



## **Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Releases 6.1(2)I2(1), 6.1(2)I2(2), 6.1(2)I2(2a), and 6.1(2)I2(2b)**

**First Published:** March 15, 2014

**Last Modified:** August 07, 2014

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### Verified Scalability Limits 1

##### Introduction 1

##### Verified Scalability Limits 1

##### Deployment Case Studies 4

##### Verified Scalability Limits for a Layer 2/Layer 3 Aggregation Topology (Max-Host Routing Mode) 4





# Verified Scalability Limits

This chapter describes the Cisco NX-OS configuration limits for the Cisco Nexus 9000 Series switches.

- [Introduction, page 1](#)
- [Verified Scalability Limits, page 1](#)
- [Deployment Case Studies, page 4](#)

## Introduction

The values provided in this guide should not be interpreted as theoretical system limits for Cisco Nexus 9000 Series hardware or Cisco NX-OS software. These limits refer to values that have been validated by Cisco. They can increase over time as more testing and validation is done.

## Verified Scalability Limits

This table lists the unidimensional verified scalability limits for Cisco NX-OS Releases 6.1(2)I2(1), 6.1(2)I2(2), 6.1(2)I2(2a), and 6.1(2)I2(2b). These limits are validated with a unidimensional configuration. The values provided in these tables focus on the scalability of one particular feature at a time.

Each number is the absolute maximum currently supported by this Cisco NX-OS release for the corresponding feature. If the hardware is capable of a higher scale, future software releases might increase this verified maximum limit. Results might differ from the values listed here when trying to achieve maximum scalability with multiple features enabled.

**Table 1: Verified Scalability Limits (Unidimensional)**

Feature	9500 Series Verified Limit	9300 Series Verified Limit
IPv4 unicast routes (LPM)*	128,000 16,000 (max host mode)	12,000
IPv6 unicast routes (LPM)*	20,000 4000 (max host mode)	6000 (5000 routes < /64, 1000 routes > /64)

Feature	9500 Series Verified Limit	9300 Series Verified Limit
IPv4 host routes**	88,000 60,000 (max host mode)	90,000
IPv6 host routes**	20,000 30,000 (max host mode)	40,000
IPv4 multicast routes**	32,000	8000
Multicast outgoing interfaces (OIFs)	40	40
BGP neighbors	1000	150
OSPFv2 neighbors	1000	200
OSPFv3 neighbors	300	200
IPv4 ingress ACLs	3072 (per network forwarding engine)	3072 (per network forwarding engine)
IPv4 egress ACLs	768 (per network forwarding engine)	768 (per network forwarding engine)
IPv6 ingress ACLs	1536 (per network forwarding engine)	1536 (per network forwarding engine)
IPv6 egress ACLs	256 (per network forwarding engine)	256 (per network forwarding engine)
Configurable SPAN or ERSPAN sessions	32	4
Active SPAN or ERSPAN sessions <sup>1</sup>	4 to 32, based on the number of line cards and the session configuration	4
Active localized SPAN or ERSPAN sessions per line card <sup>2</sup>	4	4
Source interfaces per SPAN or ERSPAN session (Rx and Tx, Rx, or Tx)	48	48
Destination interfaces per SPAN session	1 (physical interface)	1 (physical interface)
Source VLANs per SPAN or ERSPAN session	32	32

Feature	9500 Series Verified Limit	9300 Series Verified Limit
IPv4 ARP	60,000	45,000
IPv6 ND	30,000	20,000
MAC addresses	90,000	90,000
MST virtual ports	85,000	48,000
RPVST virtual ports	22,000	12,000
HSRP groups per interface or I/O module	490	250
VRRP groups per interface or I/O module	250	250
Port channel links	32	8
VLANs	4000	3900
VLANs in RPVST mode	500	500
vPCs***	275	100
SVIs	490	250
MST instances	64	64
VRFs****	1000	500
<b>VXLANs</b>		
Virtual network identifiers (VNIs) or VXLAN-mapped VLANs	Not applicable	640
Overlay multicast groups	Not applicable	128
Overlay MAC addresses	Not applicable	64,000
Remote VXLAN tunnel endpoints (VTEPs)	Not applicable	256

<sup>1</sup> A single forwarding engine instance supports four SPAN or ERSPAN sessions. For Cisco Nexus 9300 Series switches, if the first three sessions have bidirectional sources, the fourth session has hardware resources only for Rx sources. This limitation might also apply to Cisco Nexus 9500 Series switches, depending on the SPAN or ERSPAN source's forwarding engine instance mappings.

<sup>2</sup> The number of SPAN or ERSPAN sessions per line card reduces to two if the same interface is configured as the bidirectional source in more than one session.

