

Configuring MODBUS TCP

This chapter provides the following sections:

- Understanding MODBUS TCP, on page 1
- Configuring the Router as the MODBUS TCP Server, on page 3
- MODBUS TCP Registers, on page 3

Understanding MODBUS TCP

Use Modicon Communication Bus (MODBUS) TCP over an Ethernet network when connecting the router to devices such as intelligent electronic devices (IEDs), distributed controllers, substation routers, Cisco IP Phones, Cisco Wireless Access Points, and other network devices such as redundant substation routeres.

MODBUS is a serial communications protocol for client-server communication between a router (server) and a device in the network running MODBUS client software (client). You can use MODBUS to connect a computer to a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

The client can be an IED or a human machine interface (HMI) application that remotely configure and manage devices running MODBUS TCP. The router functions as the server.

The router encapsulates a request or response message in a MODBUS TCP application data unit (ADU). A client sends a message to a TCP port on the router. The default port number is 502.

Note For information about the registers that a client can query on the router that functions as a MODBUS TCP server, see MODBUS TCP Registers, on page 3.

MODBUS and Security

If a firewall or other security services are enabled, the router TCP port might be blocked, and the router and the client cannot communicate.

If a firewall and other security services are disabled, a denial-of-service attack might occur on the router.

To configure quality of service (QoS) to set the rate-limit for MODBUS TCP traffic, create an access-list that only permits traffic sending to port number 502 that is reserved for MODBUS communication. Then attach the access-list to the input class-map and attach it to the interface and set the rate limit to permit traffic via default port 502 and prioritize SCADA packets.

```
DUT-1:
!
class-map match-any Modbus-out-Traffic
 match qos-group 1
class-map match-any Modbus-In-Traffic
 match access-group 101
!
policy-map Modbus-In
 class Modbus-In-Traffic
  set qos-group 1
policy-map Modbus-Out
 class Modbus-out-Traffic
  police 10000000
  priority
!
!
interface GigabitEthernet0/1/1
 switchport mode access
 service-policy input Modbus-In
!
interface GigabitEthernet0/1/2
 switchport mode access
 service-policy output Modbus-Out
!
!
interface Vlan1
 no ip address
 ip access-group 101 in
 rate-limit input access-group 101 8000 8000 8000 conform-action transmit exceed-action
drop
!
!
!
access-list 101 permit tcp 10.10.10.0 0.0.0.255 any eq 502

DUT-2:

interface Vlan1
 ip address 192.168.1.2 255.255.255.0
```

This example shows that 133 SCADA packets were classified.

```
DUT-1#show policy-map interface GigabitEthernet0/1/2
 GigabitEthernet0/1/2
  Service-policy output: Modbus-Out
    Class-map: Modbus-out-Traffic (match-any)
      133 packets
      Match: qos-group 1
      police cir 10000000 bc 312500
         conform-action transmit
         exceed-action drop
      conform: 133 (packets) exceed: 0 (packets)
        Priority
      Output Queue:
        Max queue-limit default threshold: 272
        Tail Packets Drop: 0
```

Multiple Request Messages

The router can receive multiple request messages from clients and respond to them simultaneously.

You can set the number of client connections from 1 to 5. The default is 1.

Configuring the Router as the MODBUS TCP Server

Defaults

The router is not configured as a MODBUS TCP server.

The TCP port number is 502.

The number of simultaneous connection requests is 1.

Enabling MODBUS TCP on the Switch

Beginning in privileged EXEC mode:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enter global configuration mode.
Step 2	**scada modbus tcp server**	Enables MODBUS TCP on the router.
Step 3	**scada modbus tcp server** [**port** *tcp-port-number*]	(Optional) Sets the TCP port to which clients send messages. The range for *tcp-port-number* is 1 to 65535. The default is 502.
Step 4	**scada modbus tcp server** [**connection** *connection-requests*]	(Optional) Sets the number of simultaneous connection requests sent to the router. The range for *connection-requests* is 1 to 5. The default is 1.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

To disable MODBUS on the router and return to the default settings, enter the **no scada modbus tcp server** global configuration command.

To add security when using MODBUS TCP, configure an ACL to permit traffic from specific clients or configure QoS to rate-limit traffic.

MODBUS TCP Registers

This section lists the read-only MODBUS registers. MODBUS clients use them to communicate with a MODBUS server (i.e., the IR8340 router). There are no writable registers.

