



Release Notes for Cisco Plug-in for OpenFlow Agent 1.1.1

First Published: January 6, 2014

Last Updated: February 06, 2013

Text Part Number: OL-31256-02

Current Release: Cisco Plug-in for OpenFlow Agent Release 1.1.1

This document describes the features, caveats, and limitations for Cisco Plug-in for OpenFlow Agent releases up to and including Cisco Plug-in for OpenFlow Agent 1.1.1. Use this document in combination with documents listed in the Related Documentation section.

Contents

- [Introduction, page 1](#)
- [Cisco Image Information, page 2](#)
- [Supported Cisco Software Releases, page -2](#)
- [System Requirements, page 2](#)
- [Caveats, page 3](#)
- [New and Changed Information, page 12](#)
- [Related Documentation, page 13](#)
- [Obtaining Documentation and Submitting a Service Request, page 13](#)

Introduction

Cisco Plug-in for OpenFlow Agent Release 1.1.1, supports OpenFlow Switch Specification Version 1.1.0 (Wire Protocol 0x01), and provides better control over networks, making it more open, programmable, and application-aware.



Americas Headquarters:

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

© 2009-2013 Cisco Systems, Inc. All rights reserved.

OpenFlow Switch Specification Version 1.1.0 (Wire Protocol 0x01) was defined by the Open Networking Foundation (ONF) standards organization. For more information about the OpenFlow protocol, refer to the ONF website.

For information on new features and commands that are supported by Cisco Plug-in for OpenFlow Agent 1.1.0, see the [“New and Changed Information” section on page 12](#).

Cisco Image Information

The image names of the Cisco NX-OS release that support the Cisco Plug-in for OpenFlow Agent 1.1.1 are:

- n6000-uk9-kickstart.7.0.0.N1.1.bin
- n6000-uk9.7.0.0.N1.1.bin
- n5000-uk9-kickstart.7.0.0.N1.1.bin
- n5000-uk9.7.0.0.N1.1.bin

The image names of the Cisco NX-OS release that support the Cisco Plug-in for OpenFlow Agent 1.1.0 are:

- n3000-uk9-kickstart.6.0.2.U2.1.bin
- n3000-uk9.6.0.2.U2.1.bin

Supported Cisco Software Releases

[Table 1](#) summarizes information about the Cisco Nexus platforms and software release versions that Cisco OpenFlow Plug-in supports.

Table 1 *Cisco Plug-in for OpenFlow Compatibility Matrix*

Switches	Cisco Plug-in for OpenFlow
Cisco Nexus 5000 Series Switches NX-OS 7.0(0)N1(1)	ofa-1.1.1-n5000-r2-SPA-k9.ova
Cisco Nexus 6000 Series Switches NX-OS 7.0(0)N1(1)	ofa-1.1.1-n6000-r2-SPA-k9.ova
Cisco Nexus 3000 Series Switches NX-OS 6.0(2)U2(1)	ofa-1.1.0-n3000-r2-SPA-k9.ova

System Requirements

This section describes the system requirements for Cisco Plug-in for OpenFlow Agent 1.1.1.

Supported Hardware

Cisco Plug-in for OpenFlow Agent 1.1.1 is supported on the following devices

- Cisco Nexus 5000 Series Switches.
- Cisco Nexus 6000 Series Switches.

Cisco Plug-in for OpenFlow Agent 1.1.0 is supported on the following devices

- Cisco Nexus 3000 Series Switches.
- Cisco Nexus 3100 Series Switches.

