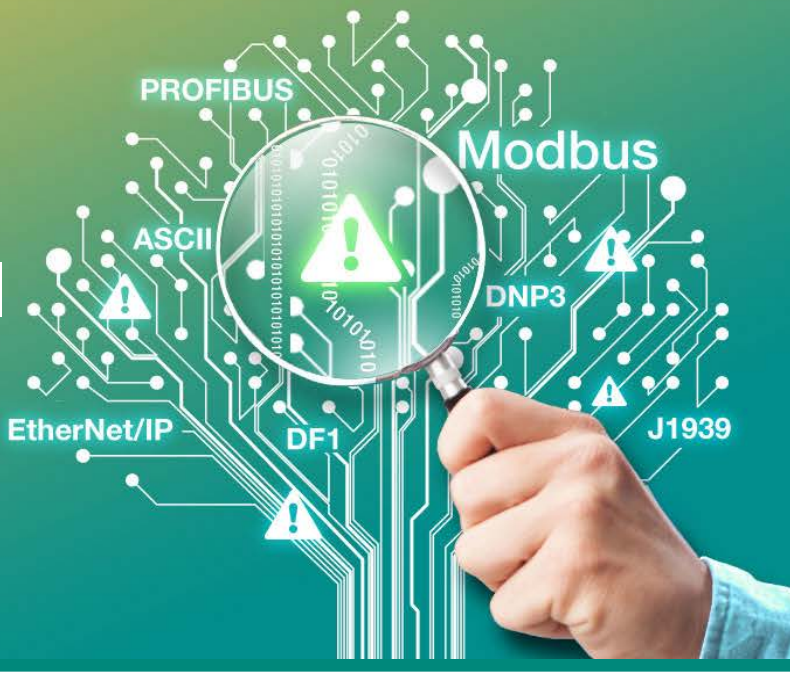
MOXA
Reliable Networks Sincere Service

Modbus Gateways

How to Easily Troubleshoot Protocol Gateways



White Paper

Modbus Gateways

Abstract

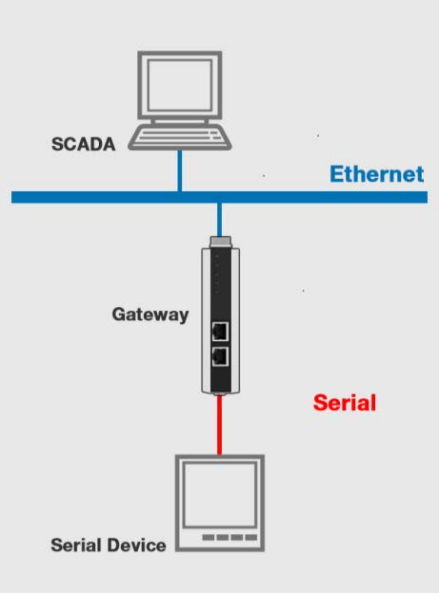
The rise of the Industrial Internet of Things (IIoT) has been galvanized by the worldwide drive to leverage data. Analysis of data collected from a large number of meters, sensors, and other devices has helped enterprises parlay their subsequent findings into palpable benefits, such as operational optimization, predictive maintenance, revenue protection, capacity planning, energy savings, and so on.

However, transmitting much-needed data from the edge of a network to the cloud for analysis is not always so straightforward. Without exception, protocol gateways are required to perform protocol conversions between management systems and field devices when data is being collected. Furthermore, applications commonly deal with a variety of protocols, posing headaches for many engineers as they are not familiar with all of the protocols. As a result, engineers often spend a lot of time and effort on the configuration and maintenance of devices. It is with regard to maintenance where their stress reaches boiling point as they are often unable to find a quick solution when an issue occurs on a network.

