Network Redundancy Protocols

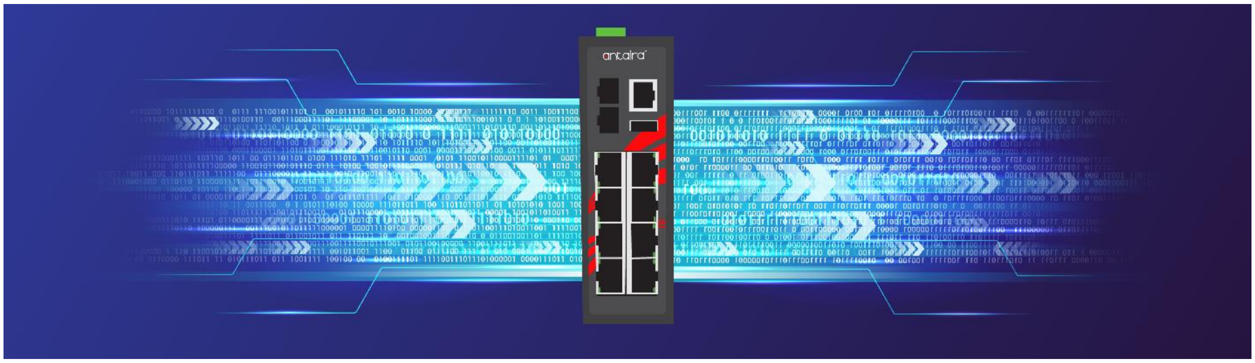
antaira®

making connectivity simple...

If industrial networks fail, the results could be disastrous. While data interruptions are worrisome for any business, sudden gaps in connectivity could put industrial organizations at risk of significant productivity loss or introduce substantive safety concerns. In practical terms, unplanned downtime costs manufacturing companies worldwide $50 billion each year — and with pandemic pressures continuing to impact both supply and demand frameworks, even small network interruptions can have big consequences.

The result? For industrial firms to drive sustained success, robust network redundancy is critical. But not all redundancy approaches are created equal. At Antaira, we recognize the need for interoperation over proprietary production. That's why we've taken an open protocol approach. In practice, this means our industrial switches are fully customizable, flexible, and easily interoperable with switches from major providers such as Cisco.

Looking to improve your network redundancy but not sure where to start? We've got you covered with a look at common connective pain points, popular network redundancy protocols, and approaches to help your team find the best business protocol.



The Challenge of Continuous Uptime

It's a question of when, not if, networks will face the challenge of unexpected disruption. The culprit could be cyberattacks, power failures, or weather events that knock connections offline. Without effective layer 2 redundancy, companies face an uphill climb to get systems back up and running and get production back on track.

Redundancy protocols help solve this problem by proving a network failover framework — if one node fails, protocols automatically reroute traffic to minimize the impact of downtime. But redundancy itself often presents a challenge when it comes to finding and deploying industrial access points, routers, and switches at scale. Here's why: while large-scale providers may promise the benefit of a substantive switch ecosystem to help boost network recovery, the protocols used by these switches are often proprietary. While this may not pose a problem for companies operating in a limited geographic area, business networking expansion quickly becomes problematic as companies are compelled to keep building out proprietary systems, even if current solutions no longer meet their needs.

Another issue is the need to overcome legacy expectations. Historically, industrial applications in SCADA or ICS systems were entirely internal. Many were air-gapped and lacked any connectivity to public networks at large. Even within intranets, access was strictly controlled to limit the risk of unauthorized use. The advent of the Industrial Internet of Things (IIoT), however, has changed the nature of networks. Now, interconnection is a key facet of operations. From sensors that help pinpoint problems or notify managers of proactive maintenance needs to internet-facing devices that interface with supplier and logistics portals, there's no facet of operations that remains untouched by the move to always-on, on-demand connections.

