Hospital Networking Guide

A practical guide to optimizing the care pathway for hospitals by developing an ideal network infrastructure
One private network for every department, delivered on a single network infrastructure.

A hospital’s network is the foundation for the critical applications that run on it, where most of those applications are related to the hospital’s core businesses. The return on the investments made in EMR (electronic medical records), PACS (picture archiving and communication system), clinical imaging systems and workstations on wheels, can only be truly realized if those assets are always available to the people in need in a reliable, secure and highly optimized way, at a fixed location, or while mobile.

In addition, the hospital’s network is under constant pressure from new requirements driven by emerging technologies and digital social behavior. Clinicians are in need of access to information on their personal mobile devices, such as smart phones and tablets, while patients and visitors demand Internet connectivity for social networking and entertainment. IoT devices and sensors are creating “smart” hospitals that heavily affect clinician and patient experiences in the hospital as well.

Many hospitals use a separate network infrastructure for every department as a way to provide security and performance. Separate networks may exist for bio-medical devices such as infusion pumps and meters. There may be one for security supporting video cameras and secure access to the buildings. Another one may exist for facilities which would include laundry, kitchens and heating, ventilation and air conditioning systems (HVAC). Plus another for patient entertainment, such as TV and Internet access, with yet one more for clinicians and their communication and computing systems. Each network infrastructure includes its own networking and management equipment, all connected to servers, gateways and other platforms.
iFab and SPB simplify your network
Separate networks, separate management and separate storage and computing for each department. This is an expensive way to go. Instead, you could benefit from one private network for every department for instance, delivered on a single network infrastructure while maintaining security and segmentation between departments. Using ALE technology such as iFab (Intelligent Fabric) reduces equipment, management and operating costs, while providing the security and performance needed for all users, devices, equipment and applications. iFab delivers automated network provisioning, and leverages Shortest Path Bridging (SPB) to provide service provisioning for link optimization, virtualization and fast convergence.

This is an example of the single network infrastructure for a hospital. You’ll note the many devices and sensors that need to be connected to their respective storage and/or computing servers.

We now show a virtual private network for each department, represented as different clouds. Each cloud enables segmentation of the network, providing a secure and robust network with uncompromised performance, single network management system, with lower equipment and operating costs.

Maintaining network performance and security without burning out limited IT resources requires a highly converged system and a virtual network approach. This document provides a series of recommendations to build “One private network for every department delivered on a single network infrastructure” that will meet the needs of your users today and for years to come.
Single network management system with Smart Analytics and PALM
The benefit of having one network management system is that from a single platform it is possible to enable user and device access, manage the mobile campus, have visibility and metrics of the data center and network backbone.

With advanced Smart Analytics, you have a view of the network and how it's being used. This enables you to be more proactive about restricting or limiting access to specific applications, setting time limits for visitors, and securing patient information from prying eyes. You will even have the ability to plan for any network upgrades and possible expansions based on projected bandwidth utilization built upon current usage patterns.

ALE's Virtual Machine Manager simplifies functionality and operations of Software Defined Networks (SDN) in your data center allowing for fast connectivity of newly created virtual machines, as well as fast migration of existing virtual machines in data centers, yet preserving their connectivity and assigned quality of service (QoS).

To simplify the support and maintenance of your network, the Proactive Lifecycle Management tool (PALM), provides proactive lifecycle management of your infrastructure hardware and software products. PALM is an asset management cloud service that connects to your network management platform to provide new services including a view of the network, information of software versions, status of the support service subscription, etc.

This is the objective: Simplify IT - One network infrastructure with a single network management system.
Unified Access provides a consistent user experience for LAN/WLAN users

The need for unified access is driven by a user-centric approach securing a consistent high-quality user experience throughout the wired and wireless network. Unified access empowers clinical staff to use, in addition to corporate devices, personal tablets and smart phones to access medical information, preserving the same user experience and overall network security. This is achieved with a set of network services that apply to the wired and wireless network which, in other words, behave as one network. Unified Access also removes the burden for IT administrators to repeat the same configuration steps for multiple devices, reducing the possibility of making errors. Unified Access can be deployed using a single management platform (OmniVista 2500) that avoids duplication of tasks for multiple devices and provides end-to-end visibility across the unified network.

