Key Considerations for your Healthcare IT Network Edge

White Paper
Key considerations for your healthcare IT network edge

TRIFECTA NETWORKS

Alcatel·Lucent Enterprise

Table of Contents

Overview

Are your local area and wireless networks strong, safe, and robust enough to keep up with the increased bandwidth requirements, security concerns, and multitude of growing IoT/IoMT devices?

Healthcare has become more sophisticated, patient care continues to evolve, and operations flex to keep up with the multitude of changes. As we move from Digital Hospitals to Smart Hospitals, connected healthcare is growing exponentially. The way healthcare is delivered has changed and will continue to mature and advance. Increased remote work, the hybrid workplace, and telehealth add to the complexity. Internet of Things (IoT) and Internet of Medical Things (IoMT) have changed the network landscape. These new and exponentially growing devices, advanced modalities, and complex software applications, along with the growing bandwidth demands from medical staff, patients, and guests, all place a strain on the hospital's IT infrastructure. The IT department has grown at the fastest pace in history and is in a constant state of keeping up, adding, changing, and retiring hardware and network equipment. Often the result is a patchwork architecture that continues to be more time consuming to manage.

Healthcare operations rely on a high-performing, predictable, and secure network, especially at the network edge where the demand is greatest for more connections, both wired and wireless. Compliance and security requirements add to the challenges of keeping a healthy, robust, and safe LAN/WLAN network. If the network edge is your most pressing need and you have decided to embark on an edge refresh, here is what you should consider when selecting a vendor.

Refreshing the network edge – what to consider

While there are many factors to consider when refreshing your network edge, below are three essential considerations that will ensure your network can deliver an outstanding end-user experience today and well into the future, with your budget top of mind.

Performance: Capacity, security, and resilience in both wired and wireless networks

Manageability: Fast provisioning, troubleshooting, and analytics, with unified management of Wi-Fi Access Points and switches, regardless of how the management platform is connected (on-site or cloud)

Total Cost of Ownership (TCO): Hard and soft costs, both up-front and throughout the life of the equipment

Performance

Upgrading your wireless network

An important decision point when refreshing the network edge for a healthcare facility or campus is wireless capacity. Many Wi-Fi networks in hospitals today cannot handle the growing number of IoT/ IoMT devices, including the rapid expansion of intelligent clinical communication, inventory management, location and tracking, guest network, robotics, automation, and the exponential growth of healthcare monitoring devices and modalities used by clinical staff. The IoMT market alone is predicted to reach $176 billion by 2026[1].

The recently approved Wi-Fi 6 standard can enable healthcare systems to increase WLAN capacity and performance that older networks could not. An upgrade such as this can offer 2-3 times the bandwidth throughput of earlier deployments. Wi-Fi 6 is also more spectrum efficient and scales beyond prior technologies, especially in high-density environments like hospitals. Upgrading to Wi-Fi 6 is a key element in future proofing your network.

1 Fortune Business Insights, IoT-in-Healthcare-Market-to-Reach-USD-176-82-Billion-by-2026-Emerging-Popularity-of-Smart-Wearables-and-Remote-Patient-Monitoring-to-Add-Impetus-to-Market.html, February 20, 2020

Access, uplinks, and power

The demands on healthcare IT personnel and the network are at an all-time high. Accessibility must be balanced with security requirements. Patient metrics need to be maintained and healthcare professionals have a myriad of clinical technology that must be simultaneously supported, at critical speeds, to maintain the patient care metrics.

Healthcare IT systems need, and care providers' demand, the latest systems that have both wide accessibility and broad compatibility with the latest technologies, and the highest security standards. Today's healthcare IT network infrastructure provides not only the bedrock for day-to-day hospital administration and patient access to health data, but all essential clinical applications required to provide quality healthcare. Upgrading access points will increase the number of Wi-Fi enabled devices that can connect to the Wi-Fi network, as well as increase the bandwidth generated.

As more and more high-powered IoT/IoMT devices become available and in full use, the need to enhance your edge switching will be required. LAN switches should be evaluated to determine their ability to handle the additional bandwidth and power requirements that WiFi-6 will need. Links to access points and the core of your network also need to be considered. While modern edge switches can now serve multigigabit speeds to access points over existing data cable infrastructure, switches require high-speed uplinks to the core and distribution network to realize full capability.

Your edge switches require sufficient power for healthcare connected smart devices and high-capacity Wi-Fi access points. To receive full functionality, you may need 30 watts or more of power per port. Wi-Fi 6 access points can operate with less power but will not deliver the full performance without the switch upgrades. Understanding your AP power requirements and switch POE costs is an important line item in your budget.