For additional information about Cisco Nexus Switches see the documentation at:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Caveats

Caveats describe unexpected behavior in Cisco software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

- [Resolved Caveats—Cisco Plug-in for OpenFlow Agent 1.1.1, page 3](#)
- [Open Caveats—Cisco Plug-in for OpenFlow Agent 1.1.1, page 4](#)
- [Open Caveats—Cisco Nexus 5000 and Nexus 6000 Series Switches, page 6](#)
- [Open Caveats—Cisco Plug-in for OpenFlow Agent 1.1.1, page 4](#)
- [Open Caveats—Cisco Nexus 3000 Series Switches, page 10](#)

Resolved Caveats—Cisco Plug-in for OpenFlow Agent 1.1.1

The caveats in this section are resolved in Cisco Plug-in for OpenFlow Agent 1.1.1 but may be open in previous Cisco Plug-in for OpenFlow Agent releases.

- CSCum08772

Symptoms: The Openflow agent gets killed due to lack of memory.

Conditions: This symptom occurs when there are flows installed that punt the packets to the controller. The packet buffer is not freed and gets leaked. This is seen with scale tests when packets get punted to the controller in large numbers at a very high rate.

Workaround: Do not add flows that punt the packets to the controller.

Open Caveats—Cisco Plug-in for OpenFlow Agent 1.1.1

This section describes possibly unexpected behavior by Cisco Plug-in for OpenFlow Agent 1.1.1. All the caveats listed in this section are open in Cisco Plug-in for OpenFlow Agent 1.1.1. This section describes only severity 1, severity 2, and severity 3 caveats.

- CSCuj02751

Symptoms: For pipeline 202, the lookups & match counters for Table 1, MAC Forwarding Table, do not increment even though the traffic matches the MAC table flow rules. Instead the counters increment for Table 0 as the packets match the default rule in the ACL table.

Conditions: This symptom occurs when pipeline 202 is configured for the openflow switch and traffic matches flow in the MAC Forwarding Table.

Workaround: There is no workaround.

- CSCuj07822

Symptoms: When a significant number of flows are added while debug commands are turned on, the CLI hangs momentarily before eventually recovering automatically.

Conditions: This symptom occurs when a significant number of flows are simultaneously programmed and when debugs are turned on.

Workaround: Turn off the debugs or limit the number of debugs being turned on. Or wait until the flows are setup before running the show commands.

- CSCuj44931

Symptoms: The Mac Forwarding Table flows are all configured as static entries and all the flows have the same priority. Also, the MAC table supports the exact matching on the destination MAC address and the VLAN ID, and the only actions supported are drop and output to port.

However, the Openflow Agent will accept flow add/modify messages for the MAC flows with configurations for the flow priority and the idle/hard timeouts, and matching on other fields. These invalid matches/actions are ignored and the flow is still installed in the MAC table with only the correct supported attributes.

Conditions: This symptom occurs when the openflow switch is configured with pipeline 202 and flow add messages include unsupported matches and actions like setting the flow priority, setting the idle/hard timeouts, matching on IP src/dest address, TCP/UDP protocol, TOS, L4 src/dest ports etc.

Workaround: Install flows with only the supported matches and actions for the MAC Forwarding Table in Pipeline 202.

- CSCul67703

Symptoms: With pipeline 202, when the default-miss is configured to drop, two default flows are added, one each for the ACL and the MAC table. The ACL table installs a default rule of “permit” to allow packet matching in the MAC table. The MAC table installs a default rule of “drop” to drop all unmatched packets.

However, “show openflow switch 1 flows” displays both the rules to have the action “drop” instead of having the action “goto” or “normal” for the table 0.

Conditions: This symptom occurs when the switch is configured to use pipeline 202 and the default-miss is configured as “drop”.

Workaround: The **show ip access-lists | beg onep** command can be used to display the rule that is actually installed in the ACL table. The default rule will be similar to the following:

```
permit ip any any priority -1
```

- CSCul70028

Symptoms: When the Openflow agent-installed default flow is modified by adding another default rule from the controller, the following issues are observed

1. The **show openflow switch 1 flows controller** command does not show this controller installed default flow
2. When the controller tries to fetch flow stats for this default flow, the Openflow agent does not provide the stats for this default flow.

