

Important Notes:

- **iNET and iNET-II units are not compatible in firmware nor in their radio links. iNETs cannot link with iNET-IIs nor upgrade to iNET-II functionality.**

01/19/2022

iNET and iNET-II Release 8.3.0

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware. Release files SHA256 sum:

dm2-8_3_0.ipk	3ee0f6c1824c8f7777a70409754c8a3515f9591233282b1fd95cff59b80bbd4d
dm300-8_3_0.ipk	29062e11c7cbdbd5098bf22a761bcb5d621ecd89d20fc2705050ef7efaf871a4
dm-8_3_0.ipk	0333f8f1b4f4d63c94df7cdbc48f4a8538ca0c90577762f8f7919feebcef3b0d
inet2-8_3_0.ipk	630f870a0ce144441e150dbfbc4ce918219f1c2e3d444b2732325b486ac4dfa7
inet300-8_3_0.ipk	9cd1dde1885791114e079279da2f6d453cb3b015f26616df1318dd452e837174
inet-8_3_0.ipk	9130d45d89caad4fd991787c6fed3f9c305dd3b2562e0b032c46731a9b67aa1f
lanlink2-8_3_0.ipk	e5392515baf0dfd00e115ea76f8b931c6d678c73f85d4c52b48ae623c29a7d8b
lanlink-8_3_0.ipk	bdf2c6de8e25baa4c05305d868de996317b0e17a3c28bfb5b0bba857db8d0df7
ts30-8_3_0.ipk	7f0a888e177d03f17ab41f0600c222ad7df586008c6cddb5f4d6dfd56246973e

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- XCTBYRG-64: Change non-user passwords to use salted hash and more than 8 characters. Factory and engineering passwords have changed. Factory logins will take around 30 seconds to check the hashed value.
- XCTBYRG-63: Add security options "X-Frame-Options: SAMEORIGIN" and "X-Content-Type-Options: nosniff" to HTML response headers.
- XCTBYRG-62: Remove 'authcode' and authorization key entry at password prompt for login.

Defect Fixes in Firmware

- XCTBYRG-63: Updated GoAhead webserver for Authentication Header Buffer Overflow.
- Prevent the 'Rebooting...' screen being overwritten when the user selects to reboot (Device Mode, RF Hopping Format, or Reboot Device).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' event log tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.2.0

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Apply patch for GoAhead Webserver CVE-2017-17562.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions. The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' event log tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.1.9

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Case GS-01289082: Add SNMP OID inetNcBridgeStp to control whether the bridge uses Spanning Tree Protocol.
- Support bundles will now include the OID for SNMP requests (they didn't for GS-01289050).

Defect Fixes in Firmware

- Case GS-01359746: Skip power control on Remotes when association state is Scanning. This prevents 'RF Power Control Saturated Low' (EVENT_POWER_LOW) alarm when Remotes remain in Scanning for extended periods. (With release 8.1.1 the alarm occurred after 2.5 hours of scanning regardless of 3841/42 MAC. With 6.9.1 and 3.0.0 the alarm occurred after about 14 hours of scanning.)

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions. The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' event log tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.1.8

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add logininfo factory command to display event log capacity.
- Add feature INET_SPURIOUS_REBOOT_DELAY to 1) delay aircctl initialization until after pcmcia cardmgr completes module installation and 2) delay dhcp, serdata, and sntpd interface polling until after aircctl brings up the bridge. With this change, the p_boot_sequence wait loop in menu.c main() has been removed (see "unexpected reboot" in release 8.1.3).

Changes/Additions to Existing Features in Firmware

- Prevent apparent failure of web event log view by closing any existing logWindow. Handle the view log request outside the header/footer block to avoid spurious 'HTML' line appearing onscreen during generation.
- Prevent SNTP time assignment from breaking DHCP client timeouts by using monotonically increasing time. (Powering on an iNET RM with DHCP client enabled and a valid SNTP server logged multiple, rapid DHCP requests on the DHCP server due to timeout corruption by the SNTP assignment.)
- Change nh_wait() to not use gettimeofday since it can return discontinuous time at reboot when the SNTP assignment occurs.
- Change set_console_baud() to call tcsetattr() only when the requested baud differs from the last one. This should prevent mysterious login failures at reboot due to corrupted input when serdata calls set_console_baud() at the same time as a login attempt.
- Change serdata interface wait loop to set SER_ESC only on updates.
- Add confirmation prompt to Send Log and Send Support Bundle console menu items, matching behavior of the web.
- Change getparm factory command:
 - 'getparm -a' with no match string displays all params
 - unrecognized param types are treated as integer redefinitions to display an appropriate value
 - params that are too large for the read buffer are skipped
- Remove copyright footer from banner web page since it renders no body (it only alerts if needed).
- Grey out the labels of unavailable channels on the Channel Configuration web page.
- Change Auto-Upgrade web page Reboot Remotes Now from a link to a button.
- Image size constraints – these changes reduce the .ipk package size 8 KB:
 - consolidate code for Ethernet Filtering to Ethernet Port web page
 - consolidate code for RSSI by Zone, Packets Received by Zone, and Wireless Network Status to Performance Information web page

Defect Fixes in Firmware

- IR60: Add captions to Ethernet Link settings and separate H/W Watch from Poll Address group to clarify the use of these settings.
- Remove unconditional syslog call in print_hop_table(), other FPGA debug logging is enabled via engineering command.
- Check the SNTP validation response to avoid setting the system time to an outlandish value.
- Change Packets Received by Zone console menu to show single percent sign.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions. The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' event log tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.1.7

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add Login Banner setting to the Device Security UIs, cfgscript, and SNMP. This provides a 500-character banner on serial, telnet, and ssh login consoles. When the setting is empty, the banner defaults to the Device Name (if set) or the Model Number (if Device Name is blank)—see the Device Information UIs. Non-default values bring up an alert after login on the web UI.
- Add feature LOGIN_BANNER_DEFAULT_NOTICE. When enabled, the Login Banner edit UIs show a notice that the displayed value is a default when appropriate.
- Add feature CFGSCRIPT_PROCESSING_PERCENT_STEP to control percent complete feedback during cfgscript import processing.
- Add feature SENDLOG_PERCENT_STEP to control percent complete feedback during log export.

Changes/Additions to Existing Features in Firmware

- Case GS-01159647: Add source of the alarm to “AP Ethernet Link Disconnected” event log entries.
- Change cfgscript import parsing to remove the last instance of semicolon from an input line rather than the first. This allows string parameters to include semicolon as long as the input line ends with the parameter help comment.
- Capture TFTP error details during transfer. Update certmgr, cfgscript, and sendlog console and web message handlers to use the returned detail string.
- Provide status feedback on console while generating and sending an event log or support bundle rather than using the sendlog_complete mutex.
- Change menu help prompt for enumeration settings to include Backspace key.
- Change Wireless Security web page Force Key Rotation from a link to a button.
- Increase the size of the Authorization Key web page entry box to avoid scrolling the entry. Correct a typo in the MAX_AUTH_ERRORS alert.
- Complete the RFC2349 transfersize support. This could be used by certificate or cfgscript import.
- Deprecate p_web_enable ('HTTP Enable') from cfgscript export and import—it was deprecated for SNMP in iNET release 5.7.2.
- Remove explicit handling of p_AP_priority parameters for cfgscript export—it only changes the help string in the export file and param_table.h could be updated to use the previous help text.
- Support bundle: correct the check for known unexported params from release 8.0.7 so blank entries aren't included.
- Add PARAM_CFG_PREVIOUS_NAMES_LIST and cfgscript.c name_change function to centralize param name changes.
- Remove unused RAM parameters to workaround airtcl assembly truncation problem that was introduced by the 20160106 Sabayon Linux update of my development machine.
- Image size constraints:
 - consolidate code for Login Status and Device Names to Device Information web page
 - use cgi_util functions for Starting Information and Configuration Summary web pages

Defect Fixes in Firmware

- Updated build to resolve the GHOST vulnerability.
- Correct Event Log web page submit navigating to a blank page (broken in 8.1.4).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions. The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' event log tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.1.6

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add feature EVENTLOG_PARM_CHANGE. When enabled, the event log stores 'Parameter Change <ParmName> <NewValue>' when flash parameters are stored.

Changes/Additions to Existing Features in Firmware

- Prevent console display of airtcl MAC reset during initialization—it's in the event log as usr1MAC.
- Reset SNR and RSSI to appropriate values per device mode so Performance Information UIs continue to show 'AP' on Access Points rather than changing to 'N/A'.
- Show 'Invalid Choice' for Network Interface Configuration console menu items that aren't available when VLANs are disabled.
- Restore menu help prompt for enumeration settings with a confirmation prompt: Network Config, Device Mode; Radio Config, Hop Format; Serial Config, Port Status; Device Info, Console Baud.
- Reduce SNTP validation interval from 1 minute to 2 seconds to ensure EVENT_TIME_FROM_SERVER is stored as quickly as possible (seems to apply to Access Points more than Remotes).
- Skip any event log entries >= EVENT_LAST.
- Remove unused RAM parameters to workaround airtcl assembly truncation problem that was introduced by the 20160106 Sabayon Linux update of my development machine.
- Change the project to use the mds_toolbox git archive rather than cvs.
- Resolve pcmcia build warnings and bridge-utils and pcmcia patch warnings.

Defect Fixes in Firmware

- Case 818032: Use separate buffers for settings requiring a reboot so the desired value isn't overwritten with the current value (Network Config, Device Mode).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions. The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.1.5

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add feature ALGOS_MERGED_FROM_MOCANA_DSF for SHA224, 256, 384, and 512 support with 802.1X device auth.

