MODBUS TCP Configuration

This chapter provides the following sections:

- Understanding MODBUS TCP
- Configuring the Switch Module as the MODBUS TCP Server
- Displaying MODBUS TCP Information

Understanding MODBUS TCP

Use Modicon Communication Bus (MODBUS) TCP over an Ethernet network when connecting the switch module 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 switches.

MODBUS is a serial communications protocol for client-server communication between a switch module (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 switch module functions as the server.

The CGR 2010 ESM 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 switch module. The default port number is **502**.

Note For information about the registers that a client can query on a switch module that functions as a MODBUS TCP server, see Appendix C, "MODBUS TCP Registers."

- MODBUS and Security, page 16-1
- Multiple Request Messages, page 16-2

MODBUS and Security

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

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

- To prevent a denial-of-service attack and to allow a specific client to send messages to the switch module (server), you can use this standard access control list (ACL) that permits traffic only from the assigned source IP address *10.1.1.n*:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

- To configure quality of service (QoS) to set the rate-limit for MODBUS TCP traffic:

```
interface FastEthernet0/1
ip address 10.1.1.1 255.255.255.0
ip access-group 1 in
 rate-limit input access-group 101 8000 8000 8000 conform-action transmit
exceed-action drop
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 any eq 502
```

Multiple Request Messages

The switch module 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 Switch Module as the MODBUS TCP Server

- Defaults, page 16-2
- Enabling MODBUS TCP on the Switch Module, page 16-2

Defaults

- Switch module is not configured as a MODBUS TCP server
- TCP switch module port number is 502
- Number of simultaneous connection requests is 1

Enabling MODBUS TCP on the Switch Module

Beginning in privileged EXEC mode:

	Step	Command
Step 1	Enters global configuration mode.	`configure terminal`
Step 2	Enables MODBUS TCP on the switch module	`scada modbus tcp server`

	Step	Command
Step 3	(Optional) Sets the TCP port to which clients send messages. The range for *tcp-port-number* is 1 to 65535. The default is 502.	**scada modbus tcp server port** *tcp-port-number*
Step 4	(Optional) Sets the number of simultaneous connection requests sent to the switch module. The range for *connection-requests* is 1 to 5. The default is 1.	**scada modbus tcp server connection** *connection-requests*
Step 5	Returns to privileged EXEC mode.	**end**
Step 6	Displays the server information and statistics.	**show scada modbus tcp server**
Step 7	(Optional) Saves your entries in the configuration file.	**copy running-config startup config**

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

To clear the server and client statistics, enter the **clear scada modbus tcp server statistics** privileged EXEC command.

After you enable MODBUS TCP on the switch module, this warning appears:

```
WARNING: Starting Modbus TCP server is a security risk.
Please understand the security issues involved before
proceeding further. Do you still want to start the
server? [yes/no]:
```

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

Displaying MODBUS TCP Information

Table 16-1 show scada modbus Command

Command	Description
show scada modbus tcp server	Displays the server information and statistics
show scada modbus tcp server connections	Displays the client information and statistics