Management and Wireless in the Data Center
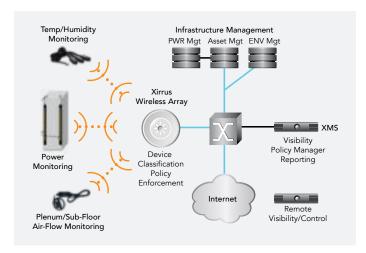
Raritan
Know more. Manage smarter.™

XIRRUS®
High Performance Wireless Networks

Management and Wireless in the Data Center

Worldwide demand for new and more powerful IT-based applications, combined with the economic benefits of consolidated physical assets, has led to an unprecedented expansion of data centers in both size and density. Limitations of space and power, along with the enormous complexity of managing a large data center, have given rise to a new category of tools with integrated processes – Data Center Infrastructure Management (DCIM).

Once properly deployed, a comprehensive DCIM solution provides data center operations managers with clear visibility of all data center assets along with their connectivity and system status. However, along with the advantages of this new approach come challenges, specifically how to interconnect all the intelligent monitoring and control devices.

First generation data center monitoring systems relied on Ethernet, but this required additional cabling, switches, cooling, rack space, and more. Historically wireless was seen as only an overlay technology, supporting but not replacing the wired infrastructure. That view is now changing as the result of advances in Wi-Fi technology as well as the explosion of hand-held devices penetrating the data center. Many industries including military, banking and medical have tested and verified that wireless systems can indeed support the reliability, performance and security requirements of mission-critical systems.

Xirrus and Raritan has joined together to provide a sophisticated wireless monitoring and management solution, which addresses three areas. These include:

- Reliability
- Security
- Monitoring

Xirrus – High Performance Wi-Fi for Secure Environments

Reliability

Reliability is probably the number one concern of IT administrators and also the most misunderstood of wireless capabilities. Deployed correctly wireless can actually be more reliable than a wired network. Consider this, if a wired connection is broken (port, cable, patch panel, switch), IT intervention is required to correct the failure. Wired networks were always highly reliable at the closet and core layer and able to route traffic around failures; however resiliency fell short from the switch to the client with only a single, static cable. With Xirrus wireless, a client that loses connection with one radio can quickly send transmissions to another radio within tens of milliseconds.

The key to reliability is taking advantage of the 'dynamic' healing that is available with Xirrus wireless:

- **Radio/Client Level** – Wireless is designed for mobility at its core, engineered to allow devices to 'roam' from one radio to another and this capability is not limited to mobile clients. Fixed devices, like system monitors, are able to logically roam to another radio if the primary connection is lost and this requires no IT intervention. Most roaming is accomplished in under 50ms so the impact and potential loss of data is minimized.

- **Device Level** – Design the network so each wireless client can 'see' multiple Xirrus Arrays, so failure of one device will not take down the network. Second, eliminate any potential single point of failure, such as legacy centralized wireless controllers. In this way a failure can be compensated by neighboring devices, eliminating any potential for a system-wide failure.

- **Uplink/Backhaul Level** – Ensure that all wireless access devices provide multiple uplink options, both wired and wireless. In this way failure of one device cannot disable a segment of the network. A wireless or wired failure can be routed around the problem.

- **Access Point Level** – Access Point (AP) requirements will be based on building construction. The use of Xirrus Arrays with multi-radios and high-gain antennas provide the most flexibility. Heavy use of concrete block walls will require more APs, while sheetrock environments considerably less. All environments will vary, even building-to-building and floor-to-floor. It is recommended a predictive survey be performed and which is validated with an on-site survey if required.

Security

Wireless networks are now common in many security conscious industries such as healthcare, financial services and even government facilities. A wireless network designed with best practices is widely considered equal to or more secure than a wired network. By applying multiple layers of security through the Xirrus Array such as encryption, authentication, firewalls, and Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), the wireless network can be secured.

- **Wireless Security** – Security in most wired networks is based on physical containment of the network. As long as only authorized users have access to the cables, equipment, and servers communications are secure. But, the RF signal from an Array cannot be contained within a specific physical area. As a result, protection methods – most importantly securing the data itself – are employed to secure the communication channel. With this approach, even if communication is observed or intercepted, the actual data is not compromised.

