Happy Health Systems

Voice and Data Infrastructure

2014

[David Magnaterra]

12/23/2014

Table of Contents

[Version Control 2](#_Toc318118926)

[Executive Summary 3](#_Toc318118926)

[Project Scope 3](#_Toc318118926)

[Stakeholders 7](#_Toc318118926)

1.1 [Network Topology 8](#_Toc318118926)

[IP Addressing and Routing Architecture 9](#_Toc318118926)

[1.2 Research Facility 10](#_Toc318118926)

[2.1 Hardware 11](#_Toc318118926)

[Long Distance Plan 11](#_Toc318118926)

[1.3 Long Distance Topology 1](#_Toc318118926)2

[1.4 Network Architecture 1](#_Toc318118926)3

[1.5 MAN Infrastructure 1](#_Toc318118926)4

[1.6 Risk Matrix 1](#_Toc318118926)5

[Risk Mitigation 15](#_Toc318118926)

[1.7 New Bandwidth Output 1](#_Toc318118926)7

[Maintenance 17](#_Toc318118926)

[References 19](#_Toc318118926)

**Version**

|  |  |  |
| --- | --- | --- |
| Version Number | Deployment Model | Date |
| 5.0 | **05A1** | **12/23/2014** |

# 

# Executive Summary

A need has become apparent for centralized data management and consolidation of LAN line communications. The goal is to create standardization across the network thus linking the sites and creating a scalable environment with low overhead. Voice over IP systems will apply integration of telecommunications over the Internet. Session initiation protocol (SIP) will manage multiple media types thus generating a scalable architecture for VOIP, video conferencing, media streaming, and instant messaging. Email exchange servers will integrate with the telecommunication architecture by providing access to missed calls and voice mail.

The network circuits will be provided by Time Warner. Class A IP addressing will provide the scope the business requires. Various VLANs will identify the site of the Layer 3 switches; this type of switch will enable routing protocols for packet security. WAPS (wireless access points) will be installed at all sites for ease of access and patient contentment. The WAPs will have three channels, one for patient access, one for domain access, and one for VOIP phones.

**Project Scope**

**Project summary and rationalization**

Larry Macon, CFO of Happy Health Systems, called for the telecommunication alignment project to support effective Internet based communication across the sites. Happy Health Systems is a network of hospitals and clinics located in southwest Ohio. We pride ourselves on accurate diagnosis derived by high technological means. A demand for secure confidential information access and sharing generates a new need for a topology change. Secure communication between sites will ensure compliance and data integrity. Patient information will inherit HIPPA compliant securities. The projected budgetary responsibility is 1.5.million dollars. Standardization strategically increases productivity and enhances patient care. The estimated annual support budget is $250,000 which will be drawn from the operational budget. Support is projected to become proficient for the IT systems served to the end users. The current LAN telecommunication is outdated and lacks redundancy. The Fax systems rely upon modem connectivity hence generating a signal point of failure. The concept is to deploy Internet based functionality therefore employing the redundancy and protocols associated to routing packets. Security will be increased by creating VLANs for the VOIP systems.

**Project Overview**

The undertaking of this project derives from a legacy support parameters and security constraints. The annual cost of legacy systems exceeds $300,000. Maintaining LAN lines will discontinue upon cabling and layer 3 switch alignment.

**Project Charter**

* Data traffic testing will begin with the current servers to gauge connectivity constraints.
* Volume estimates will be compiled and analyzed.
* Security will be tested.
* Additional RJ45 wall panels will be installed
* Cable will be run to the new switches.
* An additional WAP channel will be available for wireless VOIP connectivity.
* CISCO wireless and wired phones will be ordered.
* Session initiation protocol will consent the various voice medias.
* Firewall filtering will secure external access to the network.
* Session initiation protocol proxy will manage the firewall.
* Exchange will integrate with voice transfers.
* Microsoft Lync will integrate voice and conferences functionality.

**The scope of this project includes and excludes the following items:**

Included

* Format: An Internet portal (Citrix) will provide the remote access point.
* Users: Will be provided Active Directory accounts.
* Users: Will be provided Exchange access.
* Users: Will be provided MS Lyncs access.
* Users: Will be provided VOIP phones gauged upon job requirements.
* Update messages: Information regarding updates will be conveyed by email and the home page of the web portal.
* Security: Redundant Cisco F5 routers will manage firewall and SIP communication.
* Routing: Redundant Cisco F5 routers will load balance the telecommunications.
* Internet: Redundancy for the switches will be provided.
* Access: VOIP lines will be available 24 hours, 7 days a week.
* Support: The network support center will be available 24 hours, 7 days a week.
* Support: Each system will have an on-call administrator available 24 hours, 7 days a week.