Why does this help hospitals? The majority of clinical staff use tablets or smart phones to access medical information and Wi-Fi provides access to real-time information and electronic patient records which can be used for patient location and remote monitoring. The same network services (policy management, access control, etc.) and applications are available for LAN and WLAN connected equipment and devices.

Unified Access differentiates the ALE solution from the competition and is the key element to enable the next-generation workplace.
Advanced access control for clinicians, administrators, patients and visitors

Advanced access control enables configuration of the network to fingerprint a device type, schedule access time, limit data, check user/device integrity, on board devices and users, and more. It enables you to setup separate, specific policies for individuals such as doctors, nurses, administrators, patients and visitors, including entire departments. It can be configured to accept only specific iPhone and Android smart phones and tablets, and block jail-broken devices. Advanced access control provides a flexible, granular and secure network for clinicians, administrators, patients and visitors.

Network Security (a multi-layered approach)

There is a growing trend in Healthcare network exploits which needs to be addressed. ALE’s IoT security strategy uses a multi-layered approach to prevent cyber threats. We start with device and user authentication, which only allows authorized users and devices to be connected to the network. Next, we use Access Guardian which is a built-in feature of our network switches, enabling you to select the type of authentication method and security to use. We follow that with our Quarantine Manager, which uses intrusion detection and automatic quarantine functions to safely prevent users and devices from connecting to the network. We then add CodeGuardian to further protect the operating system software in each network switch.

Together, they make up the key elements of an ALE network solution security strategy.

Here we present a series of recommendations to build “One private network for every department delivered on a single network infrastructure.” that will meet the needs of your users today and for years to come.
Recommendation 1

Choose the right technology

The transformation to digital imaging is complete. The adoption of digital records is underway. The addition of networking capability for clinical devices (pumps, patient monitors, and nurse call systems) and everyday objects (doors, thermometers, water sensors, signs and may others) is growing with each passing month. A hospital network needs to be ready for the hyper-connected near term. This means having connectivity - wired and wireless - throughout a facility is critical. This also means having sufficient bandwidth allocated throughout the network, but this doesn’t mean over-provisioning.

There are different technologies and approaches available for you to achieve this objective. From traditional ones using virtual LANs and STP (spanning tree protocol), to implementing virtual private networks with MPLS (multi-protocol label switching). The latest approach uses SPB technology which enables you to set up and expand virtual networks by only provisioning the edge of your network, provides fast fault recovery and uses multiple active paths, which is ideal for large networks and provides significantly lower hardware and operational costs than a MPLS network. All around, SPB technology is the best option to support the growing market of IoT devices which analysts predict will reach anywhere from 20 billion to 50 billion devices by the year 2020. Using SPB based virtual private networks enables you to consolidate your network infrastructure and this brings equipment and operational costs down.

Your network needs to:

- **Be user-aware.** A doctor accessing a PACS image should have the same experience, no matter what device is being used to provide a patient with an explanation. Do you compete for network access or do you get access by using your credentials? Competing for network availability and bandwidth with a patient streaming a video for entertainment is not acceptable.
• **Be application-aware.** User and device awareness is necessary, but not sufficient, to get the most out of your network investment. The network needs to be able to identify, differentiate and prioritize real-time applications versus those applications more tolerant to latency and jitter. And with the increased use of Virtual Desktop Infrastructure (VDI), the network needs to be able to prioritize applications inside the VDI sessions as well.

• **Be secure.** Security doesn’t end at the edge, it only begins. You need a network infrastructure that is secure from the edge to the core so only those authorized have access to the information they need. A secure network that is user-, device- and application-aware, will ensure you have enough bandwidth to meet the needs of the all-digital world that is emerging without over-provisioning or under-securing your network.

**Customer story**

Europe Hospital, in Belgium, updates network with ALE infrastructure to computerize systems, integrating patient care records electronically, automating prescriptions and improving the patient experience.

