

Send feedback to nexus4k-docfeedback@cisco.com



Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Release Notes, Release 4.1(2)E1(1i)

Date: July 5, 2012

Part Number: OL-20701-09 A0

This document describes the features, caveats, and limitations for Cisco NX-OS software for use on the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter. Use this document in combination with the documents listed in the “[Related Documentation](#)” section on page 11.



Note

Release notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Release Notes*:

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Table 1 shows the online change history for this document.

Table 1 Online History Change

Part Number	Revision	Date	Description
OL-20701-09	A0	July 5, 2012	Created release notes for Cisco NX-OS Release 4.1(2)E1(1i).
OL-20701-08	A0	February 20, 2012	Created release notes for Cisco NX-OS Release 4.1(2)E1(1h).
OL-20701-07	A0	August 22, 2011	Created release notes for Cisco NX-OS Release 4.1(2)E1(1g).
OL-20701-06	A0	November 15, 2010	Created release notes for Cisco NX-OS Release 4.1(2)E1(1f).
OL-20701-05	A0	August 6, 2010	Created release notes for Cisco NX-OS Release 4.1(2)E1(1e).



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2009–2012 Cisco Systems, Inc. All rights reserved.

Send feedback to nexus4k-docfeedback@cisco.com

Table 1 **Online History Change (continued)**

Part Number	Revision	Date	Description
OL-20701-04	A0	June 11, 2010	Created release notes for Cisco NX-OS Release 4.1(2)E1(1d).
OL-20701-03	A0	May 14, 2010	Created release notes for Cisco NX-OS Release 4.1(2)E1(1c).
OL-20701-02	A0	December 18, 2009	Created release notes for Cisco NX-OS Release 4.1(2)E1(1b).
OL-20701-01	A0	October 15, 2009	Created release notes for Cisco NX-OS Release 4.1(2)E1(1).

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Upgrade/Downgrade Caveats, page 6](#)
- [New Software Features, page 6](#)
- [Limitations, page 7](#)
- [Caveats, page 9](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation and Submitting a Service Request, page 11](#)

Introduction

The Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter (also referred to in this document as the *switch*) is a Layer 2 device, which runs Cisco NX-OS. The Cisco NX-OS Release 4.1(2)E1(1i) software supports the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter including certain features that are specific to the product. The Cisco NX-OS software also interoperates with any networking operating system that conforms to the IEEE and RFC compliance standards.

The switch is a 10/1-Gb Ethernet switch for the IBM BladeCenter chassis. The switch offers a solution in high-end data centers where server virtualization and I/O consolidation are required.

System Requirements

This section includes the following topics:

- [Memory Requirements, page 3](#)
- [Hardware Supported, page 3](#)
- [Software Compatibility, page 3](#)

Send feedback to nexus4k-docfeedback@cisco.com

Memory Requirements

The Cisco NX-OS software requires 2 GB of memory.

Hardware Supported

The Cisco NX-OS software supports the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter. You can find detailed information about supported hardware in the *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter Hardware Installation Guide*.

Software Compatibility

This section briefly describes the salient features supported in Cisco NX-OS Release 4.1(2)E1(1i) for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter. For detailed information about the features listed, see the documents listed in the “[Related Documentation](#)” section on page 11.

The Cisco NX-OS software provides a unified operating system that is designed to run all areas of the data center network including the LAN and Layer 4 through Layer 7 network services.

The Cisco NX-OS software also supports distributed multithreaded processing on symmetric multiprocessors (SMPs), multi-core CPUs, and distributed data module processors. The Cisco NX-OS software offloads computationally intensive tasks, such as hardware table programming, to dedicated processors distributed across the data modules. The modular processes are created on demand, each in a separate protected memory space. Processes are started and system resources are allocated only when you enable a feature. A real-time preemptive scheduler helps to ensure the timely processing of critical functions.

