Empowering Modern Healthcare with Seamless, Secure Wireless Networks

Overview

The university hospital in Gangdong District faced significant network challenges, including frequent connectivity drops, congestion in high-density areas, and network security concerns. To address the issues, the hospital collaborated with Newnet Information Technology and Zyxel Networks to deploy a secure, high-performance, and easy-to-manage WiFi network capable of supporting heavy outpatient traffic while maintaining strong network protection. These upgrades significantly improved operational efficiency and enhanced satisfaction for patients and staff.

Challenges

The hospital faced significant wireless network challenges across its main, annex, and research administration buildings. Aging equipment struggled to handle rising WiFi traffic, leading to frequent disruptions and unstable connectivity. A lack of centralized management further compounded these issues. The hospital needed a reliable and secure wireless solution that could segment networks, keeping staff WiFi hidden from visitors, while enabling automatic connections throughout the hospital and even when moving between buildings. At the same time, reliable WiFi for visitors was essential to enhancing patient satisfaction and overall experience.

Solutions

The hospital serves approximately 4,000 outpatients daily, with hundreds of devices connecting and generating traffic, including video streaming and mobile gaming. In the central lobby on the first and second floors, WiFi usage exceeds 70% on both 2.4GHz and 5GHz bands due to a mix of business and telecom APs. Usage above 70% can slow WiFi, and above 90% may cause disconnections. DFS channels were used to expand available spectrum, though radar signals often disrupted service.

To minimize downtime, WAX650S APs with Zero-Wait DFS were deployed. Each WAX650S features a third radio capable of scanning channels separately while maintaining WiFi service. When a radar signal is detected, the network immediately switches to an available channel, ensuring uninterrupted connectivity.

Customer
University Hospital in Gangdong

Industry
Healthcare

Location
Seoul, South Korea

Partner
NewNet Information Technology

Customer Background

The hospital, comprising a 15-story main building and a 4-story annex, houses over 700 patient beds and provides medical services to thousands of visitors daily. A reliable wireless network is essential to ensure smooth operations for both staff and patients, ranging from accessing patient records to enabling visitors to stay connected during their time at the facility.

Results

With these improvements, the hospital's network infrastructure became more reliable, secure, and easier to manage. Zyxel Networks' solution empowered staff to focus on their work, confident that the technology would support their tasks. Staff can move freely between floors and buildings without worrying about connection drops. The new network boosted operational efficiency; patients and visitors enjoy stable, high-speed internet, even in crowded areas such as lobbies and waiting rooms. Advanced cybersecurity measures protect data while maintaining network integrity, and the centralized management platform enables real-time monitoring and rapid issue resolution, reducing downtime and improving overall productivity.

- Stable high-density WiFi connections supporting 4,000 daily outpatients and hundreds of concurrent devices with Zero-Wait DFS
- Seamless roaming via Smart Steering for uninterrupted medical team mobility between floors
- Advanced data security using Zero Trust architecture and isolated SSIDs
- Centralized management enabling real-time monitoring and proactive troubleshooting

Areas used by hospital staff, such as IT offices, research labs, nursing headquarters, operating rooms, and inpatient wards, have lower user density and were equipped with NWA90AX APs. The NWA90AX provides enough performance for clinical tasks while also allowing patients and caregivers to browse and stream smoothly. After deploying access points based on user density, QoS was configured to manage limited bandwidth and prevent any single user from monopolizing resources, ensuring stable WiFi for all. Separate SSIDs and VLANs were established for staff and visitors, enabling independent policies and secure network isolation. The APs support up to eight SSIDs, providing flexible segmentation. The staff SSID is hidden to prevent unauthorized access, while the guest network allows internet access but blocks device-to-device communication for enhanced security. As patients move between examination rooms, testing areas, and amenities, and staff work across wards, unified WiFi names enable automatic connection to nearby APs. Smart Steering ensures seamless roaming by switching devices to a stronger AP when the device's wireless signal drops below a certain threshold.

All network equipment is centrally managed, giving IT staff real-time visibility across multiple buildings. Summary reports provide hourly usage and client statistics, while a mobile app and real-time push and email alerts facilitate troubleshooting and minimize downtime. SecuReporter, a cloud-based intelligent analytics and reporting service, provides detection details for blocked malicious traffic and attack types, with AI insights and reports sent to registered email addresses.

Product List

- NWA90AX WiFi 6 Access Point
- WAX650S WiFi 6 Access Point

- GS1920-24HPv2 Smart Managed PoE Switch

- USG FLEX 700 Firewall
- USG FLEX 500 Firewall