6330-MX / 6335-MX LTE Router Changelog

18.10.225.15 - November 28, 2018

- IPSec IKEv2 support
- GRE tunneling support with keepalives
- Added configuration options for domain-based routing
  - set as a Destination option in Policy-based routes
- DRM support on all ACL products
- Change 6310-DX to passthrough mode by default (WAN port still enabled)
- Updated DHCP tftpserver option to accept http URL
- Fixed bug where OpenVPN connection information wasn't being cleared when OpenVPN restarts
- Updated the Status page of the local web UI to display WiFi channel and frequency information
- Added configuration option to select the country for WiFi (controls Tx Power and Channel requirements)
- Added configuration options to control IPSec SA lifetime and IKE lifetime settings
- Added configuration options to use x509 or RSA authentication methods for IPSec tunnels
- Added configuration option to the aView tunnel for it to use as an x.509 authentication the same signed SSL certificate used by the device to get its configuration settings from aView (disabled by default)
- Fixed bug where users had to lock the APN for a 1002-CM04 to connect with a Verizon SIM

18.8.14.124 - October 10, 2018

- Full support for the IX14 model
- Full support for the ConnectIT4 model
- Support for all Telit LE910 modem variants

- Added CaptivePortal feature, which can be configured and applied to both wired and wireless interfaces
- Added support in device configuration for setting up exernal USB-to-serial adapters and accessing them via the console login prompt
- Added option in device configuration to enable/disable roaming on a cellular modem interface
- Added new options for **Scheduled tasks → custom scripts** to control memory limit, log output, singlethreaded versus multi-threaded execution, and follow-up action(s) once the custom script finishes
- Added new option for **Network → Modems → Modem** entries to limit the maximum number of interfaces that can be associated to a particular modem
- Added crmstatic.bell.ca.ioe to APN fallback list for Bell Canada SIMs
- Added 12655.mcs to APN fallback list for AT&T SIMs
- Added orange.m2m.spec and orange.m2m to APN fallback list for Orange (France) SIMs
- Added Telemach carrier (Slovenia), Telia carrier (Finland), data.dna.fi (Finland) and julkinen.dna.fi (Finland) APNs to APN fallback list
- Added button on System page of web UI to reboot the device
- Added new WiFi scanning and setup tool on System page of the local web UI
- Updated local web UI to only show the Dashboard page if Intelliflow is enabled
- Enhanced load speed of WebUI's status page by loading each page tab as a new page
- Added **ipsec** option to Admin CLI to show debug info of device's IPSec tunnels
- Added **runtdump** and **runtget** options to the modem utility in the shell console
- Added sftp tool
- Added requirement for user to provide login credentials when accessing the 3-pin serial console of the device
- Enhanced serial login mode so sessions do not close/open on every reload
- Track and display the RSRP, RSRQ, and band for Telit LE910 modems
- Use RSRP and RSRQ of Telit modems for calculating signal strength, same as Sierra modems

- Updated default QoS settings to use the correct TOS headers to prioritize SIP/VoIP traffic
- Enhanced OpenVPN status in WebUI's tunnel page to include the state of 'connected'
- Improved reliability of carrier SIM/firmware matching by referencing PLMN first, then ICCID if no matching PLMN is found
- Added system log when someone presses the SIM select button
- Enhanced system log to show HTTP error code when aView certificate cannot be obtained
- Updated AT&T SSL certificate chain
- Updated service for handling remote commands to only accept POST HTTP requests, and deny GET requests
- Prevent HTTP Header Injection by allowing only alphanumeric characters in the username entered into the web UI
- Prevent HTTPS Cross Site Request Forgery (CSRF) by not accepting auth token in the cookie of POST requests
- Fixed vulnerability to WebUI clickjacking
- Fixed bug with carrier SIM/firmware matching when ICCID or MNC weren't the typical number of characters
- Fixed bug where signal strength LEDs were not displayed on 54xx-RM devices
  - bug present in firmware versions 18.4.x.x
- Fixed bug where Intelliflow would reset if network interfaces were enabled or disabled, or if the order of those interfaces changed
- Fixed issue where WiFi AP would be setup first, choosing a channel, before the client connection, which would prevent it from scanning to find the desired SSID on the proper channel.
- Fixed bug where IMEI would not be displayed if a SIM wasn't present
- Fixed bug with obtaining internal temperature of Sierra-based modems
- Fixed bug where serial port could not be used if a user pressed Ctrl+d at the login prompt (restarting the seriald process or rebooting the device would temporarily fix this)
- Fixed bug where OpenVPN clients couldn't access other networks on the device running the OpenVPN server
- Fixed bug preventing users from remotely changing configuration settings through a SSH command
- Fixed bug with multicast support in OpenVPN
- Fixed bug where user could be required to enter in credentials twice to login to the local web UI

