# Bahir Dar University

## Computer Science and Engineering Department


GROUP MEMBERS

- MICHEAL GIRMA - 0401143
- MISGANAW DINKLG - 0401875
- REDIET GEDEFAW - 0401322
- SAMSON ENDALE - 0401365
- TSION ABEBE - 1962/03

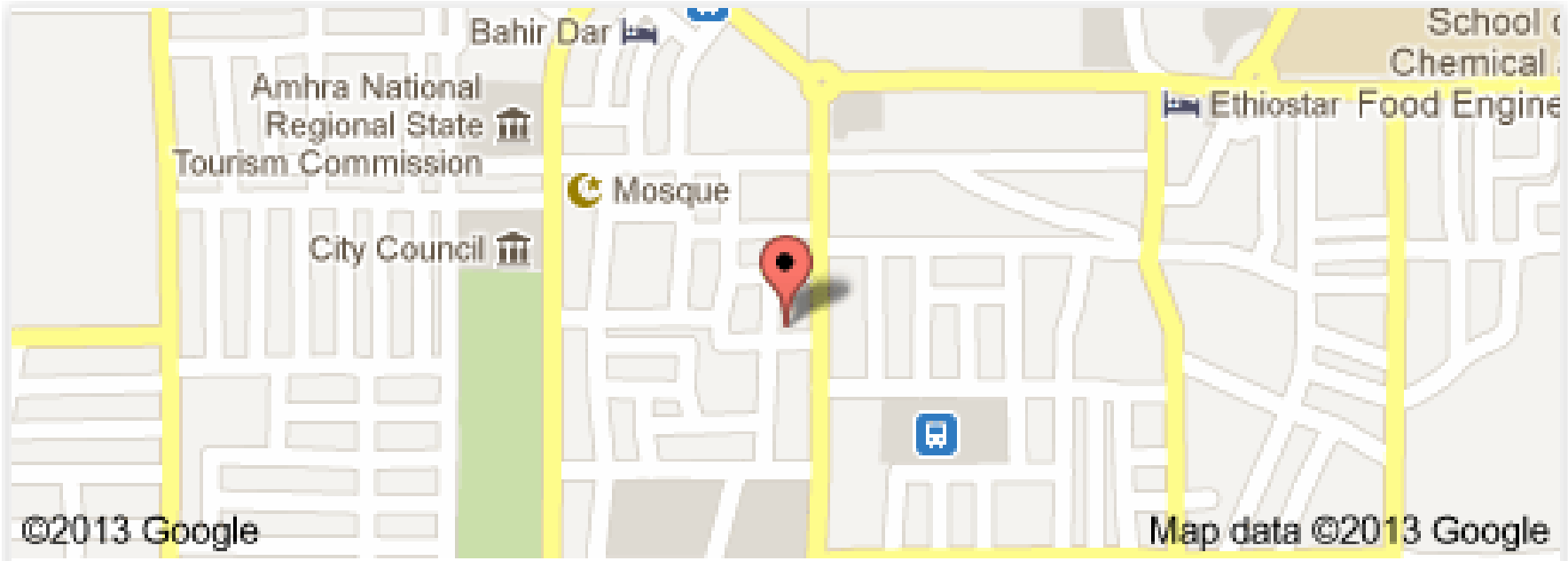

SUBMITTED TO GETASEW

DEAD LINE Tuesday, February 13, 2013

# GAMBI HOSPITAL

THE FRONT GATE OF GAMBI
(img src : www.google.com.et)

MAP OF GAMBI HOSPITAL




# Gambi Higher Clinic

**Address:** Bahir Dar

**Transit:** Minibus to Zege

**TABLE OF CONTENTS**

# I. EXECUTIVE SUMMARY

Gambi Hospital is interested in an upgrade to its network system. The current network supports email, basic Internet access, and a few specialized medical software tools. Users have complained about occasional downtime and slow response times when accessing the network, especially at peak access times. At a minimum, Gambi wishes to correct these issues through an upgrade to their system, but management is also looking to be able to improve productivity and increase security of the confidential data sent over their network.

The proposed solution that follows involves significant changes to Gambi's network systems. The current hardware used throughout the network was purchased over a long period of time and uses many different technologies. The new basic physical network architecture will require several upgrades in hardware that address these incompatibilities and older technologies. The result will be higher speeds, more reliability, and easier maintenance of network components. The upgraded hardware will use up-to-date, compatible technologies that will greatly facilitate troubleshooting and maintenance as well as resolve the slow access times that are currently being reported.

In addition to updating the hardware, the proposed solution outlines some changes in the network configuration. These changes, if implemented, will provide greater reliability and security for all users of the Gambi network. Along with the new hardware, the new network configuration will open the door for Gambi to explore new possibilities in using the network to increase overall productivity and, in the end, better serve the needs of their patients.

The solution outlined below will provide the greatest benefit possible for Gambi meeting all of their current needs and providing for future expansion at the lowest cost possible. The total estimated cost for the project is just under $900,000; this takes into account not only resolving current network problems, but also the overall cost of network ownership in the future.

## OVERVIEW

Gambi Hospital is medium-sized local hospital located in Bahir Dar, with approximately 500 staff members supporting up to 1000 patients. The hospital is interested in updating its network system in its facility. The hospital network carries critical patient care data in real time from both a mainframe host and several servers to workstations in operating rooms, doctors offices, the billing office, teaching labs, and remote clinics across the region. Of course, all of the data transferred is highly confidential and must not be lost or accessed by unauthorized personnel. Within the hospital, a regional regulation was enforced to its employees and staff. One aspect of this regulation addresses the security and privacy of medical records, including those stored or transmitted electronically. The hospital employs data encryption and email protection as a means of protecting confidential patient information.

Gambi has four small remote clinics. The building has four floors with wiring closets per floor. The hospital is aggressively expanding its clinic and alternative emergency room. Due to population growth in general, plans to enlarge the hospital building are also under way. The hospital is doing fairly well financially. It wants to selectively deploy cutting-edge technology for better patient care and high productivity. Management is tired of network downtime and slowness affecting patient care. The staff members have frequently complained about slow response times. There appears to be severe congestion of the LAN, especially at peak hours. The hospital would like to upgrade the WAN infrastructure to provide sufficient bandwidth between the remote clinics and headquarters at the same time. The applications that the organization is currently running include standard office applications, plus some specialized medical tools running over IP. Gambi radiology, oncology, and other departments do medical imaging. As these departments acquire new tools, they are adding real-time motion to highly detailed medical images, requiring large amounts of bandwidth. Many lack uninterrupted power supplies or proper environmental controls.

