



## Product Support Notice

© 2016 Avaya Inc. All Rights Reserved.

PSN # PSN004896u

Original publication date: 29-Nov-16. This is Issue #01, published date: 29-Nov-16. Severity/ risk level **Medium** Urgency **When convenient**

### Name of problem

B179 with 2.4 or later releases freezes or becomes unresponsive, when Link Layer Discovery Protocol (LLDP) is enabled on the switch port.

### Products affected

B179 with 2.4 or later

### Problem description

B179 running 2.4 or later release, with LLDP enabled on switch port becomes unresponsive or freezes after sometime. A reboot is required make the phone working again.

### Resolution

- Install patch 2.4.2.12 (encryption disabled),  
Or
- install the patch 2.4.13 (encryption enabled)

### Workaround or alternative remediation

Disable LLDP on switch port where the phone is connected.

### Remarks

n/a

## Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

### Backup before applying the patch

n/a

### Download

- **Download patch 2.4.2.12 (encryption disabled):**  
[ftp://ftp.avaya.com/incoming/Up1cku9/AvayaT4APP/IPT/B179PatchesAndSoftware/2.4.2.12/B179-IPT-SIP-R2\\_4\\_2\\_12-111816.zip](ftp://ftp.avaya.com/incoming/Up1cku9/AvayaT4APP/IPT/B179PatchesAndSoftware/2.4.2.12/B179-IPT-SIP-R2_4_2_12-111816.zip)
- **Download patch 2.4.2.13 (encryption enabled):**  
[ftp://ftp.avaya.com/incoming/Up1cku9/AvayaT4APP/IPT/B179PatchesAndSoftware/2.4.2.13/B179-IPT-SIP-R2\\_4\\_2\\_13-111816.zip](ftp://ftp.avaya.com/incoming/Up1cku9/AvayaT4APP/IPT/B179PatchesAndSoftware/2.4.2.13/B179-IPT-SIP-R2_4_2_13-111816.zip)

### Patch install instructions

n/a

### Service-interrupting?

No

### Verification

Login to WebUI and check the Firmware version.

The phone must show Firmware (FW) version 2.4.2.12 or 2.4.2.13, as per the installed patch.

### Failure

n/a

### Patch uninstall instructions

n/a

## Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

### Security risks

n/a

## Avaya Security Vulnerability Classification

Not Susceptible

## Mitigation

n/a

**If you require further information or assistance please contact your Authorized Service Provider, or visit [support.avaya.com](http://support.avaya.com). There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support [Terms of Use](#).**

**Disclaimer:** ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.  
All other trademarks are the property of their respective owners.

## BusinessPartner Notes

Additional information for BusinessPartners

n/a

## Avaya Notes

Additional information for Tier 3, Tier 4, and development

n/a