Happy Health Systems

Network Infrastructure Alignment and Application Integrations

We will provide a centralize solutions for EMR and clinical applications

2014

[David Magnaterra]

12/23/2014

Table of Contents

[Version Control 2](#_Toc318118926)

[Executive Summary 3](#_Toc318118926)

[Project Scope 4](#_Toc318118926)

[Stakeholders 8](#_Toc318118926)

[Project Requirements 8](#_Toc318118926)

1.1 [Network EMR Topology w/Integration 12](#_Toc318118926)

1.2 [Philips iSite PACS Topology 13](#_Toc318118926)

[IP Addressing and Routing Architecture 13](#_Toc318118926)

1.3 [Network Topology 14](#_Toc318118926)

[Network Components 15](#_Toc318118926)

[Backup Plans 16](#_Toc318118926)

1.4 [Network Replication 17](#_Toc318118926)

[Security 20](#_Toc318118926)

[Backup Strategy 21](#_Toc318118926)

[UNIX and Linux File Systems 22](#_Toc318118926)

[UNIX – EPIC Deployment 22](#_Toc318118926)

[1.5 EPIC Deployment 23](#_Toc318118926)

[UNIX – Ensemble Deployment 24](#_Toc318118926)

[1.6 Ensemble Server – Server Architecture 24](#_Toc318118926)

[UNIX Design 25](#_Toc318118926)

[Windows – UNIX 25](#_Toc318118926)

[UNIX Implementation 26](#_Toc318118926)

[Operating Systems and Hardware 26](#_Toc318118926)

[1.7 Network Diagram – All Nodes 27](#_Toc318118926)

[Printing Infrastructure 30](#_Toc318118926)

[1.8 Centralized Printing 30](#_Toc318118926)

[1.9 Remote Faxing and Telecommunications – SIP Technology 31](#_Toc318118926)

[IP Design 32](#_Toc318118926)

[References 35](#_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 applications. The goal is to create standardization across the network thus linking the sites and creating a scalable environment with low overhead. The server operating systems and SQL will be promoted to 2008 R2 versions at the Enterprise platform. Licensures for Microsoft, AIX and Linux will be evaluated for the best enterprise solution.

Domain controllers will be accessible by the network nodes upon orientation and business need. Windows Server 2012 R2 will become the standard for all Microsoft server nodes. Enterprise licensing for Windows Server 2012 R2 enables wide use of the new operating system moreover promoting virtualization and integration of new server roles and features. Window Deployment Services will be the vessel for server OS upgrades. This deployment will be systematic addressing domain controls first then DNS, SEP, and DHCP servers. All other application servers will inherit the new versions of the server OS after a database backup. Upon database servers being upgraded, the tables will be indexed to ensure a clean transition.

User workstations will have the option to select between multiple domains upon Active Directory user and group assignment. A DMZ (demilitarized zone) will host various virtual server environments thus providing efficient patient care for Physician and clinics.

The network circuits will be provided by Time Warner. Class C 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 two channels, one for patient access and another for domain access.

Applications aligned with the standardized network infrastructure will enable seamless upgrades and administration. EPIC applications and derivatives, will liquidate many current applications for reporting. Secure access to the EMR and PACS will be delivered for effective and efficient patient care. Microsoft Office will be deployed to client nodes by Microsoft SCCM scripting. A report will be generated once the client nodes are joined to the domain. PeopleSoft ERP will be deployed from SCCM by group membership to the finance group. Once the user authenticates to the domain controller an unattended installation will be pushed to the user’s computer. Symantec security and Spybot Search and destroy will be encapsulated within the standard Windows 7 x64 image. SCCM imaging will occur by means of network PXE.

**Project Scope**

**Project summary and rationalization**

Larry Macon, CFO of Happy Health Systems, called for the network and application alignment project to support cost with the business needs. 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.

**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 database updates will discontinue upon vendor support constrictions.

**Project Charter**

* Data traffic testing will begin with the current servers to gauge connectivity constraints.
* Volume estimates will be compiled and analyzed.
* Modality entries will be added (PACS).
* Physical nodes will be clustered for redundancy.
* Virtual nodes will utilize vMotion for redundancy.
* High availability servers will be placed at our disaster recovery site for another layer of redundancy.
* Security will be tested.
* Work flow changes will be defined for the department.
* Down time processes will be defined.