Conditions: This symptom occurs when the Openflow agent-installed default flow is over-ridden by another default rule installed by the controller.

Workaround: The controller-installed default flow can be seen with the **show openflow switch 1 flows default** command. However, the stats for this default flow will not be sent to the controller.

- CSCul87549

Symptoms: The OpenFlow plugin incorrectly sends an OFPHFC_INCOMPATIBLE error in response to an OFPT_FLOW_MOD message.

Conditions: This symptom occurs when an attempt is made to program a flow using matches not supported by the configured pipeline.

Workaround: Ensure that the flows are programmed with matches/actions that are supported for the pipeline.

- CSCum22686

Symptoms: There is a mismatch between controller flows and the ACL entries.

Conditions: This symptom occurs while performing the open flow switch unconfiguration and configuration. Either copy/paste or copying to the running configuration may create the issue.

Workaround: Perform shutdown/no shutdown under the open flow switch configuration.

- CSCum59162

Symptoms: Openflow memory allocation increases if the rate of packets being punted to the controller increases at more than 2000 packets per second (pps). If this rate persists over a long time, then the openflow agent could run out of memory and restart.

Conditions: This symptom is seen with a persistent rate of more than 2000 pps being sent to the controller.

Workaround: Reduce the rate of packets being sent to the controller to the supported rate of around 1000 pps. The control plane policing policy can be configured to 1000 pps to limit the rate of incoming packets.

- CSCuj08625

Symptoms: Flow packet counters are different in the outputs of the **show ip access-list** and the **show openflow switch 1 flow** commands.

Conditions: This symptom occurs because the hardware counters are 64 bit long and the openflow counters are 32 bit long, and the counters will start to get different after there have been 2^{32} packets that match the flow.

Workaround: Get the flow match counters from the output of the **show ip access-list** command instead of the **show openflow switch 1 flow** command.

- CSCum77755

Symptoms: In scale testbeds with more than 1000 flows, the virtual service restarts when the openflow switch is shutdown.

Conditions: This symptom is seen when the **logging flow-mod** command is enabled and the openflow switch is shutdown when there are more than 1000 flows installed on the switch.

Workaround: Disable **logging flow-mod** on openflow switches that have a large number of flows installed.

- CSCul65769

Symptoms: Sometimes some of the flows fail to get installed. This is usually seen in scale testbeds.

Conditions: This symptom is seen in scale testbeds.

Workaround: After the flows are added, you can use the output of **show openflow switch 1 flows summary** and **show openflow switch 1 controller stats** to ensure that all the flows are correctly installed. Or check for error messages from the agent during flow setup on the controller. If any errors are found, read only the failed flows and ensure it was successfully added.

- CSCum05753

Symptoms: The Openflow Agent does not send a “TABLE_FULL” error when the OFA flow table is full.

Conditions: This symptom is seen when the maximum supported flows for any table are already installed and the controller attempts to add additional flows. The flow adds fail and error messages are sent to the controller. However, the error is not the “TABLE_FULL” error.

Workaround: There is no workaround. There is no functional impact to this bug.

Open Caveats—Cisco Nexus 5000 and Nexus 6000 Series Switches

NX-OS 7.0(0)N1(1)

This section describes possibly unexpected behavior in the underlying Cisco NX-OS system software which may affect the behavior of Cisco Plug-in for OpenFlow Agent 1.1.1. All the caveats listed in this section are open in Cisco NX-OS 7.0(0)N1(1). This section describes only severity 1, severity 2, and severity 3 caveats.

- CSCui25370

Symptom: CLI commands added by a container-based onePK application may not be removed when a container fails to install following a reboot.

Conditions: A container-based onePK application adds CLI commands to the router using the onePK CLI extensions feature. Upon reboot of the router the container fails to install properly. The CLI commands added prior to rebooting still remain even though the container is no longer installed.

Workaround: Install and uninstall the container for a second time to clean up the remaining CLI commands.