Changes/Additions to Existing Features in Firmware

- IR25/TR9482: Add feature EVENTLOG_KEY_ROTATION. When enabled, the event log shows 'MAC Parameter Changed' when the new key takes effect.
- Web UIs reordered so Security, RADIUS Config remains the third item, matching the console menu.
- Web navtree reordered so Redundancy Config follows Maintenance, matching the console menu.
- Allow redundancy settings to be changed while redundancy is disabled. (For previous behavior, enable feature REDUND_HELPER_TEXT.) Remove parentheses from options unit strings.
- Minor console menu changes
 - a. use standard layout for Redundancy Configuration submenus
 - b. all redundancy submenus show 'Invalid Choice' for entries outside the available items
 - c. Ethernet Filtering Config, DHCP Server Config, Trap Manager Config, Prioritized AP Config, Event Log, and Reprogramming console menus updated to use new macros
- Consolidate UI and SNMP code for package version string to new utility function.
- Resolve mocana debug build warnings.

Defect Fixes in Firmware

- None

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device authentication tested up to 4096-bit, sha512 on iNET-II with FreeRADIUS 3.0.10 modified to allow more than 50 rounds.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions. The dentry monitor introduced for iNET in release 8.1.4 will automatically reboot the unit with a 'MemAllc' tag under these conditions. Testing found no need for the monitor in iNET-II.

iNET and iNET-II Release 8.1.4

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add LOG_DATA_STR_UINT to support a 3-letter tag in event log entries with numerical extra data.
- Add feature EVENTLOG_STATS. When enabled, the first page of the event log contains statistics on lost associations during this power-on session.
- Add feature CMDLINE_GETPARMSIZE including a param_sizes array. When enabled, the getsize factory command can be used to find the largest parameters or list the size of a parameter.

Changes/Additions to Existing Features in Firmware

- Add the cert signature algorithm to Display Certificates UIs.
- Add feature DEVICE_AUTH_RESULT_FILE for supplicant mocana error detail UI and event log entries. Change the Performance Information, Wireless Network Status console menu to display mocana error detail for device auth method 802.1X in the Connection Detail field.
- Minor console menu changes
 - a. Security Config, Wireless Security, Approved List console menu changed to show the number of associated remotes or MAC address of current AP and the number of entries stored in the approved list
 - b. clear the prompt line in Network Config, Interface Config console menu (VLANs enabled) if the Ethernet Port Mode or Management VLAN Mode enum selection is escaped
 - c. Security Config console menu reordered so RADIUS Config is always item C
 - d. Engineering console menu reordered so SlabInfo is always item C
 - e. move Skip Zones console menu limit warning up one line
 - f. Device Names, Config Scripts, and WLAN Debug console menus updated to new macros
 - g. functions with no references compiled out
- Use LOG_DATA_STR_UINT to tag FPGA+MAC reset counts with 'MAC'.
- Use EVENT_ASSOC for usr1MAC and RMACDth event logging (matching AMACDth) so EVENTLOG_STATS only has one event to check for that category.
- Match the slabinfo_monitor scan format to the max name width (17) so large active object counts are parsed correctly. Change EVENT_UNUSED1 to EVENT_RESOURCE_LIMIT for slabinfo_monitor event log entries. Use LOG_DATA_STR_UINT to show the active object count for 'filp' resource warnings in the event log ('size' warnings still show the kernel buffer size and active object count). Add a dentry cache monitor using LOG_DATA_STR_UINT to identify dentry resource warnings in the event log. Prevent console lockup/network interface unresponsiveness on iNETs running an auto-refreshing web page by performing a MemAlloc reboot when the dentry cache exceeds 27000 entries. (Tests on iNET-II did not find a dentry cache limit so the monitor is disabled on iNET-II.)
- Match Configuration Scripts, Event Log, Manage Certificates, and Support Bundle web page file transfer parameter layouts to the Reprogramming page (40-character filename).
- Support bundle: include error code if dhcp client start fails; remove duplicate param task identifier.
- Remove explicit 384x MAC identifier from UIs and add it to the support bundle.
- Add a running count of packets and bytes to TFTP reprogramming DBG_VERBOSE debug builds, logged at intervals of 500 packets.
- Image size constraints: multiple copies of lookup tables have been consolidated as follows
 - a. redundancyInfo and ExtraEventInfo from nheventd.c, menu_redund.c, monitor.c, and redundconfig.c to event_util.c—reduce the .ipk file 12KB
 - b. complete_def_value from cfg_flash.c to util.c—reduce the param executable 16KB
 and code consolidated as follows
 - a. remove the size element from param.c param_disp—reduce the param executable 1KB
 - b. use cgi_util functions for Ethernet Port, Network, Radio, and SNMP Configuration web pages—reduce httpd by 7KB

- c. use `cgi_util` functions and consolidate submit functions for Configuration Scripts, Event Log, Reprogramming, and Support Bundle web pages—reduce `httpd` by 1KB
- Consolidate `valid_field` cases to use `param_types` and `param_sizes`. This removes parameter-specific validators in favor of generic validators based on type.

Defect Fixes in Firmware

- Correct Network Configuration web page so submitting a Device Mode change takes effect.
- Prevent System Error with SHA1 certificates by forcing SSL retries to use separate thread instances. This reverts a change for TR12033/7711 introduced in release 7.3.7/3.0.7.
- Prevent Maintenance, Support Bundle console menu returning to Event Log menu on exit if Current Alarms is viewed before entering Maintenance menu.
- Stop concatenating `EAP_TLS` and `EAP_INTERMEDIATE` reason strings.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the `dentry_cache` is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.1.3

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Case 712819 – Add Validate Cert Chain setting to the Manage Certificates UIs using a RAM parameter—the setting defaults to enabled at every power on. Skip chain validation when the setting is disabled to support tiered PKI without storing the intermediate or issuing CA certs.
- Add Display Certificates to the iNET-II Manage Certificates UIs.
- Add GHOST vulnerability check. Since there is no testui command on iNET the check is added as the test-ghost executable, available to root logins.

Changes/Additions to Existing Features in Firmware

- TR-7812 workaround – Use initctl to reboot if the call to /sbin/shutdown fails for factory DEFAULT command, console menu Reset to Factory Defaults, snmp or web device mode change, login password serial number single-remote mode toggle, or p_auth_override disable.
- When mobility is disabled and beacon learning is “on association” (iNET-II RMs), use 10% trimmed mean RSSI calculation rather than the running average of every sample (merged from 7.5.7).
- Move 3842 MAC Reprogramming UIs' minimum build warning above Current Firmware. The previous line is used for console Image Verify, Reboot Device, and general invalid choice feedback.
- Add Support Bundle to the Maintenance web page.
- Separate two-value event log data entries with a semicolon to reduce confusion that it's one value with a thousands mark. Use the correct log data type to prevent truncation when a value is < -99.
- Reduce dhcp client monitor from 3 to 1 minute intervals and use zero PID acquisition retries to keep the restart delay as short as possible.
- Reduce console monitor PID acquisition retries from 10 to 3 to reduce restart delay.
- Consolidate console endpoint, remote perf, and SDB debug menu code to remote listing menu.
- Consolidate Endpoint List and Remote List web page code.
- Consolidate Bridge Status and Bridge Configuration web page code.
- Consolidate dropdown code for Security Configuration and Device Information web pages.
- Align Database Timeout with the other entry fields on the Network Configuration web page.
- Empty the view, clear, and send status when exiting the Event Log and Support Bundle menus.
- Free path_info memory on web pages that auto-refresh.

Defect Fixes in Firmware

- TR-12869 – Change GET_MAC_TIMEDOUT to return the result of driver call regardless of success. Re-enable periodic MAC timeout check for both AP and RM. Removing the rem_ctl.c HopSMAC MAC reset in release 8.1.2 has resolved the spurious reboots with data on iNET 3842 MAC RMs.
- TR-11132 – Restore the restricted hfa384x_cmd_initialize interrupt disable that was first released in 8.0.5 and then removed in 8.1.0. Removing the rem_ctl.c HopSMAC MAC reset in release 8.1.2 has resolved the spurious reboots with data on iNET 3842 MAC RMs.
- Correct SNMP inetChannelConfigTable walk broken by TR9633 in release 7.2.6/2.9.6.
- Correct SNMP walk on RMs by restricting update_sdb_cache to APs.
- Prevent iNET unexpected reboot at immediate login after power on by delaying the login prompt until serdata has initialized. This applies to iNET (not iNET-II) build variants regardless of MAC HW.
- Correct console monitor to attempt restart if the monitor PID is 0 after the retries are exhausted.
- Change console monitor to confirm 5 seconds after the monitored process is found missing. This closes a timing hole found with repeated login/exits.
- Use HTML entities so unknown IP addresses aren't blank in Remote and Endpoint Listing web UIs.
- Ensure unknown IP addresses aren't hyperlinked in Remote Listing web UI.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Display Certificates UIs are omitted from iNET build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.7 and iNET-II Release 3.2.7

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.5.6** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Disable `RSSI_DEBUG_PRINT_S` and remove RSSI history debug logging code. iNET-II RMs will use 10% trimmed mean RSSI while mobility is disabled and beacon learning is on association. `snmpget iNetStaRssi` debug logging enabled in 7.5.4/3.2.4 remains in place (forgot to remove it).