Excluded

* External: VOIP phone range will be limited to site resources.
* Internet: Access will be granted by MAC addressing
* Email: The email usage will be internal Microsoft Exchange.
* Instructions: Instructions will be defined by the facility.

**Approach**

Sequential Processes

* Cable lines will be connected to the new wall panels
* Network closets will be assessed for power.
* Dedicated DHCP servers will be deployed.
* DHCP reservations will be created.
* Switches will be assessed.
* Legacy Layer 2 switches will be replaced.
* Wireless access points will have dedicated channels for wireless nodes, linked by MAC address.
* Connectivity validation will begin.
* Site deployment will start at the clinics.
* Upon success, the final cut-over date will be determined for the hospitals, research facility, and Physician’s office.
* Network naming schemas and architectures will be standardized.
* Wired phones will connect to the walls.
* LAN lines will be decommissioned.
* Email and Lync integration will be pushed out over the network.

Cohesive planning and strategic implementation will enable a prudent outcome.

* **Strengths:** Critical thinking and well trained professionals will provide positive outcomes.
* **Weaknesses** The network bandwidth metrics will need to be analyzed or modified. Administration of systems will be transformed.
* **Opportunities** Aligning the network resources will enable a scalable environment with low overhead. The upgrades and hardware administration will be managed by centralized support hence minimizing system diversification.
* **Threats** The legacy systems may not be able to be fully tested parallel to the go-live.
* **Risks** Network failure could stop access. The redundancy will need to be assessed system by system.
* **Constraints** The budget will not stretch to fund unforeseen variables. The team is limited to ten members. The timeline is smaller than other site’s metrics.
* **Assumptions** The appropriate tools are available. Each team member is competent in their role. The risk management has been analyzed accordingly. The ROI will exceed the initial investment.

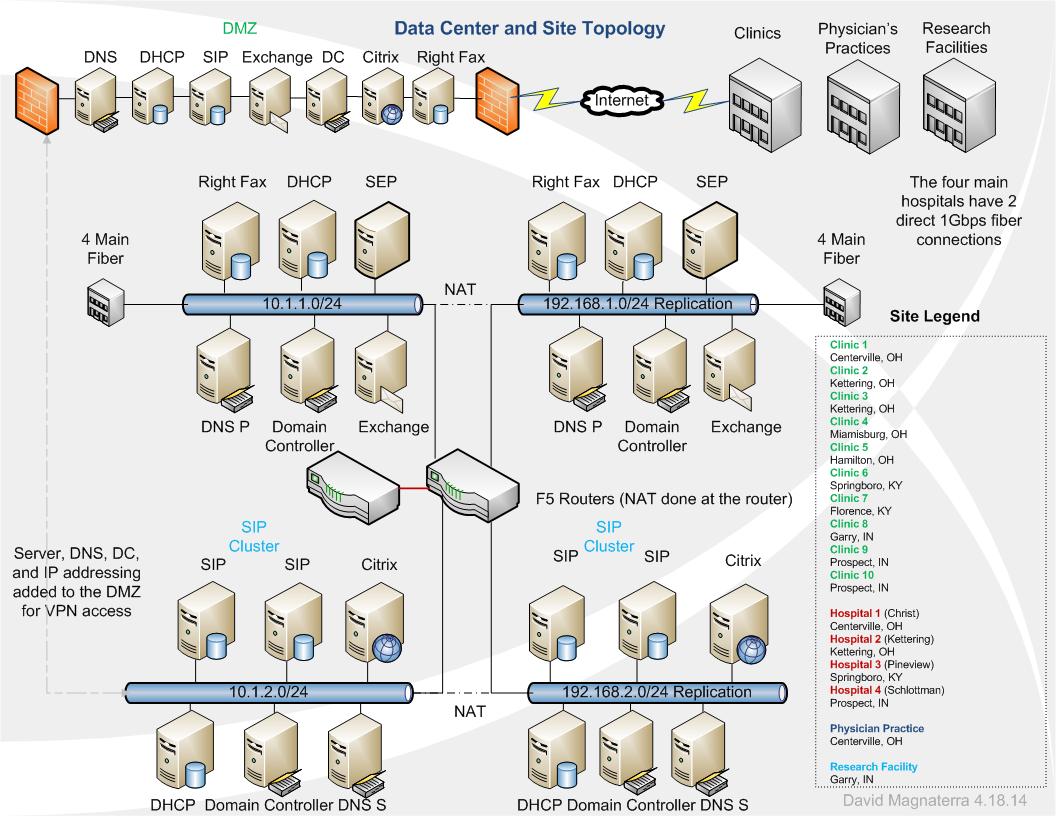
**Stakeholders**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Management Type** | **Role** | **Project Phase** |
| Larry Macon | Capital Budget Allocation | CFO | Phase 1, 2 |
| Dan Johnson | Network Engineering | Manager | Phase 1, 2, 3, 4, 5 |
| Bob Smith | Infrastructure | Manager | Phase 1, 2, 3, 4, 5 |
| Lisa Connell | Clinical Informatics | User Liaison | Phase 4, 5 |
| David Magnaterra | Infrastructure | Analyst | Phase 2, 3, 4, 5 |
| Carl Canter | Infrastructure | Analyst | Phase 2, 3, 4, 5 |
| Durral Kisone | Infrastructure | Network Administrator | Phase 2, 3, 4, 5 |
| Shane Wackson | Network Engineering | Engineer | Phase 2, 3, 4, 5 |
| Justin Walken | Network Engineering | Engineer | Phase 2, 3, 4, 5 |
| Greg Courtney | Contractor | Cabling | Phase 2, 3, 4, 5 |
| Dan Acape | Contractor | Wall Drops | Phase 2, 3, 4, 5 |

