CIP and MODBUS Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches

Cisco Catalyst IE9300 Rugged Series
Updated September 28, 2026

Topics included

1 MODBUS....4
MODBUS protocol....5
Cisco catalyst IE9300 MODBUS TCP registers....5
Interpreting the port state value....15
Configure the MODBUS TCP server....16
MODBUS display commands....17
Feature history....18

2 Common Industrial Protocol....20
Information about CIP....21
CIP restrictions....21
Enabling CIP....21
CIP password encryption....22
Guidelines and restrictions of CIP....23
Configure CIP password encryption....23
Additional references....24

1 MODBUS

Topics:

- MODBUS protocol
- Cisco catalyst IE9300 MODBUS TCP registers
- Interpreting the port state value
- Configure the MODBUS TCP server
- MODBUS display commands
- Feature history

MODBUS protocol

Explains the MODBUS protocol and its key features for network device communication.

Modicon Communication Bus (MODBUS) is an application-layer protocol for client-server communication between a switch and a network device running MODBUS client software. MODBUS can operate over a serial line and connect a computer to a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. This setup allows efficient communication among remote computers within SCADA networks.

Note

MODBUS is supported only on standalone Cisco Catalyst IE9300 Rugged series switches.

MODBUS also operates on Ethernet TCP or IP networks. MODBUS TCP connects the switch to devices, such as intelligent electronic devices (IEDs), distributed controllers, substation routers, IP phones, wireless access points, and redundant substation switches. The protocol increases connectivity options across networked devices.

A client, such as an IED or a human-machine interface (HMI) application, can remotely configure and manage devices running MODBUS TCP. The switch functions as the server. The switch encapsulates request and response messages in a MODBUS TCP application data unit (ADU). A client sends these messages to a specific TCP port on the switch.

Cisco catalyst IE9300 MODBUS TCP registers

Lists the read-only MODBUS TCP registers available on Cisco Catalyst IE9300 switches. Provides register address details, descriptions, formats, and values for both system and port information registers.

This document lists the read-only registers for IE9300 switches. MODBUS clients use these registers to communicate with a MODBUS server, the switch. These switches do not support writable registers.

System information registers

The address spaces 0x0800 through 0x0FFF contain read-only system information registers. These 2048 registers are accessible using MODBUS function code 0x03 `Read Multiple Registers`.

Table 1: System information registers

Address	Number of registers	Description	R/W	Format	Value
0x0800	64	Product ID	R	Text	-
0x0840	64	Software image name	R	Text	
0x0880	64	Software image version	R	Text	
0x08C0	64	Hostname	R	Text	
0x0900	1	Number of Gigabit Ethernet ports	R	Uint 16	
0x0901	1	Number of 10 Gigabit Ethernet ports	R	Uint 16	
0x0902	1	Number of mGig Ethernet ports	R	Uint 16	
0x0903	1	Number of power supplies	R	Uint 16	

Address	Number of registers	Description	R/W	Format	Value
0x0904	1	Power supply 1 status	R	Uint 16	0–Not present 1–Present
0x0905	1	Power supply 2 status	R	Uint 16	0–Not present 1–Present
0x0906	1	System or sensor ID 0 temperature	R	Uint 16	-
0x0907	1	Alarm 1 description	R	Uint 16	
0x0947	2	Alarm 2 description	R	Uint 16	
0x0987	1	Number of alarms	R	Uint 16	
0x0988	1	Alarm 1 status	R	Uint 16	0–Alarm off 1–Alarm on
0x0989	2	Alarm 2 status	R	Uint 16	0–Alarm off 1–Alarm on
0x098A	64	Alarm 3 description	R	Text	-
0x09CA	64	Alarm 4 description	R	Text	
0x0A0A	1	Alarm 3 status	R	Uint 16	0–Alarm off 1–Alarm on
0x0A0B	1	Alarm 4 status	R	Uint 16	0–Alarm off 1–Alarm on

Port information registers

The address spaces 0x1000 through 0x3FFF contain read-only port information registers. These 12,000 registers are accessible using MODBUS function code 0x03 `Read Multiple Registers`. The registers update each time the switch receives a read request.

This table lists the memory map for all interface registers with 64-bit counters in the address space 0x1000 through 0x2FFF (8,000 registers).