Network manageability is important because Gambi has a tradition of basing operations on small support staffs with high productivity. Gambi's upgrade timeframe is 6 to 12 months.

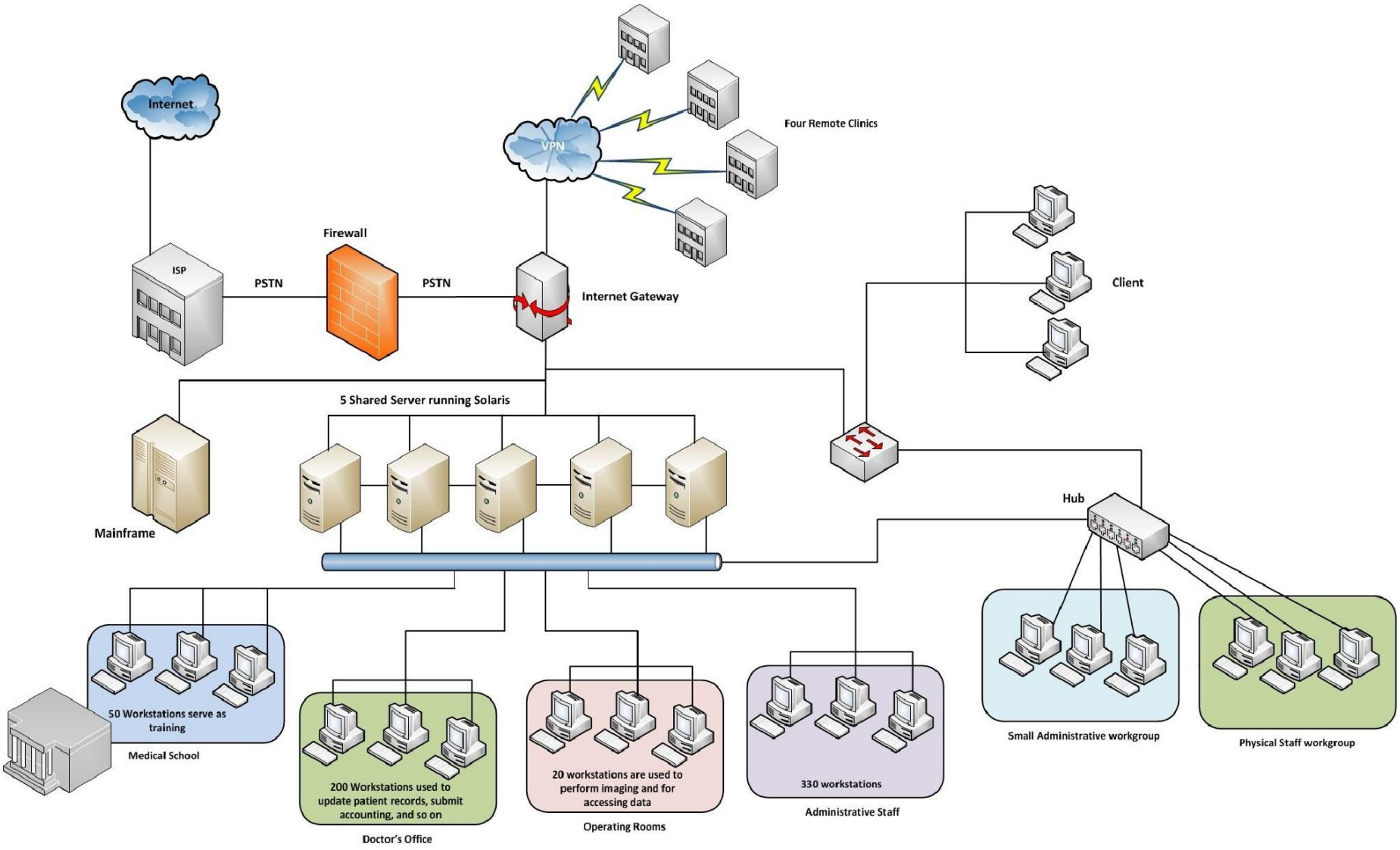
While we were researching about Gambi, we ask information from the hospital in person but, we couldn't get any so we assume some of the data we used.

## CURRENT SITUATION

The current network uses inexpensive switches from several vendors, purchased over time. They comply with various standards, depending on when they were purchased. Specifically, the network is configured as follows:

- Six hundred workstations are connected to five shared servers that run Solaris. Fifty of these workstations serve as training computers in medical school classrooms. Two hundred workstations sit in doctor's offices and are used to view and update patient records, submit accounting information, and so on. Twenty workstations are used in operating rooms to perform imaging and for data access in real time. The remaining workstations are used by administrative staff.
- The clients are connected in a mostly switched, star-wired bus network using Ethernet 100Base-T technology. In the few instances where switches are not used, hubs serve smaller workgroups of administrative and physician staff.
- An Internet gateway supports e-mail and online medical searches.
- The WAN uses 56-kbps links to two of the remote clinics and dialup connectivity to the other two. The one router uses static routing that was configured by a previous network designer.
- A firewall prevents unauthorized access from the PSTN connection into the hospital network.

## GAMBI EXISTING NETWORK DIAGRAM



## PROJECT OBJECTIVES

The major objective of this project is to upgrade the network of Gambi Hospital in order to:

- Provide more than adequate bandwidth between the remote clinics and headquarters
- Improve and consolidate network performance at Gambi Hospital.
- Provide increased network capacity
- Provide future expansion capability.
- Improve the network's fault tolerance, security, and high speed connection, which will increase the efficiency of day-to-day operations in the hospital by making access time quicker.
- Identify the critical points of failure in the existing network and propose on how to eliminate them.
- Recommend which points of failure should be addressed to increase availability and how to increase this goal.