- CSCuj45245

Symptom: The following error message is seen:

```
%$ VDC-1 %$ %VMAN-5-VIRT_INST_NOTICE: VIRTUAL SERVICE n3k LOG: OVS:
sw1<->tcp:5.0.1.6:6641: connection failed (Interrupted system call should be
restarted)
```

Conditions: This symptom is an intermittent issue seen after some triggers, for example, clear controller command, switch unconf/conf, switch shut/noshut, cotroller unconf/conf etc.

Workaround: Virtual-service deactivate & reactivate fixes this issue.

- CSCuj66918

Symptom: All packets do not reach the controller from the Cisco Nexus 3064 switch at 500pps to 1000pps. There is no issue on the Cisco Nexus 3048 switch.

Conditions: The symptom is seen under the following conditions:

- About 1700 packets reached the controller when 2000 lldp packets were sent to the controller at 500pps.
- About 1050 packets reached the controller when 2000 lldp packets were sent to the controller at 1000pps.

Workaround: There is no workaround.

- CSCuj70716

Symptom: The following system message seen on uninstalling ova. There is no functionality impact.

```
onep:ONEP Appli[5784]: rwsem unexpected owner->magic 6b6b6b6b ? kernel
```

Conditions: The symptom is seen after uninstalling ova.

Workaround: No workaround is needed as there is no functionality impact.

- CSCul48306

Symptom: A deadlock in the Netstack or DPSS components blocks the openflow agent process until the process is killed by the watchdog timer.

Conditions: This symptom is seen when the openflow agent is repeatedly unconfigured, configured, shut, and no-shut in a continuous cycle. It usually takes about 15-20 cycles for the deadlock to occur and for the process to crash.

Workaround: Enter the switch unconfiguration or configuration command manually or slower with a few seconds between each command.

- CSCul99528

Symptom: The openflow-agent logical-switch configuration **default-miss cascade normal** does not take effect in pipeline 201.

Conditions: This symptom is seen in the openflow pipeline 201 mode when the incoming packets do not match any of the flows installed and cannot be subjected to the regular forwarding logic in pipeline 201.

Workaround: Openflow logical switch configuration can be changed to pipeline 202 in which the **default-miss cascade normal** works as expected.

Further Problem Description: The following are the steps to reproduce this symptom:

1. Configure pipeline 201.
2. Configure the openflow logical-switch configuration **default-miss cascade normal**.
3. Configure two ports in openflow with the same vlan configuration.
4. Check if no flow is installed and if the traffic is following as per the normal forwarding path.
5. Check whether all openflow ports in same vlan are receiving the packets.

Traffic does not get forwarded to the destination even though the ports are in the same vlan.

- CSCum23745

Symptom: On Flapping OF switch with 1200 acl flows installed and sending traffic at line rate(10Gb) large ONEP mem-leak is observed.

Conditions: This symptom is seen After installing 1200 and could see huge memory leak at ONEP CLI extensions code and also in other places too.

Workaround: There is no workaround.

- CSCum79887

Symptom: In the monitor-manager based openflow topology when there is a flow with the port-channel as the output port then the traffic drop might happen when the port-channel link is flapped or a link failure happens. In this case the monitor-monitor recalculates the topology and tries to forward packets using the next available path which fails due to the software issue.

Conditions: This symptom is seen in the monitor-manager based openflow topology when there is a flow with the port-channel as the output port.

Workaround: Perform a shut and no-shut of the openflow logical switch.

Open Caveats—Cisco Plug-in for OpenFlow Agent 1.1.0

This section describes possibly unexpected behavior by Cisco Plug-in for OpenFlow Agent 1.1.0. All the caveats listed in this section are open in Cisco Plug-in for OpenFlow Agent 1.1.0. This section describes only severity 1, severity 2, and severity 3 caveats.