Table 2: Generic port information values

Address	Number of registers	Description	R/W	Format
0x1000	64	LAN port 1 name	R	Text
0x1040	64	LAN port 2 name	R	Text
0x1080	64	LAN port 3 name	R	Text
0x10C0	64	LAN port 4 name	R	Text
0x1100	64	LAN port 5 name	R	Text
0x1140	64	LAN port 6 name	R	Text

Address	Number of registers	Description	R/W	Format
0x1180	64	LAN port 7 name	R	Text
0x11C0	64	LAN port 8 name	R	Text
0x1200	64	LAN port 9 name	R	Text
0x1240	64	LAN port 10 name	R	Text
0x1280	64	LAN port 11 name	R	Text
0x12C0	64	LAN port 12 name	R	Text
0x1300	64	LAN port 13 name	R	Text
0x1340	64	LAN port 14 name	R	Text
0x1380	64	LAN port 15 name	R	Text
0x13C0	64	LAN port 16 name	R	Text
0x1400	64	LAN port 17 name	R	Text
0x1440	64	LAN port 18 name	R	Text
0x1480	64	LAN port 19 name	R	Text
0x14C0	64	LAN port 20 name	R	Text
0x1500	64	LAN port 21 name	R	Text
0x1540	64	LAN port 22 name	R	Text
0x1580	64	LAN port 23 name	R	Text
0x15C0	64	LAN port 24 name	R	Text
0x1600	64	LAN port 25 name	R	Text
0x1640	64	LAN port 26 name	R	Text
0x1680	64	LAN port 27 name	R	Text
0x16C0	64	LAN port 28 name	R	Text
0x1700	1	LAN port 1 state	R	Uint 16
0x1701	1	LAN port 2 state	R	Uint 16
0x1702	1	LAN port 3 state	R	Uint 16
0x1703	1	LAN port 4 state	R	Uint 16
0x1704	1	LAN port 5 state	R	Uint 16
0x1705	1	LAN port 6 state	R	Uint 16
0x1706	1	LAN port 7 state	R	Uint 16
0x1707	1	LAN port 8 state	R	Uint 16
0x1708	1	LAN port 9 state	R	Uint 16
0x1709	1	LAN port 10 state	R	Uint 16
0x170A	1	LAN port 11 state	R	Uint 16
0x170B	1	LAN port 12 state	R	Uint 16

Address	Number of registers	Description	R/W	Format
0x170C	1	LAN port 13 state	R	Uint 16
0x170D	1	LAN port 14 state	R	Uint 16
0x170E	1	LAN port 15 state	R	Uint 16
0x170F	1	LAN port 16 state	R	Uint 16
0x1710	1	LAN port 17 state	R	Uint 16
0x1711	1	LAN port 18 state	R	Uint 16
0x1712	1	LAN port 19 state	R	Uint 16
0x1713	1	LAN port 20 state	R	Uint 16
0x1714	1	LAN port 21 state	R	Uint 16
0x1715	1	LAN port 22 state	R	Uint 16
0x1716	1	LAN port 23 state	R	Uint 16
0x1717	1	LAN port 24 state	R	Uint 16
0x1718	1	LAN port 25 state	R	Uint 16
0x1719	1	LAN port 26 state	R	Uint 16
0x171A	1	LAN port 27 state	R	Uint 16
0x171B	1	LAN port 28 state	R	Uint 16

Table 3: Port information values for 64-bit counters

Address	Number of registers	Description	R/W	Format
0x171C	4	LAN port 1 statistics–number of packets received	R	Uint 64
0x1720	4	LAN port 2 statistics–number of packets received	R	Uint 64
0x1724	4	LAN port 3 statistics–number of packets received	R	Uint 64
0x1728	4	LAN port 4 statistics–number of packets received	R	Uint 64
0x172C	4	LAN port 5 statistics–number of packets received	R	Uint 64
0x1730	4	LAN port 6 statistics–number of packets received	R	Uint 64
0x1734	4	LAN port 7 statistics–number of packets received	R	Uint 64
0x1738	4	LAN port 8 statistics–number of packets received	R	Uint 64
0x173C	4	LAN port 9 statistics–number of packets received	R	Uint 64
0x1740	4	LAN port 10 statistics–number of packets received	R	Uint 64
0x1744	4	LAN port 11 statistics–number of packets received	R	Uint 64
0x1748	4	LAN port 12 statistics–number of packets received	R	Uint 64
0x174C	4	LAN port 13 statistics–number of packets received	R	Uint 64
0x1750	4	LAN port 14 statistics–number of packets received	R	Uint 64

