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

Release Notes Q2 2016

Firmware Version PCS16A_

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_
2014-06-20	Release notes for PCS14B_
2014-09-18	Release notes for PCS14C_
2014-12-11	Release notes for PCS15__
2015-03-20	Release notes for PCS15A_
2015-05-06	Release notes for PCS15B_
2015-06-09	Release notes for PCS15C_
2015-09-21	Release notes for PCS15D_
2015-11-20	Release notes for PCS16__
2016-03-15	Release notes for PCS16A_

Introduction

Release

The products in the Spectralink IP-DECT portfolio are based on the same software platform. These release notes include 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 PCS16A_ of the firmware. The release replaces the PCS16__ 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 required. Part number 14075260
Master Spectralink IP-DECT Server Redundancy	License required. Part number 14075250
Microsoft Lync Interop. Incl. Spectralink Software Security Package (SRTP) (IP-DECT Server 6500)	License required. Part number 14075270

Feature	*Comment*
Software Security Package (TLS, SRTP)	License required. Part number 14075280
Handset sharing	License required. Part number 14075460
G.729	License required. Part number 14075480
Cisco Unified CM Enhanced features (IP-DECT Server 400)	License required. Part number 14075490
Cisco Unified CM Enhanced features (IP-DECT Server 6500)	License required. Part number 14075495
Microsoft Lync Interop. Incl. Spectralink Software Security Package (SRTP) (IP-DECT Server 400)	License required. Part number 14075510
Multi cell (IP-DECT Server 400)	License required. Part number 14075520
LAN Sync (IP-DECT Server 400)	License required. Part number 14075600
LAN Sync (IP-DECT Server 6500)	License required. Part number 14075610
Frequency Swap	License required. Part number 14075620

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

Version PCS16A_ - Q2, 2016

Added or Changed Features

- Lync Quality of Experience (QoE) reporting. This feature enables advanced monitoring and reporting of a large number of metrics and information about the media quality, device types, participants etc. involved in calls.
- Add `endpoint_partial_clear` function to XML-RPC interface. The function is used to clear messaging and calling lists in the handset.
- PP7 generation handset part numbers are recognized in the user interface.
- Lync DNS based auto discovery of the frontend server / pool. This changed the DNS procedures to be more like the Microsoft client, allowing for easier integration into a Lync environment.
- Streaming packet capture and log download. This allows for capturing packets and logging system events for long periods of time as it is no longer stored on the server but downloaded directly in the browser.
- The default maximum length of MSF messages has been increased from 72 to 180 characters and the default maximum callback number length has been increased from 24 to 64 characters. The old maximum lengths will be used if the setting dect.allow_long_messages is set to false.
- The legacy KWS600v3 MSF protocol is now disabled by default. It can be enabled from the Wireless Server configuration page.
- When Lync is enabled an Accept-Language header will be added to outgoing INVITE messages, allowing remote endpoints like voicemail and IVR to select which language to use. The value sent is controlled by the Phone Language setting.
- The SIP registration and re-registrations time interval now includes a random portion to help reduce the load of a server after restarts etc.

Removed Features

None

Corrections

- Fix one-way audio issues when connecting to certain PSTN gateways in a Lync environment and RTP encryption is enabled. This addresses DECTESC-666 and DECTESC-676.
- Fix LAN sync support when using UDP as transport. This addresses DECTESC-652.

- The LAN sync adjustment algorithm parameters have been adjusted to allow it to work on a larger range of switches.
- Eliminate blocking when setting up a TLS connection.
- Remove buffer overflow when receiving very large DNS results.
- Eliminate memory leak when a SIP redirect loop is detected.
- Eliminate memory leak when the SNMP ipDectAbnormalReleaseTotal counter is requested.
- Do not generate a new Cisco Unified CallManager SEP number when changing the username of a user is changed.
- Only handle registration-notify events in SIP NOTIFY messages when Lync is enabled as other SIP registrars has been observed sending these events in a format not understood by the Wireless Server.

Configuration File Parameter Changes

None

Known Issues

- After upgrading to PCS16A_, it is no longer possible to downgrade to PCS15__ or earlier. As a workaround, first do a downgrade to PCS16__ and then to the desired version.

Version PCS16__ - Q1, 2016

Added or Changed Features

- The IP-DECT Server is now able to join calls into a bridged ad hoc conference on Cisco Unified Communications Manager.

  The feature is available when two calls are active on the handset and is invoked by selecting “Join in conference” from the call Options menu. When the conference is established further participants can be added by adding a new call and joining it into the conference.

  Ad hoc conference requires the newest handset platform and is supported on Spectralink 7522, 7532, 7622, 7642, 7722 and 7742 handsets. It is not supported on the 7480, Butterfly, 7202 and 7212 handsets. Furthermore, the “Cisco Unified CM Enhanced features” license is required.

- Automatic Lync presence bootstrapping is now supported.

  Lync requires bootstrapping of presence for a user in order for a device to be able to publish presence. In previous releases of the firmware automatic bootstrapping was not supported and the administrator had to issue Power Shell commands or login with a Lync client in order to enable presence. Starting with this release the IP-DECT Server will automatically perform this

bootstrapping and no manual steps have to be taken in order to activate presence.

- The corporate phonebook now supports LDAPS for secure communication with a corporate directory. This is utilized by configuring a ldaps:// URI in the phonebook configuration.
- The IP-DECT Server now supports internal/external ring-patterns on Cisco Unified Communications Manager. CUCM supports using specific Alert-Info headers to indicate whether a call is internal or external. These headers are now parsed and recognized by the IP-DECT Server. Spectralink handsets have two variants of each ring-pattern making it possible to hear whether a call is internal or external. The symbol for an incoming call will also reflect whether the call is internal or external.
- DECT dummy bearer handling has been improved in the base stations.

  The radio is now faster to find the best DECT channel for the dummy bearer when the dummy bearer is moved. This reduces the chance that handsets or base stations that uses dummy bearer for synchronization will lose the signal.
- For LAN based synchronization require that the delay in both directions is low before using packets for sync. Otherwise the system might end up in a loop with increasing skew that cannot be corrected. This addresses DECTESC-639 and improves the stability of the LAN based synchronization.
- Restart PTP sync algorithm if not in sync after 2000 sync cycles. This addresses DECTESC-639 and improves the stability of the LAN based synchronization.
- Let the transmission of early RTP be controlled by the peer ICE status and not the session ICE status.

  This makes the media resource transmit early RTP for outgoing calls to non-ICE peers even if the global ICE setting is enabled. This is required in order to punch a hole to receive early media through a NAT/firewall.
- Keep the base station radio active for about three minutes when the connection to the IP-DECT Server(s) is lost.

  This increases the availability of the system because minor server connection interruptions and server reboots will not tear down the synchronization and the handsets will not lose their DECT signal.
- The handling of SUBSCRIBE NOTIFY signalling has been improved when connected to a Microsoft Lync server.
  The IP-DECT Server now allows Lync to piggyback the first NOTIFY with the 200 OK for SUBSCRIBE.
  Furthermore the BENOTIFY request is now supported. BENOTIFY is best-effort NOTIFY, which is a NOTIFY that is sent without a transaction and which does not require a response.

  Both improves scalability as the amount of signalling required is reduced.

- The handling of SIP registrations has been improved when connected to a Microsoft Lync. The IP-DECT Server now supports Lync keepalive signalling. When SIP registrations are sent from the IP-DECT Server it indicates to Lync that it supports Lync keepalive,and extracts the keepalive timeout from the register response and sends keepalive signals at the rate specified by Lync. Also, when a REGISTER is sent to Lync the-IP DECT Server will omit the "Expires" header from the REGISTER because Microsoft recommends that. When Lync keepalive is used the re-register period is increased from 900 seconds to 7200 seconds by the Lync server. However, the IP-DECT Server still has a default re-register period of 3600 seconds, which will be used unless configured otherwise.
- Change the SIP signalling with Cisco Unified Communications Manager to be more like the Cisco SIP Phones.

  This was required in order to be able to establish an ad hoc conference. The CUCM now uses remote call control and sometimes sends playtonereq and statuslineupdatereq instead of standard SIP responses. This is for example the case when calling a busy user. The IP-DECT Server interprets the requests and plays a tone or displays the status text.
- The IP-DECT product portfolio now uses a new library for secure communications with TLS.

  Amongst other things this means that the IP-DECT products now support certificates with sha384 and ecdsa signatures.
- Update the default CA bundle. This updates the list of Certificate Authorities known by the IP-DECT Server, which ensures that the system knows new ones and insecure ones are removed.
- Several open source packages included in the firmware have been updated in order to keep track with upstream development to get improvements and security fixes.
- The Linux kernel has been updated from version 3.16.2 to version 4.2.3.
- The RTP and STUN/TURN/ICE handling has been restructured in order to make it more correct and easier to maintain.

