

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

**Date: August 9, 2011**
**Part Number: OL-20701-07 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 12.

**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-20701-01 | A0 | October 15, 2009 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1). |
| OL-20701-02 | A0 | December 18, 2009 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1b). |

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

*Table 1 Online History Change (continued)*

| Part Number | Revision | Date | Description |
|---|---|---|---|
| OL-20701-03 | A0 | May 14, 2010 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1c). |
| OL-20701-04 | A0 | June 11, 2010 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1d). |
| OL-20701-05 | A0 | August 6, 2010 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1e). |
| OL-20701-06 | A0 | November 15, 2010 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1f). |
| OL-20701-07 | A0 | August 09, 2011 | Created release notes for Cisco NX-OS Release 4.1(2)E1(1g). |

# Contents

This document includes the following sections:



# 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(1g) 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

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(1g) 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 12.

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

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

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.

### Ethanalyzer

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethanalyzer is a command-line version of Wireshark for capturing and decoding packets. You can use Ethanalyzer 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

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.

## Traffic Routing, Forwarding, and Management

This section includes the following topics:



### 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)

# Upgrade/Downgrade Caveats

Upgrades and downgrades between 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(1g).

# New Software Features

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

This section includes the following topics:



## TACACS+ Command Authorization

The Cisco NX-OS Terminal Access Controller Access Control System Plus (TACACS+) command authorization support allows you to configure authorization for commands on TACACS+ servers. Command authorization determines whether a given command is allowed for use in a TACACS+ session. By default, command authorization is done against a local database in the Cisco NX-OS software when an authenticated user enters a command at the command-line interface (CLI).

# Limitations

This section describes the limitations in Cisco NX-OS Release 4.1(2)E1(1g) 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.

  **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 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 follows:

```
switch(config)# vlan access-map vacl1 10
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-one
switch(config-access-map)# vlan access-map vacl1 20
switch(config-access-map)# action drop
switch(config-access-map)# match mac address mac-acl-two
switch(config-access-map)# vlan access-map vacl1 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 (the direction being 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 on the front panel management port mgmt 0 and using the AMM on the management port mgmt 1. This configuration is not considered an error and both the 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. As 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".

- CSCtb99418

  **Symptom**: If you configure a switch port speed to auto by entering the **speed auto** command under the **interface** sub-command, 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.

# Caveats

This section describes caveats and includes the following topics:

# Open Caveats

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

This section includes the following open caveats:

- CSCsz81239

  **Symptom**: The version of the Network Time Protocol (NTP) software used on the switch is 4.2.0a. Therefore, it is vulnerable to CVE-2009-0159.

  **Conditions**: This symptom occurs when you operate the switch.

  **Workaround**: No workaround is available.

- CSCta41968

  **Symptom**: The SSH becomes disabled while applying the “ssh key rsa 2048” line after a reload.

  **Conditions**: You may see this symptom upon reloading, when the ASCII configuration containing the line “ssh key rsa 2048” is copied to the running configuration.

  **Workaround**: If you lose access to the switch, use the serial console to enable it.

- CSCtb28328

  **Symptom**: FIP sessions do not come up even though it appears as though enabling FIP snooping on a VLAN has succeeded when the ACL table is full.

  **Conditions**: You may see this symptom because the ACL table is full and attempts to install ACLs when FIP is enabled on a VLAN fail.

  **Workaround**: Whenever it is possible to do so, reduce the number of ACLs in use, save the configuration, and reload.

- CSCtb99161

  **Symptom**: Whenever a type qos policy is applied on a port channel, the show commands do not show that policy on the member interfaces of that port channel.

  **Conditions**: You may see this symptom when a type qos policy is applied on a port channel and you type a show command to show that policy.

  **Workaround**: In the hardware, the policy is applied correctly to the member interfaces, and whenever a policy is applied on a port channel, any existing policy on the member interface is overridden by the policy on the port channel.

- CSCth14602

  **Symptom**: When the user disables the external management from AMM, all the switch virtual interfaces (SVIs) on the switch are disabled.

  **Conditions**: This symptom occurs when SVIs configured on the switch are administratively brought up from the CLI and enabled from AMM. If users want to disable the SVIs later, they must do so using the AMM or the switch CLI. If the user disables external management using AMM, and then reloads the switch, this configuration is lost and the SVIs are enabled on the switch.

  **Workaround**: To permanently disable external management, always disable SVIs from the CLI using the **interface vlan** CLI commands.

# Resolved Caveats

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

This section includes the following caveats:

- CSCti40356

  **Symptom:** In a virtual port channel (vPC) topology where a switch is connected to two Cisco Nexus 5000 Series switches, when you reboot the primary Cisco Nexus 5000 Series switch, the port channel link connected to the switch is placed in the error disabled (err-disabled) state.

  **Conditions:** This symptom occurs when you reload the primary Cisco Nexus 5000 Series switch.

  **Workaround:** Use the **shutdown** command, and then the **no shutdown** command on the port of the Cisco Nexus 4000 switch that connects to the vPC.

- CSCtj47111

  **Symptom:** The switch stops forwarding traffic for one or more multicast groups.

  **Conditions:** This symptom occurs when IGMP snooping is enabled on the switch.

  **Workaround:** Do one of the following:

  - Remove and reapply IGMP snooping.
  - Flap a non-edge interface to generate a Spanning-Tree Protocol (STP) topology change notification (TCN) flag.

- CSCtj66065

  **Symptom:** On a switch in an IBM server chassis, the internal connection to a server might come up at 1–Gigabit speed rather than at 10–Gigabit speed.

  **Conditions:** You may see this symptom on a switch that runs Cisco NX-OS Release 4.1(2)E1(1e) using interface auto-negotiation, or after a server reboot.

  **Workaround:** Do the following:

  - If you see the problem only when the interfaces are auto negotiating, configure the speed of the interfaces by using the **speed** *x* command.
  - If the problem appears when the switch uses auto-negotiation, shut down the interface that has come up at come up at 1–Gigabit speed and then bring the interface up.

- CSCtk04651

  **Symptom:** If you reload or upgrade a switch that has the link-state tracking (LST) feature enabled with the server interfaces shut down, the server interfaces come up momentarily after the reload.

  **Conditions:** This behavior is noticed on the server interfaces of a switch that has the LST feature enabled.

  **Workaround:** Disable LST on the switch. Server interfaces remain shut down if the LST feature is disabled on the switch.

- CSCtk53995

  **Symptom:** Port channel bounces on a Cisco Nexus 7000 or Cisco Nexus 5000 primary switch and the port on the Cisco Nexus 4000 switch that connects the virtual port channel (vPC) secondary switch is placed in the error disabled (err-disabled) state.

  **Conditions:** This behavior is noticed in the following situations:

  - vPC connections between Cisco Nexus 7000 or Cisco Nexus 5000 switch and a Cisco Nexus 4000 switch.
  - Port channel uses the Link Aggregation Control Protocol (LACP) as the negotiation protocol.
  - When you reload a vPC secondary switch.

  **Workaround:** Set the port channel mode of the interface to **on** for the port channel between the vPC pair and the Cisco Nexus 4000 switch.

- CSCtl21341

  **Symptom:** Spanning tree topology change notification (TCN) counters return to zero after 59:59:59 in the output of the **show spanning-tree detail** command.

  **Conditions:** This behavior is noticed under normal working conditions.

  **Workaround:** This issue is resolved in Cisco NX-OS Release 4.1(2)E1(1g).

- CSCtn63567

  **Symptom:** When you shut down and reload a management interface (mgmt 0), the SNMP Link state down (linkDown) or Link state up (linkUp) traps are not sent out for any interface.

  **Conditions:** You may see this symptom only when the management interface (mgmt 0) is shut down and the chassis reloaded.

  **Workaround:** After you power cycle the system, use the **no shutdown** command on the management interface to bring the interface up, and then use the **shutdown** command if the interface needs to be shut down.

- CSCto45255

  **Symptom:** TACACS+ is sending timestamps in the start_time and stop_time records as STRING values instead of LONG INT representing epoch time since Jan 1 1970.

  **Conditions:** You may see this symptom on a switch that has TACACS+ feature enabled with per command authorization enabled on the TACACS+ server.

  **Workaround:** This issue is resolved in Cisco NX-OS Release 4.1(2)E1(1g).

- CSCto95499

  **Symptom:** After you reload the switch and apply the running configuration from a file that has the previously saved configuration, some modules, such as DNS and quality of service (QoS) Manager commands, are configured incorrectly.

  **Conditions:** This behavior is noticed when you copy the running configuration to a file, then reload the switch, and then copy the configuration from the file.

  **Workaround:** You must reconfigure the commands.

- CSCtq13164

  **Symptom:** When a switch is discovered or managed by the Cisco Data Center Network Manager (DCNM) client, the following error message will appear in the logs:

  ```
  %XMLMA-3-XMLMAERR: XML master agent: XML subagent session 5066 terminated, may be
  crashed or killed.
  ```

  The DCNM client cannot manage the switch.

  **Conditions:** You may see this symptom on a switch that runs Cisco NX-OS Release 4.1(2)E1(1f) and managed by the DCNM client.

  **Workaround:** Do not monitor the switch with the DCNM client.

- CSCtq43808

  **Symptom:** A Cisco Nexus 4000 switch in an IBM blade chassis that runs Cisco NX-OS Release 4.1(2)E1(1f) does not allow an user to configure IPv6 trap receiver as a destination.

  ```
  switch(config)# snmp-server host x::y traps version 2c public
  Invalid hostname or IPv4 address.
  ```

  **Conditions:** This behavior is noticed when a switch is configured to be managed using IPv6.

  **Workaround:** Use an IPv4 trap receiver.

- CSCtq71652

  **Symptom:** Servers in an IBM chassis with a Cisco Nexus 4000 switch lose the storage path and generates excessive Rx Pause frames that prevents the switch to process Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP).

  **Conditions:** This symptom occurs when a server in the chassis generates excessive Rx Pause frames. This is usually a Converged Network Adapter (CNA) issue in the server.

  **Workaround:** Run the **show interface flowcontrol** command few times to determine the server interface that is causing **Rx Pause** on the Cisco Nexus 4000 switch, and then investigate the reason the server or CNA is generating the pause frames. Alternatively, shut down the specific server interface that generated the pause frames.

- CSCtq85059

  **Symptom:** When a switch is discovered or managed by Cisco Data Center Network Manager (DCNM) client, the following error message appear in the logs:

  ```
  %SYSMGR-2-SERVICE_CRASHED: Service "AAA Daemon" (PID 2515) hasn't caught signal 11
  (core will be saved).
  ```

  The DCNM client cannot manage the switch.

  **Conditions:** You may see this symptom on a switch that runs Cisco NX-OS Release 4.1(2)E1(1f) and managed by the DCNM client.

  **Workaround:** Do not monitor the switch with the DCNM client.

- CSCtq90610

  **Symptom:** SNMP trap configuration fails when user copies and pastes the configuration.

  **Conditions:** You may see this symptom on a switch that runs Cisco NX-OS Release 4.1(2)E1(1f) and has the SNMP trap receiver configured to use a specific virtual routing and forwarding (VRF) instance.

  **Workaround:** Configure SNMP trap by using the **snmp-server host** *x.x.x.x* **use_vrf** {**management** | **default**} command.

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