**Challenges**

• Create an IP network capable of supporting existing capacity and scaling for future growth expectations

• Enable the introduction of new services and third-party applications, while remaining device-neutral

• Introduce presence notification for medical staff and support computerized medical records and prescriptions

**Benefits**

• Delivered scalability and capacity to cope with future growth, including planned expansion to new locations

• Provided infrastructure for integrated medical systems, including patient records and prescriptions, from the doctor to the bedside

• Allowed the introduction of new entertainment systems for patients, including smart devices, improving patient experience and corporate reputation

“The network is fundamental to our future plans. Everything is built on it, so it needs to be open. Getting rid of the emphasis on the device, as long as it connects to the network, makes us far more future-proofed.”

Dr. Dirk Lambrechts, CIO and CFO, Europe Hospital
Recommendation 2

Deploy pervasive WLAN using Unified Access

You should presume that the default mode of most devices on your network is wireless. The majority of devices in healthcare depend on being mobile: User devices like VoIP phones, WoWs (Workstation on Wheels), tablets and smart phones, clinical devices like infusion pumps, mobile image capture (radiology, MRI) and other devices like location tags, temperature sensors and door locks. People expect the same performance from their wireless LAN devices as they do from wired LAN devices. Having a network that supports the same performance and connectivity characteristics can only be delivered when Unified Access is supported.

Wireless will dominate as a means of accessing patient information as EMRs become more and more tablet- and smart phone-friendly. The standardization of ultra-fast gigabit wireless (today IEEE 802.11ac) means that large files can now be transferred quickly, driving increased usage of mobile image capture and mobile image viewing. There are even manufacturers of 802.11-based medical telemetry equipment, the first step to eliminating proprietary protocols based on Wireless Medical Telemetry Service (WMTS) frequencies.

Coverage is, of course, assumed inside the facility, but do not neglect areas where staff, patients or visitors congregate outside the wards and examination areas – cafeterias, gardens, parking lots and even elevators are areas where coverage can make a huge difference to clinical productivity and an overall satisfying experience for patients and visitors. Pay close attention to coverage in “popular” areas to ensure sufficient density of access points are provided: nurses’ stations, auditoriums, cafeterias and staff lounges.

But full coverage is not enough – to maintain high performance for ALL users of the wireless spectrum, capacity is critical. For this reason, IEEE 802.11ac is the recommended standard for all new deployments. Personal devices for the most part already support 802.11ac, and even older devices that support 802.11n will benefit from increased throughput and increased battery life.
Customer story

Casa Di Cura Beato Palazzolo, in Bergamo, Italy, enables doctors to retrieve and review patient data from their laptop or smart phone.

Challenges

- Strengthen the existing network to manage medical systems, diagnostic imaging and video streaming applications
- Wire the whole structure in order to implement a 10Gb fiber backbone that can support a high level of traffic, avoiding bottlenecks
- Provide total Wi-Fi coverage

Benefits

- Simple and immediate examination of electronic patient records from laptop or smart phone
- Faster remote visualization of diagnostic images
- Smart collaboration between branches
- More mobility and collaboration within the organization
- Video streaming enables virtual doctor assistance in surgical procedures and helps in training other staff

“Thanks to Alcatel-Lucent’s technology and Com.Tel’s competence and professionalism, our medical staff can now access patient data anytime and anywhere.”

Edoardo Manzoni, General Director, Casa di Cura Beato Palazzolo
Recommendation 3

Evaluate the entire access network

Your wired LAN access network, like all elements of a modern healthcare network, needs to focus on maximizing up time and performance. Eliminate single points of failure by deploying a robust and resilient network architecture that can reroute around failed links, using a technology such as SPB. Bring a device or network element online or offline automatically, using an intelligent auto provisioning technology such as iFab. Provide a single network management system, which has a view of the entire network for both wired and wireless devices. Deploy redundant network elements and power supplies. Increase user and device security by deploying a policy management approach, such as BYOD.

