

网测科技

2021/1/20



目录

1.	Modbus 用例说明	3
2.	创建 Modbus 测试用例	3
3.	运行 Modbus 测试用例	5
4.	详解客户端读或写的指令	7
	4.1 状态码 01 读线圈	7
	4.2 状态码 02 读离散输入(触点)状态	7
	4.3 状态码 03 读保持寄存器数据	8
	4.4 状态码 04 读输入寄存器数据	8
	4.5 状态码 05 写单个线圈状态	8
	4.6 状态码 06 写单个寄存器数据	9
	4.7 状态码 15 写多个线圈状态	9
	4.8 状态码 16 写多个寄存器数据	
5.	服务器从站的配置	
	5.1 添加从站	
	5.2 下载 Pcap 报文验证	



1. Modbus 用例说明

客户端模拟 Modbus 的主站, 服务器模拟 Modbus 的从站, 主站向从站发送指令, 从站 接收并回复状态, 完成协议模拟并进行各种统计。

2. 创建 Modbus 测试用例

依次点击,用例 -> 网关设备测试 -> 协议仿真-> 工控协议 -> Modbus-> 增加。 单击增加,在弹出的选择用例选项中,编辑用例网络选项,根据需要修改配置参数,然后点 击确定,进入用例配置页面。

◎ 网测科技 nelitest.com		'n			V20.12.06	Supernova-88D
■ 阿夫役首別は ●	Modbus					
В натринатрукатра О	APRILING THE STATE STATE AND A LOUGH AND A LOUGH AND A LOUGH					
RISP/RTP/RTCP						
O VPN	用例列表					
% UDP/TCP						
O PROMINENCE	+ 1012 8 899					R SA C SM
■ 1012/05/4	· 编号 运行 任规则表 用户	87	99	克和	i¥knast	导出 历史记录
◆ TCP协议						
UDPINX NUCENNY	10 0-0 of 0	择用例选项				
► IPOERRY						
▶ IGMPtbb2		1P版本 ⑧ v4 〇 v6 〇 混合				
▶ 工控协议		受到股份工作模式 ● 通明编式(TP) ●				
> Modbus		○ 踏曲模式(NAT) @				
		网络醋酚醋 RKU MPRE 🗸				
· DDcoliges		第日報道 🗌				
0 Dunman						
o iteranito O						
El Hassenit o						
O SERVICE						
Let PRODUCTION O						

输入用例的名称,设置测试时长,选择测试端口,配置网络。

<u>ب</u>	例名称 Modbus_TP_admin_20210 合法手符类型: A-Z / a-z / 0-9 / :	120-16:31:46 / - / _ (不支持中文符号)			源成时长(时分秒) 新	0 :: :::::::::::::::::::::::::::::::::	10 : 0 74882:1999()41		
网络 参数	客户端 服务器	记录							
网络设置									配形法
<i>{</i> 户端				S 🖉 🗰 🖻 💼 🖻	服务端				
sonta					port/				
原用所口				MAC 68:91:d0:63:4b:54					MAC 68:91:d0:63:2
HT-meets					CPORODE				
SRXXSBSX				•	HCX/MEX				
迷率与MAC				•	速举与MAC				
QinQ (慧用)				-	QinQ (前用)				
子网 😧				+ 源20子网 🔺	子网 🛛				+ 漆加子网
11个子同				自 移除于同 ② 禁用于同	第1个子网				自移除子网 ② 禁用子科
	测试仪跳口IP地址或范围	19.1.2.2-19.1.2.201	0			测试仪键口IP地址或范围	19.1.1.100	0	
	测试仪第口子网接码	16	Θ			测试仪端口子网掩码	16	0	
	虚拟器由	19.1.254.1				虚拟路由	19.1.254.2		
	测试仪第日网关	19.1.1.1	0			测试仪装口网关	19.1.1.1		
	VLAN ID		0			VLAN ID		0	
	子网模拟	只模拟春户講	~			子网機拟	只機以服务誘	~	
	服务调新在主机	192,168,16,228							
	服务端所在端口	port7	~						
	服备编纸在子网	第1个子网	~						



设置主要参数,Modbus 主要配置参数如下:

基本信息 (Modbus)		
用砌名称 Modbus_TP_admin_20210120-16:31:46		题成组织 (1855年) 0 : 10 : 0
合法学符类型 AZ/az/091:1-1_(不支持中文符号	3	例如在在起程时长后台的时候,例如时长不能超过999小时
网络 参数 客户端 服务器 记录		
用例参数 通用参数		
	Beadmin占国内东 60	68
	用户admin申请占用的内存数量。可以到资源	の存留理茨原申请
	用例运行占用内存 60	GB
	並行此用例占用的内存空间。包括DPDK的大型 DPDK大页内存占比 50	19時, UUSSL会法品用的普遍集用的時, 范囲: 2-60GB 1910
	DPDK大页内存占用例运行内存的百分比,运行	
	从站数量 247 第二、247 第二へ来の論語の二日から118 万元	客户端即为从站
	Modbus模式 TCP模式 V	工作模式
_	Modbus模式包括:TCP模式。RTU基于TCP的	
20	基Modbus命令速率 1 每秒主站像每个从站发送的Modbus命令数量。	友达 部令 迷 率 (地震 や) 100000
l		
	启动	Q27 \$276
基本信息(Modbus)		
Highwas		80/fe12/ /e14/04/1
用例容称 Modbus_TP_admin_20210120-16:31:46 合法字符提起 A-Z / a-z / 0-9 / : / · / _ (不改時中文符)	g)	(第5回時代(第5分号) 0:10:0:0 (10:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:
网络参数 春户端 服务器 记录		
	源號口范围 10000-65535 四形 1.000-65535	
	an	
	2943/378 2014/1111 ACHIVITI	
	24该输入高存器数据 2	和学家自得发兴动范围也不
	205尾单个线圈状态 🕑	10 宣告广始次达303人40日マ
	205号单个寄存器数据 2	
	☑ 15号条个线圈状态 US ☑ 15号条个线圈状态 US	
	启动	6777 8038
基本信息 (Modbus)		
Harten To a table 2020/02/02 45 24 45		
Models_12_admin_20210120-10:31:46 合法字符提述 A-2 / a-2 / 0-9 / : / - / _ (不受持中文符	9)	#88#41年(1939年7) 0:10:00 満成在配型时代后自动培养、満た対抗不能超过999小时
网络参数 春户端 服务器 记录		
Land Land Land Land Land		
	从站对象的世 默认Modbust地址	
	服务體調山 502	///如庆443日文编辑