  The handling had some issues that could cause a crash in some special situations. These issues are eliminated with this restructure.
- Use SIP Warning header in the log message if a transaction fails. Cisco Unified Communications Manager puts additional error information in the Warning header. This information is now added to the log message to make debugging easier.
- Improve the way media resource channels are released.

  This is to eliminate the critical log message “Received session new for unused ResourceId=1”, which could occur if a call was terminated while it was established. Furthermore degrade log messages from critical to error because they do not impact the overall system.

- Improve the way base stations handle settings received from the IP-DECT Servers in a redundant setup.

  Previously, for example changed radio synchronization settings were received by a base station but in some situations they were not activated correctly and a base station restart was required to fix it.
- Add an additional SRTP SDP crypto line without MKI if MKI is enabled and update local MKI setting from remote.

  This is to improve the ability to negotiate SRTP encryption with various SIP endpoints. Specifically, this enables successful negotiation with the Pidgin client when connected to Lync.
- The build system used for building the firmware has been updated. Going forward firmware builds of a specific release will be generated in two different formats. A binary format available for download on the Spectralink Support portal and another format used in the production process.

Removed Features

None

Corrections

- Provisioning is supported by IP-DECT Servers only, it is not supported by media resources and base stations. Previously this was not enforced correctly and a base station could in some cases attempt to start provisioning, which could lead to issues. This problem was reported in DECTESC-633 and is now corrected.
- Set the current peer when completing ICE, this eliminates one-way audio problems in some call forking scenarios.
- Fix attended transfer to unreachable or busy number for non-NG handsets.

  If an attended transfer was attempted with a non-NG handset and the transfer target was unreachable or busy it was not possible to return to the original call or attempt a new transfer. This was reported in DECTESC-643.
- Do not send TURN refresh requests in encapsulated in data indications.

  The TURN connection was not correctly maintained when TURN was used in a non-Lync setup.
- Do not use IPv4 TURN relay for IPv6.
- Remove crash if MWI or presence data is deleted while pending delivery to handset.
- Avoid crash if remote peer is missing an expected ICE component.

Configuration File Parameter Changes

None

Version PCS15D_ - Q4, 2015

Added or Changed Features

- Radio/LAN Gateway functionality added.
  Support for a new type of base station synchronization has been added. If configured as Radio/LAN Gateway an IP base station will use an over-the-air synchronization as the source of synchronization and act as a LAN sync master. With this type it is possible to add a LAN synchronized segment of IP base stations to an existing synchronization chain of base stations. As an example it is now possible to augment an existing DECT Server 8000 system with digital base stations with a segment of IP base stations which use sync over LAN.
- It is now possible to set the Microsoft Lync presence status using the handset. The presence status will be sent to the Lync infrastructure and will affect the status on all connected devices for the Lync user. If a manual change of status is performed on the Spectralink handsets or on the Lync Client (e.g. manually setting the status to DND) this will be reflected on the Spectralink handset with a yellow/red/green icon. An automatic change of status on the Lync Client (e.g. making a phone call) will not be reflected on the Spectralink handset.

  Setting the presence status requires the newest handset platform and is supported on Spectralink 7522 handsets and on the upcoming 7532, 7622, 7642, 7722, 7742 handsets. It is not supported on the 7480, Butterfly and upcoming 7202 and 7212 handsets.
- Starting with this release the server supports Software Update Over The Air for the upcoming 72 series Spectralink handsets. Older IP DECT Server firmware revisions will report bad file for a 72xx SUOTA image.
- The supported G.726 codec is now advertised and displayed as AAL2-G726-32. This allows for low bandwidth consuming calls between a Lync Client and Spectralink DECT, as the Lync Client recognizes and supports this codec.
- The Ms-Subnet header is now included in REGISTER messages to the Lync Server. This enables support for Location Based Routing by the Lync Server.
- Improve handling of SIP transaction timeouts. The default client transaction timeout has been increased from 4000ms to 16000ms. This is to be more forgiving to SIP servers and endpoints that sometimes fail to respond quickly. The increased timeout will make the communication more robust but at the price of prolonged detection of failure. If a faster detection is required the timeout can be decreased by changing the setting Configuration|SIP|Client transaction timeout.
- Starting with this Firmware the IP DECT Server will re-register earlier to make room for the increased client transaction timeouts and still maintain a valid registration to a secondary SIP server in a failover situation. The Re-register timeout now depends on the client transaction timeout.

- On timeout only blacklist if SIP request is INVITE outside a dialog or REGISTER and no response is received at all. Previously the blacklisting of a SIP proxy could be too effective and blacklist a server due to a missing response from another endpoint. This was observed at an external site in a large CUCM deployment.
- On registration expire and connection failure do not issue a re-register if a register is pending. Before this change a new useless REGISTER was put in the queue and send after the pending registration was finished.
- Improve detection of transport errors when connecting to SIP servers. The SIP stack will now be faster to detect transport errors while connecting.
- If a Spectralink external antenna is mounted it is now reported in the WEB-GUI. The Administration|Base station page will show an antenna icon in the Status column if an external antenna is mounted. Furthermore it is now possible to control the antenna configuration if a Spectralink external antenna is mounted. In the base station configuration page a combo box allows for three different configurations.

  - Use internal & external antenna
  This is the default setting and recommended in most cases where an external antenna is used.

  - Use internal antenna only
  This is mainly used for tuning deployment and can be helpful in assessing the need for an external antenna.

  - Use external antenna only
  This can be useful if the coverage of the internal antennas creates reflections/hotspots and you only need the coverage supplied by the external antenna.
- Introduced scope of syslog settings. Currently remote syslog settings are distributed from the server if configured on the server. In this case they will override local settings. Starting with this firmware it is possible to override that and configure e.g. base stations individually. This addresses DECTESC-616.
- When synchronising over-the-air the base stations now require a different multi frame number 8 times before we change our multi frame number. This adds resilience against disturbance from foreign systems.
- The Administration | Base station page on the WEB GUI has been augmented with LAN sync delay and jitter columns. These columns reflect the current LAN sync delay and jitter respectively. Under normal condition the jitter should be below 1000 ns.
- If two IP DECT Servers are configured for redundancy and changes are made to media-resource settings for all media resources these changes will not apply to the media resource on the redundancy peer (slave). Previously if a restart all

media-resources was issued from the Master IP DECT Server this would make the slave IP DECT Server restart.

- Improvements to the SIP dialog handling for the dialog event package, RFC4235, which is used by CUCM and others to monitor the endpoint call state. These improvements are to better handle creation, deletion and inconsistencies in the SIP dialog state and avoid error messages in the log.
- Implement XML-RPC PP attach and detach. These handles can be utilized by an external application to detect when a handset is switched On/Off. Refer to the XML-RPC SDK for more info.
- Include CUCM device name in the exported users.xml.
- Avoid "Killed too old SIP transaction" when ICE completion fails and send a 488 “Not acceptable here” SIP response.
- Handle spaces in the file name of a SUOTA image e.g. "Spectralink PCS15HA.bin" if the file is uploaded from the "Users" page | "Firmware Update". Previously this caused the server to report "Invalid handset firmware file". This change addresses an issue reported in DECTESC-613.
- Improve handling of non-ICE calls when ICE is enabled. Re-INVITE with RTP address updates are not supported for calls with ICE. With ICE enabled the media resource did not allow address updates even though ICE was not used for the specific call. This caused the call to have one-way audio and is now fixed.
- SIP MSF handling has been refactored and optimized. This is used to send Standby text updates e.g. in connection with CFU status, MWI updates etc.
- Use a more efficient encoding of phase of neighbour base stations when sent from the base station to the IP DECT Server. This introduces an incompatibility that will not allow older revisions of IP DECT Server firmware to receive phase information from PCS15D_ or newer revisions of base station firmware. The Offset column in the RSSI map available when selecting a base station in the Administration|Base stations WEB-GUI, will in this case be empty.
- The internal buffers for signalling between the Radio part and the IP part of the base station have been increased to handle communication regarding LAN sync Gateway functionality.
- The internal web-server in the IP DECT Server now handles the HTTP header If-Modified-Since better by responding 304 Not Modified not only when the request timestamp is older than the content timestamp (as has been the case previously) but also if timestamps are the same. This improves MoH download to media resources.