- CSCuj02751

Symptoms: For pipeline 202, the lookups & match counters for Table 1, MAC Forwarding Table, do not increment even though the traffic matches the MAC table flow rules. Instead the counters increment for Table 0 as the packets match the default rule in the ACL table.

Conditions: This symptom occurs when pipeline 202 is configured for the openflow switch and traffic matches flow in the MAC Forwarding Table.

Workaround: There is no workaround.

- CSCuj07822

Symptoms: When a significant number of flows are added while debug commands are turned on, the CLI hangs momentarily before eventually recovering automatically.

Conditions: This symptom occurs when a significant number of flows are simultaneously programmed and when debugs are turned on.

Workaround: Turn off the debugs or limit the number of debugs being turned on. Or wait until the flows are setup before running the show commands.

- CSCuj44931

Symptoms: The Mac Forwarding Table flows are all configured as static entries and all the flows have the same priority. Also, the MAC table supports the exact matching on the destination MAC address and the VLAN ID, and the only actions supported are drop and output to port.

However, the Openflow Agent will accept flow add/modify messages for the MAC flows with configurations for the flow priority and the idle/hard timeouts, and matching on other fields. These invalid matches/actions are ignored and the flow is still installed in the MAC table with only the correct supported attributes.

Conditions: This symptom occurs when the openflow switch is configured with pipeline 202 and flow add messages include unsupported matches and actions like setting the flow priority, setting the idle/hard timeouts, matching on IP src/dest address, TCP/UDP protocol, TOS, L4 src/dest ports etc.

Workaround: Install flows with only the supported matches and actions for the MAC Forwarding Table in Pipeline 202.

- CSCul67703

Symptoms: With pipeline 202, when the default-miss is configured to drop, two default flows are added, one each for the ACL and the MAC table. The ACL table installs a default rule of “permit” to allow packet matching in the MAC table. The MAC table installs a default rule of “drop” to drop all unmatched packets.

However, “show openflow switch 1 flows” displays both the rules to have the action “drop” instead of having the action “goto” or “normal” for the table 0.

Conditions: This symptom occurs when the switch is configured to use pipeline 202 and the default-miss is configured as “drop”.

Workaround: The **show ip access-lists | beg onep** command can be used to display the rule that is actually installed in the ACL table. The default rule will be similar to the following:

```
permit ip any any priority -1
```

- CSCul70028

Symptoms: When the Openflow agent-installed default flow is modified by adding another default rule from the controller, the following issues are observed

1. The **show openflow switch 1 flows controller** command does not show this controller installed default flow
2. When the controller tries to fetch flow stats for this default flow, the Openflow agent does not provide the stats for this default flow.

Conditions: This symptom occurs when the Openflow agent-installed default flow is over-ridden by another default rule installed by the controller.

Workaround: The controller-installed default flow can be seen with the **show openflow switch 1 flows default** command. However, the stats for this default flow will not be sent to the controller.

- CSCul87549

Symptoms: The OpenFlow plugin incorrectly sends an OFPHFC_INCOMPATIBLE error in response to an OFPT_FLOW_MOD message.

Conditions: This symptom occurs when an attempt is made to program a flow using matches not supported by the configured pipeline.

Workaround: Ensure that the flows are programmed with matches/actions that are supported for the pipeline.

- CSCum08772

Symptoms: The Openflow agent gets killed due to lack of memory.

Conditions: This symptom occurs when there are flows installed that punt the packets to the controller. The packet buffer is not freed and gets leaked. This is seen with scale tests when packets get punted to the controller in large numbers at a very high rate.

Workaround: Do not add flows that punt the packets to the controller.

- CSCum22686

Symptoms: There is a mismatch between controller flows and the ACL entries.

Conditions: This symptom occurs while performing the open flow switch unconfiguration and configuration. Either copy/paste or copying to the running configuration may create the issue.

Workaround: Perform shutdown/no shutdown under the open flow switch configuration.