**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 database access outside of LDAP (iSite, Cerner)
* Users: Will be provided EPIC securities.
* Users: A zero footprint viewer will be integrated into EPIC for access to PACS imaging.
* Update messages: Information regarding updates will be conveyed by email and the home page of the web portal.
* Infrastructure: Server remote upgrades.
* Infrastructure: Workstation remote upgrades.
* Infrastructure: Manual workstation hardware upgrade.
* Infrastructure: Manual workstation software upgrade.
* Infrastructure: Virtual host servers built.
* Infrastructure: VMWare vSphere 5.5 integration
* Infrastructure: Windows 2012 Hyper Visor domain controller cloning.
* Security: All data pulled/pushed from the DMZ will be encrypted with 256 bit SSL.
* Search tools: The end user is provided searching and history features within EPIC, Cerner, and iSite.
* Internet: Access to the web hosted applications must comply with IE8 and IE9 browsers.
* Access: The web portal 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

* Promotion: The web portal will not be promoted to other hospitals.
* Internet: Content and color schemes are not amendable.
* Email: The email usage will be internal Microsoft Exchange.
* Instructions: Instructions will be defined by the facility.

**Approach**

Sequential Processes

* Servers and clients will receive remote OS deployment
* Client workstations will be upgraded and imaged.
* A bi-directional tunnel will be established between clinic sites and servers.
* The physical servers will be clustered with a HA server (high availability) at a disaster recovery site.
* The virtual servers will be redundant by vMotion with a HA server (high availability) at a disaster recovery site.
* Data will be migrations will be completed after hours.
* Databases will be validated.
* The biomedical team will create new entries on all modalities (Radiology PACS) in the network.
* Dry run testing will begin.
* Upon success, the final go-live date will be determined.
* Network naming schemas and architectures will be standardized.

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 applications and 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. Patient information will inherit added security therefore enhancing patient care.
* **Threats** The legacy systems may not be able to be fully tested parallel to the go-live. Workstations and print servers will be exchanged during 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 six 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 | Applications | Manager | Phase 1, 2, 3, 4, 5 |
| Bob Smith | Infrastructure | Manager | Phase 1, 2, 3, 4, 5 |
| Lisa Connell | Clinical Informatics | Physician Liaison | Phase 4, 5 |
| David Magnaterra | Clinical Applications | Trainer | Phase 3, 4, 5 |
| Carl Canter | Infrastructure | Analyst | Phase 2, 3, 4, 5 |
| Durral Kisone | Infrastructure | Workstation Lead | Phase 2, 3, 4, 5 |
| Shane Wackson | Infrastructure | NOS | Phase 2, 3, 4, 5 |
| Justin Walken | Infrastructure | Network Engineering | Phase 2, 3, 4, 5 |
| Greg Courtney | Application | Analyst | Phase 2, 3, 4, 5 |
| Dan Acape | Application | Analyst | Phase 2, 3, 4, 5 |
| Larry Kiser | Application | Analyst | Phase 2, 3, 4, 5 |

**Project Requirements**

**Process**

The budgetary means equate to 55 million dollars capitol allocated for the project. The organization strategies include deployment by October 18, 2014. This is not a tentative date; the fiscal year must prove the EPCI EMR functions due to federal compensation and kickbacks. These kickbacks will negate cost thus enabling the new strategies to take form.

**Organizational Assessment**

Organizational constraints consist of data migration from the legacy Novell infrastructure. A single domain and forest will be executed for the new topology. Email migration from Novell GroupWise to Microsoft Exchange will occur and data validation will transpire as well. All DICOM data from the current databases will migrate to the Philips iSite IBM SAN. VCEs (virtual modules) will incorporate the structured DICOM datasets. A Vendor Neutral Archive (VNA) deployment will allow ownership, cost leverage, and DR capabilities for the proprietary iSyntex (compressed DICOM type) data. ACUO temporal routers will drop a copy on the Philips iSite SAN and the VNA thus providing the preceding capabilities illustrated in diagram 1.2. DNS and DHCP servers will be deployed at the four main facilities. A demilitarized zone (DMZ) will be constructed for remote access and public addressing. Lab datasets will migrate into the Cerner Pathnet Oracle database. Validation will occur upon migration. EPIC 2012 will become the EMR. All data from the prior Carecast EMR will be migrated into the EPIC environment. HL7 feeds will connect both Pathnet and iSite with EPIC illustrated in diagram 1.1.