\*The IPv4 and IPv6 routes share the same hardware table. Limits are provided for both the default line card mode and the max host line card mode.

\*\*The IPv4/IPv6 host routes and IPv4 multicast routes share the same hardware table. Limits are provided for both the default line card mode and the max host line card mode.

\*\*\*The number of VLANs per vPC supported should be within the MST or RPVST virtual port count specified in this table, depending on the topology.

\*\*\*\*The VRF limits have been tested and verified only for Cisco NX-OS Releases 6.1(2)I2(2a) and 6.1(2)I2(2b).

**Note**

The SPAN and ERSPAN scalability limits have been tested and verified only for Cisco NX-OS Releases 6.1(2)I2(2a) and 6.1(2)I2(2b). For Cisco NX-OS Releases 6.1(2)I2(1) and 6.1(2)I2(2), 32 local SPAN sessions and 4 system SPAN sessions have been tested and verified for the Cisco Nexus 9500 Series switches and 4 SPAN sessions have been tested and verified for the Cisco Nexus 9300 Series switches.

**Note**

High availability (graceful restart and stateful switchover) is not supported when unicast or multicast aggressive timers are configured at any scale.

**Guidelines and Limitations for OSPF Verified Scalability Limits**

- To achieve the highest scale, we recommend that you use a single OSPF instance instead of multiple instances.
- Each OSPFv2 and OSPFv3 scale value might vary when combined with other parameters.
- The graceful restart timeout value might need to be increased in multi-dimensional scenarios.

## Deployment Case Studies

This section provides sample topologies for some common deployments. For each topology, the scalability numbers are the limits with all of the listed features enabled at the same time.

**Attention**

These numbers are not the maximum verified values if each feature is viewed in isolation. For these numbers, see [Verified Scalability Limits, on page 1](#).

## Verified Scalability Limits for a Layer 2/Layer 3 Aggregation Topology (Max-Host Routing Mode)

This Layer 2/Layer 3 aggregation topology consists of Cisco Nexus 9508 switches as virtual port channel (vPC) aggregation pairs. These aggregation nodes are fully loaded with N9K-X9564TX, N9K-X9564PX, and N9K-X9636PQ line cards. The N9K-X9636PQ line cards are used in normal mode and breakout mode. Cisco



Nexus 9396PX and 93128TX switches are used as top-of-rack units with Cisco Nexus 3000 Series switches to achieve the desired vPC scale.

The Cisco Nexus 9508 switch is also used as a core Layer 3 node that connects to a pair of vPC aggregation nodes. The focus of the topology is to test IPv4 ARP, IPv6 neighbor discovery (ND), and Layer 2 scalability and other routing, switching, and Layer 4 through Layer 7 features for management and operations. All Layer 3 interfaces are configured for dual stack, and the traffic is dual stack for all VLANs.

In the following table, the Verified Limit column lists the verified scaling capabilities with all listed features enabled at the same time. The scale numbers listed here exceed those used by most customers in their topologies. These numbers are not the maximum verified values if each feature is viewed in isolation.

**Table 2: Verified Scalability Limits for a Layer 2/Layer 3 Aggregation Topology (Max-Host Routing Mode)**

Feature	9500 Series Verified Limit (Max-Host Routing Mode)	9300 Series Verified Limit
Fully loaded chassis	6 N9636PQ line cards + 1 N9564TX line card + 1 N9564PX line card + 6 fabric modules + 2 system controllers + 2 supervisors	Not applicable
Physical interfaces enabled	300	Not applicable
Multicast S,G routes	12,000	Not applicable
Multicast *,G routes	3400	Not applicable
IPv4 unicast routes (LPM)	2400	2200
IPv6 unicast routes (LPM)	2200	2200
IPv4 ARP	60,000	5000
IPv6 ND	30,000	5000
MAC addresses	90,000	72,000
VLANs	500 (RPVST)	3900 (MST)
vPCs*	275	100
OSPFv2 neighbors	16	200
OSPFv3 neighbors	16	200
BGP (IPv4) neighbors	64 (eBGP)	150 (iBGP)
BGP (IPv6) neighbors	64 (eBGP)	150 (iBGP)
SVIs	490	250
MST instances	Not applicable	64

Feature	9500 Series Verified Limit (Max-Host Routing Mode)	9300 Series Verified Limit
HSRP VLANs (IPv4/IPv6)	490	250
Virtual ports	3000 (RPVST)	24,000 (MST)
Port channel links	32	8

\* The number of VLANs per vPC supported should be within the MST or RPVST virtual port count specified in this table, depending on the topology.