

Redundant Serial-to-Ethernet Data Connections for Mission-critical Devices

Daniel Lai, Moxa Product Manager

daniel.lai@moxa.com

The popularity of serial-to-Ethernet technology has increased steadily since the release of the first serial device servers in the late 1990's. There are two main benefits to using Ethernet to transmit data signals between serial devices and host computers. The first benefit is that the limited transmission distance of serial-only connections can be extended to essentially any distance with Ethernet. The second benefit is centralization. If needed, it is possible to route serial signals from an entire factory to one central location where the data can be analyzed, modified, and then acted upon.

For serial-only systems, redundancy generally involves keeping spare devices on hand in case of device failure, and ensuring that a reliable backup power supply is available in case of power outages. Backing up the serial line itself is less important, since serial connections tend to be more localized compared to the more modern TCP/IP networks. In addition, serial data transmission protocols are relatively straightforward.

Ethernet networks, however, are a different matter. A typical Ethernet LAN is designed to support communication between many different network hosts, and as such the topology of such networks can be quite complicated. Another complicating factor is that Ethernet networks use a wide array of hubs,

Released on July 4, 2008

Copyright © 2008 Moxa Inc., all rights reserved.

Moxa manufactures one of the world's leading brands of device networking solutions. Products include industrial embedded computers, industrial Ethernet switches, serial device servers, multiport serial boards, embedded device servers, and remote I/O solutions. Our products are key components of many networking applications, including industrial automation, manufacturing, POS, and medical treatment facilities.

How to contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778
Web: www.moxa.com
Email: info@moxa.com



This document was produced by the Moxa Technical Writing Center (TWC). Please send your comments or suggestions about this or other Moxa documents to twc@moxa.com.

switches, and other devices for transmitting data throughout the network.

In fact, in recent years Ethernet has been adopted as the backbone communications medium for many industrial applications. For this reason, setting up reliable redundancy for Ethernet networks is absolutely essential, since the failure of all or even part of an industrial communications network could cause huge financial losses for companies that rely on such networks to transmit all types of data.

Approaches to Serial-to-Ethernet Redundancy

Ethernet networks consist of a collection of links between hosts and switches, and switches and switches, combined to form a tree topology. Ethernet networks could consist of literally hundreds if not thousands of point-to-point wired connections. Since the route taken when sending data from one network host to another is determined by the network and not the sender, a failure of any link in the network could bring the entire operation to a grinding halt.

Saying that an Ethernet network is redundant can mean one of several things. In all likelihood, it means that a small portion of the network is kept idle until another part of the network fails, at which point the "redundant" portion is activated to maintain the flow of data. Another possibility is that a large portion of the network, or even the entire network itself, is duplicated to provide redundancy.

In this paper, we consider three types of Ethernet redundancy: Single-network redundancy, dual-network redundancy, and multi-host redundancy.

Single-network Redundancy

Single-network redundancy uses a physical link in the network as the backup path. The redundancy software identifies a particular link in the network that if active could cause data packets to return to the sender before reaching their

destination. To avoid broadcast storms, data is blocked from being transmitted across the redundant link during normal operation, and the link is only activated if one of the live links in the network fails.

Two types of single-network redundancy are in common use. Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP), referred to collectively as STP/RSTP, can be used on very general, mesh-type networks. The other type of redundancy is restricted to networks arranged in a ring topology. Note that for industrial networks, the major determiner of which redundant protocol to use is the "recovery speed."

Dual-network and Multi-host Redundancies

Dual-network redundancy involves creating a complete backup to the Ethernet network. In general, with dual-network redundancy, the servers and hosts used on the network are not duplicated.

With multi-host redundancy, one or more duplicates of the host computers on the network are set up to provide backups in case the primary host crashes.

A more complete type of redundancy involves setting up backups for the network *and* the hosts.

Single-network Redundant Network Solutions

Moxa's NPort 6000 series of device servers support the IEEE spanning tree protocols, plus the proprietary Turbo Ring protocols developed by Moxa.

Spanning Tree and Rapid Spanning Tree Protocols

IEEE 802.1D, or Spanning Tree Protocol (STP), was introduced in 1990 to protect the network from broadcast storms caused by unintended loops, and to reduce network crashes due to the failure of a single link in the network. An enhanced version of STP, called IEEE 802.1w or Rapid Spanning Tree Protocol

(RSTP), was released in 1998. STP/RSTP detects duplicate paths in the network and then blocks data from being transmitted across the duplicate paths.