This section describes the key Cisco NX-OS software and includes the following topics:

- [Serviceability, page 3](#)
- [Manageability, page 4](#)
- [Traffic Routing, Forwarding, and Management, page 5](#)
- [FCoE Initialization Protocol, page 5](#)
- [Quality of Service, page 5](#)
- [Network Security Features, page 5](#)

Serviceability

The Cisco NX-OS software has serviceability functions that allow the device to respond to network trends and events. These features help you with network planning and improving response times.

This section includes the following topics:

- [Switched Port Analyzer, page 4](#)
- [Ethanalyzer, page 4](#)
- [Call Home, page 4](#)
- [Online Diagnostics, page 4](#)

[Send feedback to nexus4k-docfeedback@cisco.com](mailto:nexus4k-docfeedback@cisco.com)

Switched Port Analyzer

The Switched Port Analyzer (SPAN) feature allows you to analyze all traffic between ports (called the SPAN source ports) by nonintrusively directing the SPAN session traffic to a SPAN destination port that has an external analyzer attached to it.

Ethalyzer

Ethalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethalyzer is a command-line version of Wireshark for capturing and decoding packets. You can use Ethalyzer to troubleshoot your network and analyze the control-plane traffic.

Call Home

The Call Home feature continuously monitors hardware and software components to provide e-mail-based notification of critical system events. A versatile range of message formats is available for optimal compatibility with pager services, standard e-mail, and XML-based automated parsing applications. It offers alert grouping capabilities and customizable destination profiles. You can use this feature, for example, to directly page a network support engineer, send an e-mail message to a network operations center (NOC), and employ Cisco AutoNotify services to directly generate a case with the Cisco Technical Assistance Center (TAC).

Online Diagnostics

The Online Health Management System (OHMS) is a hardware fault detection and recovery feature. It ensures the general health of the switch.

Manageability

This section includes the following topics:

- [Simple Network Management Protocol, page 4](#)
- [Role-Based Access Control, page 4](#)
- [Cisco NX-OS Device Configuration Methods, page 4](#)

Simple Network Management Protocol

The Cisco NX-OS software is compliant with Simple Network Management Protocol (SNMP) version 1, version 2, and version 3. A large number of MIBs is supported.

Role-Based Access Control

With role-based access control (RBAC), you can limit access to device operations by assigning roles to users. You can customize access and restrict it to the users who require it.

Cisco NX-OS Device Configuration Methods

You can configure devices using the CLI from a Secure Shell (SSH) session or a Telnet session. SSH provides a secure connection to the switch. You can also configure devices using the XML management interface, which is a programmatic method based on the NETCONF protocol that complements the CLI.

Send feedback to nexus4k-docfeedback@cisco.com

Traffic Routing, Forwarding, and Management

This section includes the following topics:

- [Ethernet Switching, page 5](#)
- [IP Multicast, page 5](#)

Ethernet Switching

The Cisco NX-OS software supports high-density, high-performance Ethernet systems and provides the following Ethernet switching features:

- IEEE 802.1D-2004 Rapid and Multiple Spanning Tree Protocols (802.1w and 802.1s)
- IEEE 802.1Q VLANs and trunks
- 512-subscriber VLANs
- IEEE 802.3ad link aggregation
- Private VLANs
- Unidirectional Link Detection (UDLD) in aggressive and standard modes

IP Multicast

The Cisco NX-OS includes the following multicast protocols and functions:

- Internet Group Management Protocol (IGMP) Versions 1, 2, and 3 router role
- IGMPv2 host mode
- IGMP snooping

FCoE Initialization Protocol

The Cisco NX-OS supports the FIP snooping bridge feature. The switch operates as a loss-less Ethernet bridge transparently forwarding FCoE packets.

Quality of Service

The Cisco NX-OS quality of service (QoS) support allows you to classify the network traffic, police and prioritize the traffic flow, and provide congestion avoidance.