System Information Registers

Memory address spaces 0x0800 through 0x0FFF are system information registers. Clients use the 0x03 Read Multiple Registers MODBUS function code. The system-information register mapping is as follows:

Table 1: System Information Registers

Address	# of Registers	Description	R/W	Format
0x0800	64	Product ID	R	Text
0x0840	64	Software image name	R	Text
0x0880	64	Software image version	R	Text
0x08C0	64	Host name	R	Text
0x0900	1	Number of Gigabit Ethernet ports	R	Uint16
CPU Core Temperature Related Registers				
0x0901	1	CPU core-0 temperature (in Celsius)	R	Uint16
0x0902	1	CPU core-1 temperature (in Celsius)	R	Uint16
0x0903	1	CPU core-2 temperature (in Celsius)	R	Uint16
0x0904	1	CPU core-3 temperature (in Celsius)	R	Uint16
0x0905	1	CPU core-4 temperature (in Celsius)	R	Uint16
0x0906	1	CPU core-5 temperature (in Celsius)	R	Uint16
0x0907	1	CPU core-6 temperature (in Celsius)	R	Uint16
0x0908	1	CPU core-7 temperature (in Celsius)	R	Uint16

Port Information Registers

Memory address spaces 0x1000 through 0x3FFF are read-only interface registers. Clients use the 0x03 Read Multiple Registers MODBUS function code to access the registers.

The following table shows the memory map for all interface registers, with 64-bit counters (address space 0x1000 – 0x2FFF, 8K registers):

Table 2: System Information Registers

Address	# of Registers	Description	R/W	Format
0x1000	64	WAN Port 1 name	R	Text
0x1040	64	WAN Port 2 name	R	Text
0x1080	64	LAN Port 1 name	R	Text
0x10C0	64	LAN Port 2 name	R	Text
0x1100	64	LAN Port 3 name	R	Text
0x1140	64	LAN Port 4 name	R	Text
0x1180	64	LAN Port 5 name	R	Text
0x11C0	64	LAN Port 6 name	R	Text
0x1200	64	LAN Port 7 name	R	Text
0x1240	64	LAN Port 8 name	R	Text
0x1280	64	LAN Port 9 name	R	Text
0x12C0	64	LAN Port 10 name	R	Text
0x1300	64	LAN Port 11 name	R	Text
0x1340	64	LAN Port 12 name	R	Text
0x1380	1	WAN Port 1 state	R	Uint16
0x1381	1	WAN Port 2 state	R	Uint16
0x1382	1	LAN Port 1 state	R	Uint16
0x1383	1	LAN Port 2 state	R	Uint16
0x1384	1	LAN Port 3 state	R	Uint16
0x1385	1	LAN Port 4 state	R	Uint16
0x1386	1	LAN Port 5 state	R	Uint16
0x1387	1	LAN Port 6 state	R	Uint16
0x1388	1	LAN Port 7 state	R	Uint16
0x1389	1	LAN Port 8 state	R	Uint16
0x138A	1	LAN Port 9 state	R	Uint16
0x138B	1	LAN Port 10 state	R	Uint16

Address	# of Registers	Description	R/W	Format
0x138C	1	LAN Port 11 state	R	Uint16
0x138D	1	LAN Port 12 state	R	Uint16
Values for 64-Bit Counters				
0x138E	4	WAN Port 1 Statistics – Number of packets received	R	Uint64
0x1392	4	WAN Port 2 Statistics – Number of packets received	R	Uint64
0x1396	4	LAN Port 1 Statistics – Number of packets received	R	Uint64
0x139A	4	LAN Port 2 Statistics – Number of packets received	R	Uint64
0x139E	4	LAN Port 3 Statistics – Number of packets received	R	Uint64
0x13A2	4	LAN Port 4 Statistics – Number of packets received	R	Uint64
0x13A6	4	LAN Port 5 Statistics – Number of packets received	R	Uint64
0x13AA	4	LAN Port 6 Statistics – Number of packets received	R	Uint64
0x13AE	4	LAN Port 7 Statistics – Number of packets received	R	Uint64
0x13B2	4	LAN Port 8 Statistics – Number of packets received	R	Uint64
0x13B6	4	LAN Port 9 Statistics – Number of packets received	R	Uint64
0x13BA	4	LAN Port 10 Statistics – Number of packets received	R	Uint64

