Cisco Nexus 3164Q NX-OS Verified Scalability Guide, Releases 6.1(2)I3(4) and 6.1(2)I3(4a)

First Published: 2015-03-15

Last Modified: 2015-05-18

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

CONTENTS

Preface

This preface includes the following sections:

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Documentation Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.

Convention	Description
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Documentation Feedback

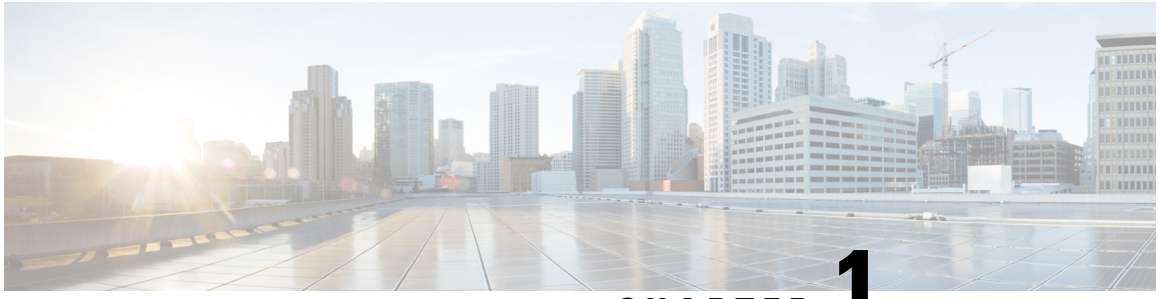
To provide technical feedback on this document, or to report an error or omission, please send your comments to . We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

Verified Scalability Limits

This chapter describes the Cisco NX-OS configuration limits for the Cisco Nexus 3164Q switch.

Introduction

The values provided in this guide should not be interpreted as theoretical system limits for Cisco Nexus 3164Q 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 (Unidimensional)

The tables in this section list the unidimensional verified scalability limits for Cisco NX-OS Releases 6.1(2)I3(4) and 6.1(2)I3(4a) on the Cisco Nexus 3164Q switch. 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: Interfaces Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
BFD sessions	250
Generic routing encapsulation (GRE) tunnels	8
Port channel links	32
SVIs	250
vPCs	60

Table 2: Layer 2 Switching Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
MST instances	64
MST virtual ports	48,000
RPVST virtual ports	12,000
VLANs	3900
VLANs in RPVST mode	500

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

Table 3: Multicast Routing Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
IPv4 multicast routes	32,000
Outgoing interfaces (OIFs)	40 (see CSCum58876)
IGMP snooping groups	32,000
PIM neighbors	250

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

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

Table 4: Security Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
IPv4 ingress ACLs	3070 (per network forwarding engine)
IPv4 egress ACLs	765 (per network forwarding engine)
IPv6 ingress ACLs	1530 (per network forwarding engine)
IPv6 egress ACLs	250 (per network forwarding engine)

Note The ACL scalability limits also apply to policy-based ACLs (PBACLs).

Table 5: System Management Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
Configurable SPAN or ERSPAN sessions	4
Active SPAN or ERSPAN sessions[1]	4
Active localized SPAN or ERSPAN sessions per line card[2]	4
Source interfaces per SPAN or ERSPAN session (Rx and Tx, Rx, or Tx)	48
Destination interfaces per SPAN session	1 (physical interface)
VLAN sources per SPAN or ERSPAN session	32

1 A single forwarding engine instance supports four SPAN or ERSPAN sessions. If the first three sessions have bidirectional sources, the fourth session might have hardware resources only for Rx sources, depending on the SPAN or ERSPAN source's forwarding engine instance mappings.

2 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.

Table 6: Unicast Routing Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
eBGP	1000
HSRP groups per interface or I/O module	250
IPv4 ARP	48,000
IPv4 host routes	88,000
IPv6 host routes	20,000
IPv6 ND	30,000
IPv4 unicast routes (LPM)	128,000
IPv6 unicast routes (LPM)	16,000
MAC addresses	80,000
OSPFv2 neighbors	200
OSPFv3 neighbors	200
VRRP groups per interface or I/O module	250

Feature	3164Q Verified Limit
VRFs	1000
Policy-based routing (PBR)	
Number of configured sequences per policy	256
Number of next-hop addresses per policy	32
Number of IPv4 ACEs (unidimensional)	3072 (per network forwarding engine)
Number of IPv6 ACEs (unidimensional)	1536 (per network forwarding engine)
Number of IPv4 and IPv6s ACEs	2048 IPv4 + 256 IPv6
Number of interfaces with PBR policy	512

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

Note The IPv4/IPv6 host routes and the 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.

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 multidimensional scenarios.

Table 7: VXLAN Verified Scalability Limits (Unidimensional)

Feature	3164Q Verified Limit
Virtual network identifiers (VNIs) or VXLAN-mapped VLANs	1000
Overlay multicast groups	128
Overlay MAC addresses	64,000
Remote VXLAN tunnel endpoints (VTEPs)	256