Infrastructure assets range in operating systems. The current architecture consists of Windows Server 2000, 2003, and 2008. Windows Deployment Services will assist in server upgrades. Philips iSite and EPIC incorporate vendor owned hardware, these system comprise Windows platforms and UNIX architectures. These operating systems will not be a part of the deployment scope as they are supported by the vendor. Client workstations need hardware upgrades to facilitate the applications and the 64 bit upgrade. Moving from an x86 to an x64 platform allows larger use of memory for the workstations. Memory will be upgraded to expand performance. Virtualization of application server will occur for Cerner Pathnet and PeopleSoft. The two systems will become redundant with VMWare vMotion technologies. A HP 3PAR SAN will be attached to all virtual nodes thus providing redundant storage with fiber channel bandwidth approaching 8 Gbps.

**Requirement Management (multi-tier)**

**Network Administration**

* Domain configurations consist of one domain with four domain controller one per hospital. Active Directory will entail user and group administration, DHCP, static IP scopes, site sub netting, DNS replication, and DFS sharing. Group policies will be deployed by SCCM as well as all unattended installer packages. (10/21/2014)
* Remote operating system deployment begins with servers which incorporate Windows Server 2008 or lower. Windows Deployment Services will deliver remote OS upgrades for servers and clients. Client must meet the following specifications to be in the WDS scope: dual core processor, 6 GB of RAM. Any client outside of the scope will be manually imaged by SCCM PXE distribution. (10/27/2014)
* Security will be managed by IPSEC technologies and SSL encryption. All non-LDAP databases will align security measures with standardized protocols. Users, network administrator, systems analyst, and domain administrator securities will be defined. Groups, organizational units and all other containers will be configured for centralize policy management. (11/2/2014)
* Email accounts migration into the Exchange platform will begin. Inbox storage allocation will be standardized. (11/10/2014)
* A parallel network will exist for testing; the current Novell network will coexist with the new Microsoft Server 2012 R2 Active Directory driven environment. After bi-directional connectivity is established, users and groups will be migrated. (11/10/2014)
* Network modifications will begin. The current existing routing and switch environment will be upgraded to a Layer 3 switch environment with F5 routing. (11/10/2014)
* Client Workstations will have to meet a specification of Intel E7600 2 core processors, HP 6000 pro workstations, 6 GB of RAM, Windows 7 x64, and IE 8 browser. (12/1/2014)
* Radiology Diagnostic Workstations will have to meet a specification of Intel Xeon E5620 4 core processors, HP Z800 workstations, 12 GB of RAM, Windows 7 x64, and IE 8 browser. Video will meet a specification of a Barco MXRT-7400 graphic card and a minimum of one Barco Coronis Fusion 6 MP MDCC-6130 monitor coupled with a minimum of one HP LA2405wg monitor. The standards will double the video specifications. (12/5/2014)
* Cutover and deployment will begin after business hours on a Friday. (12/18/2014)

Threshold -----------------------------------------------------------------------------------------------------------------------------