## PROJECTED BENEFITS

- Improved network reliability, security, and fault tolerance. Critical points of failure will be identified and redundancy will be implemented to provide fault tolerance. This will save Gambi a great deal of money lost from a network failure a single failure would likely cost Gambi at least $10,000. Additionally, a breach in security could potentially cost millions in lawsuits.

→ While we were assuming cost, we used ("www.amazon.com and www.ebay.com") so all the prices we used are in USD.

- Improved network scalability--an estimated savings in upgrade costs and hardware purchase cost of $300,000 over the next 5 years. The hardware purchased with this proposed upgrade will facilitate incremental expansion of the network as demand increases. It will also help reduce the costs of the next upgrade several years in the future.
- Improved network speed and capacity--a projected savings of $5,000 per month in staff pay due to higher productivity. Gambi will be able to process more records and accomplish more work with fewer staff. Much less time will be spent waiting on the network.

## PROJECT BUSINESS AND TECHNICAL GOALS

**Business goals**

- Reduce operational costs
    - Measured in terms of real Total Cost of Ownership (cost per computer per year). **Current**: Around $2,203,000 per year. **Projected**: $1,153,272
- Reduce operational inefficiencies:
    - Measured in terms of network availability (hours of downtime per month). **Current:** Average of 7.4 hours per month. **Projected:** 4.5 hours per month. Every hour that the network is unavailable costs the hospital an estimated $2,000 - $3,000 per hour.
    - Also measured in average time to process a medical record (from opening a record to submitting all changes). **Current:** Median time of 3.2 minutes per record. **Projected:** 2.5 minutes per record.
- Increase employee productivity:
    - This will be measured in terms of average number of staff hours per month: **Current:** 28,400 hours per month. **Projected:** 27,600 hours per month. Note: view this alongside number of patients per month.

**Technical goals**

- Improve Network Speed and Capacity:
    - Replace PSTN line with T3 lines. T3 is a digital carrier standard in North America that can carry the equivalent of 672 channels for voice and data, voice, video, or audio signals
    - 56 Kbps and Dial-up connection from the CO to the four remote clinics will be replaced to a frame relay and site-to-site IPsec VPN in order to have WAN backup links and security.
- Improve Network Security:
    - Create an isolated VLAN for the Medical School in order to prevent students accessing data from the other servers
    - Replace hubs with managed switch. Managed switches provide all of the features of an unmanaged switch and provide the ability to configure, manage, and monitor your LAN. And this gives greater control over how data travels over the network and who has access
    - Comply fully with regional regulations.

## PROJECT PROPOSAL

The following are the major design areas to be addressed:

- Indentify the relevant network applications, their logical connectivity requirements, and the services required.

- Redesign the Gambi LAN: The entire network needs to be redesigned because there is no redundancy. Included in the redesign fix the placement of the servers that will be implemented and the identification of the single point's failure in order to find solutions to eliminate them.
- Upgrade the WAN links: The upgrade of the WAN links is essential because, according to the company, the current bandwidth seems insufficient. The WAN uses 56-kbps links to two of the remote clinics and dialup connectivity to the other two. Furthermore, the hospital is using a new medical imaging application that takes a lot of bandwidth.
- Isolated VLAN of Medical School: The 50 workstations connected to the five-shared servers that serve as training to medical school need to have an isolated VLAN in order to prevent unauthorized data access by medical student from the main server.
- Firewall: There should be a firewall in between the router that connects to the four remote clinics in order to prevent unauthorized access from outside Gambi.

## CAPITAL AND OPERATING REQUIREMENTS

This section of the report covers the estimated costs for this project.

| | | | | | |
|---|---|---|---|---|---|
| *Cisco Catalyst 6509-E Switch* | *$* | *5,354.95* | *6* | *$* | *32,129.70* |
| *Cisco Catalyst 3560-X Series Switches* | *$* | *8,225.47* | *13* | *$* | *106,931.11* |
| *Cisco Nexus 7000 Series Switches* | *$* | *12,739.00* | *2* | *$* | *25,478.00* |
| *Cisco 881 Integrated Services Router* | *$* | *618.99* | *8* | *$* | *4,951.92* |
| *CyberPower CP1500AVRLCD UPS - 900 Watt - 8.5 Ah* | *$* | *149.99* | *20* | *$* | *2,999.80* |
| *Cisco ASA 5510 Security Plus Firewall Edition - Security appliance* | *$* | *2,475.00* | *8* | *$* | *19,800.00* |
| *Cisco Small Business Pro POES5 PoE splitter* | *$* | *24.99* | *6* | *$* | *149.94* |
| *Cisco 10/100 8-Port VPN Router* | *$* | *266.95* | *4* | *$* | *1,067.80* |
| *Cisco Catalyst 3560G-24TS Switch - 24 ports - L3 - managed* | *$* | *2,235.00* | *10* | *$* | *22,350.00* |
| *RJ 45 Plugs *Pack of 50* | *$* | *49.99* | *12* | *$* | *599.88* |
| *Cisco Small Business VC 220 Dome Network Camera* | *$* | *567.47* | *5* | *$* | *2,837.35* |
| *T1 Access Installation (monthly fee)* | *$* | *350.00* | *4* | *$* | *1,400.00* |
| *T3 Acess Installation (monthly fee)* | *$* | *7,000.00* | *1* | *$* | *7,000.00* |
| *5-Mbps increments times $75 plus $5 per PVC* | *$* | *5.00* | *4* | *$* | *20.00* |
| *Labor (@ $75 per hr)(≈ 1,350 ETB)* | *$* | *75.00* | *900* | *$* | *67,500.00* |
| *Network Analysis and Design* | *$* | *150,000.00* | *1* | *$* | *150,000.00* |
| *Network implementation* | *$* | *150,000.00* | *1* | *$* | *150,000.00* |
| *Training* | *$* | *100,000.00* | *1* | *$* | *100,000.00* |
| *Ongoing Network Supposrt and Maintenance* | *$* | *100,000.00* | *1* | *$* | *100,000.00* |
| *Other neccessay labor* | *$* | *20,000.00* | *1* | *$* | *20,000.00* |
| | | | | | |
| ***TOTAL COST*** | | | | ***$*** | ***815,215.50*** |

## SUMMARY OF RECOMMENDATION

In summary, the primary goal of this project is to upgrade the existing network of Gambi. Accomplishment of the goal will be the redesign of the hospital LAN and the upgrade of the WAN links, the creation of an isolated VLAN for the Medical School students, patients, and visitors; and superior firewall protection. As part of our upgrade recommendation, the inclusion of the physical and logical design and specifications for the network is shown on a diagram, which also includes these modifications. A security evaluation attained to determine the security of the network, incorporate toward the establishment of a new Gambi network security policy that takes into account the network upgrade, and follow regional standards. The estimate for implementation of the network upgrades per recommendation will incur a cost of less than nine hundred thousand dollars to Gambi Hospital. Our belief, with the new network upgrades, Gambi will achieve its goal of modernizing its technological resources. In addition, the implementation of the new network upgrades will provide the critical and much-needed benefit of improving Gambi's fault tolerance and security, as well as provide a high-speed connection.