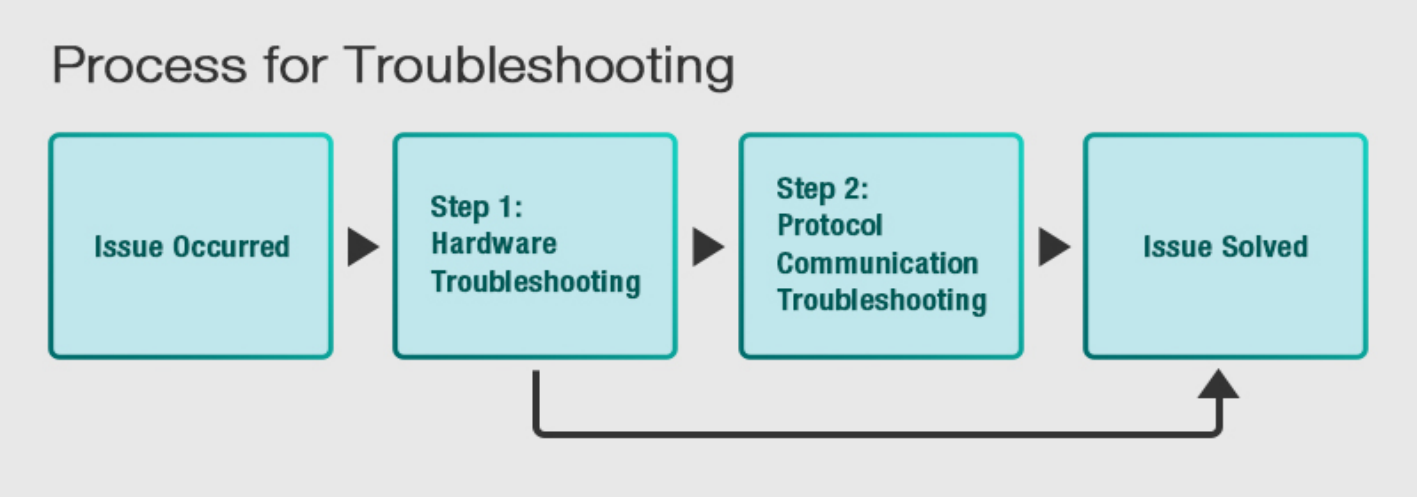
This white paper takes a closer look at troubleshooting methods and the pain points that frustrate engineers, and then sets out to present a solution that simplifies the troubleshooting of protocol gateways.

Getting the Whole Picture

Before we get to the bottom of the issues with troubleshooting, we first need to understand the topology of a standard network to have a better grasp of the mechanisms of the troubleshooting process. The typical topology of a network is illustrated in the figure on the right. Nowadays, most management systems, such as supervisory control and data acquisition (SCADA) and Human Machine Interface (HMI) systems, collect data through industrial protocols like Modbus TCP, PROFINET, and EtherNet/IP. These management systems connect to network infrastructure via a large number of switches. Protocol gateways, in their capacity as protocol converters, communicate with SCADA or HMI systems through Ethernet on one side; on the other side, they connect to field devices and communicate with fieldbus protocols through serial interfaces such as RS-232/422/485. Thus, gateways play an important role in collecting data.



When there is a problem in a network, engineers first need to determine whether it is a hardware or communication issue. The troubleshooting process is illustrated in the figure below.



In most applications, engineers usually detect something is amiss when certain values cannot to be monitored or when an alert is triggered in the management system. The first step is to check the apparent behavior of devices, and this can be done by inspecting the LED indicators, cable connections, pin assignments, and so on. If the issue is not related to the physical side of the network, then it is very likely a protocol communication problem. Unlike hardware issues, communication issues cannot be assessed by the naked eye; therefore, diagnostics tools are required.

Troubleshooting Hardware Problems

Engineers commonly overlook these conditions when they troubleshoot hardware.

1. **Power Connection:** Check whether the power input range of the devices and power supply output match. For example, if a power adapter's output is 12 VDC, but the gateway's range is 24VDC, then clearly the gateway will not work. Most devices have a LED indicator that shows the power status.