Open Caveats—Cisco Nexus 3000 Series Switches

NX-OS 6.0(2)U2(1)

This section describes possibly unexpected behavior in the underlying Cisco NX-OS system software which may affect the behavior of Cisco Plug-in for OpenFlow Agent 1.1.0. All the caveats listed in this section are open in Cisco NX-OS 6.0(2)U2(1). This section describes only severity 1, severity 2, and severity 3 caveats.

- CSCui25370

Symptom: CLI commands added by a container-based onePK application may not be removed when a container fails to install following a reboot.

Conditions: A container-based onePK application adds CLI commands to the router using the onePK CLI extensions feature. Upon reboot of the router the container fails to install properly. The CLI commands added prior to rebooting still remain even though the container is no longer installed.

Workaround: Install and uninstall the container for a second time to clean up the remaining CLI commands.

- CSCuj45245

Symptom: The following error message is seen:

```
%$ VDC-1 %$ %VMAN-5-VIRT_INST_NOTICE: VIRTUAL SERVICE n3k LOG: OVS:
sw1<->tcp:5.0.1.6:6641: connection failed (Interrupted system call should be
restarted)
```

Conditions: This symptom is an intermittent issue seen after some triggers, for example, clear controller command, switch unconf/conf, switch shut/noshut, cotroller unconf/conf etc.

Workaround: Virtual-service deactivate & reactivate fixes this issue.

- CSCuj70716

Symptom: The following system message seen on uninstalling ova. There is no functionality impact.

```
onep:ONEP Appli[5784]: rwsem unexpected owner->magic 6b6b6b6b ? kernel
```

Conditions: The symptom is seen after uninstalling ova.

Workaround: No workaround is needed as there is no functionality impact.

- CSCul64410

Symptom: As per the Cisco Nexus 3000 design, the OpenFlow switch should allow a maximum of 16 output ports for the redirect action. However, the current release supports more than 17 redirect output ports.

Conditions: This symptom occurs when the OF controller is pushing down the flows with 17+ redirect output port action. The ACLMGR/AFM component allows to install those flows on the OF switch.

Workaround: Install flows with a maximum of 16 redirect output port actions.

- CSCul69881

Symptom: Flows are created for non-existing vlans.

Conditions: Install flows with non existing vlans on the agent via controller and the agent accepts the flows.

Correct Behaviour: Agent should reject the flow

Workaround: There is no workaround.

- CSCum06922

Symptom: When flow provisioned from the controller for non-ip ethertype with an output to port action, then the flow gets rejected.

Conditions: This symptom occurs only on flows provisioned via API(Openflow Agent).

Workaround: Modify the Openflow ACL via CLI and add the output to the port ACE manually.

Example: onep-acl-1 has been provisioned by OpenFlow Agent. Now Modify CLI to add the non-ip ethertype ACE using the following steps:

[1]Get the if_index corresponding to the output port using:

```
switch# sh interface snmp-ifindex | inc Eth1/1
Eth1/1          436207616 (0x1a000000) <==if_index
```

[2]Confirm onep-acl exists on OF Interface:

```
switch(config)# sh run int e1/1
```

```
!Command: show running-config interface Ethernet1/1
```

```
!Time: Sat Dec 14 08:35:11 2013
```

```
version 6.0(2)U2(1)
```

```
interface Ethernet1/1
```

```
  ip port access-group onep-acl-1 in
```

```
  no lldp transmit
```

```
  spanning-tree bpdupfilter enable
```

```
  mode openflow
```

```
switch# sh ip access-lists onep-acl-1
```

```
IPV4 ACL onep-acl-1
```

```
  statistics per-entry
```

```
  2147483647 deny ip any any priority -1 [match=2728807324]tfo c7
```

[3] Add the non-IP ethertype rule via CLI

```
switch# conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
switch(config)# ip access-list onep-acl-1
```

```
switch(config-acl)# permit ethertype 0x8847 ip an an redirect 0x1a001000
```

```
switch# sh ip access-lists onep-acl-1
```

```
IPV4 ACL onep-acl-1
```

```
  statistics per-entry
```

```
  2147483647 deny ip any any priority -1 [match=2728807324]
```

```
  2147483657 permit ip any any ethertype 0x8847 redirect 0x1a001000 [match=0]
```

- CSCum11307

Symptom: A core is observed while adding and deleting flows on Cisco Nexus 5000 series switches and Cisco Nexus 3000 series switches.

