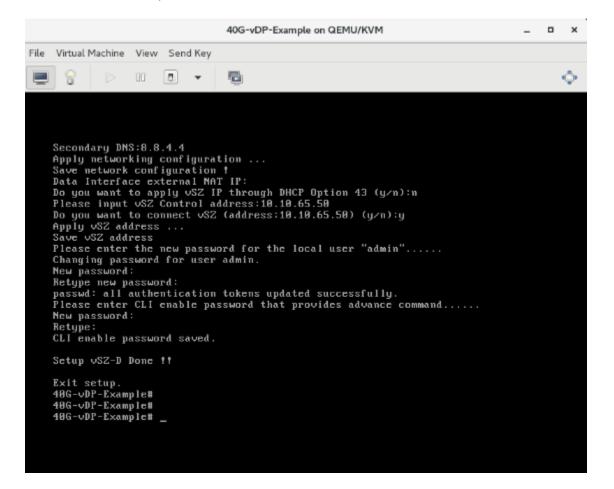
10. Select **Begin Installation** as shown in the following figure.

FIGURE 63 Begin Installation

			vDP-Example on QEMU/KVM		×
1	Begin Installation	💥 Cancel Insta	allation		
E	Overview CPUs	Basic Details Name:	vDP-Example		
	Memory Boot Options VirtIO Disk 1 NIC :ae:b2:28 NIC :4f:19:a2 Mouse Display Spice	UUID: Status: Title: Description:	268ca1bf-ae63-4784-9275-4ee682d0a243		
	Sound: ich6 Console Channel spice Video QXL Controller USB USB Redirector 1 USB Redirector 2	Hypervisor De Hypervisor: Architecture: Emulator: Firmware: Chipset:	KVM		
	Add Hardware			Cancel	pply

11. The Data Plane setup is complete as shown in the following image.

#### FIGURE 64 Installation Complete



#### vSZ-D/SZ100-D/SZ144-D Connect to vSZ Using CLI

Follow the below procedures for vSZ-D/SZ100-D/SZ144-D to connect to vSZ.

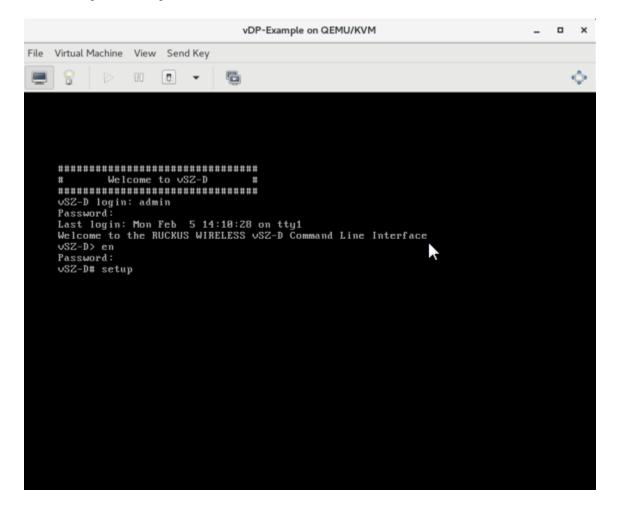
Open a CLI console window to run the deployed vSZ-D/SZ100-D/SZ144-D.

#### FIGURE 65 Run vSZ-D/SZ100-D/SZ144-D on the console

vDP-Example on QEMU/KVM	- 🖓 🗖 🗙
File Virtual Machine View Send Key	20
💻 💡 ▷ 🗉 🗷 🖛	$\diamond$
Booting from Hard Disk	
Press any key to enter the menu	
Booting rootfs2 in 0 secondsProbing EDD (edd=off to disable) ok	
sched: Error, all isolcpus= values must be between 0 and 3 sched: Error, all isolcpus= values must be between 0 and 3	
detect_ipmi detect_car2030	
The platform is "vmSCG" [: 28: -gt: unexpected operator	
Unable to read the board data: not found board data Operation failed!!	
1 logical volume(s) in volume group "vg88" now active 1 logical volume(s) in volume group "rootfs_vg" now active	
fsck from util-linux-ng 2.17.2 bootfs: clean, 40/65536 files, 14596/261881 blocks	
fsck from util-linux-ng 2.17.2 datafs: clean, 21/190080 files, 29455/759808 blocks	
Failed to find device for physical volume "/dev/dm-4". [: 42: Illegal number: -	
No upgrading is in action. Nothing to do.	
Welcome to _	

1. At the login prompt, login using **administrator** credentials of username and password. At the > prompt, enter the **enable (en)** command and the admin password to change the mode to Privileged-exec mode.

