90000

JunglePAX – Release Notes

Firmware Package p/n   90000-01

Version: 1.16c

Release Date: June 4th, 2020

Type of Release: Production Release

Lentronics JunglePAX

TABLE OF CONTENTS

RELEASE SUMMARY

REQUIREMENTS

- A networked PC with access to the JPAX subnet

- Web-browser (latest version of Chrome, IE or Firefox)

- Terminal session. Putty.exe

- Optional Advanced NMS (90000-50, -50/G, -51, -50/G) version 8.2

DOCUMENTATION CONTROL

Document Version 1.00	PR 1.16c 27955	June 4th, 2020

PRODUCT/COMPONENT

This production firmware release is comprised of numerous individual firmware components packaged together and distributed as a controlled JunglePAX part number 90000-01. The overall product structure, including hardware and firmware contains the following sub-components

- CHASSIS, p/n 90001-01

    o   Comprised of Backplane, daughter-card and mechanical

- CORE Module, p/n 90010-01

    o   EM-10 firmware version 1.16c   (jpax_nms.itb)   Management Plane
    o   DP-10 firmware version 1.16c   (jpax_dp.itb)   Data Plane - OS
    o   FP-10 firmware version 1.16   (jpax_fpga.itb)   Data Plane - FPGA
    o   UB-10 firmware version 1.07   (jpax_uboot.itb)   Bootloader

- 48/130 VDC POWER Module, p/n 90110-01, HW version 0103

- 115/250 VAC POWER Module, p/n 90100-01, HW version 0104

- ACCESS CONTROL, Bootloader version 1.08.05   (ab90xxx08.bin & ab90xxx50.bin)

- ETHERNET SFP Unit, p/n 90200-01

    o   Application firmware version 2.01.16   (ac9020001.bin)

- ETHERNET RJ45 Unit, p/n 90201-01

    o   Application firmware version 2.01.11   (ac9020101.bin)

- T1/E1 Unit, p/n 90300-01

    o   Application firmware version 2.01.08   (ac9030002.bin)

- CBUS Unit, p/n 90301-01
    - Application firmware version 2.01.08   (ac9030101.bin)
- PROTECTION C37.94 Unit, 1-port, p/n 90360-01
    - Application firmware version 2.01.15   (AF9036001.bin)
    - FPGA version 1.13
- PROTECTION C37.94 Unit, 4-port, p/n 90360-02
    - Application firmware version 2.01.15   (AF9036002.bin)
    - FPGA version 1.13
- PROTECTION Direct Relay Unit (RS232 & G.703), 1-port, p/n 90350-01
    - Application firmware version 1.08   (AF9036002.bin)
    - FPGA version 2.01.03
- PROTECTION Direct Relay Unit (RS232 & G.703), 4-port, p/n 90350-02
    - Application firmware version 1.08   (AF9036002.bin)
    - FPGA version 2.01.03
- PROTECTION G.703, 4-port, p/n 90366-01
    - Application firmware version 1.03   (AF9036601.bin)
    - FPGA version 1.00.00

CORE UNIT DATA PLANE FIRMWARE

The data plane firmware provides the real-time operating environment responsible for the real-time components of the JPAX system and where all the time critical functionalities are implemented, including:

- data path configuration
- data path status monitoring
- alarm monitoring and reporting
- hardware drivers and control
- inter-core operation
- system initialization
- inventory
- node health status
- logging and event notification

The data plane is comprised of critical interfaces and associated systems that affect the flow of data within a JunglePAX node (Inter-core configuration and monitor) and across a JunglePAX network, including the CBUS Interface, TDM packetizer, MPLS capable switch, FPGA, Power Supply, DPLL, SFP status, alarm control and status, access unit control, and system logging functionality.

CORE UNIT MANAGEMENT PLANE FIRMWARE

The management plane firmware provides embedded management environment responsible for management plane functionality of the JunglePAX including:

- Configuration
- Alarm logging
- Status reporting
- Transaction and Session Management
- Security, including role-based access control
- Firmware upgrades
- Network discovery and remote management

The EM10 system is comprised of functional modules including the ConfD Infrastructure, Applications and Daemons, and the Interfaces that support the configuration of, and status/alarms-reporting from, the RTOS Components, which are also referred to as the Data Plane Components.

A JunglePAX model is created through the YANG modelling language and incorporated into the code build. The ConfD compilation infrastructure creates the north-bound interfaces (Netconf, CLI, HTTPS and SNMP). SNMP is not currently supported in this release. Each parameter set/get request is sent to the ConfD server, which will pass it via an Application or Daemon (often

referred to as a Data Provider) to the Data Plane. The Data Provider uses functions in the Interfaces to send the requests to the Data Plane.