- **Layered Security** – Network security, wired or wireless, encompasses a number of layers – from the physical security of devices all the way up to the security of applications running on the network. Layered security uses a suite of protection methods. An example of this is an Internet firewall. It is a fundamental security tool in protecting networks from attacks via the Internet. However, if a malicious attack is launched from the inside by an employee, one level of security has already been breached and it is up to other layers to contain the attack.

Raritan – Monitoring Systems for Data Centers

Monitoring

Monitoring systems are essential elements of any data center deployment and many critical elements must be considered for success.

- **Intelligent Rack PDUs** – Sophisticated energy management systems utilized with Ethernet-based intelligent rack power distribution units (iPDUs) are now available for wireless networks. Raritan iPDUs offer modular, scalable building blocks for the data center and are a key element for successfully deploying power and monitoring systems. One of the easiest ways to implement such a system is with an iPDU which supports USB wireless transmitters.

Some factors to consider when selecting an Raritan iPDU are the following:

- Monitoring and metering of current (amps), voltage, power (kVA, kW) and energy consumption (kWh)
- ISO/IEC +/- 1% billing-grade accuracy of kWh
- Power information from individual outlets, lines and circuit breakers

- **Electronic Asset Tracking** – Even modest-size data centers have an enormous number of IT assets, from servers to storage to networking equipment. Tracking these assets is often accomplished using spreadsheets and Visio® diagrams, or by developing a home-grown system, which can be very labor intensive. However, if you miss a few moves, adds or changes, it can become a challenge to know what you have and where it is located.

  Raritan electronic asset tracking can now be done wirelessly and provide robust readings which allow data center operators to have accurate, automated, real-time inventory of all IT assets and their location. An asset management solution helps manage the physical components from acquisition to deployment to provisioning to redeployment to disposal.

- **Power Monitoring and Metering** – The first step to managing power is to baseline current power consumption. Ideally, this will be done in a way that provides useful statistics to be compared over time. Using Xirrus Arrays eliminate the need for deploying Ethernet connections to the Raritan PDUs.

  Ideally, the power should be measured at the individual outlets of a rack PDU. Monitoring the power at the outlet level ensures that IT equipment power consumption can be uniquely identified to a particular device. This means specific actions can be taken to improve efficiency such as eliminating less efficient devices or virtualizing some physical servers.

- **Environmental Monitoring** – Another way to improve efficiency is to increase the temperature of the air used to cool IT equipment thereby reducing the power consumed by cooling and moving air. However, care must be taken that hotspots don't develop. To ensure that all IT equipment is in a healthy environment it is wise to mount temperature and humidity sensors at each rack. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommend placing temperature sensors at the top, middle and bottom of the cool air inlet side.

  Airflow and air pressure sensors may be deployed to make sure that the cooling system is working properly. Airflow sensors can be placed in plenums to monitor the movement of air. Air pressure sensors can monitor the difference in pressure between the floor and the subfloor or a hot aisle and a cold aisle.

- **DCIM Solution Software** – The information generated by the monitoring systems described above can be aggregated and analyzed by Raritan DCIM software. Managers who are concerned about the utilization, availability and cost of power can track this information from a central location. Data center managers can use information gathered by various sensors to be more energy efficient and to fully utilize their infrastructure.

Those who are concerned about monitoring capital assets can tap into the same DCIM platform to view real-time information about facilities, networks and IT. Such a tool can visualize the infrastructure to help manage the placement of IT equipment and support informed capacity management decisions and keep accurate track of data center assets.

Xirrus and Raritan – Cost Efficient Secure Monitoring for Data Centers

While most IT administrators understand the advantage of deploying enterprise wireless infrastructure, some of the benefits might not be as obvious. These include the following:

- **Lower capital and operational investment** – When you combine the material costs, the cabling, installation and deployment time, the total cost of a Xirrus wireless network can be dramatically lower than that of a wired network. Less devices, less cabling, less switch ports equal less cost to deploy and less cost to support and manage. Some data centers are now allocating only one Ethernet drop per cabinet.

- **Faster installation** – A wired network requires miles of cabling, wall jacks, patch panels, equipment racks, at least one switch port per connection, lots of patch cables, closet power, cooling and finally an enormous amount of time to install or down time to upgrade.