用例参数配置完成后,可以点保存,保存编辑完成的用例配置,同样也可以点击启动, 直接启动运行测试用例。

基本信息(Modbus)									
用例	名称 Modbus_TP_admin_20210 合法学符类型: A 2 / arz / 0-9 / :	120-16:31:46 /-/_(不支持中文符号)			测试时长 (时分秒)	0 : 2014-2025-01-5.550-01-5.2000-0-5.2000-0-5.2000-0-5.2000-0-5.2000-0-5.2000-0-5.2000-0-5.2000-0-5.2000-0-5.2000-0	10 : Anticitation	0	
网络参数	客户端 服务器	记录							
保存网络设置									配要讓口線
客户端					服务端				
port3					port7				
◎ 第用第□				MAC 68:91:d0:63:4b:54	◎ 無用満口				MAC 68:91:d0:63:2e:2a
CPU核绑定				•	CPU核绑定				•
报文捕获				-	报文捕获				•
速率与MAC				•	速率与MAC				•
QinQ (#\$/8)				-	QinQ (如用)				•
子网 0				+ 激加子同 🔺	子网 😡				+ 源加子网 🔺
篇1个子网				會都除子网 ◎ 禁用子网	算1个子网				自移除子列 ② 禁用子列
	测试仪纳口IP地址或范围	19.1.2.2-19.1.2.201	0			测试仪纳口IP地址或范围	19.1.1.100	0	
	测试仪端口子网掩码	16	Θ			测试仪施口子网掩码	16	0	
	虚拟路由	19.1.254.1	0			虚拟路由	19.1.254.2		
	测试仪跳口网关	19.1.1.1	0			游试仪端口网关	19.1.1.1		
	VLAN ID					VLAN ID		0	
	子网模拟	只授於政府講	~			子网模拟	只機拟服务请	~	
	服务颁新在主机	192,168,16,228							
	报告律所在第 日	port7	~						
	ID Street T 70	\$. A70							
	服务通用社士网	1 ME 1 1 7793	× 1						

3. 运行 Modbus 测试用例

1. 点击 Modbus,选择编辑完成的测试用例,点击启动按钮,运行启动测试用例。

◎ 网测科技			ikin iki	admin			V20.12	56 Su	oernova-88D
用关设备测试 Ø	Modbus								
HTTP/HTTPS/HTTP2 O RTSP/RTP/RTCP	電产調整KMoobudi注注。								
D VPN	用例列表								
() scarster	+ 3833 (3) 8889								8 80 A C 80€
■ 90汉代英	0 49 E	任务列表	甩户	名字	995	克隆	详细的型	号出	历史记录
 TCPI协议 LIDPINIX 	_ · 🔀) 🗰	admin	Modbus_TP_admin_20210120-16:31:46	/	ත			0
DHCP101X IPoE101X	显示行数: 10 × 1-1	点击运行编辑 of 1	lf完成的测试 F	目例					< 1 >
► IGMPI的议 ▶ 工控制议									

2. 用例启动后,可以在监控页面查看用例运行数据信息

Modbus 新式用户: add	min 用例名称: M	Addbus_TP_admin_2	0210120-16:31:46					
键结果			状态			网络尼		
						AND 新建 61章 广播		
2.168.16.228 - Port3	树植	233	应用层					
DBUS_发送请求	1,976	67,184	Bf0 port3 port3			192.168.16.228 - Port3	EMB	
IDBUS_图应请求	0	0	and poor poor			报文操收	1,976	
1.168.16.228 - Port7	1940	88		移動	28	税式发送	2,223	
DBUS_发进编辑	0	0	MODBUS_发送请求	1,976	67,184	192.168.16.228 - Port7	96	
IDBUS_EI应编末	1,976	67,184	MODBUS_BACKREE	1,976	67,184	报文编校	2.223	
			MOOBUS」與亞威法		67.184	167.22.2	1,976	
			MODBUS_晚应异常		0			
			MODBUS_册权请求	1,976	67,184			
			MODBUS」與亞邊來	1,976	67,184			
			MODBUS 通常异称	0	0			
加获 .168.16.228 - Port3		en a				乾煞局 284		
編获 .168.16.228 - Port3 市場もの量		288 0				逆路层 送车 192.168.16.228 - Port3		
始获 168.16.228 - Port3 物語NARO量 1947的量		2830 0 0	2000 D			 - U的名字 - USE 16.228 - Port3 - CE集成 		
))6获 1.168.16.228 - Port3 中的限制(20))型 23-FTRO型 23-FTRO型		く 	/(始辰 @		•	 ● 送業 192.168.16.228 · Port3 ※出始次 注册分支 		
1600 1.168.16.228 - Port3 2時間転取量 大学行政量 2月86.16.228 - Port7	e	より 	代始日 O 王句 port port		-	 (通知后) (返本) 192.168.16.228 - Port3 (三級知道) (三級知道) 192.168.16.228 - Port7 		
補統 - 新務 - 新務 - 学行教堂 - - - 新務 - - - - - - - - - -	į	より 	KMBE 0 0 B0 port port?	Pat	-	代数記 送着 192.168.16.228 - Port3 元振動改 用意改迭 192.186.16.228 - Port7 元振動改		
結誌 168.16.228 - Port3 宇市設置 5年で設置 5年で 5年での15 5年 5年での15 5年 5年での15 5年 5年での15 5年 5年 5年 5年 5年 5年 5年 5年 5年 5		▲ ジン の の 三回)日は停止 ジン の の の	代始日 0 	Pit 0	4 8 27	 ・込施記 		
格获 168.16.228 - Port3 资源後認識 学行教題 188.7 168.16.228 - Port7 政策指数量 学行教題 148.			代始記 0 居然 port3 port3 TO 主体研究時	00 0	200 207	 ・・ ・ <li< td=""><td></td><td></td></li<>		
	1		代始版 の 国際 原のは 9xx7 TO まの時間5番 TO まの時間5番 TO まの時間5番 TO まの時間5番	Pit 0 0	A 207 207 207	 記書 192.168.16.228 - Port3 三型時代 <li< td=""><td></td><td></td></li<>		
	ti ti		FilleR 0 500 SEE pert pert TO patentiation pert	80 0 0 0	207 207 207 207 207	 ・ ・ ・		
新藤枝 108, 16, 28 - Port3 新藤田田田 長子町秋道 切蔵尺 (18, 16, 28 - Port7 初焼代か田油 大子町秋道 古崎代	, E		代始版 の 国際 国の 国の	Pil 0 0 0	6 88 30 30 30 30 30 30 30 30	 (1) 読む (注意) (注) (注) (注) (⊥) (⊥)		
編載 (105.16.28 - Port3 地理学功效量 (学行效量 可能で 106.16.228 - Port7 106.86.528 - Port7 106.86.528 - Port7 106.87.528 - Port7 106.87.528 - Port7 106.87.528 - Port7 106.87.528 - Port7 106.87.528 - Port7 106.87.528 - Port3 106.87.528 - Port3 106.87.558 - Port3 106.87.558 - Port3 107.87.578 - Port3 106.87.578 - Port3 106.87.578 - Port3 106.87.578 - Port3 106.878 - Port3 106.87	E L	▲ 	EX.MAR.CO BSC perct perct TO JSSE perct percent TO JSSE percent percent TO JSSE percent percent TO JSSE percent percent percent TO JSSE percent p	98 0 0 0	20 20 20 20 20 20 20 20 20 20 20 20 20 2	使用記 認識 認識 [19:146.228 - Pert 3 法庭院院 描述分析 描述分析 花園の院 花園の院 花園の院 花園の院 花園の院 花園の院		
	Ę	お数 の の 日空学止 名数 の	Kidda O BSD port2 port7 TO	Pil 0 0 0	A 88 20 20 20 20 20 20 20 20 20 20 20 20 20	(1) (1) (1) (1) (1) (1) (1) (1) (1)		
新築 168.16.228. Port3 地球電気度 学习取量 58.7 1981年223. Port7 28.8 29.8 29.8 29.8 29.8 29.8 29.8 29.8 20.8	, () t	ス 200 0 10 10 10 10 10 10 10 10 1	KideE の BE pro1 pro1 TO - 2540656 TO - 25406565	98 0 0 0	A M M M M M M M M M M M M M	セラストロージョン ビス (1) (2) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2		
Mit 在 108.16.228 - Rort 3 前所出版集 分析版集 108.16.228 - Rort 7 95時に応信 108.16.228 - Rort 7 95時に応信 108.16.228 - Rort 7 95時に応信 108.16.228 - Rort 7 95月に 108.16.228 - Rort 3 95月に 108.16.228 - Rort 3 95月に 108.15.228 - Rort 3 95月 108.15.228 - Rort 3 95月 108.15.228 - Rort 3 959 108.15.228 - Rort 3 959 108.15.228 - Rort 3 959 108.15.228 - Rort 3 959 108.15.258 - Rort 3 959 109.159 100.159 100.159 1	. (. (ム 	Kidda O BD port3 TO	Pil 0 0 0	A 88 20 20 20 20 20 20 20 20 20 20 20 20 20	セラルに 正応 第25.16.228.Ford3 に出版化 に出版化 102.156.16.228.Ford3 ドロルスペ 日本のの 日本の 日本	Rose	Ĕ
新算式 (148.16.228. Port3 相対能なの点 生学で形成 ・ ですていた。 ですででいた。 ですていた。 ですていた。 ですていた。	. (ت د د د د د د	く 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1	化価化の BE port 102 法の指定 103 法の指定 103 法の指定 104 法の指定 105 法の指定 105 法の計算 105 法の計算 105 法の計算 106 法の計算 107 法の注意	P8 0 0 0	A BB 20 20 20 20 20 20 20 20 20 20 20 20 20	elation set set set set set set set set		8