2. **Cable Connection:** Troubleshooting Ethernet connectivity is fairly easy because Ethernet cables are standardized. Troubleshooting, however, becomes much more complicated when it comes to serial cables due to the different interfaces, complete with different pin assignments. Because pin assignments for serial interfaces differ from vendor to vendor, devices and protocol gateways are frequently connected incorrectly due to wrong pin connections. To fix this, refer to the pin connections in the user's manual and then check them carefully.

Serial Signal: Of all three serial interfaces, the RS-485 interface has the most benefits: it has better noise immunity than the standard RS-232 interface, it can connect more devices via a daisy-chain network, and it can maintain communication over longer distances. However, the RS-485 interface is not immune to communication failures when engineers are cascading several RS-485 devices during installation. In the event of a communication failure, an oscilloscope, which captures the waveforms, is the ideal tool to get to the crux of the matter quickly. Unfortunately, an oscilloscope is a luxury, and, therefore, not commonly used at field sites. What's more, many field engineers don't know how to use an oscilloscope. Hence, a good gateway has built-in pull-up and pull-down resistors, as well as a terminator resistor on each serial port, to overcome most scenarios. The pull-up and pull-down resistors can increase the noise immunity in the bus, and the terminator resistors, enabled at both ends, can reduce signal reflections.

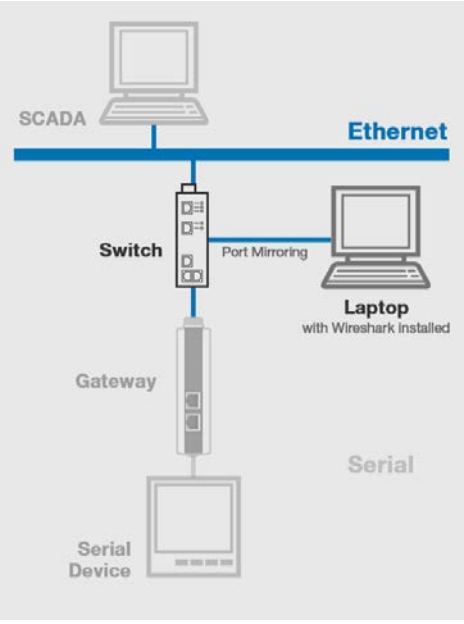
If the issue still exists after completing this checklist, then you are very likely dealing with a communication problem, and troubleshooting tools are needed to fix it.

Troubleshooting Communication Issues

Troubleshooting communication issues without any tools is a cumbersome task—no matter whether it is done on the Ethernet or serial side of a network. For this reason, engineers are always on the lookout for helpful tools to help them save time and effort. Let's take a closer look at the issues that arise when built-in troubleshooting tools are not available.

Installing Third-Party Software Requires Effort

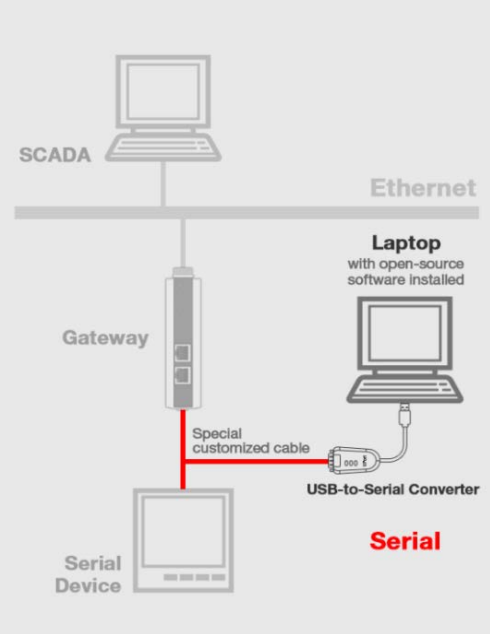
As most low-end protocol gateways don't provide any troubleshooting tools, the open-source software Wireshark is often the go-to tool. In order to capture Ethernet data packets, the tool must be installed in the management system. However, for various reasons, Wireshark cannot be installed on all management systems. For example, some PLCs don't have the capacity to install third-party software. In the case of SCADA systems, IT staff may not allow the installation of Wireshark due to security issues. For these kinds of situations, engineers have to prepare a switch with a mirror-port function, which needs to be added between the gateway and the management system. (See figure on the right.) Engineers should configure the mirror port to capture packets from the switch port that connects either to the gateway or network infrastructure.



