Indio Networks

Connected Healthcare

Helping healthcare leverage WiFi for bettering the lives of healthcare workers and patients.

Introduction

The world around us is already extensively connected. The presence of WiFi is dominant and exists across almost all verticals. Healthcare has not been an exception. Healthcare facilities today are getting connected at a rate much faster than ever before. WiFi in healthcare facilities has been known to be an additional support to patients in aiding their recovery by keeping them constantly connected with their loved ones.

The number of connected healthcare machinery is also increasing by the day. These IoT enabled machines need mediums of communication through which they transmit real-time data on to monitoring systems. Many of these machines are WiFi enabled. WiFi is fast and reliable for communicating data securely since patient data security is imperative in these scenarios.

Guest WiFi is touted to be one of the major requirements in the healthcare space. Visitors to the hospital expect to receive good WiFi connectivity in the hospital. However, guest and patient WiFi must be segregated to protect data.

WiFi enabled asset tracking is another important functionality of WiFi that healthcare can use. Healthcare facilities have extremely expensive machinery in use. This machinery can be tracked using WiFi. Healthcare can take a toll on people. In tough times, helping them engage with their loved ones, keeping them connected at all times can greatly help their psyche and allow them to heal better, and faster. Secure WiFi networks and encrypted data allow us to achieve this objective.

The healthcare data analytics market will reportedly rise to $50B by 2024 [1]. Data analytics is driven by fast internet. The healthcare sector needs fast WiFi to silo all the data gathered from facilities to process for improving healthcare and treatment to patients, on-premise WiFi can enable quick transfer of data.

Key Requirements for Healthcare WiFi

- Fast and Reliable WiFi
- High Availability
- Strong Security Posture
- Single Console Management
- Patient Management Information Systems
- Authentication & Access of patients
- Low infrastructure cost
- Bifurcation of Guest, Staff and Patient networks

In Depth on WiFi services for Healthcare

Let us take a detailed look at what healthcare services really require from WiFi.

Securing Critical Data

Healthcare & patient data is one of the most sensitive categories of data out there. Healthcare records are protected by law and leaking healthcare data to anyone is a crime that attracts harsh punishment. How can healthcare facilities secure their data? By securing their network. A lot of hospital data is routed through WiFi, having in place robust mechanisms to identify and eliminate potential threats are important. The WiFi itself should be very secure to prevent unauthorised access into the network. Healthcare in the past has suffered heavy costs due to breaches. According to reports, a single data hack can cost the industry up to $2.2M, with its cumulative value going upwards of $6.2B [2]. When it comes to healthcare, we cannot stress enough about how necessary it is to secure your networks.

Partitioning Patient, Staff and Guest WiFi

Patient, Staff and Guest networks must be segregated inside healthcare facilities. Staff members might receive sensitive data over their devices which should not to be accessed by anyone else other than patients. Patient and Guest WiFi should also be segregated for data protection. Guest WiFi is usually free and session-limited, hence it's better to keep them separated.

Bandwidth Management

Bandwidth in healthcare is one of the major concerns that people are confused about addressing. Connected hospitals move vast amounts of data every minute, if bandwidth is not aggregated properly across all devices & machinery, it can create bottlenecks resulting in inadequate bandwidth to all devices. Mission critical machinery that transmits sensitive data must be given a higher priority and a greater rate of bandwidth should be assigned to that machinery. Devices such as smartphones need lesser priority in this scenario.

Policy Management Function

Healthcare WiFi should not be used for committing illegal acts. The hospital can be held liable for illegal activities conducted through its network. The best way to protect against it, is to prevent these activities through policy enforcement. Several compliance based as well as bandwidth based policies should be set up to monitor the network and set parameters as to what one can and cannot do on the network.

Web Logging and URL filtering

Web logging is necessary to store records of what websites the user has accessed in their connected time. Sensitive URLs should be blocked through URL filtering. URLs banned by the TRAI or DoT should not be available for access.