Address	Number of registers	Description	R/W	Format
0x1754	4	LAN port 15 statistics–number of packets received	R	Uint 64
0x1758	4	LAN port 16 statistics–number of packets received	R	Uint 64
0x175C	4	LAN port 17 statistics–number of packets received	R	Uint 64
0x1760	4	LAN port 18 statistics–number of packets received	R	Uint 64
0x1764	4	LAN port 19 statistics–number of packets received	R	Uint 64
0x1768	4	LAN port 20 statistics–number of packets received	R	Uint 64
0x176C	4	LAN port 21 statistics–number of packets received	R	Uint 64
0x1770	4	LAN port 22 statistics–number of packets received	R	Uint 64
0x1774	4	LAN port 23 statistics–number of packets received	R	Uint 64
0x1778	4	LAN port 24 statistics–number of packets received	R	Uint 64
0x177C	4	LAN port 25 statistics–number of packets received	R	Uint 64
0x1780	4	LAN port 26 statistics–number of packets received	R	Uint 64
0x1784	4	LAN port 27 statistics–number of packets received	R	Uint 64
0x1788	4	LAN port 28 statistics–number of packets received	R	Uint 64
0x178C	4	LAN port 1 statistics–number of packets sent	R	Uint 64
0x1790	4	LAN port 2 statistics–number of packets sent	R	Uint 64
0x1794	4	LAN port 3 statistics–number of packets sent	R	Uint 64
0x1798	4	LAN port 4 statistics–number of packets sent	R	Uint 64
0x179C	4	LAN port 5 statistics–number of packets sent	R	Uint 64
0x17A0	4	LAN port 6 statistics–number of packets sent	R	Uint 64
0x17A4	4	LAN port 7 statistics–number of packets sent	R	Uint 64
0x17A8	4	LAN port 8 statistics–number of packets sent	R	Uint 64
0x17AC	4	LAN port 9 statistics–number of packets sent	R	Uint 64
0x17B0	4	LAN port 10 statistics–number of packets sent	R	Uint 64
0x17B4	4	LAN port 11 statistics–number of packets sent	R	Uint 64
0x17B8	4	LAN port 12 statistics–number of packets sent	R	Uint 64
0x17BC	4	LAN port 13 statistics–number of packets sent	R	Uint 64
0x17C0	4	LAN port 14 statistics–number of packets sent	R	Uint 64
0x17C4	4	LAN port 15 statistics–number of packets sent	R	Uint 64
0x17C8	4	LAN port 16 statistics–number of packets sent	R	Uint 64
0x17CC	4	LAN port 17 statistics–number of packets sent	R	Uint 64
0x17D0	4	LAN port 18 statistics–number of packets sent	R	Uint 64
0x17D4	4	LAN port 19 statistics–number of packets sent	R	Uint 64
0x17D8	4	LAN port 20 statistics–number of packets sent	R	Uint 64

Address	Number of registers	Description	R/W	Format
0x17DC	4	LAN port 21 statistics–number of packets sent	R	Uint 64
0x17E0	4	LAN port 22 statistics–number of packets sent	R	Uint 64
0x17E4	4	LAN port 23 statistics–number of packets sent	R	Uint 64
0x17E8	4	LAN port 24 statistics–number of packets sent	R	Uint 64
0x17EC	4	LAN port 25 statistics–number of packets sent	R	Uint 64
0x17F0	4	LAN port 26 statistics–number of packets sent	R	Uint 64
0x17F4	4	LAN port 27 statistics–number of packets sent	R	Uint 64
0x17F8	4	LAN port 28 statistics–number of packets sent	R	Uint 64
0x17FC	4	LAN port 1 statistics–number of bytes received	R	Uint 64
0x1800	4	LAN port 2 statistics–number of bytes received	R	Uint 64
0x1804	4	LAN port 3 statistics–number of bytes received	R	Uint 64
0x1808	4	LAN port 4 statistics–number of bytes received	R	Uint 64
0x180C	4	LAN port 5 statistics–number of bytes received	R	Uint 64
0x1810	4	LAN port 6 statistics–number of bytes received	R	Uint 64
0x1814	4	LAN port 7 statistics–number of bytes received	R	Uint 64
0x1818	4	LAN port 8 statistics–number of bytes received	R	Uint 64
0x181C	4	LAN port 9 statistics–number of bytes received	R	Uint 64
0x1820	4	LAN port 10 statistics–number of bytes received	R	Uint 64
0x1824	4	LAN port 11 statistics–number of bytes received	R	Uint 64
0x1828	4	LAN port 12 statistics–number of bytes received	R	Uint 64
0x182C	4	LAN port 13 statistics–number of bytes received	R	Uint 64
0x1830	4	LAN port 14 statistics–number of bytes received	R	Uint 64
0x1834	4	LAN port 15 statistics–number of bytes received	R	Uint 64
0x1838	4	LAN port 16 statistics–number of bytes received	R	Uint 64
0x183C	4	LAN port 17 statistics–number of bytes received	R	Uint 64
0x1840	4	LAN port 18 statistics–number of bytes received	R	Uint 64
0x1844	4	LAN port 19 statistics–number of bytes received	R	Uint 64
0x1848	4	LAN port 20 statistics–number of bytes received	R	Uint 64
0x184C	4	LAN port 21 statistics–number of bytes received	R	Uint 64
0x1850	4	LAN port 22 statistics–number of bytes received	R	Uint 64
0x1854	4	LAN port 23 statistics–number of bytes received	R	Uint 64
0x1858	4	LAN port 24 statistics–number of bytes received	R	Uint 64
0x185C	4	LAN port 25 statistics–number of bytes received	R	Uint 64
0x1860	4	LAN port 26 statistics–number of bytes received	R	Uint 64