Conditions: The core that is observed seems to be an intermittent problem that does not occur or happen every time we add / delete 1500 flows. The element chunk memory that gets freed on xos_list_remove is not yet overwritten or used when the next call to xos_list_get_next() is made most of the times (xos is just freeing not setting the parameter to null).

Workaround: There is no workaround. This issue is not seen consistently.

- CSCum16186

Symptom: A deadlock in the Netstack or DPSS components blocks the openflow agent process until the process is killed by the watchdog timer.

Conditions: This symptom is seen when the openflow agent is repeatedly unconfigured, configured, shut, and no-shut in a continuous cycle. It usually takes about 15-20 cycles for the deadlock to occur and for the process to crash.

Workaround: Enter the switch unconfiguration or configuration command manually or slower with a few seconds between each command.

- CSCum23124

Symptom: Sometimes when openflow is enabled and unconfigured using the **no openflow** global configuration command, an error is seen when a proper cleanup of configuration is done. This issue has no functionality impact.

Conditions: This symptom is seen in the “no openflow” configuration.

Workaround: There is no workaround.

New and Changed Information

This section lists the new hardware and software features supported by Cisco Plug-in for OpenFlow Agent 1.1.1 and contains the following subsections.

- [New Hardware Features in Cisco Plug-in for OpenFlow Agent 1.1.1., page 12](#)
- [New Software Features in Cisco Plug-in for OpenFlow Agent 1.1.1., page 12](#)
- [New Hardware Features in Cisco Plug-in for OpenFlow Agent 1.1.0., page 12](#)
- [New Software Features in Cisco Plug-in for OpenFlow Agent 1.1.0., page 12](#)

New Hardware Features in Cisco Plug-in for OpenFlow Agent 1.1.1.

There are no new hardware features in Cisco Plug-in for OpenFlow Agent 1.1.1.

New Software Features in Cisco Plug-in for OpenFlow Agent 1.1.1.

There are no new software features in Cisco Plug-in for OpenFlow Agent 1.1.1.

New Hardware Features in Cisco Plug-in for OpenFlow Agent 1.1.0.

There are no new hardware features in Cisco Plug-in for OpenFlow Agent 1.1.0.

New Software Features in Cisco Plug-in for OpenFlow Agent 1.1.0.

This section describes new and changed software features in Cisco Plug-in for OpenFlow Agent 1.1.0.

- OpenFlow-hybrid (Ships-in-night) model is supported.
- ACL and MAC Forwarding tables are supported and can be configured using pipelines.
- Transport Layer Security (TLS) is supported in Cisco Agent for OpenFlow and controller communications.
- VLAN priority has been introduced as a flow action.
- Configuration of default forwarding rule via openflow switch CLI.

Related Documentation

The following section describes the documentation available for Cisco Plug-in for OpenFlow Agent 1.1.1.

- Cisco OpenFlow Agent Configuration Guide 1.1.1
- Cisco OpenFlow Agent Release 1.1.1 Command Reference
- Cisco Nexus 5000 Series Switches Command Reference at:
http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html
- Cisco Nexus 6000 Series Switches Command Reference at:
http://www.cisco.com/en/US/products/ps12806/prod_command_reference_list.html
- Cisco Nexus 3000 Series Switches Command Reference at:
http://www.cisco.com/en/US/products/ps11541/prod_command_reference_list.html

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.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 13.

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 used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright © 2009-2013 Cisco Systems, Inc.
All rights reserved. Printed in USA.

