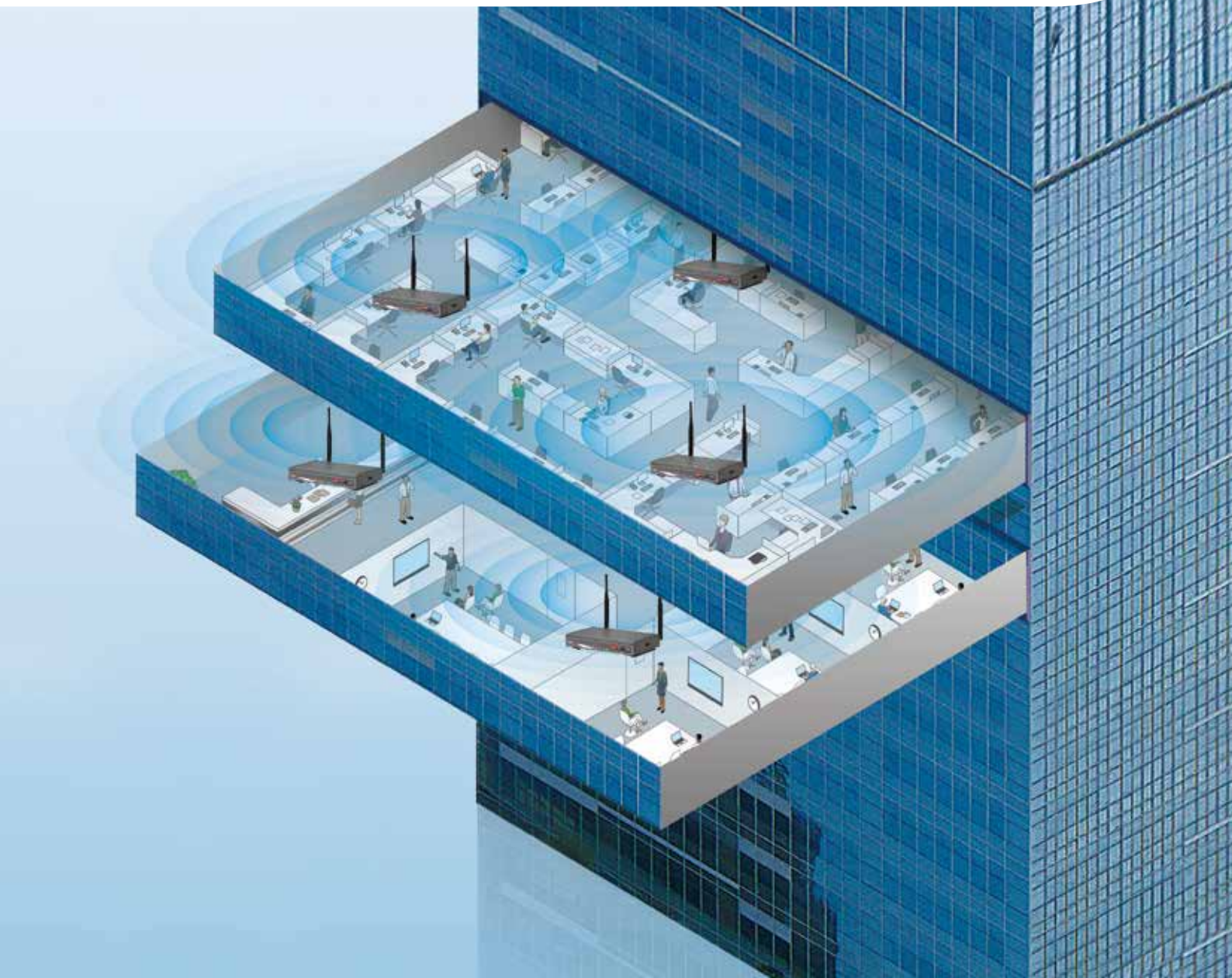
NEXCOM
The Intelligent Systems

Application Story

Enterprise Wi-Fi Controllers
Unify Wireless Working Environment



As business expands and mobile tech gadgets flock into the working environment, enterprises need a wireless network that is reliable, secure, manageable, and yet flexible to keep up with their operation and worldwide expansions. Like other enterprises, NEXCOM also faced challenges in building a scalable Wi-Fi infrastructure when its staff numbers increased from about 400 to over 700 and its manufacturing and office space quadrupled during 2011 to 2015.

The staff numbers almost doubled and applications such as video conferencing, voice communication and multimedia streaming accessed by bring your own device (BYOD) all consumed significant amount of wireless bandwidth. This placed a heavy resource burden on the existing wireless network. In addition, the existing wireless infrastructure lacked centralized management and the capability to provide a seamless and secure roaming network between NEXCOM global headquarters and factory site that operated in different areas, each with many floors. A trusted, manageable wireless network infrastructure was required to unify data communications.