The five phase process allows the key stakeholders to start their procedures and overlap for validation. Upon validation the next phase will be underway. Various roles deliver perspective to the multiple layers of the project. The contractors will execute the physical layers regarding cable and wall panel connections across the network. DHCP reservations will be configured by the MAC address thus ensuring ownership of the VOIP address. DHCP servers will incorporate relay agents working between a split scopes. A class A IP address range will be incorporate the facilities VOIP clients. The following address scopes have been created for the sites:

|  |  |  |
| --- | --- | --- |
| Site | Scope Subnet | Lease Period |
| Christ | 10.1.3.1 - 10.1.10.254 | **Static –RES** |
| Kettering | 10.1.11.1 - 10.1.18.254 | **Static –RES** |
| Pineview | 10.1.19.1 - 10.1.26.254 | **Static –RES** |
| Schlottman | 10.1.27.1 - 10.1.34.254 | **Static –RES** |
| Clinics | 10.1.35.1 - 10.1.36.254 | **Static –RES** |
| Physicians | 10.1.37.1 - 10.1.39.50 | **Static –RES** |
| Research | 10.1.39.51 - 10.1.39.90 | **Static –RES** |

The IP scopes concern the toe VOIP phones and work directly with the architecture resources. The SIP architecture will be a cluster environment managed by a virtual IP address. A failover feature will be installed on both servers. A 3PAR SAN will be attached. A quorum, DTS, and data volume will be committed on separate SAN logical unit numbers (LUNS). SIP will be integrated into the Microsoft Office components to facilitate VOIP, Instant Messaging, and dynamic multimedia interactivity. SIP will enable the users to utilize soft phone integrated into smart phones and mobile devices. The SIP integration will negate cost per call and allow use of standard VOIP phones as well. The diagram below illustrates the topology.  
**1.1 Network Topology**



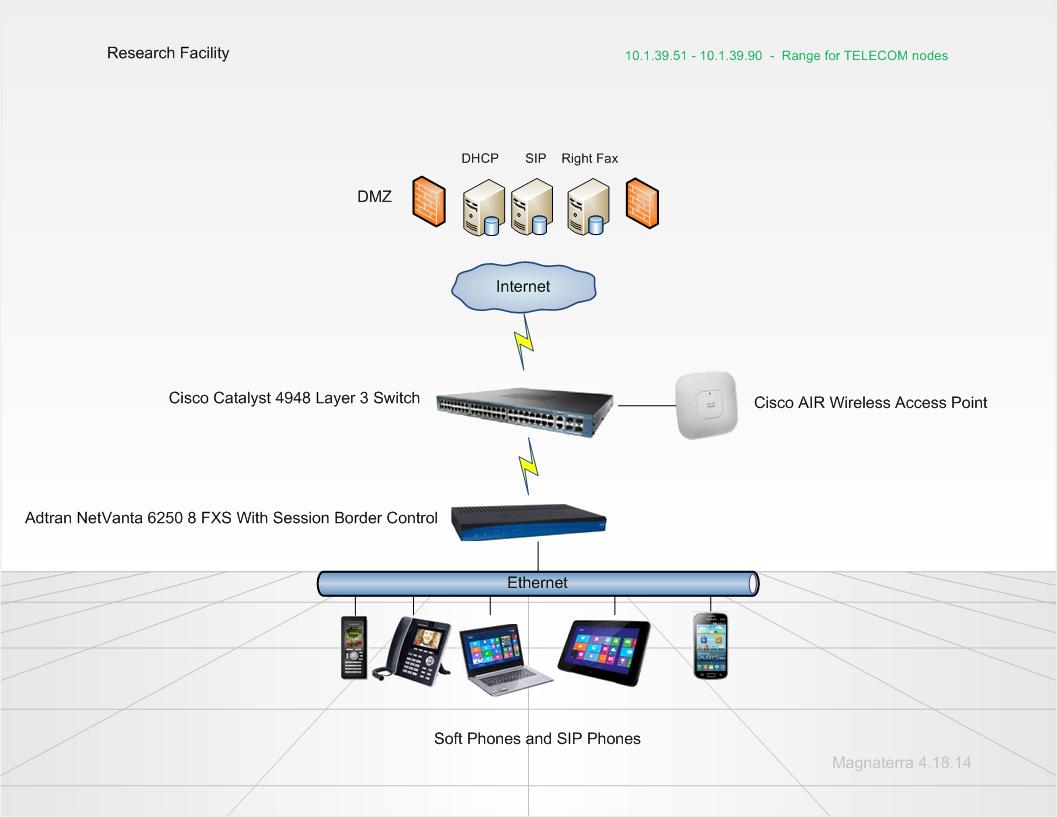
**IP Addressing and Routing Architecture**

