Release Notes for Embedded Service 3300 Series Switches

The following release notes support the Cisco Embedded Service 3300 Series Switches (ESS3300). These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

Contents

This publication consists of the following sections:

Image Information

Note: You must have a Cisco.com account to download the software.

Cisco ESS3300 operates on the following Cisco IOS images:

- ess3x00-universalk9.16.09.01.SPA.bin

Software Downloads

The latest image file for the ESS3300 is:

https://software.cisco.com/download/home/286320893/type/282046477/release/Fuji-16.9.1

Related Documentation

The following documentation is available:

- All of the Cisco ESS3300 documentation can be found here:

  https://www.cisco.com/c/en/us/products/switches/embedded-service-3300-series-switches/index.html

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats

- **CSCvk75175**

  IGMP snooping is not letting unknown multicast traffic reach the mrouter interface.

  Symptoms: Multicast does not work when **ip igmp snooping** is enabled on mixed switches (s5410, s5700, ESS3300).

  Conditions:

  ip igmp snooping enabled on ESS3300 switches only, no issue

  ip igmp snooping enabled on non-ESS3300 switches only, no issue

  ip igmp snooping enabled on mixed switches, the issue is seen.

  Workaround: Will be fixed in IOS-XE 16.10.1 .

- **CSCvk18119**

  DHCP Client is not getting ip when mac table space is unavailable.

  Symptoms: DHCP Client will not get IP address when mac table space is fully utilized.

  Conditions: When the device has learned the maximum number of mac addresses(8K), the mac address table is fully loaded. During this condition, DHCP clients will not be provided with an IP address.

  Workaround: Reduce mac address table utilization.

- **CSCvi96736**

  ACL logging is not working for IGMP Packets.

  Symptoms: ACL logging not working for IGMP packets.

  Conditions: When an ACL is configured to drop IGMP packets and logging is enabled. Logging of denied packets will not happen.

  Workaround: There is no workaround.

- **CSCvg81130**

  ARP packets not getting forwarded with DAI enabled.

  Symptoms: ARP Unicast packets not getting forwarded with DAI enabled. Works fine with ARP broadcast packets.

  Conditions: When DAI is configured with DHCP snooping binding, the ARP packets are not getting forwarded as expected. Problem seen with ARP unicast packets, where as works fine with ARP broadcast packets.

  Workaround: There is no workaround.

- **CSCvk05044**

  QoS egress policy map counter is incorrect.

  Symptoms: Mismatch in QoS counters after clear counters.

  Conditions: When clear QoS counters is performed and counters are checked after that, there may be difference in the number of ingress and egress packets as counters are not cleared completely.

  Workaround:

  Clear counters and wait for 5 seconds before checking for QoS counters.
  -Or
  Issue clear counters twice

- **CSCvk18018**

  CISCO-PROCESS MIB is not functional

  Symptoms: SNMP query on the CISCO-PROCESS-MIB is not returning any value.

  Conditions: SNMP get on CISCO-PROCESS-MIB oids.

  Workaround: There is no workaround, this MIB is not supported.

- **CSCvi94624**

  CISCO-FLASH-MIB is not giving flash information.

  Symptoms: CISCO-FLASH-MIB is not functional.

  Conditions: SNMP get or walk on the CISCO-FLASH-MIB OIDs agent returns " No Such Object available on this agent at this OID"

  Workaround: There is no workaround, use CLI to get the flash content and size of the flash.

- **CSCvk20216**

  IPv6 ACL stale entries are present in TCAM even after un-configuring the ACL.

  Symptoms:

  Create ACL and apply to interface.