3. 用例运行结束,点击查看历史,可以查看测试报告。

Modbus 测试用户: admin	用例名称	Aodbus_TP_admin_3	20210120-16-31:46 运行结果:●成功 (重要衍史) (通信文件)					芥井
跟结果			状态			MISLE		
						· · · · · · · · · · · · · · · · · · ·		
2.168.16.228 - Port3	6910	222	应用层		^			
UDBUS_双述指示	1,976	122,512	(110 port3 port7			192.168.16.228 - Port3	砂值	
JDBUS_四座論家	-		And Areas			极文操改	1,976	122
. 100. 10.228 - PORT/	010	Sax		砂塘	SR	探文武法	2,223	138
	1 070	100	MODBUS_发送请求	1,976	122,512	192.168.16.228 - Port7	移植	
NOUS CONTRACTOR OF A	1,376	122,512	MODBUS_编校编程	1,976	122,512	报文接收	2,223	13
			MODBUS_晚空成场		122,512	报文发送	1,976	12
			MODBUS_购应异常		0			
			MODBUS_播放请求	1.976	122.512			
			MODBUS、周亞請求	1.976	122,512			
			MODBUS_请求释案	0	0			
165K 168.16.228 - Port3		- 50				1985 188		
168.16.228 - Port3		- 88				影然后 注意		
1683年 168.16.228 - Port3 前時代政治国 171111111						E社務設置 注意 192.168.16.228 - Port3		
6获 168.16.228 - Port3 2日初章 2日初章			化输尿 0			ELTRE 注意 192.168.16.228 - Port3 无型操作		
格获 168.16.228 - Port3 約證化改量 并行動量 順記		▲ 5数 0 0 ■回 日紹停止	代版記 0 영업 port port?		<u> </u>	 計算器 192.168.16.228 - Port3 注意等 注意等 		
相扶 168.16.228 - Port3 前提出政策 学行数量 順記 168.16.228 - Port7 時間: 6.228 - Port7			代始記 0 SR port port7		-	 ・記書 ・注意 ・注意 ・		
信氏 168.16.228 - Port3 前部北部語 新聞 電子 168.16.228 - Port7 時間(16.228 - Port7 時間(16.228 - Port7	1		代MAR © BR port3 port7	eg	SR	 · 日本市会 · 日本会 · 日本会		
信氏 168.16.228 - Port3 転換出改量 学行取量 電子 168.16.228 - Port7 取扱気改量 学行取量 MP	1		代地版 0 原作 por3 por7 T07主政府教会会	96 0	207	時期間 192.168.16.228 - Port3 近面地穴 近面地穴 万面地穴 万面地穴 万面状穴 万面状穴 万面状穴		
#获 168.16.228 - Port3 188.16.228 - Port3 188.16.228 - Port7 188.16.228 - Port7 188.16.288 - Port7 188.16.2	1	ク の の 三型)日成学止 参数 の の の の の の の の の の の の の	代始記 0 毎年 1907 30077 107 主体術をあら 170 主政術をあら 170 主政術をあら	98 0 0	600 247 247			
新鉄 168,16-228 - Port3 約約5020 学刊的量 第次 168,16-228 - Port7 約第5020 美 168,16-228 - Port7 約第5020 美 168,16-228 - Port7 約第5020 美 168,16-228 - Port3 169,16-228 - Port3 169,16-28	1	く ジン の 日日の学生 ジン の の の の の 日日の学生 日日の学生 の の の の の の の の の の の の の	代始版 の 回 の の の の の の の の の	Pa 0 0	4 4 247 247 247 247	 ●動配数 主要 192,163,16,228 - Port3 二面密吹 二面完吹 192,163,16,228 - Port7 二面完吹 二面完吹 二面完吹 		
新鉄 168.16.228 - Port3 新聞後起28 学行改量 学行改量 学行改量 学行改量 学行改量 通信 2.15	1			90 0 0 0	4 8 34 247 247 247 247	USAGE 注意 192.164.16.28 - Pert3 元数形式 可能形式 192.164.16.28 - Pert7 元数示式 用数分通		
格	,		代始版 の の の の の の の の の	Pa 0 0 0	A 68 247 247 247 247 247 247 247	 は数に はために 		
新天 196,16,238 - Port3 新聞来が急 学り取量 現在 196,16,238 - Port7 新聞来の 新聞の発 美術家 発 現代		ク 0 0 三回 日成停止 名数 0 0 三回 日紀停止		00 0 0 0	247 247 247 247 247 247 267 0	KS (Mat) KE ISS IS ISS IS I		,
MER: 198.16.228 - Port3 新聞祭328 新聞 198.16.228 - Port7 新聞祭328 学び取録 単で取録 第27	1	名数 0 0 三日の今止 名数 0 0 0 三日の今止	代始版 0 田(9013 9017 マッエスの称形在5 マッエスの称形在5 マッエスの称形在5 マッエスの称形在5 マッエスの称形在5 マッエスの称形在5 マッエスの称形在5 マッエスの称形の在5 マッエスのからのため マッエスのからのため マッエスのからのため マッエスのからのため マッエスのからのため	Pa 0 0 0	Α Απ 3σ 3σ 3σ 3σ 3σ 3σ 0 0	此数に 正成 一部の 一部の 一部の で 一 で 一 一 一 一 一 一 一 一 一 一 一 一 一		
新存 166.16.228 - Port3 1日間を知道 子が取曲 166.15.228 - Port7 回時完全級 子が取曲 単ない 制化 を 記 を 予約 の 10.15.228 - Port7 の 時代の 子がの し の 10.15 0 10.15 0 10 10 10 10 10 10 10 10 10 10 10 10 1	,	4数 0 0 10 10 10 10 10 10 10 10 10 10 10 10	KVIDE 0 BE port3 port7 TO 3.5084588 TO 3.5084588 TO 3.5084588 TO 3.5084588 TO 3.6084588 TO 3.6084588	89 0 0	A 30 30 30 30 30 30 0 0 0	此語に 「別」 日本		
新日本 164.16.228 - Port3 日前日にお加 新日本 新日本 新日本 新日本 新日本 新日本 新日本 新日本	,	よ 2000 1	代始版 0 医位 port3 port7 TO 生気物感音等 TO 生気が感音音 TO 生気が感音 TO 生気が感音音 TO 生気が感音 TO 生気が TO 生気 TO 生気が TO 生気 TO 生気 TO 生気 TO 生活 TO 生活	Pa 0 0 0	4 80 307 307 307 307 307 0 0 0 0 0 0 0	低計数は 田田 田 1	₩×××	
編長 198315228-Ford3 198315228-Ford3 2085 2085 2085 2085 2085 2085 2085 2085)) 45935		化価化の BE port3 port7 TO port8 port7	98 0 0 0	* *** *** *** *** *** *** *** ***	Statut UK 19510141223-Pert3 20205 2005 20	₩×≈₽	, , 187

