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

Date: February 21, 2013
Part Number: OL-20701-10 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-20701-10	A0	February 21, 2013	Created release notes for Cisco NX-OS Release 4.1(2)E1(1j).
OL-20701-09	A0	July 12, 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).

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-20701-05	A0	August 6, 2010	Created release notes for Cisco NX-OS Release 4.1(2)E1(1e).
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

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(1j) 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(1j) 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. Call Home 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(1j), 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(1j).

New Software Features

There is no new feature since Cisco NX-OS Release 4.1(2)E1(1h).

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
snmp-server community *community-name* **use-acl** *acl-name* **Example:** `switch(config)# snmp-server community public use-acl my_acl_for_public`	Assigns an ACL to an SNMP community to filter SNMP requests.

Limitations

This section describes the limitations in Cisco NX-OS Release 4.1(2)E1(1j) 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 might 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: Users cannot resequence rules in a VACL.

  Conditions: You might 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 then add them again.

  If there is a VACL as shown in the following example, users cannot 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 might 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 **show hardware internal ele-fwd driver-info** command 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 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 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: The outgoing CPU-generated traffic cannot be spanned.

  Conditions: You might 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 might 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: The “port not compatible [speed]” error message appears while adding the downlink ports to a port channel.

  Conditions: You might 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 might be some confusion in identifying the mismatch in speed. The default speed for the downlink interface is automatic 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 automatic by entering the **speed auto** command under the **interface** subcommand, the port might not link up.

  Conditions: You might 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 might 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: When 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 might take 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(1j) 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 re-synchronize 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

- CSCty92059

  Symptom: A security scan on Cisco Nexus 4000 Series switch logs authentication bypass vulnerability message. Remote attackers may be able to bypass authentication. For example, if OpenSSH cannot create an untrusted cookie for a client X, due to the temporary partition being full, a trusted cookie will be used instead. This allows attackers to violate intended policy and gain privileges by causing their client X to be treated as trusted.

  Conditions: This vulnerability occurs with OpenSSH v4.5 and OpenSSL v0.9.7l on Cisco NX-OS Release 4.1(2)E1(1g) onwards.

  Workaround: No workaround is available.

- CSCts95953

Symptom: System Queuing policy does not get applied to the port channel interface on Cisco Nexus 4000 Series switch. This can cause the traffic to be prioritized improperly.

Conditions: This issue occurs with the Cisco NX-OS Release 4.1(2)E1(1g). Service policy **policy-fcoe-bandwidth** attached to the system ipqos is not pushed on to the port channel interfaces that are created.

Workaround: Apply the policy directly to the port-channel interface.

- CSCua25612

  Symptom: Authentication fails on Cisco Nexus 4000 Series switch running NX-OS 4.1(2)E1(1j).

  Conditions: This occurs when a "\" is included in the username.

  Workaround: Select a username without a "\".

- CSCuc98373

  Symptom: Users cannot use VLAN other than the default VLAN1 as the native VLAN. If the native VLAN is changed on both sides, then Nexus 4000 switch is unable to view its neighbor through CDP.

  Conditions: This occurs if Cisco Nexus 4000 Series switch is running on Cisco NX-OS Release 4.1(2)E1(1i).

  Workaround: Keep the native VLAN1 to control traffic and manually switch-off VALN1 to limit the VLAN1 data traffic.

Resolved Caveats

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

This section includes the following caveats:

- CSCuc21944

  Symptom: Cisco Nexus 4000 Series switch crashes when polled from Cisco Data Center Network Manager (DCNM).

  Conditions: SNMP polls Entity MIB. This occurs due to the Electra power supply module which is a part of the Entity MIB.

  Workaround: This issue is resolved.

- CSCub72074

  Symptom: SNMP walk on ifTable MIB results in high CPU utilization. After a **`snmpwalk`** on 20 or more OIDS of ifTable, the CPU utilization rises. More than one polling of the same ifTable MIB results in 100% CPU utilization.

  Conditions: Multiple polling crashes the Cisco Nexus 4000 Series switch. Expensive logging of the Electra Driver and Stats Infra modules and costly stats client library operations can worsen this situation.

  Workaround: This issue is resolved. See CSCub12635 for further information.

- CSCub12635

  Symptom: When multiple SNMP requests are sent simultaneously to the Cisco Nexus 4000 Series switch causes Denial of Service. This can distort existing FIP sessions causing storage connectivity issues.

Conditions: When an entire SNMP table is polled, the CPU spikes up for the poll duration before recovering. This problem was diagnosed while polling the IANA Enterprise Number OID, 1.3.6.1.4.1 using two network management tools: Spectrum and E-Health.

Workaround: An SNMP pacer is introduced to avoid high CPU utilization.

- CSCua63010

  Symptom: Ethernet Port Channel crashes on Cisco Nexus 4000 Series switch.

  Conditions: SNMP walk on dot3adAggPortIndex object leads to array out-of-bounds for ifIndex. This results in the node reset due to the High Availability (HA) Policy of Ethernet Port Channel module.

  Workaround: This issue is resolved.

- CSCua92050/CSCua84146

  Symptom: Cisco Nexus 4001 Series switch restarts continuously after upgrading from Cisco NX-OS Release 4.1(2)E1(1f) to 4.1(2)E1(1h) version.

  Conditions: Restarting IBM power blade servers (PS704 2xWide) running AIX OS (v5.0 onwards) cause Cisco Nexus 4000 Series switches to reload after a while. Switch reset can be reproduced by: turning down (i.e., not plumbed) the BCM interfaces then waiting, and also by turning down the BCM interfaces and restarting the power blade servers. There is burst of IRQs from USD to Electra driver resulting in ethpc crash (HA policy). This behavior occurs when two or more double-wide power blade servers are hosted with 2xBroadcom(4-portx1G) CFFh.

  Workaround: This issue is resolved. Existing timer interval for Electra Guardian MAC No Sync received signal is bumped up. The switchport is set to errDisabledExcessportInt state when the IRQ burst is received preventing the node from a restart. Alternatively, shutting down the switch interface before turning down the BCM interfaces can be used as a workaround.

- CSCty77323

  Symptom: DCBX service crashes in Cisco Nexus 4000 Series switch.

  Conditions: This occurs after upgrading from Cisco NX-OS Release 4.1(2)E1(1f) to 4.1(2)E1(1h) or 4.1(2)E1(1i) version. A buffer overrun while parsing LLDP packets results in the service crash.

  Workaround: This issue is resolved.

- CSCud09351

  Symptom: TFTP of running configuration from a Cisco Nexus 4000 Series switch via SNMP fails.

  Conditions: This occurs when TFTP is over the vrf management interface.

  Workaround: This issue is resolved. Electra blade now supports upload/download of running configuration file over vrf management for TFTP.

- CSCub42038

  Symptom: ACLs configured for vty lines are not displayed in running configuration. It cannot be saved in the startup configuration as well.

  Conditions: This occurs after creating an access class and applying it to a vty line. ACLs are taking effect under the line vty.

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