Improving Health Care Quality in Zambia

The Zambia Electronic Perinatal Records System (ZEPRS) Network

1 Network Specifications

ZEPRS Background

The Zambia Electronic Perinatal Record System (ZEPRS) is an electronic medical record (EMR) system designed for public obstetric clinics and the University Teaching Hospital (UTH) in Lusaka. RTI is building the ZEPRS application under contract to the University of Alabama at Birmingham (UAB) with funding from the Bill & Melinda Gates Foundation. A team of UAB and Zambian doctors conceived the idea based on the very successful model of a web-based perinatal records system that the UAB had built in Birmingham that had improved patient outcomes there. ZEPRS, which uses a wireless network, is built using open-source components and best-of-breed Web-based application architecture. This minimizes operating costs and makes it easier to expand usage within Zambia and transfer to other countries. The application and electronic patient records are maintained in a central data center established at the Center for Infectious Disease Research in Zambia (CIDRZ). Medical personnel in connected facilities access the ZEPRS application through a Web browser. The high mobility of patients within the Lusaka health district and the need to share patient information across the dispersed health facilities lead the team to choose a web-based system. The system is designed to serve an estimated 55,000+ perinatal patients each year.

This project is designed to improve the quality of perinatal care in 23 participating clinics and UTH of the Lusaka Urban District by:

- allowing better access to patient records;
- implementing patient-care prompts into the system to make sure critical care issues are addressed during and from pregnancy to pregnancy;
- enabling health administrators and researchers to access data to help design interventions to further improve perinatal patient care; and

Basic network design

When the ZEPRS project was first started, in early 2002, the design for a network of clinics in the city of Lusaka, Zambia called for an expandable and robust Wide Area

Network to be setup. This network was meant to achieve a series of goals as resiliency, expandability and low-cost and at the same time allow the interoperability of equipment from different providers.

To achieve this goal, RTI's engineers worked together with regional firms to decide on the basic design for this network and its minimum specifications together with a growth path for the coming years.

Given the low availability and reach of the communications infrastructure in the city (poor telephone lines, nonexistent metropolitan fiber optics rings) the most adequate option to interconnect all the centers in this network was using wireless links. The scenario is not uncommon to other cities in Africa and technical skills and equipment is usually available from local resellers.

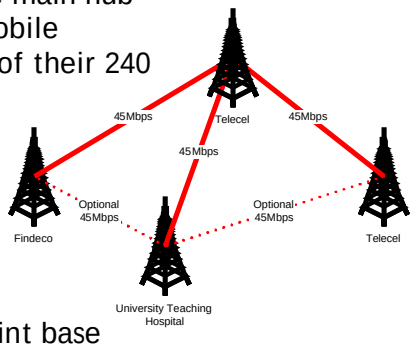
The basic layout called for a set of four "high sites" each one connected with a 45Mbps link in a star-shaped design and from each site a 10Mbps direct link to the participating clinics and centers.

This design allows for great flexibility and reduces the numbers of hops from the clinics to the datacenter while it can be easily interconnected in a partial mesh design to improve reliability.

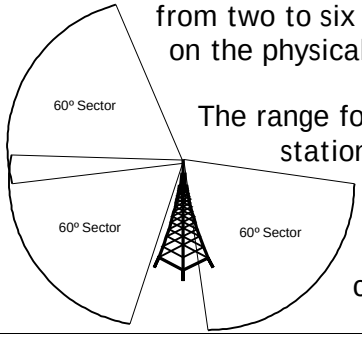
Aware of the increasing saturation of the 2.4GHz band in Lusaka it was decided to use equipment in the 5.8GHz band for the network backbone and the last-mile connection to the clinics, while 2.4GHz equipment was used in some non-core point-to-point (PTP) links and mostly reserved for local networks.

First links

To avoid the excessive cost of the masts needed for the main hub sites; arrangements were made with Telecel, a local mobile telephony provider, to co-locate our equipment in two of their 240 feet towers and with the administrators of the Findeco building, almost 300' above surface. With the towers secured, the first 5.8GHz/45Mbps Tsunami point-to-point links were installed, building the network backbone and its main link to the datacenter, still under construction.



Each tower was provided with a set of point-to-multipoint base stations (BS) from Proxim, also in the 5.8GHz band and with a maximum throughput each of 20Mbps. Each base station covers an area of approximately 60º and each main site has from two to six base station, to cover a sector from 120º to 360º, depending on the physical location of the clinics it serves.