IP addressing will comprise of a Class A scope and a Class C scope. The translation between the two networks will be done by NAT processes on the router. Replication between environments will take place across networks; this will ensure redundancy and enable separate physical networks thus safeguarding the network redundancy.

Clinics, Physician’s practices, and the research facility will apply VPN tunneling for access to the DMZ (demilitarized zone). The DMZ will incorporate DNS, DHCP, SIP, MS Exchange, and Citrix. This will enable secure access to the network applications and telecom resources, the Class A private network will NAT for communication to the public networks. The Servers will be added to the DMZ with IIS web hosting and account management. The four main hospitals will have two 1 Gbps fiber connections to the datacenter. One connection to the Class A network and one connection to the Class C network therefore providing redundancy. The F5 router will load balance between the two networks dependent upon bandwidth usage and peak hours. Adding the F5 router/load balancer will provide a dynamic process for throughput management. The projected usage will baseline at 35% with the new measures implemented.

LAN bases phones and faxing will be liquidated. SIP technology will replace the legacy architecture and integrate into network infrastructure resources. CISCO Catalyst L3 switches will be the backbone for the new architecture. The CISCO switches communicate with the DHCP servers and apply reservations. Adtran NetNanta 6250 session border controllers will communicate with the SIP servers and manage telecommunications. The physicians practice, clinics, and research facility will tunnel to the DMZ. The DMZ will provides the needed network resources for all communications. Right Fax will enable faxing to become digital. Ethernet protocols manage the throughput for all types of communication across the network therefore standardizing the infrastructure components across the wide area network (WAN). Diagram 1.2 projects the flow analysis for the research facility.

**1.2 Research Facility Telecommunications**

****

Legacy phones and fax machines will no longer be needed for the new design. A fax can be scanned if it is a hard copy, email formats can transmit seamlessly over the Ethernet resources. The users can access telecommunication in four formats: SIP integrated cellular phones, SIP phones, PCs, and tablets. Multiple new layers of mobility will be generated thus providing ease of access of the end users. Hardware associated to the new model is exemplified below within table 2.1. The combination of the hardware allows external sites to interconnect with the main data center. Most network resources are contained within the data center. The data center has a sister disaster recovery site. The IP addressing is translated to a class C addressing model.