For this release of the EM-10, access to the JunglePAX is via the **webui (aa.bb.cc.dd),** where **abcd** represent the IP address of the locally connected CORE module. This release supports local and remote unit access, with remote navigation provided by a Network node list. Access to either left or right remote CORE units is offered through the network node list.

Physical access to the embedded manager is provided through the TOP NMS port (RJ-45) on either left or right CORE modules.

Access to the Command Line Interface (CLI) is accessible via the webUI interface by pressing the CLI button or using an SSH client like PuTTY on the standard SSH port 2222. Connect to IP address of the CORE unit. The advantage of the SSH client is better window size flexibility and text handling like pasting scripts.

CORE UNIT BOOTLOADER

The Core Unit Bootloader controls the boot process of JPAX. It is responsible for the following:

- Loading factory firmware images from TFTP or SD card
- Extracting/Verifying and Booting EM and DP firmware images
- Extracting/verifying/flashing FPGA images to serial flash
- Configuring system memory map for all peripherals
- Storing MAC addresses, default IP settings and factory calibration settings
- Low-level system debugging support

ACCESS UNIT FIRMWARE

The access unit firmware for the microprocessor consists of two parts: the bootloader and the user application. There are different user applications to support the six types of access units

- 4-port Ethernet Optical (SFP),
- 4-port Ethernet Copper (RJ-45),
- T1/E1,
- CBUS,
- 1 & 4-port C37.94
- 1 & 4-port Direct Relay unit supporting RS232 (up to 4 ports) and G.703 (1 port), and
- 4-port G.703

RELEASE DETAILS

SUMMARY - NEW FEATURES (1.16C)

GE's JunglePAX is a purpose-built optical packet switched solution that's hardened through layers of redundancy for secure and dependable utility communications. This production release of the CORE units' firmware introduces a variety of new product features and fixes with the major items summarized below. The complete list is included along with their JIRA (issue tracking) number. Where a detailed description of the issue is required, please contact GE with the JIRA number

Firmware version 1.16c new features

- Added support for a new 4-port G.703 unit (p/n 90366-01)
    - This access cards uses JPAX's iCBUS (internal Channel BUS), a proprietary backplane interface that connects up to 240 DS0 channels between the core card and multiple access cards.

- WAN port support for Hybrid TDM Mode (SONET-Layer)
    - 1G WAN ports #3 and #5 to carry 84 VTs
    - 10G WAN ports #1 and #2 to carry 20 VTs

- Core Card Hybrid Mode support including:
    - Hybrid P2P-nx64K (iCBUS, CBUS, T1E1) and P2P-BulkT1E1 services
    - VTU-Thru/Drop (VTU = Virtual Tributary Units)
    - VT-MPLS Tunnel Stitching
    - OAM-Signaling Conversion
    - VT alarm and status monitoring: AIS, LOP, High BER, RDI
    - VTU Tests: loopback, Tx test bytes, Rx Test bytes
    - Local Tunnel
    - VTU protection switching
    - Hybrid VTU DROP Transmit and Receive Testbyte functionality - JXKSO-2095
    - Hybrid VTU DROP Local and Remote Loopback functionality - JXKSO-2098
    - Improved robustness in VT alarm detection and protection switching
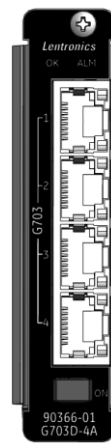
G703
Access Card

JPAX Hybrid Mode

JunglePAX Hybrid[+] Technology offers the best of both worlds by preserving SONET/SDH performance in a packet-switched network. This is achieved by adding an independent SONET/SDH layer alongside the MPLS-TP layer (without impacting its capacity) over the same optical WAN link. Use of this layer is optional and is intended for TDM-based relaying applications (C37.94, RS-232 Mirrored Bit, G.703 64k etc.) that are extremely delay sensitive.
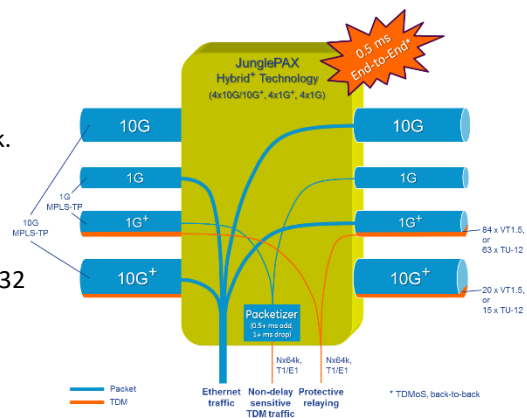
- Node Centric Configuration for Interfaces, Tunnels and Services