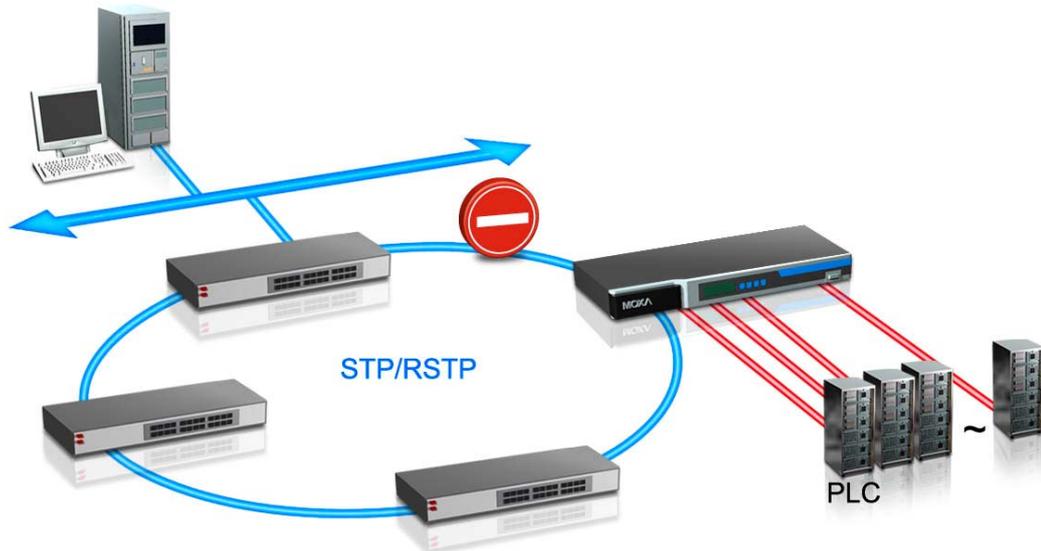


Figure 1: STP/RSTP Protocol for Single-network Redundancy

One of the advantages of STP/RSTP is that it can be used with complicated mesh-type networks. In fact, system engineers can set up a mesh-type network without worrying about loops, and then when the network is activated, the STP/RSTP algorithm analyzes the network automatically to determine if any loops exist. If loops are discovered, the algorithm determines which links in the loops should be blocked, and the blocked loops are then reserved for use in the event that an active link is broken. When this occurs, the STP/RSTP algorithm springs into action by activating one of the redundant links in the network.

The main drawback to using STP/RSTP with industrial networks is that the recovery time is relatively slow. STP can take up to 30 seconds to recover, and RSTP can take up to 5 seconds. Since data is transmitted from device to device in a matter of milliseconds, a recovery time of 5 seconds is often too slow.

Turbo Ring and Turbo Ring V2

Moxa developed the proprietary Turbo Ring protocol to optimize communication redundancy and achieve a faster recovery time on the network. The Turbo Ring and Turbo Ring V2 protocols identify one switch in the ring as the master, and then automatically blocks packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected, the Turbo Ring protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

The user does not need to configure any of the switches as the master to use the Turbo Ring protocols. If none of the switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. The sole purpose of the master is to identify which segment in the redundant ring acts as the backup path.