4. 生成报告数据及 HTML/PDF/Word 报告, 报告生成后, 可以下载 HTML/PDF/Word 格 式测试报告

信息					
Modbus_TP_admin_20210120-16:31:46			用例类型 Modbus		
用户 admin			开始时间 2021-01-20 16:39:04		
結果 💿 测试运行正带结束			结束时间 2021-01-20 16:40:17		
数据					
再次运行 📄 生成报告 🗋 生成文档	म्इस्तिमाला 🔄 म्इस्ट्रिय 🕅	裁Word			回 删除此记
188 3月山 天城昭集 353					
	2012		作物已 (1997年)		
心用层 (应用管)	2718	28	传输层(会通知计	野債	en
RE3 3FL1 天間(6)第 343 应用层 (应用(6)力) MODBUS_发送请求	දහාම වැඩි 2.008	总数 122.512	传输层 (余颜明) TCP_主动病語连接	9년 4	总数 247
ADD 2010年 2010年 2019 成用层 (仮用約17) MODBUS、发送请求 MODBUS、发送请求	2008 2.008 2.008	2数 122.512 122.512	传输层 (約值 4 4	総数 247 247
(24) 3711 天曜16年 349 成旧居 (原用時行) MODBUS 支援演奏本 MODBUS 支援政務政 MODBUS 支援政務政	දනය එහිළි 2.008 2.008	2数 122.512 122.512 122.512	传输层 (<i>金透明计</i>) TCP 主动标准连接 TCP 生动体成连接 TCP 电动体成连接	9値 4 4	総数 247 247 247 247
RGE 2011日 天田20日本 2019 成用局 ((2)用除け) MODBUS 変統時年 MODBUS 変統時年 MODBUS 変統時年 MODBUS 変形常常	දහාම දිනාම 2.008 2.008	2280 122,512 122,512 122,512 122,512 0	传输层 (@3007) TCP 主动相连接 TCP 生动相连接 TCP 振动曲运接 TCP 振动曲动探索	10년 4 4 4	总数 247 247 247 247 247 247
(201 2011) 天田(12) 天田(12) (2011) (9%6 2.008 2.008 2.008	288 122,512 122,512 122,512 0 0 122,512	传输层 (金統計) 102 主动能能操 102 主动能能操 102 运动能能操 102 运动能能操 102 运动能动能是 102 运动能动性发展 102 运动能动性发展	196 4 4 4	総数 247 247 247 247 247 247
CG2 2011は 天地2013年 2499 成川用层 (広用除け) MODBUS 実活情末 MODBUS 実施50時 MODBUS 実施50時 MODBUS 実施50時末 MODBUS 実施50時末	Pe値 2,008 2,008 2,008 2,008 2,008 2,008	88 122,512 122,512 122,512 0 122,512 122,512		හයු 4 4 4	総数 247 247 247 247 247 247 247 0
	P96 2008 2008 2008 2008 2008 2008 0	88 122512 122512 122512 0 122512 122512 0	传输层 (金融社) TCP 主动相连接接 TCP 主动相连接接 TCP 运动相连接接 TCP 运动自动将发展量 TCP 运动自动将发展量 TCP 运动自动将发展面 TCP 运动和VK名和成功 TCP 运动和VK名和成功	998 4 4 4	総数 247 247 247 247 247 247 0 0 0
(2021 2011年 天地)に第二日 前用层 (近期後日) MODBUS 実施時年 MODBUS 実施時時 MODBUS 実施時年 MODBUS 実施時年 MODBUS 実施時年	9% 2,008 2,008 2,008 2,008 2,008 2,008 2,008 2,008	88 122.512 122.512 122.512 0 122.512 122.512 122.512 0		1968 4 4 4	総数 247 247 247 247 247 247 0 0 0 0
(2021 2月に) 未知 成用局 (症用物) MODBUS 実践構成 MODBUS 実験的解剖 MODBUS 現象的解剖 MODBUS 現象的構成 MODBUS 現象的構成 MODBUS 現象的構成 MODBUS 現象的構成 MODBUS 現象的解文	砂塘 2.008 2.008 2.008 2.008 2.008 2.008 0 0	88 122512 122512 122512 0 122512 122512 122512 0	传输展 (金5557) 107 主动和能振動 107 生动和能振動 107 単动和振動地 107 単动和振動地 107 単动和振動地 107 単动和振動地 107 単动和PAK動し 107 単动和PAK動し 107 単动和PAK動地 107 単动和PAK動地 107 単动和PAK動地	908 4 4 4	888 247 247 247 247 247 0 0 0 0 0 0 0
CG2 2011日 天田26日第 第9 前川田県 (近期をけ) MODBUS 実施時来 MODBUS 実施時来 MODBUS 実施時来 MODBUS 実施時来 MODBUS 講座時来	P96 2008 2008 2008 2008 2008 0	88 122512 122512 122512 122512 122512 122512 122512 0	传输展 (金融計) 「CP」主动物能活動 「CP」主动物能活動 「CP」主动物能活動 「CP」当応力体活動 「CP」当応力体活動 「CP」当応力体活動 「CP」当応力体活動 「CP」主动のために 「CP」」 「CP」主动のために 「CP」」 「CP」	606 4 4 4	830 247 247 247 247 247 0 0 0 0 0 0 0 0
	9% 2,008 2,008 2,008 2,008 2,008 2,008 2,008 2,008	88 122.512 122.512 122.512 0 122.512 122.512 0		99 6 4 4 4	830 247 247 247 247 247 0 0 0 0 0 0 0 37 372