Removed Features

None

Corrections

- If the remote end sends a Remote-Party-ID containing an invalid URI (specifically an URI without a host part which is not allowed as per RFC3261), the IP DECT server could crash. Now an invalid Remote-Party-ID header is ignored. This addresses DECTESC-621.
- In a setup with redundancy and CUCM the handling of the CUCM SEP number when a new user is created has been changed. The SEP number is derived from the UUID. Previously the UUID was generated in the local database (either Redundancy Master or Slave) and therefore not replicated until the next re-connect from the slave. Now the UUID is generated by the entity that updates the database and it is replicated correctly. This addresses DECTESC-615.
- Advertise our own ms-implementation-version, not the version received from the remote peer. This addresses a connectivity issue with remote Skype for Business clients. Reported in DECTESC-611.
- In a Lync configuration with Call Admission Control (CAC) enabled, the local relay address was incorrectly labelled as the local site address. Furthermore the port numbers of the remote endpoint was set to the TCP port numbers, not the UDP port numbers. This is now corrected and solves some connectivity issues with remote clients behind firewalls when CAC is enabled. Reported in DECTESC-611.

  This also addresses a problem reported in DECTESC-603 with an IP-DECT Server connected to a Skype for business server. After upgrading from Lync 2013 to Skype problems were experienced with incoming calls from normal skype users (from federated external users). Incoming calls were disconnected after 10 seconds, and they did not have this issue with their Lync 2013 servers. This scenario is also fixed with this firmware.
- Report LAN sync master status when changing LAN sync master without resetting sync. Previously this could result in a wrong RPN number being displayed in the WEB-GUI on the Administration | Base station Sync source column.
- Avoid a buffer overflow if neighbour RPN is higher than the number of maximum supported base stations. One example of this is if an IP DECT Server 400 has a multi-cell license installed (which allows for 4 base stations) and a RPN over 4 is detected.
- If a CUCM license is loaded it was correctly displayed in the loaded license list in the Administration | License page. It was however not displayed correctly in Active License Summary section of the same page and in the License information available at Status | Wireless Server. This has been corrected.
- In a Redundancy setup if a non-recoverable inconsistency between Master and Slave user database was detected, the server could crash when the slave database is cleared from master. This is corrected.

- When using handset sharing some log messages could report an incorrect username causing erroneous logging. As an example the username could be erroneous when logging an abnormal call release.
- Correct a problem with collecting DECT frame error statistics from the handsets. The server did not collect DECT frame errors from handsets with the latest firmware. This is now corrected.
- Fix multi-select Un-subscribe, which left the in-memory database inconsistent and SIP de-registered the user. Now the handset is simply DECT de-subscribed and the SIP registration is un-touched.
- When updating MoH file the old file was not properly deleted. This could lead to problems when uploading a new MoH file.
- Fix Music-on-Hold load on external and slave media resources. MoH did not work with external media resources.
- Eliminated a number of warning/errors
  - Remove not important State/Event error when deleting/disabling a user.
  - Avoid S/E error when NG call control is received while releasing the DECT call.
  - Avoid S/E error on timeout when semi-attended call transfer fails.
  - Avoid S/E error with GAP handsets with two calls where the active call has failed.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Changed	sip.client_transaction_timeout	Specifies the timeout for client transactions. This controls timer B and F as specified in RFC3261 Values: Milliseconds (1000-32000). Default: 16000.

Version PCS15C_ - Q3, 2015

Added or Changed Features

- LAN based synchronization of the DECT radios is no longer in beta and is now released. A license is required in order to enable this new feature. IMPORTANT: If the beta release of LAN based synchronization is used and this new firmware is installed the synchronization will be reverted to be radio based. Therefore it is highly recommend to load the license BEFORE upgrading the firmware.

- Provide IP-DECT Server generated Music-on-Hold (MoH). This adds the ability to play music when a call is put on hold on a SIP server that does not provide MoH itself. This is for example the case with Microsoft Lync, which relies on the endpoints to generate MoH. The feature is enabled by uploading a music file to the IP-DECT Server via the web GUI at Configuration | SIP | Call status | Provide Music-on-Hold. The music file must be an 8kHz, 16-bit, mono WAV file with a maximum size of 7MB. If MoH is also provided by the SIP server the MoH provided by the IP-DECT Server might conflict and the behaviour is unpredictable.
- Avoid “certificate not yet valid” errors when establishing a SIP TLS connection at boot up. Furthermore, avoid failed registrations because the TLS connection is not yet ready. The problem occurred because the time was not set by NTP prior to the attempt to establish a TLS connection. Now TLS connection establishment and SIP registration via TLS is withheld until a valid time is obtained via NTP. This was reported in DECTESC-596 in a Microsoft Lync setup.
- Faster detection of connection failure to SIP servers connected via TCP or TLS. Some internal timers have been adjusted to reduce the time required to detect a TCP connection failure from 15-30 minutes to a little more than 100 seconds. This enables the IP-DECT Server to be faster to failover to a secondary SIP server and hence reduce the time where users cannot be contacted. This was reported in DECTESC-597 in a Microsoft Lync setup.
- In the case of a Lync trusted server configuration, the IP-DECT Server now supports fail back to the primary proxy when registered with the secondary proxy. Previously the IP-DECT Server would stay with the discovered proxy server when re-registering as Lync trusted server. With regard to registration Lync behaves differently when configured for NTLM or trusted server. When configured for NTLM the client is redirected to the home server and it must keep registering towards this one. When configured for trusted server any Lync server will accept the registration and the request is routed to the home server internally within the Lync environment.
- In previous firmware revisions if a hostname was configured for the IP-DECT Server (Configuration|General|Hostname (FQDN)). The IP-DECT Server would always add the configured hostname to SIP Contact and Via headers. It has been discovered that this caused problems for some SIP servers and in setups where the DNS was not properly configured. To avoid these issues the hostname is now only added if mutual TLS is used, in which case the hostname is required.
- The IP-DECT Server now supports adding a ms-endpoint-location-data header to SIP INVITE in a Microsoft Lync configuration. The remote peer can utilize this to do bandwidth management according to our network location. This was reported in DECTESC-595 in a Microsoft Lync setup.
- Improve handling of incoming BYE for current call while a call is waiting.

    - For Spectralink handsets with firmware 2015-Q3 or later start alerting with the waiting call.
    - For Spectralink handsets with firmware earlier than 2015-Q3 show hold screen and let resume accept the waiting call.
    - For GAP handsets do not update display and let the R key accept the waiting call.
- Improve handling of receiving DTMF tones with SRTP enabled. When SRTP was enabled the incoming RFC2833 DTMF events affected the jitter buffer and the overall sound quality of the call could be degraded.
- If redundancy of IP-DECT Servers is configured avoid that the primary server never starts up if an incompatible secondary server is trying to connect. Previously the primary server could be kept in a startup state if an incompatible secondary server continuously tried to establish a connection.
- The Random Number Generator (RNG) has been improved to increase security. Seeding of the RNG is improved.
- LAN based synchronization has been improved. The sending of delay requests used for LAN based synchronization is now randomized to reduce the probability of flooding the LAN synchronization master at system start and during normal operation.
- Consolidate the display of base station RPN numbers and RSSI. RPN numbers are now always shown as decimal numbers and not hexadecimal. RSSI is shown in dB and the ADC value is removed.
- Update the base station status file, rfps.xml to include the firmware version of the base stations and synchronization lost/inactive values for LAN based synchronization.
- Upgrade the JavaScript library that handles tables on the web GUI to the latest version. This is to get better performance and prepare for later improvements.
- Correct the HTTP content type for the exported configuration. Content type text/xml is more correct and is also used when exporting the users in XML format.
- Make create user and device buttons on the web GUI be enabled/disabled by the licensed number of users and not the maximum number of users of the IP-DECT Server.
- Correct the endianess of the port number send from the IP-DECT Server to the media resource when updating firmware on handsets. This change breaks handset firmware update if the media resource firmware is updated and the IP-DECT Server firmware is not updated.
- Make the LDAP reader of the central phonebook more robust. If the LDAP server returned some unexpected data the central phonebook could crash.
- The handling of incoming SDP media attributes for controlling media flow and call hold has been simplified in order to make the code easier to maintain.

- Add more verbose logging when a response cannot be sent because the SIP transaction is unknown. This is added in order to assist with debugging problems.
- Log a NOTICE message when a TCP connection used for SIP fails.
- Remove a potential buffer overflow in the internal database handling. This is to avoid future backward compatibility problems when increasing the record size in the internal databases.
- Update the default CA bundle. This updates the list of Certificate Authorities known by the IP-DECT Server, which ensures that the system knows new ones and insecure ones are removed.