Defect Fixes in Firmware

- None

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the `dentry_cache` is not properly cleaned up under low memory conditions.

iNET Release 7.5.6 and iNET-II Release 3.2.6

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.5.5** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Add missing p_rssi update flag for the original calculation path (mobility is enabled or beacon learning is not "on association").
- Correct SNMP walk on RMs by restricting update_sdb_cache to APs.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.5 and iNET-II Release 3.2.5

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.5.4** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Disable monitor RSSI_BY_CHANNEL_DEBUG and change RSSI_DEBUG_PRINT_S from six- to three-minute intervals to investigate point-to-point RSSI variation reported by customer.
- When mobility is disabled and beacon learning is "on association", use 10% trimmed mean RSSI calculation rather than the running average of every sample.

Defect Fixes in Firmware

- None

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.4 and iNET-II Release 3.2.4

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.5.3** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- Add GET_MAC_TIMEDOUT ioctl to directly return the result of an hfa384x_docmd_wait call (merged from 8.1.0 and corrected to return the result regardless of success).

Changes/Additions to Existing Features in Firmware

- Enable monitor RSSI_BY_CHANNEL_DEBUG and RSSI_DEBUG_PRINT_S at six-minute intervals to investigate point-to-point RSSI variation reported by customer.
- Enable snmpget iNetStaRssi debug logging to investigate point-to-point RSSI variation reported by customer.
- Save extra data so timestamps can be resolved after a log clear in previous power on cycles (merged from 8.0.6).
- Quiet fixup_log_timestamps debug logging.

Defect Fixes in Firmware

- TR-12869 – Use GET_MAC_TIMEDOUT in airctl MAC monitor rather than relying on macFailCnt (merged from 8.1.0 and adapted for APs).
- Correct inetChannelConfigTable walk broken by TR9633 in mainline release 7.2.6/2.9.6, crc release 3.0.1.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.1.2

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Remove HopSMAC MAC reset. Under PAG gauntlet test (compression, encryption, 802.1X device auth with data mix including TCP, UDP, modbus, web, and pings) 3842 MAC RMs can reboot when scanning for 10 minutes, 3841 MAC RMs can log a MemAlloc reboot when scanning for several hours. (On iNET-II RMs the scanning is being extended due to the AP IP finalize association check that should also be looked at. iNET-II RMs that aren't using mobility should have up to 10 seconds to obtain the AP IP address before it's needed for the IP connection ping.)

Defect Fixes in Firmware

- None

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Config UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET 300MHz build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.1.1

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Disable the TR12869 RM MAC timeout check for now—release 8.1.0 seems to have more reboot-with-data on iNET 3842 MAC RMs and one messages log showed the MAC timeout yet the aircctl monitor did not trigger a MAC reset.

Defect Fixes in Firmware

- None

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Config UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET 300MHz build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.1.0

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add GET_MAC_TIMEDOUT ioctl to directly test the result of hfa384x_docmd_wait.
- Merge BEACON_CHANGE_TX_DELAY feature from release 7.3.5/3.0.5 on the crc branch. For now, use it only for auto-upgrade and AP MAC parameter changes and AP forced reboot of RMs.
- Prevent 3842 MAC hardware from downgrading to releases less than 8.0.0 unless initiated by a root console login. Reprogramming UI warning text remains in place.

Changes/Additions to Existing Features in Firmware

- Show device status as well as 'Alarmed' (when applicable) on the Starting Information Screen.
- Stop logging an event when DHCP client monitor triggers a client restart.
- Hide selection letter for Fragmentation Threshold when encryption is enabled on RMs.
- Update airctl monitor to use get_procinfo.
- Increased the size of the temp string buffer in oid_to_str() and added a length check to make sure we don't overrun it (merged from Mercury-e 3.5.4).

Defect Fixes in Firmware

- TR-12869 – Use GET_MAC_TIMEDOUT in airctl MAC monitor rather than relying on macFailCnt.
- TR-12867 – Fixed inability to set empty strings (and set things to an empty string) via snmp (merged from Mercury-e 3.5.4).
- Partially revert TR11132 by removing the interrupt disable in hfa384x_cmd_initialize (see release 7.2.4). The disable may be contributing to the reboot-with-data issue occurring in PAG large system test. The wlandev state set part of TR11132 in prism2sta_initmac remains in place.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Config UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET 300MHz build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.9

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Change factory LINK command on APs to return the number of associated remotes (as Mercury does) rather than the text 'AP'.
- Update console monitor to use get_procinfo and allow 10 restart attempts.
- Change slabinfo_monitor to log the unused event for the pool limit debug rather than 'User Selected Reboot' so it won't imply a reboot failed.
- Always log an event for excessive join request association loss.

Defect Fixes in Firmware

- TR-12869 – Exercise MAC driver in airctl monitor on RMs to detect MAC timeout.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Config UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET 300MHz build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.8

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Restart the DHCP client if it dies (log EVENT_SYSTEM_ERROR for now).
- Add a warning to 3842 MAC Reprogramming UIs stating minimum build number.

Changes/Additions to Existing Features in Firmware

- Bridge Status UIs have been omitted from iNET 300MHz build variants due to image size.

Defect Fixes in Firmware

- TR-12873 – Remove trailing comma from MIB mdsINetEventObject, inetRedundancyEventName.
- TR-12876 – Merge the max beacon wait immediate scan adjust into ReturnToScanning so any ongoing 802.1X device auth session is cleaned up.
- Free sdb_list obtained with hw_wlan_get_sdb_list.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Config UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET 300MHz build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.7

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Restore max beacon wait trigger to 10s to match the features in 8.0.5. Remove 5s rapid adjust after max beacon wait is triggered but retain the immediate scan adjust.
- Restore TR11999/9467 periodic AP IP request to match the features in 8.0.5.
- Add 500ms delay for 3842 MAC RMs between rejoin associate and join calls (see TR11558, 8.0.5).
- Consolidate Remote Performance Listing web page code with Remote Listing to reduce build image size. Restore Bridge Status UIs to the iNET 300MHz MDS build.
- Cleanup 'convert_value_to_string failed' warnings for known unexported params in cfgscript and support bundle.

Defect Fixes in Firmware

- Use FPGA+MAC reset when AP MAC death watch finds the MAC has become unresponsive (merged from 7.5.3).
- Increment macFailCnt when transmit returns -ETIMEDOUT to trigger AP airctl.c MAC_HasFailed (merged from 7.5.3).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Config UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.3 and iNET-II Release 3.2.3

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.5.2 and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Increment macFailCnt when ioctl returns -ETIMEDOUT to trigger airctl.c MAC_HasFailed (merged from 8.0.6).

Defect Fixes in Firmware

- Use FPGA+MAC reset when AP MAC death watch finds the MAC has become unresponsive.
- Increment macFailCnt when transmit returns -ETIMEDOUT to trigger AP airctl.c MAC_HasFailed.
- Correct statement order in prism2sta_initmac so allocate error can be logged.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.6

This is an iNET and iNET-II release based on mainline. It supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add Maintenance, Support Bundle console menu with a shortcut in the Event Log menu.
- Partial RFC2349 transfersize support – add size for cfgscript, event log, and support bundle export.
- Add SIGUSR1 (print) and SIGUSR2 (force) to snptd to debug remotes not getting time assignment.
- Add LOG_DATA_UINT, _INT2, and _UINT2 for debugging with event log extra data.
- Add feature EVENTLOG_FILTER. When enabled, the console event log view can be restricted by priority (critical, major, or minor).

Changes/Additions to Existing Features in Firmware

- TR-11132 – Increment macFailCnt when a WLAN driver ioctl times out to trigger MAC reset.
- Revert TR11999/9467 periodic AP IP request to reduce uplink data load—RMs will only get AP IP address changes on reassociation.
- Increase RM max rejoin attempts from 5 to 10.
- Decrease RM max beacon wait trigger from 10 to 5 seconds. When a max beacon wait occurs, do an immediate scan adjust (FPGA reset) and continue scan adjusts every 5 seconds for 1 minute.
- Save extra data so timestamps can be resolved after a log clear in previous power on cycles.
- Change log service from numbering event log entries one line at a time to five lines at a time.
- Defer MemAllc reboot for two minutes when FPGA+MAC reset is enabled and a RM is connected (merged from 7.5.2).
- Ignore PLL unlock immediately after FPGA+MAC reset (merged from 7.5.2).
- Add DEBUG_FLAGS for mocana and WLAN debug control. Move AES_CRYPTO to SECURITY_FLAGS.
- Decode TxExc frame in debug log. Log TxExc type and rx frame type when WLAN debug level > 2.
- Identify rogue data packet source address in debug log.
- Bridge Config UIs have been omitted from iNET non-MDS build variants due to image size.
- Bridge Status UIs have been omitted from iNET 300MHz build variants due to image size.

Defect Fixes in Firmware

- Stop sendlog getting stuck by exiting tftp_send_nextpacket when there are no more retries.
- Prevent iNET-II RMs never getting time by updating snptd when p_remote_ap_ip_addr changes (due to TR11999/9467 being reverted in this release as well, iNET-II RMs may still never get time).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Bridge Status UIs are omitted from iNET non-MDS build variants due to image size constraints.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.2 and iNET-II Release 3.2.2

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.5.1** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- Add LOG_DATA_UINT, _INT2, _UINT2 for debugging with event log extra data (merged from 8.0.6).

Changes/Additions to Existing Features in Firmware

- Defer MemAllc reboot for two minutes when FPGA+MAC reset is enabled and a RM is connected.
- Ignore PLL unlock immediately after FPGA+MAC reset (airctl up).
- Always log the IP address whether the RM reassociated or changed address (merged from 8.0.5).
- Bridge Status UIs have been omitted from iNET non-MDS build variants due to image size (merged from 8.0.5).

