Release Notes: American Power Conversion, Console Port Server (CPS) Product Family

This document outlines the new features and bug fixes for the Console Port Server (CPS) product family (including BETA releases that are designated with a letter after the version number).

V2.6.0-5
(upgrade from V2.6.0-4)
May 2, 2007

A) Bug Fixes

The SNMP daemon no longer shuts down unexpectedly.

V2.6.0-4
(upgrade from V2.3.0-3)
September 21, 2006

A) New Features

- Upgrade of the Linux Kernel to 2.6.11 version which includes improvements in many areas, including scalability, device support, and performance.
    - Compact Flash: The Virtual Flash File System was implemented. It is mounted in the "/mnt/flash" directory during the boot time. These are the files:
        - boot_ori
        - boot_alt
        - boot_conf (old config)
        - zImage
        - config.tgz (old scripts)
    - Modules: The file with modules configuration was changed from **/etc/modules.conf** to **/etc/modprobe.conf**.
    - IPSec: The 2.6 kernel uses Openswan 2.3.0 in place of Freeswan (see Change Log for upgrade notes)
        - The Openswan 2.3.0 support for NAT-Transversal allows IPSec to be used behind any NAT device by encapsulating ESP in UDP.
        - The client must include the following line in the **/etc/ipsec.conf** file: **nat_transversal=yes**
    - LAN Bonding (Active Backup only)
        - Achieve redundancy on the Ethernet devices.
        - The standard Ethernet interface and one PCMCIA card act as one unique interface, answering for the same IP address, with the same MAC address.
        - No manual intervention is required when the primary connection is lost or recovered.
        - The failover is transparent and all connection sessions continue working with no interruption.

- Authentication Enhancement:

  - The administrator can choose different authentication types for access to the CPS and access to the port. Authentication types can be configured using the Web interface or using the Command Line Interface (CLI).
  - Each authentication server configuration is stored in its own configuration file:
    - Radius: **/etc/raddb/server**
    - TacacsPlus: **/etc/tacplus.conf**
    - Kerberos: **/etc/krb5.conf**
    - LDAP: **/etc/ldap.conf**
    - NIS: **/etc/yp.conf**
  - The PAM configuration file was divided into several files, one file per service. The configuration file name has the same service name for which it provides information. They are saved under **/etc/pam.d/**.

- Group Authorization Enhancement: Retrieves "group" information from the authentication servers (TACACS+, RADIUS, and LDAP) in order to perform "network-based" authorization.

- TIMEZONE: The CPS image includes official time zones. The administrator must run the **set_timezone** script to display a sequential menu, or configure it using the Web interface or CLI. This menu shows basic options or regions. Browse the options to choose one. (See Change Log for upgrade notes.)

- Power Management: Support for APC Switched Rack PDU models AP77*xx*, AP78*xx*, and AP79*xx*.

- IPMI Enhancements :
  - Removed the "ipmiutils".
  - IPMI devices are managed with ipmitool 1.6.0.
  - In the Web interface, the page **IPMI Power Mgmt** was added to the Applications Menu.
  - In the CLI command, device configuration was implemented.

- Web Interface: New or Changed Pages
  - Ports Menu
    - Ports Statistics - Table with columns that represent the following fields:
      - Serial port number
      - Serial port alias
      - Baud rate
      - TX bytes (bytes sent)
      - RX bytes (bytes received)
      - Frame (error)
      - Parity (error)
      - Overrun (error)
      - Access Tab (Physical Ports) - The configuration of the server authentication was removed.
    - Applications Menu
      - rPDU Multi-Outlet Ctrl - Manage groups of outlets (multi-outlet devices).
      - IPMI Power Mgmt. - Add IPMI devices and manage them.
      - Connect - A pop-up window with 3,000 lines and with the Copy/Paste features.
    - Network Menu
      - Syslog - Allow the administrator to configure filters by level.
      - PCMCIA Management in Configure Pop-up - Added CDMA as a card type.
    - Security Menu
      - Authentication - Allow the administrator to configure the authentication method for access to the box and the authentication servers.
    - Help Buttons are removed temporarily.
  - CLI - New Commands
    - When configuring PCMCIA cards, the user can insert (load) or eject (unload) the cards using these commands:

        - **cli>config network pcmcia #card insert**
        - **cli>config network pcmcia #card eject**
    - PortSlave - New Protocols
        - **Console (Telnet/SSH)** - Allows the client to access the serial port using a Telnet or SSH connection (i.e., it accepts any Telnet or SSH connection to access the serial port).
        - **Bidirectional Telnet (dynamic mode)** - Support for **socket_server** and **login** mode. When the *enter* key is typed in the terminal connected to the serial port, CPS presents the login banner and prompts to the user at the terminal. When in idle mode, the CPS accepts Console(telnet).
        - **generic_dial** - Generic Dial Framework will control this port.
    - Upgrade of OpenSSL to 0.9.8
        - This product is not affected by the vulnerability **SSL 2.0 Rollback (CAN-2005-2969)**
    - Upgrade of OpenSSH to 4.1p1
        - **X.509** - Support for X.509 certificates
        - SSHD keys are generated in the first boot of this version (the SSHD will be able to accept connections after the keys are generated).
        - If you use PuTTY, you must upgrade it to version 0.58.
    - Upgrade of OpenLDAP to 2.2.26 (see Change Log for upgrade notes)
    - Upgrade of PAM_LDAP module to 1.7.8
        - Fixed a potential security vulnerability, the failure to re-start TLS when following referred connections. (This can result in credentials being sent in clear text when pam_ldap attempts to rebind.)
    - Upgrade of MGETTY to 1.1.33
    - Upgrade of NET-SNMP to 5.2.1.2 - This version eliminates a potential security vulnerability:
        - Fixed a denial of service vulnerability when stream sockets have been configured for use (such as TCP but not UDP).
    - Upgrade of WIRELESS-TOOLS to 27
    - Upgrade of ZLIB to 1.2.3 - Version 1.2.3 eliminates potential security vulnerabilities in zlib 1.2.1 and 1.2.2 (CAN-2005-1849).
        - Eliminates a potential security vulnerability when decoding invalid compressed data
        - Eliminates a potential security vulnerability when decoding specially crafted compressed data
    - Upgrade of MODULE-INIT-TOOLS to 3.1-pre6
    - Kerberos - Applied a patch that fixes potential security vulnerability (CAN-2005-1689, VU#623332)
    - Upgrade BUSYBOX to 1.00
        - Contains the login utilities. (Note: The tinylogin package was removed.)
    - Added support for the following PCMCIA cards:
        - Xircom-XE2000 10/100 Network PC Card Adapter
        - Option Wireless-GlobeTrotter Universal Tri-band GPRS/GSM PC-Radio Card
        - Growell-iCARD800 CDMA 1XRTT GW-1031C

B) Bug Fixes

- ts_menu utility:
    - The ACL does not have the correct treatment.
    - The "-ro" option does not work in Clustering environment.
    - The "-s" option does not work in Clustering environment.
    - The CTRL+Z key sequence is not sent through the serial port when the "-auth" option is not used.
- SNMP
    - There are two config files for SNMP: **/etc/snmpd.conf** and **/etc/snmp/snmpd.conf**. Both files use the same name, but they have different functions.
    - Some OIDs regarding the eth0 interface are wrong (speed and operation status).
    - **cySPortRemoteIP** value is wrong.

- Web interface:
  - Crashes when LDAP is used for authentication
  - The **Add User** page allows the admin user to enter special characters in the shell field
  - When configuring one Syslog server, one filter is included in the Syslog configuration
  - The firewall configuration is not saved when the client saves or loads the configuration using the backup configuration page
  - Crashes when Clustering is configured and the "Connect" page is accessed
  - Adding new users fails in some situations
  - The "Privileged Users" field under Multi User (Physical Port) does not accept spaces
  - Customers have their LDAP Base Domain Name in the server with 60 characters.
  - Unsaved changes indicator turns red even when no changes were made to the Physical Ports pages
  - Firmware upgrade may fail, depending on the FTP server
- WebUI - Java Apple
  - Has an expired certificate
  - Access to clustering port works for CAS (telnet), but not for CAS (SSH)
  - Message shows when web-session times out and the client clocks in Connect
  - TAB key is not being sent to the device when the JRE version is 1.5.0
- PMD daemon no longer looks for the value assigned to pmNumOfOutlets parameter
- **pmCommand** would not report the status of current protection
- Second dialout PPP session does not work
- syslog messages are shown after the dial-in hangup
- CAS(telnet)
  - Sending RFC-2217 - Notify Modem State
  - Does not relay DCD changes per RFC-2217
  - When there is any sniff session opened, CPS does not relay DCD changes
  - Many CAS sessions terminate during a weekend stress test (under constant data flow)
- Route command segmentation fault
- TACACS+ authentication falls back to second server
- WIZ command accept only 1 DNS server
- nsupdate generated error messages
- Assigning multiple power ports no longer works
- Invalid users were included in the /etc/passwd file; problem should happen only in the *Local / *DownLocal authtype schemes
- When using the telnet client of Windows 2003 Server to access the port where the rPDU is connected, the session does not work
- bootconf utility allows you to select BOOTP option but when the configuration is saved, bootconf changes the BOOTP option to TFTP
- CLI: SNMP configuration was wrong. Increased the maximum length of the community name
- The CAS (SSH) does not work when sttyCmd parameter is configured as **raw -echo -echoe -echok -iexten -echoctl -echoke** in pslave.conf
- CPS holds data for 10-15 seconds. It should send data once per second to a device attached to a serial port of a CPS configured with 300 bps, 8 data bits, no parity, 1 stop bit, and no flow control. The protocol is raw_data and half duplex (rs232_half)
- Enabled **ssh root access** in **Open** & **Moderate** profile. It should be disabled in **secure** profile.
- The ipppd option **deldefaultroute** does not work.
- [ISDN callback] ipppd is brought up with wrong parameters for CALLBACK.
- Instead of md5, old DES-hashed passwords are used to save the password in the shadow file.
- With one serial port configured as CAS telnet (socket_server) and using data buffering, there was a delay in showing data from the serial port.
- Upgrading the Firmware version of the CPS through the Web interface can fail depending on the FTP server you use.
- Possible memory leak in the shared memory when using the factory configuration.
- The command **ts_menu -s** does not show all virtual ports configured.