Removed Features

None

Corrections

- Fix Call Admission Control issues with Microsoft Lync. The IP-DECT Server did not maintain and release TURN connections correctly and this caused it to not maintain and release reserved bandwidth correctly when CAC was enabled. This was reported in DECTESC-595 in a Microsoft Lync setup.
- Correct a problem in the network driver with regard to LAN based synchronization. In some situations base stations synchronized via LAN could lose their synchronization every 2 hours and 17 minutes.
- Fix a problem not removing deleted devices on the backup when data is replicated at start up. This made the databases in the primary and the backup inconsistent and could cause problems.
- Correct the handling of incoming SIP UPDATE requests with SDP that modify the media flow. The media flow was not updated correctly and the RTP handling was not correct.
- In some call waiting scenarios all calls were not correctly released internally, which could result in the web GUI Statistics | Active calls page displaying hanging calls. This was reported in DECTESC-593 and DECTESC-589 and has been corrected.
- Fix a problem that only allowed the IP-DECT Server to load the maximum users minus one. That is 29 for IP-DECT Server 400 and 4095 for IP-DECT Server 6500. The IP-DECT Server kept crashing and a reset to default or a firmware update was required in order to make it work again. This is corrected and the numbers are now 30 and 4096.
- Fix an issue with handset software update and redundancy. A release reason was not transferred correctly from the backup to the primary server and therefore an incorrect abnormal release was reported when a handset was on the backup and out of range.

- Fix a problem not allowing to delete more than one handset firmware at a time from the web GUI.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	sip.music_on_hold	Used for controlling Music-on-Hold generated by the IP-DECT Server. For MoH to be generated this setting must be set to true and a WAV file must be loaded into the IP-DECT Server. Values: true: Generate MoH. false: Do not generate MoH Default: false
config.xml	Removed	sip.use_domain_names	

Version PCS15B_ - Q2, 2015

Added or Changed Features

None

Removed Features

None

Corrections

- Fixed a problem where users were not displayed in the users list on the web GUI. This was reported in DECTESC-598. An analysis of the root cause of this minor problem, revealed that the nature of the problem could potentially cause severe unpredictable behaviour of the firmware. The problem was introduced in PCS15A_ and it is highly recommended to update the firmware of all units running PCS15A_.

Configuration File Parameter Changes

None

Version PCS15A_ - Q2, 2015

Added or Changed Features

- IMPORTANT for handset sharing. Since handset sharing was introduced with PCS14__ the device database format has been changed. If the firmware is downgraded from PCS15A_ or any newer to a firmware between PCS14__ and PCS15__ the device database will be erased. If a handset sharing license is loaded, and a firmware downgrade is required, make sure to create a backup before the downgrade and restore the backup after the downgrade.
- The IP-DECT Server will no longer page handsets that are currently powered off. This will improve the user experience for users calling a powered off DECT handset. Without this improvement the IP-DECT Server will page the handset for 12 seconds before giving up and returning a SIP error response. With this improvement the IP-DECT Server will immediately return a SIP error response and the caller will not need to wait for 12 seconds. This addresses various issues reported in different scenarios, e.g. on CUCM.
- The IP-DECT Server can now be configured to SIP de-register the associated user, when a handset is powered off (the handset tells the server it is powered off by sending a DETACH to the server). This is controlled by a new setting "Handset power off action", available in Configuration | SIP | General. Default for this setting is to ignore the power off event and keep the registration.
  The handset power off state is not persisted in flash, and after a reboot the IP-DECT Server will assume that all handsets are powered on. The server will learn the state when handsets are powered off. The current known state can be viewed in the users and devices list. One use case of this setting is presence in a Microsoft Lync setup. It is now possible to set your Lync presence status to OFFLINE by turning off the DECT handset. Previously the Lync presence status would never be offline if a DECT handset was connected to your Lync account.
- Record and display the activity from handsets. The IP-DECT Server will now keep track of the latest activity from handsets and display it in the users and devices list on the WEB GUI. The following activities are recorded:
  - Unknown: No activity with the handset has been registered since last reboot.
  - Location registration: Latest activity from the handset is a location registration.
  - Voice/data: Latest activity was a voice or data connection.
  - Out of range: Latest attempt to communicate with the handset failed because it was out of range.
  - Turned off: The handset was powered off while in the range of the system.
- Add limited support for draft-liess-dispatch-alert-info-urns to determine external or internal alert tone from an incoming INVITE. This was added to improve interoperability with Alcatel OxO.

- Microsoft Lync ms-diagnostics header, which is added to SIP error responses by Lync, are included in log messages. This will make Lync SIP related log messages more verbose, which allows for easier debugging in Lync environments.
- In the users list on the WEB GUI only display registration status red when the registration is not OK. When the registration is inactive display the status grey.
- Accept 200 OK for REFER and handle unexpected REFER 2xx response correctly. Normally, REFER is accepted with a 202 Accepted response but some SIP servers sends 200 OK instead. Allow this and handle other 2xx responses more gracefully. This addresses DECTESC-578 where the handset was unusable on an Alcatel OxO until a reboot after attempting a transfer.
- Fix call transfer initiated while performing ICE triggered re-INVITE. When an outgoing call is established with ICE a re-INVITE is issued shortly after the call is answered in order to complete the ICE negotiation. If a transfer was initiated while this INVITE was pending a state/event error was triggered and the call was terminated.
- The quick status on the front page of the WEB GUI has been updated. The status indication is giving a quick overview of the health of the overall system.
    - SIP
      - Green: All registrations are OK.
      - Yellow: At least one registration is failing.
      - Red: All registrations are failing.
    - Redundancy
      - Green: Connection to other node is OK.
      - Red: Connection to other node is failing.
    - Base stations
      - Green: All enabled base stations are OK and no synchronization loops are present.
      - Yellow: At least one enabled base station is failing or synchronization loops are present.
      - Red: All enabled base stations are failing.
    - Media resources
      - Green: All enabled media resources are OK.
      - Yellow: At least one enabled media resource is failing.
      - Red: All enabled media resources are failing.
    - Provisioning
      - Green: Provisioning is active and OK.
      - Red: Provisioning is active but failing.
      - Grey: Provisioning is not active.
    - NTP
      - Green: NTP is active and OK.
      - Red: NTP is active but failing.
      - Grey: NTP is not active.

- Update the default CA bundle to Mozilla 2015-02-19. This updates the list of Certificate Authorities known by the IP-DECT Server, which ensures that the system knows new ones and insecure ones are removed.
- For SIP over UDP decrease the re-transmission rate when a 100 Trying is received for non-INVITE client transactions. This reduces the amount of re-transmissions and is more standards compliant.
- The XML-RPC function endpoint_heartbeat_config() has been made backwards compatible with customer applications built during the development phase.
- Degrade log message about sending more than two DECT frames from INFO to DEBUG. This is likely to happen when an extra called party is send to the handset.
- Add support for product name send by future handsets at DECT location registration. This information is used to display the correct handset product names in the users list on the WEB GUI.
- Start handset firmware update even though no media resources are connected. This eliminates a problem where handset firmware update gets stuck at boot time. Furthermore, fix another problem that could make handset firmware update get stuck.
- For incoming calls extract original called party from History-Info or Diversion header and send it to the handset. This can be used by future handsets to indicate that an incoming call is for example forwarded or a group call.
- Update the library used for packet capture and improve capture when VLAN tagging is used. VLAN tagged packets are no longer captured twice as two identical packets.
- Remove a state/event error if the user presses a key on the handset while an outgoing text call is being established.
- Add a confirmation dialog for sign out and unsubscribe from the users list in the WEB GUI. These actions have big impact on the users and are tedious to revert and therefore a confirmation is desirable before executing the action.
- Reduce writes to the internal flash when users are enabled/disabled from the users list.
- Avoid error "Failed to send BYE - No dialog defined" when a call is replaced and terminated while a media session is being allocated. This has been seen on Microsoft Lync.
- Reset handset specific info when the IPEI of a device is changed. Without this the IP-DECT Server displayed wrong information until the new handset made a location registration.
- The build system used for building the firmware has been updated and several open source packages included in the firmware have been updated in order to keep track with upstream development to get improvements and security fixes.