The range for each base station (10 Kms.) was appropriate for most base-station-to-subscriber-unit link, but since this band requires unrestricted line of sight (LOS) and since some places were located near the maximum reach of these units, additional PTP equipment had to be installed to ensure proper coverage of all the clinics. The Quickbridge units from Proxim

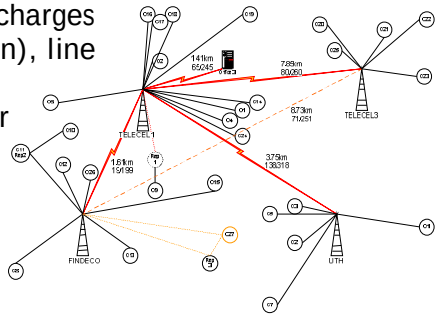
were selected due to their low cost and ease of installation.

Connecting clinics

All the participating clinics were provided with one Tsunami subscriber unit (SU) capable of providing a maximum throughput of 17Mbps, each one pointed to one of the already installed BSs, and terminating internally on a 100Mbps switch.

All the indoor equipment was located in wall-mounted 19U racks with fans and protected with an APC SmartUPS 1500.

In order to protect this equipment against electrical discharges (such as lightning, very common in Zambia's rainy season), line filters from Transtector and Polyphaser were installed; using two units, one near the outdoor unit, and one near the cable entrance to the building provided very good protection against lightning. The power-over-Ethernet connectors (PoE) saved many hours of work during the installation and allowed us to protect both data and power lines with the same filter.



At this stage, the network had a reach of 25 different locations within the city of Lusaka and it was ready to start receiving additional devices.

Setting up the local area networks

All of the clinic's networks and most of the equipment installed at the University Teaching Hospital of Lusaka (UTH) is wireless. Due to its broad market penetration and interoperability, 802.11b was chosen as the standard (with a clear upgrade path to 802.11g in the future).

To simplify the required support skills and the time to troubleshoot the LAN equipment, all the clinics were furnished with the same LAN hardware consisting of one 100Mbps desktop switch, one SmartUPS 1500 with an additional battery, one MVP 210 VoIP adapter and one Cisco Aironet 350 access point, all located in a wall-mounted cabinet.

From that basic LAN "kit" other devices were added to allow for extended wireless coverage: running cables to connect additional wireless access points at the UTH halls or directional antennas to link far-off wards with wireless repeaters.

Desktop computers

The main requirement for the computers within the clinics was mobility. With cost, theft-deterrence and mobile printing capacity as important issues to consider, the possibility of using laptop computers was discarded, and instead a series of small-footprint desktop computers were selected (Dell Optiplex) and installed on mobile carts, each one provided with a SmartUPS 1500 with one backup battery, an HP Laserjet printer with a wireless print server and security cables connecting every device to its metal cart for added security. Each battery set will provide up to seven hours of uninterrupted operation.

The carts can be moved around very easily and are sturdy enough to ensure that the equipment is safe from accidental mishaps or theft. Cable locks with master keys have been provided to secure all the equipment to the carts, including keyboards and mouse, and to prevent unauthorized users to open the computers.

There are three different computer models used at the clinics, hospital and datacenter, two from Dell and one from IBM, and for each one of those models a desktop computer software image was created and is regularly maintained by the local staff. Performing the rollouts based on software images allowed the team to keep a standardized software base and also to reduce the time required for desktop troubleshooting.

All the software updates are centrally managed through an instance of Windows Update Services running on the datacenter, with the desktops configured to check in at different times and download the operator-approved updates to the desktop computers. Our local staff has been operating with this model for more than a year now and through 3 separate computer rollouts with excellent results.

Datacenter

The datacenter for the project is located at the Center for Infectious Disease Research in Zambia (CIDRZ), a non profit organization founded by Zambian and US –based (University of Alabama at Birmingham) health professionals. Three Dell PowerEdge 2450 servers running Linux, with an external storage unit and a multi-tape capable backup unit share the load for the Java application engine, provide replicated database services, web services, email services, DNS, wireless authentication security through RADIUS and help on the monitoring of the network.

The following table shows a brief summary of the main products used at the datacenter level:

Platform Component	Selected Solution[1]
Server Operating System	Red Hat Enterprise Server 3
Server Backup	Arkeia Backup 5.2
Wireless Authentication	AEGIS Premium Server 1.1.4
Relational Database	MySQL 4.0
Web Application Server	Apache 2 + Tomcat 5
E-mail	Cyrus IMAP, Sendmail, Spam Assasin with Squirrel Mail E-mail Web Interface
Firewall	SonicWALL
Client Anti-virus	McAfee VirusScan 8
E-mail Server Anti-virus	AMaVIS

Software elements at the datacenter level

To support the Windows-based monitoring applications and the desktop computers update services, there is a Windows 2000 Server co-located in the datacenter.