Network Security Features

Cisco NX-OS includes the following security features:

- Authentication, authorization, and accounting (AAA)
- RADIUS and TACACS+
- SSH Protocol Version 2
- SNMPv3
- Policies based on MAC and IPv4 addresses supported by named ACLs (port-based ACLs [PACLs], VLAN-based ACLs [VACLs])
- Traffic storm control (unicast, multicast, and broadcast)

Send feedback to nexus4k-docfeedback@cisco.com

Upgrade/Downgrade Caveats

Upgrades and downgrades between Cisco NX-OS Release 4.1(2)E1(1i), Cisco NX-OS Release 4.1(2)E1(1h), Cisco NX-OS Release 4.1(2)E1(1g), Cisco NX-OS Release 4.1(2)E1(1f), Cisco NX-OS Release 4.1(2)E1(1e), Cisco NX-OS Release 4.1(2)E1(1d), Cisco NX-OS Release 4.1(2)E1(1b), and Cisco NX-OS Release 4.1(2)E1(1) will preserve configurations. However, an upgrade or downgrade will be disruptive.

There are no upgrade or downgrade caveats for Cisco NX-OS Release 4.1(2)E1(1i).

New Software Features

Cisco NX-OS Release 4.1(2)E1(1i) for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter has the following new software features.

This section includes the following topics:

- [ACL on VTY Line/SNMP-Server, page 6](#)

ACL on VTY Line/SNMP-Server

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.

Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol (UDP or TCP)

Use the following command in global configuration mode to assign an ACL to a community to filter SNMP requests:

Command	Purpose
<code>snmp-server community community-name</code> <code>use-acl acl-name</code> Example: <code>switch(config)# snmp-server community</code> <code>public use-acl my_acl_for_public</code>	Assigns an ACL to an SNMP community to filter SNMP requests.

Send feedback to nexus4k-docfeedback@cisco.com

Limitations

This section describes the limitations in Cisco NX-OS Release 4.1(2)E1(1i) for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter.

This section includes the following caveats:

- CSCsy59059

Symptom: If you configure a switch with the **switchport block unicast** command or the **switchport block multicast** command, the commands have no effect.

Conditions: You may see this symptom because the switch does not support the **switchport block unicast** command or the **switchport block multicast** command.

Workaround: Use the **storm-control unicast level 100.00** command or the **storm-control multicast level 100.00** command instead.

- CSCsz85289

Symptom: It is not possible to resequence rules in a VACL.

Conditions: You may see this symptom when you attempt to resequence VACLs. Once the rules are added to a VACL in a sequence, you cannot change the sequence.

Workaround: Delete the entire set of rules in the VACL, and add them again.

If there is a VACL as in the following example, it is not possible to resequence the VACL matching IP ACL to 10 and VACL matching MAC ACL to 20:

```
switch(config)# vlan access-map vlan1 10
switch(config-access-map)# match mac address mac1
switch(config-access-map)# action forward
switch(config-access-map)# statistics per-entry

switch(config)# vlan access-map vlan1 20
switch(config-access-map)# match ip address ip1
switch(config-access-map)# action drop
switch(config-access-map)# statistics per-entry
```

Use a simple CLI for the workaround as follows:

```
switch(config)# vlan access-map vlan1 10
switch(config-access-map)# no match mac address mac1
switch(config-access-map)# no action forward
switch(config-access-map)# match ip address ip1
switch(config-access-map)# action drop
switch(config-access-map)# exit

switch(config)# vlan access-map vlan1 20
switch(config-access-map)# no match ip address ip1
switch(config-access-map)# no action drop
switch(config-access-map)# match mac address mac1
switch(config-access-map)# action forward
switch(config-access-map)# exit
```

- CSCta26017

Symptom: The bandwidth allocation does not work accurately if the egress traffic for a CoS is only multicast.

Conditions: You may see this symptom when the multicast traffic is to be transmitted on multiple ports. The symptom only occurs if destination ports are in the same port group.