## II. NETWORK ANALYSIS

In the preceding section, the team presented the existing network diagram of Gambi. In this diagram, the team had identified critical points of failure. Please see the Table 1- Suggestion How to Eliminate Them.

Table 1- Suggestion How to Eliminate Them

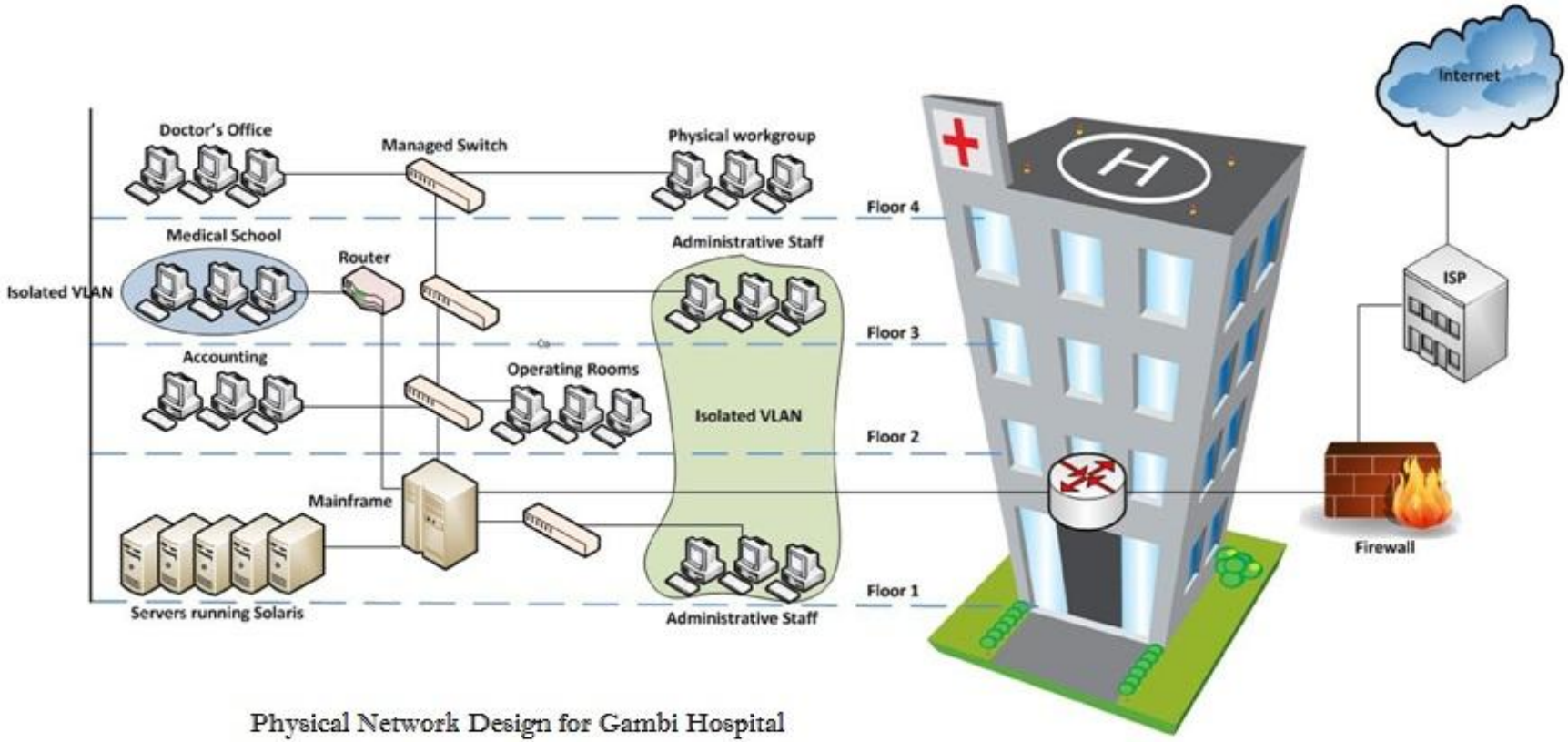
| CRITICAL POINTS OF FAILURE | SUGGESTION ON HOW TO ELIMINATE THEM |
|---|---|
| • Each server that contains patient records or other critical data, and the NICs, hard disks, cabling, memory and CPU in those servers.<br><br>• Switches and Hubs that link to the operating rooms, doctors office, billing offices, teaching labs | Sometimes computer users unintentionally harm data, applications, software configurations, or even hardware. The Gambi network administrator must take precautionary measures and pay regular, close attention to systems and networks to protect them such as:<br><br>• All possible redundancy should be employed to protect the availability of the operating room systems, including redundant cabling, redundant NICs in the server that those workstations use, fail-over capabilities in the switches these machines attach to, UPS backup for the servers that contain patient records, and centralized data backup for all servers.<br><br>• Switch redundancy: if network problems exist due to switch A failure, switch B still functional and supply the links to the server; to the other two distribution switches and to the WAN link. This redundancy solution will prevent the network system down due to a single switch failure.<br><br>• Link redundancy: backup the link when there is a link failure to the server; or to the switches. The trunk ports of the switch are specifically used for backbone connection between switches. |

| | |
|---|---|
| PSTN link to a local ISP | PSTN link to the ISP should be replaced into T3. Upon replacement there would ideally be two T3's from different providers bundled together for ease of use by a router using EtherChannel or a similar protocol. The link to the ISP should have a backup mechanism, either a dial-back ISDN line or an arrangement with the ISP to have a second dedicated line available for emergencies. For example the telephone company would provide the T3 and the cable company would provide the secondary circuit |
| Internet Gateway | The internet gateway would need to be duplicated. If all three items (email, VPN, and online medical searches) are housed on the gateway it would be best to duplicate these on the second gateway. Today's router or firewall can handle multiple links of failover but it would be a very good idea to have a preconfigured firewall on standby. |
| The connection from the server to the 50 workstations that serve as training in the Medical School | There should be an isolated VLAN to prevent the students to access patient records. |
| The connection to administrative workstations | Isolated VLAN can also be implemented on this in order to prevent the administrative staff from accessing the records found in the doctor's office and so on. |
| VPN connection to the four remote clinics | There should be a firewall on each VPN connection. Firewall is set up to prevent unauthorized access outside from the hospital and encrypts traffic between the sites. |