Address	# of Registers	Description	R/W	Format
0x13BE	4	LAN Port 11 Statistics – Number of packets received	R	Uint64
0x13C2	4	LAN Port 12 Statistics – Number of packets received	R	Uint64
0x13C6	4	WAN Port 1 Statistics – Number of packets sent	R	Uint64
0x13CA	4	WAN Port 2 Statistics – Number of packets sent	R	Uint64
0x13CE	4	LAN Port 1 Statistics – Number of packets sent	R	Uint64
0x13D2	4	LAN Port 2 Statistics – Number of packets sent	R	Uint64
0x13D6	4	LAN Port 3 Statistics – Number of packets sent	R	Uint64
0x13DA	4	LAN Port 4 Statistics – Number of packets sent	R	Uint64
0x13DE	4	LAN Port 5 Statistics – Number of packets sent	R	Uint64
0x13E2	4	LAN Port 6 Statistics – Number of packets sent	R	Uint64
0x13E6	4	LAN Port 7 Statistics – Number of packets sent	R	Uint64
0x13EA	4	LAN Port 8 Statistics – Number of packets sent	R	Uint64
0x13EE	4	LAN Port 9 Statistics – Number of packets sent	R	Uint64
0x13F2	4	LAN Port 10 Statistics – Number of packets sent	R	Uint64

Address	# of Registers	Description	R/W	Format
0x13F6	4	LAN Port 11 Statistics – Number of packets sent	R	Uint64
0x13FA	4	LAN Port 12 Statistics – Number of packets sent	R	Uint64
0x13FE	4	WAN Port 1 Statistics – Number of bytes received	R	Uint64
0x1402	4	WAN Port 2 Statistics – Number of bytes received	R	Uint64
0x1406	4	LAN Port 1 Statistics – Number of bytes received	R	Uint64
0x140A	4	LAN Port 2 Statistics – Number of bytes received	R	Uint64
0x140E	4	LAN Port 3 Statistics – Number of bytes received	R	Uint64
0x1412	4	LAN Port 4 Statistics – Number of bytes received	R	Uint64
0x1416	4	LAN Port 5 Statistics – Number of bytes received	R	Uint64
0x141A	4	LAN Port 6 Statistics – Number of bytes received	R	Uint64
0x141E	4	LAN Port 7 Statistics – Number of bytes received	R	Uint64
0x1422	4	LAN Port 8 Statistics – Number of bytes received	R	Uint64
0x1426	4	LAN Port 9 Statistics – Number of bytes received	R	Uint64
0x142A	4	LAN Port 10 Statistics – Number of bytes received	R	Uint64

Address	# of Registers	Description	R/W	Format
0x142E	4	LAN Port 11 Statistics – Number of bytes received	R	Uint64
0x1432	4	LAN Port 12 Statistics – Number of bytes received	R	Uint64
0x1436	4	WAN Port 1 Statistics – Number of bytes sent	R	Uint64
0x143A	4	WAN Port 2 Statistics – Number of bytes sent	R	Uint64
0x143E	4	LAN Port 1 Statistics – Number of bytes sent	R	Uint64
0x1442	4	LAN Port 2 Statistics – Number of bytes sent	R	Uint64
0x1446	4	LAN Port 3 Statistics – Number of bytes sent	R	Uint64
0x144A	4	LAN Port 4 Statistics – Number of bytes sent	R	Uint64
0x144E	4	LAN Port 5 Statistics – Number of bytes sent	R	Uint64
0x1452	4	LAN Port 6 Statistics – Number of bytes sent	R	Uint64
0x1456	4	LAN Port 7 Statistics – Number of bytes sent	R	Uint64
0x145A	4	LAN Port 8 Statistics – Number of bytes sent	R	Uint64
0x145E	4	LAN Port 9 Statistics – Number of bytes sent	R	Uint64
0x1462	4	LAN Port 10 Statistics – Number of bytes sent	R	Uint64

Address	# of Registers	Description	R/W	Format
0x1466	4	LAN Port 11 Statistics – Number of bytes sent	R	Uint64
0x146A	4	LAN Port 12 Statistics – Number of bytes sent	R	Uint64
Values for 32-Bit Counters				
0x146E	2	WAN Port 1 Statistics – Number of packets received	R	Uint32
0x1470	2	WAN Port 1 Statistics – Number of packets received	R	Uint32
0x1472	2	LAN Port 1 Statistics – Number of packets received	R	Uint32
0x1474	2	LAN Port 2 Statistics – Number of packets received	R	Uint32
0x1476	2	LAN Port 3 Statistics – Number of packets received	R	Uint32
0x1478	2	LAN Port 4 Statistics – Number of packets received	R	Uint32
0x147A	2	LAN Port 5 Statistics – Number of packets received	R	Uint32
0x147C	2	LAN Port 6 Statistics – Number of packets received	R	Uint32
0x147E	2	LAN Port 7 Statistics – Number of packets received	R	Uint32
0x1480	2	LAN Port 8 Statistics – Number of packets received	R	Uint32
0x1482	2	LAN Port 9 Statistics – Number of packets received	R	Uint32

