Spectralink IP-DECT Server 400
Spectralink IP-DECT Server 6500
Spectralink IP-DECT Base Station
Spectralink IP-DECT Media Resource

Release Notes Q2 2014

Firmware Version PCS14A_

Table of Contents

Revision History

Date	*Description*
2013-03-11	Release notes for PCS13B_
2013-06-11	Release notes for PCS13E_
2013-09-24	Release notes for PCS13F_.
2013-12-16	Release notes for PCS14__
2014-03-24	Release notes for PCS14A_

Introduction

Release

The products in the Spectralink IP-DECT portfolio are based on the same software platform. These release notes includes information about software updates and corrections for the following products:

- Spectralink IP-DECT Server 400 (previously known as KIRK Wireless Server 400).
- Spectralink IP-DECT Server 6500 (previously known as KIRK Wireless Server 6500).
- Spectralink IP-DECT Base Station
- Spectralink IP-DECT Media Resource (previously known as KIRK Media Resource 6500).

This version specifically applies to version PCS14A_ of the firmware. The release replaces the PCS14__ release as the latest generally available (GA) release.

Important Notes

Some features require specific versions of the firmware loaded into the base stations or media resources.

Feature License and Platform Limitations

The following table summarizes features that require a particular hardware platform and/or a license key for activation.

Feature	*Comment*
Backup Spectralink IP-DECT Server Redundancy with ARI Swap License	License required. Part number 14075260
Master Spectralink IP-DECT Server Redundancy	License required. Part number 14075250
Software Security Package (TLS, SRTP)	License required. Part number 14075280
Microsoft Lync Interop incl. Software Security	License required.

Feature	*Comment*
Package (TLS, SRTP)	Part number 14075270
Automatic Alarm Call	License required. Part number 14075450
Handset sharing license	License required. Part number 14075460
Cisco Unified CM Enhanced features	License required. Part number 14075490, 14075495

System Requirements

Hardware

Hardware Platform	*Description*
KWS6500 HW PCS 01__ or newer	KWS6500 Server
Media Resource 6500 HW PCS 01__ or newer	Media Resource 6500
KWS400 HW PCS 09__ or newer	KWS400 Server
IP-DECT Base Station HW PCS 09__ or newer	IP-DECT Base Station

Software

The IP-DECT Server communicates with media resources and base stations using a version controlled communication protocol.

When an IP-DECT Server is updated with new firmware, this might introduce a new version of the communication protocol towards either media resource or base station.

To minimize downtime when an IP-DECT Server, media resources and base stations are updated with new firmware, the following approach is recommended.

Update all infrastructure units: base stations, media resources, and IP-DECT Server to new firmware before rebooting any of these. The new firmware and thus the new protocol will not be active until the unit has been rebooted. When the firmware update of all units is successful, reboot the system in the following order: Base stations first, then media resources, and finally the IP-DECT Server.

The reason for this recommendation is that the base stations and the media resources can be rebooted from the IP-DECT Server and this is much easier than logging into each unit manually. If the IP-DECT Server is updated first, it might no longer be possible to control the base stations from the IP-DECT Server.

Often new firmware of, for example, the IP-DECT Server allows for - but does not require - an update of media resource and base station firmware.

The following table lists the firmware revisions of the IP-DECT Server that introduce new protocol versions and therefore require an update of base stations and media resources.

IP-DECT Server Firmware	*Media resource protocol*	*Base station protocol*	*Media resource Firmware*	*Base station Firmware*
PCS13E_	12	7	PCS13B_	PCS13E_

IP-DECT Server Firmware	*Media resource protocol*	*Base station protocol*	*Media resource Firmware*	*Base station Firmware*
PCS13B_	12	6	PCS13B_	PCS13A_
PCS13__	11	6	PCS12D_	PCS13A_

Distribution Files

Download the latest software at the Spectralink Support Portal. Sign up for Spectralink's technical newsletter Tech Point to get updated on new software releases and technical information.

Changes

Unless specifically mentioned, the described changes are relevant for all products based on the entire Spectralink IP-DECT portfolio. If an individual change is relevant only for one or some products, this is specifically mentioned before the description of the individual change (example: **IP-DECT Base Station only**).

Version PCS14A_ – Q2, 2014

Added or Changed Features

- IMPORTANT the default password for the WEB GUI has been changed from " ip6000" to "admin". This change has been made in order to use the same default password for all current IP DECT infrastructure components. This change has no impact if the default password has been changed or if the Configuration|Security settings have been saved, in which case the default password would have been saved to the configuration file.
- **IP-DECT Server 400 and 6500 only**
  Integration with Cisco Unified CM has been improved significantly. The IP-DECT Server can now be connected to the Cisco Unified CM as a known phone type instead of just being a third party SIP device. This gives handsets connected to the IP-DECT Server access to additional features not supported for third party SIP devices:

  Music-On-Hold.
  The handsets can put the remote party on hold with Music-On-Hold.

  Call pickup.
  The handsets have access to various kinds of call pickup by dialing feature codes.

  Meet-Me Conferencing.
  The handsets can initiate a Meet-Me based conference by dialing a feature code.

  Call Forward Unconditional.
  Call Forward Unconditional is controlled within the Cisco Unified CM instead of locally in the IP-DECT Server. This means that if Call Forward Unconditional is enabled from the DECT handset other devices sharing the same line in the Cisco Unified CM will also be forwarded. Similarly if Call Forward Unconditional is enabled on a shared line device it will be displayed on the DECT handset.

  Furthermore, administration of many DECT handsets on a Cisco Unified CM has been improved. The IP-DECT Server now supports exporting CSV files, which can be imported directly into the Cisco Unified CM Bulk Administration.

The improved integration requires a COP file to be loaded into the Cisco Unified CM and a license to be loaded into the IP-DECT Server. Please refer to the Cisco Unified CM integration application note for further details. If no license is loaded into the IP-DECT Server it can still be connected to the Cisco Unified CM as a third party SIP device and nothing is changed.