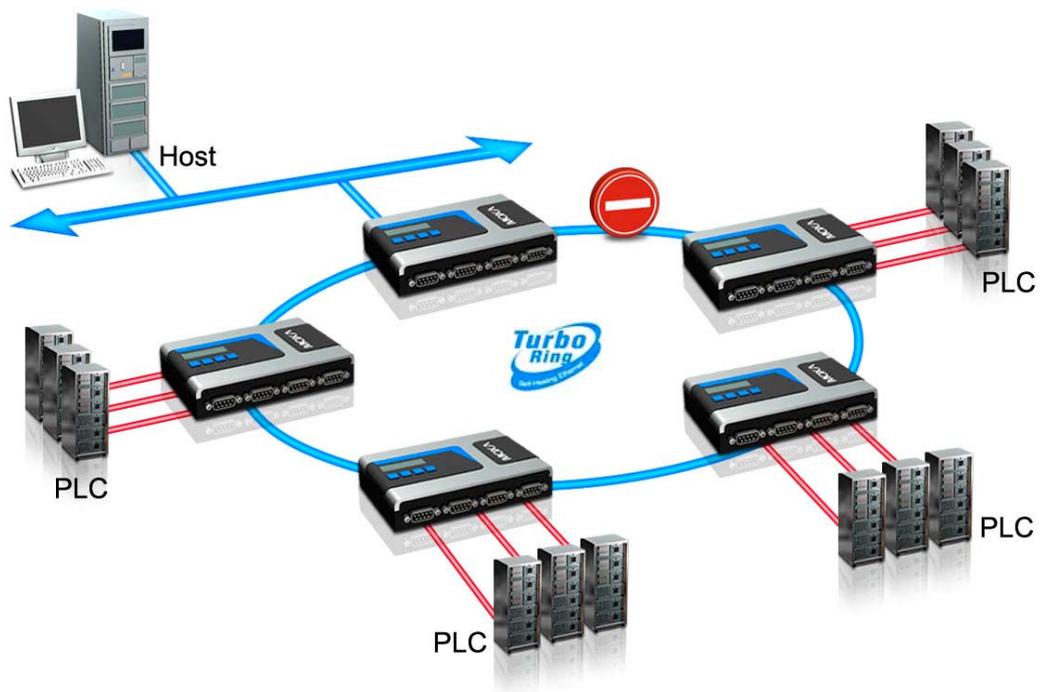


Figure 2: Turbo Ring Protocol for Single-network Redundancy

Moxa's Dual-network and Multi-host Redundant Network Solutions

Moxa's CN2600 series of terminal servers provides dual-network redundancy in the form of Redundant COM mode, multi-host redundancy in the form of Multi-host TTY mode, and combined dual-network/multi-host redundancy in the form of DRDAS (Dual-host Redundant Data Acquisition System) mode.

Redundant COM Mode

The Redundant COM operation mode can be used to set up a redundant LAN between the serial devices connected to the device server's serial ports and the host computer. The redundant structure involves using the device server's two LAN ports to set up two independent LANs that connect the device server to the host computer. If either of the two LANs fails, the other LAN will continue transmitting packets between the serial devices and the host, with the packets passing through the device server. In fact, one of the biggest advantages of the Redundant COM mode is that the "switching time" is zero.

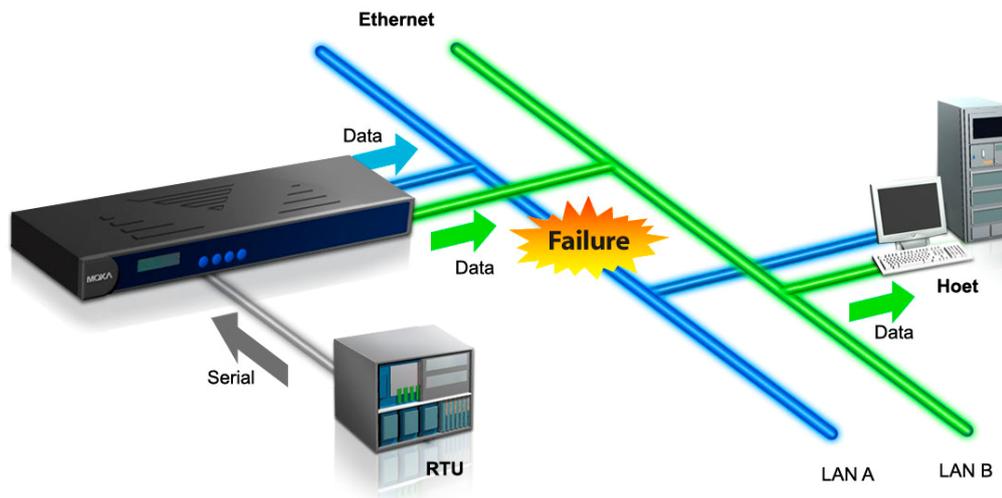


Figure 3: Dual-network Redundancy

Multi-host Mode

With Multi-host mode, multiple hosts can establish TCP connections to the serial port at the same time. The device server duplicates the serial data and transmits the data to all of the hosts at the same time. Ethernet data is sent on a first-in first-out basis to the serial port when data comes into the device server from the Ethernet interface.