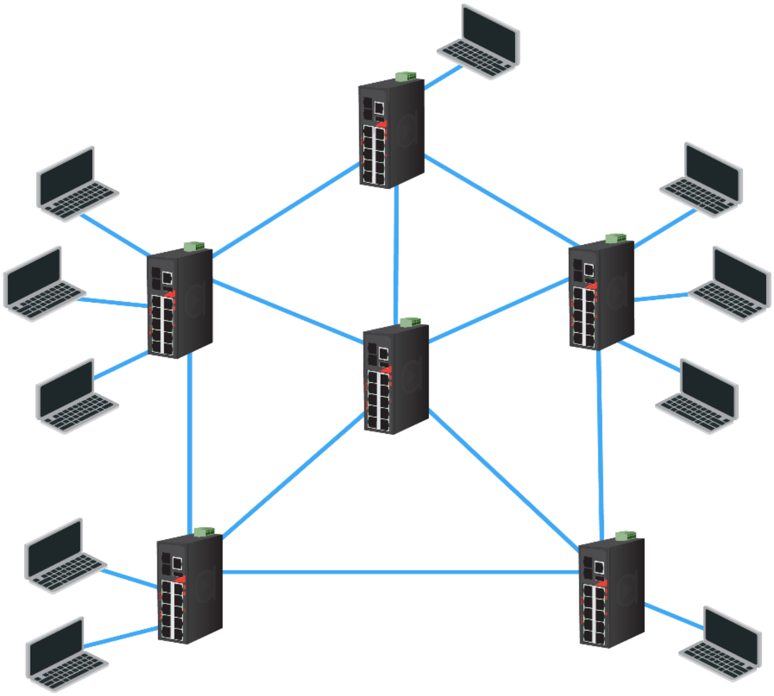
The result is a paradox: companies need protocols to deliver continuous uptime, but they're often stuck in a system that doesn't permit the flexibility they need to keep pace with changing market conditions.

Popular Network Redundancy Protocols

So what are your options when it comes to industrial network redundancy protocols? Popular types include:

Spanning Tree Protocol (STP)

Spanning Tree remains a popular layer 2 protocol. Most deployments leverage the IEEE 802.1D specification across bridges and switches, Spanning Tree creates a topology of redundant links on your network while avoiding the creation of loops. These redundant links are similar to file backups in your network. If one link fails, the connected backup links activate so users can continue to work. In practice, Spanning Tree diagrams often look like spiderwebs; multiple devices connected to a single switch, which is in turn connected to several switches to create a multi-path failover framework.



Multiple Spanning Tree (MST)

MST expands the usability of PST to include multiple trees across differing network sites. This is especially useful for companies undergoing growth and expanding into new satellite offices or operational facilities. In practice, MST makes it possible for administrators to map their preferred number of VLANs to a single MST instance — for example, if you have two distinct layer 2 topologies but six VLANs, you only need to create two MST instances and then distribute your VLANs as desired.

Rapid Spanning Tree (RSTP)

RSTP leverages the IEEE 802.1w specification to both increase availability and reduce the risk of redundant loops. By allowing network traffic to be rerouted around failed nodes, RST makes it possible to boost both network performance and availability to minimize overall downtime.

It also improves the process of preventing redundant loops by blocking redundant paths on a network. This is critical since redundant paths within a network redundancy solution cause more problems than they solve. Consider the issue of "broadcast storms." If switches in a loop configuration detect a failed node and begin broadcasting duplicate data packets, these packets inevitability reach the next node in the loop, which then receives and rebroadcasts the information. The result is a continual cycle of broadcast and rebroadcast that can quickly degrade network performance and overwhelm switches.

Ethernet Ring Protection Switching (ERPS)

ERPS offers a different approach to network redundancy. Instead of opting for the "spiderweb" approach of STP, ERPS uses the ITU-T G.8032 standard to create a ring of nodes that is naturally configured to prevent loop issues. Here's how: while nodes are arranged in a ring, one connection is always blocked to prevent the creation of a loop. This means that traffic can flow in both directions around the ring but always stops at the blocked link.

If another link in the ring goes down, however, it becomes the blocked link and the previously-blocked link is opened, in turn allowing data flow to continue at the same rate with virtually no loss of speed. ERPS rings can also be connected in multiple layers to create larger stacks that offer greater overall performance than STP. Even over hundreds of miles of fiber connections, the protected ring structure of ERPS means that ping won't drop and connections will remain stable.