Address	Number of registers	Description	R/W	Format
0x1864	4	LAN port 27 statistics–number of bytes received	R	Uint 64
0x1868	4	LAN port 28 statistics–number of bytes received	R	Uint 64
0x186C	4	LAN port 1 statistics–number of bytes sent	R	Uint 64
0x1870	4	LAN port 2 statistics–number of bytes sent	R	Uint 64
0x1874	4	LAN port 3 statistics–number of bytes sent	R	Uint 64
0x1878	4	LAN port 4 statistics–number of bytes sent	R	Uint 64
0x187C	4	LAN port 5 statistics–number of bytes sent	R	Uint 64
0x1880	4	LAN port 6 statistics–number of bytes sent	R	Uint 64
0x1884	4	LAN port 7 statistics–number of bytes sent	R	Uint 64
0x1888	4	LAN port 8 statistics–number of bytes sent	R	Uint 64
0x188C	4	LAN port 9 statistics–number of bytes sent	R	Uint 64
0x1890	4	LAN port 10 statistics–number of bytes sent	R	Uint 64
0x1894	4	LAN port 11 statistics–number of bytes sent	R	Uint 64
0x1898	4	LAN port 12 statistics–number of bytes sent	R	Uint 64
0x189C	4	LAN port 13 statistics–number of bytes sent	R	Uint 64
0x18A0	4	LAN port 14 statistics–number of bytes sent	R	Uint 64
0x18A4	4	LAN port 15 statistics–number of bytes sent	R	Uint 64
0x18A8	4	LAN port 16 statistics–number of bytes sent	R	Uint 64
0x18AC	4	LAN port 17 statistics–number of bytes sent	R	Uint 64
0x18B0	4	LAN port 18 statistics–number of bytes sent	R	Uint 64
0x18B4	4	LAN port 19 statistics–number of bytes sent	R	Uint 64
0x18B8	4	LAN port 20 statistics–number of bytes sent	R	Uint 64
0x18BC	4	LAN port 21 statistics–number of bytes sent	R	Uint 64
0x18C0	4	LAN port 22 statistics–number of bytes sent	R	Uint 64
0x18C4	4	LAN port 23 statistics–number of bytes sent	R	Uint 64
0x18C8	4	LAN port 24 statistics–number of bytes sent	R	Uint 64
0x18CC	4	LAN port 25 statistics–number of bytes sent	R	Uint 64
0x18D0	4	LAN port 26 statistics–number of bytes sent	R	Uint 64
0x18D4	4	LAN port 27 statistics–number of bytes sent	R	Uint 64
0x18D8	4	LAN port 28 statistics–number of bytes sent	R	Uint 64