The Dell tape changer simplifies the backup process and prevents errors that may result from inserting tapes out of sequence, or forgetting to replace them. All the backup functions are performed by an instance of Arkeia backup running under Linux and with agents running on the other servers to provide for centralized backup.

Internet connectivity is also provided and managed at the datacenter level, with one dedicated, multiport firewall filtering traffic and keeping the different networks secure and one server providing caching and traffic shaping services for the client computers.

These servers, together with the communications equipment, including the existing PABX system and the newly-installed VoIP system, are located in a closed room with a password-protected lock and protected by a 3000VA UPS connected to an auto-starting diesel generator.

Network layout

In its first stage, the network was conceived as a single switched broadcast domain, with 100Mbps switches at each main sites and 100Mbps switches at each clinic. This decision was taken based on the estimated total number of devices to be installed on the network (approximately 150) and the fact that each high site can be turned to a separate segment by adding a router, if traffic or redundancy needs made it necessary.

[1] The indicated versions are the ones used at the start of the Project and it's likely that upgrades within the same product line have been performed.

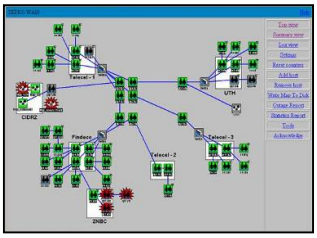
The initial traffic measurements and the ongoing monitoring of the network showed that excessive broadcast were not an issue. To help reduce unwanted or "maintenance" traffic to a minimum, the protocol and applications suite to be installed at each desktop was carefully evaluated to reduce network traffic.

Network monitoring

All of the devices that form the network infrastructure, together with the servers and the services they provide are monitored 24 x 7 from the datacenter, and data related to uptime, faults and performance is collected regularly and can be queried easily to help troubleshooting and capacity planning efforts.

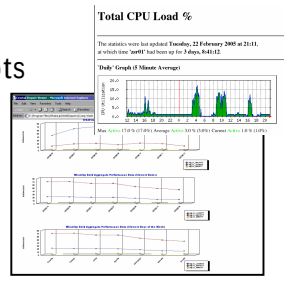
The main tool for real-time data collection and display is What's Up Gold (WUG). This tool keeps an updated map of the network, reporting information on failed links, sending alerts via email and SMS to the technical staff mobile phones.

WUG is SNMP compliant and can communicate with the SNMP modules running on the wireless devices and the servers.



On a weekly basis, WUG's automated report generation tool provides staff and management with customized reports on network uptime.

As a long-term data collection tool, the Linux-based version of MRTG is being used. MRTG collects information though SNMP for baselining and historical analysis of performance on network traffic, storage space availability, power availability, processor utilization on the main servers, etc.



The management suite is completed with some custom-made scripts that allow for interoperability between the UPS management software (PowerChute) and the Linux servers in the datacenter.

With strong web access, all these monitoring tools were of immense value to follow the functioning of the network from remote locations while it was being setup and to perform the daily maintenance tasks by the local staff.

VoIP Services

Voice services are a must for clinics that need to deal with sometimes life-and-death situations, but for many clinics the luxury of a phone line was a distant reality, mostly due to cost or to the unavailability of phone lines in the area.

In order to work around this limitation, some of the clinics already had two-way radio equipment, similar to the kind used for CB (Citizens Band). This equipment was expensive and certainly more complicated to use than telephone handset and not widely installed, only allowing certain clinics to reach the UTH to inform of patient referrals and other incidents.

To leverage the installed network, a complete VoIP (Voice over IP) system was installed and interconnected with the existing PABX at CIDRZ.

Each clinic was provided with a Multitech MVP210 unit, capable of up to two phone connections each. This unit was located together with all the networking equipment at the clinic level and protected by the same UPS.

At the datacenter level, several Multitech MVP 810 units were installed to allow for termination of the lines from the clinics and to interconnect the existing telephone lines, allowing the system to reach to the national grid.

The Multitech system allows restricting calls to certain numbers and thus keeping strict control on the costs of running the telephone system.