4. 详解客户端读或写的指令

执行方法	选择所有 <u>取消所有</u>			
	 ○ 01读线圈状态 ○ 02读离散输入(触点)状态 ○ 03读保持寄存器数据 ○ 03读保持寄存器数据 ○ 04读输入寄存器数据 ○ 05写单个线圈状态 ○ 06写单个表存器数据 	01-06, 最常用	15,16为状态码, 的八种指令	是modbus协议中
	 ☑ 15写多个线圈状态 ☑ 16写多个寄存器数据 			

4.1 状态码 01 读线圈

起始地址	0	在什么位置开始读
	可用地址》	范围: 0 - 65,535
数量	10	连续读多少
	范围: 1 - 2	2,000, 且不大于可用地址数量 (可用地址数量 = 65536 - 起始地址)

4.2 状态码 02 读离散输入(触点)状态

02读离散输入(触点)状态	
起始地址	• 在哪里开始读 ^{可用地址范围: 0 - 65,535}
数量	10 <u> </u>
	确定取消



4.3 状态码 03 读保持寄存器数据

03读保持寄存器数据			
起始地址	0	在哪里开始读	
	可用地	址范围: 0 - 65,535	
数量	10	连续读多少	
	范围: 1	- 125, 且不大于可用地址数量	(可用地址数量 = 65536 - 起始地址)

4.4 状态码 04 读输入寄存器数据

04读输入寄存器数据		
起始地址	0 在哪里开始读 可用地址范围: 0 - 65,535	
数量	10 连续读多少 范围: 1 - 125, 且不大于可用地址数量 (可用地	址数量 = 65536 - 起始地址)

4.5 状态码 05 写单个线圈状态

05写单个线圈状态	
	超始地址 0 在哪里开始写 可用地址范围: 0 - 65,535
	下一步取消
05写单个线圈状态	
起始地址: 0, 数量: 1	
00000	
0 0 ~	
1 0	写0或1
2 1	
3	
4	
5	
6	_
7	-
8	-
9	

在 wireshark 中 16 进制 0 显示为 0000, 1 显示为 ff00;



4.6 状态码 06 写单个寄存器数据

06写单个寄存器数据		
起始地址		
数值类型	□用旭业已包围: U - 65,555 16位无符号整型 ~	无符号的取值可以为0到65535
	16位无符号整型 16位有符号整型 下一步 取消	有符号的取值可以为-32768到 32767

06写单个寄存器数据

起始地址: 0, 数量: 1, 数值类型: 16位无符号整型

30 	00000
0	<u> </u> 1
1	
2	
3	
4	
5	
6	
7	
8	
9	

在写单个寄存器数据中,无符号整型 0 的 16 进制表示法为 0000,65535 表示为 ffff;有 符号整型的 0 为 0000,1 为 0001,-1 为 ffff,-2 为 fffe;

4.7 状态码 15 写多个线圈状态

15写多个线圈状态	
起始地址数量	0 可用地址范围: 0 - 65,535 10
	范围: 1 - 2,000, 且不大于可用地址数量 (可用地址数量 = 65536 - 起始地址) 下一步 取消



15写多个线圈状态 起始地址: 0, 数量: 10 00000 0 1 ~ 写多个线圈,每个线圈写0或1 1 0 V 2 1 V 3 0 V 4 1 ~ 5 1 V 6 1 V 7 1 V 8 0 V 9 1 ~

在写多个线圈中,16进制的表示方法是需要计算得到的,如上图写1010111101这10个数字,每8位是1个字节,超出8位不足16位的在后面添加0到16位,也就变成1010111101000000,由于计算机写入时会把每8位都拿出来从后往前写即第一个8位11110101,第二个8位00000010,最后转换成16进制即f502;

4.8 状态码 16 写多个寄存器数据

16写多个寄存器数据		
起始地址	0	
	可用地址范围: 0 - 65,535	
数量	10	
	范围: 1 - 123, 且不大于可用地址数量	量(可用地址数量 = 65536 - 起始地址)
数值类型	16位无符号整型	
	16位无符号整型	16位32位64位分别代表在填入数据
	16位有符号整型	时占用几个小格子, 16占1个, 32
	32位无符号整型	占2个, 64占4个
	32位有符号整型	調状を 🕑
	64位无符号整型	
	64位有符号整型	TTTREAGE LD
	32位浮点类型	調状态 🕜
	64位双精度类型	



	起始地	址: 0, 数量: 10,	数值类型:	32位有符号整型
		00000		
ſ	0	1		
L	1			
	2	1		
	3			
	4	1		
	5			
	6	1		
	7			
	8	1		
	9			
			7	

起始地址	业: 0, 数量: 10,	数值类型:	64位无符号整型
	00000		
0	1		
1			
2			
3			
4	1		
5			
6			
7			
8			
9			

16 位无符号所填值的范围 0 到 65535

32 位无符号所填值的范围 0 到 6294967295

64 位无符号所填值的范围 0 到 18446744073709553000

16 位有符号所填值的范围-32768 到 32767

32 位有符号所填值的范围-2147483648 到 2147483647

64 位有符号所填值的范围-9223372036854776000 到 9223372036854776000



5. 服务器从站的配置

5.1 添加从站

依次点击,对象 -> Modbus 地址 -> 增加。单击增加,在弹出的配置选项中,编 辑 Modbus 配置选项,根据需要修改配置参数,然后点击保存,保存 Modbus 地址对象。服 务器端从站的设置与功能和主站的设置与功能类似,主站向从站写入和获取指令。