## III. PHYSICAL DESIGN

In this section, the physical topology demonstrates the direction of the physical design implementation and illustrates the major points of the network upgrade, which includes the devices, locations, and cable installation.

In the main floor of the building, the mainframe and the five servers are in place. The mainframe connects to the five servers. The managed switches from the different floors then connect to the mainframe. Please see the figure below.




Physical Network Design for Gambi Hospital

The physical design has the following features:

- The building is equipped with Category 5e cabling and wallplates in the offices, classrooms, labs, and so on.
- Within the building, managed switches are used. Managed switches give more control over LAN traffic and offer advanced features to control that traffic. It provides the ability to configure, manage, and monitor LAN and this gives greater control over how data travels over the network and who has access to it. In addition, managed switches use protocols such as the Simple Network Management Protocol, or what we call SNMP, for monitoring the devices on the network. SNMP is a protocol that facilitates the exchange of management information between network devices. SNMP queries can determine the health of the network or the status of a particular device. By displaying this data in an easily understood format, IT managers located at a central site can monitor the performance of the network and quickly detect and repair network problems without having to physically interact with the switch.
- A separate router is used in the third floor. The sole purpose of this router is to manage the VLAN of Medical School in order to prevent the students from accessing the critical information of the hospital such as patient information.
- The ISP stands for Internet Service Provider. These are companies that provide access to the Internet.
- The firewall is a device designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

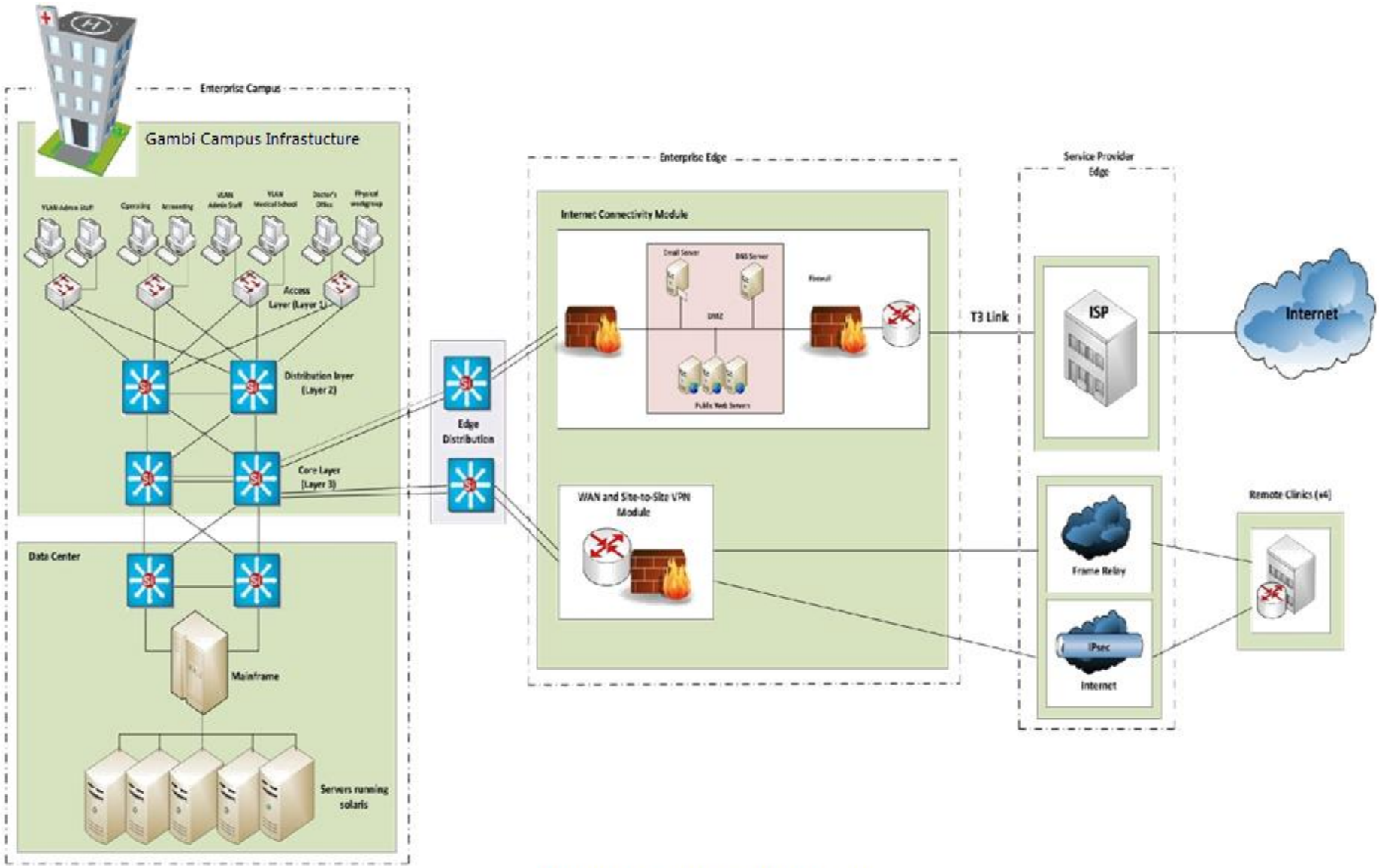
## IV. LOGICAL DESIGN

In order to meet Gambi's business and technical goals, the team applied the Cisco SAFE Architecture in designing Gambi Hospital logical design. The principal goal is to provide best practices information on designing and implementing secure networks. This architecture uses a modular approach. The modularity built into the architecture allows flexibility in network design and facilitates implementation and troubleshooting. Cisco SAFE Architecture takes a defense -in-depth approach, in which multiple layers of protection are strategically located throughout the network. These layers are under unified strategy for protecting the entire network and the various components of the network, including individual network segments, infrastructure devices, network services, endpoints, and applications.