#### FIGURE 66 Login and Privileged mode



2. Run the **setup** command to configure the IP address for management and data interface. It is recommended to add a new host if you have multiple hosts for various configurations

#### FIGURE 67 Execute the setup command



#### Deployment of vSZ

Deploy vSZ-D with 40GB NIC on Linux Server

3. Choose the IP address setup (IPv4 only or IPv4 and IPv6) for Management and Data interface by either selecting manual or DHCP. On defining the IP setup the process of vSZ-D/SZ100-D/SZ144-D connecting to vSZ controller starts.

FIGURE 68 Management interface

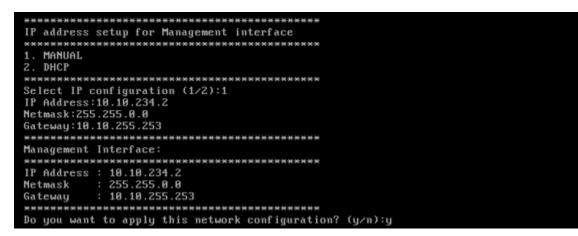
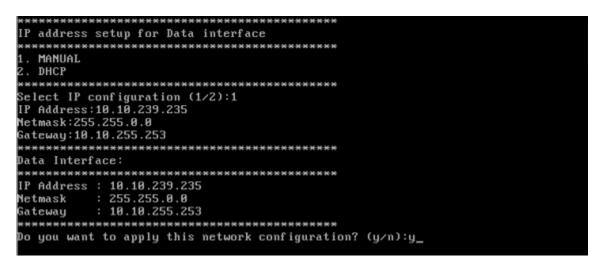


FIGURE 69 Data interface



4. Enter the DNS setting and select Enter to skip the NAT IP setting.

FIGURE 70 DNS setting

```
Primary DNS:8.8.8.8
Secondary DNS:8.8.4.4
Apply networking configuration ...
Save network configuration !
Data Interface external NAT IP:_
```

5. Enter vSZ control interface IP address. Follow the set of sequences as seen below for the vSZ-D/SZ100-D/SZ144-D to connect to vSZ controller. This changes the mode for vSZ-D/SZ100-D/SZ144-D as well as for vSZ.

FIGURE 71 vSZ control IP address

```
Please input vSZ Control address:10.10.234.1
Do you want to connect vSZ (address:10.10.234.1) (y/n):y
Apply vSZ address ...
Save vSZ address
```

FIGURE 72 Connecting to vSZ

```
Please enter the new password for the local user "admin".....
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Please enter CLI enable password that provides advance command.....
New password:
Retype:
CLI enable password saved.
Setup vSZ-D Done !!
Exit setup.
vDP-Example# _
```

6. Exit from CLI console.

7. To view and approve the vSZ-D/SZ100-D/SZ144-D, login to the web interface. Navigate to **Clusters** > **Data planes**. Select the vSZ-D/SZ100-D/SZ144-D and click on **Approve**. On approval the status is greyed.

#### FIGURE 73 Approve the vSZ-D/SZ100-D/SZ144-D

_								
🖉 Configure 🔦	Approve	🖬 Delete 上 Download				search table		Q 2
Name 🔺	DP T	ove the data plane	Data IP	Management/Co	Model	Serial Number	Firmware	Manage
vDP-Example	External-V	irt 00:0C:29:81:D1:46	10.10.239.235	172.17.65.235	vSZ-D	972M3WP03B	5.0.0.372	vSZ-EX

#### FIGURE 74 Approved status

Data Plane	es									
🖉 Configure	e 🖌 Appro	ove <u>व</u> Delete	🛓 Download				search table	Q	C	
nagement/Co	Model	Serial Number	Firmware	Managed By	DP Status	Registration State	Uptime	Last Seer	n On	¢
.17.65.235	vSZ-D	972M3WP03B	5.0.0.372	vSZ-EXample	Managed Approved		27m 37s	2018/02/		

You have successfully added the vSZ-D/SZ100-D/SZ144-D image to the vSZ controller.