  Observe TCAM entries are shown. Upon removing ACL globally the entry still remains.

```
Switch(config)#ipv6 access-list ipv61
Switch(config-ipv6-acl)#permit ipv6 host 1001::10 host 1001::1000
Switch(config-ipv6-acl)#permit ipv6 host 1001::11 host 1111::1001
..
Switch#sh access-lists ipv61
IPv6 access list ipv61
    permit ipv6 host 1001::10 host 1001::1000 sequence 10
    permit ipv6 host 1001::11 host 1111::1001 sequence 20

Switch(config)#int TenGigabitEthernet 1/2
 ipv6 traffic-filter ipv61 in

Switch#sh hardware acl as 0 tcam int TenGigabitEthernet 1/2 ipv6 detail
<this will ave entry for the ACL>
Remove the global ACL
```

```
Switch (config)#no ipv6 access-list ipv61
Switch#sh hardware acl as 0 tcam int TenGigabitEthernet 1/2 ipv6 detail
```

Still shows the entry

Conditions: IPV6 ACLs are configured and bind to an interface. Delete the ACL at global config mode.

Workaround:

Unbind the ACL at interface.

Shut the interface

Unshut

```
Switch(config)#int TenGigabitEthernet 1/2
Switch(config-if)#ino ipv6 traffic-filter ipv61 in
Switch(config-if)#shut
Switch(config-if)#no shut
```

Stale entries in TCAM are present for IPV6 ACLs when the ACL is removed at the global config level. Unbind the ACL at the interface, shutting the interface will clear the TCAM table. Therefore, this step is necessary to create space in TCAM table.

- **CSCvk14196**

  TCAM installation fails for IPv4/IPv6 ACLs with ACEs scaled within limit

  Symptoms: TCAM installation fails for IPv4 ACL with ACEs scaled within the limit (254 ACEs) and none of the entries are seen. Issue happens on ACL updating with same ACL binded to multiple interfaces.

  Workaround: There is no workaround.

- **CSCvk14148**

  Crash observed on binding ACL when device has scaled number of ACEs.

  Symptoms: Create ACE's > 32 (32 ACEs are recommended limit per ACL type). Bind the ACL to an interface. The system can crash if the number of ACE's per ACL type exceeds recommended value of 32.

  Conditions: System has ACE's greater than the recommended limit of 32.

  Workaround: There is no workaround, the recommended limit of 32 must be followed.

- **CSCvk14168**

  CPU hog with process = IMSP ACL Manager and tracebacks seen with scaled ACEs on device.

  Symptoms: Create ACE's > 32 (32 ACEs are recommended limit per ACL type). Bind the ACL to an interface. After ACE's have reached recommended limit of 32 per ACL type. Any additional ACEs being added to device and binding ACL will lead to CPU HOG.

  Conditions: System has ACE's greater than the recommended limit of 32 per ACL type. Add ACE's after this condition on the device and binding the ACL will lead to CPU HOG.

  Workaround: There is no workaround, the recommended limit of 32 must be followed.

- **CSCvk21561**

  Peer switch is detected as a powered device and gets continuous power deny messages.

  Symptoms: Intermittent power deny messages on console for a peer switch.

Conditions: No special conditions. Sometimes observed that the peer switch is detected as a PD and always shows power deny. This is mostly seen with default power budget.

Workaround: Increase power budget.

- **CSCvk17003**

  Non-stop error messages displayed with a large ACL in input policy-map.

  Symptoms: Create ACL with ACE's greater than the recommended limit (32 ACE's per ACL type). Attach to interface.

  ```
  config t
  interface TenGigabitEthernet1/1
  service-policy input ipaccess
  ```

  Observe error message as follows:

  *Jun 28 16:11:58.770 CDT: imsp_update_mqc_queue_ingress_stats,1454: QOS ERR:Invalid qid found for classmap ipaccess (id 1) during stats update for Te1/1 policy ipaccess

  Conditions: The ACE's in an ACL have exceeded recommended value. Attach ACL to interface in this condition.

  Workaround: There is no workaround, recommended limit of ACE's has to be followed.

- **CSCvj72532**

  IMSP: ACT2 SUDI PL I2C read issue at 400Khz

  Symptoms: Additional reload of the device when ACT2 authentication fails for Expansion Module.