Send feedback to nexus4k-docfeedback@cisco.com

Workaround: Distribute the destination ports among different port groups. Use the command **show hardware internal ele-fwd driver-info** to locate the front port and ASIC port mapping. There are four port groups in our system: (0–4), (5–9), (10–14), and (15–19). The numbering is indicated in terms of the ASIC ports in the output following the command.

- CSCta28309

Symptom: Actions on a VACL with no rules affect the traffic matching credible VACL rule.

Conditions: A single VLAN access map can have different actions for different ACLs. The commands used to configure it are as follows:

```
switch(config)# vlan access-map vac11 10
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-one
switch(config-access-map)# vlan access-map vac11 20
switch(config-access-map)# action drop
switch(config-access-map)# match mac address mac-acl-two
switch(config-access-map)# vlan access-map vac11 30
switch(config-access-map)# action redirect eth1/10
switch(config-access-map)# match mac address mac-acl-three
```

The three VACLs in the preceding example are part of one VLAN access map. Any change to any one of the access maps will result in reprogramming the entire access map (of all the sequence numbers). The reprogramming might result in traffic disruption.

Workaround: To prevent traffic disruption, define the VLAN access map in separate VLAN access maps (with different names).

- CSCta48031

Symptom: Outgoing CPU-generated traffic cannot be spanned.

Conditions: You may see this symptom when an interface is configured as a source port of a SPAN session (transmit only or transmit and receive). The CPU generated traffic could be for SoL, CDP, STP, and so on.

Workaround: No workaround is available.

- CSCtb40514

Symptom: The switch can be configured with the same IP address by using the front panel management port mgmt 0, and using the alarm maintenance and management (AMM) module on the management port mgmt 1. This configuration is not considered an error, and both interfaces remain operational.

Conditions: You may see this symptom when you configure the same IP address on management port mgmt 0 and management port mgmt 1.

Workaround: Do not configure the same IP address on management port mgmt 0 and management port mgmt 1.

- CSCtb68736

Symptom: Users see a “port not compatible [speed]” error message while adding the downlink ports to a port channel.

Conditions: You may see this symptom under the default configuration setting, when a downlink port is added as a member of port channel interface.

Workaround: Enter the **speed 10000** command on the member port before adding it to the port-channel interface. Because the **show interface brief** command displays the running speed of the downlink port, there may be some confusion in identifying the mismatch in speed. The default speed for the downlink interface is auto which does not match the default speed of the port channel interface which is 10 G.

Send feedback to nexus4k-docfeedback@cisco.com

- CSCtb99418
Symptom: If you configure a switch port speed to auto by entering the **speed auto** command under the **interface** subcommand, the port may not link up.
Conditions: You may see this symptom when the blade server has the NetXen NIC installed.
Workaround: Configure the port speed to 10 G by entering the **speed 10000** command.
- CSCtc01560
Symptom: A monitor port cannot be the destination port for more than one SPAN session.
Conditions: You may see this symptom when the destination port of one session is configured as the destination port for the second session.
Workaround: No workaround is available.
- CSCtx66246
Symptom: Login attempt fails.
Conditions: Whenever a username of all uppercase letters is used with a serial port connection, the login fails. The first time you attempt to log in, you see the “LOGIN INCORRECT” message. When you enter the information again, the login succeeds.
Workaround: If you have a username with all uppercase letters, it may take you two attempts to log in to the switch when using a serial port connection. You can use an out-of-band mechanism such as Telnet or SSH to log in without any failures.

Caveats

This section describes caveats and includes the following topics:

- [Open Caveats, page 9](#)
- [Resolved Caveats, page 10](#)

Open Caveats

This section describes the open caveats in Cisco NX-OS Release 4.1(2)E1(1i) for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter.