In addition, your LAN access needs to ensure it isn’t a bottleneck for your wired users but also for your wireless deployment - gigabit speed at the edge and implementation of wireless 802.11ac standards are essential for your network. Having sufficient Power over Ethernet (PoE) capability is also critical; powering VoIP handsets and access points is, of course, a prime consideration, but more and more hospitals are migrating to IP-based video cameras to secure their facility and protect patients and staff alike. All of these devices will require PoE and HPoE (High Power-over-Ethernet).
Customer story

Shanghai Punan Hospital, located in Shanghai’s prestigious Pudong District, introduced a new network system which offers a high availability and enables data, voice and video convergence applications.

Challenges
- Connect three buildings situated in different locations in the district
- Install an active/active virtualization data center for their server farm
- Ensure full wireless coverage throughout all areas of the hospital

Benefits
- The high availability of the network system enables data, voice and video convergence applications
- Having a unified access policy for both wired and wireless networks creates an improved synergy of communication, data and voice, in all areas of the hospital
- The Access Guardian solution provides powerful and simple access control, with a User Network Profile policy, creating a highly reliable network structure
- The solutions implemented have reduced operational costs by 30%
- Thanks to now having secure and consistent wired and wireless internet access, staff and patients are benefiting from the high availability and improved performance of Punan Hospital’s network

“Alcatel-Lucent Enterprise’s wireless unified access solution not only ensured high security protection, but also significantly reduced our operational costs. This shortens the duration of consultations, while providing prompt and effective service to the patients and staff at the hospital.”

Hui Jin, IT Manager, Shanghai Punan Hospital
Recommendation 4

Right-size the Core

An efficient, high-performance access network is only as good as the core network it connects to. The core is the most critical part of your hospital infrastructure; again, redundancy, resiliency and performance are paramount.

When planning your new network consider:

- Deploying access switches with 10G links to a 40G or 100 G core eliminates bottlenecks and supports a virtual network design
- Right-sizing with a choice of small form factor switches forming a reliable and resilient virtual chassis or a high density modular chassis based solution to provide more than 10 Tb/s of switching capacity per single logical unit
- Streamlining your wired infrastructure by reducing the number of layers in your network design by eliminating the distribution layer, which reduces your capital expenditures (CAPEX) and operating expenditures (OPEX)
- Rethinking Virtual LANs (VLANs) with software-defined, flow-based policies that optimize wired and wireless traffic paths without changing your existing network
- Choosing newly designed switches with lower power requirements
- Vendors that support pay-as-you-grow strategies that reduce budget pressures, but don’t compromise product features or scalability
- A network with a core that is the center of a robust infrastructure that supports main overlay technologies like SPB
- A core which supports an auto provisioning technology such as the ALE award winning (Best of Interop 2015) Intelligent Fabric (iFab) technology, for its superior set of auto installation, auto expansion and self-healing features.
• Smart Analytics to improve network usage and costs
• CodeGuardian for a hardened operating system (added security at the OS level)
• IoT containerization securing introduction of coming medical devices
• Network agility (Application Fluent Network) for application and QoS flexibility

Customer story

Advocate Health Care is the largest fully integrated, not-for-profit healthcare system in metro Chicago — and ranked among the top 10 in the entire U.S. Advocate chose Alcatel-Lucent Enterprise because of the network solution architecture, mobility vision, and cloud service integration.

Challenges
• Provide an IT infrastructure to support Advocate’s growing demands that voice, video, data and imaging continued to place on their network systems
• A solution from the edge to the core, to support today’s needs and their future requirements

Benefits
• A right sized core with consolidated network facilities and centralized management, simplifying operations
• Virtualized IT operations, reducing costs by lowering power consumption, increased network availability and up time, while making the network more flexible.
• With these improvements, Advocate Health Care was able to speed application deployment

“Advocate Health Care will definitely consider Alcatel-Lucent Enterprise for inclusion in future projects because of the proven track record of reliability.”

Gary Horn, V.P. Technical Service and CTO
Recommendation 5

Simplify network management and enhance application and service visibility with Smart Analytics and PALM

Hospital IT staff are stretched to the limit so a new approach is needed to streamline network management operations and reduce errors that can have catastrophic impact. A modern hospital must be run on something other than traditional CLI (Command Line Interface)-based element management; a simpler and more cost-effective unified network solution can manage both wired and wireless networks. With an integrated management solution, your IT staff can better manage the application and device experience of users on networks that extend across geographically dispersed locations – from hospitals to clinics to home users.