Address	# of Registers	Description	R/W	Format
0x1484	2	LAN Port 10 Statistics – Number of packets received	R	Uint32
0x1486	2	LAN Port 11 Statistics – Number of packets received	R	Uint32
0x1488	2	LAN Port 12 Statistics – Number of packets received	R	Uint32
0x148A	2	WAN Port 1 Statistics – Number of packets sent	R	Uint32
0x148C	2	WAN Port 2 Statistics – Number of packets sent	R	Uint32
0x148E	2	LAN Port 1 Statistics – Number of packets sent	R	Uint32
0x1490	2	LAN Port 2 Statistics – Number of packets sent	R	Uint32
0x1492	2	LAN Port 3 Statistics – Number of packets sent	R	Uint32
0x1494	2	LAN Port 4 Statistics – Number of packets sent	R	Uint32
0x1496	2	LAN Port 5 Statistics – Number of packets sent	R	Uint32
0x1498	2	LAN Port 6 Statistics – Number of packets sent	R	Uint32
0x149A	2	LAN Port 7 Statistics – Number of packets sent	R	Uint32
0x149C	2	LAN Port 8 Statistics – Number of packets sent	R	Uint32
0x149E	2	LAN Port 9 Statistics – Number of packets sent	R	Uint32

Address	# of Registers	Description	R/W	Format
0x14A0	2	LAN Port 10 Statistics – Number of packets sent	R	Uint32
0x14A2	2	LAN Port 11 Statistics – Number of packets sent	R	Uint32
0x14A4	2	LAN Port 12 Statistics – Number of packets sent	R	Uint32
0x14A6	2	WAN Port 1 Statistics – Number of bytes received	R	Uint32
0x14A8	2	WAN Port 2 Statistics – Number of bytes received	R	Uint32
0x14AA	2	LAN Port 1 Statistics – Number of bytes received	R	Uint32
0x14AC	2	LAN Port 2 Statistics – Number of bytes received	R	Uint32
0x14AE	2	LAN Port 3 Statistics – Number of bytes received	R	Uint32
0x14B0	2	LAN Port 4 Statistics – Number of bytes received	R	Uint32
0x14B2	2	LAN Port 5 Statistics – Number of bytes received	R	Uint32
0x14B4	2	LAN Port 6 Statistics – Number of bytes received	R	Uint32
0x14B6	2	LAN Port 7 Statistics – Number of bytes received	R	Uint32
0x14B8	2	LAN Port 8 Statistics – Number of bytes received	R	Uint32
0x14BA	2	LAN Port 9 Statistics – Number of bytes received	R	Uint32

Address	# of Registers	Description	R/W	Format
0x14BC	2	LAN Port 10 Statistics – Number of bytes received	R	Uint32
0x14BE	2	LAN Port 11 Statistics – Number of bytes received	R	Uint32
0x14C0	2	LAN Port 12 Statistics – Number of bytes received	R	Uint32
0x14C2	2	WAN Port 1 Statistics – Number of bytes sent	R	Uint32
0x14C4	2	WAN Port 2 Statistics – Number of bytes sent	R	Uint32
0x14C6	2	LAN Port 1 Statistics – Number of bytes sent	R	Uint32
0x14C8	2	LAN Port 2 Statistics – Number of bytes sent	R	Uint32
0x14CA	2	LAN Port 3 Statistics – Number of bytes sent	R	Uint32
0x14CC	2	LAN Port 4 Statistics – Number of bytes sent	R	Uint32
0x14CE	2	LAN Port 5 Statistics – Number of bytes sent	R	Uint32
0x14D0	2	LAN Port 6 Statistics – Number of bytes sent	R	Uint32
0x14D2	2	LAN Port 7 Statistics – Number of bytes sent	R	Uint32
0x14D4	2	LAN Port 8 Statistics – Number of bytes sent	R	Uint32
0x14D6	2	LAN Port 9 Statistics – Number of bytes sent	R	Uint32

Address	# of Registers	Description	R/W	Format
0x14D8	2	LAN Port 10 Statistics – Number of bytes sent	R	Uint32
0x14DA	2	LAN Port 11 Statistics – Number of bytes sent	R	Uint32
0x14DC	2	LAN Port 12 Statistics – Number of bytes sent	R	Uint32

Interpreting the Port State

Table 3: Interpreting the Port State

Address	Description	Value
0x1380 to 0x138D	Port state information	The upper byte represents the interface state: • 0x0: Interface is down • 0x1: Interface is going down • 0x2: Interface is in the initializing state • 0x3: Interface is coming up • 0x4: Interface is up and running • 0x5: Interface is reset by the user • 0x6: Interface is shut down by the user • 0x7: Interface is being deleted The lower byte represents the line protocol state: • 0x0: Line protocol state is down • 0x1: Line protocol state is up