🚫 M测科技			v20.12.06 Supernova-88D
网络后州 Modbust	·····································		
物议代选项			
SSL证书要件 SSL证书要件 BSLI2746 Z36	E 197		
有效数原題	2019 / 70520707/006 AUTOMENSEDHEL, ANEOTOME, AUTOMO, AUTOMOUS 75/11100/006/201301/4		
TCLBIA:	5 G7	3405 509	and there is
城名地址列表 0	A CONTRACTOR CONTRACTOR OF	/ 43	R 1
安量列表 0 显示行数:	10 × 1-1 of 1		. (1) ».
HTTP事务列表 🕑			
TCP////#RE			
98(4)(38			
PCRPA380 (6)下ウ注			
ModbustRit			
文件现象			
羅斯日振対象			
网络协议路口研究 0			
防火爆振曲测试			
基本信息			
	对象名称 ModbusObject_20210120-16:45:49		
	· 田法子州回盟/AZ/8-2/10-9/1-1-/_(A-交团中又4/号)		
Modbus			
袁名	影响時往	数量	
奏名 姚面兴志表	起始地址 0	数屋 10	
表名 线圈状态表 触亦形态表	80mbs/ 0 0	政府 10 10	
教名 划画状态表 触点状态表 但时 有 口器表	8280004 0 0	8%88 10 10 10	
素名 (4回)大印表 記が代わ来 (1)代本の指表 知られたの来 (1)人本の指示	8285664 0 0 0 0	8%8 10 10 10 10	**************************************
秦公 《國內法法 他们的边面 《回外路78章 載 》、西門國政	8285864 0 0 0 0 0	8%9 10 10 10 10 10 10 10 10 10 10 10 10 10	10日 10日 10日 10日 10日 10日 10日 10日
教名 (4回)(10天 (10)(145)(155) (10)(145)(155) (155)(155)(155)(155) (155)(155)(ICG 10 10 10 10	
教名 (編末の表 総合がある (保持条句話表 紙入表句語表	8281004 0 0 0 0 0 0 0 0	IX4 10 10 10 10	**************************************
教社 (3周代の後 記のだの周 (25年55日前後 記入後79日前後	8384642 0 0 0 0 0 0 0 0 0 0 0 0 0	RM 10 10 10 10	
表記 (編末)(古書 泉水赤沙漠市 泉水赤沙漠市 泉水赤沙漠市	838/84/ 0 0 0 0 0 0 0 0 0 0 0 0 0	8% 10 10 10 10 10 10 10 10 10 10 10 10 10	
表名 (編末公表 熱析が必須 風外振う発表 記入振行接表 記入振行接表	828/84/ 0 0 0 0 0 0 0 0 0 0 0 0 0	80 10 10 10 10 10 10 10 10 10 10 10 10 10	******** / / /
案名 (昭秋の時 総介化の度 (紀今年の22後 (紀)、法示理論 (紀)、法示理論		X ₩ 10 10 10 10	
名名 名名 総称な成本 総称な成本 総称な成本 総かな成本 総かなの本 総かる 総かなの本 総かる の 総かなの本 の の の の の の の の の		X ₩ 10 10 10 10	
		ECC 10 10 19 10 10	
教名 教授(安)表 教授(安)表 第5件会学習後 第二年(百日)	EXHAUL 0 0 0 0 0 0 0	KH 10 10 10 10	
表名 (4周秋の後 秋日水のあ (日秋日本) 日水中の日本 日水中の日本 赵本小信四 日本 秋日 日本		RH 10 10 10 10 10	
表名 (昭和の後年) 昭和の後年 (昭和の後年) 第二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十二十	S264.001 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2010120101201043040 0 20101201043040,021/01/01/01/01/01/01/01/01/01/01/01/01/01	Re 10 10 10 10	
家名 総計状態 総計状態 総計状態 総計状態 総計状態 総計状態 総計状態 近年登録 総計状態 近年登録 総計状態 近年登録 総計状態 近年登録 総計状態 近年登録 総計状態 近日状態 総計状態 近日状態 総計状態 原料 総計状態 原料 総計状態 原料 総計状態 原料 総計状態		RM 10 10 10 10	
総合		I0 I0 I0 I0 I0	
家名 ((四)(今点 紀元(公点 ((回)(今点 紀元(公点 ((回)(今点 紀元(公点 ((回)(今点 麗志 ((回)(今点 麗志 ((回)(今点 龍元(四)(四)(四) ((回)(四)(四)(四)(四)(四)(四)(四)(四)(四)(四)(四)(四)(四)		Rel 10 10 10 10	
表名 (昭文の書) 記のでの面 (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)		RM 10 10 10 10 10	
表名 製品がなる。 製作用の温泉、 メニア活用	Skiteli 0 0 0 0 0 0 0	RM 10 10 10 10	



5.2 下载 Pcap 报文验证

用例配置中,设置开启报文捕获

用例名称 Modbus	TP_admin_20210 E:A-Z/a-z/0-9/:	120-16:31:46 /・/_(不支持中文符号)		第5日 年(11分秒)	0 Rittmentchemer, Rittri	1 : 0 K74858822999/NJ	
网络 参数 客户端 路设置 户端 vr3	服务器			服务端			
*897977							100000000000000000000000000000000000000
CPU核缩定			MAC 00.91.00.0340.34	CPUIKING			MAC 00.91.00.03.2
	CPU被ID	4 CPU核期空可造ID为0.1.2.3.4.5.6.7.8.9 远路多个标时,谨使用完文,"分割, 不同满口不能使用相同的CPU核, 为了系统规定和增益精确, 建议留两个核0.1给系统U及数据率			CPU總D	8 CPU統領亞可語的为点1.2.3.4.5.6.7.8.9 選擇多个條則、資使用這的たい比較。 为了系統是並可能結構編。 建议習幣个核回、始系明以及数量庫	
政連续				报文捕获			
	协议类型 IP地址	全部 連击控制说的类型。无表示不高用抓包 测P地址或者目的P地址,例如17.1.1.2			协议类型		
	第日 Pcap文件大小	環境口式20世界的第二,例5080			第日 Pcap文件大小	現新口北京都 目的5時口,例6080	
	捕获包数	pcap又件大小、0 - 2000MB (新小小) 50000 范囲: 0 - 6000000 (低认)	用例配置中设置开启报文捕获	茨	捕获包数	pcap文件大小、0 - 2000MB (第5人) 50000 范囲: D - 6000000 (第5人)	
率与MAC 			Exa	速本与MAC			
刘运行结朱,	▶ 毛	, Pcap / k 🗴	Y Agin				v20.12.06 Supernova-8
			目前没有正在 www.file.144.15.28 pertured www.file.144.28 pertured www.file.144.28 pertured www.file.144.28 pertured	运行的测试			

通过 Wireshark 打开, 查看验证运行结果

9 2.000599	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	0;	Unit:	0,	Func:	1:	Read Coils	
10 2.000660	17.1.1.100	17.1.2.2	Modbus/TCP	65 Res	sponse:	Trans:	0; 1	Unit:	0,	Func:	1:	Read Coils	
11 2.000663	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	1;	Unit:	0,	Func:	2	Read Discrete Inputs	
12 2.000674	17.1.1.100	17.1.2.2	Modbus/TCP	65 Res	sponse:	Trans:	1;	Unit:	0,	Func:	2	Read Discrete Inputs	
13 2.000676	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	2; 1	Unit:	0,	Func:	3	Read Holding Registers	
14 2.000743	17.1.1.100	17.1.2.2	Modbus/TCP	83 Res	sponse:	Trans:	2; 1	Unit:	0,	Func:	3	Read Holding Registers	
15 2.000745	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	3; 1	Unit:	0,	Func:	4	Read Input Registers	
16 2.000755	17.1.1.100	17.1.2.2	Modbus/TCP	83 Res	sponse:	Trans:	3; 1	Unit:	0,	Func:	4	Read Input Registers 仄念	码和对应的名称
17 2.000757	17.1.2.2	17.1.1.100	Modbus/TCP	69	Query:	Trans:	4; 1	Unit:	0,	Func:	15	Write Multiple Coils	
18 2.000767	17.1.1.100	17.1.2.2	Modbus/TCP	66 Res	sponse:	Trans:	4; 1	Unit:	0,	Func:	15	Write Multiple Coils	
19 2.000769	17.1.2.2	17.1.1.100	Modbus/TCP	313	Query:	Trans:	5; 1	Unit:	0,	Func:	16	Write Multiple Registers	
20 2.000828	17.1.1.100	17.1.2.2	Modbus/TCP	66 Res	sponse:	Trans:	5; 1	Unit:	0,	Func:	16	Write Multiple Registers	
21 2.000831	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	6; 1	Unit:	0,	Func:	5	Write Single Coil	
22 2.000840	17.1.1.100	17.1.2.2	Modbus/TCP	66 Res	sponse:	Trans:	6; 1	Unit:	0,	Func:	5	Write Single Coil	
23 2.000843	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	7; 1	Unit:	0,	Func:	6	Write Single Register	
24 2.000852	17.1.1.100	17.1.2.2	Modbus/TCP	66 Res	sponse:	Trans:	7; 1	Unit:	0,	Func:	6	Write Single Register	
25 2.020830	17.1.2.2	17.1.1.100	TCP	60 100	000 + 50	2 [ACK] Seq	=34	7 Ack=12	29 W	lin=655	35 I	en=0	