IoT/IoMT connectivity, network segmentation, and quality of service

With the explosion of devices at the network edge, automation for getting those devices connected securely becomes imperative. Your edge network must be IoT/IoMT aware and provide easy identification (fingerprinting) and secure connection to devices automatically. This capability requires access to a comprehensive IoT/IoMT inventory database that enables automatic device detection and connection.

The network must also be able to automatically segment devices into categories. For example, security cameras should be on a separate segment from the HVAC system as they have higher priority and security needs, just as infusion pumps require priority over door locks. Only authorized employees should have access to certain devices and sets of devices, much like segregation of duties in healthcare ERP systems. A technician in Sterile Processing for example, will not have the same access as a physician, who also may have different access than an administrator. Different roles have unique requirements and access to device categories.

With different segments for different devices, Quality of Service (QoS) is critical. Flexible QoS rules can provide more bandwidth to mission critical devices and can prioritize time sensitive traffic such as real-time alerts. This lets you optimize performance for each user or device connecting to your network edge based on their role, authorization, or priority.

Manageability

Unified across the LAN, WLAN, and IoT

Many network management systems are a collection of tools designed for specific switches, access points and other network elements. They often do not work together, and this increases the time and cost of managing the network. It also makes maintaining consistent security polices across wired and wireless access cumbersome.

Your hospital's network management system should be a single platform that can see, manage, secure, and analyze the entire network, including the LAN, WLAN, and even IoT/IoMT devices. Since today's network elements and devices are increasingly integrated and interoperable, the ability to manage the entire network reduces costly delays in deployment, analysis, and trouble resolution.

Cloud-based or on-site: Full capability when moving from one to the other

Many management systems offer the option of on-site or cloud-based operation and services. For many healthcare organizations, cloud-based management systems offer benefits such as automatic upgrades with no interruptions, no maintenance, and high-availability assurance. While other healthcare organizations value local control, preferring an on-site management system which may be required for legal, HIPAA and/or privacy reasons. When selecting a cloud-based system, it is essential to verify that all the capabilities of an on-site platform are available from the cloud. Some cloud-based systems offer limited services when compared to on-site capabilities. Pay particular attention to the hardware supported. Some vendors require a totally different product line if you are deploying a cloud-based versus an on-site management platform.

Policy management and security

To support a consistent and seamless experience, the network management platform should provide unified policy management across the entire network to support both wired and wireless users and devices. Security should be centered on a zero trust basis, which assumes no device or user has access to the network until properly identified and authenticated.

Analytics

Insight into the health of the network and understanding trends and trouble spots are vital to resilient operations and minimizing interruptions. The management system should provide network analytics with performance insights and predictive analytics that spot trends. Access to an IoT/IoMT inventory database for early warning of problems is critical to the user experience and the timely delivery of IoT/IoMT data for analysis and action.

Total Cost of Ownership (TCO)

When considering the cost of refreshing your network edge, it is important to look beyond the price points of switches and access points. Consider the typical five- to seven-year lifespan of network equipment and take a closer look at both hard costs such as hardware, maintenance, licensing and support, and soft costs such as network downtimes and operational efficiency. Saving capital by understanding the true TCO allows for funds to be reallocated or a Return on Investment (ROI) to be realized sooner.

Hard costs

Consider the cost of equipment and include licenses for capabilities such as IoT/IoMT, applications analysis, and registering users who bring their own devices (BYOD). Often, vendors charge by the feature or simply charge more for basic capabilities, based on their brand.

Factor in maintenance over the life of the product and what a maintenance agreement will cover. Some contracts provide only partial support, and others have extra charges for response times and levels of tech support.

Soft costs

While hard costs provide a straightforward dollars and cents view of upgrading the network edge, soft costs, such as network downtimes and operational efficiency, can often have a more significant impact during the life of the product.

IoT automation: Adding an IoT device should be simple, providing access to an existing database and registering devices automatically. Valuable time is lost if IT staff must manually create an IoT/IoMT inventory database and then research each new device to register and add them to the database.

Security breaches: It is essential to consider the value of resilience and security of network switches and access points when comparing equipment prices and maintenance costs. Security breaches are costly, as are network failures, but in the case of healthcare they can be life threatening.

Troubleshooting time: Using separate tools for the wired and wireless edge will add significant time to troubleshooting and resolution of network issues. It is also important to consider how network issues may negatively impact patients, HCAHPS (patient satisfaction) scores and reimbursement, as well as a hospital's overall ability to deliver critical healthcare services.

