IoT IS HERE
IS YOUR SWITCHING INFRASTRUCTURE READY TO WEATHER THE STORM?

IN THIS ERA OF THE INTERNET OF THINGS (IoT), THE FORECAST IS OMINOUS: NETWORKS NEED TO ADAPT TO MEET THE DEMANDS OF THE VAST NUMBERS OF IoT DEVICES, THREATENING THE LOOMING SECURITY RISKS.

While no network can escape the approaching IoT storm, you can be prepared for the inevitable with:

- Weather the IoT storm with a next-gen network
- Make the switch to Aruba CX

IoT is bringing a flurry of innovation that is poised to decimate networks run by old software. Outdated software lacks flexibility to support the new demands of IoT. Fortunately, you can prepare for the storm by upgrading to a modern, programmable network—one that can adapt for mobile users, numerous sensors, and more IoT devices.

With the exponential growth of IoT devices and connectivity requirements comes a turbulent sea of security risks. Brace your network with better segmentation strategies. Dynamic Segmentation for unified policy enforcement across wired and wireless networks keeps traffic, devices, and users more secure.

There’s no torrential downpour quite like IoT devices on today’s networks. These devices will require adequate power from network switches, both now and into the future as IoT footprints grow. Set your network up for future success with always-on Power over Ethernet (PoE) and the ability to dynamically monitor and allocate PoE consumption.

As more IoT devices are onboarded onto the network, IT tasks become more complex. Simplify network management with automation. You can bid farewell to manual, static configurations like VLANs and ACLs, while improving network efficiency, reliability, and productivity.

IoT is on the rise
Around 20 billion connected devices are forecast by 2023, of which around 18 billion will be related to IoT.

80% of IT organizations report they’ve found IoT devices on their networks that they didn’t install, secure, or manage.

41% of IT teams admit that their network security and segmentation is not properly implemented.

Global IoT spending is expected to top $1 trillion by 2023.

41% of IT teams admit that their network security and segmentation is not properly implemented.

Innovation freeze due to outdated software

A Blizzard of Complexity

As more IoT devices are onboarded onto the network, IT tasks become more complex.

- Simplify network management with automation.
- You can bid farewell to manual, static configurations like VLANs and ACLs, while improving network efficiency, reliability, and productivity.

There’s no torrential downpour quite like IoT devices on today’s networks. These devices will require adequate power from network switches, both now and into the future as IoT footprints grow. Set your network up for future success with always-on Power over Ethernet (PoE) and the ability to dynamically monitor and allocate PoE consumption.

Lightning strikes: power drain likely

With the exponential growth of IoT devices and connectivity requirements comes a turbulent sea of security risks. Brace your network with better segmentation strategies. Dynamic Segmentation for unified policy enforcement across wired and wireless networks keeps traffic, devices, and users more secure.

Looming security risks

While no network can escape the approaching IoT storm, you can be prepared for the inevitable with:

- Turnkey automation for easier, simplified operations
- Dynamic segmentation for enhanced security
- Distributed analytics to ease network management
- Always-on PoE and multi-Gig Ethernet to boost capacity and reconfigure easily

With an end-to-end switching solution, your network will have just what it needs for every potential IoT hazard.

To learn more, please visit: www.cspitechsolutions.com or call your CSPi representative at 800-940-1111 or email tech_solutions@cspi.com