- The tables used to display information on the WEB GUI have been improved in order to better handle many users and base stations. The improvements include a search function, allowing searching all table data for a specific string, and a sort function, allowing sorting the table data with respect to any column. Finally, a pagination function, allowing breaking down the table data into suitable page sizes is now available.
- **IP-DECT Server 400 and 6500 only**
  The IP DECT server now supports internationalized system messages sent to handsets. The status and error texts send from the DECT Server to the handsets are available in Danish, Dutch, English, French, German, Italian, Norwegian, Portuguese, Russian, Spanish and Swedish. This is to give a better user experience for the end users. The language can be configured on the Configuration|Wireless Server GUI page. This does neither replace - nor affect - the handset language configured locally in the phone.
- **IP-DECT Server 400 and IP-Base station only**
  The IP-DECT Server 400 and Base station now supports the mounting of an external antenna. When an external antenna is detected the base station will automatically include the external antenna in the antenna selection algorithm, and issue an INFO level log message: "External Antenna detected". If an external antenna is un-mounted the antenna selection algorithm will automatically revert to using internal antennas only, and issue an INFO level log message: "External Antenna un mounted."
- **IP-DECT Server 400 and 6500 only**
  Optimize the internal signaling in the IP DECT server to better handle if the SDP from the other end is received late in the call setup process for incoming calls. Typically SDP from the other end is included in the incoming INVITE. However in some PBXs/scenarios no SDP is received before the final ACK. Previously a delay in the audio setup could be experienced if the ACK was received very late. DECTESC-524 describes an issue with audio transmission starting late, after answering an incoming call on a DECT handset.
- **IP-DECT Server 400 and IP-Base station only**
  Improved handling of synchronization, the base station will not attempt a shift to secondary sync master if a secondary is not defined.
- **IP-DECT Server 400 and IP-Base station only**
  The algorithm used for synchronization over-the-air has been improved. The sync over air algorithm has been made less prone to oscillating by adding

integration in the frequency adjustment feedback loop.
Slicer setting corrected to 2 bit implementing fixed/measured slicing for improved noise immunity over the coverage range.
Synch fall-over to another DECT bearer added to be more robust towards channel and sliding collision caused by foreign systems.
Improved search to find another bearer on the same base when dummy bearer is lost.

- **IP-DECT Server 400 and 6500 only**
  The IP DECT server WEB GUI now supports displaying the HW version, SW version, Production ID and Production date for Spectralink handsets. The same information is available in the users.xml part of a log export generated by Status|Logs|Export. The information is sent by newer handsets at subscription & location registration.
- **IP-DECT Server 400 and 6500 only**
  The IP DECT server will, starting with this release, accept a new incoming call while an incoming call release is pending. Before this change the IP-DECT Server would reject the new incoming call with a busy response. Now, the new call is accepted and sent to the handset, as soon as the pending release is completed. The IP-DECT Server is required to accept this signaling in order to handle Cisco Unified CM call pickup and some kinds of hunt groups. For this to work perfectly a handset firmware update is required as well. If the handset firmware is not updated the new incoming call may be reported as an abnormal call release instead of a busy.
- **IP-DECT Server 400 and 6500 only**
  Release LCE (lower layer) instance correctly when an incoming call is released. The LCE instance was not released correctly when an incoming call was released and if a new call was received within a few seconds after the release, it ended as an abnormal release. This addresses DECTESC-522 where a hunt group initiates new calls to a handset shortly after the release of the previous call. In the specific use case reported, one of the users in a ring group is busy, then the ring group is being called and while the other handsets in the ring group are ringing, the busy member of the ring group terminates the call and gets (immediately) a new incoming call, as it is part of the same ring group. Previously the IP-DECT Server would respond "Temporarily not available"; now the IP-DECT server can handle the second incoming call.
- **IP-DECT Server 400 and 6500 only**
  Handle multiple 180 Ringing responses. In scenarios where an outgoing call is forked or forwarded multiple 180 Ringing responses may be received from different endpoints. The first ringing response was sent to the handset but any additional ringing responses were dropped. This caused the handset display not to be updated correctly. Now all ringing responses are sent to the handset and the display will be updated correctly.

- Change the WEB_GUI date display format from DD-MM-YYYY to YYYY-MM-DD. The new format is more standardized and is less ambiguous especially for users in the US.
- **IP-DECT Server 400 and 6500 only**
  In some call tear-down scenarios the IP DECT server previously potentially would attempt to terminate a media session after the termination of the DECT Call using the media session. This would result in logging a "Session Free: lid (##) not in use" message with level critical. Now the IP DECT server will skip releasing the media session when it has been released by the DECT call.
- **IP-DECT Server 400 and 6500 only**
  Call state handling has been changed. When a SIP CANCEL request is received early in a call attempt to release the link layer with a LinkRelease instead of attempting to release the call control layer with a CCRelease.
- **IP-DECT Server 400 and 6500 only**
  Make sure that STUN information sent to MR is correct if UDP or TCP parameters are missing from the Lync server. Correct handling of missing UDP or TCP address for TURN. With this change the IP DECT Server is more robust towards missing UDP or TCP parameters in STUN/TURN parameters provisioned by a LYNC server.
- **IP-DECT Server 400 and 6500 only**
  The IP DECT server will only accept Microsoft Lync conference invitations if they contain audio. Previously the IP-DECT Server did not check for audio in a conference invitation before it was accepted and this caused unintended behaviour.
- **IP-DECT Server 400 and 6500 only**
  Show phase/offset in neighbours list. This value represents the offset between a base and the other bases (neighbours), it can see over the air. Handsets (and base stations) can compensate for measured offsets of +/- 10, thus a large offset is not necessarily a problem, however the neighbours with strongest signal strength (RSSI) should have an offset within +/- 10.
- **IP-DECT Server 400 and 6500 only**
  On incoming text calls ignore 0-9,*,# to align with DECT Server 2500/8000. Before this change pressing these keys before pressing ok to accept the incoming text call would result in the release of the text call with cause 84. This is based on feedback from Connexall.
  Pass R,X,O,H through before a MSF text call is accepted in order to signal what button the user pressed to release the text call. On request from Connexall. This can be used by an application to determine why a text call was released if not by pressing ok or reject (i.e. hook, etc.)
- **IP-DECT Server 400 and 6500 only**
  If the server does not allow using SW-G729 codec (which requires a license on the server) remove G.729 support. This addresses DECTESC-514 "KWS400 G.729 works without license"