#### NOTE

Once the vSZ-D is registered and managed by the vSZ controller, the CLI login credentials will be the same as the vSZ superadmin. The CLI **enable password** remains the admin password set during vSZ-D configuration.

# **Upgrade Procedure**

## **Upgrade Procedure**

Procedure for upgrading to a new vSZ-D/SZ100-D/SZ144-D version.

#### Controller and vSZ-D/SZ100-D/SZ144-D Firmware Compatibility Matrix

The below table indicates the compatibility matrix. In general, Ruckus supports N-2 vSZ-D/SZ100-D/SZ144-D releases with vSZ.

vSZ	SZ144	I-D				SZ100-D Release							vSZ-D Release								
	6.1. 1	6.1. 0	6.0. x	5.2. 2	5.2. 1	6.1. 1	6.1. 0	6.0.x	5.2. 2	5.2. 1	5.2. 0	5.1. x	6.1.1	6.1. 0	6.0. x	5.2. 2	5.2. 1	5.2. 0	5.1. x	5.0.x	3.6. 2
6.1. 1	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No	No	No	Yes (*)
6.1. 0	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	No	No
6.0. x	No	No	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No	No
5.2. 2	No	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes
5.2. 1	No	No	No	No	Yes	No	No	No	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes
5.2. 0	No	No	No	No	No	No	No	No	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes
5.1. x	No	No	No	No	No	No	No	No	No	No	No	Yes	No	No	No	No	No	No	Yes	Yes	Yes
5.0. x	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes	Yes
3.6. 2	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Yes

TABLE 10 Controller and vSZ-D/SZ100-D/SZ144-D Firmware Compatibility Matrix

#### NOTE

Before starting this procedure, you should have already obtained a valid software upgrade file from Ruckus<sup>®</sup> Support or an authorized reseller.

#### NOTE

\* - Additionally 3.6.2 GD in 6.1.1 LT for special requirements is supported. (In general, N-2 GD is only supported in GD release.)

#### NOTE

If you are upgrading both vSZ and vSZ-D/SZ100-D/SZ144-D, Ruckus<sup>\*</sup> recommends upgrading vSZ first before vSZ-D/SZ100-D/SZ144-D.

There is no order in upgrading the AP zone or vSZ-D/SZ100-D/SZ144-D. During the vSZ upgrade, all tunnels stay up except the main tunnel which moves to the vSZ. Once the upgrade procedure is completed, allow ten minutes for the vSZ-D/SZ100-D/SZ144-D to settle.

Upgrade to R5.0 does not support data migration (statistics, events, administrator logs). Existing system and network configuration is preserved. For further clarification, Contact Ruckus support.

Follow these steps to upgrade the vSZ-D/SZ100-D/SZ144-D version.

- 1. Copy the software upgrade file that you received from Ruckus<sup>®</sup> to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
- 2. Go to Controller web interface > Administration > Upgrade.

FIGURE 75 Upgrade Section

<b>#</b>	🐣 Monitor	🚓 Net	work 🛡 Sec	curity Q	C Services	Administration	*	search menu	∨ Q	Administration	• Administration	∪pgrade >	DP Patch
Upgrade	DP Patch	AP Patch	Switch Firmware										
Patch F	ile Upload												
1 U;	pload		ant to use to upgrade the	e DP. Browse									
vSZ-D	SZ100-D	SZ144-D											
	ch File Name	N/A											
Pate	ch File Size	N/A											
Pate	ch Version	N/A											
Data	a Planes												
C	🚯 Backup 🤞	🗈 Restore 🖌	<sup>*</sup> Upgrade to N/A										
	Name		DP MAC Add	iress	Current Firmwar	e Backup Firmware	e La	st Backup Time	Process State	DP Status			

- 3. Select the **DP Patch** tab. The **DP Patch** page appears.
- 4. In the Patch File Upload section, click the Browse button, and then browse to the location of the software upgrade file.