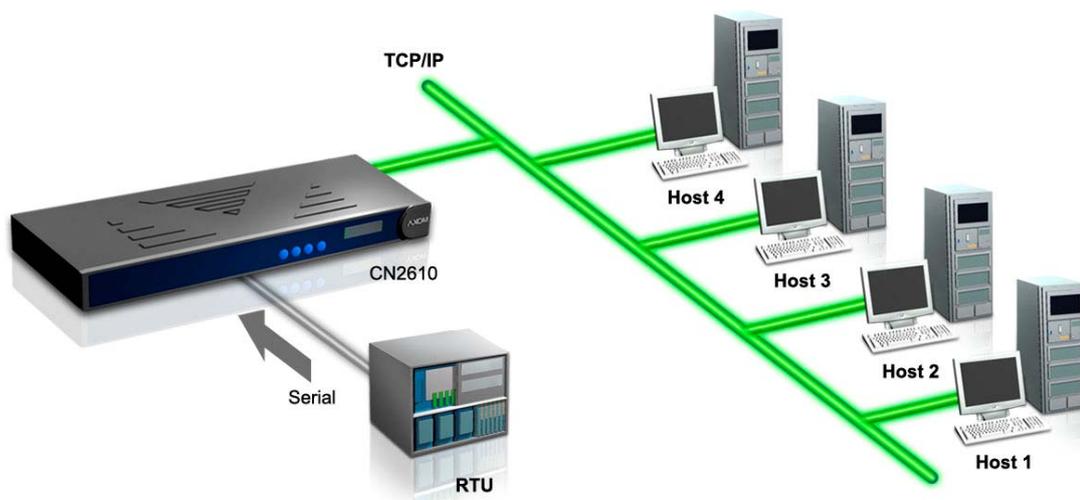


Figure 4: Multi-host Redundancy

DRDAS Mode

The DRDAS operation mode provides a highly redundant network structure that takes advantage of the CN2600's dual LAN ports, dual IP addresses, and dual MAC addresses. DRDAS uses a backup PC that is set up to take over when the primary PC fails. The CN2600's dual-host redundant configuration sends serial data to 4 IP addresses on the network. Users select a Primary IP and 3 Secondary IPs. When the Primary IP fails, the backup IPs take over by using the switching library. With this kind of redundant setup, if one of the secondary IPs tries to send commands to the serial device, the commands are discarded by the CN2600, since only the Primary IP is allowed to conduct bi-directional transmission. During normal

operation, the backup IPs are only allowed to receive data from the CN2600.

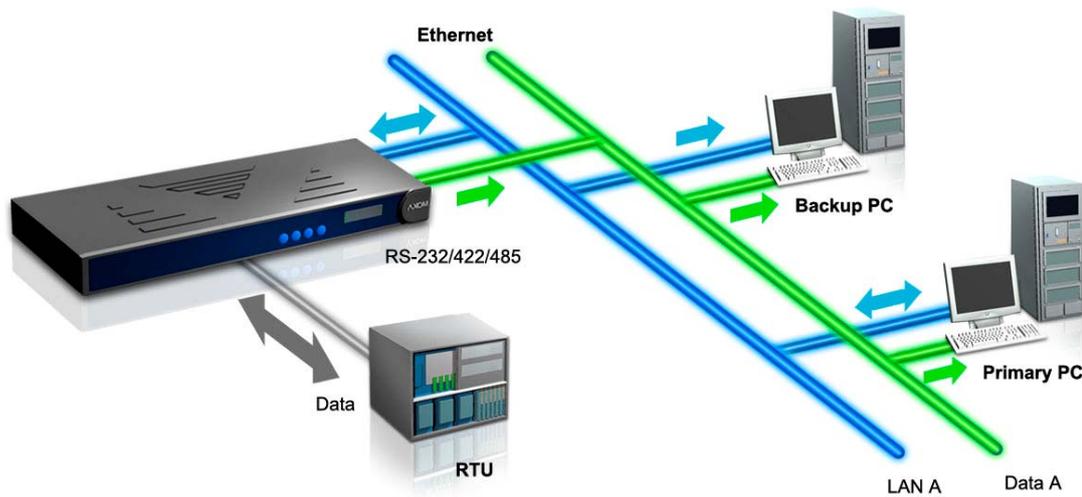


Figure 5: Combination of Dual-network and Multi-host Redundancy

Application: Redundancy for Power Substations

Dual-network architectures are becoming more and more common in power substations, which rely on complex and sophisticated networks for data acquisition and access control. Typically, costly software development and specialized hardware are required to manage redundant systems. Many devices, including protection relays, controllers, switch gears, and RTUs, still have RS-232 or RS-485 serial interfaces, so device servers are used to integrate them into major automation systems and enable communication with PC hosts over an Ethernet LAN.

