MADRID PROPELS NEW EMERGENCY HOSPITAL IN THREE MONTHS IN CITY’S BATTLE WITH COVID

Provide secure, critical network connectivity to a new 1,000-bed hospital built in record time.
Few 1,000-bed hospitals are built in just 100 days but the Covid pandemic has forced health authorities to rethink their project timelines.

"Hospital de Emergencias Enfermera Isabel Zendal is a response to the pandemic but it has been designed for the long term," says Jose Maria Dominguez, Networks Transformation Manager, Madrid Digital, the organisation that manages technology for all public healthcare sites across the Spanish capital. “We wanted to take advantage of the latest advances in campus networks to develop a hospital model that is more agile and also easier to operate.”

**EMERGENCY HOSPITAL ADDRESSES THE URGENCY OF COVID**

Hospital de Emergencias Enfermera Isabel Zendal in Madrid’s northern suburbs was built to relieve strain on the city’s struggling healthcare system. Plans for the hospital were sketched out in July 2020. Fully financed by the European Regional Development Fund (ERDF) and developed by the Community of Madrid, it opened just over three months later in late November.

The environment needed to be fully functional, with all systems and applications running reliably, while delivering on the vision of a fully digital hospital and connected care. All staff, whether clinical or ancillary, would need the ability to communicate and access their platforms and information. Added to that, all critical equipment and technology was to be reliably and securely onboarded and connected to the network.

The Covid situation added an extra layer of complexity to the challenge. Access to the hospital and footfall needed to be carefully managed, whether for the public or for staff.

The crisis also meant that Madrid Digital was required to work across multiple projects and so resources for the Hospital Enfermera Isabel Zendal build were tight.

**REQUIREMENTS**

- Enable Madrid to open an all-new, fully operational hospital in three months
- Remote management to reduce the need for on-site support
- Allow complete mobility across the 80,000sqm site

**SOLUTION**

- Wi-Fi 6 Aruba Unified Access Points
- Mobility Controllers
- Mobility Conductor
- Aruba CX 8325 Core Switches
- Aruba CX 8325 Aggregation Switches
- Aruba CX 6200 Access Switches
- Policy Enforcement Firewalls (PEF)
- ClearPass Policy Manager with NAC
- ClearPass Device Insights
- AirWave Network Management
- NetEdit
- User Experience Insight Sensors (UXI)
- Dynamic Segmentation

**OUTCOMES**

- Meets demanding project timelines, with hospital operational to published deadline
- Enables hospital to create ‘clean’ zones with secure access, complete mobility and environmental sensors
- Establishes layered network security for different users and devices
- Ensures network flexibility to allow for dynamic change of space and purpose across the site
- Profiles, secures and manages connectivity of all authorized IoT devices, while excluding all other

"This project began in record time and we’ve been able to install the network without impacting the physical build of the site," says Dominguez.

**ENSURING CONTROLLED SITE ACCESS**

Aruba technology became a linchpin of the hospital. It creates a unified architecture, bringing together IoT infrastructure, smart sensors and occupancy tracking, integrated on Aruba’s Wi-Fi 6 platform. It also ensures a zero-trust approach to device and user security.

It means that Hospital Enfermera Isabel Zendal can control network access on the site and confidently deploy the latest
We have almost 2,000 devices connected to the network, around one quarter by Wi-Fi. To manage such complexity was possible thanks to Aruba ClearPass Device Insight.

JOSE MARIA DOMINGUEZ
Networks Transformation Manager, Madrid Digital

connected medical technology and innovations. The network can be managed remotely, meaning fewer technicians have to visit the site. This reduces risks to personnel in the short term, while ensuring increased efficiency and productivity over time.

“Right now, it’s important that we limit access to only the most important people. Aruba helps us create a safe, monitored workplace,” says Dominguez.

NETWORK VISIBILITY IN A FAST-CHANGING HOSPITAL ENVIRONMENT
Monitoring and visibility over the hospital’s Aruba architecture is provided through the AirWave network management platform, while for additional granularity of configuration and change management for the switching infrastructure, NetEdit software is used.

To complete the visibility over the network and to ensure seamless access control, Aruba ClearPass Policy Manager provides the necessary role-based policy automation, unified for both the wired and wireless network.

To further enhance the IT team’s view over the entire spectrum of the connectivity experience, Aruba UXI sensors have been deployed throughout the hospital. This is a cloud-based service assurance solution that emulates an end-user device to check on network health and troubleshoot problems on the fly. It constantly evaluates the performance, connectivity and responsiveness of the network infrastructure as well as internal and external services or applications.

Unified infrastructure architecture simplifies rapid deployment
The hospital’s access network is mainly based on around 300 Wi-Fi 6 APs with integrated Bluetooth and Zigbee interfaces, while an Aruba CX switching architecture offers a consistent and scalable approach to design, management and maintenance of the wired infrastructure.

