AVAYA

Product Support Notice

PSN # PSN004134u					
Original publication date: 28-Jan-14. This is Issue #01, published date: 28-Jan-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 H.323 phones from firmware version 1.3.3 or 1.3.4 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 to 1.3.2 will be affected, resulting in phones having the same MAC (duplicated) address, and cannot be recovered in the field. 1.3.5 (and future releases) will fix this problem.

Example behavior for affected phones

- After implementation, phones downgraded from 1.3.3 or 1.3.4 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.

Resolution

1. Ensure that the customers file server is using 1.3.3 or 1.3.4. 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.
   a. Please check for the latest 16xx H.323 firmware on the Avaya Support website. 1.3 Maintenance Release 4 (1.3.4) is the most current firmware release as of August 27, 2013.

2. Phones downgraded from 1.3.3 or 1.3.4 to 1.3.2 resulting in the defaulted/duplicated MAC address condition need to be replaced via the Avaya Return Materials Authorization (RMA) process.

3. Future Resolution – There will be a future software version released to Avaya Support website that prevents the downgrade of any phone 1.3.3 or newer to 1.3.2. Release Date TBD.

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.