Experienced engineers can easily analyze the captured packets to determine the root cause. If they are lucky, the issue is on the Ethernet side of the network, which can be solved quickly.

Capturing Serial Data is a Nightmare

Whereas troubleshooting Ethernet communication is fairly easy, the same cannot be said for serial communication though. Troubleshooting serial communication is complicated because it is hard to capture serial data in the bus. Engineers need to go to great lengths to create a special serial cable. Furthermore, they have to prepare a USB-to-serial converter, which connects to the serial bus to log incoming data. (The cabling is illustrated in the figure on the right.)
The gateway and serial devices communicate with each other, and the inserted path connected to the USB-to-serial converter is used to capture data transmission in a computer through a serial analyzer tool. Reading the data, however, is difficult because it is raw data.

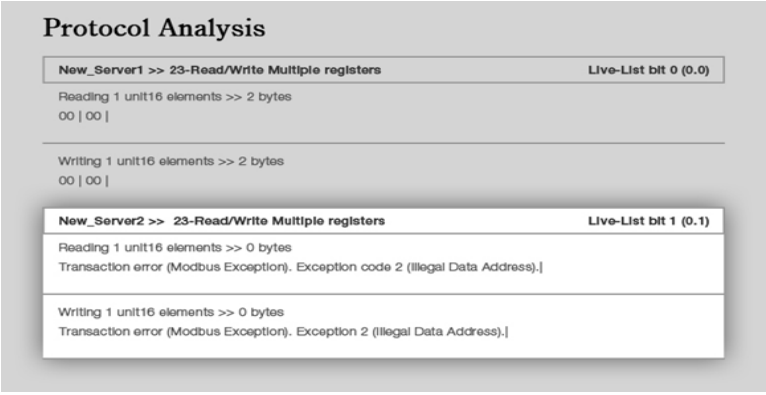


So, troubleshooting without built-in tools often creates more pain points than easy solutions. These pain points can include an increase in costs because of the additional parts and devices required, longer downtime to analyze raw data, and time and effort needed to install third-party software.

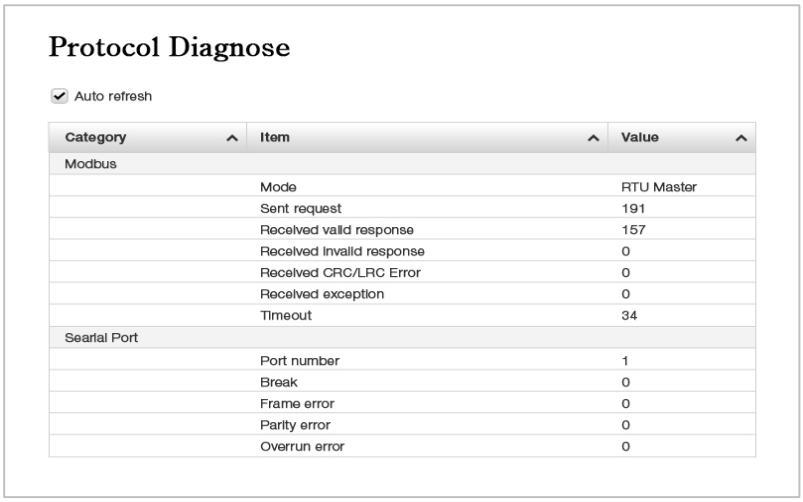
Let Tools Do the Work for You

Most high-end protocol gateways provide a choice of troubleshooting tools, namely protocol analysis, protocol diagnostics, and traffic monitoring.