- Fixed bug where HTML/Javascript code could be executed from a SSH login without authenticating
- Fixed bug where management priority value would not be reset correctly after switching from WAN primary to backup, or vice-versa
- Fixed bug where tab completion in CLI would cause segmentation fault
- Fixed bug where large-sized packets would be lost when sent through an IPSec tunnel built over a WAN connection with a MTU lower than 1500 (e.g. cellular)
- Fixed bug where a policy-based router entry with a destination of "Zone Any" directed out an interface without a default route result in the firewall DROPping the packets
- Fixed bug with reconnecting Telit modem after device was power cycled.
- Fixed firmware downgrade functionality. Future firmware versions after 18.8.14.0 will be able to downgrade to 18.4.54.41 or newer
- Fixed bug with performing WebUI OTA updates for Telit LE910-NA V2 modems (previously, only manual firmware upload and aView remote commands worked)
- Fixed slowdown of initial connectivity with Optus SIMs
- Removed reporting of MSL code on the Modem page of the WebUI (Sprint only)
- Reduced TCP fragment limits for security vulnerability
- Linux kernel update from 4.15 to 4.17
- openssl update with 1.0.2o patch
- stunnel update from 5.37 to 5.46

18.4.54.41 - July 5, 2018

- Fixed bug where resetting management priority option back to 0 would not set correctly unless the device was rebooted.
  - Bug present in firmware versions 16.10.32-18.4.54.28
- Fixed bug where ICCID values starting with 890 would have the zero not displayed in the web UI or Accelerated View
  - Bug present in firmware versions 18.4.54-18.4.54.28
- Fixed bug preventing devices from being configured to connect to Verizon-only SIMs
  - Bug present in firmware versions 18.4.54-18.4.54.28

- Fixed bug preventing SIM failover if no modem interfaces matched the SIM present in the active SIM slot, or if no SIM was detected in the active SIM slot.
  - Bug present in firmware versions 18.4.54-18.4.54.28
- Fix bug preventing Carrier Smart Select from functioning properly on cat3 and cat6 Sierra MC73xx/MC74xx modems.
  - Bug present in firmware versions 18.4.54-18.4.54.28
- Shorten the time between when a device establishes its tunnel to ispec.accns.com and when it logs its management IP address to aView.
  - Previously, this could take up to 5 minutes. Now, it should happen within seconds.
- Cleaned up the **Configuration** page of the local web UI to show the appropriate default settings when central management is enabled.
  - Bug present in firmware versions 18.4.54-18.4.54.28
- Fixed bug where IPSec packets could be corrupted when sent through a Sierra modem.
  - Bug present in firmware versions 18.4.54-18.4.54.22

18.4.54.28 - June 25, 2018

- Fixed bug where firmware cannot be correctly downgraded from aView (bug present in firmware versions 17.10.74 to 18.4.54.22)
- Fixed bug with mangling IPSec tunnel traffic on firmware 18.4.54 with Sierra modems
- Fixed inbound modem passthrough filtering
- Fixed bug preventing modem interfaces from establishing an IPv4-only or IPv6-only connection
- Fixed bug where tab complete causes segmentation fault in empty arrays in CLI interface

18.4.54.22 - May 25, 2018

- Fixed bug with LE910v2 LTE registration on AT&T
- Fixed bug where IPSec's source address assignment was often incorrect

