ComAp
The heart of smart control

CM-Ethernet

Ethernet plug-in module

SW version 2.1.4

Written by Jan Tomandl
Prague, Czech Republic
ComAp a.s., U Uranie 1612/14a,
170 00 Prague 7, Czech Republic
Tel: +420 246 012 111
E-mail: info@comap-control.com, www.comap-control.com

New Features List

1 General information

1.1 Version information

The version 2.1.4 is a bug-fix version.

1.2 Clarification of Notation

Note: *This type of paragraph calls the reader’s attention to a notice or related theme.*

> **IMPORTANT: This type of paragraph highlights a procedure, adjustment etc., which can cause a damage or improper function of the equipment if not performed correctly and may not be clear at first sight.**

> **Example:** This type of paragraph contains information that is used to illustrate how a specific function works.

2 Changes in the version 2.1.4

2.1 Bug fixes

- AirGate connection fixed.
  - AirGate connection was not functional in previous build 2.1.3

3 Changes in the version 2.1.3

3.1 Bug fixes

- HTTP POST request issue.
  - If a POST request was sent to the module separated into two TCP packets (body and parameters) it will not be processed.
- Active e-mails issue
  - Active e-mails would not be sent or would have damaged content if a retransmission occurs at TCP layer while communicating with SMTP server.
- Packet repeating issue
  - Sending of the very first TCP packet in ComAp/TCP protocol was not repeated if ACK not received. This might cause establishing of the connection to the controller failed and client had to repeat it.

4 Changes in the version 2.1.2

4.1 Bug fixes

- Issue with e-mail address longer that 32 characters.
  - If recipient address of an active e-mail was longer than 32 characters the address was shortened and became invalid. Although that e-mail was successfully submitted to SMTP server it was not deliverable.
  - Such an e-mail was reported to controller (and then written into controller history) as successfully sent, but in fact it was not delivered to the recipient due to invalid address.

5 Changes in the version 2.1.1

5.1 Bug fixes

- All running TCP sockets might have been interrupted.
  - The built-in DHCP client used incorrectly "broadcast flag" in DHCP options while renewing IP address although the renewal message is sent as IP unicast. Some DHCP servers might evaluate such message as invalid and the renewal procedure failed. Consequently the IP address lease time elapsed and the module invalidated it's IP address and started complete DHCP handshake again.
  - In the moment of invalidation of the IP address all running TCP sockets were closed and thus communication with the module was interrupted (e.g. MODBUS/TCP communication).

6 Changes in the version 2.1.0

6.1 New features

- Support for latest controller firmwares
  - Web interface is now available for all InteliLite, InteliGen200 and InteliMains210 firmwares including the latest releases.

7 Changes in the version 2.0.1

7.1 Bug fixes

- Programming firmware or configuration into the controller via CM-Ethernet module might not work.
  - Fixed problem with TCP segmentation that might cause interruption of the connection when attempting to program configuration or firmware into the controller.
  - This issue occured at connections with small MTU size (e.g. AirGate or Virtual Private Networks)

8 Changes in the version 2.0.0

8.1 New features

- Support for latest controller firmwares
  - Web interface is now available for all InteliLite and InteliGen200 firmwares
- Cybersecurity improvements
  - New ciphering suite is used for "Direct IP" as well as "AirGate" connection. The ciphering suite consists of ECDH algorithm for session key agreement and AES-256 in CBC mode for ciphering of the data stream in both directions.
  - It is possible to completely disable the web interface by a controller setpoint. This will allow, in addtition with disabling all other unsecured protocols like MOBUS/TCP or SNMP, exposing the controller ethernet interface into an untrusted infrastructure.
  - Function for "retrieving the lost password" (aka "password decode") was completely removed. It was replaced by a secure method for resetting password to default value. Detailed description is available in the controller or InteliConfig manual.

Note: *The new cybersecurity features are available only with updated controller firmwares which support these features as well.*

8.2 Bug fixes

- Cybersecurity issues
  - Random value is now used for session ID in web connection
  - TCP sequence number is now initialized to random value.
- Controller web interface troubles
  - If a setpoint group containing large number of setpoints was displayed the web session might get completely frozen.
- Problems with sending active e-mails
  - It might occur that the module returned failure response to the controller although the e-mail was sent correctly. This might happen especially if AirGate SMTP was used.
  - If the password for SMTP server contained characters "!" ,""", "#", "$", "%", "&" and AUTH PLAIN method was used for authentication the authentication was not successful as the password was improperly encoded into the base64 string.
- SNMP Agent might stop working
  - The built-in SNMP Agent stopped responding to the SNMP manager requests if a request from the manager came while a periodic ARP update for the manager's IP address was being processed.

9 Changes in the version 1.2.0

9.1 New features

- SNMP v2c support
  - Added "community based" version of SNMP v2
  - SNMP v1 remains supported as well, the module responds using the same version as used in the request
  - Both PDU types "notification-type" and "inform-type" can be used with SNMP v2c. The adjustment of PDU type used for unsolicited messages is done in the controller via it's setpoints and this adjustment must be supported also in the controller firmware. The PDU "trap-type" is used by default if the adjustment is not supported in the controller firmware.

***Note:** The MIB table can be now exported using [[[Undefined variable TechnicalTerms.LiteEdit]]] in either SMIv1 or SMIv2 format.*

9.2 Bug fixes

- SMTP server authentication CRAM-MD5
  - Uppercase hex characters were used in the digest hex string, which might lead to refusing the user credentials even if they were correct.
  - If the username was longer than 15 characters the login message that was sent to the server was malformed and thus the server refused it.

10 Changes in the version 1.1.0

10.1 New features

- Supported controller firmwares
  - Added support for InteliLite-1.1.0
- SNMP Traps
  - Added support for SNMP v1 TRAPs.
  - This feature can be used only with controller firmware which also support SNMP Traps (e.g. InteliLite-1.1.0 and above.
- Secondary DNS Server
  - Added support for the secondary DNS server.
  - The secondary DNS server is used if the primary DNS server does not work or is not able to perform the requred DNS translation.
  - In fixed IP address mode both DNS servers are to be adjusted via appropriate controller setpoints.
  - In automatic IP address mode the DNS servers are adjusted automatically by the DHCP server. It may occur that the DHCP server does adjust only the primary DNS server. In such case the secondary DNS is taken from the controller setpoint. However, the update of the secondary server is performed only in the moment of the DHCP negotiation is finished, so if the user changes the secondary DNS setpoint afterwards the change is not taken into account immediately.
- DNS transcation number and outgoing port randomization
  - The transcaction numer and outgoing port number are pseudo-randomized instead of being constant.
- Number of MODBUS/TCP clients increased
  - The total number of MODBUS/TCP clients, that can be connected simultaneously, is increased to 2.

11 Notes

11.1 General note

CM-Ethernet modules containing firmware version **1.0.0 can not be updated** to any newer version. Please ask for replacement in this case.

11.2 Document history

Revision number	Related sw. version	Date	Author
1	1.1.0	10.3.2016	Jan Tomandl
2	1.2.0	16.9.2016	Jan Tomandl
3	2.0.0	4.1.2018	Jan Tomandl
4	2.0.1	23.5.2018	Jan Tomandl
5	2.1.0	9.1.2019	Jan Tomandl
6	2.1.1	7.1.2020	Jan Tomandl
7	2.1.3	10.9.2020	Jan Tomandl
8	2.1.4	12.10.2020	Jan Tomandl