Table 4: Port information values for 32-bit counters

Address	Number of registers	Description	R/W	Format
0x18DC	2	LAN port 1 statistics–number of packets received	R	Uint 32
0x18DE	2	LAN port 2 statistics–number of packets received	R	Uint 32
0x18E0	2	LAN port 3 statistics–number of packets received	R	Uint 32
0x18E2	2	LAN port 4 statistics–number of packets received	R	Uint 32
0x18E4	2	LAN port 5 statistics–number of packets received	R	Uint 32
0x18E6	2	LAN port 6 statistics–number of packets received	R	Uint 32
0x18E8	2	LAN port 7 statistics–number of packets received	R	Uint 32
0x18EA	2	LAN port 8 statistics–number of packets received	R	Uint 32
0x18EC	2	LAN port 9 statistics–number of packets received	R	Uint 32
0x18EE	2	LAN port 10 statistics–number of packets received	R	Uint 32
0x18F0	2	LAN port 11 statistics–number of packets received	R	Uint 32
0x18F2	2	LAN port 12 statistics–number of packets received	R	Uint 32
0x18F4	2	LAN port 13 statistics–number of packets received	R	Uint 32
0x18F6	2	LAN port 14 statistics–number of packets received	R	Uint 32
0x18F8	2	LAN port 15 statistics–number of packets received	R	Uint 32
0x18FA	2	LAN port 16 statistics–number of packets received	R	Uint 32
0x18FC	2	LAN port 17 statistics–number of packets received	R	Uint 32
0x18FE	2	LAN port 18 statistics–number of packets received	R	Uint 32
0x1900	2	LAN port 19 statistics–number of packets received	R	Uint 32
0x1902	2	LAN port 20 statistics–number of packets received	R	Uint 32
0x1904	2	LAN port 21 statistics–number of packets received	R	Uint 32
0x1906	2	LAN port 22 statistics–number of packets received	R	Uint 32
0x1908	2	LAN port 23 statistics–number of packets received	R	Uint 32
0x190A	2	LAN port 24 statistics–number of packets received	R	Uint 32
0x190C	2	LAN port 25 statistics–number of packets received	R	Uint 32
0x190E	2	LAN port 26 statistics–number of packets received	R	Uint 32
0x1910	2	LAN port 27 statistics–number of packets received	R	Uint 32
0x1912	2	LAN port 28 statistics–number of packets received	R	Uint 32
0x1914	2	LAN port 1 statistics–number of packets sent	R	Uint 32
0x1916	2	LAN port 2 statistics–number of packets sent	R	Uint 32
0x1918	2	LAN port 3 statistics–number of packets sent	R	Uint 32
0x191A	2	LAN port 4 statistics–number of packets sent	R	Uint 32
0x191C	2	LAN port 5 statistics–number of packets sent	R	Uint 32

Address	Number of registers	Description	R/W	Format
0x191E	2	LAN port 6 statistics–number of packets sent	R	Uint 32
0x1920	2	LAN port 7 statistics–number of packets sent	R	Uint 32
0x1922	2	LAN port 8 statistics–number of packets sent	R	Uint 32
0x1924	2	LAN port 9 statistics–number of packets sent	R	Uint 32
0x1926	2	LAN port 10 statistics–number of packets sent	R	Uint 32
0x1928	2	LAN port 11 statistics–number of packets sent	R	Uint 32
0x192A	2	LAN port 12 statistics–number of packets sent	R	Uint 32
0x192C	2	LAN port 13 statistics–number of packets sent	R	Uint 32
0x192E	2	LAN port 14 statistics–number of packets sent	R	Uint 32
0x1930	2	LAN port 15 statistics–number of packets sent	R	Uint 32
0x1932	2	LAN port 16 statistics–number of packets sent	R	Uint 32
0x1934	2	LAN port 17 statistics–number of packets sent	R	Uint 32
0x1936	2	LAN port 18 statistics–number of packets sent	R	Uint 32
0x1938	2	LAN port 19 statistics–number of packets sent	R	Uint 32
0x193A	2	LAN port 20 statistics–number of packets sent	R	Uint 32
0x193C	2	LAN port 21 statistics–number of packets sent	R	Uint 32
0x193E	2	LAN port 22 statistics–number of packets sent	R	Uint 32
0x1940	2	LAN port 23 statistics–number of packets sent	R	Uint 32
0x1942	2	LAN port 24 statistics–number of packets sent	R	Uint 32
0x1944	2	LAN port 25 statistics–number of packets sent	R	Uint 32
0x1946	2	LAN port 26 statistics–number of packets sent	R	Uint 32
0x1948	2	LAN port 27 statistics–number of packets sent	R	Uint 32
0x194A	2	LAN port 28 statistics–number of packets sent	R	Uint 32
0x194C	2	LAN port 1 statistics–number of bytes received	R	Uint 32
0x194E	2	LAN port 2 statistics–number of bytes received	R	Uint 32
0x1950	2	LAN port 3 statistics–number of bytes received	R	Uint 32
0x1952	2	LAN port 4 statistics–number of bytes received	R	Uint 32
0x1954	2	LAN port 5 statistics–number of bytes received	R	Uint 32
0x1956	2	LAN port 6 statistics–number of bytes received	R	Uint 32
0x1958	2	LAN port 7 statistics–number of bytes received	R	Uint 32
0x195A	2	LAN port 8 statistics–number of bytes received	R	Uint 32
0x195C	2	LAN port 9 statistics–number of bytes received	R	Uint 32
0x195E	2	LAN port 10 statistics–number of bytes received	R	Uint 32
0x1960	2	LAN port 11 statistics–number of bytes received	R	Uint 32