WiFi coverage

Hospitals have multiple levels with different requirements of coverage. Hospitals must conduct a wireless survey to gauge where they need to place what type of Access Points that best serve the necessities and requirements of that place. A waiting room requires a higher concurrency than patient corridors.

Deployment Challenges

Hospitals are information sensitive places. The primary concern of a healthcare network is ensuring its complete security. However, with that said, there are a few other things that need to be checked in a healthcare facility like:

- Network planning
- RF Design
- Ensuring maximum WiFi coverage
- Securing the users
- Segmentation of users

How we help Healthcare with WiFi.

Indio offers a single vendor, end-to-end Healthcare WiFi solution with an emphasis on a strong security posture & a tough firewall to protect critical patient data. We also provide an easy to integrate asset tracking solution that helps hospitals track machinery around the hospital. Here is a general feature-set of our solution for healthcare WiFi:

- Single Console Management
- Integration with Active Directories LDAP / AP / Gsuite
- Network Discovery & DHCP IP Assignment
- Dynamic VLAN management
- Patient Management Information System
- User Authentication
- Policy Management
- Bandwidth Flow Control
- Access Point Management
- Live coverage of AP & heat maps
- Real-Time traffic information

Implementation

We deploy a system consisting of UniBox, our integrated hotspot controller which controls UniMax Access Points connected through our Trinity series PoE switches. UniBox controller is placed between the ISP and the Access Points. L3 switches connect the ISP to the UniBox, and L2 switches connect the Access Points to the UniBox. The UniBox essentially functions as an intermediary between the end-users and the internet. UniBox can configure policies based on bandwidth, policy and routing that are to be applied to end-users.

Since network security is the primary concern of healthcare facilities. UniBox comes with a range of features to secure the network and internal users. You can set up multiple VLANs segregated as in-patient WiFi, out-patient WiFi and Staff WiFi. Healthcare Staff SSIDs are separated from other SSIDs, they use a higher protection, a more robust security protocol 801.x, or WPA2E, for authentication since healthcare workers devices receive critical patient information. OPD VLANs are also separated as per TRAI and DoT norms to protect the data present in all levels of the healthcare facility.

UniBox and UniMax Access Points come in different models to support different use-cases.

UniBox, when working with UniMax APs work as a network monitoring system from where you can control and configure all UniMax APs in the network through the UniBox Dashboard. With Zero Touch Provisioning, you can get the entire network of Access Points up and running in less than 20 minutes. All UniMax Access Points can be auto-configured through UniBox.

UniBox comes with a loading balancing mechanism that utilises all available bandwidth effectively by aggregating it between connected ISPs. If in case the primary connection fails, then UniBox smoothly transitions on to the secondary or standby connection with a responsive failover mechanism. This ensures that downtimes are kept as low as possible at all times, this is especially important in a healthcare facility where electronic monitoring machines constantly broadcast data to doctors and other staff working in the facility.

Although it is best practise to use original manufacturer deployments for optimum experience, Indio's hotspot controller solutions are vendor-agnostic and work with hardware from any vendor.

Solution Benefits

We have served over thousands of patients in healthcare facilities in several countries across the world. Patients have reported an enjoyable WiFi experience facilitated by our solutions. Here are a few ways in which our solutions impacted WiFi in healthcare:

- Patients reported a comforting experience by connecting with their loved ones through seamless WiFi
- Hospital's network administration made easy
- Improved network performance
- Managing in-patient, out-patient and staff WiFi made easier
- Managed bandwidth effectively to make sure critical systems are never affected by a network failure
- Solution very cost effective when compared to our competitors
- Easy integration of third party APs
- Seamless failover mechanism for smooth transition
- System up and running in under one week

Connect with our sales team.

sales@indionetworks.com

+020-67157377

+020-67157373

REFERENCES
[1] https://www.marketsandmarkets.com/Market-Reports/healthcare-data-analytics-market-905.html
[2] https://www.darkreading.com/threat-intelligence/healthcare-suffers-estimated-$62-billion-in-data-breaches/d/d-id/1325482

Do not publish or reprint any part of this document without prior permission.