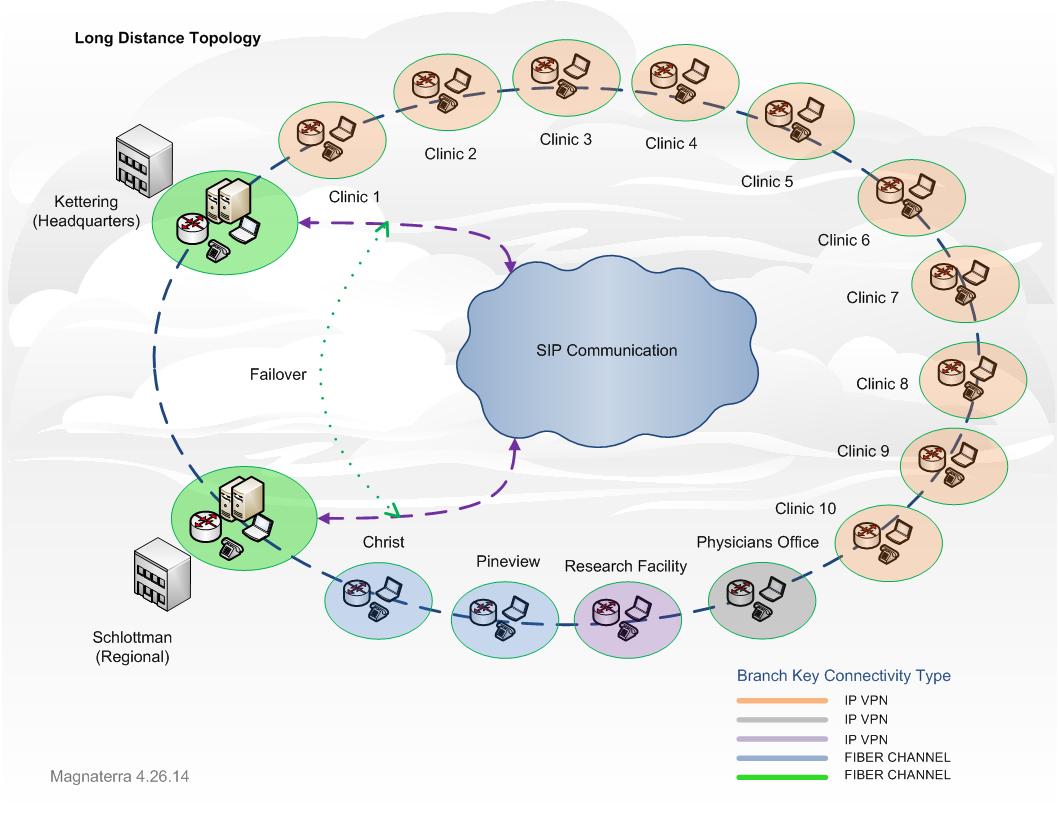
**2.1 Hardware**

|  |  |  |
| --- | --- | --- |
| Hardware Type | Model | Function |
| DHCP Server | HP DL 380 2U | IP Management |
| SIP Server | HP DL 380 2U | Telecom Management |
| Right Fax Server | HP DL 380 2U | Fax Management |
| Domain Controller | HP DL 380 2U | Network Management |
| Exchange Server | HP DL 380 2U | Mail Management |
| DNS Server | HP DL 380 2U | Name Resolution |
| SEP Server | HP DL 380 2U | Antivirus |
| CISCO L3 Switch | CISCO 4948 | VLAN Management |
| CICSO F5 Router | CISCO 3824 | Firewall, Load Balancing, NAT |
| Adtran NetVanta | Adtran 6250 8 FXS | Session Border Controller |
| SIP Phone | Grandstream GXV3140 | Dual Stack ‘Skype’ & ‘SIP’ |
| Wireless SIP Phone | Simply WiFi | Wireless VOIP |
| Wireless Access Point | CISCO AIR AP1142N-A-K9 | Wireless Access |

**Long Distance Plan**

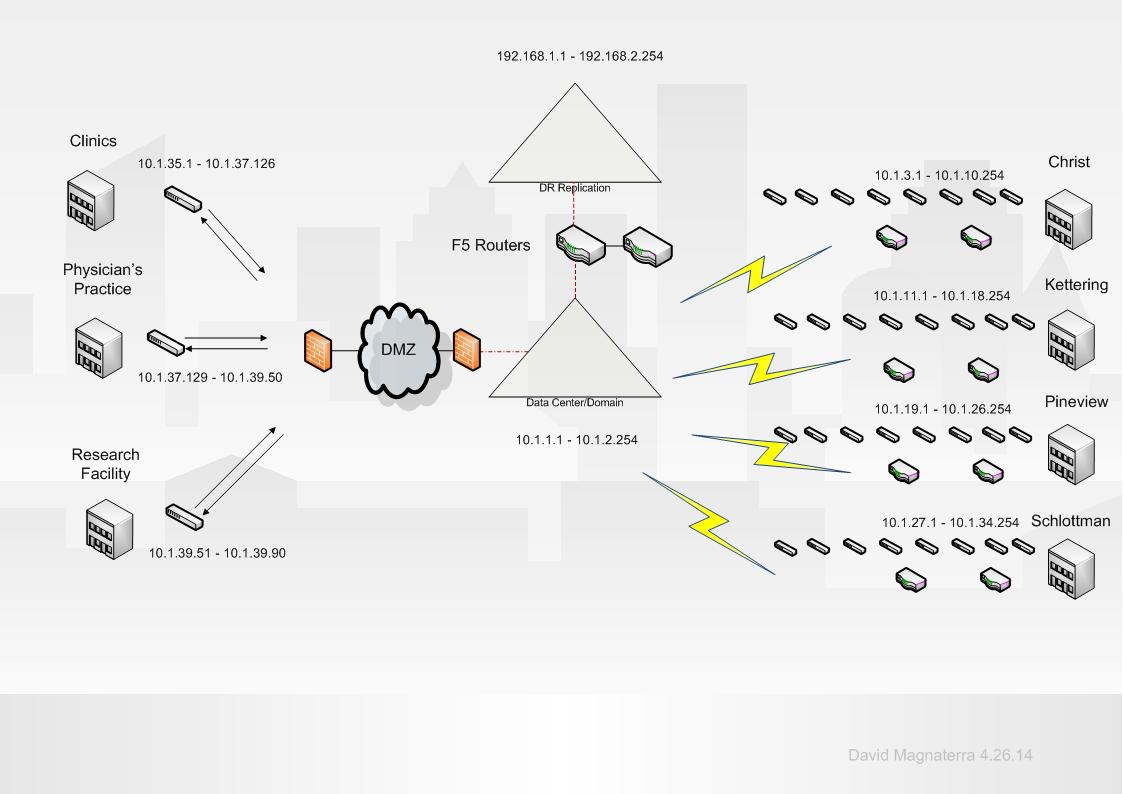
A centralized approach will streamline the long distance SIP environment. VOIP systems incorporate a layer of redundancy for the network by implementing a failover solution between the headquarters and the regional sites. If the connection to the SIP cluster fails or becomes degrades the architecture will dynamically failover to the regional datacenter thus negating downtime. Bandwidth will range between 1.5 Mbps to 1 Gbps for telecommunications. DHCP relay agents manage the IP addressing and VLAN structures by reservations tied to the device’s physical (MAC) address. An IP Multimedia Subsystem (IMS) architecture will provide the platform for the VOIP communications “both wireless and wire line operators soon realized that IMS could become a universal service architecture for the world’s communications services, and that IMS enabled operators to hatch new services by the dozen in a multi-vendor friendly network” (Grigonis, 2007). Diagram 1.3 illustrates the topology as well as the integrated components.