In this use case, NEXCOM is going to share what its MIS team has done in its global headquarters and factory site to build a trusted, seamless wireless network environment. The new wireless network even covers two China subsidiaries into its infrastructure. Soon, NEXCOM will also implement this successful model to its worldwide subsidiary offices and fulfillment centers located in China, Japan, Italy, Taiwan, United Kingdom, and United States.

Key Objective

Build a high bandwidth, reliable wireless infrastructure with security mechanism to enhance working efficiency and protect confidential information.

Challenges

The existing wireless networking infrastructure struggled to handle the increased bandwidth demands of growing staffs, and lacked flexible security policies to define, restrict and control access of the many different types of BYOD devices. Management of the wireless network was also cumbersome as no centralized management was in place.

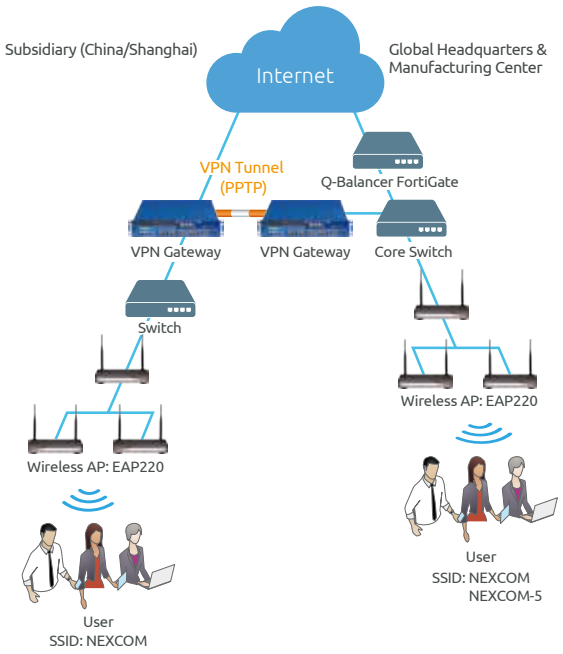


Figure 1. Former Wi-Fi solution management layout

The challenges that NEXCOM's MIS team faced included:

How to deliver seamless roaming with a one-time login

All NEXCOM staffs needed to login to the corporate domain network first then to the Wi-Fi access points (AP) to gain connectivity. A one-time login through employee account can simplify login process and offer staffs seamless wireless roaming when moving across different work floors and factory sites.

How to build a trusted and secure Wi-Fi access

Implement flexible security policies for different users and BYOD devices based on the authentication, authorization and accounting (AAA) framework, and support user-based login tracking for monitoring access and usage.

How to carry out central management of field APs

Map out and design a wireless network with a single point of centralized management that can manage up to thousands of APs. In addition, implement remote management capabilities to aid the MIS team to remotely access, diagnose, and solve issues for field APs across offices and factory sites.

How to offer visitors Wi-Fi service

Provide visiting guests with seamless Wi-Fi connectivity while making sure that the public guest network and internal private network are securely separated to ensure critical data is secured and protected.

Solution and Benefits

Realizing that these challenges will require a wireless network with broad Wi-Fi coverage, seamless roaming, and central management, NEXCOM's MIS team chose to implement an enterprise Wi-Fi network using WLAN controllers to supervise all field APs across its global headquarters, factory sites, and worldwide subsidiaries.

Deploy AAA to build secure, seamless roaming with one-time login

NEXCOM's WLAN controllers offer 802.1X user authentication to ensure that only authorized users can access the corporate network through validating their original employee login name. For security control, role-based policies define the permissions of different user groups on the corporate network. Combined with multiple AP roaming support and one-time login, users can experience uninterrupted Wi-Fi connections when traversing between office floors and factory sites.

