Eldorado, August 2017.

Dear Customer,

DATACOM is glad to present MPU10G firmware version 13 (*Wed Aug 30 20:43:54 UTC 2017*), file 0294-32.im.

Corrected Issues

- SNMPv3 requisitions were not working properly after a system date change.
- User's permissions window was not working properly for user with similar name root.
- Possibility of creating new users with empty passwords.
- Standby MPU was reconfiguring the output clock incorrectly causing noises on the output signal.
- Fix wrong generation of SDH alarms HP_RET_FAIL, TX_AU_LOP and TX_HP_RET_FAIL.

Improvements

- MPU Wander performance improved to eliminate long term phase deviation.
- User password policy was improved, for security reasons.
- Management connection through serial interface is closed after an idle time of 10 minutes.
- Logging when configuring SNMP, Network, NTP or boot parameters.
- More detailed user database modifications logs.

New Features

- OPI measurement. Monitoring and alarm triggering based on the variance of received power in transceivers with Digital Diagnostics.
- Option to disable unsecure management protocols.
- Secure firmware upgrade using SFTP.
- Log deletion TRAP.
- TRAP for successful and fail login attempt.

Management System

- FW13 is fully supported in DmView 9.6.0-2 or higher version. It's strongly recommended to update DmView to this version because FW13 contains new features that are incompatible with older DmView versions. The side effect will be the generation of polling in DmView indefinitely.

This new version will be available from August 2017. Additional information can be obtained by contacting DATACOM support (support@datacom.ind.br or +55 51 3933-3122).

Regards,

DATACOM

Details:

SNMPv3 requisitions were not working properly after system date was changed:

When the system date was changed with a big offset (the issue was deterministic for a value of one year or more), SNMP daemon stopped to answer get and set requisitions. Now, when system date is changed, manually or via NTP, SNMP daemon is restarted.

User's permissions window was not working properly for user with similar name root:

In the user permissions configuration window in the DM800 terminal (Administration/Users/User_permissions), when a logged user tried to change permissions of other user with the same root name, the action could not be performed. The user name compare method was improved to fix this.

Possibility of creating new users with empty passwords:

The equipment allowed creating users with empty passwords, which were not able to login. A password policy was implemented, which forces passwords to be 8 characters long.

Standby MPU was reconfiguring the output clock even when it was not needed:

During the synchronization process between the MPUs, the standby MPU was always configuring the clock source, even if it was not needed. Now, the standby MPU will only set its clock when the clock source of active MPU has changed.

Fix wrong generation of SDH alarms HP_RET_FAIL, TX_AU_LOP and TX_HP_RET_FAIL :

The programmable logic of interface cards was fixed. The cards are able to identify a communication failure with MPU and switch quickly to the other MPU automatically. But, there was a problem in the detection of faults in communication channel between MPU and interface cards, causing spurious commutations. As a consequence, SDH alarms were generated due to data traffic interruption. The bug had a very low probability of occurring.

MPU Wander performance improved to eliminate long term phase deviation:

DM880 clock recovery mechanism presented a very low long term phase deviation when tested in a chain of multiples equipment. In spite of this deviation being within the limits specified in ITU-T G.823 for a SEC equipment (MTIE and TDEV masks) DATACOM proceeded with adjustments to make it negligible. In DM880 the clock recover is controlled by a PID controller in the Active MPU. In order to reduce the phase deviation to a value closer to zero the integral term of this controller was increased by 1.5. In a PID controller

the integral term accelerates the movement of the process towards set point and eliminates the residual steady-state error (long term phase deviation in this case) that occurs with a pure proportional controller.

User password policy was improved, for security reasons*:

The password policy was improved for security reasons. When creating new users in the equipment, the user password must have 8 characters long and must contain at least one number, one special character, one uppercase and one lowercase letter. The valid special characters are shown on the configuration screens with inputs for password. **Please see known issues.*

Management connection through serial interface is closed after an idle time of 10 minutes:

In case a session on the serial interface was not closed, other users could connect in the serial interface and use that session. Now, once a session on the serial becomes idle for 10 minutes, that section will be closed and a new login will be required.

Logging when configuring SNMP, Network, NTP or boot parameters:

If SNMP, Network(Router, RIP, OSPF), NTP or boot configuration is changed via WEB interface, terminal or DmView, a log will be generated: *User <user> saved network config*. Where *<user>* is the user name. A similar message will be generated for other configurations.

More detailed user database modifications logs:

Whenever an administrator modified the user database, there was no information which operation was done. The additional messages have the format *User <oper> added user <user>*, where *<oper>* is the operator and *<user>* is the user being modified. Aside from “add” operation, there are logs for “delete”, “change password” and “set permissions”

OPI measurement:

This firmware includes the OPI measurement and monitoring feature. When enabled, for a specific port, it starts to monitor received RX power from the transceiver inserted and it triggers an alarm if the calculated mean is beyond the configured alarm threshold. The OPI data are stored each 6 hours in order to generate a history that can be viewed in DmView.

Option to disable unsecure management protocols:

This new feature allows enabling and disabling all strictly unsecure management protocols, such as Telnet, FTP, HTTP and the proprietary PCGA protocol. The unsecure

protocols can only be enabled/disabled simultaneously. All incoming/outgoing traffic on the aforementioned protocols' ports will be dropped by the equipment. Secure protocols, such as SSH, SFTP and HTTPS will be always enabled. For a fully secure operation mode, SNMP must be properly configured by disabling SNMPv1 and SNMPv2 and enabling SNMPv3 only, for both accessing the equipment and sending traps.

Secure firmware upgrade using SFTP:

The equipment now supports firmware upgrade via SFTP. As in the firmware upgrade via FTP, the user allowed to upload the image file is fixed, with name "adminftp" and a configurable password. Since DmView version 9.6, the firmware will be sent via SFTP protocol (when supported in the equipment's version), regardless of whether the unsecure protocols are disabled or not.

Log deletion TRAP:

In case an user delete the user logs, a trap and the corresponding log will be generated, indicating the name of the user which deleted the logs.

TRAP for success and fail login attempt:

Every time an attempt to authenticate on the equipment occurs, a trap will be generated, indicating the user's name and access method of the attempt. There are traps for both success and failure, and also a corresponding log message.

Known issues:

When adding a new user with a name longer than 8 characters, login may not be performed properly. Login can be denied for this user.