- Added Quality Of Service (QOS)
- Major modem support update
  - Dual PDN/APN
  - Support for multiple modems
  - Complex modem/SIM/APN mappings
- Added configuration option to manually set SIM phone number
- Added *11904.mcs* and *wbb.attbusines.net* to the AT&T APN list
- Added NAT keep alive configuration for IPSec tunnels
- Added Telit modem firmware update support on devices
- Added basic multi-interface support for PCAP based DAQ intrusion detection in SNORT
- Added links to **System** page of web UI for downloading OpenVPN (.ovpn) configuration files
- Added ability to toggle SIM slot based on remote command received from aView
- Fixed bug to allow IPv6 passthrough and DHCPv6 server to run on a device
- Fixed rare bug where duplicate static IP addresses would cause DHCP server crash
- Fixed rare bug where pressing the enter key for a text entry on the Configuration page of the web UI would inherently save the configuration instead of performing the "Add" action.
- Fixed rare bug where cellular modem service would crash if no SIM was detected
- Fixed bug with setting a custom gateway for static bearers
- Improved system resources by stop reloading configurations in system pages of the web UI
- Improved network interface/device status format on the Dashboard page of the web UI
- Improved web UI Device Details page to auto-refresh values
- Improved OpenVPN server configuration to allow specific designation of IP
- Implemented "Server managed certificate" modes in OpenVPN
- Redesigned network interface and modem configurations in WebUI
- Updated IntelliFlow copyright information
- **Network > Advanced** section is added from a WebUI restructuring
- Linux Kernel update: from 4.14 to 4.15
- Fixed bug where OpenVPN tunnel names would clash for servers and clients due to the use of the same "o_" prefix

- Fixed bug with incorrectly matching MAC addresses 6330-MX bootenv variables
- Fixed bug where temperature milliCelsius was incorrectly converted to Celsius
- Improved SIM ICCID accuracy by revised search logic
- Fixed bug where MNC and ICCID does not match correctly
- Fixed bug where 540X signal strength was not displayed on LEDs

18.1.29.41 - March 16, 2018

- Add ability to customize skin and logo of the local web UI
- Added ability to sync with AT&T-owned instances of Accelerated View by default
- Added wbb.attbusiness.net APN to the list of fallback APNs for AT&T/Vodafone SIMs
- Updated OpenVPN to support operating as a fully fledged netifd client
- Fixed bug where devices in passthrough mode would not send their primary IP address to Accelerated View

18.1.29.10 - February 1, 2018

- Improved system resource by only setting up the Intelliflow process if a collector is configured.
- Improves upon the 18.1.29 firmware implementation
- Improved caching on the **Configuration** page of the local web UI
- Auto-refresh details displayed on the **Status** page of the local web UI
- Improved support report to include ARP-related information
- Updated company logo on local web UI
- Added new **System → Log → Event categories → Active recovery** configuration option to allow enabling/disabling of success or error logs resulting from Active recovery tests
- Fixed bug preventing users from saving a configuration on a device's local web UI if the config settings included a single-quote to (i.e. ').
- Bug present on firmware version 18.1.29
- Fixed bug where IPv6 forwarding packets could get mistakenly dropped by the firewall

18.1.29 - January 26, 2018

- SNMP agent support
- New Intelliflow tool for displaying the Accelerated device's system resources, and the data/port usage of connected local clients.
- Support for 5-tuple Policy-based routing
- Support for OpenVPN inbound and outbound tunnels (client/server)
- Multicast routing support
- Added option to set a IPv4 and/or IPv6 MTU on each network interface
- Added Group rekey interval option to set a group rekey interval on each SSID (default 10 minutes)
- Improved isolated IPSec tunnel setup and management. Changing settings on one tunnel won't cause all tunnels to reestablish
- Enhanced user authentication settings to allow stacked authentication methods.
- Reduced the frequency of logging the last modem disconnect reason
- Improved DNS entry cleanup to prevent duplicate and non-applicable entries
- Increased font size of navigation links on the local web UI
- Added ARMT and AVWOB servers to list of default central configuration domains
- Enabled localhost DNS rebinding by default
- Added new log to report system/CPU info to Accelerated View
- Fixed bug where device would not always log that its central config was disabled
- Fixed broken routing after unplug/repluging passthrough device
- Fixed bug preventing devices in passthrough mode from using the 192.168.210.254 default gateway in the absence of another WAN connection
- Fixed bug when setting up static IPv6 passthrough routes
- Improved system resources by only starting DynDNS service when enabled
- Fixed WAN failover consistenct when the primary link bounces quickly (less than 5 seconds)
- Fixed bug where different status events inherited the same counter value (i.e. cnt=)