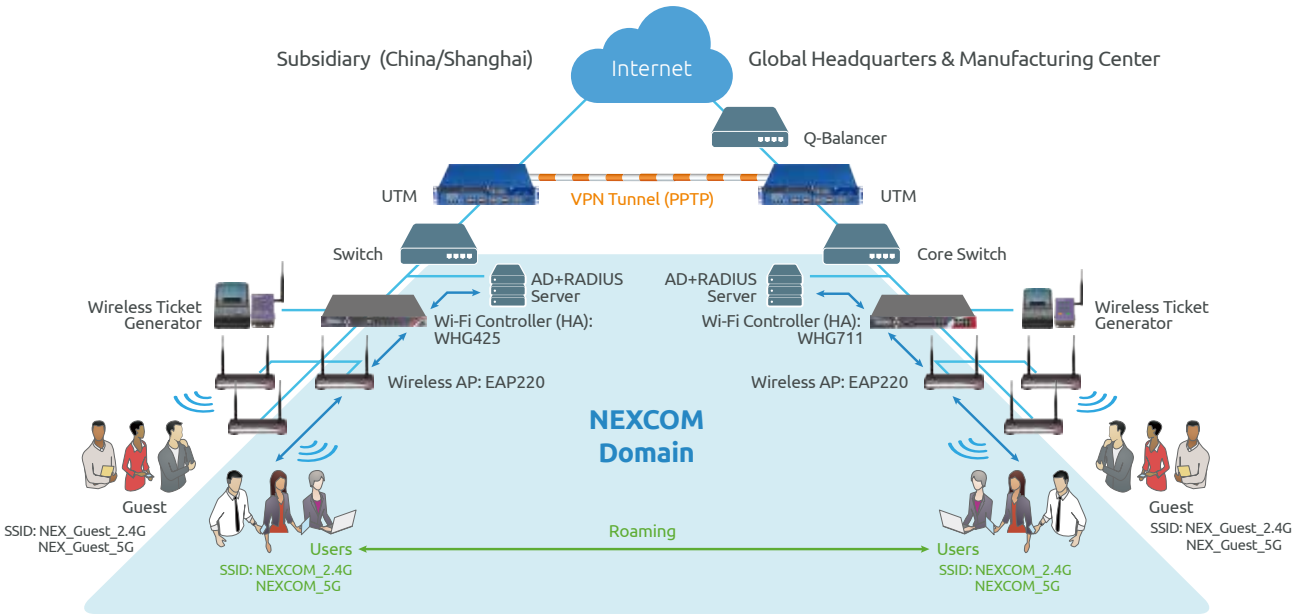


Figure 2. Redesigned Wi-Fi solution with wireless controllers and APs

Incorporate high availability (HA) into enterprise Wi-Fi controllers

The WLAN controllers support controller service failover to provide HA to ensure a reliable and always-on wireless network.

Offer secure remote AP management and maintenance

VPN and remote management allow real-time AP management, monitoring and reporting to simplify troubleshooting and enable MIS to quickly react and debug wireless connectivity issues in a secure, encrypted tunnel.

Monitor and analyze traffic

In addition to AP monitoring, the WLAN controllers can keep track of event logs, detailed user and network traffic activities for MIS to easily analyze data behavior and measure network efficiency.

Allow visitors use social media login

Grant visiting guests free Wi-Fi access conveniently through social media login such as Facebook, Twitter and Google+.

Solution list

The controllers and APs used in NEXCOM's wireless network infrastructure are as below:

Model	Description
WHG425	WHG425 secure WLAN controller 19" 1U, Gigabit
EAP220	Light industrial AP, 802.11an+802.11b/g/n, dual RF, concurrent AP (0°C to +60°C)

Summary

By leveraging enterprise Wi-Fi controllers, NEXCOM's offices and factory sites are now operating under a trusted Wi-Fi infrastructure, integrating into the business operation wirelessly and seamlessly. The secure and robust remote management, monitoring and reporting capabilities offer MIS unparalleled flexibility and efficiency in maintenance, while the wide Wi-Fi coverage and speedy connection provide both staffs and guests a convenient and reliable internet access at anywhere and anytime. After a few months of trial run, the staffs and MIS team were satisfied not only with the convenience, but also the effectiveness of the wireless working environment.

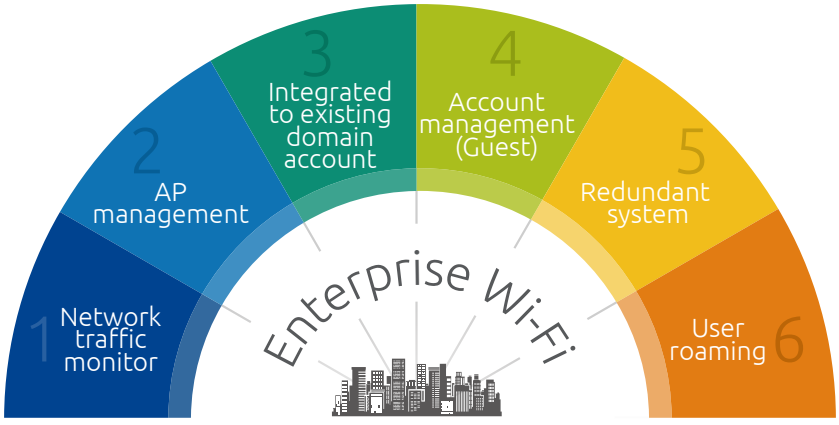


Figure 3. Manage enterprise Wi-Fi networks to meet surging demands

Founded in 1992, NEXCOM integrates its capabilities and operates six global businesses, which are Multi-Media Solutions, Mobile Computing Solutions, IoT Automation Solutions, Network and Communication Solutions, Intelligent Digital Security, and Medical and Healthcare Informatics. NEXCOM serves its customers worldwide through its subsidiaries in five major industrial countries. Under the IoT megatrend, NEXCOM expands its offerings with solutions in emerging applications including IoT, robot, connected cars, Industry 4.0, and industrial security.

www.nexcom.com

 Published in October 2015