By using the VoIP system the clinics have a much easier way to reach not only CIDRZ and UTH, but also other clinics with almost no running-costs and using far cheaper equipment. Nurses require no training to use the system and in case of emergency they can also reach numbers outside the VoIP network.

Security management

Providing network security in this highly distributed, high-transit wireless environment required a careful evaluation of the risks involved together with a balance between usability and security.

Clearly, the distributed wireless access points (at least one in each clinic) were one of the main concerns, in order to secure and audit those connections a RADIUS server was installed at the datacenter for each AP to authenticate and negotiate WEP keys with it; a log is kept of all the devices connected to the network and it also allows for a way to centrally distribute configuration options (as timeouts, security policies, etc) through RADIUS options.

The APs were also configured to send SNMP traps to the central management console and inform of rogue APs detected, unsuccessful logins to the AP, etc, and in order to detect strange traffic patterns, the network monitoring tools keep traffic information on all the wireless devices in the network.

The configuration for the APs is centrally managed and replicated and updated to the APs over-the-wire, using a web-based application.

To allow for a simpler setup, desktop security is not centralized but instead each computer behaves like a thin client, with a minimum set of applications, a common login scheme and all the applications being accessed through a web-based interface. The web browser's interface has been heavily customized to restrict configuration changes and to present a cleaner look to the user.

Initially, all the servers, datacenter desktops and wireless network were located on the same network segment; this was deemed as not secure and a proposal to create different "network domains" was drafted to UAB, where a central firewall will control the flow of data from one network to the other keeping a separate network for external services (SMTP), main servers, IT personnel, and wireless clinics.

Configuration and Asset management

In order to build a document library to serve as a source of reference, RTI worked closely with the local staff on the documentation of the steps, technologies and services implemented on the network, keeping this information readily available and ensuring the staff can easily understand what has been written and add to it in the future as the network evolves.

Along with the technical documentation, RTI's network specialist created a central repository for configuration files and policies. He also created documents detailing the regular maintenance and monitoring tasks needed to keep the network running smoothly.

To allow the project to keep control of the hardware belonging to the project, a web-based inventory system was installed; this simple system allows for the tracking of assets by location, the follow-up of service requests and the reporting and alerting functions needed to order consumables and spares parts and is backed by the existing web and database services running on the central servers.

Local Staff and Training

A key aspect of sustainability of the ZEPRS network is to ensure that there is a strong local technical team able to troubleshoot any problems that arise and to perform routine maintenance. At every step of the installation of the network the local staff - ICT coordinator, User Support Technician and Datacenter Technician -were brought in to participate and learn through on-the-job training; several dedicated training sessions were setup, and a laboratory (able to replicate the server installation at the datacenter) was setup to allow the technicians to test new tools and practice with new configurations, without risking the stability of the network. An RTI home office network specialist and other project team members supported the local team with technical advice and training.

Supplemental training, provided by the equipment vendors was given at local and international locations.

A key element in the knowledge-transfer process was working with the local technical staff to apply the configuration and rollouts for networking equipment and PCs while having RTI personnel setting up the path and then providing minimum guidance. This allowed the staff to learn by doing and to encourage their sense of ownership and pride.

2 Concept Replication

The ZEPRS Network involves many different sites, networking and security equipment, servers and employs a group of people for its maintenance, all this necessary to distribute the ZEPRS applications, ancillary services and other services (not related to the project) that benefit from a high-speed network that now reaches places that previously were lacking even basic phone service.

Now, is this a replicable installation? Can this setup be used in a project that requires an application like ZEPRS to be used but that can not afford the complexity of this network?

Certainly.

There are some aspects of this network that would allow it to be used in different scenarios with minor alterations, doing a "rightsizing" of its components to suit each particular scenario.

The network design for ZEPRS can easily be replaced by a scaled-down implementation that deals with a reduced number of sites, and even the networking equipment can be switched to other models, brands or even frequencies if the uptime or traffic congestion in the selected band allows. The multiple-server approach can be easily reduced by consolidating multiple services in a single server; this will require a careful load planning and testing but will allow for a simpler setup.

All the applications used in this network are based on open standards and most of them use open source technologies or can be easily replaced by equivalent software released as open source, thus lowering the initial setup costs, and since there are no requirements on the client side beside the ability to run the open source Firefox browser there's nothing that will prevent choosing freely between different architectures and operating systems, or to customize the client to each installation.

For more information contact Pablo Destefanis, pdestefanis@rti.org, +1 (919) 541-6207 or Gordon Cressman, gmc@rti.org, +1 (919) 541-6363