9 2.000599	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 0; Unit:	0, Func: 1: Read Coils
10 2.000660	17.1.1.100	17.1.2.2	Modbus/TCP	65 Response: Trans: 0; Unit:	0, Func: 1: Read Coils
11 2.000663	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 1; Unit:	0, Func: 2: Read Discrete Inputs
12 2.000674	17.1.1.100	17.1.2.2	Modbus/TCP	65 Response: Trans: 1; Unit:	0, Func: 2: Read Discrete Inputs
13 2.000676	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 2; Unit:	0, Func: 3: Read Holding Registers
14 2.000743	17.1.1.100	17.1.2.2	Modbus/TCP	83 Response: Trans: 2; Unit:	0, Func: 3: Read Holding Registers
15 2.000745	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 3; Unit:	0, Func: 4: Read Input Registers
16 2.000755	17.1.1.100	17.1.2.2	Modbus/TCP	83 Response: Trans: 3; Unit:	0, Func: 4: Read Input Registers
17 2.000757	17.1.2.2	17.1.1.100	Modbus/TCP	69 Query: Trans: 4; Unit:	0, Func: 15: Write Multiple Coils
18 2.000767	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 4; Unit:	0, Func: 15: Write Multiple Coils
19 2.000769	17.1.2.2	17.1.1.100	Modbus/TCP	313 Query: Trans: 5; Unit:	0, Func: 16: Write Multiple Registers
20 2.000828	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 5; Unit:	0, Func: 16: Write Multiple Registers
21 2.000831	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 6; Unit:	0, Func: 5: Write Single Coil
22 2.000840	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 6; Unit:	0, Func: 5: Write Single Coil
23 2.000843	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 7; Unit:	0, Func: 6: Write Single Register
24 2.000852	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 7; Unit:	0, Func: 6: Write Single Register
25 2.020830	17.1.2.2	17.1.1.100	TCP	60 10000 → 502 [ACK] Seq=347 Ack=	29 Win=65535 Len=0

 25 2.220830
 17.1.2.2
 17.1.1.100
 TCP
 60 10000

 Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 Ethernet 11, 5cr: Xteam_{12}7:3:32 (00:16:31:6;76:33), Dst: Xteam_{2}7:3:34 (00:16:31:6;26:33)

 Internet Protocol Version 4, Src: 17.1.2.2, Dst: 17.1.1.100
 Transmission Control Protocol, Src Port: 10000, Dst Port: 502, Seq: 1, Ack: 1, Len: 12

 Modbus/TCP
 Modbus
 .0000 0001 = Function Code: Read Colls (1)

 Reference Number: 0
 Bit Count: 10



主站向从站发起获取指令,在0的位置开始连续读10个

• 9 2.000599	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	0;	Unit:	0,	Func:	1: Read Coils
10 2.000660	17.1.1.100	17.1.2.2	Modbus/TCP	65 R	esponse:	Trans:	0;	Unit:	0,	Func:	1: Read Coils
11 2.000663	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	1;	Unit:	0,	Func:	2: Read Discrete Inputs
12 2.000674	17.1.1.100	17.1.2.2	Modbus/TCP	65 R	esponse:	Trans:	1;	Unit:	0,	Func:	2: Read Discrete Inputs
13 2.000676	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	2;	Unit:	0,	Func:	3: Read Holding Registers
14 2.000743	17.1.1.100	17.1.2.2	Modbus/TCP	83 R	esponse:	Trans:	2;	Unit:	0,	Func:	3: Read Holding Registers
15 2.000745	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	3;	Unit:	0,	Func:	4: Read Input Registers
16 2.000755	17.1.1.100	17.1.2.2	Modbus/TCP	83 R	esponse:	Trans:	3;	Unit:	0,	Func:	4: Read Input Registers
17 2.000757	17.1.2.2	17.1.1.100	Modbus/TCP	69	Query:	Trans:	4;	Unit:	0,	Func:	15: Write Multiple Coils
18 2.000767	17.1.1.100	17.1.2.2	Modbus/TCP	66 R	esponse:	Trans:	4;	Unit:	0,	Func:	15: Write Multiple Coils
19 2.000769	17.1.2.2	17.1.1.100	Modbus/TCP	313	Query:	Trans:	5;	Unit:	0,	Func:	16: Write Multiple Registers
20 2.000828	17.1.1.100	17.1.2.2	Modbus/TCP	66 R	esponse:	Trans:	5;	Unit:	0,	Func:	16: Write Multiple Registers
21 2.000831	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	6;	Unit:	0,	Func:	5: Write Single Coil
22 2.000840	17.1.1.100	17.1.2.2	Modbus/TCP	66 R	esponse:	Trans:	6;	Unit:	0,	Func:	5: Write Single Coil
23 2.000843	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	7;	Unit:	0,	Func:	6: Write Single Register
24 2.000852	17.1.1.100	17.1.2.2	Modbus/TCP	66 R	esponse:	Trans:	7;	Unit:	0,	Func:	6: Write Single Register
25 2.020830	17.1.2.2	17.1.1.100	TCP	60 1	0000 ÷ 54	02 [ACK]	Seq=3	47 Ack=	129 1	vin=655	35 Len=0
<pre>> Frame 10: 65 byte: on wire (520 bits), 66 bytes captured (520 bits) > Ethernet II, Sr:: Kteam_f2:f3:34 (00:16:31:f2:f3:34), DSt: Kteam_f2:f3:35 (00:16:31:f2:f3:35) > Internet Protocol Version 4, Sr:: 17.1.106, Dst: 17.1.2.2 > Transmission Control Protocol, Src Port: 502, Dst Port: 10000, Seq: 1, Ack: 13, Len: 11 > Modbus/TCP > Modbus 000 0001 = Function Code: Read Colls (1) </pre>											
Daca, 0805	Data: da03										