Defect Fixes in Firmware

- Exit nextpacket when there are no more retries to prevent stuck sendlog (merged from 8.0.6).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.5

This is an iNET and iNET-II release based on mainline. It merges the features of 8.0.4 and 7.5.1 and supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add authcode login to simplify factory production due to security changes introduced in 7.2.6.

Changes/Additions to Existing Features in Firmware

- TR-12859 – Change login and lockdown events to persist across reboots.
- TR-11132 – Restrict the interrupt disable part of the solution to 3842 MAC hardware (see 7.2.4).
- Always log an event for the call to Reset_MAC when the HopSyncCount limit is exceeded.
- Always log the current IP address whether the RM reassociated or had an IP address change.
- Retain Maintenance, Ping Utility menu settings across logins.
- Remove the word 'Workaround' from the FPGA reset UIs and cfgscript. Map old name to correct parameter when importing cfgscripts.
- Use the FPGA reset action to label the reset period in the Configuration Summary Radio status.
- Consolidate data rate strings and RM performance state strings for Radio Config, Remote Listing, and Remote Performance Listing UIs.
- Show the upgrade firmware version as '<major>.<minor>.x', e.g. 8.0.x, since only the major and minor version numbers are significant.
- Bridge Status UIs have been omitted from iNET non-MDS build variants due to image size.

Defect Fixes in Firmware

- TR-12858 – Change COMPANY_URL from microwavedata.com to gemds.com.
- TR-11558 – Add HOP_SYNC substate SET_SSID_REJOIN. Use it on 3842 MAC RMs to call associate_nethop rather than simply attempt_to_join when Assoc_WaitLoop finds the link status is DISCONNECTED and calls TryToRejoin. This solves the 3842 false association case due to somehow mishandling the AP's disassociate message when the database timer expires.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.1 and iNET-II Release 3.2.1

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.4.7** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- Add p_fpgaNoAssocAction flash parameter to control what occurs at AP no-remotes FPGA reset. Add action FPGA_ACTION_FPGA_MAC_RESET to reset both the FPGA and MAC. Add function start_ap_bh() to WLAN_AP builds to support MAC reset.
- Add fpgaaction factory command to provision p_fpgaNoAssocAction if necessary.
- Add the iNET300 channel count to Configuration Summary Radio status (merged from 8.0.4).
- Add the remote count to the AP's Configuration Summary Connection status (merged from 8.0.4).
- Add the AP addresses to the RM's Configuration Summary Connection status (merged from 8.0.4).

Changes/Additions to Existing Features in Firmware

- Log the FPGA reset period when the reset is enabled regardless whether reset logging is enabled.
- Show FPGA reset settings even when the reset is disabled.
- Change FPGA Workaround Reset to numeric display—showing 'Off' suggested one should enter 'On' to enable the reset. Log the FPGA reset period when the reset is enabled (merged from 8.0.4).
- Retry TFTP send when received ack is for the preceding packet (merged from 8.0.4).
- Log an event for calls to Reset_MAC due to USR1 signal and AP or RM MAC death watch (merged from 8.0.4).

Defect Fixes in Firmware

- Reacquire DHCP client ifindex rather than exiting when a socket error occurs (merged from 8.0.4).
- Ensure bridge init opens the socket only once (merged from 7.2.8).

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.4

This is an iNET and iNET-II release based on mainline. It includes the features of **8.0.3** and supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- Add htable factory command to display the current hop table at any time.
- Add the iNET300 channel count to Configuration Summary Radio status.
- Add the number of associated remotes to the AP's Configuration Summary Connection status.
- Add the AP MAC and IP addresses to the RM's Configuration Summary Connection status.

Changes/Additions to Existing Features in Firmware

- TR-7777 – Change EVENT_CNTY_MISMATCH wording to 'Hop Format/SkipZone Mismatch'.
- Use the original MACDEV_IOC_DISABLE_MACPORT sequence on remotes regardless of 384x MAC. The new sequence will only be used on 3842 MAC APs.
- Change FPGA Workaround Reset to numeric display, showing 'Off' suggested one should enter 'On' to enable the reset. Log the FPGA reset period when the reset is enabled.
- Retry TFTP send when received ack is for the preceding packet.
- Log an event for calls to Reset_MAC due to USR1 signal and AP or RM MAC death watch.
- Hide Key Rotation in the AP's Wireless Security menu when Encryption is disabled, they don't apply.
- Use prev_menu_msg prompt in the RM's Skip Zones menu.

Defect Fixes in Firmware

- TR-12767 – Radius API will now store off state AVP dynamically, instead of truncating to 16 bytes.
- TR-12402 – Revert the SIGHUP handler in sshd and add a monitor in menu for sshd exiting.
- TR-12395 – Verify the DHCP client param when the 15-second airctl startup delay is used.
- TR-11688 – Prevent user-initiated reboot during bootloader programming.
- TR-7777 – Set EVENT_CNTY_MISMATCH and reject the beacon if the channel bytes in the beacon are on when the RM is using a non-channel hop format (iNET only).
- Reacquire DHCP client ifindex rather than exiting when a socket error occurs.
- Correct SysInfo and SlabInfo redraw in the Engineering menu.

Compatibility

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- 802.1X device auth tested up to 4096-bit certs, sha1 signatures, on Windows FreeRADIUS 1.1.7.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.5.0 and iNET-II Release 3.2.0

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of **7.4.6** and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- Update FPGA to support 3842 MAC hardware—handle MAC data output on either TX clock edge.

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- FPGA transmit TX_PE exception handled, adjacent packets in this case will now be processed.
- FPGA unused P_PHY_TXR set to high impedance to avoid MAC T/R_SW output on the same pin.
- Ensure bridge init opens the socket only once (merged from 7.2.8).

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.7.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.3

This is an iNET and iNET-II release based on mainline. It includes the features of 7.4.7 and supports both 3841 and 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR11738 – Revert the MAX_BEACON_WAIT_RESET_MAC feature from 8.0.1, it causes dropped ethernet packets.
- TR11742/11558 – Revert the FALSE_ASSOCIATION_MONITOR feature from 7.2.8, it has a memory leak.

Known Errata and Limitations in Firmware

- Running a non-3842-supporting release on 3842 MAC hardware will prevent association. Check the Configuration Summary for a unit's MAC hardware.
- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.7.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.7 and iNET-II Release 3.1.7

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.6 and the listed changes. Specifically, it has FPGA support for 3842 MAC hardware but no driver support.

New Features Present in Firmware

- Update FPGA to support 3842 MAC hardware—handle MAC data output on either TX clock edge.
- Add Configuration Summary UIs including 384x MAC variant and FPGA revision.
- Add getparm factory command (merged from 7.2.7).
- Add wlaninfo -getridwithsize for RIDs with sizes other than just 16-bit values (merged from 7.2.2).

Changes/Additions to Existing Features in Firmware

- Change some association event log entries to persist across reboots (Association Established/Lost, Association Lost - AP's Ethernet Link Down, Current AP Dropped - RSSI, Current AP Drop - Forced).
- Use beacon channel RSSI in the Performance Information and Wireless Network Status console menus to avoid confusion when the mobility RSSI association threshold is applied.
- Move DHCP Server Config console item G) Commit Changes to column 2 to make it more visible.
- Match web Event Log, Packet Stats, Reprog, and Config Script field name format to the console UI.
- Add CFISupRange to the RID_INFO_LIST so it can be retrieved with just wlaninfo -getrid. CFISupRange is used to distinguish 3842 MAC from 3841.
- Consolidate the definitions of param_names and _types to reduce image size (merged from 7.2.7).
- Reduce TFTP debug logging.

Defect Fixes in Firmware

- FPGA transmit TX_PE exception handled, adjacent packets in this case will now be processed.
- FPGA unused P_PHY_TXR set to high impedance to avoid MAC T/R_SW output on the same pin.
- Apply the current mobility RSSI association threshold backoff step to the disassociation threshold, preventing immediate disassociation when the backoff triggers association.
- Match web Reprogramming and Config Script field error processing to the web Event Log.
- DHCP running process check now includes one retry to prevent intermittent process restart failure. Also clear the read buffer to stop sequential calls returning the same value for client and server.
- Add compile-time definitions for SNMP sysObjectID (merged from 7.2.8).

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.7.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.6 and iNET-II Release 3.1.6

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.5 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Add RSSI channel history RAM parameter for RMs in mobility mode with beacon learning "on association". Use the beacon channel RSSI (if available) for the association threshold check.
- Add EVENT_TIME_FROM_SERVER to regenerate real timestamps in event logs from previous power-on cycles (merged from Mercury).

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Add missing EVENT_FACT_ACCESS, EVENT_MOBILE_AP_DROP, EVENT_FORCE_MOBILE_AP_DROP, EVENT_CERT_VERIFY, and EVENT_CERT_CHAIN to SNMP function send_event_trap_to_agent.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.5 and iNET-II Release 3.1.5

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.4 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Add RSSI association threshold backoff time and step flash parameters, available in the Mobility Configuration UIs on RMs.
- Added distribute_zip build target to support new PLM ECO process.