The logical network topology for Gambi is divided into three functional areas (also called modules), as illustrated in the logical design below.

- Enterprise Campus - This area contains all the functions required for independent operation within one campus location; it does not provide remote connections.
- Enterprise Edge - This area contains all the functions required for communication between the Enterprise Campus and remote locations, including the Internet, remote employees, partners, and so forth.
- Service Provider Edge - This functional area is not implemented by the organization; rather, it is included to represent WANs and Internet connections provided by service providers.

Each of this functional areas contains network modules, which in turn can include the core, distribution, and access layer functionality.




**Logical Network Design for Gambi Hospital**

The following are considerations provided to the functional areas and modules.

**Gambi Hospital Campus Infrastructure Module**

The Campus Infrastructure module connects devices within a campus to the Data Center and Enterprise Edge modules. The Campus Infrastructure module includes three layers:

- **Access Layer**

  The Access layer, located within a campus building, aggregates end users from different workgroups and provides uplinks to the Building Distribution layer. This contains all the devices to allow authorized users in the building to access the network. This includes end-user devices, such as workstations, etc., as well as devices to interconnect the end users to the services they require. This layer is responsible for ensuring that only users who are authorized to access the network are admitted. This layer provides important services, such as broadcast suppression, protocol filtering, network access, IP multicast, and QoS.

- **Distribution Layer**

  The Distribution layer provides access between workgroups and to the Core. Routing is implemented in this layer. This layer controls access to services by implementing filters or access lists. Redundant switches and redundant links to both the access and backbone is also implemented. So in case the one of the routers or links will be down, the network can still continue to function.

- **Core Layer**

  The Core layer provides a high-speed connection between the access layer, distribution and the data Server and Edge Distribution. Redundancy is implemented to ensure a highly available and reliable backbone.

**Data Center Module**

The data center contains internal Gambi servers. These servers include e-mail, file, and print servers, or any other servers that are necessary for the network solutions. Redundancy is also implemented within this layer and to the Core so that authorized users always have access to the servers they need.

**Edge Distribution Module**

The Edge Distribution could be optional. This module aggregates the connectivity from the various elements at the enterprise edge and routes the traffic into the Campus Core layer. In addition, the Edge Distribution module acts as a boundary between the Enterprise Campus and the Enterprise Edge and is the last line of defense against external attacks.

The Edge Distribution provides additional security between the Enterprise Campus and the Enterprise Edge. The edge distribution protects from the following threats:

- IP spoofing—the edge distribution router protects the core from spoofing of IP addresses.
- Unauthorized access—Controls access to the network core.
- Network reconnaissance—filtering of network discovery packets to prevent discovery from External networks.
- Packet sniffers—the edge distribution separates the edge's broadcast domains from the campus, preventing possible network packet captures.

**Enterprise Edge Internet Connectivity Module**

The Internet Connectivity module provides internal users with connectivity to Internet services, such as HTTP, FTP, Simple Mail Transfer Protocol (SMTP), and DNS. This module also provides Internet users with access to information published on an

enterprise's public servers, such as HTTP and FTP servers. Devices in this module include DNS servers, public servers (FTP and HTTP), DMZ, firewalls, and edge routers. Major components used in the Internet Connectivity module include the following:

- **SMTP mail servers**: Act as a relay between the Internet and the intranet mail servers.
- **DNS servers**: Serve as the authoritative external DNS server for the enterprise and relay internal DNS requests to the Internet.
- **DMZ**: It prevents outside users from getting direct access to a server that has hospital data.
- **Public servers (for example, FTP and HTTP)**: Provide public information about the organization. Each server on the public services segment contains host-based intrusion detection systems (HIDS) to monitor against any rogue activity at the operating system level and in common server applications including HTTP, FTP, and SMTP.
- **Firewalls:** Provide network-level protection of resources, provide stateful filtering of traffic, and forward VPN traffic from remote sites and users for termination.
- **Edge routers**: Provide basic filtering and multilayer connectivity to the Internet.

**WAN and Site-to-Site VPN Module**

This module provides reliable WAN connectivity. This module supports traditional, circuit switched, and more advanced media. A backup WAN link with site-to-site IPsec VPN is also added in order to provide security and redundancy.

Below are the following options for Gambi Hospital WAN connectivity.

| Option | Technology | Speed | Price Per Month | Monthly Cost |
|---|---|---|---|---|
| **1** | Leased line: T1 at clinics into T3 at main hospital building | T1 or T3 | $400 for each T1,<br>$8000 for the T3 | 4* $400 = $1600<br>1* $8000 = $8000<br>Total = $9,600 per month |
| **2** | Frame Relay: T1 access at clinics,<br>T3 access at main hospital building | T1 or T3 | $350 for T1 access,<br>$7000 for T3 access<br>circuit plus CIR in | 4* $350 = $1,400<br>1* $7000 = $7000<br>* 1.544/5 * $75 = $92.64 |

| | | | | |
|---|---|---|---|---|
| | | | 5-Mbps increments times $75 plus $5 per PVC | 4 * $5 = $20<br>Total = $8, 512.64 per month |
| **3** | MPLS VPN: T1 access at clinics, T3 access at main hospital building | T1 or T3 | $500 for T1 access, $8500 for T3 access | 4 * $500 = $2000<br>1 * $8500 = $8500<br>Total = $10, 500 per month |
| **4** | High-speed business cable service at clinics | 6 Mbps downstream, 768 kbps upstream | $90 | 4 * $90 = $360<br>1 * $4000 = $4000<br>Total = $4, 360 per month |
| | T3 Internet at main hospital building | T3 | $4000 | |

Based from the calculation above, the cable connection is quite competitive on price but does not provide the same bandwidth upstream. This would be an issue (as it would be with asymmetric DSL) because moving images from the remote offices to the central office is limited to the 768-kbps upstream speed. An alternative would be to store the images at the main hospital if cable technology is used. This calculation suggests that more bandwidth would be useful. T1 Frame Relay at the remote clinics into T3 at the main hospital building is recommended. This approach provides guaranteed bandwidth with a good SLA at a reasonable price. Assuming that the carrier supports it, multilink Frame Relay could be used to add bandwidth up to 6 Mbps in the future.