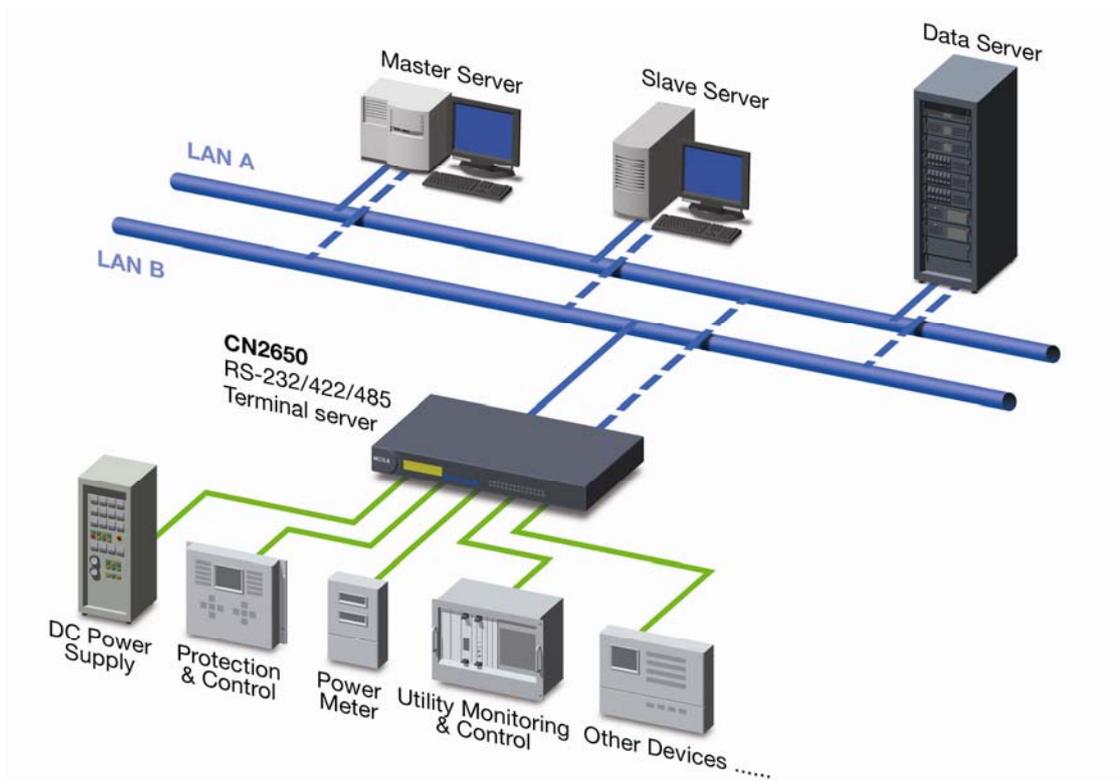


Figure 6: Application of Dual-network Redundancy

With this application, legacy RS-232 and RS-485 serial devices are connected to an Ethernet network to provide advanced management capability, and to synchronize operations between local and remote control sites. This type of setup provides stability and reliability for data acquisition and access control through redundancy.

Application: Real-time Environment Sensors for Trains

Modern rail systems are a marvel of engineering and coordination. Not only are trains expected to arrive and depart on time, but for safety and control reasons, each car must remain in constant contact with the central control center. In fact, some rail companies now go one step further and provide passengers with ready access to the current time and environmental conditions.

In the example described here, each car in the train has separate temperature and humidity sensors connected directly to an Ethernet network. The sensor values are transmitted in real time to the central control center, which uses the information to manage the heating and cooling system in the cars. In addition, the current time is flashed on LCM screens so that passengers can keep track of the train's progress.