Changes/Additions to Existing Features in Firmware

- TR-11999/9467 – Add DHCP_RM_AP_MONITOR feature to configure iNET-II RMs' AP IP request.
- Wireless Network Status console menu includes RSSI, SNR, and connection detail in mobility mode.
- Reinstate console event numbering code for UI performance (partially revert TR12394 changes).
- The Ethernet Port Config web page now matches the item names used on the console menu.
- Redundancy Configuration now uses standard selection in the console menu (merged from 8.0.1).
- Redundancy Config web page layout changed to fit items without wrapping (merged from 8.0.1).
- Web navtree now always links to Redundancy Config pages rather than conditionally alert (merged from 8.0.1).
- Add Log Extra Assoc setting to WLAN Debug engineering menu for runtime control of debug info (merged from 8.0.1).
- Update RSSI By Zone and VLAN Packet Stats menu accessibility. Change Performance Information submenu prompts to new prev_menu_msg or view_list_msg (merged from 8.0.0).
- Radio Config menu only shows selection letter for accessible items, matching the web page (merged from 7.2.8).
- Engineering menu layout and prompts match standard layout and behavior (merged from 7.2.8).

Defect Fixes in Firmware

- TR-12437 – Delete existing default route to prevent EVENT_ROUTE_ADD (Route Add Failed).
- TR-12395 – Use 15-second DHCP client startup delay only when p_airctl_up is false (at power on).

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high at power on even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.4 and iNET-II Release 3.1.4

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.3 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Add ifconfig, route, and brctl to support bundle.

Changes/Additions to Existing Features in Firmware

- Align IP Address Config console menu with the main menu so E) Commit Changes is more visible.

Defect Fixes in Firmware

- TR-11999/9467 – iNET-II RMs request the AP IP address every two minutes once associated to update Wireless Network Status if the AP gets a DHCP assignment.
- Add dropped AP to the blacklist when Mobility Mode is enabled, Beacon Learning is on association, and the RM drops association due to max beacon wait (exclusive APs).
- IP Address Configuration console menu now reports invalid_choice_msg if E) Commit Changes is selected when no change has been made.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.3 and iNET-II Release 3.1.3

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.2 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Exclude current channels from the scan table when Mobility Mode is enabled, Beacon Learning is on association, and the RM drops association due to RSSI or max beacon wait (exclusive APs).
- Add RSSI association threshold and channel config groups to the cfgscript.

Changes/Additions to Existing Features in Firmware

- Poll the AP immediately when Beacon Learning is on association rather than waiting for the monitor loop to schedule a poll.
- Cfgscripts include settings regardless of current device mode, AP or RM.
- Omit empty DF1 settings from support bundle cfgscripts.
- Change factory ping command to accept -c count option.

Defect Fixes in Firmware

- TR-12426 – Erase existing certs when a new root cert is loaded.
- TR-12425 – Stop logging X.509 Certs Failure (EVENT_CERT_VERIFY) on AP power up.
- Make AP bridge UIs and cfgscripts consistent with actual bridge priority value.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.2 and iNET-II Release 3.1.2

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.1 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Include cfgscript in support bundle "mds_eng_conf.log".

Changes/Additions to Existing Features in Firmware

- Add RSSI event log detail: AP MAC address for beacon whose RSSI is below association threshold.
- Interpret the system uptime for previous event log entries as days, hours, minutes, and seconds.
- Change cfgscript header time to use UTC offset.

Defect Fixes in Firmware

- TR-12403 – Add certutils to iNET builds and validate certs on RMs when retrieved.
- TR-12401 – Add refresh to login.cgi for when the web lockout expires.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.1 and iNET-II Release 3.1.1

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.4.0 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Log EVENT_SYSTEM_ERROR if the AP's beacon MAC changes.
- Add RSSI association threshold flash parameter, available in the Mobility Configuration UIs on RMs.
- Backspace key selects previous value for enumeration menu items (merged from 7.2.8).

Changes/Additions to Existing Features in Firmware

- Add RSSI event log detail: current RSSI level, threshold.
- Add Received Beacon event log detail: length, CRC, or current RSSI level, threshold.
- FPGA workaround moved to Radio Config, Advanced Config on APs (console only); all login levels.
- Starting screen UIs always show the current IP address rather than based on p_dhcp_enable.
- Add IP connectivity event log detail: reassociate or new address.
- Authcode logins support engineering password enable, with no user feedback (merged from 8.0.0).
- Ethernet Port, Network, and Radio Config web page layouts changed to fit items without wrapping (merged from 7.2.8).
- Performance Information web page for APs shows Actual Data Rate, matching the console (merged from 7.2.8).
- Prioritized AP Configuration web page now includes a link to the Approved Access Points list, matching the console (merged from 7.2.6).
- Network Config web page uses center alignment for Rem-to-Rem Bridging (merged from 7.2.4).
- Change wlaninfo -getrid engineering tool to try get_config_rid_with_size before get_config_rid.

Defect Fixes in Firmware

- TR-12402 – Register sshd for SIGHUP so logging in then quitting the client won't hold resources.
- TR-12398 – Add lockout case when other RADIUS error occurs and local fallback is disabled.
- TR-12394 – Exported event logs include entry numbers, matching the console and web views.
- TR-12376 – Serial wizard data baud detail web page shows set value rather than always 9600. Similarly the flow control detail shows set value rather than always disabled (merged from 7.2.2).
- TR-12037 – Auto-Upgrade web page now handles multiple changes in one submit.
- Authcode logins show 'Setting factory defaults' only when password reset authorization is present (merged from 8.0.0).
- Prevent errors from appearing on the console during support bundle generation.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as release 6.9.1 or 3.0.0.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.4.0 and iNET-II Release 3.1.0

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.9 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Add detail to ioctl error debug logging in add_route. Prevent the dbglog filling with 'ioctl() for ip addr failed' when DHCP client address has not yet been assigned.

Defect Fixes in Firmware

- TR-12372/12373/12377 – Revert the solution to TR-11735 from release 7.3.2; DHCP client routing will work now but lease expiration will no longer reset the unit's IP address.
- TR-12371 – Revert the solution to TR-12279 from release 7.3.8 and add dhcpc_daemon_exited as an alternate. Verify current IP configuration before applying settings.
- TR-11119 – Avoid test mode PLL unlock by setting synth controls (merged from 7.2.4).
- Clear EVENT_RSSI alarm when association is lost.

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as previous releases.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.9 and iNET-II Release 3.0.9

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.8 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Add factory command line ping command (merged from Mercury-e).

Changes/Additions to Existing Features in Firmware

- Add empty filename check to Event Log console Send Log, matching the web (merged from 8.0.1).
- Add confirmation prompt to Event Log console Clear Log, matching the web (merged from 8.0.1).
- Add Send Event Log settings to Event Log web page, matching the console (merged from 8.0.1).
- Add letter keys to navigate logs/lists: (U)p, (D)own, (P)gUp, PgD(n), (H)ome, (E)nd (merged from 7.2.7).

Defect Fixes in Firmware

- TR-12306 – Revert TFTP default block size to 512 bytes, it broke file export at the smaller size.
- TR-11541 – Add console baud to the Device Information web page (merged from 7.2.8).
- TR-7055 – Web event log entries are numbered, matching the console (merged from 7.2.4).
- Prevent 'RootFS 93%' when image copy region changes from kernel to rootfs (merged from 8.0.1).
- Enable backspace and control keys in the factory and shell command line (merged from 7.2.8).

Known Errata and Limitations in Firmware

- Auto-upgrading your network may take more than twice as long as previous releases.
- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior, the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.8 and iNET-II Release 3.0.8

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.7 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- Log EVENT_SYSTEM_ERROR if the console menu dies.
- Remote Listing console menu includes disassociate and remove controls for engineering logins.

Changes/Additions to Existing Features in Firmware

- Returned max time in scanning/wait for beacon state from 6 to 1 minute (merged from 7.2.8).
- Reduce TFTP default block size from 512 to 256 to improve auto-upgrade performance under load.
- Stop p_package_ver updates debug logging 'unrecognized parameter' during reprogramming.

Defect Fixes in Firmware

- TR-12279 – DHCP running checks now include the starter task.
- TR-11834 – SNMP walk of mdsReprogramming OID now returns all elements.
- TR-9477/3564 – Toggling auto key rotation with encryption enabled no longer drops all remotes.

Known Errata and Limitations in Firmware

- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.7 and iNET-II Release 3.0.7

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.6 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- TR-10731 – The no remotes workaround FPGA reset and logging are now under parameter control in the Radio Configuration console menu for factory logins and above (merged from 7.2.4).
- Bring iNET300 channel config menu up-to-date with changes from TR11819.
- Add invalid_choice_msg to RM's wireless security menu key rotation options.

Defect Fixes in Firmware

- TR-12033/7711 – Retry SSL_negotiate on error. Log EVENT_SYSTEM_ERROR on RMs if airctl dies.
- TR-11990 – Fail the empty image check in verify_image for empty regions rather than pass.
- Fix alerts and other popup behavior on Ethernet Port, Event Log, Network Interface, Radio Config, Skip Zone Options, and VLAN Config web pages (merged from 7.2.4).

Known Errata and Limitations in Firmware

- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.6 and iNET-II Release 3.0.6

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.5 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- TR-11914 – Remove BEACON_CHANGE_TX_DELAY_SECS feature—large system test shows auto-upgrade duration doubled with it in place.

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.5 and iNET-II Release 3.0.5

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.4 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- TR-12068 – Upgraded mds_toolbox for mocana_ssuite to support 4096-bit certs and lower.

Defect Fixes in Firmware

- TR-11914, 11820 – Add BEACON_CHANGE_TX_DELAY_SECS feature to control how long the beacon should be disabled on AP param change. Initially set to 6 seconds.

