NAS Wireless
Proven Strategies for the Implementation of the Cisco Stack

Unleashing the full potential of a robust solution portfolio like that of Cisco's can be a daunting task even for enterprises that have a large IT force. Clearly, the need of the hour for these behemoths is to partner with a firm that would bring in in-depth know-how, share their expertise, and empower them with the right suite of functionalities in an economical manner. To this end, a company called NAS Wireless is saving the day for businesses. NAS Wireless' proven methodology emphasizes on establishing an active partnership with their client as they prep them up for the quick and successful implementation of Cisco's solutions. The crucial role that
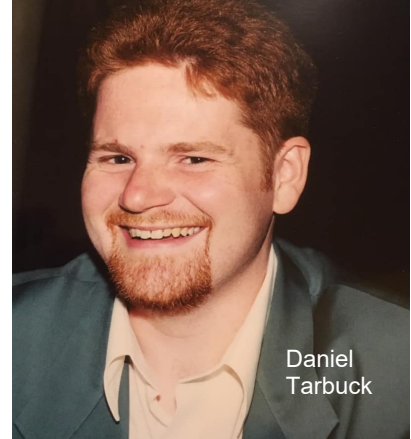
leverage their practical experience in the Cisco arena to create success stories akin to those mentioned above. "As a professional service provider, we are here to help the big players in tapping the Cisco solution stack at a reduced cost," states Jim Bradfield, the CEO and director of NAS Wireless. Comprised of an agile team of highly skilled technology veterans with an average experience of 12 years, NAS Wireless removes the noise around the selection and deployment of the right solution while executing Cisco-based projects globally. The company analyzes the existing infrastructure of its clients, their business requirements, and outlays an elaborate roadmap before embedding its products.

Daniel Tarbuck

> **As a professional service provider, we are here to help the big players in tapping the Cisco solution stack at a reduced cost**

NAS Wireless plays in the Cisco space can come to the fore through a real-life scenario, where a customer had to deliver a new wireless experience based on the Cisco solution stack to its employees. The client sought support from NAS Wireless when the implementation of the solution almost touched its deadline. In its endeavor to help the company, NAS Wireless collaborated with the client's solution architect, performed a gamut of tests to ensure successful deployment of the Cisco-driven wireless solution, and enabled them to meet their desired objective within their estimated timeframe.

Unlike their theory-oriented competitors, NAS Wireless and its team

To institutionalize a universal enterprise network that facilitates interoperability and seamless communication between a variety of devices, NAS Wireless deploys Cisco Aironet access points that can connect Wi-Fi devices, which are a part of multiple wireless environments. Through Cisco's Wireless Controllers, they eliminate the complexities that may arise in the configuration and management of these devices. NAS Wireless acknowledges the significance of automating device operations, and to that end, they introduce the Cisco DNA Center for network management. While unlocking data and analytics through the Cisco DNA Center, a clear-view of network performance,

at the individual device level, can be rendered at a reduced cost. Businesses can now create network policies, automate their implementation, and ensure better uptimes and enhanced security.

While NAS Wireless continues to untangle the puzzles in the Cisco landscape, they also ace the in the field of wireless communications. "We are not afraid to face the challenge," says Daniel Tarbuck, the Principal Solutions Architect at NAS Wireless. To illustrate their proficiency in wireless solutions, Tarbuck highlights the episode of how they helped a warehousing company counter their challenges. The client faced inefficiencies in collaboration while operating their warehousing facilities. NAS Wireless recommended applications that could be used to enhance their operation and communication for the customer. Eventually, the warehousing firm achieved optimal operating efficiency, and they were able to facilitate seamless communication among all stakeholders.

In the good books of several successful businesses, NAS Wireless has ambitious plans in the pipeline. As a part of its expansion strategy, the company aims to enter into IoT and the cloud arena and solve business problems in security. CR