**1.3 Long Distance Topology**



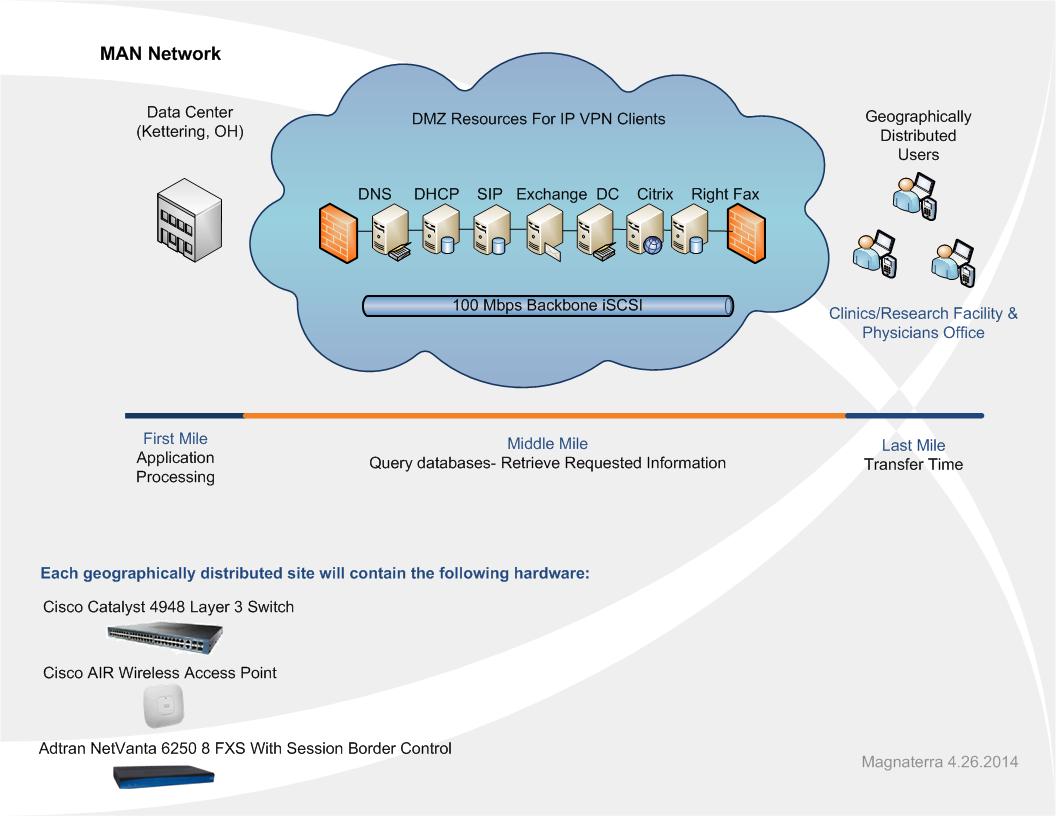
The core architecture comprises multiple layer three switches which deliver connectivity and allow separate VLANs for enhance security and bandwidth management. CAT 6 cable unites the wired clients with the infrastructure. All wireless access points will be powered by Ethernet hence subtracting the need for power resources. Communications leave the facilities by means of redundant routers located at each facility. The IP VPN clients utilize firewall crypto domains which permit tunneling and secure bidirectional communications “Modern processors make very quick work of the encryption/decryption process, and as long as you choose a fast VPN provider then you will find the impact minimal” (Zaborszky, 2013). Diagram 1.4 projects the infrastructure resources allocated for the TCP/IP communication.