Known Errata and Limitations in Firmware

- 802.1X device auth tested up to 4096-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7. Client certs larger than 1024 bits may require more than 50 rounds to authenticate.
- Due to legacy behavior the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.4 and iNET-II Release 3.0.4

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.3 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- TR-12068 – Upgraded mocana_ssuite subsystem supports 2048-bit certs and lower using sha1WithRSAEncryption signature algorithm.
- TR-11997 part 1 – Correct the p_blacklistTimer helpString.

Defect Fixes in Firmware

- TR-12035 – SNTP continues waiting until DHCP assigns an address and validates after assignment.
- TR-12034 – Add valid_multicast_ip_addr for multicast IP addr cfgscript import. This also causes the default in cfgscripts and UI to change from 0.0.0.0 to 224.0.0.0.
- TR-12033 – Upgrade the mocana_ssuite subsystem to the mainline tip (matching release 8.0.2).
- TR-11987 – Restrict the fallback DHCP process check to match the process command line.
- TR-11986 – Add the same guard conditions & daemon handling for DHCP to cfgscript as in the UIs.

Known Errata and Limitations in Firmware

- 802.1X device auth was tested with 1024-bit client certs on Windows FreeRADIUS 1.1.1 and 1.1.7.
- Due to legacy behavior the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.3 and iNET-II Release 3.0.3

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 7.3.2 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- TR-7812 detection – Log EVENT_REPROG_STARTED only when reprogramming starts successfully. Log extra info for EVENT_REPROG_FAILED to identify the type of failure.
- Include more detail in the build hop table debug logs to investigate the 'isolated AP wont associate' problem.

Defect Fixes in Firmware

- TR-11917 – Omit the magic number when verifying the boot image, it can be corrupted.
- TR-11914, 11820, 10187, 8551, 7542 – Retry disassociation on auto upgrade changes to force RM reconnect (merged from 7.2.4).
- TR-11688 – Web and SNMP interfaces check for existing processes before reprogramming, image copy, or reboot (match the behavior of the console, merged from 8.0.0).
- TR-11041 – Add missing parameter read settings and beacon status updates for RM reconnect when ethernet link watch or polling is disabled (merged from 7.2.4).
- Workaround UDP multipoint data stop by restarting COM2 after reassociating (merged from 7.2.7).
- Match the hop_format logic of the console when adding the channel config link to the navtree.

Known Errata and Limitations in Firmware

- Due to legacy behavior the COM2 RTS line is driven high even if the port is disabled.
- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.3.2 and iNET-II Release 3.0.2

This is an iNET and iNET-II release based on the 2.9.1 branch. It includes only the features of 3.0.1 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- TR-11848 – Add user control of SNMP accounts. Include Trap Manager #5 in the SNMP Trap Manager UIs, cfgscript, and SNMP.
- TR-11802 – DHCP client remotes will renew their DHCP lease on association.
- DHCP assigned lease time now appears on the console and web IP Address Configuration UIs.
- IP Address Config now includes a Renew option when IP Address Mode is Dynamic (eng. console).
- DHCP Server Config now includes DHCPD Lease and View Leases options (eng. console).
- Event log now includes the time it was generated in the header.

Changes/Additions to Existing Features in Firmware

- TR-11819 – Add connection state to the Channel Config UIs on iNET-II remotes when beacon learning is enabled or “on association”. Indicate which channels were scanned but not learned and which were learned but not scanned for “on association” mode.
- TR-7812 workaround – Use initctl to reboot if the call to /sbin/shutdown fails for auto-upgrade and user-commanded reboots.
- TR-4111 – Leading zeroes no longer cause octal values in IP address entries (merged from 7.2.4).
- DHCP Server UIs prevent server enable when DHCP client is active (merged from 7.2.6).

Defect Fixes in Firmware

- TR-11856/11857 – Add SNMP groups to enforce security requirements of SNMP accounts.
- TR-11854 – SNMP Agent Config web page now processes SNMP Mode and Trap Version correctly.
- TR-11749 – DHCP server status changes now use the process status rather than a status variable.
- TR-11735 – DHCP lease expiration will now reset the unit's IP address.
- TR-11334 – DHCP client code formats parameter for IP address conversion (merged from 7.2.5).
- TR-6591/10763 – Static IP param changes don't apply in Dynamic IP mode (merged from 7.2.4).
- Channel Config web page uses correct initialization of beacon learning on iNET remotes.
- Fixed issues reported by SilverCreek test suite
 - Correct get_fh_data_compress so that inetRcCompression.0 on remotes matches the MIB
 - sysContact.0, sysName.0, and sysLocation.0 are allowed to be empty strings

Known Errata and Limitations in Firmware

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET-II Release 3.0.1

This is an iNET-II release based on the 2.9.1 branch. It includes only the features of 3.0.0 and the listed changes. Specifically, it has no support for 3842 MAC hardware.

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Security update – Factory and engineering access is now disabled by default. Factory access may be authorized temporarily and will end when the unit reboots (merged from 2.9.6). Additionally:
 - factory & engineering passwords changed
 - factory reset clears engineering access
 - enabling factory access logs an alarm
 - eng off clears temporary & persistent access
- SNMP MIBs updated for SMIv2 compliance (merged from 2.9.6).
- SNMP fixed some issues reported by SilverCreek test suite (merged from 2.9.7).

Defect Fixes in Firmware

- TR-11833 – SNMP handles bad indexing of mdsRpgRetrievalTable as an error (merged from 2.9.7).
- TR-11803 – Update iNET MIBs to be SMIv2 compliant (merged from 2.9.6).
- TR-11703 – SNMP sysUpTime is now correct regardless of time of day (merged from 8.0.1).
- TR-11685 – Disable COM2 during boot then drive COM2 RTS high during kernel init. Enable COM2 flow control as soon as possible in serdata and drive RTS high when flow control is disabled (merged from 8.0.0).
- TR-10244 – Fix hang when setting ipRoute entry, added exit() on exec fail (merged from 2.9.2).
- TR-9633 – SNMP MIB walk is now working (merged from 2.9.7).

Known Errata and Limitations in Firmware

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET-II Release 3.0.0

This is an iNET-II release based on the 2.9.1 branch. It includes only the features of 2.9.1 and the listed changes for the Australia rail CRC.

Specifically, it has no support for 3842 MAC hardware and omits the security update of release 2.9.6, the SNMP fixes from release 2.9.7, and the COM2 RTS change from release 8.0.0.

New Features Present in Firmware

- Bridge Configuration added to Network Configuration UIs and cfgscript.
- Bridge Status added to Performance Information UIs.
- SNMP supports reading the scalar elements of BRIDGE-MIB dot1dBase and dot1dStp.
- Beacon Learning setting added to Radio Configuration UIs, cfgscript, & SNMP for iNET-II remotes. Changing learning to disabled allows user channel configuration. Changing learning to "on association" allows user channel configuration of scan channels then on association the hopping channels are learned.

Changes/Additions to Existing Features in Firmware

- Reduce the minimum bridge forwarding delay from 4 seconds to 1.
- RF Output Power limit for GSM hop format increased from +24dBm to +30dBm.

Defect Fixes in Firmware

- TR7264 – Web interface now correctly displays channels for iNET-II.

Known Errata and Limitations in Firmware

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.2

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR-11732 – Restore existing DHCP settings if client is enabled when max beacon wait occurs.

Known Errata and Limitations in Firmware

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.1

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Revert wlan MAC buffer handling to 2.9.8 baseline to try to reduce max beacon wait timeouts.
- Reset MAC when max beacon wait timeout occurs to reduce reassociation time.
- Programming the inactive AP image with auto-upgrade and 802.1X device auth enabled waits for programming complete to disassociate the RMs.
- Redundancy Config console menu changed to standard selection method for redundancy enable.
- Redundancy Config web page layout changed to fit items without wrapping.
- Web page navtree now always links to Redundancy Config pages rather than conditionally alert.
- Add confirmation prompt to Event Log console menu Clear Log, matching the behavior of the web.
- Add Send Event Log settings to Event Log web page, matching the behavior of the serial console.
- Add Log Extra Assoc setting to WLAN Debug engineering menu for runtime control of debug info.
- Add letter keys for navigation of the Approved devices, Remote, Endpoint, Remote Perf, and SDB Debug lists: (U)p, (D)own, (P)g-Up, Pg-D(n), (H)ome, (E)nd. Change Approved devices and SDB Debug lists prompt to view_list_msg.

Defect Fixes in Firmware

- TR-11703 – SNMP sysUpTime is now correct regardless of time of day (merged from Mercury-e).
- Radio Config console menu prevents selecting FPGA Workaround Logging if the workaround is off.
- Stop showing 'RootFS 93%' during image copy when the region changes from kernel to rootfs.

Known Errata and Limitations in Firmware

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET and iNET-II Release 8.0.0

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Version numbers for iNET and iNET-II products are synchronized with this release. 8.0.0 is the first iNET release after 7.2.9 and the first iNET-II release after 2.9.9.
- Reduce the minimum bridge forwarding delay from 4 seconds to 1.
- Authcode logins support engineering password enable authorization, there is no user feedback.
- Update RSSI By Zone and VLAN Packet Stats menu accessibility. Change Performance Information submenu prompts to new prev_menu_msg or view_list_msg.

Defect Fixes in Firmware

- TR-11688 – Web and SNMP interfaces check for existing processes before starting reprogramming, image copy, or reboot (match the behavior of the serial console).
- TR-11685 – Disable COM2 during u-boot then during kernel init drive COM2 RTS high. Enable COM2 flow control as soon as possible in serdata and drive RTS high when flow control is disabled.
- Authcode logins show 'Setting factory defaults' only when password reset authorization is present.