- Adapt to new time zone for Moscow. Moscow is no longer using Daylight Savings Time, and is fixed at GMT+4; this is now reflected in the time-zone string for Moscow.
- **IP-DECT Server 400 and 6500 only**
  Minor changes to WEB_GUI for administering base stations. The Administration|Base station table has undergone minor layout changes and no longer displays which synchronization source is currently used for synchronization.
- **IP-DECT Server 400 and 6500 only**
  Respect CLI restrictions sent from Cisco Unified CM in Remote-Party-ID header. The Remote-Party-ID header has a privacy part, which can be used to control whether or not Display Name and Number should be displayed by the endpoint. If either are marked as restricted the IP-DECT server will not send them to the handset.
- **IP-DECT Server 400 and 6500 only**
  The IP DECT Server now supports handling SIP bodies starting with \n. Previously this was not supported and Cisco Unified CM has been seen to send SIP bodies starting with \n in connection with remote call control.
- **IP-DECT Server 400 and 6500 only**
  Incoming early media handling has been improved. The IP DECT server now handles a=inactive in SDP in a 1XX response.
- **IP-DECT Server 400 and 6500 only**
  Added a new setting to the GUI: "TCP ephemeral port in contact address". Enable this to add the TCP ephemeral port (the local TCP port of the outgoing connection) to the contact header used in outgoing SIP messages. Otherwise the local listening port is used.
- **IP-DECT Server 400 and 6500 only**
  Add the correct port number to the SIP contact header when configured with a local port different from 5060 or configured with endpoint separate ports enabled. Without this correction no port number was added and the default 5060 was assumed.
- **IP-DECT Server 400 and 6500 only**
  Delete GRUU when registration data is cleaned up. When connected to a SIP server that supports Globally Routable UA URI (GRUU) a GRUU is retrieved as part of the registration process. The GRUU should be deleted when the registration data is reset, because a new one is received on the next successful registration.
- **IP-DECT Server 400 and 6500 only**
  Starting with this release the IP DECT Server will support a maximum of 32 allowed peers in a forked call. Previously a maximum of 8 were supported. One use case affected by this change is an outgoing call from a DECT phone to a Lync user who has a ring group (either Team group or Delegate) that rings multiple Lync users. Previously if the group had more than 8 members and no-

one answered, the call would be diverted to voicemail after some period of time and the DECT phone making the call would display "Media Failed". Now - the call is transferred successfully to voicemail as long as the number of members in the group is 32 or less. This issue was reported in DECTESC-477.

- **IP-DECT Server 400 and IP-Base station only**
  The base station will now send phase/offset to the IP DECT Server in neighbours list. This value represents the offset between a base and the other bases (neighbours) it can see over the air.
- **IP-DECT Server 400 and 6500 only**
  Handle XML escape characters in description when generating rfps.xml.
- **IP-DECT Server 400 and 6500 only**
  Do not log a notice message when "481 Call Leg/Transaction Does Not Exist" is received for BYE. This is not uncommon in transfer scenarios and is not a problem.
- Degrade log message from warning to debug when the HTTP connection is lost while displaying the log. This is not uncommon and not a problem for the system.

Removed Features

None

Corrections

- **IP-DECT Server 400 and 6500 only**
  Use the correct component index when creating TCP srflx candidates and correct cleanup of srflx candidates. This resolves an issue reported in DECTESC-515 which describes a situation where it is not possible to make calls from a DECT handset to a Microsoft Lync client.
- **IP-DECT Server 400 and 6500 only**
  Save SRTP authentication parameter so we do not trigger a new SRTP creation on each configure. Furthermore do not create new SRTP if no parameters have changed. Before this change sequence numbers on SRTCP could get out of sync with what a Mediation server would expect, which could lead to the disconnection of calls. This resolves an issue reported in DECTESC-528. In a Microsoft Lync setup if an external user is on-hold from a DECT handset, the external party might be disconnected after 30 seconds.
- **IP-DECT Server 400 and 6500 only**
  Fix a bug with SIP dialog event package which is used for Busy Lamp Function (BLF) and by Cisco Unified CM. When an outgoing call was initiated the NOTIFY dialog event was sent before the dialog was initialized and data was invalid.
- **IP-DECT Server 400 and 6500 only**
  When sending peer reflexive ICE candidates, add correct relative address and

select correct candidate for RTCP. This resolves an issue reported in DECTESC-527 concerning Skype calls in a setup with Lync 2013 and IP-DECT server. An external Skype user calls over federation service and the call can be answered with a Lync Client or a handset on the IP DECT server. If the call is answered with the DECT device, the call would terminate after a few seconds.

- **IP-DECT Server 400 and 6500 only**
  If handset sharing is activated always save user access code in users file. Previously if handset sharing was activated and a device was bound to a user, a change of the user PIN would not be persisted and the IP DECT server would revert to the old PIN after a reboot.
- **IP-DECT Server 400 and 6500 only**
  Reset in-memory SIP authentication data when user parameters related to authentication is changed. The authentication mechanism was not reset correctly when user data with impact on the authentication was modified. This potentially had the effect, that administrator changes did not take effect until the system was restarted, or the user was disabled and enabled again.
- **IP-DECT Server 400 and IP-Base station only**
  The startup sequence of processes during a boot has been changed. With the previous startup sequence, a firmware update could result in the unit stopping to do provisioning checks. This means the unit would need to be manually rebooted or power-cycled after the update to start the provisioning checks again. The issue exists potentially in older versions of the firmware, thus downgrading from version PCS14A_ to a previous version might still exhibit this problem.
- **IP-DECT Server 400 and 6500 only**
  Previously the IP DECT Server could in some cases attempt to access TCP connection data on TCP connections which were no longer valid. This has been corrected.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	language	Specifies the language used for sending system messages to the phones. Values: da danish, de german, en english, es spanish, fr french, it italian, nl dutch, no norwegian, pt portuguese, ru russian, sv swedish. Default: en.
config.xml	Added	feature_codes.pickup.local	Specifies the feature code used for enabling call pickup on Cisco Unified

File	*Action*	*Parameter*	*Description*
			CM. Values: The feature code users must dial for call pickup local. Default: **3
config.xml	Added	feature_codes.pickup.group_other	Specifies the feature code used for enabling call pickup other group on Cisco Unified CM. Values: The feature code users must dial for call pickup other group. Default: **8
config.xml	Added	feature_codes.conference.meetme	Specifies the feature code used for enabling Meet-Me Conference on Cisco Unified CM. Values: The feature code users must dial for Meet-Me Conference. Default: **5$
config.xml	Added	sip.tcp_contact_ephemeral_port	Enable this to add the TCP ephemeral port (the local TCP port of the outgoing connection) to the contact header used in outgoing SIP messages. Otherwise the local listening port is used. Values: true/false Default: false.