Removed Features

None

Corrections

- A problem that made the media resource crash when Call Admission Control (CAC) was enabled on Microsoft Lync has been fixed. This was introduced with PCS15__.
- Corrected error handling for SIP over TCP. A TCP transport error during SIP registration could completely stop registrations until rebooted.
- Fix internal handset to handset messaging. This was broken in PCS15__.
- Complete internal media negotiation correctly for incoming calls when ICE is not used. When ICE was not used the media handling ended in an intermediate state and this could cause crackling sound quality. This problem was introduced in PCS15__.
- Fix translation of Message Waiting Indication status message on handset. This addresses DECTESC-584.
- Fix handling of incoming CANCEL for INVITE. The CANCEL was not correctly matched to the INVITE transaction. This made cancelling a waiting call not working if the callee was also callee in the existing call. The waiting call was not cleared at the callee and the handset kept indicating a waiting call.
- When handset firmware upgrade is not possible because the handset is in a call correctly show busy status instead of "out of range".
- Correct the device statistics, text setup failed column. The percentage and the failed count was incorrect. For this to work an updated handset firmware is required as well.
- Parse SIP Contact header with <> in a generic parameter in a SIP URI without <>. This eliminates SIP registration problem with AVAYA Session Manager. This addresses DECTESC-559.
- For handset sharing fix sign-out requested from the users list in the WEB GUI. Previously this would erroneously DECT unsubscribe the handset.
- Fix a problem where SIP settings must be saved twice when Lync is enabled. This was introduced in PCS15__.
- Sort durations correctly in tables on the WEB GUI. Specifically, active calls duration and device call time was not sorted correctly for durations.
- Do not sometimes show bogus durations in active calls list in a redundant system. The durations was calculated in such a way that the result could be wrong in redundant systems.
- In a redundant system correctly show node M(aster) in the users and devices list if the slave is not connected.

- Fix problem with VLAN tagging and IPv4 for base station synchronization via LAN. LAN synchronization did not work if PTP over IPv4 was used with VLAN tagging.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	sip.dect_detach_action	Used for controlling what happens with the SIP endpoint if a handset is powered off. Values: ignore: Nothing happens. deregister: The SIP endpoint is de-registered. Default: ignore

Version PCS15__ - Q1, 2015

Added or Changed Features

- The IP-DECT server now supports updating firmware on Spectralink handsets over-the-air, if this feature is supported by the handset. This drastically reduces the effort necessary to update handsets, as it is possible to update the firmware of a handset remotely, without having to physically locate and handle the handset.

  Handsets can be updated individually, where an administrator individually schedules specific handsets for a firmware update. It is also possible to update handsets automatically. I.e. an administrator uploads a firmware version and all connected handsets automatically update to that firmware. When a handset with a different firmware version is encountered by the system, it will be automatically updated to the uploaded version.
- It is now possible to control the base station transmit power levels from the server, if supported by the base station (power level control is only available for the newest generation IP base stations). It is only possible to reduce the power level compared to the default power level. It is e.g. not possible to increase the power level on a NA base station. Power levels can be controlled system-wide i.e. for all base stations, or individually for each base station. A system-wide level can be controlled in the WEB-GUI at Configuration|Wireless Server|System TX power. If a system-wide power level is configured, this will override any base station specific power setting. Base station specific power levels, can be configured at the individual base station configuration page (TX power setting), available through Administration|Base station. A warning is

issued in the log if global system TX power control is enabled, and base stations not supporting this are active. Furthermore if base stations with a different local TX power setting configured are present and active, a warning is issued that this local setting will be overridden by the system wide setting.

- STUN, TURN & ICE are now supported for efficient NAT and firewall traversal as well as IPv4/IPv6 dual stack media connectivity.
- The XML-RPC application interface has added support for the endpoint_heartbeat_config(), endpoint_heartbeat_res() and endpoint_retry_config() functions. These functions give an application access to the heartbeat and retry configuration functionality of the 7640 and 7740 handsets. For further information refer to the XML-RPC SDK version 1.11.
- Re-work of the messaging system to enable continuous maintenance and development. The messaging is used internally in the IP-DECT server (i.e. MWI and phonebook) as well as external messaging controlled through the XML-RPC application interface.

  Connection release and timer handling has been changed as part of the messaging re-work. Before, the connection in some scenarios was released immediately. Now a timer is started, and the connection is released after a short while of inactivity. This is to eliminate some race conditions, where the handset and the server release a connection at the same time. This addresses an issue reported in DECTESC-555.

  The messaging system previously had a queue, to reduce the chance of flooding the base stations with incoming messaging setups. This has proven to be an unreliable solution, and the messaging applications need to implement their own throttling mechanism. The internal messaging queue has been eliminated because it adds undesired complexity.
- Base station synchronization over LAN (beta).
  In a multi-cell DECT system, the base station radios must be synchronized to each other in order to achieve the optimum handover experience, when handsets are moving around among base stations. The Spectralink IP DECT portfolio supports synchronizing base stations via the radio. With this release beta support for LAN for synchronization of the DECT radios is available.

  The Spectralink LAN based synchronization has several advantages over synchronizing via the radio. The configuration is much simpler, because no synchronization chains need to be configured and maintained. The synchronization is self-healing, because the system itself can handle if any base station is failing. Finally, the system can be deployed with fewer base stations, because the base stations no longer are required to be in range of each other.

  The LAN based radio synchronization is administrated centrally from the WEB-GUI of the IP-DECT Server. However, the synchronization is handled

autonomously by the base stations and the server is not involved and hence, does not need to be on the same network segment.

Attention! LAN based radio synchronization is still in beta, and is not recommended for production use. LAN based synchronization requires an enterprise grade network with enterprise quality switches.

For more information on base station synchronization over LAN refer to Application Note: DECT LAN Based Radio Synchronization.

- The user administration part of the WEB-GUI has been improved.
  It is now possible to select several users (multi select) and perform the same operation on these users in one operation. Previously if an administrator wanted to e.g. disable or delete 40 specific users, it had to be done in 40 individual operations. Now it is possible to select these 40 users and disable/delete them in one operation.
- Randomize base station re-connect timer and add exponential back off. The first re-connect attempt will be randomized between 1 and 21 seconds. Before this change it was always 10 seconds. Before this change, an installation with a high number of base stations, would result in a re-connect storm towards the server, which could result in a more prolonged reconnect time than necessary. In addition to the above, the IP-DECT server has been tuned to better handle new connections from a larger number of base stations.
- Reset RTP session when a new peer is added. Only accept RTP packets from the last added peer. This change addresses a previously unsupported scenario reported in DECTESC-554. The issue relates to a scenario where an outgoing call from the IP-DECT Server, is forked to different endpoints, which support different levels of encryption (SRTP and RTP). When these endpoints send early media, the authorization of encrypted voice packets (SRTP) could fail, resulting in silence or noise and a log notice about RTP problems.
- Allow the SSRC to change with a re-INVITE when SRTP is used. This increases interoperability because some implementations change the SSRC during a call.
- Various STUN/TURN/ICE interoperability improvements. Including improved debugging info and logging of STUN/TURN/ICE problems. Furthermore the maximum number of ICE candidates is increased from 20 to 30.
- Improved SIP registration handling with redundancy. All users are now re-registered on redundancy failover and failback, in order to ensure that the registration status is correct shortly after an outage. Before this improvement, it could take some time before the registrations were correct after an outage.
- When allocating a resource only add requested codecs, do not always allocate the worst case cost. Addresses DECTESC-548.
- Previously a free running base station would automatically restart when the textual description was changed. This is no longer the case. Furthermore the restart indications, (***) for the fields have been corrected.

- It is now possible to provision a handset sharing pin code.
- Display Device ARI on the Status|Wireless Server WEB-GUI when an Redundancy with ARI Swap License is installed. System ARI is the ARI used by the system. Device ARI is the ARI with which the unit was produced. These are different if e.g. a redundancy license is installed.
- When a handset performs a location registration, the IP-DECT server will now request enlarged part number and PCS info as well as PPStatistics from the handset. These elements are proprietary for Spectralink systems, and are used to augment functionality. Additionally the IP-DECT server will send the type (DECT/IP DECT), and generation of the system to the handset. This will be utilized in the handset in the future, to only send new features to the newest generations of DECT servers. This is done to ensure that new upcoming handset features do not break backward compatibility with older generations of servers.
- A Microsoft Active Directory has a Global Catalogue feature that gives access to the entire directory if an LDAP request is sent to port 3268. This can be used to access the entire directory of an Active Directory, and is now supported by the Server. Refer to http://technet.microsoft.com/en-us/library/cc978012.aspx for additional information.
- Avoid displaying reboot required when no setting that requires a reboot is changed. This happened when a WEB-GUI form, which contained settings that require a reboot, was saved for the first time. These false reboot required messages are now eliminated.
- Microsoft Lync can report insufficient bandwidth when an outgoing call is initiated. This indication is now displayed on the handset.
- Various interoperability issues discovered at the SIPit interoperability test event have been eliminated and general SIP, SRTP/RTP, ICE/STUN/TURN, and IPv6 support has been improved.
    - Do not use SIPS URI scheme per default when TLS is configured as transport for SIP. It is recommended to instead use the URI parameter transport=tls. The SIPS URI scheme can still be enabled via the configuration if required. Furthermore, request _sips._tcp for TLS via DNS SRV even when SIPS URI scheme is not used. This is recommended practice.
    - Do not fall back to unencrypted RTP, when the other end offers RTP/SAVP, and the IP-DECT Server is unable to parse the crypto line in the SDP offer. Instead respond with 488 Not Acceptable Here.
    - Improved SRTP interoperability with regard to the lifetime parameter. Allow SRTP lifetime to differ from 2^31 and set default lifetime to 2^48. For Microsoft Lync continue using 2^31.
    - For non-ICE incoming calls send 200 OK for INVITE and complete media in parallel. This simplifies internal signalling, and the OK response will be sent earlier, reducing the overall call setup time.