Known Errata and Limitations in Firmware

- iNET-II releases > 2.0.0 are not compatible with previous releases. All remotes must be rebooted to any new version prior to upgrading the AP.
- Reprogramming a unit at any time may leave it unable to run new programs. For example, new web pages, telnet sessions, or reboot requests may fail.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.9 and iNET-II Release 2.9.9

New Features Present in Firmware

- Beacon Learning mode "On Association" added for iNET-II remotes. This mode allows user channel configuration of scan channels then on association the hopping channels are learned.

Changes/Additions to Existing Features in Firmware

- Upgraded wlan driver's MAC buffer handling per manufacturer recommendation (serialize access).

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- Starting to reprogram a unit within 45 seconds of the login prompt appearing at the local console may cause the unit to fail and either become unresponsive or fail to soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.8 and iNET-II Release 2.9.8

New Features Present in Firmware

- Bridge Configuration added to Network Configuration UIs and cfgscript.
- Bridge Status added to Performance Information UIs.
- SNMP supports reading the scalar elements of BRIDGE-MIB dot1dBase and dot1dStp.
- Beacon Learning setting added to Radio Configuration UIs, cfgscript, & SNMP for iNET-II remotes. Changing learning to disabled allows user channel configuration.
- Enumeration menu items can select the previous value by using the backspace key.

Changes/Additions to Existing Features in Firmware

- RF Output Power limit for GSM hop format increased from +24dBm to +30dBm.
- Returned max time in scanning/wait for beacon state from 6 minutes to 1 minute.
- Ethernet Port, Network, and Radio Config web page layouts changed to fit items without wrapping.
- Performance Information web page for APs shows Actual Data Rate, matching the menu.
- Radio Config menu only shows selection letter for accessible items, matching the web page.
- Log the cramfs_inflate return msg when the kernel fails a page load ("error while decompressing").
- Engineering menu layout and submenu prompts changed to match standard layout and behavior.

Defect Fixes in Firmware

- TR11541 - Add console baud to the Device Information web page.
- Workaround remotes reporting false association by monitoring data connectivity at the AP.
- Enable backspace and control keys when entering the factory or shell command line.

Known Errata and Limitations in Firmware

- Starting to reprogram a unit within 45 seconds of the login prompt appearing at the local console may cause the unit to fail and either become unresponsive or fail to soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.7 and iNET-II Release 2.9.7

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- SNMP MIBs updated to fix some issues reported by SilverCreek test suite.
- Add letter keys for navigation of the event log: (U)p, (D)own, (P)g-Up, Pg-D(n), (H)ome, (E)nd.
- Getparm command added to factory command line.
- Consolidate the multiple definitions of param_names and param_types to reduce image size.

Defect Fixes in Firmware

- TR9633 – SNMP MIB walk is now working.
- Workaround UDP multipoint data stop by restarting COM2 after reassociating.

Known Errata and Limitations in Firmware

- Starting to reprogram a unit within 45 seconds of the login prompt appearing at the local console may cause the unit to fail and either become unresponsive or fail to soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.6 and iNET-II Release 2.9.6

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Security update – Factory and engineering access is now disabled by default. Factory access may be authorized temporarily and will end when the unit reboots. Additionally:
 - factory & engineering passwords changed
 - factory reset clears engineering access
 - enabling factory access logs an alarm
 - eng off clears temporary & persistent access
- SNMP MIBs updated for SMIv2 compliance; fixed some issues reported by SilverCreek test suite.
- Trying to enable DHCP server with DHCP client enabled displays an error message.
- The Prioritized AP Configuration web page now includes a link to the Approved Access Points list.

Defect Fixes in Firmware

- TR11389 – Web interface now allows adding prioritized APs.
- TR7264 – Web interface now correctly displays channels for iNET-II.

Known Errata and Limitations in Firmware

- Starting to reprogram a unit within 45 seconds of the login prompt appearing at the local console may cause the unit to fail and either become unresponsive or fail to soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.5 and iNET-II Release 2.9.5

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR11334 – DHCP client code now uses correct parameter format for IP address conversion.

Known Errata and Limitations in Firmware

- Starting to reprogram a unit within 45 seconds of the login prompt appearing at the local console may cause the unit to fail and either become unresponsive or fail to soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.4 and iNET-II Release 2.9.4

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- TR10731 – The no remotes workaround FPGA reset and its logging behavior are now under parameter control in the Radio Configuration console menu for factory logins and above.

Defect Fixes in Firmware

- TR11132 – Upgraded wlan drivers to check the MAC device variant when disabling the MAC port, preventing console and network management interfaces becoming unresponsive.
- TR11119 – Avoid PLL unlock in test mode by setting the controls cleared during synth setup.
- TR11041 – Add missing parameter read settings and beacon status updates for RM reconnect when ethernet link watch or polling is disabled.
- TR10763, 6591 – Static IP parameters no longer change the configuration in Dynamic IP mode.
- TR10187, 8551, 7542 – Retry disassociation on auto upgrade changes to force RM reconnect.
- TR07055 – Number the entries in the web event log view so it matches the console view.
- TR04111 – IP address entries with leading zeroes are no longer interpreted as octal addresses.

Known Errata and Limitations in Firmware

- Starting to reprogram a unit within 45 seconds of the login prompt appearing at the local console may cause the unit to fail and either become unresponsive or fail to soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- A lack of free memory can cause lockups, crashes, failure to run programs, or watchdog reboots. This can occur when the dentry_cache is not properly cleaned up under low memory conditions.

iNET Release 7.2.3 and iNET-II Release 2.9.3

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Revert change to mocana_ssuite code in CERT_VerifyCertificatePolicies() to not require the keyUsage certificate extension to be present, to preserve existing functionality in iNET/iNET-II/Mercury-D.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.2.2 and iNET-II Release 2.9.2

New Features Present in Firmware

- Support for both the 3842 and 3841 MAC hardware.
- Ability to build initsyslog app and send log messages to the configured syslog server.

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR4693 – Fix network connectivity loss on SNMP set of the ifAdmin state of an interface.
- Serial wizard flow control detail screen reflects the value set rather than always disabled.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.2.1 and iNET-II Release 2.9.1

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR#10682 – Factory reset changes hop format to CHANNELS

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.8 and iNET-II Release 2.8.8

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- **Over-the-air compatibility break:** iNET300s now calculate and transmit the channel count differently than previous releases. Units running previous builds will not communicate with units running release 7.1.8 and above.
- Changed handling of channel entry for AUS and BRAZIL (for iNET-II) to force the disallowed channel bits, so that the channel count will reflect the displayed channels.
- Calls to kill dhcpd now accept result ESRCH (no process found) without returning an error.

Defect Fixes in Firmware

- TR#10612 – “CHANNELS” value for hop format missing in cfgscript
- TR#9681 – COM port 1 may be configured for MODBUS via cfgscript

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.7 and iNET-II Release 2.8.7

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Changed Test menu to send TEST_MENU message to airctl to prevent it from resetting the FPGA on an AP while you are in the test menu.
- Changed the Redundancy menu to display and allow factory level access to use the engineering event test.

Defect Fixes in Firmware

- TR#10600 – Changed menu to no longer restrict the display of the hop format to Hop Protocol 0 or 1.
- TR#10601 – Removed the logic checking for hopProtocol 0 or 1 that caused the switch statement to not be handled, and fall into the next case without a break statement.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.6 and iNET-II Release 2.8.6

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Removed JOB_FLAGS from wlan target, since it isn't parallel build safe. The objects are compiled differently to make up the AP and RM versions.

Defect Fixes in Firmware

- TR#8590 - In web/cgi-bin/security.c changeList retrieve p_system_mode outside the pdata check, so that we know the device mode before using it.
- TR#10540 - Changed process_new_watch_link to get p_watch_link, p_poll_address, and p_poll_address2 to determine the watch_link status, instead of forcing the bit on/off based on any of the single parameter changes.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.5 and iNET-II Release 2.8.5

New Features Present in Firmware

- Each instance of EVENT_REBOOT uses an extra info string to identify the process triggering the event.

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR-10242 – Fix lack of remotes failover when the setting is greater than 60 seconds.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.4 and iNET-II Release 2.8.4

New Features Present in Firmware

- CRC-0102 - Added initial support to iNET 300 for Indonesia hop format.

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Changed hop format select_option handling to correct inability to choose iNET 300 specific hop formats. Error was introduced in changes that added back Australia and Brazil hop_format support to iNET-II.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.3 and iNET-II Release 2.8.3

New Features Present in Firmware

- Added a second Ethernet Link Poll Address, and a poll logic parameter, to allow a user to decide how the results of polling the two hosts will be used when determining if the Ethernet link should be reported as up or down. The user can choose between the OR and AND operations. If a poll address is 0.0.0.0, it is treated as un-configured, and the logic does not apply.

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.2 and iNET-II Release 2.8.2

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Added call to `set_tty0_status(SER_ESC)` if the unit is configured to try and run MODBUS TCP Server on COM1, which it not available, to prevent the console from locking up.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the `/tmp` directory, will cause the `dentry_cache` to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.1.1 and iNET-II Release 2.8.1

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Re-added Hop Format parameter handling support in iNET-II in order to force the limitation of the available channels a user can select for in Australia (GSM) and Brazil (SPLIT). Modified UI's to display unavailable channels as NA. Fixed SNMP's ability to write values to the Channel table. This fix is also applicable to iNET if the Hop Format parameter is set to Channels.