Interoperability: When choosing a vendor, ensure they offer network equipment interoperability to allow for a phased upgrade approach. This way the network edge can be refreshed without affecting the network core. Rarely is a network going to be ripped and replaced. True and proven interoperability of edge equipment is critical to work seamlessly with the core.

ALE: Your vendor of choice for a network edge refresh

Alcatel-Lucent Enterprise offers a comprehensive portfolio that delivers the network foundation, performance, management, and low TCO to support digital transformation. From the edge, to the core, to the cloud, ALE supports your healthcare IT network evolution without disrupting daily operations.

As healthcare delivery and payment modalities evolve, efficiency across the healthcare landscape is necessary, and that includes the heart of the healthcare system – the networking and communications infrastructure. ALE provides digital age networking, communications and cloud solutions, with tailored services. Flexible business models in the cloud, on premises, and in hybrid environments help ensure your healthcare customer success. All solutions have built-in security and limited environmental impact. We are diligent in our focus to work alongside our healthcare customers to understand their communications and clinical strategy requirements.

Performance

Alcatel-Lucent OmniAccess® Stellar Access Points provide scalability and low latency, all without the bottleneck and cost of a controller. The OmniAccess Stellar line offers a range of Wi-Fi 5 and Wi-Fi 6 access points to support entry-level to harsh outdoor environments. These access points can handle high-density traffic and the large numbers of IoT/IoMT devices found in healthcare settings. And, they allow for both 2.4Ghz and 5Ghz Wi-Fi bands with channel optimization.

The Alcatel-Lucent OmniSwitch® line of edge switches offers both Layer 2 and Layer 3 functionality, including hardened switches for outdoor and harsh environments. These switches provide gigabit and multigigabit access and 10- to 25-gigabit uplinks to accommodate modern access points and easily handle heavy hospital employee, patient, and guest traffic.

The OmniSwitch line, enables you to avoid expensive electrical cabling costs as it provides power over ethernet (PoE) and high power over ethernet (HPoE) to easily handle the demands of modern access points, cameras, and other devices that need switch-connected power. The switches also provide easy device connectivity, automated device segmentation, and fine-grained QoS to handle every need.

Management

The Alcatel-Lucent OmniVista® 2500 Network Management System (NMS) provides network-wide visibility and advanced analytics for a full view of wired and wireless devices, IoT/IoMT devices and applications, and predictive analytics for planning, all in a single pane.

OmniVista enables easy connection and "fingerprinting" of IoT/IoMT devices and provides a cloud-based inventory with a library of over 30 million known devices. The system automates the rollout of devices and network elements with policy-driven provisioning for compliance and security.

Single policy management of the entire healthcare network is enabled with Unified Policy Authentication Management (UPAM) services. This capability allows wireless and wired devices and end-users to be governed with a single set of policies.

OmniVista offers a cloud-based service (Alcatel-Lucent OmniVista® Cirrus Network Management as a Service) and an on-site platform (OmniVista 2500), both with nearly identical capabilities. Whether in the cloud or on-site, the platforms can manage the same hardware (switches and access points), with the same feature set, providing comprehensive and flexible network management.

TCO

ALE lowers TCO by adhering to industry standards and offering interoperability with your healthcare organization's existing wired and wireless network. You can refresh your edge in phases without the worry or cost of changes to your core network. For example, ALE's edge solutions have been deployed by many customers who have kept their existing non-ALE core networks.

The OmniVista NMS feature set includes all the capabilities many vendors charge extra for such as support for guests, BYOD, Wi-Fi, IoT/IoMT, management and analytics – all in one software package. OmniVista also lowers cost through its automated provisioning and eliminate repetitive tasks and expensive on-site support visits.

ALE's distributed Wi-Fi control eliminates controller costs such as maintenance, licensing, and capital expenditures. This allows you to pay as you grow, adding more access points as you need them.

A simple licensing program offers full transparency for both upfront and on-going costs. A single operating system across all ALE products reduces the learning curve and all hardware comes with a Limited Lifetime Warranty (LLW).

Refresh the edge to take your healthcare organization to the next level

Whether you decide to refresh your network edge in phases or all at once, considering performance, management and TCO will help you make the decision that best serves your operations today and tomorrow.

Many hospitals and healthcare systems are already seeing a payoff from IoT/IoMT technologies, enhanced access, and user satisfaction. The journey towards an IoT/IoMT analytics-driven transformation of business processes, and new business models, holds tremendous promise for both community hospitals and large enterprise healthcare systems. That journey begins at your network edge where everything connects.

TRIFECTA NETWORKS

Alcatel·Lucent Enterprise