Address	Number of registers	Description	R/W	Format
0x1962	2	LAN port 12 statistics–number of bytes received	R	Uint 32
0x1964	2	LAN port 13 statistics–number of bytes received	R	Uint 32
0x1966	2	LAN port 14 statistics–number of bytes received	R	Uint 32
0x1968	2	LAN port 15 statistics–number of bytes received	R	Uint 32
0x196A	2	LAN port 16 statistics–number of bytes received	R	Uint 32
0x196C	2	LAN port 17 statistics–number of bytes received	R	Uint 32
0x196E	2	LAN port 18 statistics–number of bytes received	R	Uint 32
0x1970	2	LAN port 19 statistics–number of bytes received	R	Uint 32
0x1972	2	LAN port 20 statistics–number of bytes received	R	Uint 32
0x1974	2	LAN port 21 statistics–number of bytes received	R	Uint 32
0x1976	2	LAN port 22 statistics–number of bytes received	R	Uint 32
0x1978	2	LAN port 23 statistics–number of bytes received	R	Uint 32
0x197A	2	LAN port 24 statistics–number of bytes received	R	Uint 32
0x197C	2	LAN port 25 statistics–number of bytes received	R	Uint 32
0x197E	2	LAN port 26 statistics–number of bytes received	R	Uint 32
0x1980	2	LAN port 27 statistics–number of bytes received	R	Uint 32
0x1982	2	LAN port 28 statistics–number of bytes received	R	Uint 32
0x1984	2	LAN port 1 statistics–number of bytes sent	R	Uint 32
0x1986	2	LAN port 2 statistics–number of bytes sent	R	Uint 32
0x1988	2	LAN port 3 statistics–number of bytes sent	R	Uint 32
0x198A	2	LAN port 4 statistics–number of bytes sent	R	Uint 32
0x198C	2	LAN port 5 statistics–number of bytes sent	R	Uint 32
0x198E	2	LAN port 6 statistics–number of bytes sent	R	Uint 32
0x1990	2	LAN port 7 statistics–number of bytes sent	R	Uint 32
0x1992	2	LAN port 8 statistics–number of bytes sent	R	Uint 32
0x1994	2	LAN port 9 statistics–number of bytes sent	R	Uint 32
0x1996	2	LAN port 10 statistics–number of bytes sent	R	Uint 32
0x1998	2	LAN port 11 statistics–number of bytes sent	R	Uint 32
0x199A	2	LAN port 12 statistics–number of bytes sent	R	Uint 32
0x199C	2	LAN port 13 statistics–number of bytes sent	R	Uint 32
0x199E	2	LAN port 14 statistics–number of bytes sent	R	Uint 32
0x19A0	2	LAN port 15 statistics–number of bytes sent	R	Uint 32
0x19A2	2	LAN port 16 statistics–number of bytes sent	R	Uint 32
0x19A4	2	LAN port 17 statistics–number of bytes sent	R	Uint 32

Address	Number of registers	Description	R/W	Format
0x19A6	2	LAN port 18 statistics–number of bytes sent	R	Uint 32
0x19A8	2	LAN port 19 statistics–number of bytes sent	R	Uint 32
0x19AA	2	LAN port 20 statistics–number of bytes sent	R	Uint 32
0x19AC	2	LAN port 21 statistics–number of bytes sent	R	Uint 32
0x19AE	2	LAN port 22 statistics–number of bytes sent	R	Uint 32
0x19B0	2	LAN port 23 statistics–number of bytes sent	R	Uint 32
0x19B2	2	LAN port 24 statistics–number of bytes sent	R	Uint 32
0x19B4	2	LAN port 25 statistics–number of bytes sent	R	Uint 32
0x19B6	2	LAN port 26 statistics–number of bytes sent	R	Uint 32
0x19B8	2	LAN port 27 statistics–number of bytes sent	R	Uint 32
0x19BA	2	LAN port 28 statistics–number of bytes sent	R	Uint 32

Interpreting the port state value

Lists the meanings of port state values, including the interpretation of interface and line protocol states for IE9300 series switches.

This section provides information for determining the port state.