Choose a single solution that enables you to provision, monitor and manage:

- Network elements and resources of a hospital main campus, data center and remote clinics, including doctor practices and home offices
- SPB based Virtual Private Networks across the network
- Security and priority policies across the access layer on both wired and wireless networks
- Application awareness and fluency across the network
- “Bring-Your-Own-Device” (BYOD) services including authentication, authorization, and accounting policies to name just a few
- A simplified, integrated network management approach that spans wired and wireless networks will enable you to better manage IT time and resources.
Customer story

Liverpool Hospital is the largest hospital in New South Wales (Sydney, Australia) and one of the leading trauma centers in Australia. It is also a leading Australian teaching hospital and research facility and they turned to Alcatel-Lucent Enterprise to build an end-to-end network including voice, data and wireless access.

Challenges

• Provide secure and reliable access to clinical information and images
• Implement a state-of-the-art network infrastructure supporting voice, data and wireless access
• Ensure comprehensive wireless coverage in all care venues to enable clinicians to work more effectively

Benefits

• Reliable and secure access to EMRs, wherever and whenever needed, at nurses’ stations or on the move with smart devices
• Access to the information the staff needs to make the best decisions for patients, improving communication and workflow, and reducing errors
• Cloud-ready solution that provided innovative and collaborative conversation services
• Single-vendor solution for network and communications leads to an overall successful implementation
• Simplified network management

“We needed a robust, highly available and performing fixed and wireless data network that was capable to support current and emerging clinical, corporate and innovative collaboration applications and services.”

Nick van Domburg, CIO, Liverpool Hospital
Recommendation 6

Provide secure Internet access and BYOD, with minimal impact

Patients and guests can spend a lot of time in a hospital facility. Providing Internet access will help them pass the time more pleasantly and productively, increasing patient satisfaction and enhancing your reputation in the community. However, providing patient and resident access should not have a measurable impact on your organization’s most important users – clinical providers and your IT staff. We recommend a guest and patient Internet service that:

- Spans securely both the wired and wireless network access options, sharing identical privileges
- Uses the same physical infrastructure but logically separated from clinical and corporate networks
- Is tuned to ensure that care provider access or performance is not compromised
- Is automated so guest and patient access does not require IT involvement

For many hospitals, to support secure Internet access, BYOD has been implemented as affiliated doctors demand access to both in-house and external/remote practice applications and assets. Managing BYOD in a secure way that protects patient information has traditionally been a manual, labor-intensive process, increasing the workload for an already-stretched IT team. But security doesn’t end with clinicians. With an advanced BYOD solution you can:

- Enforce differentiated network access based on contextual information, such as user roles (doctor, nurse, administrator), device types (Workstation on Wheels, tablets, smart phones), and location (hospital, clinic, home use), which enables secure management and enforcement of differentiated policies
• Simplify and automate device on-boarding by allowing users to self-enroll, granting network access privileges based on user roles, device types and location

• Opt for advanced security features like 802.1X authentication with Advanced Encryption Standard (AES), which allow users to enter a user name and password or self-enroll by automatically generating and installing device certificates through a web portal with no IT assistance

• Add mobility for patients improving their communications experience while in the hospital

• Add mobility for staff and clinical devices for better services and tracking

Customer story

Azienda Ospedaliera Della Provincia Di Lodi in Lodi, Italy was looking to integrate BYOD and simplify network management for their wired and wireless LAN network.

Challenges
• Introduction of a Guest User management system for occasional guests on the hospital’s wireless network
• Fully automated BYOD for personal devices
• High access control and information security
• Optimization of internal resources

Benefits
• Physicians, doctors and clinicians can access data more quickly to make their jobs easier
• Users (patients and visitors) can access the Internet easily and quickly with their personal devices. The new infrastructure enabled the hospital to reduce its dependence on external resources to support the network and to optimize the workload of IT personnel

“The fully automated access to the network helps us to optimize internal resources and has been much appreciated also by our employees, who can now access to their own personal service.”