## V. Gambi SECURITY POLICY

The following policy outlines data security at Gambi Hospital. All employees of Gambi agree to adhere by this policy for the duration of their employment at the hospital. In addition, it is the responsibility of every employee to report any known or suspicious activity that may be in violation of this policy. Therefore, familiarity with this security policy is mandatory for all employees.

### SECURITY

Security is of highest priority for Gambi Hospital. Information pertaining to patients and employees is, in many cases, confidential and personal. All business information and medical records will be secured and protected from unauthorized users. Also, users within the hospital should only have access to certain records and other information. Gambi will use the best network security measures available so all information will be adequately protected. These measures include a strong firewall that prevents any outside connections not explicitly authorized by Gambi, mandatory authentication in order to access any workstation, and isolation of the VLAN for the Medical School, and installing security cameras especially where the data center is located.

The use of physical security in Gambi Hospital Network will consist of measures designed to ensure:

- Control physical access to facilities – Effectively controlling physical access to your organization's facilities should be the single top concern for both your physical security staff. The use of the lock-and-key mechanism with key card access will be provided to essential and designated hospital personnel.

- Control physical access to data centers – Data-center access can utilize any of the preceding mechanisms in addition to PIN-reader-only access. The important difference with data-center access is that you are often dealing with a smaller set of operators – the key personnel authorized to enter and access the data center of the Gambi VLAN. When entering in and out in the Data Center make sure the door is always locked in order to prevent any intruders.
- Prevent password-recovery mechanisms in insecure locations – This would be particularly useful in insecure hospital offices or other locations where the physical security of a network device cannot be assured.
- Be aware of cable plant issues – The risk of an attacker accessing your physical cabling is important to consider because that level of access often can bypass other security controls and provide the attacker with easy access to information.
- Be aware of physical PC security threats – Provide file encryption on all desktop computers to prevent unauthorized access. And, provide secure network access to prevent unauthorized access: strong network passwords for each specified user, securing the desktop to location, and being vigilant.

## AUTHENTICATION

Users at Gambi will be assigned a personal profile with a specified security level based on the amount of information they need to access on a routine basis. A user's security level will range from 1-10, with 10 having the most access to Gambi information. In order to log on to a workstation anywhere in the hospital, a user must enter their login credentials, which will allow them access to the workstation and any information they are authorized to see. In addition to level 1-10 access, users can be granted access to specific areas of information throughout the hospital depending on their needs. These settings will all be configured by the network administrator. Once a user logs in, the workstation will automatically log out after 5 minutes of inactivity in order to maintain a high level of security. After this time, the user will be required to log back in to continue working.

## VIOLATION OF INFORMATION SECURITY

Even with network security and authentication in place, it is possible for information security to be compromised. The following list is not comprehensive, but it does specify a broad range of activities that constitute violation of the Gambi security policy:

- Leaving a workstation without logging out so that someone else could work on that workstation under your profile
- Giving out authentication information (user name, password) to anyone else
- Allowing someone else to look over your shoulder while you are logged on to a workstation (so that a password could be seen, or other private information)
- Attempting to access features, settings, or information that you are unauthorized to access
- Using a workstation under another user's profile
- Attempting to navigate to unauthorized websites that could potentially introduce a virus
- Attempting to tamper with, or alter in any unauthorized way, records or other information contained in Gambi's information systems. So this proposal is high confidential, should only be seen by authorized (Getasew).
- Taking any records or other information outside of the hospital premises without specific permission
- Attempting to alter any network configuration settings, or tamper with any network hardware or software

It is every employee's responsibility to report any suspicious activity that may be in violation of this policy. Per Gambi terms of employment, every Gambi employee agrees to abide by this policy and to help ensure that this policy is adhered to throughout the Gambi campus.

## VI. NETWORK COST OF OWNERSHIP

# System TCO by Category

The System Total Cost of Ownership (TCO) is defined by the following categories in implementing the network system at Gambi Hospital.

| Category | Gambi Hospital Network Infrastructure Costs |
|---|---|
| Power Equipment | $208,938 |
| Cooling Equipment | $100,800 |
| Engineering and Installation Labor | $233,320 |
| Electricity (at 0.07 per kw hour) | $473,514 |
| Service | $122,520 |
| Racks and Enclosures | $56,000 |
| Space Used for Network | $354,000 |
| System Monitoring | $1,620 |
| Project Management | $12,960 |
| **Totals** | **$1,153,272** |

- The total network cost of ownership per computer implemented in Gambi Hospital is projected at $1,922.13 per annum. This projected cost illustrates the new network design, implementation, and maintenance is below industry average in management of the network design.
- The initial design of the Gambi Hospital network is projected at $150,000.
- Total projected savings in the TCO is estimated to be $1,094,728 per annum or $1,749.55 less per computer operated in the system.

- Total estimated new revenues generated to Gambi Hospital with the new upgrade implemented system are $3,250,560. This estimate is determined by how well Gambi Hospital's staff is well trained and adapts into the new network set up as the success relies heavily on how well the cycle of patient account entries. Building a patient access team is a crucial step toward improving billing and collections efforts and increasing revenue cycle performance.

- Total Return of Investment (ROI) for the first year is estimated at 61%. The second year ROI is estimated to be 182% (initial projected capital and operating requirements is removed). This estimate clarifies how the new upgrade set up of the network in Gambi Hospital will improve revenue and productivity.

## VII. IMPLEMENTATION PLAN

After all details are finalized and upgrade design strategy complete, the implementation of the network upgrade will transpire with minimal or no downtime within Gambi. As part of our implementation plan, an initial network test will occur. This will be done during off-hours to minimize possible problems; however, the final test will be done during normal business hours to completely evaluate the network upgrade performance. The following items below will be completely under evaluation:

- Verify the design upgrade meets key business and technical goals.

- Validate LAN and WAN technology and device selections.