    - Do not log an error if a zero length SIP UDP packet is received, this is legal.
    - Retransmit 200 OK for incoming INVITE with TCP/TLS transport. RFC3261 requires this for UDP and TCP/TLS because 200 OK for INVITE can get lost in complex proxy scenarios, even if the first proxy uses TCP/TLS. Continue to not retransmit when configured for Microsoft Lync.
    - Improve handling of transport errors when sending 200 OK for INVITE. Do not release the call without notifying the user, but display an error message in the handset.
    - When using IPv6 and IPv4 but registering via IPv4 select IPv4 for IP address in SDP.
    - Fix a problem with DNS where IPv6 addresses were resolved even if no IPv6 address was present. This has given strange logging in Status|Log messages.
- Support for several new RFCs has been implemented.
    - RFC3327 "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts"
    - RFC3581 "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing"
    - RFC6026 - Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests.
- The built-in packet capture feature has been improved to better capture SIP over TCP, SIP over TLS in mixed IPv4/IPv6 and SIP in fragmented UDP datagrams.
- Change a NOTICE to DEBUG when a calling party no is too long and is removed
- The record sizes used in the base station database and the device database have been increased to handle more information, and be prepared for future changes. The changes are backward compatible, and the server will automatically convert from the old format to the new format.
- Add FQDN hint to hostname setting and rename domain to search domain.
- The standard date/time format which is used in the status log on the WEB-GUI, is now also used in the exported log. I.e. 2014-09-23 16:46:48.433 instead of 23-09-2014 16:46:48.433.
- The RSSI-scanner, in the "hidden" (/maintenance) part of the base station WEB-GUI, has been updated. It now recognizes new EIC (Equipment Installers Code) used in Spectralink DECT and IP-DECT servers in production from approximately December 2014.

Removed Features

None

Corrections

- Re-work the SIP TCP receive buffer handling to allow larger SIP messages. The buffer is now dynamically resized and the maximum message size is increased to 256kB. Furthermore the remaining receive buffer is not discarded when a SIP message cannot be parsed. This addresses DECTESC-551 where Microsoft Lync sent very large SIP messages.
- Fix a buffer overflow in XML-RPC and make the built-in HTTP server more robust to malicious clients. This addresses DECTESC-556.
- In a redundant system, interchanging the IPEI of two users while the backup/slave node was disconnected could cause a crash of the backup/slave when it re-connected. This is corrected.
- Improved mute detection if CRC errors are detected on the radio link. This eliminates some undesired side effects caused by changes in the mute functionality on the base station introduced in PCS14C_. The base station will now handle mute in the case of frame errors better. This change reduces the impact frame errors will have on the audio quality, in the direction from the handset to the base station.
- Properly handle a slow DNS SRV response that arrives after the SIP transaction time out. This could previously cause a crash.
- Do not leak calls when several calls are received, while releasing an existing call. This could previously result in the active calls list showing calls which were already released.
- Eliminate a log message saying "Trying to remove I/O handler on fd:-1, aborting." when replicating disabled RFP or MR. This was not a problem.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	dect.global_tx_power	Used for controlling (reducing) the output power of all connected base stations supporting power control. Unless set to default, this will override any base station specific power setting. Values: 0-13 0: default (no reduction) 1: 0 dBm (1 mW) 2: 2 dBm (1.6 mW) 3: 4 dBm (2.5 mW) 4: 6 dBm (4 mW) 5: 8 dBm (6.3 mW) 6: 10 dBm (10 mW) 7: 12 dBm (16 mW) 8: 14 dBm (25 mW) 9: 16 dBm (40 mW)

File	*Action*	*Parameter*	*Description*
			10: 18 dBm (63 mW) 11: 20 dBm (100 mW) 12: 22 dBm (158 mW) 13: 24 dBm (250 mW) Default: 0
config.xml	Added	rfp.default_sync_type	Default sync type for new base stations connecting to the server. Values: “freerunning” The base will not synchronize on anything, it will act as a sync-over-air master. "radio" The base will synchronize on another base over-the-air. "lan" The base will synchronize over LAN. Default: “radio”
config.xml	Added	rfp.ptp.transport	The protocol transport layer used by PTP for LAN sync. Values: “l2”: Ethernet. “ipv4”: IPv4 “ipv6”: IPv6 Default: “ipv4”
config.xml	Changed	sip.use_sips_uri	Normally SIP communication on a TLS connection is using the SIPS: URI scheme. Disabling this option causes the KWS to use the SIP: URI scheme with a transport=tls parameter for TLS connections Values: true/false Default: false
config.xml	Changed	sip.media.ice.enable	Enable the support for Interactive Connectivity Establishment (ICE) (RFC 5245) Values: true/false Default: false
config.xml	Changed	sip.media.turn.enable	Enable the support for Traversal Using Relays

File	Action	Parameter	Description
			around NAT (TURN) (RFC 5766) Values: true/false Default: false
config.xml	Added	sip.media.turn.server	TURN server address. Value: A string. Default: Empty.
config.xml	Added	sip.media.turn.username	TURN server username. If left blank, the per-user authentication username will be used. Value: A string. Default: Empty.
config.xml	Added	sip.media.turn.password	TURN server password. If left blank, the per-user authentication password will be used. Value: A string. Default: Empty.
users.xml	Added	user.pincode	The pin code used for associate a user to a handset when using handset sharing. Value: A string consisting of max 8 digits (0-9). Default: Empty

Version PCS14C_ - Q4, 2014

Added or Changed Features

- Improved monitoring capabilities on radio interface.
  The base station will monitor active radio connections and report frame errors in voice/data packets back to the server. This is utilized in the server to display the amount of frame errors on the individual base stations. The statistics are available in Statistics|Base Station, as well as in the exported logs. These statistics should be read with care, and some amount of frame errors should be expected. The statistics can be used to get a high level overview of the health of the installation/deployment radio-wise. If a base station has a high amount of frame errors compared to the other base stations, this can be an indication of e.g. a challenging HF-environment or potentially a base station located at the edge of the coverage area with many handsets attempting connections outside

the range of normal operation for the base station.

In addition to making radio interface frame error statistics available for monitoring, an INFO message will be logged if the number of DECT frame errors detected by the base station is greater than 2% and the duration of the connection is more than 5 seconds.

```
''DECT frame errors channel:0 received:584 errors:20 3 %''
```

If the number of frame errors detected is below 2% a debug level message will be logged.

- Improved monitoring capabilities on network interface.
  The media handling will monitor active RTP sessions and report problems and packet loss to the server. This is utilized in the server to display the amount of RTP loss on the individual base stations and media resources. The statistics are available in Statistics|Base Station and Statistics|Media Resource, as well as in the exported logs. The statistics can be used to get a high level overview of the health of the installation IP network-wise.

  In addition to RTP loss statistics available for monitoring, a notice message will be logged if the number of RTP problems is greater than 2% and the duration of the connection is more than 5 seconds.

  In addition to the above a lost packets counter is added to the current RTP statistics log message.
- The statistics module has been augmented with statistics for devices. Every time a voice call is released Spectralink handsets supporting statistics, will send statistics to the server, which stores the information. The following statistics are available in the web GUI and in an exported log.
  - User
    The username currently using the device. (If handset sharing is used and no user is currently signed-in to the device, the username may be empty).
  - Call time (hh:mm)
    The total call time for the device (voice calls).
  - Abnormal releases
    The percentage and the number of abnormal/total releases (voice calls).
  - Bearer handover cancelled
    The percentage and the number of cancelled/total bearer handovers.
    A bearer handover is when the handset changes channel (frequency/timeslot) but stays on the same base station. This is typically performed if the handset detects disturbances on the current channel.

- Connection handover cancelled
  The percentage and the number of cancelled/total connection handovers. A connection handover is when the handset changes base station. This is typically performed if the handset detects a better base station than the one it is currently on.
- Call setup failed
  The percentage and the number of failed outgoing call setups. An outgoing call setup can fail for different reasons. Some examples are: If the radio connection drops while establishing the call or if the user presses on-hook/off-hook quickly.
- Text setup failed
  The percentage and the number of failed outgoing text call setups.
- Out of coverage
  The number of times and the duration in hh:mm the handset has been out of coverage.
- Frame errors
  The percentage of voice/data packets with frame errors detected while in an active radio connection.