Version PCS14__ – Q1, 2014

Added or Changed Features

- The server now supports using multicast for communicating to the base stations. This can be utilized to support up to 1024 base stations on an IP DECT Server 6500.
  To enable this, configure a multicast address in Configuration|Wireless Server| Multicast address. If multicast is not enabled, the server will not allow more than 256 base stations. Furthermore, if multicast is enabled, old base stations that do not support multicast are marked as outdated.

- **IP-DECT Server 400 and 6500 only**
  Support for handset sharing is implemented (license required).
  The traditional concept of a communication device is to have a device (phone) assigned to a number/SIP username.
  The basic concept of handset sharing is to break the link between the device and the number, and enable any number/user to sign-in to any device. Refer to separate application note describing handset sharing for additional information.
- **IP-DECT Server 400 and 6500 only**
  The DECT Server is now able to handle call forking to a mix of ICE and non-ICE enabled endpoints. Previously, a scenario with forking to a mix of ICE and non-ICE enabled endpoints could result in disabling ICE for the complete call. This sometimes resulted in issues with calls from DECT handsets to Lync clients. Sometimes the call would not be established, and an ERROR 500 would be displayed in the DECT handset display, when the call is answered. This issue has been seen in the field in a Microsoft Lync configuration, and was reported in DECTESC-507.
- **IP-DECT Server 400 and 6500 only**
  The server no longer re-transmits SIP requests when TCP or TLS is used as transport protocol. When a reliable transport is used, SIP request are not allowed to be retransmitted on timeout errors. Microsoft Lync was not able to handle these incorrect re-transmissions and spurious un-explainable errors occurred as a side-effect.
- **IP-DECT Server 400 and 6500 only**
  Abort a handover if the media resource fails to start handover. This aborts the handover faster and more gracefully, and allows the server to log an error if it happens.
- **IP-DECT Server 400 and 6500 only**
  Simplified the system backup/restore functionality. Earlier, parts of the complete backup could be restored individually. However, this could cause inconsistencies in the restored data due to interdependencies between different data such as users and DECT subscription.
- **IP-DECT Server 400 and 6500 only**
  The protocol for communication between the master and the slave server in a redundancy setup has been made more robust. Furthermore, there was a problem when more than 1000 users were replicated. This issue has been fixed.
- **IP-DECT Server 400 and 6500 only**
  If the handset and server call hold state get out of sync, it is handled gracefully, and does not result in the logging of an error. Without this correction, the handset could get stuck in a call hold state.
- **IP-DECT Server 400 and 6500 only**
  In the case where a media resource or a base station loses the connection to a server, the device will initiate a new connection to the server. The server will now accept a new connection from a device, before the server has detected a

connection failure from the same device. This eliminates the "Already connected on socket" error, and reduces the time it takes the new connection to be ready for use.

- **IP-DECT Server 400 and 6500 only**
  Since ICE was introduced in the KGAP, an abnormal call release in an incoming call would be logged with "base: Unknown", until the first handover was performed. Now, the time window where an abnormal release can report an unknown base station has been reduced drastically.

  Furthermore, information about which base station the current call is on is now improved. Previously, the part of the server that logs an abnormal call release did not know which base station the current call was on for any outgoing call before digits were received. For example, any abnormal call release in an outgoing call that was initiated by pressing off-hook (overlap dialing), resulted in an abnormal call release log entry with base: Unknown.
- **IP-DECT Server 400 and 6500 only**
  Do not check for blacklisting for the current registrar when connected to Lync or "Send all messages to current registrar" is enabled. Some SIP servers do not support this and require a re-registration to switch to another proxy.
- **IP-DECT Server 400 and IP-Base station only**
  Re-factored handling of DECT-module.
  - If a high number of connections are established, a new algorithm moves the dummy bearer to make the remaining idle slots visible to the handsets. This will make it easier for handsets to establish a new connection when many connections are already established.
  - Burst Mode Controller frequency adjustment is controlled by IP CPU for higher precision.
  - Re-introduced keep-alive signaling between the higher layers of the base station and the lower layers handling the DECT module (BMC ping). This is introduced as a security precaution, to ensure that the higher layers detect a failure in the lower layers as soon as possible.
  - Subcell mode handling implemented. This is required preparation for handling of the upcoming external antenna option.
  - The functionality for getting a RSSI map for other base stations seen in the air has been improved.
- If the system kernel hangs, it now automatically reboots after 30 seconds.
- The version of the linux kernel is bumped to version to 3.10.19.
- **IP-DECT Server 400 and 6500 only**
  The system ARI is now displayed in the List Users part of the web-gui. This way, the ARI is right at hand when subscribing handsets while monitoring progress on the List Users gui page.
- **IP-DECT Server 400 and 6500 only**
  When exporting users to a CSV or XML file using Users|Import/export, the users are sorted by username instead of by IPEI.

- **IP-DECT Server 400 and 6500 only**
  The procedure for delivering standby texts to handsets has been refactored and improved. It was previously allowed to update the standby text on the handset even in the case where an application was connected to the handset. However, this would tear down the connection between the application and the handset. As a result, changing the standby text from the GUI while the handset was in an active MSF call (e.g. corporate phonebook) meant that the server would end up in a state where it was not possible to update the standby text on the specific handset.
- **IP-DECT Server 400 and 6500 only**
  An IPEI is required before a SIP user registration is performed.
- **IP-DECT Server 400 and 6500 only**
  The free text search in the List Users part of the web-gui now supports special characters. This, for example, allows searching for a user with special characters in the display name.
- **IP-DECT Server 400 and 6500 only**
  Take care of duplicate RPNs when performing synchronization loop check. Previously. duplicate RPNs would confuse the loop check algorithm and potentially lead to misleading results such as the reporting of false positives.
- **IP-DECT Server 400 and 6500 only**
  Improved the way an address for internal RTP is selected. This avoids some connection problems in mixed IPv4/IPv6 setups.
- **IP-DECT Server 400 and IP-Base station only**
  Make sure to log at least a notice level message when the connection from the base station to the DECT server is lost.
- **IP-DECT Server 400 and 6500 only**
  When configuring a base station as freerunning, set primary and secondary sync to its own RPN and not 0. This is less misleading.
- The packet capture no longer includes the ethernet checksum bytes at the end of the packet. This matches standard pcap file conventions.
- Introduced new Equipment Manufacturer Code (0x0298), which has been used in production from (approx.) October 2013.
- Cosmetic change to Spectralink web-gui theme for submenus.