  Conditions: In rare conditions, the device may go for an extra reload, due to ACT2 authentication failure for Expansion Module.

  Workaround: There is no workaround.

- **CSCvj72942**

  LACP interface link flaps when congested

  Symptoms: LACP interface link flaps when congested.

  Conditions: IXIA-1 ----- TenG1/1 ESS3300-1 Gi2/5 & Gi2/6 --EtherChannel-- Gi2/5 & Gi2/6 ESS3300-2 TegG1/1 --- IXIA-2.

  When line rate traffic(10Gig) is sent from IXIA-1 to IXIA-2, link flaps are observed.

  Workaround: Increase ether-channel capacity by adding more 1G links.

- **CSCvj54490**

  Modify the input ACL on the fly has no effect on the traffic.

  Symptoms:

  1. Create an ACL and add policy map.

  For Example:

  ```
    access-list 101 permit ip any any dscp cs3
    class-map match-all c1
    match access-group 101
  ```

```
policy-map c1
 class c1
  police 10000000
interface GigabitEthernet1/5
 switchport mode trunk
 service-policy input c1
```

2. Send line rate traffic ip traffic with dscp= cs5 (not matching the ACL). The receiver will receive line rate traffic as expected.

3. Modify to match the dscp value.

```
       access-list 101 permit ip any any dscp cs5
```

4. Note that even though policy has 10Mbps, receiver will receive line rate traffic.

Conditions: ACL and Policy maps are created and attached to an interface. Update ACL to match different rule. This will not take into effect until policy is detached and attached to interface

Workaround: Detach and re-attach the input policy-map from the interface, receiver will receive 10 Mb/s traffic correctly.

```
Switch (conf t)#interface GigabitEthernet1/5
Switch (conf-if)#no service-policy input c1
Switch (conf-if)#no service-policy input c
```

- **CSCvk19996**

  FPGA version display issue

  Symptoms: FPGA version is displayed incorrectly. For example, version 65 should show as either 65 or 0x41. It displays as 41.

  Conditions: When show version is issued.

  Workaround: Please read it as Hex and convert to decimal.

- **CSCvk22179**

  Inventory details/transceiver o/p does not get updated until media-type sfp is configured at the port.

  Workaround: There is no workaround.

- **CSCvj53376**

  PD class should be displayed for PoE controller output.

  Symptoms: show controllers power inline doesn't display PD class for expansion module ports.

  Conditions: PDs connected to expansion module ports

  Workaround: Check the other CLI, show power inline

- **CSCvk28619**

  L2 Multicast snooping IGMP/MLD fails to install all FDB at scaled scenario.

  Symptoms: Mac learning doesn't happen for more than 426 groups (this may further go down based on total used mac space in the switch), in a Private VLAN (PVLAN) configuration. 512 groups works fine in a regular VLAN case. Issue is specific to PVLAN.

  Conditions: With Private VLANs (PVLANs) configured, when IGMP joins/MLD reports are initiated for 512 groups, only 426 are being learned by the switch, the remaining ones will be dropped.

Dynamically learned MAC count and IGMP/MLD snooping FDB entries are inversely proportional.

Note: If the Dynamically learned mac address count is Zero, then up to 426 IGMP/MLD snooping FDB entries are learned.

Workaround: In PVLAN scenario, limit IGMP/MLD snooping to 426 groups or less than total used mac space in the switch. 512 groups works alright in regular VLAN case.

- **CSCvj16530**

  Issue in Powered Devices coming up though power statically reserved & available, also recovery.

  Symptoms: PDs don't up with static power allocation until the full budget is available.

  Conditions: If switch has 4 PDs with static power configured as 30W each, until the device has a power budget of more than 120W(4x30), no PD will be powered on.

  Workaround: Provide sufficient budget or configure them as Auto.