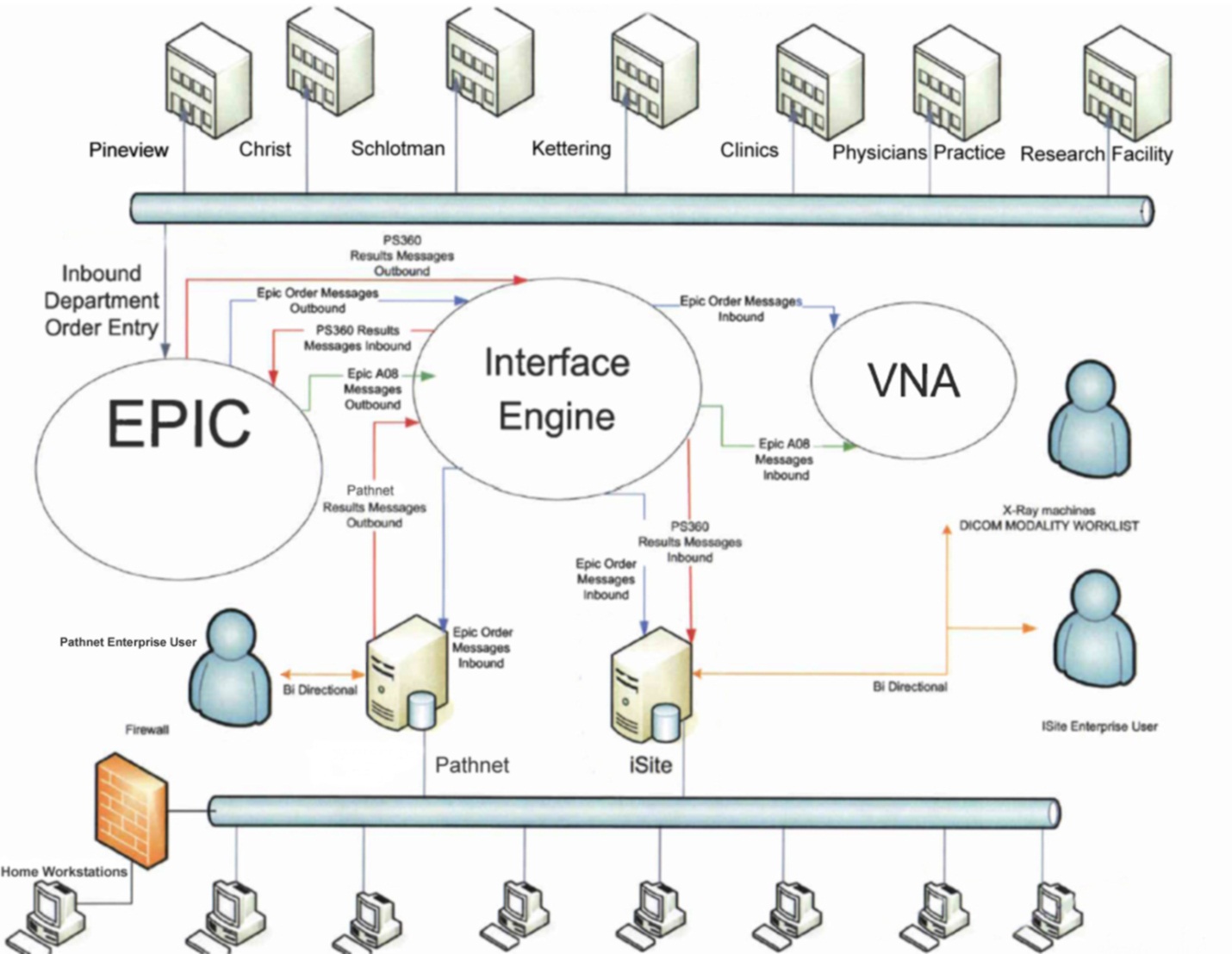
**Application Administration**

* EMR (EPIC) build will be compiled in the CER (test) environment. The design goals consist of HL7 interfaces, SUBI PACS integration, HIS management, Lab result GUIs (by HL7 messages), and PACS results GUIs (by HL7 messages). The integration engine delivering the HL7 messages will be an Ensemble integration engine. This will be the vessel for results and reporting. Groups and users will be linked to Active Directory by LDAP. Administration will be handled by the System Administrators. (12/1/2014)
* Philip iSite 3.6.150 will be the PACS. The archiving will have two DICOM stores. One store will be the SAN provided by Philips, the other store will be an Atmos VNA (vendor neutral archive) solution. The VNA will enable us to gauge the price per stored study with the vendor. Having and owning the information will provide variable leverage with the vendor. BSC (business continuity servers) will be placed at every main hospital for backup access to images these servers will be virtual. Temporal DICOM routers will live at every site for routing images to both iSite and the VNA. Groups and users will be linked to Active Directory by LDAP. Administration will be handled by the System Administrators. Results and reports will be interfaced by the Ensemble integration engine then made available to nurses and physicians. (12/10/2014)
* Cerner Pathnet will track dose and biopsy information. Groups and users will be linked to Active Directory by LDAP. Administration will be handled by the System Administrators. Cerner Pathnet will consist of two host servers carved into virtual servers. The HP 3PAR SAN will be attached to the nodes for redundant storage. Results and reports will be interfaced by the Ensemble integration engine then made available to nurses and physicians. (12/14/2014)
* PeopleSoft (virtual) will be queued to push by SCCM upon user authentication and user group membership. (12/14/2014)
* Workstations will be imaged and tested. The preconfigured systems will be deployed by a team of workstation administrators. (12/14/2014)
* Microsoft office will be deployed to all client workstations by SCCM. An inventory monitor script will run to monitor usage of the MS Office. If the product is not used in 90 days the suite will be uninstalled (a network pull by SCCM) to save enterprise licenses.(systematic upon 12/14/2014 WS deployment)