Removed Features

- **IP-DECT Server 400 and 6500 only**
  The Auto-create users functionality controlled by the Configuration|Wireless Server|Autocreate users setting has become obsolete and has been removed. If a handset with an unknown IPEI is to be allowed to subscribe to the system, the recommended approach is to create a SIP user without specifying an IPEI. When subscribing a handset with an unknown IPEI, it is automatically created/associated with the first available SIP user without a specified IPEI.

Corrections

- If the "force https" setting was enabled to ensure that exclusively encrypted access was available to the user interface, an unwanted side effect would occur. The export logs functionality would result in the export of empty log files. Specifically, all HTML and XML files would be empty. This issue was reported in DECTESC-500. Additionally, it was not possible to perform a central firmware upgrade of media resources and base stations from the server if "force https" was enabled on the server.
- **IP-DECT Server 400 and 6500 only**
  Fixed a problem where ACK send to a hostname could not be TLS validated because the hostname was reset during DNS resolution. This error was seen in some Microsoft Lync installations, when the Lync server failed to answer quickly enough.
- **IP-DECT Server 400 and 6500 only**
  Avoid a buffer overflow and log a notice message if more than 20 ICE candidates are received in SDP.
  If the server received an excessive amount of ICE candidates in an incoming SDP message (more than 20) the server could restart. If more candidates are received than the server can handle, the remaining ICE candidates are skipped and a notice message is logged to the message log. This issue was seen in the field in a Microsoft Lync setup and was reported in DECTESC-496.
- **IP-DECT Server 400 and 6500 only**
  In a setup with redundancy, enabled changes to the base station synchronization settings were in some cases not replicated correctly between the master and the slave server. As a result changes to the synchronization chain would not take effect until the base stations were rebooted.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	rfp.multicast.address	Enables multicast for base station signaling and specifies the address to use. Values: A valid IPv4/IPv6 multicast address. Default: None
config.xml	Added	rfp.multicast.ttl	Specifies the TTL of multicast messages send to the base stations Values: 1-255 Default: 1 which will limit the multicast to the local LAN. The value must be increased to extend the multicast outside the LAN.
config.xml	Removed	dect.auto_create_users	If enabled, a user is

File	*Action*	*Parameter*	*Description*
			automatically added to the Server when a DECT handset tries to subscribe to a DECT system. Values: true/false Default: false.

Version PCS13F_ – Q4, 2013

Added or Changed Features

- Previously, the attempt to correct read-errors on the internal flash, could result in the device not booting. The read-error correction has been improved to eliminate these scenarios. IMPORTANT read-errors on the internal flash may occur at some point due to wear of the flash. If the device has pre-PCS13F_ firmware, it is unable to boot if this happens. Therefore, it is highly recommended that you update to the new firmware. If the failure scenario mentioned above occurs before the firmware is updated, the device has to be returned for repair.
- The WEB-gui has been rebranded and renamed with the new Spectralink color scheme and logo.

Previous model name	***New model name***
KIRK Wireless Server 400	Spectralink IP-DECT Server 400
KIRK Wireless Server 6500	Spectralink IP-DECT Server 6500
KIRK Media Resource 6500	Spectralink IP-DECT Media Resource
KIRK IP Base Station 6500	Spectralink IP-DECT Base Station

- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The KIRK/Spectralink handsets have been renamed according to the following table.

Previous model name	***New model name***
KIRK 4020	Spectralink 7420
KIRK 4040	Spectralink 7440
KIRK 4080	Spectralink 7480

Previous model name	***New model name***
KIRK 5020	Spectralink 7520
KIRK 5040	Spectralink 7540
KIRK 6020	Spectralink 7620
KIRK 6040	Spectralink 7640
KIRK 7010	Spectralink 7710
KIRK 7020	Spectralink 7720
KIRK 7040	Spectralink 7740
KIRK Butterfly	Spectralink Butterfly
KIRK Site Survey	Spectralink 7000 Site Survey

- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The integration with Microsoft Lync has been improved. Users on the IP-DECT Server now support the Microsoft Lync framework for being invited to a Lync conference. When a user is invited to a conference, the following three steps are involved:

  Step one: When a Lync client invites a user to a conference, a special conference invitation is received by the IP-DECT Server. This is the message that goes from the “inviter” to the “invitee” giving the URI of the conference focus. The message is a special SIP INVITE request with information about the conference instead of normal Session Description Protocol content in the message body.

  Step two: The IP-DECT Server starts a signaling session with the conference focus, which is accomplished with another INVITE with a special content type of “application/cccp+xml.” CCCP stands for Centralized Conference Control Protocol, which is the protocol Lync uses for communication with conference server roles. Once this session is established, the Lync user is connected to the conference, but does not yet have any media sessions established. (This is the point where you can see someone in the conference roster, but the phone icon, IM icon, etc. next to their name is still grayed out.)

  Step three: The last step is to connect to the conference media. For an audio conference, this means dialing in to the audio/video MCU. The MCU, or Multipoint Control Unit, is the Lync component that mixes media for the conference and distributes it to the participants. When connected, media flows directly to the MCU. The last step is accomplished with a normal INVITE with Session Description Protocol content used to negotiate media transmission between the Lync user and the A/V MCU. Once this signaling session is established, and media begins flowing between the Lync user and the MCU, the conference join is complete.

- The implementation of TLS/SSL authentication of clients connecting to the device has been updated. The previous implementation did not handle clients that start with a SSL2/3 handshake well. This problem was identified in the field caused by Perl scripts connecting to the device for supervision purposes.
- Duplicate IP addresses are now handled more gracefully. Prior to using an IP address, the device checks if the address is in use by another device. If configured for DHCP, the device declines the duplicate address and requests a new one. If configured for a static IP address with an address conflict, the device does not bring up its network interface and it thereby avoids disrupting the service of the conflicting device.
- Handling of IPv6 addresses has been updated.
  On the base station menu Configuration|Base Station, it is now possible to enter an IPv6 address for the IP-DECT Server to which the base station should connect to.
  On the IP-DECT Server menu Administration|Base station and Administration|Media Resource, the link to a base station and a media resource can now handle an IPv6 address.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  If the base station or media resource is local (located on the IP-DECT Server), the link to the loopback address in RFP and MR administration, has been removed.
- The handling of Network Time Protocol (NTP) has been updated. The amount of time that can be adjusted is increased from 200 milliseconds to 1 second. Furthermore, the minimum delay for the NTP response filter is increased from 10 milliseconds to 20 milliseconds. This gives a smoother operation of the NTP handling and should reduce the number of NTP notice messages in the message log, especially in scenarios with a jittery IP connection to the NTP server.
- **Only relevant for Spectralink IP-DECT Base Station**
  Make the uplane handling on the base station more robust. Do not allow associating a new RTP resource, if one is already associated. Do not allow requesting an uplane, if a RTP resource cannot be allocated. Report to the IP-DECT Server if an uplane cannot be requested or connected.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The messaging handling in the IP-DECT Server has been refactored, and range checks for message text and callback numbers have been improved. The IP-DECT Server is now prepared for handling longer text messages and longer callback numbers. Furthermore, the IP-DECT Server now supports sending more information in a single DECT protocol message than before. The maximum length of callback numbers is now 64 characters (previously 24). The