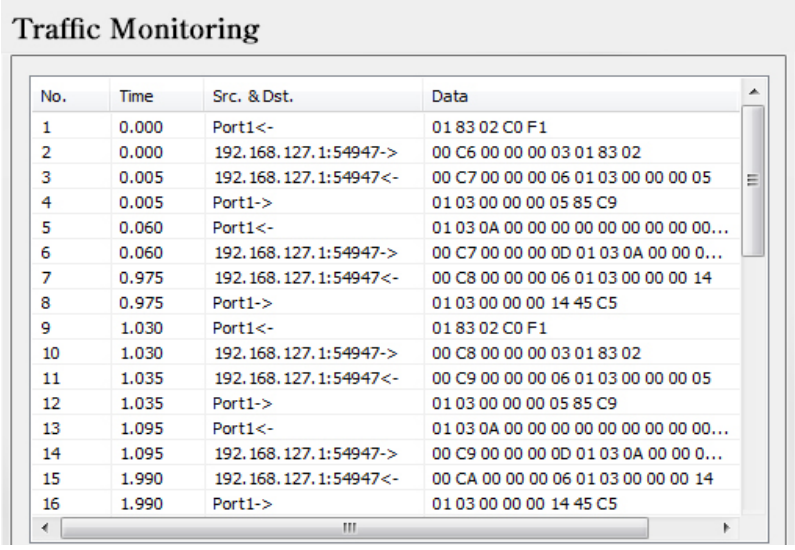
1. **Protocol Analysis Tool:** This tool saves time by immediately pinpointing whether the issue has occurred on the Ethernet or serial side of a network. What's more, this tool also provides tips to guide the troubleshooting process, which comes in very handy for junior engineers, who have a very limited knowledge of the protocols they are handling.



2. Protocol Diagnostics Tool: This tool diagnoses the status of the protocol connection and records all errors, assisting users in determining the root cause of a network failure. Previously, when a connection failed, it was very hard to find the root cause without any knowledge of what happened before the disruption. Now, engineers can rely on the protocol diagnostics tool to give them a better understanding of the failure.



3. Traffic Monitoring Tool: Usually, engineers have to use third-party tools with additional equipment to collect communication logs. Protocol gateways with an integrated traffic monitoring tool help troubleshoot communication problems by tracking traffic logs. These traffic logs can capture either Ethernet or serial data packets. However, most of the logs display raw data, which has no meaning for most engineers, and is also difficult to troubleshoot. Therefore, an efficient traffic monitoring tool should be able to handle the logs and convert the raw data into meaningful data. By taking advantage of this tool, engineers can track the root cause easily. Moreover, for those engineers who are unable to solve the problem, they can use the traffic logs as a valuable reference when they discuss the issue with the manufacturer.



Modbus Gateways

Moxa's Solutions

Moxa's powerful protocol gateways are enhanced with built-in troubleshooting tools. These tools can range from the communication analysis tool, to a protocol diagnostics tool and a traffic monitoring tool. These tools help complete the whole troubleshooting process by locating the issue on a network, checking the status of protocol connections, and monitoring traffic logs to track records. Therefore, engineers don't need to waste time figuring out what caused the downtime. Also, Moxa's troubleshooting tools can be applied in both the pre-test and maintenance stage. Moxa's gateways are further enhanced with built-in pull-up, pull-down, and terminator resistors. These built-in resistors can overcome most conditions to reduce installation time. For more information, visit https://www.moxa.com/Event/Tech/modbus-protocol-gateway/easier_troubleshooting.htm

Disclaimer

© 2017 Moxa Inc. All rights reserved.

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa

Tel: (714) 528-6777
Fax: (714) 528-6778