The file name of the software upgrade file for:

- vSZ-D is vdp-{version}.ximg
- SZ100-D is sz100d-installer {version}.ximg
- SZ144-D is sz144d-installer\_{version}.ximg
- 5. Click **Upload** to upload the software upgrade file.

The controller automatically identifies the Type of DP (vSZ-D or SZ100-D or SZ144-D) and switches to the specific Tab page. Uploads the file to its database, and then performs file verification. After the file is verified, the **Patch Available for Upgrade** section is populated with information about the upgrade file.

The following details are displayed:

- Patch File Name: Displays the name of the patch file.
- Patch File Size: Displays the size of the patch file.
- Patch Version: Displays the version of the patch file.
- 6. In Data Planes, identify the data plane you want to upgrade, and then choose a patch file version Upgrade to.
- 7. Click Apply to apply the patch file version to the virtual data plane.

The following information about the virtual data plane is displayed after the patch file upgrade is completed.

- Name: Displays the name of the virtual data plane.
- DP MAC Address: Displays the MAC IP address of the data plane.
- Current Firmware: Displays the current version of the data plane that has been upgraded.
- Backup Firmware: Displays the backup version of the data plane.
- Last Backup Time: Displays the date and time of last backup.
- **Process State**: Displays the completion state of the patch file upgrade for the virtual data plane.
- **DP Status**: Displays the DP status.

You have successfully upgraded the data plane.

- 8. To verify if the upgrade is successful after a reboot:
  - Go to **Controller web interface > Administration > Upgrade > DP Patch** to view a confirmation message that the data plane firmware upgrade is complete.
  - Go to **Controller web interface** > **Network** > **Cluster** to view a confirmation message that the data plane is managed with an upgrade firmware version.

#### NOTE

To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

# **Data Plane Performance Recommendations**

vSZ-D/SZ100-D/SZ144-D has been designed to induce minimal latency in user data aggregation and forwarding. The unique design of the vSZ-D/ SZ100-D/SZ144-D software enables consistent packet performance with minimal throughput degradation as the number of tunnels or the number of clients' increase.

The fast path processing of the vSZ-D/SZ100-D/SZ144-D is engineered to scale to the underlying NIC capacity profiles whether be it 1G or 10G speeds. vSZ-D/SZ100-D/SZ144-D is designed to scale and handle data tunnels and data forwarding capabilities at high scale.

The following are some important observations and recommendations related to the vSZ-D/SZ100-D/SZ144-D performance:

- To obtain the best throughput, Ruckus recommends operating vSZ-D in directIO mode. This recommended mode of operation applies whether the hypervisor used is VMware or KVM.
- vSZ-D supports vSwitch mode of operation for added flexibility in deployments where vSZ-D may be co-located with other VMs for service chaining on the same underlying hardware. Note that the current observations are that in the vSwitch mode of operation, there is an induced performance impact in comparison with the directIO mode of operation. This may be due to the latency or performance bottleneck in virtIO and vSwitch sharing. This is still being researched at the Ruckus R&D Labs.
- There is an expected performance impact when enabling encryption (AES 128 bit and AES 256 bit) on the Ruckus GRE Tunnels. This is due to the overhead induced by the crypto processing on Ruckus AP and vSZ-D/SZ100-D/SZ144-D due to the associated overheads of encryption and decryption on a per packet basis. The vSZ-D/SZ100-D/SZ144-D software is designed to introduce minimal latency and overheads associated in packet processing. vSZ-D/SZ100-D/SZ144-D takes advantage of the underlying Intel chip's crypto module for packet encryption and decryption and the associated impact is primarily bounded at the hardware level.

For specific recommendations and calibrations that may be needed for your deployment, contact Ruckus.



© 2022 CommScope, Inc. All rights reserved. 350 West Java Dr., Sunnyvale, CA 94089 USA https://www.commscope.com