maximum length of MSF messages is now 180 characters (previously 72). Whether to use old or new limits is controlled by the setting dect.allow_long_messages. If this setting is false (default), the old limits are enforced. WARNING this feature is not yet supported by the handsets, thus setting dect.allow_long_mesages to true is not recommended at this point.

- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  During a transfer, the IP-DECT Server now sends a BYE from the transferee to the transferor after the call to the transfer target has been established. This shortens the window where the transferee is not able to handle REFERs etc. from the transfer target. The old behavior can be restored by setting sip.send_bye_with_refer_notify=false. This solves DECTESC-485 SIP Group overflow transfer not working. The issue was identified in an interop test with Shoretel.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The media resource sends the build number of the running firmware to the KWS in the startup message.
- **Only relevant for IP-DECT Base Station**
  The base station sends the build number of the running firmware to the IP-DECT Server in the startup message.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The IP-DECT Server Web-gui now shows the build number of the firmware on IP-DECT Media Resources and IP-DECT Base Stations in the case of development/beta versions of the firmware.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The IP-DECT Server no longer responds with 400 Bad Request, when a SIP server is terminating a SIP subscription. Specifically, Microsoft Lync sometimes terminates the SIP subscription for presence, and the IP-DECT Server should respond with 200 OK. The wrong response can have caused problems in some presence scenarios.
- Make remote syslog work with dynamically changed IP address. Previously, if the device changed IP address during operation, it would stop sending remote syslog messages.
- The Linux kernel has been updated to version 3.9.9.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  Log an error on the IP-DECT Server, if an uplane cannot be requested or connected on a base station. Earlier, this was only logged locally on the base station.

- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  Log info message when provisioning download is started in order to ease debugging.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  Make the RFP number look the same in the log messages. When referring to RFP number use RfpNo not RFP.
- Make Status|Logs use HTML-safe formatting for log messages. Some messages might contain data which break HTML formatting. This is now escaped correctly.
- Add core dumping feature and include core files in exported logs. This is strictly for debugging/developer purposes. Per default this feature is not enabled, it is controlled by config set/get debug.coredumps (true/false).
- **Only relevant for Spectralink IP-DECT Server 400**
  The firmware is prepared for a new license regarding the handling of repeaters on a KWS400 system.

Removed Features

None

Corrections

- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  On handsets running in legacy mode (old generation user interface), the call waiting indication is now turned off correctly when the remote end cancels the call. When an incoming call waiting is pending, the display shows an indication and an audible indication is played. This indication was not correctly cleared when the remote end cancelled the incoming call.
- **Only relevant for Spectralink IP-DECT Base Station**
  Correct LED handling when having a primary and a secondary DECT synchronization source. When the synchronization source changed while connections were active, the LED indication was changed to idle even though it should continue indicating active. This is now corrected.
- **Only relevant for Spectralink IP-DECT Server 400 and Spectralink IP-DECT Server 6500**
  The SIP Call-ID header field uniquely identifies a particular call, or the registrations of a particular user. A Random Number Generator (RNG) is used to provide unique Call-IDs. In earlier versions, this RNG could be seeded several times, potentially compromising the uniqueness of the SIP Call-ID, which could lead to different calls/registrations having the same Call-ID.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	dect.allow_long_messages	This setting controls usage of long MSF messages and long callback numbers. If this setting is false (default) the following limits are enforced. - 24 char callback number - 72 char msf messages. If the setting is true the following limits are enforced: - 64 char callback number - 180 char msf messages. WARNING use with caution. If the handsets do not support long callback numbers and messages, enabling this feature might cause handsets to crash. Values: true/false. Default: false.
config.xml	Added	sip.send_bye_with_refer_notify	This setting controls IP-DECT Server behavior during transfer. If the setting is true the IP-DECT Server sends a BYE from the transferee to the transferor after the call to the transfer target has been established. Values: true/false. Default: true.
config.xml	Added	debug.coredumps	This setting controls whether the device will make a core dump in the case of a process crash. This setting is for debugging/developer purposes only. Values: true/false. Default: false.

Version PCS13Eb

Added or Changed Features

None

Removed Features

None

Corrections

- **Only relevant for KWS400 and KWS6500**
  Increase buffers used to create XML for SERVICE requests send to Lync. This fixes a problem discovered by Microsoft during interop test. The KWS was unable to make federated calls.
- **Only relevant for KWS400 and KWS6500**
  When moving remaining TCP buffer also move null termination. This addresses DECTESC-480 TCP problem with Avaya. The scenario leading to this issue was related to group call on an Avaya Communication Manager (ACM).
- **Only relevant for KWS400 and KWS6500**
  Delete UDP connections from connection table when they are deleted. This addresses DECTESC-430 where SIP stops to work after some connection trouble between redundancy master and slave. Furthermore cleanup connection creation.
- **Only relevant for KWS400 and KWS6500**
  If a call is set up on an existing MAC connection, re-use the old uplane if present. Solves DECTESC-471 and DECTESC-483, DECTESC-476, DECTESC-481 and DECTESC-487 which all report about problems with losing audio after a handover.
- Avoid underflow when subtracting unsigned lengths, which would cause large buffer overruns in RTP queues. One scenario which has been seen to trigger this behavior is related to changing audio-codec mid-call. This issue was reported in DECTESC-488.
- Media/RTP handling has been updated. The media load scaling used to calculate the available number of free channels on a base station, did not handle the simultaneous allocation of many channels correctly.