Ravio Cassinari, CIO, Azienda Ospedaliera Della Provincia Di Lodi
Recommendation 7

Extend connectivity beyond the hospital

Your new network should be able to go beyond the hospital and interconnect clinics, administrative offices and home users, as well as remote offices and medical vehicles.

When considering network extension options, choose:

- Environmentally hardened access switches and access points to provide connectivity around hospitals and at outdoor locations, such as parking lots and green spaces
- WLAN-based point-to-point and/or point-to-multipoint bridging connections, which offer a great way to extend your entire network to another building without having to lay cables
- Remote access points enabling doctors and other healthcare professionals to work from a home office and remote monitoring of patients/devices via Wi-Fi or Bluetooth Low Energy (BLE) from in-home access points with all the same access to services and applications they are accustomed to in the hospital
- WAN routers enabling medical and care centers to connect with each other, ensuring better care and post-care follow-up
- Connected vehicle technology that could transform your medical vehicles into mobile offices providing access to all of the patient’s data and history while already on route to the patient. With the patient on-board, your medical vehicles become mobile clinics connected to all the resources of the hospital network.
Customer story

Alcatel-Lucent Enterprise enables Inspira Health Network in New Jersey, USA, to provide doctors with secure, ubiquitous Wi-Fi access indoors, outdoors and from home.

Challenges
• Growing network of facilities, including merger with major hospital
• Comply with government mandates to deploy EMRs and increase patient satisfaction
• Make clinical staff more effective for cost control as well as making their jobs easier

Benefits
• Pervasive wireless for high performing applications
• Unified Access solution provides single pane of glass management of the wired and wireless network, increasing IT efficiency
• Doctors benefit from a wireless network that enables access to clinical applications wherever needed (desk, in the hall, in the parking lot, or at home)
• Inherent security and reliability of the network infrastructure contributes to compliance with governmental healthcare legislative requirements

“One of our main goals is to have the best wireless network possible, so that whenever we do purchase new technologies, networking and interfacing isn’t something we have to worry about.”

Francois Bodhuin, Technology Director, Inspira Health Network
Build a secure, robust, high-performing hospital network with ALE using Unified Access, iFab and SPB technologies

The network is the foundation for delivering the data, applications and IoT connectivity that ultimately drives outstanding patient care and improve outcomes. Alcatel-Lucent Enterprise network solutions for Healthcare offer excellent value with solid investment protection and seamless high-quality experiences. They provide:

- Right set of technologies (SPB & iFab) for your optimized LAN including core, edge and data center
- A pervasive WLAN with unified wired and wireless policies
- Simplified yet rich network management capabilities with a single management tool

Operations benefits
- A high quality user experience (low latency, localization of network failures, improved application availability)
- Increased agility (automated machine movement, flexible service options)
- High availability (supports organizational requirements, ensures application availability, rapid infrastructure failure recovery)
- Increased security (seamless experience on wired and wireless, enhanced and consistent device security profiles, single point of device access control, support for IoT containerization)

Business benefits
- Reduced IT operating expense (single network infrastructure, CAPEX and OPEX offers via NoD)
- Rapid deployment time (minutes, not months)
- Increased business elasticity (resources scale up and down, on demand)
- Increased investment protection (business chooses device, business automates guest/new device onboarding, business welcomes guests/devices)

Alcatel-Lucent Enterprise solutions for Healthcare provide network architectures that are reliable, secure, high-performing and resilient, and which allow care providers to focus on those who matter the most – their patients. With global reach and local focus, Alcatel-Lucent Enterprise enables healthcare providers to optimize the care pathway and enhance patient outcomes.
Find out how we can help you become a hospital that is ready for today's digitization demands and tomorrow's IoT innovations.

ADDITIONAL INFORMATION
http://enterprise.alcatel-lucent.com/?solution=Healthcare&page=overview

BLOGS FOR MORE PERSPECTIVE
http://blog-enterprise.alcatel-lucent.com/topics/healthcare