**Support**

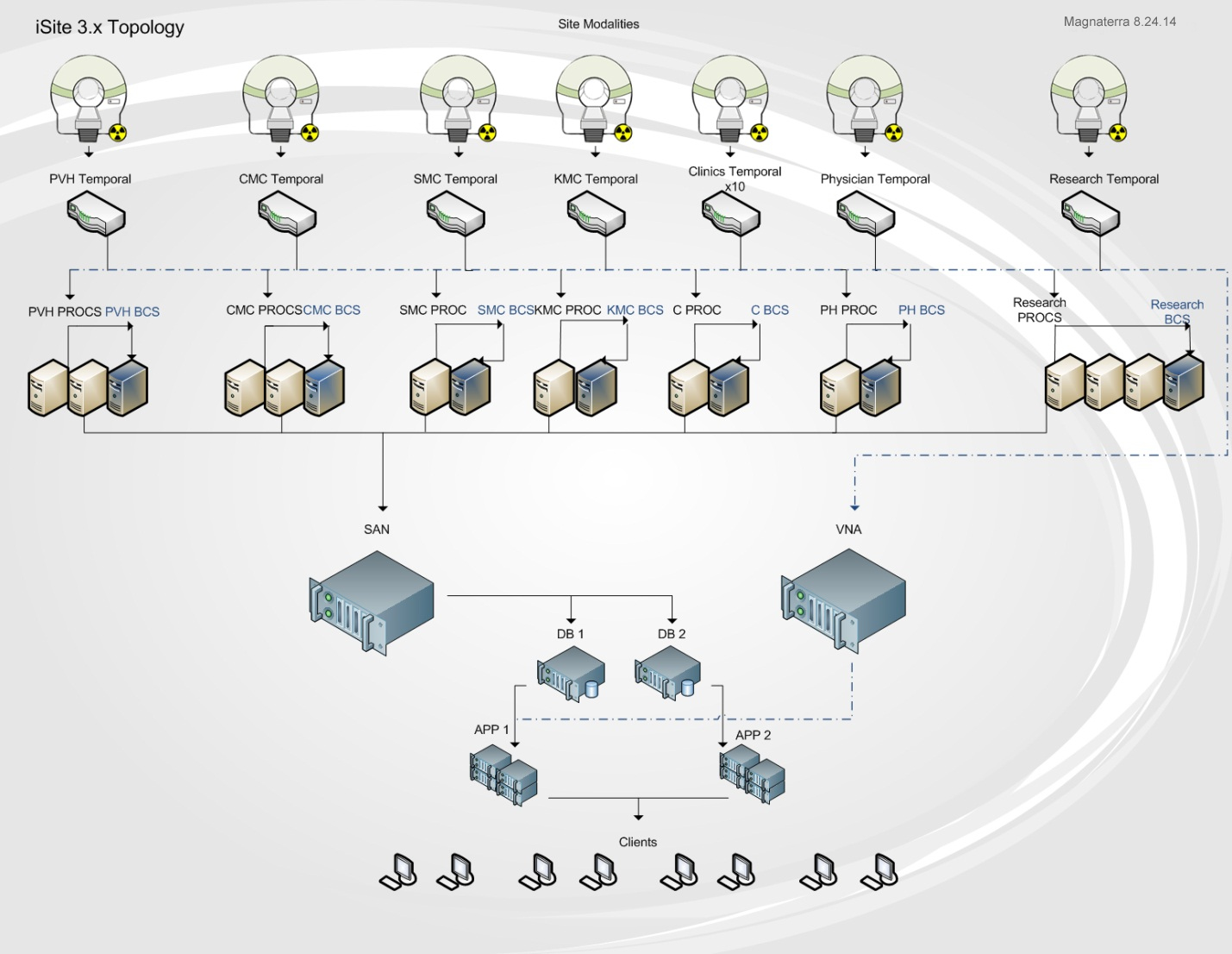
* Customer support models will be analyzed. The goal is to have application support teams, network engineering support, and network administration support 24 hours a day 365 days a year. (12/5/2014)
* Training will begin in a classroom atmosphere. Surveys will be delivered to the users. Additional onsite training will be available based on testing and feedback. (12/14//2014)

**1.1 Network EMR Topology w/Integration**

****

# Radiologist will have preconfigured workstations sent to their homes. Access will connect by token and Cisco Any Connect interfacing. EPIC will not be integrated on these workstations. The Radiologist will need to access EPIC by token through the Citrix SAP. EPIC inherits many security updates thus negating VPN functionality due to constraints. These users will be in the standard VPN and SAP groups; iSite Enterprise and EPIC will also be advertised in the SAP for remote access.