Configuration File Parameter Changes

None

Version PCS13E_ – Q3, 2013

Added or Changed Features

- Added support for IPv6. IPv4 addresses are a limited resource and the transition to IPv6 becomes more and more urgent. With this release of the firmware, the KWS is ready for the transition to IPv6.
- With this release of the firmware, the KWS can communicate with all relevant services via IPv6 and IPv4. That is, the KWS can communicate with IPv6 enabled SIP servers, XML-RPC based applications and maintenance services such as DNS and NTP.
- The implementation is dual stacked, and IPv6 and IPv4 can be mixed according to customer needs. If DNS names are used for services, the DNS will be used to determine the protocol to be used.
- The IPv6 configuration parameters can be determined in three ways:
  - Stateless Address Auto Configuration (SLAAC) - where the IPv6 address and the default gateway is retrieved via router advertisements from routers.
  - Statefull (DHCPv6) - where the IPv6 configuration is retrieved via DHCP much like IPv4.
  - Static - where the IPv6 address and the default gateway is configured from the GUI of the KWS.
- Improved handling of SIP server errors and failover. To improve the user experience and make the SIP communication smoother, the KWS now keeps track of IP addresses that cannot be reached due to transport or timeout errors. This is accomplished by blacklisting IP addresses with transport or timeout errors for 30 seconds. No communication with a blacklisted IP address is attempted if an alternative (failover) address can be determined. Specifically, this addresses DECTESC-441 where the KWS was unable to register all users to the secondary SIP server because it spent too much time waiting for timeouts from the primary SIP server.
- Support of changing IP address during operation. If the IP address is changed during operation either by DHCP (IPv4/IPv6) or router advertisements (IPv6), the KWS now handles this gracefully. In previous versions of the software, this caused internal inconsistencies which could lead to malfunction.
- Bumped base station protocol version to 7. The base station protocol version has been bumped to support IPv6.
- Changed SIP User-Agent string format to better fit RFC3261 and make Microsoft Lync client version filtering possible.

  When configured for standard SIP the User-Agent string is now product/PCSrevision.

  When configured for Microsoft Lync the User-Agent string is now product/major.minor.update.revision.

For example:

- Standard: `KWS6500/PCS13E_3123.`
- Lync: `KWS6500/13.5.0.43123`.

This addresses DECTESC-468.

- When parsing SIP Alert-Info header used for controlling internal/external ringing and auto-answer, the KWS now matches part of a string instead of the complete string.

  For example, is the following now allowed:

  ```
  Alert-Info: <http://www.vertical.com>;info=alert-external
  ```
  This was reported in DECTESC-467 which refers to the Wave PBX 4.0.0.2780 from Vertical.
- Add P-Preferred-Identity to OK response for UPDATE request when configured for Microsoft Lync. This addresses DECTESC-466 where external calls through a gateway are terminated after 30 minutes due to a failed session refresh from the gateway.
- Remove P-Preferred-Identity from OK response for PRACK request when not configured for Lync.
- Switch to a new DHCP client in order to support DHCPv6. The new DHCP client has more features, but is more pedantic with regard to the format of the vendor option used by the media resource and base station to retrieve the KWS address. The format understood by the old and new DHCP client is:

  ```
  <vendor option=43><length><sub option=43><sub length><IP
  address as string>[optional NULL].
  ```

  For example `2b 0b 2b 09 31 30 2e 31 2e 32 2e 33 00` for the KWS server IP address 10.1.2.3.
- Add support for DHCP option 2, time offset. With this option the desired time zone can be controlled by the DHCP server. The offset in seconds is expressed as a two's complement 32-bit integer. Refer to RFC2132 for details.
- Do not discard incoming SIP requests without a username in the request URI. This is correct behavior. Specifically, this makes the KWS answer correctly with a 501 Not Implemented error when a REGISTER request is received.
- Change the TCP port used for communication between redundant servers to 56017. Port 58017, which previously was used for this is in the default range for media resource external RTP. The new port 56017 is in the same port range as the other TCP signaling channels.
- More correct registration of the base station number (RfpNo) when an abnormal call release is logged. In some situations, the current base station is not known, and it was logged as RfpNo=0. This made RfpNo 0 take the blame for more abnormal releases than was correct. Now, the base station is logged as unknown when it is not known.

- When no time zone has been configured the KWS will use UTC. Previously, the Configuration|General|Timezone in the GUI would display UTC-1 (Amsterdam,Barcelona,…) even though the timezone was unconfigured. This has been changed.
- Ensure that the MAC address and UUID of the device is always handled and presented in lowercase.
- During a handover with DECT encryption enabled the encryption parameters are exchanged earlier in order to make a smoother handover.
- Prepare for new base station features and store more information about the base stations in the KWS base station database.
- Make the protocols between the KWS and the media resource and the base station more robust. This is to reduce the probability that a problem in one of the units will cause problems in the other units.

Removed Features

None

Corrections

- Correct handling of (S)RTP when an outgoing call is forked to a mix of endpoints using RTP and SRTP. The KWS switched correctly to SRTP but failed to switch back to RTP if the call was answered by an endpoint not using SRTP. This addresses DECTESC-444 where a call in a Microsoft Lync setup is forked to a PSTN gateway not using SRTP and some Lync clients using SRTP. If the call was answered by the gateway noise was played by the gateway.
- Fix a problem where an incoming call is never completing the STUN/TURN/ICE allocation. The problem is solved by not using STUN/TURN when ICE is not used. Specifically, this addresses DECTESC-461 where an incoming call from a PSTN gateway in a Microsoft Lync setup never makes the DECT handset start alerting.
- Fix a problem where the KWS released a waiting call towards the handset even though no call waiting was signaled to the handset. This resolves DECTESC-462 where a Lync team call scenario caused the handsets to generate an abnormal call release due to invalid signaling from the KWS.
- Allow connections to the HTTP and XML-RPC server from clients using TLS 1.1 and newer. Without this fix, recent versions of, for example. Google Chrome failed to connect via HTTPS.
- Correct check for synchronization loops when a base station is configured for auto sync. Without this correction base stations configured for auto sync. were not checked for sync. loops and undetected sync. loops could exist.
  Be aware that auto sync. is still not intended for production use and should only be used during the deployment phase.

