AVAYA

Product Support Notice

PSN #	PSN004134u				
Original publication date: 28-Jan-14. This is Issue #02, published date: 25-Mar-14.		Severity/risk level	High	Urgency	Immediately
Name of problem	Downgrade of 16xx H.323 phones to firmware 1.3.2 from 1.3.3 or 1.3.4 results in duplicate/default MAC and Serial Number				

Products affected

1603, 1603-I, 1603-I-SW,1608,1608-I, 1616,1616-I

Problem description

Downgrading 16xx IP Deskphones from firmware version 1.3.3 or 1.3.4.B to 1.3.2 will cause the unique MAC address and Serial Number provided on the manufacture label to be converted to default values (MAC = 00:1B:4F:13:70:08, SN = 123456789012). All phones downgraded from 1.3.3 or 1.3.4.B to 1.3.2 will be affected, resulting in phones having the same MAC (duplicated) address, and once this happens these phones cannot be recovered in the field. After implementation, phones downgraded from 1.3.3 or 1.3.4.B to 1.3.2 may not be allowed on the customer network as the phone MAC address will be the default value and be viewed as a duplicate MAC address in presentation to the network.

Firmware version 1.3.4.D, available since March 2014 does not cause this issue. Avaya recommends that Customers should upgrade their file server(s) and all 1600 Series phones to 1.3.4.D at their earliest opportunity. Note that once 1600 Series IP Deskphones in the installed base are upgraded to 1.3.4.D, they can be downgraded to earlier firmware loads without causing the duplicate MAC / Serial Number issue, but these units are still vulnerable to firmware corruption issues that have been documented in previous Release Notes. Upgrading the 1600 Series IP Deskphones to 1.3.4.D or higher will enable customers to avoid these previously documented issues entirely.

Upcoming Firmware version 1.3.5 will include the same fix as 1.3.4.D, but in addition 1600 Series IP Deskphones manufactured after April 14th, 2014, with Firmware version 1.3.4.D or 1.3.5 pre-loaded onto them will also have a new Hardware ID which prevents those units from accepting a Firmware downgrade below R1.3.5.

Resolution

1. Ensure that the customers file server is using 1.3.3 or 1.3.4.D. This is crucial, as newly manufactured phones are preloaded with firmware 1.3.3. Connecting them to the network where 1.3.2 is used will cause the phone to downgrade and get into the default/duplicate MAC condition. Please check for the latest 16xx H.323 firmware on the Avaya Support website. 1.3 Maintenance Release 4 (1.3.4.D) is the most current firmware. Avaya recommends customers upgrade their file server(s) and all 1600 Series IP Deskphones to R1.3.4.D at their earliest convenience.

2. 1600 Series IP Deskphones downgraded from 1.3.3 or 1.3.4.B to 1.3.2 resulting in the defaulted/duplicated MAC address condition cannot be recovered in the field, and should be returned to Avaya under warranty, ideally within the first 90 days under the DOA process, for a free of charge replacement.

3. Future Resolution – As of April 14th, 2014, all newly manufactured 1600 Series IP Deskphones will be pre-loaded with Firmware version 1.3.4.D or higher, and will have a new Hardware ID which prevents these units from being downgraded to earlier firmware. Customers will be able to attach these units to their systems seamlessly, since they will reject any firmware download from the file server. It is still recommended that customers upgrade file server(s) to have the most current firmware release on them. At the time of publication of this PSN update, it is recommended that customers upgrade their file server(s) and all 1600 Series phones to 1.3.4.D at their earliest opportunity.

Workaround or alternative remediation

n/a

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	
n/a	
Patch install instructions	Service-interrupting?
n/a	No
Verification	
n/a	
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. 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.