**1.2 Philips iSite PACS Topology**

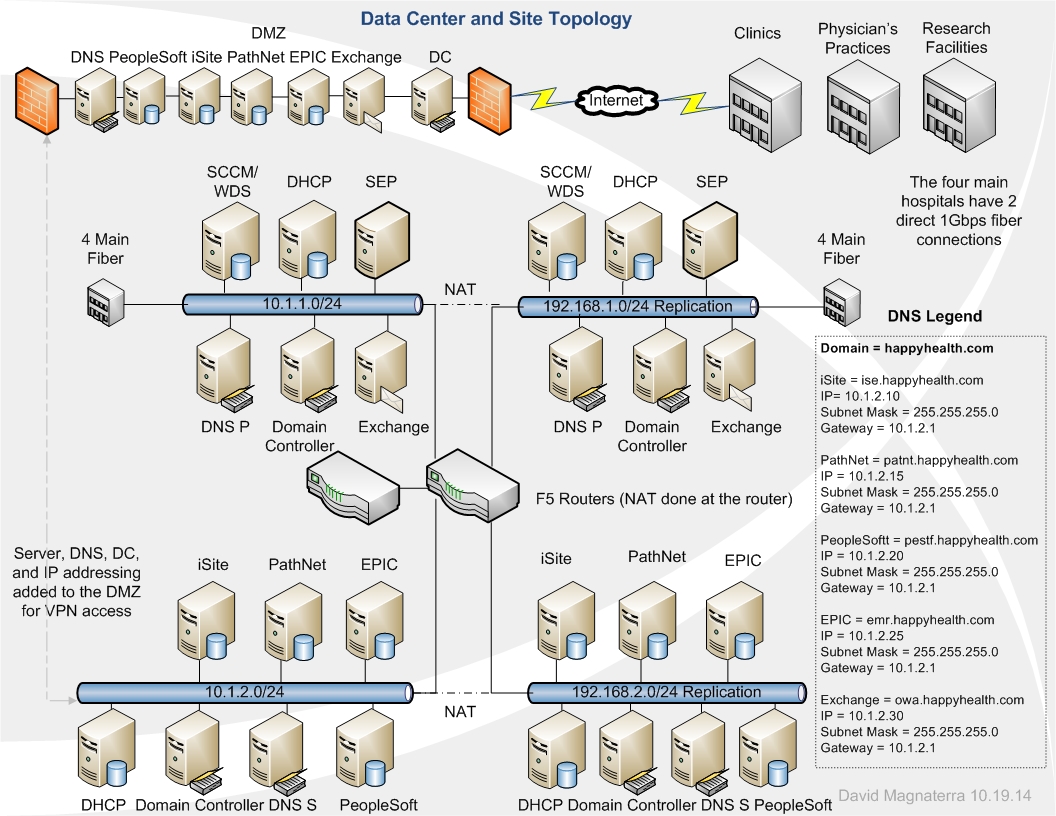


**IP Addressing and Routing Architecture**

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 iSite Enterprise, PathNet, PeopleSoft, and EPIC. This will enable secure access to the network applications, 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. Illustration 1.3 displays the technical overview of the network. 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.

**1.3 Network Topology**

****

**Network Components**

The network standard clients will consist of HP ProDesk 600 small form factors and HP ProBooks 430 models. The desktops specification equate to:

* Windows 7 Professional 64bit
* **Processor**

Intel® Core™ i3-4160 with Intel HD Graphics 4400 (3.6 GHz, 3 MB cache, 2 cores)

Chipset: Intel® Q85 Express

* Environmental: Low halogen
* **Memory**

Standard memory: 4 GB 1600 MHz DDR3 SDRAM (1 x 4 GB)