In addition to making the device statistics available for monitoring, an information message will be logged when a call is terminated if the frame error rate is above 2 %. E.g.

```
''DECT errors reported by device, Username:1292
FrameErrors:4%(4235/91952)''
```

- The user interface of the corporate phonebook has been updated and now has internationalisation support. The user interface of the corporate phonebook was previously only available in English. The Configuration|Wireless Server|Phone Language setting controls the language of text sent by the server to the handsets. Starting with this release the language of the user interface for the corporate phonebook will follow the language setting for strings sent by the server to the handsets.
- Enable slide error detection in DECT S-field.
  When the receiver on the base station is disturbed by an asynchronous system, the disturbance usually starts in one end of the signal, and thereafter slides in over the signal. Previously the base station only evaluated bit errors at the end of the signal. This could lead to a situation where an asynchronous system unnoticed could slide in from the beginning of the signal. Noticeable audio corruption would then be heard before the disturbance was detected at the end of the signal. To prevent this, the base station now also evaluates the beginning of the signal for bit errors. This can then be reported to the handset, for it to evaluate if a handover should be performed.
- When putting a call on hold the server needs a response from the other end (being put on hold). If this response is late and a second call is being initiated

before the response is received the handset would enter an undefined state and the following message would be logged:

```
LogTriggerDump("SipCall [id:####] (UserName:####)
(SipEndpointRecvNGNewInd) unexpected state endpoint:####
call:####".
```

The server now handles this situation gracefully, the handset is returned to hold state and the message is no longer logged.

- The abnormal releases statistics available at Statistics|Abnormal releases has been improved. Previously a user in an entry in this list was identified by a PPID, which is an internal identifier for users. Now the actual username is presented directly in the list for easier reference. Furthermore the IP DECT Server has been seen to restart, if a HTTP connection breaks while the abnormal releases list is being retrieved, this is no longer the case.
- For solicited MWI accept NOTIFY before the OK response is received for the SUBSCRIBE. This fixes an issue reported in DECTESC-541 where the MWI NOTIFY takes a different route than the OK response for the SUBSCRIBE and thereby arrives before the OK response. This breaks the exchange of MWI messages and no MWI is displayed on the handsets.
- The server now supports receiving item number from handsets on location registration. It is used to determine the handset name, when users and devices are displayed. This makes it possible to identify OEM branded handsets with the OEM naming.
- Base station and media resource statistics are now available on IP DECT server 400 even in a single cell configuration. Although no external base stations or media resources are present it still adds value to see the statistics for the internal ones.
- Updated translation files for strings sent from the server to the handsets. Translations have been added for "Insufficient Bandwidth" message which might be sent in a LYNC setup, when Call Admission Control (CAC) fails to allocate sufficient bandwidth.
- In the web GUI the possibilities for sorting columns with empty/non-numeric/percentage values has been improved. As an example the Administration|Base Station part of the web GUI now supports sorting base stations by synchronisation source (Prim/Sec) and by synchronisation lost counter. Furthermore the synchronisation lost column has been made easier to read by using a dash as separator between absolute numbers and percentages.
- Make sure to terminate an incoming call correctly by sending a "480 Temporarily Unavailable" response if a DECT error occurs while a media resource is being allocated.
- RTCP handling has been improved.
  RTCP lost reporting now supports negative loss, which the RFC allows.

Furthermore RTCP lost calculations now only cover current SSRC, and lost statistics and RTCP reporting is only done for a SSRC when in sync.

- SIP endpoint state/event errors were previously logged with log-level critical. This was misleading as a state/event error is unexpected behaviour however not critical. Starting with this firmware they are logged with log-level error.
- Fix a confusing notice message when a non-INVITE transaction fails. If the remote User-Agent/Server was unknown the message "`Error received from unknown`" was logged. Now the remote IP address is added to the message and "unknown" is not added to the message if the remote User-Agent/Server is unknown.
- Previously state event errors like the following could be logged as a result of a scenario where the user presses a digit while a media resource is being allocated or while toggling between calls:

  ```
  "SipEndpoint (UserName:XXXXX) (SipEndpointRecvCCInfo)
  unexpected signal/SIP in state
  ResourceAlloc/TwoCalls_OutgoingHold"
  ```

  This is not an error, and the logging has been removed. This resolves DECTESC-546.
- If a call is terminated while the media is being completed, the server would previously log the following error message:

  ```
  "MR_COMPLETE_cfm received for unexpected call
  UserName:####.
  ```

  This is not erroneous behaviour, thus the logging has been removed.
- The server will no longer send SUBSCRIBE for MWI before SIP registration is successful. If a user was updated via the GUI or via provisioning the server could send a SUBSCRIBE for MWI before a successful SIP registration. This is currently not causing problems, but it is an undesired behaviour.
- The linux kernel is updated from 3.14.3. to 3.16.1
- The RFPI-scanner in the "hidden" (/maintenance) part of the base station web-GUI has been updated and now recognizes new EIC (Equipment Installers Code) used in Spectralink DECT and IP DECT servers in production from approximately June 2014

Removed Features

None

Corrections

- Using software version 14B_ in a setup with handset sharing, has been seen to cause an error where no more status messages e.g. voicemail, call forwarding,

etc. are shown on the display of the handsets. When this error occurs the following message can be found in the log:

```
"TRIGGER MESSAGE  Hashtable duplicate insert:"
```

This behaviour was reported in DECTESC-547, and has been corrected.

- The Multicast TTL setting available in the Base stations part of the wireless Server configuration settings page on the WEB-GUI.(Configuration|Wireless Server|Multicast TTL) was not displayed correctly. If multicast towards base stations is used, the Multicast TTL is used to limit the propagation of multicast packets across routers. Previously the GUI would always display 0 or 1 even in the case of a TTL higher than 1, this is now corrected.
- If the server is configured to only support G.711 A law media codec (Configuration|SIP|Codec priority setting), the server/media resource has been seen to become unresponsive, if it receives a G.711 u-law RTP packet even if G.711 A law has been negotiated. This was reported in DECTESC-549, and has been corrected.
- A buffer overflow in connection with abnormal call release statistic for SNMP has been identified and corrected.

Configuration File Parameter Changes

None

Version PCS14B_ - Q3, 2014

Added or Changed Features

- SNMP
  Simple Network Maintenance Protocol SNMPv2c is now supported by the IP DECT portfolio. Simple Network Management Protocol (SNMP) is an "Internet-standard protocol used for monitoring devices on IP networks". To perform this monitoring, SNMP uses management systems (3rd party) and agents on the devices. The management system can be used to obtain status from the devices by polling the agents. Furthermore the agents can send “traps” to the management system, if an event has occurred on the device. SNMP agents are implemented on the newest generation of IP-DECT Servers, Base Stations and Media resources.

  SNMP consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. Essentially, SNMP agents expose management data on the managed systems as variables. These variables can then be queried by managing applications. The variables accessible via SNMP are organized in hierarchies. These

hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

General MIBs are supported by IP-DECT servers, Media resources and base stations. These provide general information e.g. uptime, number of received/transmitted udp datagrams etc. The following MIBs are implemented on the DECT devices:
IF, IP, IP-FORWARD, TCP, EtherLike, SNMPv2, IPV6, UDP.

In addition to the general information mentioned above specific Spectralink DECT information is available on the IP-DECT server only. This information is defined in a SPECTRALINK-IPDECT MIB.

This MIB includes the following groups of information:

- dectGeneralInfoGroup
  Objects which provide general information about the IP-DECT server.
- dectGeneralStatisticsGroup
  Objects which provide general statistics about the IP-DECT server.
- dectUserInfoGroup
  Objects which provide information about users on the IP-DECT server.
- dectRfpInfoGroup
  Objects which provide information about base stations (RFP) configured on the IP-DECT server.
- dectMediaResourceInfoGroup
  Objects which provide information about media resources configured on the IP-DECT server.
- dectNotificationsGroup
  Notifications that are generated by the IP-DECT server.

SNMP along with the associated Management Information Base (MIB), encourage trap-directed notification. The SPECTRALINK-IPDECT MIB includes a number of traps also called notifications. One example of a notification is "Connection to a base station is lost" another example is "Base station lost DECT synchronization".

Refer to the SPECTRALINK-IPDECT MIB for information available via SNMP

- Syslog settings are now controlled and distributed from the server. I.e. the settings on the server will override/control the settings on connected base stations and media resources. Previously if a syslog server was used, every single unit of the infra-structure needed to be configured for syslog individually, now everything can be configured in one place (at the server).