This section includes the following open caveats:

- CSCtr57523
Symptom: The **ntp sync-retry** command is not handled properly on the Cisco Nexus 4000 Series switch. The NTPD service restart fails, which results in the failure of other **ntp** commands.
Conditions: After you configure a time server, manual synchronizing with the server using the **ntp sync-retry** command fails on the Cisco Nexus 4000 Series switch.
Workaround: To resynchronize with any peer or time server, remove the existing ntp server configuration and reinitialize it. The commands used to initialize it are as follows:

```
switch(config)# no ntp server ip-address
switch(config)# ntp server ip-address
```
- CSCtx03250
Symptom: When the SNMP ACL configuration is deleted, the following error message is generated:

Send feedback to nexus4k-docfeedback@cisco.com

%VSHD-2-VSHD_SYSLOG_EOL_ERR: EOL function cli_snmp_server_config from library

Conditions: This symptom occurs when the command to delete the SNMP ACL configuration is entered twice. For example, if the following command is entered multiple times, the duplicate sequence will give an error.

```
switch(config)# no snmp-server community public use-acl my_acl_for_public
```

Workaround: No workaround is available.

- CSCua84146

Symptom: Cisco Nexus 4001I switch modules continually restarting after upgrade.

Conditions: This symptom occurs after updating to Cisco NX-OS Release 4.1(2)E1(1h) on Cisco Nexus 4001I switch modules that are connected to IBM BladeCenter PS704 blades.

Workaround: Shut down the interfaces connecting the Cisco Nexus 4001I to the IBM BladeCenter PS704 before the blades are shut down or restarted.

Resolved Caveats

All the caveats listed in this section are resolved in Cisco NX-OS Release 4.1(2)E1(1i) for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter.

This section includes the following caveats:

- CSCty29199

Symptom: Spanning Tree disputes occur after enabling IPv6 on multiple Cisco Nexus 4000 Series switches.

Conditions: This symptom occurs when IPv6 is enabled, and multiple Cisco Nexus 4000 Series switches are present on the same subnet running IPv6.

Workaround: This issue is resolved.

- CSCty66618

Symptom: FIP snooping stops working.

Conditions: Approximately 30 minutes after the FIP snooping configuration is enabled on the Cisco Nexus 4000 Series switch, the sessions stop working.

Workaround: Set the tunable pause rate threshold to disable the server port interface for a faulty Converged Network Adapter (CNA) to ensure FIP snooping sessions remain intact. See CSCtz14520 for more information.

- CSCtz14520

Symptom: FIP sessions on the uplink ports go down, causing a loss of connectivity to the storage. This problem is due to a faulty Converged Network Adapter (CNA) that is incorrectly generating pause frames. The Cisco Nexus 4000 Series switch receives the pause frames and stops processing FIP. The previous pause threshold limit of 1000 pps to error disable the server port interface was too high to prevent the FIP sessions from going down.

Conditions: A server in the chassis is generating excessive pause frames. This problem is usually caused by a faulty CNA issue in the server.

Workaround: A tunable pause frame threshold was added which allows you to set a value from 100 pps to 1000 pps. This tuning error disables the switchport that is connected to the faulty CNA and prevents the FIP sessions from going down. The commands used to tune the pause frame threshold are as follows:

Send feedback to nexus4k-docfeedback@cisco.com

```
switch(config)# hardware internal ele-fwd pause-rate ?
<100-1000> Specify pause frame rate value (pps)
switch(config)# show hardware internal ele-fwd pause-rate
```

- CSCtz14625

Symptom: CDP related crash occurs on a Cisco Nexus 4000 Series switch.

Conditions: A memory leak occurs when the CDP protocol process receives CDP packets running Cisco NX-OS Release 4.1(2)E1(1h). The memory leak affects the process memory limits and the node resets due to the CDP process High Availability (HA) policy.

Workaround: This issue is resolved.

Related Documentation

Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

The following are related documents:

- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*
- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Configuration Guide*
- *Cisco NX-OS System Messages Reference*
- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter Getting Started Guide*
- *Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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: 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)

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.

Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter NX-OS Release Notes, Release 4.1(2)E1(1i)
© 2009–2012 Cisco Systems, Inc. All rights reserved.

Send feedback to nexus4k-docfeedback@cisco.com