- Verify the service provider provides the agreed-upon service.

- Identify any bottlenecks or connectivity problems.

- Test the redundancy of the network.
- Analyze the effects on performance during network link failures.
- Determine the optimization techniques to meet performance and other technical goals.
- Analyze the effects on performance while the upgrade of network links or devices is under construction ("what-if analyses").
- Identify any risks that can impede implementation and determine the plans for contingencies.

The following are considerations to experience while a "live" test is under implementation:

- Warn users in advance about the timing of tests so they can expect some performance degradation, but ask the users to work as they typically do to avoid invalidating the test by abnormal behavior. Moreover, have the users report any issues that arise during the live test.
- Warn network administrators and other designers in advance to avoid the possibility that they could be running tests at the same time.
- Warn network managers in advance, so they are not confused by unexpected alarms on network-management consoles, and so they can account for test traffic when documenting load and availability statistics.
- If possible, we will run multiple, short (less than 2-minute) tests to minimize user impact and lessen the effects on baseline measurements.
- Monitor test results and discontinue them when test objectives are met, or the production network is severely impacted or fails.

Furthermore, we will provide a follow-up after implementation. We will follow up every day until all issues have been resolved and the design/upgrade has been fully completed.

# VII. APPENDICES

## TEAM CONTRACT

**Code of Conduct: As a project team, we will:**

- Work proactively, anticipating potential problems and working to prevent them.
- Keep other team members informed of information related to the project.
- Focus on what is best for the project team

**Participation: We will:**

- Be honest and open during all project activities
- Encourage diversity in team work
- Provide the opportunity for equal participation.
- Be open to new approaches and consider new ideas or assumptions.
- Let the project manager (Getasew) know well in advance if a team member has to miss a meeting or may have trouble meeting for a given task.

**Communication: We Will:**

- Decide as a team on the best way to communicate.
- Work together to create the project schedule.
- Present ideas clearly and concisely.
- Keep discussions on track.

**Problem Solving: We Will:**

- Encourage everyone to participate problem solving problems.
- Only use constructive criticism and focus on solving problems, not blaming people.
- Strive to build on each other's ideas

**Meeting Guidelines: We Will:**

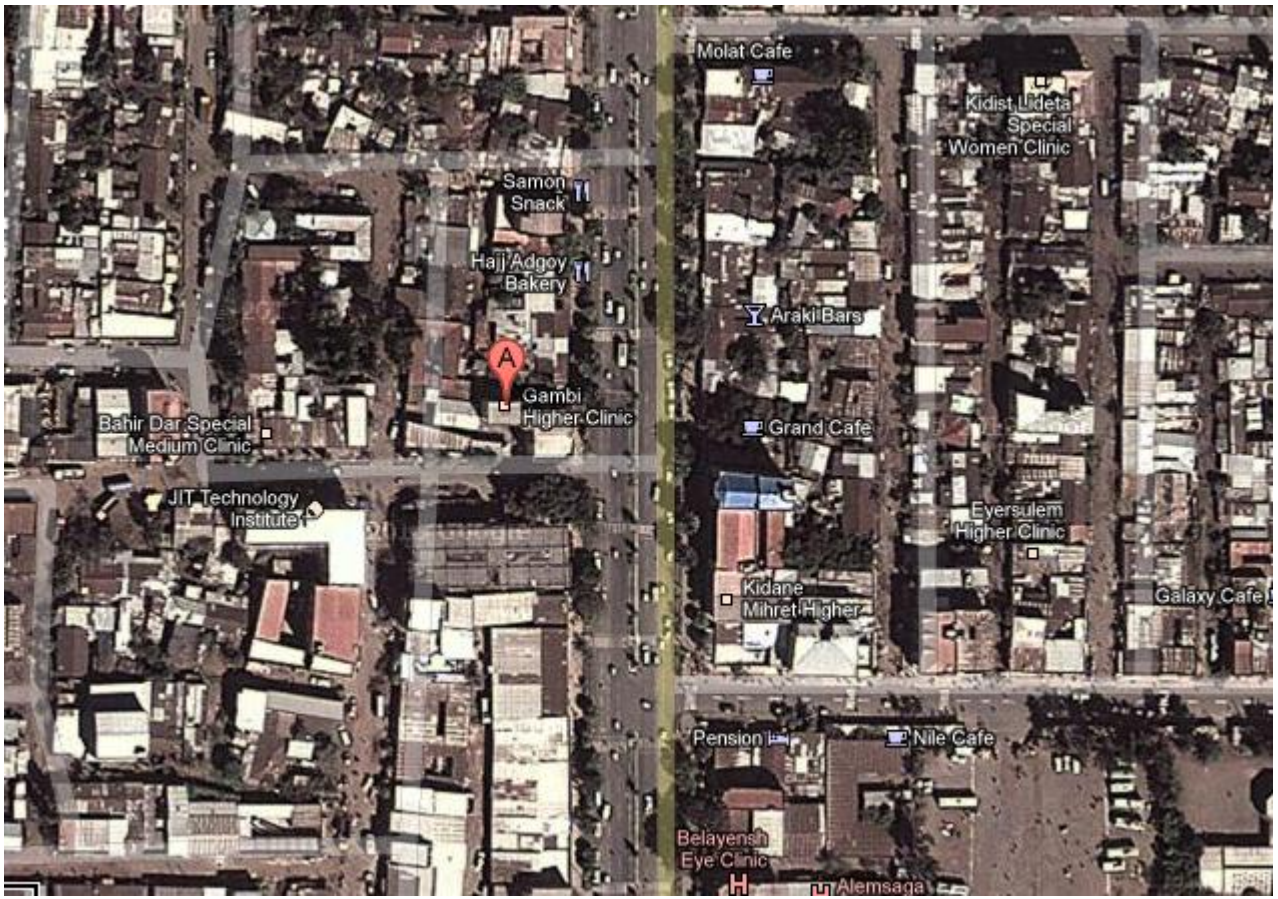
- Plan to have a meeting every day at 12 o'clock at Ethiopian local time before submission of the Part Project.

**Signatures:**

## IX. REFERENCES


- Google
- Google Map
- Amazon
- Ebay


THE SATELLITE IMAGE OF GAMBI HOSPITAL



# THE END

THANKS FOR READING