- **CSCvk41816**

  After Day0 configuration of ESS3300 accessing Web UI via https result in SSL error.

  Symptoms: After Day0 configuration of ESS3300 accessing the Web UI via https results in an SSL error.

  Conditions: Access Web UI with https after Day0 configuration.

  Workaround: Regenerate certificate in the CLI:

  ```
  no crypto key trustpoint <trust point name>
  crypto key zeroize
  no ip http secure server
  ip http secure serve
  ```

- **CSCvk36899**

  Online Help Issues on the ESS3300

  Symptoms:

  Online help navigation issues:

  - Navigate to **Administration -> Device**. Click on Online help. This takes you to page named " Configuring General System Settings"
    This is obsolete. This is not shown in left page navigation tree as well. This should have led to the page " Configuring Device Settings" .
  - Activating or Deactivating Your Software License.
    This is to be removed from help. Licensing is not available in the product.
  - Navigate to **Troubleshooting -> Audit Support**. Now click on the OLH,
    This takes you to " About Troubleshooting Your Device" instead of " Auditing Device Configuration" .
  - Navigate to **Troubleshooting -> Packet Capture**.
    This is to be removed from help.
  - The initial page says: " The Web User Interface (WebUI) for Cisco 3000 Series Switches provides network administrators with a single solution for monitoring, optimizing, and troubleshooting devices" .
    The device type will be replaced with the device name that applies, Cisco ESS3300.

Resolved Caveats

- **CSCvm88682**

  Some interfaces did not come up when the hardware revision was set to 1.0

  Symptoms: Some interfaces did not link up with the image ess3x00-universalk9.16.09.01.SPA.bin. For example:

```
Switch#show int status

Port      Name               Status       Vlan       Duplex  Speed Type
Te1/1                        connected    trunk        full    10G SFP-10Gbase-SR
Te1/2                        connected    trunk        full    10G SFP-10Gbase-SR
Gi1/3                        connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/4                        connected    2          a-full a-1000 10/100/1000BaseTX
Gi1/5                        connected    2          a-full a-1000 10/100/1000BaseTX
Gi1/6                        notconnect   3            auto   auto unknown
Gi1/7                        notconnect   3            auto   auto 10/100/1000BaseTX
Gi1/8                        notconnect   4            auto   auto 10/100/1000BaseTX
Gi1/9                        notconnect   4            auto   auto 10/100/1000BaseTX
Gi1/10                       notconnect   5            auto   auto 10/100/1000BaseTX
Gi2/1                        notconnect   5            auto   auto unknown
Gi2/2                        connected    6          a-full a-1000 10/100/1000BaseTX
Gi2/3                        connected    6          a-full a-1000 10/100/1000BaseTX
Gi2/4                        notconnect   7            auto   auto unknown
Gi2/5                        notconnect   7            auto   auto 10/100/1000BaseTX
Gi2/6                        notconnect   8            auto   auto 10/100/1000BaseTX
Gi2/7                        notconnect   8            auto   auto 10/100/1000BaseTX
Gi2/8                        notconnect   9            auto   auto 10/100/1000BaseTX
Gi2/9                        notconnect   9            auto   auto 10/100/1000BaseTX
Gi2/10                       connected    10         a-full a-1000 10/100/1000BaseTX
Gi2/11                       connected    10         a-full a-1000 10/100/1000BaseTX
Gi2/12                       notconnect   11           auto   auto 10/100/1000BaseTX
Gi2/13                       notconnect   11           auto   auto 10/100/1000BaseTX
Gi2/14                       notconnect   12           auto   auto 10/100/1000BaseTX
Gi2/15                       notconnect   12           auto   auto 10/100/1000BaseTX
Gi2/16                       notconnect   333          auto   auto 10/100/1000BaseTX
```

  Conditions: All ESS-3300 switches running ess3x00-universalk9.16.09.01.SPA.bin image

  Workaround: There is no workaround

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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.