The APs are managed by Aruba 7220 Mobility Controllers orchestrated by a Mobility Conductor. For the wired network, Aruba CX 8325 switches constitute the network’s core and aggregation layers. The access layer is based on Aruba CX 6200 switches which also provide POE for all the APs. Each layer has been constructed with full redundancy, using virtual stacks based on VSX link aggregation.

Software and firmware upgrades can be managed and automated with no interruptions to service and with very little impact on service performance. Thus, the IT team can program updates on a regular basis. Downtime for maintenance is not an option in a place like Hospital Enfermera Isabel Zendal.

A ZERO-TRUST APPROACH TO NETWORK SECURITY
The 80,000sqm hospital has a total of 1,056 beds - 48 of which are in intensive care units (ICUs). The ventilation system renewes the entire facility’s air every five minutes. Sensors track staff, patients and equipment through differentiated ‘clean’ and ‘dirty’ circuits.

This is the first hospital in Madrid where it is possible for doctors to work entirely off the wireless network.

While a seamless experience and high quality connectivity for staff, equipment, patients and guests is important, the hospital needs to ensure that only authorised entities are able to connect and that each is provided with the appropriate level and quality of access. As the network and the number of connections grow, there is a need for more visibility, intelligence and automation in the design in order to cope with the resulting complexities.

To address this challenge, the Aruba Zero-Trust architecture provides three key components for the hospital’s network.
Role-based access policy automation

Aruba ClearPass Policy Manager takes on a central role for the orchestration of the hospital’s network access management. The platform allows the team to define access policies based on the profile of users, devices and a host of definable criteria. These policies are then applied and automated by ClearPass.

To further strengthen the resilience and safety of the network against risky or unwanted devices, ClearPass Device Insight has been deployed. Device Insight collects information about all connected devices and provides a network profile for each. Depending on the profile and the policies created around them in ClearPass Policy Manager, each can be identified, authenticated and authorised for access to the network and to specific VLANs. Unrecognisable devices with no profile will simply be excluded from the network and quarantined.

“ClearPass Device Insight allows us to dynamically discover and profile all devices, mainly IoT devices, in the hospital. The integration between ClearPass Policy Manager and Device Insight means we dynamically protect the network based on user and device behaviours,” Dominguez explains. “We’re also using UXI Sensors to monitor performance from a user’s perspective.”

Simplifying network operations through automation

To further simplify network operations and to reduce the need for multiple SSIDs and ACLs, and to provide end-to-end security for every device and user, Madrid Digital has deployed an Aruba Dynamic Segmentation platform for the hospital.

Through the use of Mobility Controllers integrated with ClearPass and Aruba Policy Enforcement Firewalls (PEF), Dynamic Segmentation unifies policy enforcement across wired and wireless networks, keeping traffic secure and separate. The outcome is that business-facing operations can co-exist with corporate-managed networks with IoT and IT-managed client devices. Dynamic Segmentation utilises intelligence gathered from ClearPass role-based policies, PEF as well as Layer 7 application visibility and integrated web filtering.

Dominguez reflects: “There are almost 2,000 devices connected to the network, around one quarter through Wi-Fi. In addition, using Dynamic Segmentation, lets us separate and isolate traffic from device to port based on security levels and policies. This allows us to accelerate processes.

“The use of all this technology has allowed us to move from a traditional way of managing the network, manually assigning physical ports, to a different management model where the network identifies devices and automatically applies the appropriate isolation for the implementation of security policies.”

A SERVICE-LED APPROACH TO MANAGEMENT AND SECURITY

Madrid Digital hosts the core management functions for the Hospital Enfermera Isabel Zendal network, as it does for dozens of other hospitals in the region. At its data centre, the organisation hosts ClearPass, AirWave and NetEdit servers which allow it to manage and deliver these as remote services. Madrid Digital also hosts the Mobility Conductor which orchestrates the Mobility Controllers deployed onsite at the hospital.

FLEXIBILITY AND DIGITAL WORKFLOWS FOR THE LONG-TERM

At a time of uncertainty, with political and medical responses to the pandemic changing constantly, Hospital Enfermera Isabel Zendal provides much needed capacity to Madrid’s healthcare system.

Two thirds of the site has been given over to treating patients with Covid, the remaining third is being used to administer vaccines. Long term, the site will act as a healthcare logistics centre, it will provide extra capacity for the emergency services and act as a regional laboratory. Flexibility in connectivity and security of digital workflows will remain central to the integrity of operations.

“We’ve delivered this project in record time,” says Dominguez, “yet we’ve built something that is reliable, safe and secure. On such a technically challenging project, the support of Aruba has proved invaluable.”