- Downgrade the library used for making packet captures because the new one sometimes skipped the first packed in a capture.
- Fix a problem where the KWS failed to lookup a hostname for which it had to add the domain name in order to be able to look it up. The problem was triggered by enabling DNS SRV records for SIP.
- Remove a state/event error when MR_COMPLETE_cfm is received for a terminated call. This could happen if a call was terminated very shortly after it was established.
- Terminate call correctly if MR_COMPLETE_cfm returns bad status. In some situations when the media negotiation failed to complete correctly, a BYE was not sent and the remote endpoint had a hanging call.
- Remove memory leaks and static code analysis problems and make the software more correct and robust.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	network.ipv6.method	Specifies the method used to obtain an IPv6 configuration. Values: “slaac” Use router advertisements to obtain an IPv6 address. “dhcp” Use DHCPv6 to obtain an IPv6 address. “static” Configure IPv6 address and gateway manually. “disabled” Disable IPv6 support. Default: “disabled”
config.xml	Added	network.ipv6.ipaddr	Specify a static IPv6 address including the prefix length. Values: <IPv6 address>/prefix Example: 3000::2/64
config.xml	Added	network.ipv6.gateway	Specify a static IPv6 gateway. Values: <IPv6 address> Example: 3000::1

Version PCS13B_ – Q2, 2013

Added or Changed Features

- The KWS integration to Lync has been improved. The KWS now supports controlling the global call forward state of a Lync user. Handsets connected to Lync via the KWS are now able to manipulate the global call forward state of a Lync user, using configurable feature codes. The default feature codes are:

Feature code	*Decription*
21<extension>#	Enables unconditional call forward to extension
21	Enables unconditional call forward to voicemail
#21#	Disables call forward

- The feature codes are configurable under Configuration -> Wireless Server.
- The global call forward state is reflected in the handset display by pre-pending the standby text with either [CFU] for unconditional call forward or [CFM] for call forward to voicemail.
- The KWS will no longer require a NOTIFY event vnd-microsoft-roaming-self from Lync to be in a dialog. Lync will in some scenarios send a NOTIFY before the 200 OK that creates the dialog. This resolves DECTESC-440 where the KWS did not present the correct calling-party-number.
- Only allow INVITE with replaces for the inactive/secondary call while SIP endpoint is in a two calls state. A strange Lync transfer scenario caused a crash because INVITE with replaces was received during a transfer.
- The media handling in handover scenarios has been optimized.
During a handover the Media resource will stay on the original base station as long as media is received from it. Previously, the media resource could in some cases switch to the new base station too early, which could result in a short crackling noise during handover.
- Furthermore, SRTP handling during handover has been updated. The Media resource could previously detect false replay attacks, during handover when SRTP was received from two base stations. This is no longer the case.
- The firmware update process has been improved to eliminate potential firmware update problems.
- Previously, the KWS would log a state/event error in some scenarios where a handset ends a call which is put on hold. This is no longer the case.
- The Polycom branding and naming in the product has been removed and replaced by Spectralink. Theme handling for customizing naming and web-interface has been added.

- The IP address configuration GUI has been changed. IPv4 boot protocol selection (DHCP-assigned or static IP address) is now done using a combo box instead of two radio buttons. Additionally some more tooltips have been added to network settings.
  The VLAN setting has been moved from IP settings to Ethernet settings.
- LED handling has been changed.
  Previously, the indication LED on the KWS would be flashing green, if a voice call was active. Starting with this release, the LED flashes green if a radio connection is active, even if no voice stream is established. This makes LED indication consistent for KWS and base stations.
  If the device is a Media resource, the LED flashes green if a voice stream is active on the device.
- The default Certificate Authority (CA) bundle with trusted CAs has been updated.
- The rfp tag in the rfps.xml file now has a description property. This way the textual description will be available in the rfps.xml file.
- The conversion from handset partnumber to textual description used in the Users | List Users part of the WEB-GUI has been updated.
  The new KIRK 4080 (14122802) has been added, and several ATUS part numbers have been renamed.
- Tooltip for capture PCAP custom filter now tells to use PCAP filter syntax.

Removed Features

None

Corrections

- Fixed problem with Lync presence publication. The KWS could sometimes stop publishing the presence state of a handset and consequently the Lync user could appear as always busy. The problem was caused by incorrect handling of incoming presence NOTIFY requests without state information.
- The problem was reported in DECTESC-447. It was introduced in firmware PCS12C_ as an unwanted side effect of introducing support for SBA.
- Fixed problem with Statistics Abnormal Releases list, when running redundancy. Previously, the reported total did not include abnormal releases from the slave. Now the total is correct and the abnormal release list is sorted by timestamp (and not by master first, then slave). This addresses DECT-222.
- Mark central phonebook update as idle when a LDAP update fails. This corrects a problem where the phonebook stopped updating after a failed LDAP access, and a reboot was required.
- Previously, if a user with a username longer than 32 characters initiated a text call, this could result in a restart of the KGAP, for example, when accessing the central phonebook. This has been corrected.

- Fixed a rare problem with user database replication from master to slave in a redundant setup. If usernames or IPEIs are interchanged for two users while the slave is disconnected, the slave will not be able to store the changes and responds with an error duplicate username or IPEI. This is fixed by automatically deleting the slave user database and rebooting the slave.
  Log a critical error if the master is unable to store data in the slave during replication at connect.
  The problem was reported from the field.
- Support deleting clusters when replicating from master to slave.
- Eliminated an issue seen with redundancy and XML-RPC. If, for example, an XML-RPC application sent an SMS with an unknown username, and the KWS was running a redundancy setup, it would result in a restart of the KGAP.
- Removed memory leak in the central phonebook when empty strings are retrieved from LDAP.
- An issue with comparison of certificate validity timestamps has been addressed. This corrects a problem where the KWS claims a certificate to be expired if it expires within the current year. For example, if the current year is 2013 and the certificate expires in December 2013, the KWS will claim it expired starting from January 2013. The consequence of the bug is that the KWS will be unable to make connections via TLS for SIP or provisioning if the server presents a certificate that expires within the same year.
- When a central firmware update of MR6500 was issued from a KWS, the MR6500 did not respond correctly, which resulted in the fact that MR6500 did not support central firmware update from a KWS. This is now corrected.
- If a license was installed which allowed the KWS to handle more users than supported by the KWS, the number of allowed users was displayed incorrectly. This has been corrected.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	feature_codes.call_forward.voicemail.enable	Specifies the feature code used for enabling call forward to voicemail (CFM) on Lync. Values: The feature code users must

File	*Action*	*Parameter*	*Description*
			dial to enable call forward to voicemail. Default: *21*

Version PCS13__

Initial KWS6500 version.