- New OAM features supported
    - Link Trace, Link Fault Indication, Delay measurement, Loopback
- Alarms
    - Changed some alarm priorities, names and source field to align with specification - JXKSO-2242
    - Removed unwanted Access MUX Change alarm (was showing in Telenium system) - JXKSO-1933
    - Extracting Core Card configured with Local Tunnel does not initiate Channel AIS for JMUX Shared DS-0 traffic - JXKSO-2133
    - Implemented VT protection switching on detection of WAN (to MPLS network) alarms - JXKSO-2175
    - Resolved issue of Conversion VT Tunnels alarm cleared after Core Card is rebooted - JXKSO-2190
    - Implemented tunnel protection switching on detection of WAN (to VT network) alarms - JXKSO-2176
    - Fixed Service Alarm Status inconsistency between Left and Right core cards - JXKSO-2016

- WebUI updates
    - Fixed unwanted page refresh when changing certain parameters - JXKSO-2025
    - Added color-coded alarm highlighting in WebUI
    - Miscellaneous WebUI improvements and bug fixes
    - The actual switching for protection circuits running over these iDS0 cards is available (displayed in the WebUI).
    - WebUI Interfaces: Load only visible tabs/load data on request when UI is opened JXKSO-1835
    - WebUI Tunnels: Stitch Tunnels View JXKSO-1787
    - WebUI Tunnels: Stitch Tunnels Table JXKSO-1786
    - WebUI Interfaces TDMoS Channel Usage table (SDH) JXKSO-1775
    - WebUI Interfaces TDMoS Channel Usage table (SONET) JXKSO-1774
    - WebUI Interfaces TDMoS Channel Usage table (SONET/SDH Mode) JXKSO-1773
    - WebUI Interfaces TDMoP Channel Usage table (T1/E1 Mode) JXKSO-1772
    - WebUI Interfaces TDMoS Ports table JXKSO-1771

- Firmware upgrade
    - Enhanced Firmware Upgrade functionality in WebUI (download Firmware package).
    - Improvements in Firmware Upgrade robustness.

- Miscellaneous
    - WAN code violation monitor supported
    - B1/B3 error counters supported
    - iDS0 hairpinning supported
    - Unframed T1/E1 supported
    - T1/E1 adaptive clock recovery
    - LAN Off/On disconnect
    - Secure SSH port 2222
    - WAN port NMS disable/enable
    - Access cards now reports serial number in WebUI
    - SFP Panel information updated/corrected

- o Resolved TDMoP 1+1 iDS0 outage occurs when LSR CC is rebooting - JXKSO-2268
- o Resolved Companion Sync issue when inserting a blank Core Card - JXKSO-1319
- o Fixed iDS0 access ports LED behavior - JXKSO-2172
- o Unprotected & 1+1 VPWS services residing on a bulk port must use the same (priority) tunnel as all other services on the same port - JXKSO-2181
- o Resolved Resource Denied issue while Creating/Editing Unprotected MP Pseudowire with Extended Tunnel - JXKSO-2245
- o Resolved CBUS TDMoS protection switching problem that occurs intermittedly in case 10G WAN Fiber cut/restore - JXKSO-2315
- o Resolved CBUS Shelf Clock Loss intermittent issue that occurs during reboot - JXKSO-2364

KNOWN LIMITATIONS

The following is a list of known limitations related to JPAX firmware package 1.16c. 27955

- iDS0 services configured for Unprotected Mode will result in asymmetric paths upon single fibre break
- iDS0 services configured for Unprotected Mode cannot select Right as Rx Priority
- The same VT slot number cannot be used by different WAN ports – CLI/UI reports 'Resource Denied'
- Circuit Addressing is not supported in Jmux-Jpax Conversion services
- PHY Ethernet Diagnostics Tab View | Link-Status shows incorrect state
- G.703D-4A | Link Status shows OK for disabled ports
- iDS0 unit's status display stop updating if Core Card time is set backwards

RESOLVED LIMITATIONS

The following is a list of limitations that have been resolved

- Previously, iDS0 level units were recommended to be installed in Slots 9 to 14. This limitation has been resolved with the current release of all iDS0 hardware. Customers may contract GE Product Management for more details
- Deleting a local endpoint in a multiple VPLS configuration may result in loss of other services
- Editing an existing endpoint to a lower value for VPLS did not configure correctly
- Swapping two core cards displays incorrect node name and number on WebUI.
- PSU current alarm remains raised when current levels return to acceptable values
- Offline provisioning of iDS0 services parameters not working

ENGINEERING RULES ASSOCIATED WITH JUNGLEPAX OPERATING MODES

GE allows for a mixture of firmware release 1.12a, 1.14, 1.14a and 1.16c in the same network. Ideally, all nodes within a JunglePAX network should be running the same firmware package.

FIRMWARE UPGRADE PROCEDURE

Contact GE technical support team for instruction on upgrading the unit firmware. There is currently no cost to customers to upgrade their JunglePAX firmware to release 1.16c.

CONTACTS

For additional details or technical assistance, you may contact:

Customer Technical Service

Burnaby, BC Canada

Phone: 1-604-421-8610

Lentronics.TechServices@ge.com