**1.4 Network Architecture**

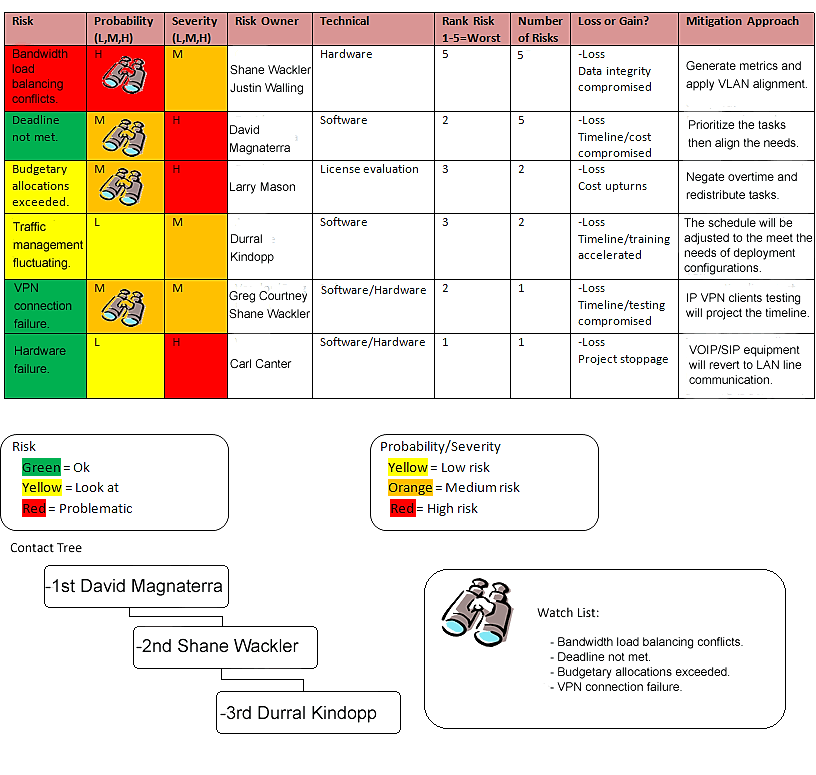


HHS middle mile network encompasses two functional layers. The first layer is access to network resources and application by publically addressing IIS (http) applications for external use. Each server in the DMZ has access to a 1 Gbps connection from the datacenter backbone “This takes enormous amounts of bandwidth, which refers to the amount of data that can be transferred from one point to another in a given amount of time” (Gaiser, 2013). The second layer comprises of bandwidth allocation for telecommunication. Access to the SIP cluster and DHCP servers is provided at a rate of 100 Mbps for all geographical distributed users. Only main hospitals are provided dual 1 Gbps fiber lines. Other facilities are utilizing the MAN infrastructure hosted by the data center in Kettering, OH. Diagram 1.5 displays the MAN infrastructure and the flow analysis of the mile movement. The 100 Mbps pipe projects the dedicated circuits available at each facility moreover each facility has their own iSCSI 100 Mbps pipe. The iSCSI pipe is separate from the DMZ fiber connection. Cabling within the GDUs will include RJ45 twisted pair CAT 6. Wall panels are punched with a set of two ports per panel. Resources in the DMZ utilize a shared redundant 7 Gbps fiber channel connection. The two channels are on separate virtual switches and provide a fail over as well as high availability. Routing protocols include RIPv2 and OSPF.

**1.5 MAN Infrastructure**



**1.6 Risk Matrix**

****

**Risk Mitigation**

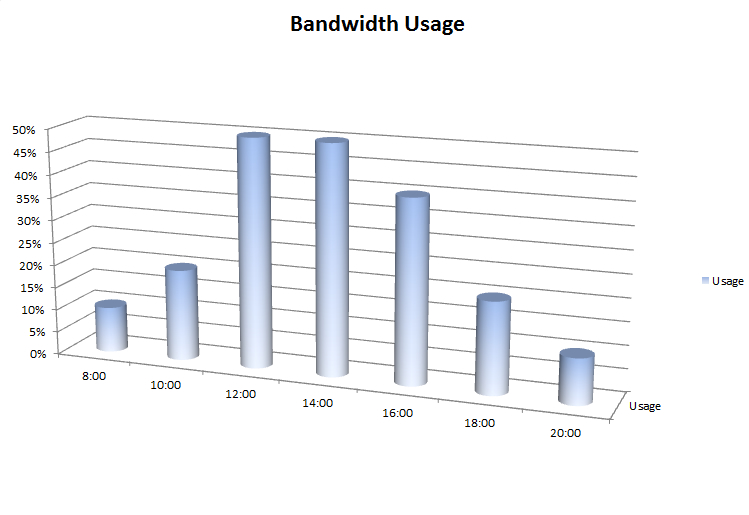
Risks associated to the VOIP deployment consist of multiple constraints. Security for traffic management must be managed effectively; moving to an IP infrastructure can transport new security risks due to the technology. Packets can be seized thus compromising the voice communication. TCP/IP technologies contest against sniffer devices which capture the data packets “these included attack by the widely available freeware known as Vomit, which can capture packets of voice data from converged voice and data networks, allowing hackers to listen to private conversations” (Savvas, 2004).Employing CISCO Call Manager for network encryption mitigates VOIP information from loss of integrity. Failover SIP clusters create the layer of redundancy as well as high availability functionality hence providing the uptime necessary to support the network availability needs.