从站回复指令,下图是从站相对应的设置

线圈状态表

起始地址: 0, 数量: 10

	000	00
0	0	~
1	1	~
2	0	~
3	1	~
4	1	~
5	0	~
6	1	~
7	1	~
8	1	~
9	1	~

1	11 2.000663	1/.1.2.2	17.1.1.100	Modbus/ICP	66 Query: Trans: 1; Unit: 0, Func: 2: Read Discrete Inputs	
	12 2.000674	17.1.1.100	17.1.2.2	Modbus/TCP	65 Response: Trans: 1; Unit: 0, Func: 2: Read Discrete Inputs	
	13 2.000676	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 2; Unit: 0, Func: 3: Read Holding Registers	
	14 2.000743	17.1.1.100	17.1.2.2	Modbus/TCP	83 Response: Trans: 2; Unit: 0, Func: 3: Read Holding Registers	
	15 2.000745	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 3; Unit: 0, Func: 4: Read Input Registers	
	16 2.000755	17.1.1.100	17.1.2.2	Modbus/TCP	83 Response: Trans: 3; Unit: 0, Func: 4: Read Input Registers	
	17 2.000757	17.1.2.2	17.1.1.100	Modbus/TCP	69 Query: Trans: 4; Unit: 0, Func: 15: Write Multiple Coils	
	18 2.000767	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 4; Unit: 0, Func: 15: Write Multiple Coils	
	19 2.000769	17.1.2.2	17.1.1.100	Modbus/TCP	313 Query: Trans: 5; Unit: 0, Func: 16: Write Multiple Registers	
	20 2.000828	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 5; Unit: 0, Func: 16: Write Multiple Registers	
	21 2.000831	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 6; Unit: 0, Func: 5: Write Single Coil	
	22 2.000840	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 6; Unit: 0, Func: 5: Write Single Coil	
	23 2.000843	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans: 7; Unit: 0, Func: 6: Write Single Register	
	24 2.000852	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans: 7; Unit: 0, Func: 6: Write Single Register	
	25 2.020830	17.1.2.2	17.1.1.100	TCP	60 10000 → 502 [ACK] Seq=347 Ack=129 Win=65535 Len=0	

 25 2.020830 17.1.2.2
 17.1.1.100
 TCP
 60 10000

 Frame 12: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
 Ethernet II, 5rc: Xteam_f2:f3:34 (0:16:31:f2:f3:35)

 Internet Protocol Version 4, Src: 17.1.1.100, Dst: 17.1.2.2
 Transmission Control Protocol, Src Port: 502, Dst Port: 10000, Seq: 12, Ack: 25, Len: 11

 Modbus/TCP
 Modbus

 .000 0010 = Function Code: Read Discrete Inputs (2)

 IRequest Frame: 11]

 Byte Count: 2

 Data: ed03



从站回复指令,下图是从站相对应的设置

触点状态表

起始地址: 0, 数量: 10

	00000)
0	1 ~	-
1	0 ~	-
2	1 ~	-
3	1 ~	-
4	0 ~	-
5	1 ~	-
6	1 ~	
7	1 ~	
8	1 ~	
9	1 ~	-

13 2.001359	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	2;	Unit:	0,	Func:	3:	Read Holding Registers
14 2.001369	17.1.1.100	17.1.2.2	Modbus/TCP	83 Res	ponse:	Trans:	2; 1	Unit:	0,	Func:	3:	Read Holding Registers
15 2.001371	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	3; 1	Unit:	0,	Func:	4:	Read Input Registers
16 2.001428	17.1.1.100	17.1.2.2	Modbus/TCP	83 Res	ponse:	Trans:	3; 1	Unit:	0,	Func:	4:	Read Input Registers
17 2.001431	17.1.2.2	17.1.1.100	Modbus/TCP	69	Query:	Trans:	4; 1	Unit:	0,	Func:	15:	Write Multiple Coils
18 2.001440	17.1.1.100	17.1.2.2	Modbus/TCP	66 Re:	ponse:	Trans:	4; 1	Unit:	0,	Func:	15:	Write Multiple Coils
19 2.001443	17.1.2.2	17.1.1.100	Modbus/TCP	313	Query:	Trans:	5; 1	Unit:	0,	Func:	16:	Write Multiple Registers
20 2.001454	17.1.1.100	17.1.2.2	Modbus/TCP	66 Re:	ponse:	Trans:	5; 1	Unit:	0,	Func:	16:	Write Multiple Registers
21 2.001456	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	6; 1	Unit:	0,	Func:	5:	Write Single Coil
22 2.001513	17.1.1.100	17.1.2.2	Modbus/TCP	66 Re:	ponse:	Trans:	6; 1	Unit:	0,	Func:	5:	Write Single Coil
23 2.001516	17.1.2.2	17.1.1.100	Modbus/TCP	66	Query:	Trans:	7; 1	Unit:	0,	Func:	6:	Write Single Register
24 2.001525	17.1.1.100	17.1.2.2	Modbus/TCP	66 Res	ponse:	Trans:	7;	Unit:	0,	Func:	6:	Write Single Register
25 2.021481	17.1.2.2	17.1.1.100	TCP	60 100	00 + 50	2 [ACK] Seq	=34	7 Ack=1	29 W	in=6553	35 L	en=0

25.021481 17.1.2.2 [Request Frame: 13] Byte Count: 20 Register 0 (UNIT6): 1238 Register 1 (UNIT6): 1238 Register 2 (UNIT6): 0255 Register 3 (UNIT6): 04 Register 5 (UNIT6): 04 Register 7 (UNIT6): 06 Register 9 (UNIT6): 07 Register 9 (UNI

由于是32位所以会有多一位的占位

从站回复指令,下图是从站相对应的设置

保持寄存器表

起始地址: 0, 数量: 10, 数值类型: 32位无符号整型

	00000
0	1238
1	
2	12
3	
4	6295
5	
6	12
7	
8	144
9	

15 2.001371	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans:	3; Unit:	0, Func:	4: Read Input Registers
16 2.001428	17.1.1.100	17.1.2.2	Modbus/TCP	83 Response: Trans:	3; Unit:	0, Func:	4: Read Input Registers
17 2.001431	17.1.2.2	17.1.1.100	Modbus/TCP	69 Query: Trans:	4; Unit:	0, Func:	15: Write Multiple Coils
18 2.001440	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans:	4; Unit:	0, Func:	15: Write Multiple Coils
19 2.001443	17.1.2.2	17.1.1.100	Modbus/TCP	313 Query: Trans:	5; Unit:	0, Func:	16: Write Multiple Registers
20 2.001454	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans:	5; Unit:	0, Func:	16: Write Multiple Registers
21 2.001456	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans:	6; Unit:	0, Func:	5: Write Single Coil
22 2.001513	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans:	6; Unit:	0, Func:	5: Write Single Coil
23 2.001516	17.1.2.2	17.1.1.100	Modbus/TCP	66 Query: Trans:	7; Unit:	0, Func:	6: Write Single Register
24 2.001525	17.1.1.100	17.1.2.2	Modbus/TCP	66 Response: Trans:	7; Unit:	0, Func:	6: Write Single Register
25 2.021481	17.1.2.2	17.1.1.100	ТСР	60 10000 → 502 [ACK]	Seq=347 Ack=1	29 Win=655	35 Len=0
[Request Frame:	15]						
D I C I 20							

 IRequest Frame: 151

 Byte Count: 20

 Register 0 (UINT16): 65535

 Register 1 (UINT16): 6

 Register 2 (UINT16): 123

 Register 3 (UINT16): 123

 Register 4 (UINT16): 1

 Register 5 (UINT16): 1

 Register 6 (UINT16): 1

 Register 7 (UINT16): 1

 Register 7 (UINT16): 1

 Register 9 (UINT16): 1