  On the other hand, a wireless network requires dramatically less cabling to pull, terminate and test, (one cable to an AP can support hundreds of connections). With just a few wireless access devices a wireless network can be deployed and operational in a fraction of the time. Time and money saved on the network means more resources can be placed on best practices for installing sensors:

  – 20 to 50 iPDUs per wireless access point, typically two iPDUs per rack

  – Upgrade from basic PDUs to iPDUs without the need for Ethernet to the PDU

  – Wi-Fi dock and USB stick/antenna installed on top of a rack to ensure proper bidirectional signal reception

- **Lower costs** – Ethernet cable run costs can range anywhere from $150 to $1000 per drop if you include cabling, termination and add costs for the switches required to connect those cables. Studies have shown it is possible to deploy a wireless network for less than the cost of just pulling the wired cables. Add to this the fact you never need to upgrade your cabling plan. This cabling for the most part cannot be relocated. However, when a wireless network is decommissioned, APs can easily be moved to the next location, eliminating almost all stranded costs.

- **Inherent redundancy** – Wired or wireless administrators require some level of redundancy in their networks. One area of wired networks where redundancy is seldom available is the final hundred meters (switch to device). If a wiring fault occurs in this area IT intervention is required to resolve the problem. Unlike wired networks, a wireless network has inherent redundancy at the edge. If deployed correctly each client should see multiple radios. If a radio/AP were to fail the station will automatically roam to another radio, normally with minimal interruption.

- **Green initiatives** – Global warming and carbon emissions have become growing concerns. Wireless technologies can help reduce a data center's carbon footprint through less cabling, cooling, copper, and plastics.

- **Reduced management role for network moves and changes** – When a wired user relocates normally IT must reconfigure switch ports, VLANs, phones service, etc. Wireless is designed to work anywhere; users are not tethered to any specific port. Typical Moves, Adds and Change efforts are essentially eliminated.

Summary

A Xirrus wireless network simplifies and speeds the deployment of Raritan environmental sensors and intelligent power monitoring, including cost benefits realized through deploying secure wireless DCIM systems. Using wireless communications eliminates the need for Ethernet cabling to iPDUs, thereby eliminating cabling, switches, rack space allocations, and costs. Wi-Fi is also a green technology that lessens a corporation's carbon footprint by reducing the power, cooling, copper and plastics consumed.

Wireless monitoring and management is reliable enough for even the most critical systems, providing an enterprise class solution that is ideal for monitoring in real-time the environmental and power conditions in IT dense areas. The Xirrus and Raritan solution not only provides the highest reliability but also an affordable, flexible and easy to deploy data center monitoring solution.

For More Information

For more details about how Xirrus can help you solve the pending influx of Wi-Fi devices visit us at **www.xirrus.com** or send us an email at **info@xirrus.com**.

For more details about how Raritan can help you solve your Data Center Power management challenges visit us at **www.raritan.com** or send us an email at **sales@raritan.com**.

About Xirrus

Xirrus is the leader in high performance wireless networking. The enterprise-grade Xirrus Wi-Fi Array enables wireless connectivity for small businesses to the Fortune 500. Headquartered in Thousand Oaks, CA, Xirrus is a privately held company that designs and manufactures its family of wireless products.

About Raritan

Raritan is a proven innovator of power management, DCIM software, KVM and serial solutions for data centers of all sizes. In more than 50,000 locations worldwide, our hardware and software solutions provide IT and facility directors, managers and administrators with the control they need to increase power management efficiency, manage assets, change and capacity, and enhance branch office operations.

Raritan is an active member of the Green Grid, Climate Savers Computing Initiative, and the Leadership in Energy and Environmental Design associations. The company has been recognized by the EPA for its contribution to the agency's data center initiative.

Raritan.
Know more. Manage smarter.™

1.800.724.8090 Toll Free in the US
Raritan Inc. 400 Cottontail Lane
Somerset, NJ 08873 USA

To learn more visit:
raritan.com or
email sales@raritan.com

XIRRUS®
High Performance Wireless Networks

1.800.947.7871 Toll Free in the US
+1.805.262.1600 Sales
+1.805.262.1601 Fax
2101 Corporate Center Drive
Thousand Oaks, CA 91320, USA

To learn more visit:
xirrus.com or
email info@xirrus.com