The upper byte indicates the interface state. The lower byte indicates the line protocol state. These values help determine the port state.

Address	Description	Value
0x1700 to 0x171B	Port state details	Upper byte: • 0x0: Interface down • 0x1: Interface going down • 0x2: Interface initializing • 0x3: Interface coming up • 0x4: Interface up and running • 0x5: Interface reset by user • 0x6: Interface shut down by user • 0x7: Interface being deleted Lower byte: • 0x0: Line protocol state down • 0x1: Line protocol state up

Configure the MODBUS TCP server

Configure the MODBUS TCP server on a switch to enable communication with MODBUS clients, set TCP ports, and adjust connection limits.

Configure the MODBUS TCP server to enable communication between MODBUS clients and the switch. This procedure includes enabling the server, setting the TCP port, and configuring connection limits.

The MODBUS TCP server listens for MODBUS client requests on TCP port 502 by default. Port 502 is enabled when the MODBUS server starts. If you configure a different port, the server uses the specified port instead.

Note

MODBUS is supported only on standalone Cisco Catalyst IE9300 Rugged Series Switches.

Before you begin

If security services are enabled, ensure the switch TCP port is not blocked. To enhance security, configure an ACL to permit traffic from specific clients. Alternatively, configure QoS to rate-limit traffic.

Procedure

1. Use **configure terminal** command to enter global configuration mode.

   Example

   ```
   Device#configure terminal
   ```

2. Use the **scada modbus tcp server** command to enable the MODBUS TCP server. To disable the server and restore its default settings, use the **no scada modbus tcp server** command.

   Example

   ```
   Device(config)#scada modbus tcp server
   ```

   ```
   Switch(config)#scada modbus tcp server
   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]: yes
   ```

   Note

   The system displays a security risk warning and prompts for confirmation.

   Enter **yes** to confirm and start the server.

3. (Optional) Use the **scada modbus tcp server port** *tcp-port-number* command to set the TCP port for client messages.

Example

```
Device(config)#scada modbus tcp server port 502
```

The range for tcp-port-number is 1 to 65535. The default is 502.

4. (Optional) Use the **scada modbus tcp server connection** *connection-requests* to set the number of simultaneous connection requests.

Example

```
Device(config)#scada modbus tcp server connection 1
```

The range for connection-requests is 1 to 5. The default is 1.

5. Use the **end** command to return to privileged EXEC mode.

Example

```
Device(config)#end
```

MODBUS display commands

This topic explains how to use commands to display and manage MODBUS TCP server information and statistics on IE9300 switches.

These commands display MODBUS TCP server details.

Table 5: Show scada modbus tcp server commands

Command	Purpose
show scada modbus tcp servers	Displays server information and statistics
show scada modbus tcp server connections	Displays information and statistics for each client connection
clear scada modbus tcp server statistics	Clears MODBUS server statistics, including statistics for each client connection

Output: show scada modbus tcp server command output

```
Switch# show scada modbus tcp server
Summary: enabled, running, process id 142
Conn Stats: listening on port 801, 4 max simultaneous connections
0 current client connections
0 total accepted connections, 0 accept connection errors
0 closed connections, 0 close connection errors
Send Stats: 0 tcp msgs sent, 0 tcp bytes sent, 0 tcp errors
0 responses sent, 0 exceptions sent, 0 send errors
Recv Stats: 0 tcp msgs received, 0 tcp bytes received, 0 tcp errors
0 requests received, 0 receive errors
```

Feature history

Lists the release details for features described in this guide, including availability and key feature information.

This table lists the release information for the features described in this guide. Unless otherwise noted, features are available in all subsequent releases.

Release	Feature	Feature information
Cisco IOS XE Dublin 17.12.1	MODBUS	Cisco Catalyst IE9300 Rugged Series Switches support the Modicon Communication Bus (MODBUS) starting with this release.

2 Common Industrial Protocol

Topics:

- Information about CIP
- CIP restrictions
- Enabling CIP
- CIP password encryption
- Additional references

Explains what common industrial protocols are and describes their key characteristics, typical applications, and importance for industrial automation systems.

Information about CIP

Explains the purpose, scope, and supported technologies of the Common Industrial Protocol (CIP).

The Common Industrial Protocol (CIP) is an industrial protocol for industrial automation applications.Previously known as Control and Information Protocol, CIP encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications - control, safety, synchronization,motion, configuration and information.