C) Known Bugs

- The **admin** username can not be added or deleted using the Web interface or the CLI. The following command can be used to add one **admin** user:
  - #adduser -g admin admin <enter>
- When the Web interface is used to edit one slave of the Virtual Ports, if the IP address is changed, the slave will be deleted.
- rPDU commands rebootduration|powerondelay|poweroffdelay don't work properly for non-admin user when the applications pm and pmCommand are used. The configuration can be completed using the Web interface.

D) Change Log

- A new directory **/etc/daemon.d** was created. This directory contains all files that are used by the daemon.sh utility. The upgrade to the old version is done by the **upgrade260.sh** program that runs in the first boot with the 2.6.0 version. Always verify your configuration after the first boot.
- The **/etc/config_files** file was changed
  - Some files were included (/etc/shadow, ...)
  - Some files were removed (/etc/TIMEZONE, /etc/getty_ttyS0, ...)
  - Include changes in the **/etc/config_files.save** and copy it to /etc/config_files and save in CF.
- Upgrade of the Linux Kernel to 2.6.11
  - The Compact Flash directory was changed from **/proc/flash** to **/mnt/flash**
  - The name of the configuration file in Compact Flash was changed from **scripts** to **config.tgz**
    - The script shell **defconf** performs the reset to the factory configuration.
    - The file with modules configuration was changed from **/etc/modules.conf** to **/etc/modprobe.conf**
      - Include your changes in the new file and add the new file in **/etc/config_files**
    - The **/etc/ipsec.conf** file was changed:
      - Copy the **/etc/ipsec.conf.save** file to **/etc/ipsec.conf** file and include your changes or edit your **/etc/ipsec.conf** file.
      - To edit your **/etc/ipsec.conf** file:
        - Include the following line: **version 2**
        - Comment out the **plutoload** and **plutostart** lines
  - Upgrade of PAM-LDAP - change the OpenLDAP SSL configuration:
    - In the **/etc/ldap.conf** file, at least one of the following parameters are required if the **tls_checkpeer** is **yes**:
      - **tls_cacertfile**
      - **tls_cacertdir**
  - TIMEZONE:
    - This feature now uses the **/etc/localtime** file.
    - The old **/etc/TIMEZONE** file is erased if you configure this new feature.
    - The image comes with no **/etc/localtime** file, but it will be created and will replace the **TIMEZONE** file if you configure the time zone.
  - Authentication Enhancement
    - The **/etc/pam.conf** file was removed and the /etc/pam.d directory was created
    - The RADIUS and TACACS+ servers need to be reconfigured by the Web interface or CLI; the configuration of these servers in PortSlave configuration was removed.
  - The **/bin/build_DB_ramdisk** shell script was changed to use ramdisk type **tmpfs** instead of **ramfs**, because **ramfs** has had a problem with maxsize.
  - The certificates that are used by SSHD and HTTPS are generated during the first boot.
  - The name of the PCMCIA modem devices was changed from **/dev/ttySxx** to **/dev/ttyMy**. Two dedicated device files (**ttyM1** and **ttyM2**) have been created for the PCMCIA modem devices.
    - If the PCMCIA modem card has already been configured, rename the existing file **/etc/ppp/options.ttySxx** to **/etc/ppp/options.ttyM1**

E) Warning

- Kerberos Authentication: Make sure there is an entry in the **hosts table** (/etc/hosts) corresponding to the hostname configured for the Console Port Server (/etc/hostname).