



Q1. Quels sont les types de messages ModBus utilisés ?

Les messages utilisés sont des requêtes (queries) et des réponses (responses). Les requêtes sont envoyées par le client (par exemple, l'IHM) et les réponses sont envoyées par le serveur (le PLC).

Q2. Quel est le Function Code du message ModBus utilisé pour lire un coil ?

Le Function Code pour lire un coil est 1 ("Read Coils").

Q3. Que signifie le champ Reference Number dans un message pour lire un coil ?

Le champ "Reference Number" indique l'adresse du premier coil que la requête cherche à lire dans le dispositif esclave.

Q4. Comment ils sont identifiés les paires de messages query et response ?

Les paires de messages requête et réponse sont identifiées par le "Transaction Identifier" qui est unique pour chaque paire de messages dans une transaction Modbus. Cela garantit que chaque requête est associée à sa réponse correcte.

Q5. Quel est le Function code du message ModBus utilisé pour écrire un coil ?

Le Function Code pour écrire un coil est 5 ("Write Single Coil").

Exercise 2

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

+br-48a2cae5b39

modbus and ip.addr==192.168.1.3

The image displays a Wireshark packet capture analysis of a Modbus TCP request. The packet list at the top shows a Modbus Read Coils request (32897) from 192.168.1.3 to 192.168.1.2. The packet details pane shows the structure of the Modbus PDU, including the function code (01) and the starting address (0242). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
32897	416.68916195	192.168.1.3	192.168.1.2	Modbus/TCP	78	Query: Trans: 0; Unit: 1, Func: 1: Read Coils
32898	416.70729895	192.168.1.2	192.168.1.3	Modbus/TCP	78	Response: Trans: 0; Unit: 1, Func: 1: Read Coils
32942	417.676797160	192.168.1.3	192.168.1.2	Modbus/TCP	78	Query: Trans: 1; Unit: 1, Func: 1: Read Coils
32944	417.70629859	192.168.1.2	192.168.1.3	Modbus/TCP	76	Response: Trans: 1; Unit: 1, Func: 1: Read Coils

Packet 32897: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface br-48a2ca4e5b39, id 0

Encapsulation type: Ethernet (1)

Arrival Time: Dec 1, 2023 08:45:32.241796419 CET

[Time shift for this packet: 0.000000000 seconds]

EPOCH Time: 1701935192.241796419 seconds

[Time delta from previous captured frame: 0.018552500 seconds]

[Time delta from previous displayed frame: 0.018578200 seconds]

[Time since reference or first frame: 416.70729859 seconds]

Frame Number: 32899

Frame Length: 76 bytes (608 bits)

Capture Length: 76 bytes (608 bits)

[Frame is marked: False]

[Frame is ignored: False]

Protocols in frame: eth:ethertype:ip:tcp:modbus

Coloring Rule Name: TCP

Coloring Rule String: tcp

Ethernet II, Src: 02:42:c8:a8:01:02 (02:42:c8:a8:01:02), Dst: 02:42:c8:a8:01:03 (02:42:c8:a8:01:03)

Destination: 02:42:c8:a8:01:03 (02:42:c8:a8:01:03)

Source: 02:42:c8:a8:01:02 (02:42:c8:a8:01:02)

Type: IPv4 (0x0008)

Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.3

0100 = Version: 4

0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 62

Identification: 0xfc87 (64647)

Flags: 0x00, Don't Fragment

0x00000000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0xbadc [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.2

Destination Address: 192.168.1.3

Transmission Control Protocol, Src Port: 502, Dst Port: 39754, Seq: 1, Ack: 13, Len: 19

Modbus/TCP

Transaction Identifier: 0

Protocol Identifier: 0

Length: 4

Unit Identifier: 1

Modbus

0000 0001 = Function Code: Read Coils (1)

[Request Frame: 32897]

[Time from request: 0.018578200 seconds]

Byte Count: 1

Bit 0: 1

Bit 1: 1

Bit 2: 0

Bit 3: 1

Bit 4: 0

0000 02 42 c8 a8 01 03 02 42 c0 a8 01 02 08 00 45 00 -B-----E

0010 00 3e fc 87 40 00 40 06 ba dc c8 a8 02 c0 a8 ->-0-

0020 01 03 01 01 76 00 4a dc e4 35 ba c0 01 07 3e 00 18 -...J 5 0-

0030 01 73 85 86 00 01 01 08 0a 7e 2b d7 c1 96 7e -.....+--

0040 77 04 00 00 00 00 00 04 01 01 01 2b -.....+

Wireshark br-48a2ca4e5b39/CDFY2 ucapano

Packets: 58113 | Displayed: 2226 (3.8%)

Profile: Default

Q1. Quels sont les types de messages ModBus utilisés ?

Comme dans l'exercice 1, ce sont des requêtes et des réponses de Modbus TCP.

Q2. Quel est l'intervalle du temps entre deux messages Query successifs ?

L'intervalle de temps entre deux requêtes successives est d'environ 1 seconde, conformément à la configuration de ScadaBR pour interroger le PLC toutes les secondes.

Q3. Quel est le Function Code du message ModBus utilisé pour le lire un coil ?

Le Function Code pour lire les coils est 1 ("Read Coils").

Q4. Combien de coils sont lus par ce message ?

D'après la capture d'écran, un seul coil est lu par la requête, comme indiqué par le "Bit Count" de 1.

Q5. Quel est le Function code du message ModBus utilisé pour écrire un coil ?

Le Function Code pour écrire un coil est 5 ("Write Single Coil").