It is supported by Open DeviceNet Vendors Association (ODVA), an organization that supports network technologies based upon CIP such as DeviceNet, EtherNet/IP, CIP Safety and CIP Sync. CIP allows users to integrate these manufacturing applications with enterprise-level Ethernet networks and the Internet.

CIP restrictions

Explains the restriction imposed on enabling CIP on switches.

CIP can be enabled on only one VLAN on the switch.

Enabling CIP

Configure the switch to enable CIP functionality and set CIP security options.

Before you begin

By default, CIP is not enabled

Procedure

1. Enters global configuration mode.

```
Configure Terminal
```

2. Sets CIP security options on the switch.

```
cip security { password password | window timeout value }
```

3. Enters interface configuration mode.

```
interface vlan 20
```

4. Enables CIP on a VLAN.

```
cip enable
```

5. Returns to privileged EXEC mode.

```
end
```

6. Verifies your entries.

```
show running-config
```

7. (Optional) Saves your entries in the configuration file.

```
copy running-config startup-config
```

8. (Optional) Displays information about the CIP subsystem.

```
show cip { connection | faults | file | miscellaneous |
object | security | session | status }
```

9. (Optional) Enables debugging of the CIP subsystem.

```
debug cip {assembly | connection manager | dlr | errors
| event | file | io | packet | infra | security | session | socket}
```

CIP password encryption

Explains how CIP password encryption protects credentials in industrial device configurations by using modern, irreversible hashing methods.

Common Industrial Protocol (CIP) password encryption is a security feature for industrial environments that

- protects CIP credentials within device configuration files,
- uses the Type 8 (SHA256) hashing algorithm to meet modern security standards, and
- ensures that stored credentials are irreversible and resistant to cryptographic attacks.

Type 8 encryption is a strong, irreversible hashing method that replaces the legacy Type 7 encryption to improve the security posture of industrial deployments.

Table 6: Feature history table

Feature name	Release information	Description
CIP password encryption	26.2.1	This feature provides enhanced security by converting legacy CIP passwords to the irreversible Type 8 (SHA256) algorithm to resist cryptographic attacks. It ensures credential integrity and uninterrupted authentication across industrial deployments.

Type 8 password encryption advantages

Type 8 password encryption provides security and operational advantages by automatically converting legacy passwords during the Cisco IOS XE software upgrade. This irreversible method reinforces credential security by preventing the system from converting passwords back to plaintext. During migration, the system handles invalid or corrupted data gracefully to ensure data integrity. By storing these passwords in the configuration file, the system maintains consistency across reboots and device transfers. It also integrates with the CIP module to provide uninterrupted authentication and communication.

CIP password encryption transitions

When you upgrade the software image to release 26.2.1 or later, the system automatically detects existing CIP passwords stored with Type 7 encryption. The system converts these passwords to the strong, irreversible Type 8 hashing algorithm and saves them into the device configuration file.

Guidelines and restrictions of CIP

Guidelines

- Downgrading to a software version earlier than 26.2.1 removes the CIP password from the configuration.
- Plaintext passwords must be stored externally as they cannot be retrieved once encrypted.
- Manual configuration transfers preserve CIP password.

Restrictions

Type 8 encryption is irreversible, and the original plaintext password cannot be recovered from the device.

Configure CIP password encryption

Set a password to secure CIP communications.

You can enter a plaintext password, which the system automatically converts to Type 8 encryption in the configuration file, or you can manually enter a pre-encrypted Type 8 (SHA256) hash.

Before you begin

Ensure the device is running release 26.2.1 or later to support Type 8 encryption.

Procedure

1. Use the `configure terminal` command to enter global configuration mode.

   Example

   ```
   Switch# configure terminal
   ```

2. Use the **cip security { password** *<pass_word>* **| password 8** *< SHA256-encrypted-password>* } command to configure the password based on your available credential format.

   Example

   ```
   Switch(config)# cip security password cisco
   ```

   Use the **cip security password 8** *< SHA256-encrypted-password>* command to enter a pre-encrypted Type 8 hash.

3. Use the **exit** command to return to privileged EXEC mode.

   Example

   ```
   Switch(config)# exit
   ```

4. Use the **copy running-config startup-config** command to copy the running configuration to NVRAM.

Example

```
Switch# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Additional references

Lists related technical documents, standards, RFCs, and technical assistance resources for further learning and support.

Related documents

Related Topic	Document Title
Cisco IOSbasic commands	Cisco IOS Configuration Fundamentals Command Reference

Standards and RFCs

Standard/RFC
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.

Technical Assistance

Standard/RFC	Title
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	*https://www.cisco.com/support*