- Fixed bug when setting a specific SIM slot in **Modem → Active SIM** slot where switching to the SIM slot would fail if both SIM slots weren't occupied
- Fixed bug preventing devices from operating in passthrough mode if the cellular connection didn't provide any DNS servers
- Upgrade to Linux kernel 4.14
- Upgrade libcyrussasl to version 2.1.26
- Upgrade libldap to version 2.4.45
- Update pam_ldap to version 185
- Improved user authentication with tokenized password validation
- Update curl to version 7.56.1
- Removed auto-refreshing of some values on the Status page of the local web UI
- Changed default WiFi SSID from Accelerated <device> (e.g. Accelerated 6350-SR) to Accelerated
- Fixed LAN/WAN LED behavior so the LAN LED gets activated by LAN traffic

17.8.128.64 - December 7, 2017

- Fixed bug preventing cat4 devices from setting a custom APN.

17.8.128.63 - November 9, 2017

- Fixed bug preventing devices in passthrough mode from building their AView IPSec tunnel.
- Improved process for uploading custom modem firmware with large file sizes.
- Fixed bug preventing **atcmd** option in the Admin CLI from selecting the correct command port.
- Fixed bug affecting devices with certain LTE cat6 modems (EU version) where the modem would not connect after initial setup.
- Fixed bug where LAN traffic would display activity on the device's WAN LED.

17.8.128.37 - October 27, 2017

- Fixed bug where Carrier Smart Select did not function with cat4 Telit modems. Issue only present in 17.8.128.24 firmware.
- Fixed bug where devices with new Verizon SIMs would register, but not connect without retrying the APN multiple times. Issue observed on firmware versions 17.5.108.6 through 17.8.128.24
  - Resolves the following knowledgebase article: https://kb.accelerated.com/m/67105/l/785640-verizon-sim-with-static-apn-registers-but-doesn-t-connect
- Security patches for KRACK WiFi vunlerability.
- Update dnsmasq to version 2.78

17.8.128.24 - October 11, 2017

Features

- Added new login page to local web UI.
- Added ability to trigger modem firmware OTA updates from Accelerated View.
- Added new configuration options for performing system maintenance tasks.
- Added new configuration options for performing scheduled custom scripts.
- Added new remote **support** command.

Enhancements

- Added a DHCP option for PXE booting.
- Added a banner at the top of the **Configuration** page of the web UI to denote if central management is enabled.
- Added cellular modem connection retry backoff in order to be more sensitive of connection/registration timing.
- Added option to select IPv4, IPv6, or both addresses for a modem (including passthrough mode).
- Store and report the modem SiNR value in the system logs and to Accelerated View.
- Added default APNs for Sprint SIM cards.
- Improved responsiveness of the web UI.

- Added ability to send SMS messages through the shell console.
- Reduced CPU/memory usage while idle.
- Added bolding in Admin CLI to highlight help text.
- Added DHCP server options
- Added the **Network** → **Interfaces** → **WAN** section to the limited set of configuration options presented on the local web UI when central management is enabled.
- Include in the system logs and in Accelerated View a count of SIM switched, if any, the device has performed since startup.
- IPSec improvements to better guarantee the device's tunnels are established properly.
- Update **Carrier Smart Select** to use Generic firmware if the carrier-specific firmware is not found.

Bug Fixes

- Fixed bug where Rogers SIMs could only establish a 3G connection.
- Fixed issue where modem firmwares could be corrupted over time.
- Fixed bug where certain devices could not be access through the Accelerated View tunnel.
- Improved IPSec setup so users don't have to add the remote networks to both the **Policy** and **NAT** sections of the config.
- Improved IPSec setup to allow multiple policies.
- Fixed rare issue where modem firmware updates would get stuck and only partially update.
- Improved handling of WAN DHCP servers when they don't provide a netmask.
- Fixed bug preventing **Carrier Smart Select** tool from selecting the correct firmware on MC7304 modems when using Vodafone SIMs.
- Improved monitoring of LAN port statuses.
- Fixed bug where DNS servers for a backup WAN were mistakenly associated with the primary WAN.
- Fixed timing error in creating IPsec logs, which was causing setup errors.
- Fixed rare bug when determining the correct default route after failing over between multiple WAN interfaces.
- Fixed rare bug wheredevices building site-to-site IPSec tunnels would get stuck connecting due to a routing change on the main site device.
- Fixed bug where device would stop routing properly if it failed over between multiple WAN interfaces a large number of times (50+).

Security Updates

- Upgrade to Linux kernel 4.11.12
- Update to Strongswan 5.5.3