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.0.6 and iNET-II Release 2.7.6

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR#9564 - Changed serInfo times to be based on uptime to prevent changes in clock time from causing things to expire, timeout prematurely, or be incorrectly displayed in the UIs. Added or modified some of the debug statements to aide in debugging. Added flushing of messages in the serdata msg queue while we are still initializing. These changes are to address how the serdata initialization sequence occurs. The old code would handle the COMMIT messages from airtcl and dhcpcd, then handle the forces re(start) message. This thrashing of the threads could cause sockets and/or file descriptors to not be correct once the initialization was finally, supposedly, complete.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.0.5 and iNET-II Release 2.7.5

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR#9354, 9481, and 9502 - Changed initialization sequence to not hold off the menu process when COM1 is not in data mode. This fixed the varying lengths of delay including the infinite delay in the case of booting with DHCP enabled but no access to a server.
- TR#9479 - Changed to use p_actual_ip_* parameters instead of p_ip_* parameters. This prevents the constant exit and restart loop, due to not being able to bind to the interface with the correct ip address.
- TR#9498 - Fixed blanking of text in wireless security menu when changing device auth mode.
- TR#9499 - Added support for the Mobility Enable parameter in cfgscript.
- TR#9518 - Changed tmpfs limit to 1536K to make sure to have room for the creation of a full event log when the debugging logs and other files are all at full size.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.0.4 and iNET-II Release 2.7.4

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- TR#9353 - Added explicit calls to `set_tt0_status(SER_ESC)` to inform menu that serdata is not running a serial service on the COM1 serial port when the PPP and DF1 are set as the mode. Also added explicit call to `set_console_baud` before handling PPP or DF1 mode on COM1 in case serdata does not need to enable serial port as a serial service.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the `dentry_cache` to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.0.3 and iNET-II Release 2.7.3

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Removed EVENT_ACTIVE_IMAGE_MISMATCH and corresponding trap info, since the bootloader reads the active_image from the param region and will still boot to image 2 even if the bootloader config is empty.
- Set the tty0_status to SER_ESC to let menu start up and present the login prompt on the serial port, since we are just going to sit in the loop until someone logs in and inputs proper authorization for any of the serdata features.
- Fixed issue with trying to boot to Image2 while the Image1 kernel is missing or corrupt. Added warning messages if the number of detected kernel images != the number expected, if no valid kernel images were found, and if we are supposed to boot the Image2 kernel, but only one is found. This kernel may or may not be a valid kernel to be used with the RootFS. If it is, then everything is ok. If it is not, the unit may still fail to boot, or behave in an unpredictable manner.
- Clear the hostname value. It is not needed, and if it is set to certain more than one word, separated by spaces, and the last word starts with the number 0 or 6 (i.e. WELL 6), it can cause the init process to get all of the words, except the first word, as arguments. Since the first character of the last word (argument) starts with 0 or 6, the init process tries to shut down the unit. The inith_shutdown function sits in a do..while loop trying to open the /dev/fpga character driver, but since the system is just starting, it has not been loaded, and therefore cannot be opened. This prevents the do..while loop from exiting and causing the following message:
"modprobe: modprobe: Can't open dependencies file /lib/modules/2.4.4/modules.dep (No such file or directory)"
to be displayed over and over. The unit will not recover, without breaking into the bootloader to change or clear the hostname environment variable.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.0.2 and iNET-II Release 2.7.2

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Case# 28356 - Change startup interaction between menu and serdata to restore console login on COM1 when data mode is not enabled.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 7.0.1 and iNET-II Release 2.7.1

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Added support to log FPGA Reset as an event.

Defect Fixes in Firmware

- Case# 28356 - Change startup interaction between menu and serdata. Fixed menu to only force setting of baudrate if it is running on the local serial console. Fix file descriptor leak in serial escape detection. Fixed notification messages on serial port when entering or leaving serial data mode.
- Changed handling of changes to p_console_baud to prevent it from changing the com1 baud rate while in data mode and properly set it when data mode is escaped or disabled.

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.8 and iNET-II Release 2.6.7

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- The 8ms dwell time is no longer supported in iNET-II. Added force upgrade of dwell time to 16ms if the current value is 8ms.
- Only allow dwell time values of 16ms – 131ms for iNET-II.
- Changed build system to optimize Df1, IPTables, and PPPd for size.

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- If you start a reprogramming process within 45 seconds of the login prompt appearing on the local console, the unit may fail and either become unresponsive or fail to perform a soft-reboot.
- Initial remote console connections made during an active reprogram session may also cause the unit to fail and either become unresponsive or fail to perform a soft-reboot.
- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.7 and iNET-II Release 2.6.6

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Added check of bootloader environment to determine if the application thinks it is in image 2 when the bootloader used its defaults and booted image 1. Includes new event for Active Image Mismatch.
- Changes to makefiles and build scripts to try and free up space to be able to make iNET builds that will actually fit in flash and try to run without errors accessing the cramfs filesystem.

Defect Fixes in Firmware

- Replaced separate syncbenv calls with synchronous function calls to update the bootloader environment with param changes, to prevent collision of reboot process and flash access to update bootloader environment from preventing the unit from rebooting.

Known Errata and Limitations in Firmware

- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.6 and iNET-II Release 2.6.5

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Changes bootloader, kernel, and user-space apps to support running project flashmap on flash hardware of a different size.

Defect Fixes in Firmware

- Added fix to AP bottom-half handler from iNET-II 2.6.a to permit the driver to service the RX queue even when it becomes full.

Known Errata and Limitations in Firmware

- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.5 and iNET-II Release 2.6.4

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Removed setting of the chinese bit in the FPGA, since the FPGA no longer needs to do spectral inversion for iNET 300. This allows new iNET 300 HW to associate properly.
- Fixed the creation of short hop tables to perform the right number of iterations to fill the array. This prevents the FPGA from trying to go to an empty record and fail to lock the PLL. On a single channel, this will break or prevent association.
- Updated the Chinese Channel Menu to properly reflect active changes to the channel list and display the commit message when it detects a change. It also does not ask you if you want to discard the changes when trying to leave the menu if you have already committed the changes.
- Changed the SNMP agent to update the engineID in the UsmUserTable and update the hashes when re-initializing the agent do to a change of IP address, to fix SNMP v3 access.
- Changed tfSetNewKeys to properly handle the setting of snmpNewPrivateKeyHashSha1 to allow sha1 auth with des priv to work properly.

Known Errata and Limitations in Firmware

- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.4 and iNET-II Release 2.6.3

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- None

Defect Fixes in Firmware

- Added explicit setting of the Ethernet MAC Address and the console baud rate from user-space code, instead of relying on the bootloader/kernel to have it setup to match the parameter configuration, since the bootloader no longer reads our parameter region.

Known Errata and Limitations in Firmware

- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.3 and iNET-II Release 2.6.2

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Changed from using RAMFS to TMPFS for the /tmp directory. Also added 512KB limit to the /tmp mount.
- Changed /proc/slabinfo monitoring to only look at file descriptors and generic memory slabs to see if there is a leak, instead of any entry.
- Changed /proc/slabinfo monitoring to try to reboot by directly writing to /dev/initctl. If that fails, it uses system to write to /dev/initctl. This replaces a system call to reboot which may fail if the system is close to locking up due to a memory leak.
- Re-enabled the proj_config version of the bootloader, so that it can read the active_image parameter itself, since the old app code doesn't know how to do a syncbenv.

Defect Fixes in Firmware

- TR#7778 - Send SERDATA_RESTART_MSG instead of SERDATA_COMMIT_MSG when the network config has been changed to make sure it is using the correct values.
- TR#7779 - Corrected link so that you go to the right page after forcing a key rotation.
- TR#7957 - Changed param_table.h to default the channels in iNET to all 0, and all odd in iNET-II to maintain compatibility with old revisions of iNET firmware.
- Changed certmgr to not try and create the 802.1x device authentication certificate files on the filesystem, if the length is not greater than 0.

Known Errata and Limitations in Firmware

- Temporary file creation in the /tmp directory, will cause the dentry_cache to grow, and its old memory may not be properly made available when memory is getting low, resulting in a lack of free memory and causing lockups, crashes, failure to run programs (such as reboot), or watchdog reboots.

iNET Release 6.9.2 and iNET-II Release 2.6.1

New Features Present in Firmware

- iNET is now using U-Boot instead of ppcboot as its bootloader.
- U-Boot has been modified for both iNET and iNET-II to no longer directly get project configuration variables from the PARAM regions of flash. The applications layer now stores of param changes that the bootloader needs to know about in the bootloader configuration region.
- U-Boot has been modified for both iNET and iNET-II to add the use of the CFI driver to detect flash, as well as other changes to allow it to determine at runtime, where the bootloader configuration is.

Changes/Additions to Existing Features in Firmware

- Merged the iNET and the iNET-II codebases to allow the building and maintenance of all iNET firmware variants from the same codebase. This includes variations in product, frequency, and OEM options.

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- None

iNET-II Release 2.5.1

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Changed FPGA image to be 0.2B.1 with synthesizer support.

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- None

iNET Release 6.9.1

New Features Present in Firmware

- None

Changes/Additions to Existing Features in Firmware

- Added 0.AB.1 FPGA that allows aborting beacon in the middle if MAC abandons TX and requires 3 beacons with updated TSF counts in a row before abandoning old timing.
- Added support for converting FPGA DEBUG_INFO interrupts into syslog messages, if the interrupt is manually enabled in the FPGA using the fpga command.
- Removed runtime debug messages in tcpmodbusd.c that were filling the dbglog at runtime making it hard to debug a system in the field.

Defect Fixes in Firmware

- None

Known Errata and Limitations in Firmware

- None