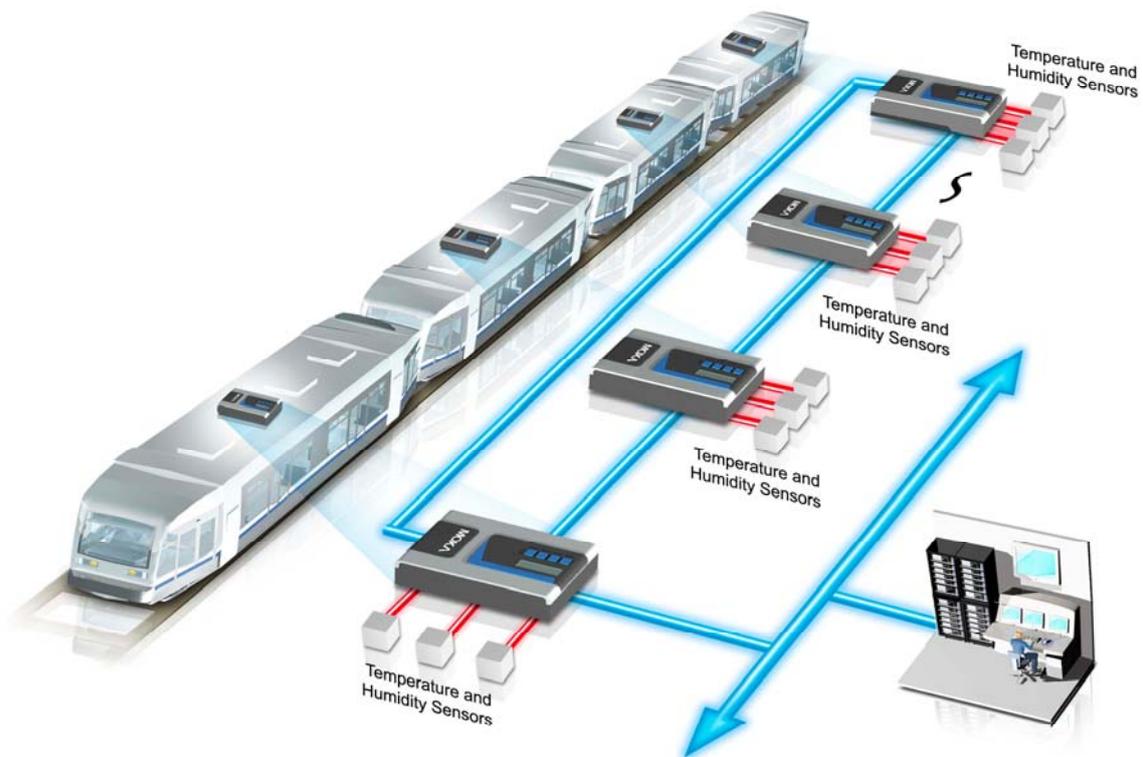


Figure 7: Application of Turbo Ring Redundancy

For this application, Moxa's NPort 6000 secure device servers are arranged in a ring topology. One NPort is installed in each of the cars, and the Ethernet ports of adjacent NPorts are connected together. To complete the ring, the two end NPorts connect directly to each other. The fact that each NPort has two Ethernet ports makes this type of topology possible.

The ring network is configured to use Moxa's proprietary Turbo Ring protocol, which supports a reconnection time of less than 100 milliseconds*.

* Note that Moxa's proprietary Turbo Ring protocol was originally developed for Moxa's complete line of Ethernet switches, which support a recovery time of under 20 milliseconds.

Conclusion

The topic of this paper is Ethernet redundancy for serial device servers. Three types of redundancy are available:

- **Single-network redundancy** includes STP/RSTP protocols for mesh-type topologies, and the proprietary Turbo Ring protocol for ring-type topologies. Turbo Ring for Moxa's NPort 6000 series of secure device servers supports a recovery time of under 100 milliseconds, compared to a recovery time of about 5 seconds for RSTP.
- **Dual-network redundancy** includes Moxa's Redundant COM mode, which has a recover time of "zero seconds" due to the fact that data is transmitted simultaneously over both networks.
- **Multi-host redundancy** is set up to transmit the same data simultaneously to up to four hosts. The device server duplicates the serial data and transmits the data to all of the hosts at the same time.

In addition, Moxa's DRDAS mode provides a combination of dual-network and multi-host redundancy.

Disclaimer

This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form for any purpose, without our prior written permission.