  This means that the following settings will be set on the base stations and media resources controlled by the server.

- log.syslog.host
- log.syslog.port
- log.syslog.facility
- log.syslog.level

- The system time and date as well as the time zone is now controlled and distributed from the server. I.e. the settings on the server will override/control the settings on connected base stations and media resources.
- If handset sharing is enabled and a busy user is re-associated the behaviour was un-predictable. Now this scenario is handled gracefully. The call is terminated and the re-association is effective
- When parsing SIP parameters, the server is now more forgiving with lower/upper case of some SIP parameters. This addresses DECTESC-534 where a "replaces" require was not understood from a specific Lync endpoint. This resulted in problems making a transfer from Zeacom (Lync SW based attendant console) to DECT handsets.
- A second incoming call (a call waiting call) is no longer automatically accepted if the other end of the original call terminates the original call. If A and B are in a call and C calls A, A will receive a call waiting indication. Previously, in the case of B hanging up, this would automatically result in A accepting the call. This is not necessarily what A wants, thus this has been changed. Now A actively needs to accept the new call.
- In an outgoing call, if a other party display name is received in a 1XX response to the outgoing INVITE, the other party display name is displayed in the handset. As an example this means that if A calls B, the display on A will indicate the display name of B already when phone B starts ringing. Previously the display name would not be updated before the call was answered by B.
- DAD (Duplicate Address Detection) has been improved. Previously DAD would only detect duplicate IP addresses if the IP address was assigned using DHCP. Now DAD will also report duplicate IP addresses in the case of a static IP address. To accomplish this, the start up sequence has been modified to wait for ethernet link before continuing.
- The IP-DECT server now supports parsing a SIP Contact header with a comma in the URI. This addresses an issue reported in DECTESC-535 regarding call transfer in a Shoretel PBX environment. The scenario causing the issue is as follows:
  An incoming call from a mobile phone hits a reception workgroup and makes a number of DECT handsets start alerting. The call remains unanswered and after a timeout, controlled by the Shoretel PBX, the call is automatically forwarded to a hunt group. A DECT handset, which is part of that hunt group, answers the call and attempts a consulted transfer to another phone. The above mentioned scenario failed before and is successful with the latest firmware.

- The name and version string of the connected SIP Server/Registrar is now logged when available. As an example when an OK is Received for a SIP REGISTER the Server Name/User Agent string received in the OK is logged in an INFO level log message. See the following for example log messages:

  ```
  ‘‘SIP user 2602 registered at 172.29.198.3 OpenSER (1.3.4-
  tls (i386/linux))’’
  ```

  ```
  ‘‘SIP REGISTER response 404 Not Found from:2602 to:2602
  Error received from Cisco-CUCM10.0’’
  ```

- The unit is designed to operate on a 100 Mbit full-duplex network. If the unit is deployed on e.g. a 10 Mbit network the DECT radio will drift in frequency. Although not encountered in real installations, some test lab setups involving a hub instead of a switch have been seen to operate with 10 Mbit. If the network is not 100 Mbit full-duplex mode the DECT radio will potentially drift out of the specified range, which will result in faulty behaviour. Starting with this firmware a warning will be logged if the network is not 100Mbit full-duplex.
- The base station is now more resilient towards being flooded with DECT page requests from the server. The number of page requests that can be suspended has been limited. When the base station reaches 75 page requests in the suspend queue, all incoming page requests will be dropped until the queue is reduced to 30 suspended page requests.
- Several minor improvements have been made to synchronization over the air.
- Some log messages indicating Signal link up/down were causing confusion because some customers interpreted these as if the IP link was up/down. It is now written as DECT signalling link up/down, to avoid confusion. Reported in DECTESC-530.
- In a redundancy setup the slave did not log the reason for TCP connect failure with the master. This made debugging of failure scenarios difficult. Now the reason is logged.
- Previously every time a DHCP lease was refreshed, it would result in a re-write of DNS information to the flash. Now a rewrite is only performed if the DNS information is actually changed.
- A state/event error is no longer logged, if an outgoing call is put on hold while ICE is completed. This is not an error situation and should not be logged as such.
- Dialog event package handling has been improved to provide more correct signalling towards e.g. Cisco Unified Call Manager.
- The Linux kernel is updated to 3.14.3.
- Various improvements to TCP/ICE handling. This includes more elaborate logging in failure scenarios to facilitate debugging and better handling of problematic scenarios.

- Logging of media handling has been augmented, this has no impact on normal usage however it increases the possibilities for debugging media-stream related problems.

Removed Features

None

Corrections

- If a call transfer to an entry in the phonebook was attempted on a 74-series handset, it was not successful. The signalling is now changed to allow for such a call transfer to succeed. This addresses an issue reported in DECTESC-533.
- Media handling has been improved. Make sure that resources and sessions are reset when allocated. This fixes an issue introduced in PCS14A_ which made handover and internal SRTP not work reliable. If internal SRTP was enabled some handover scenarios would result in noise in the media.
- The handling of handover signalling has been improved. In very rare scenarios, with handover occurring early in the call establishment, the handover could fail potentially resulting in loss of audio. This is now handled more gracefully.
- The process of subscribing handsets without requiring a specific IPEI has been improved. Previously if a SIP user was created without assigning a specific IPEI (device) and a handset attempted a subscription, the IPEI of the handset would be saved in the database even in the case of an unsuccessful subscription (e.g. if a wrong AC was entered). This resulted in the fact that any subsequent subscription attempts would require the same handset to be successful (otherwise the IPEI would not match). Now the IPEI is not stored in the case of an unsuccessful subscription.
- If the IP DECT Server receives a Lync conference Notify from a Lync server, it now responds with a 481 (Call/Transaction does not exist) instead of 500 (Internal server error) if no Lync conference is present. This is more correct.
- If the base station radio detects a high amount of unknown base stations, it could cause an overflow in unknown bases table, which in rare cases could result in a restart of the base station. This has been corrected.
- Handling of internal timers has been improved. Previously it was not always possible to find the end of timer list in all situations. In high load scenarios this could result in restarts.

Configuration File Parameter Changes

File	*Action*	*Parameter*	*Description*
config.xml	Added	snmp.enable	This enables SNMP and when enabled the device will respond to SNMP requests.

File	Action	Parameter	Description
			Values: true/false Default: false
config.xml	Added	snmp.community	The community string used for SNMP. The device will respond to requests for this community. Values: a string. Default: empty
config.xml	Added	snmp.traphost	The host to which SNMP traps are sent. Values: a hostname or an IPv4/IPv6 address Default: empty
config.xml	Added	snmp.trapcommunity	The community used for sending traps. Values: a string Default. empty
config.xml	Added	snmp.syslocation	A descriptive text telling the physical location of the device. Values: a string Default: empty
config.xml	Added	snmp.syscontact	The textual identification of the contact person for this host, together with information about how to contact them. Values: a string Default: empty

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.

- 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.
- 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.

- 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."
- 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.
- Improved handling of synchronization, the base station will not attempt a shift to secondary sync master if a secondary is not defined.
- 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.)

- 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.
- 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.
- 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.
- 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.
- Incoming early media handling has been improved. The IP DECT server now handles a=inactive in SDP in a 1XX response.
- 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.
- 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.
- 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.
- 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.

- 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.
- Handle XML escape characters in description when generating rfps.xml.
- 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

- 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.
- 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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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 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.

File	Action	Parameter	Description
			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.
- 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.
- 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.

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- When exporting users to a CSV or XML file using Users|Import/export, the users are sorted by username instead of by IPEI.
- 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.
- An IPEI is required before a SIP user registration is performed.
- 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.
- 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.
- Improved the way an address for internal RTP is selected. This avoids some connection problems in mixed IPv4/IPv6 setups.
- Make sure to log at least a notice level message when the connection from the base station to the DECT server is lost.
- 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

- 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.
- 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.
- 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.
- 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

File	Action	Parameter	Description
			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 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

- 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
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

- 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.
- 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.
- 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.
- 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.

- 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.
- The media resource sends the build number of the running firmware to the KWS in the startup message.
- The base station sends the build number of the running firmware to the IP-DECT Server in the startup message.
- 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.
- 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.
- 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.
- Log info message when provisioning download is started in order to ease debugging.
- 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).

- The firmware is prepared for a new license regarding the handling of repeaters on a KWS400 system.

Removed Features

None

Corrections

- 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.
- 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.
- 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

File	Action	Parameter	Description
			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

- 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.
- 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).
- 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.

- 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.

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

Version PCS13__

Initial KWS6500 version.