Social media can become a threat for VOIP architectures by means of Phishing scams. Sensitive information can become compromised from spoofing the caller ID functionality of the VOIP systems “The phishing site is a replica of one of the telecommunication carrier’s sites and requests the victim’s log-in credentials and the last four digits of their Social Security number” (IVN , 2014). The caller generates an internal number which links to the user profile, information is requested and stolen. These utilities are available as free application for smart phones and can be loaded on servers that route information.

Security parameters will be applied to counter the sniffers and Phishing technologies. CISCO Call Manager 4.1 will be installed on the SIP clusters. The SIP devices are provided encryption; the server verifies the hashing with the SIP device. All SIP features are included comprising video and multiple line interactions. Skinny Client Control Protocol (SCCP) establishes the translation between the devices and the server software. Defense against Phishing begins on the Symantec End Point Servers “although significant improvements have been made in endpoint protection, NSS recommends organizations look for products that provide consistent protection and rapid response to socially engineered malware threats” (Kanowitz, 2014). Bitdefender is integrated into the End Point security thus shielding malware attacks therefore fortifying the architecture.

Quality of Service (QoS) for the new VOIP architecture and topology is managed by the CISCO Call Manager. Coverage management and services can be qualified by monitoring the network call quality and pursuing the most efficient levels of consistency for the network. Statistics are generated in the form of charts and diagrams. Servers within the data center and the disaster recovery site will utilize fiber channel connections at 10 Gbits/sec. The link between the main data center and the disaster recovery will comprise iSCSI connectivity at 1 Gbps. The sites will be geographically diversified. All the latest upgrades to the infrastructure have been generated for optimizes statistics. Throughput will be maximizes by use of fiber channel connectivity. Chart diagram 1.7 exemplifies the bandwidth usages with the new resources allocated.

**1.7 New Bandwidth Output**

****

**Maintenance**

Task management for processing, performance, users, and services will be generated by multiple Windows utilities. Task manager output will be analyzed periodically by network administrators assigned to the servers in their scope. Performance monitor data collectors with counter alert parameters will have thresholds which facilitate the resulting logs to be analyzed then cross referenced. Reliability monitor will generate historical records of changes linked to various events. Software installation, system failures, and hardware failures create a record which compile within the system stability index. The chart can be analyzed and provisions can be validated. These three utilities will become a part of each network administrator’s day to day tasks. SCOM alerts will send an email to the primary administrator on the system and log a ticket with the support center. Server updates and patched will be deployed by GPO .msi unattended installations.

**References**

Gaiser, Heidi. (2013). Boosting bandwidth: Middle-mile fiber-optic line will move more data at faster speeds. Retrieved April, 2014, from <http://www.dailyinterlake.com/business_and_finance/local_montana/article_58db650e-cb1c-11e2-b88d-001a4bcf887a.html>

Grigonis, Richard. (2007). SIP and IMS. Retrieved April, 2014, from <http://www.tmcnet.com/sip/0307/feature_articles_sip_and_ims.htm>

IVN. (2014). Phishing Attacks on Telecommunication Customers Resulting in Account Takeovers Continue. Retrieved May, 2014, from <http://www.imperialvalleynews.com/index.php/news/latest-news/8427-phishing-attacks-on-telecommunication-customers-resulting-in-account-takeovers-continue.html>

Kanowitz, Stephanie. (2014). What to look for in social malware defense. Retrieved May, 2014, from <http://gcn.com/articles/2014/05/01/socially-engineered-malware-protection.aspx>

M5 Networking. (2012). SIP…Not Just for VOIP Application. Retrieved April, 2014, from <http://m5networkingaz.com/sip-not-just-for-voip-application/>

Office SIP. (2014). Office SIP Server is freeware VoIP, SIP server for Windows. Retrieved April, 2014, from <http://www.officesip.com/>

Savvas, Antony. (2004). Roadshows warn of IT security risks in deploying VOIP. Retrieved May, 2014, from <http://www.computerweekly.com/news/2240059259/Roadshows-warn-of-IT-security-risks-in-deploying-VoIP>

Zaborszky, Pete. (2013). 5 Best VPNs for VOIP. Retrieved April, 2014, from <https://www.bestvpn.com/blog/5860/5-best-vpns-for-voip/>