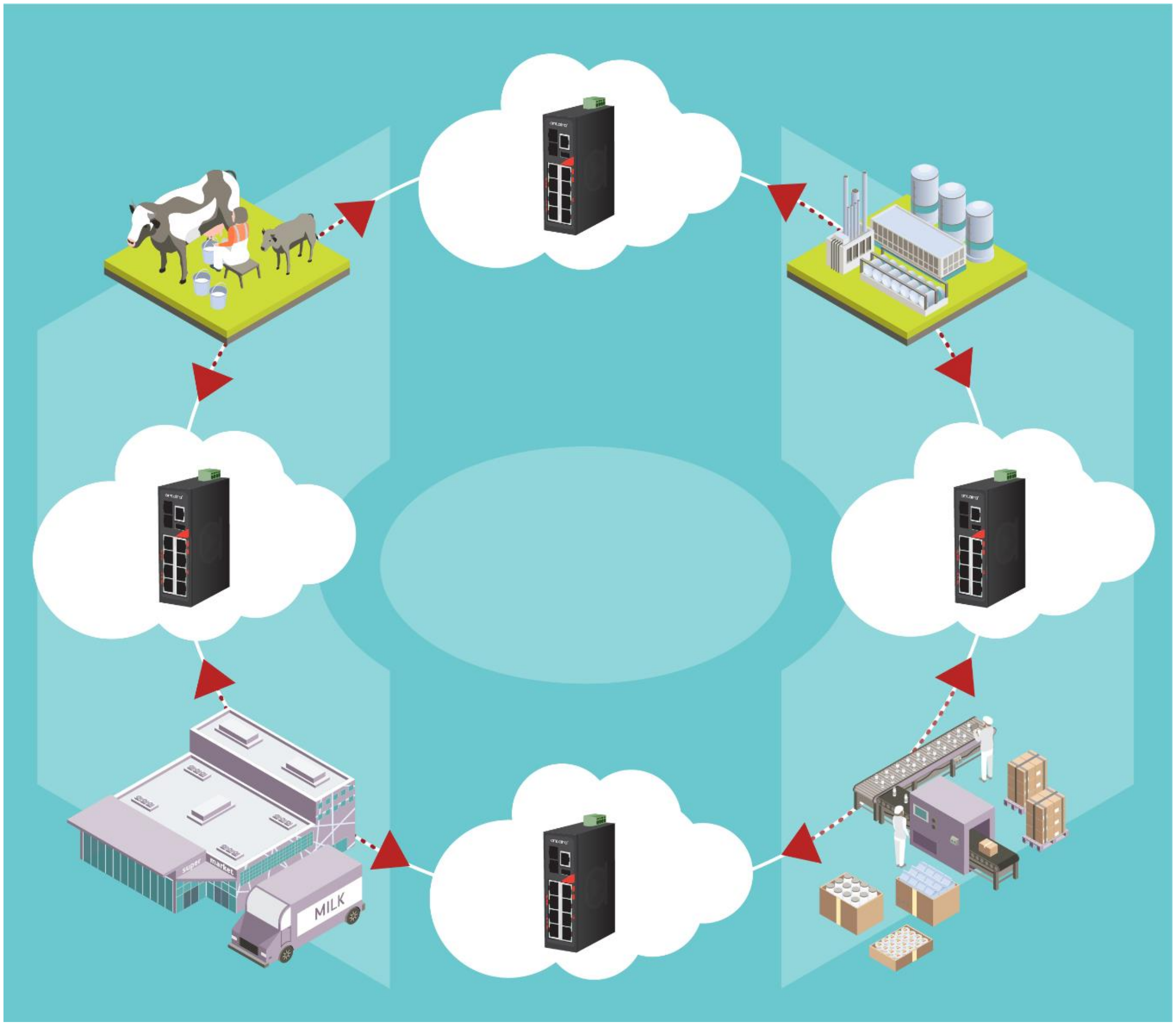
How Do I Pick the Right Protocol for My Business?

So what's the best choice for your business? Are you better served by STP or one of its variants, or is ERPS the ideal choice? The answer? It depends.

If you already have an MSTP or RSTP deployment in place and need to add new switches, it's likely more cost-effective to keep the same redundancy protocols. While removing all current STP links and rebuilding redundancy from scratch would eventually result in a more reliable network, the amount of time and effort to achieve this goal often makes it prohibitive for industrial enterprises that rely on continual uptime to maximize productivity.

ERPS, meanwhile, is a great choice if you're developing a new network deployment. With fewer complications and faster recovery times, if nodes do go down, ERPS provides the ideal framework to support mission-critical applications but comes with both time and resource commitments. It's also worth noting that ERPS is an open-source framework used by many large telecom providers, which means that it adheres to carrier-grade standards of performance and interoperability. In addition, ERPS permits link aggregation across networks, which makes it possible to create multiple links across networking switches to boost overall redundancy.

Put simply? Your use case, budget, and current framework typically determine your best fit for redundancy protocols. While ERPS does offer increased performance and reliability, this may be offset by its initial setup costs and time, especially if existing MST and RST deployments are complex and interconnected. If you're looking at building out a new redundancy framework that prioritizes rapid recovery, however, ERPS may be your best choice.



The Antaira Advantage

No matter what other manufacturers are in your cabinet, Antaira has your back when it comes to network redundancy. Operability — not proprietary ownership — is our primary focus. It's our mission to make your layer 2 redundancy both strong and simple; by using best-of-breed open source solutions, we ensure that no matter where, how, and when you connect, you've always got options to ensure your data layer delivers.

We're also here every step of the way. From technical consulting to help your business find the best-fit networking protocol to the pros and cons of popular frameworks, our teams help ensure you're on the right track. And it doesn't stop there. Our experts help set up your new networking redundancy framework and tech support is always included. Even better? Antaira customers can talk directly to our engineers to gain a better understanding of how network redundancy can be best deployed across existing industrial access points for maximum benefit.

Ready to learn more about network redundancy and reduce the risk of failure? Explore Antaria.