CHAPTER 5

Configuring MODBUS TCP

Understanding MODBUS TCP

Use Modicon Communication Bus (MODBUS) TCP over an Ethernet network when connecting the switch 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 (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 functions as the server.

The switch 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. The default port number is 502.

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

MODBUS and Security

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

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

- To prevent a denial-of-service attack and to allow a specific client to send messages to the switch (server), you can use this standard access control list (ACL) that permits traffic only from the 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 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 as the MODBUS TCP Server

Defaults

The switch is not configured as a MODBUS TCP server.

The TCP switch port number is 502.

The number of simultaneous connection requests is 1.

Enabling MODBUS TCP on the Switch

Beginning in privileged EXEC mode:

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

	Command	Purpose
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 switch. The range for *connection-requests* is 1 to 5. The default is 1.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show scada modbus tcp server**	Displays the server information and statistics.
Step 7	**copy running-config startup config**	(Optional) Saves your entries in the configuration file.

To disable MODBUS on the switch 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, 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 5-1 show scada modbus Commands

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