Memory slots: 4 DIMM

* **Storage**

Internal drive: 500 GB 7200 rpm SATA

Optical drive: Slim SATA SuperMulti DVD writer

Internal drive bays: One 2.5"; One 3.5"

External drive bays: One 3.5"

* **Graphics**

Graphics: Intel HD Graphics 4400

* **Communication**  
  Network interface: Integrated Intel I217LM GbE
* **Power supply**  
  240W

Laptop specifications incorporate the following:

* Windows 7 Professional 64
* Processor  
  Intel® Core™ i3-4005U with Intel HD Graphics 4400 (1.7 GHz, 3 MB cache, 2 cores)

Chipset: Chipset is integrated with processor

* **Memory**  
  4 GB 1600 MHz DDR3 SDRAM (1 x 4 GB)

Memory slots: 2 SODIMM   
Internal drive: 500 GB 5400 rpm SATA

* **Graphics**

Intel HD Graphics 4400

* **Display**  
  13.3" diagonal HD anti-glare LED-backlit (1366 x 768)
* **Communications**

Wireless: Broadcom 802.11a/b/g/n/ac (2x2) and Bluetooth® 4.0 Combo

Network interface: Realtek Ethernet (10/100/1000)

* **Power supply**

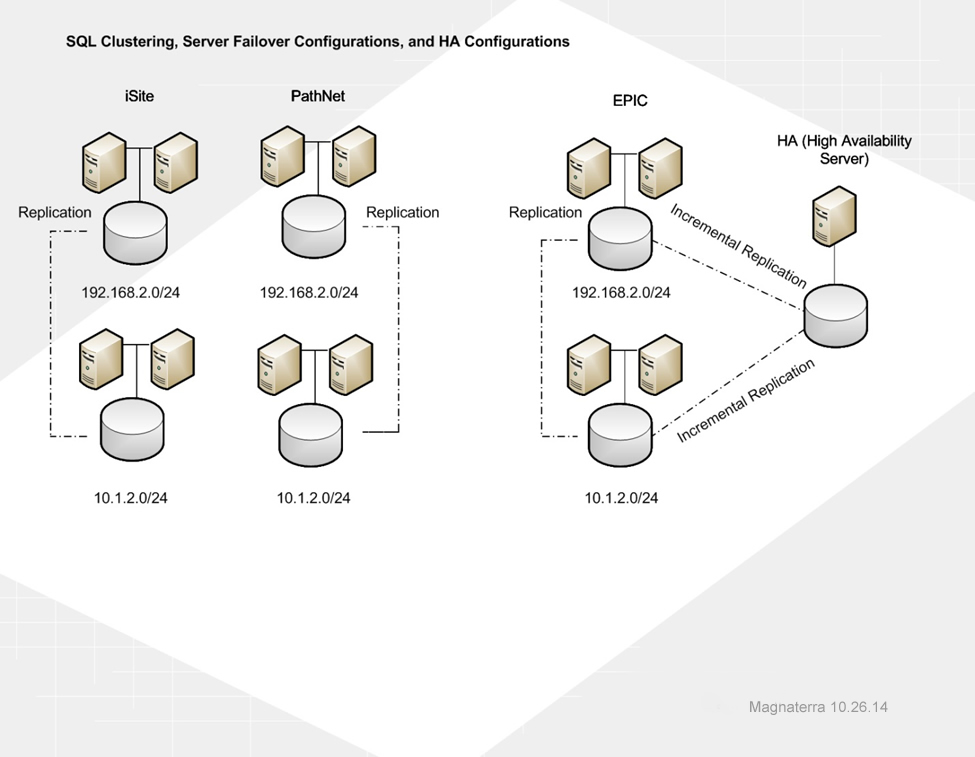
65 W EM Smart AC adapter; 45 W Smart AC adapter

Battery type: 4-cell, 44 WHr Li-ion

**Backup Plans**

Performance architectures will comprise strategic management of high demand systems in essence providing the needed mechanisms to provide redundancy by clustering. iSite and PathNet will incorporate a dual clustered architecture. The physical servers will be setup as a fail over cluster manager feature. Each fail over will have a SQL cluster associated with it. The fail over process will be managed by a virtual IP address (VIP). If one node fails SQL services and Microsoft features will cutover seamlessly. A HP 3 PAR SAN will be attached to each cluster managed by a Quorum. Replication will occur between networks to insure redundancy and bandwidth management. NAT will be managed at the router for replication. EPIC will follow the same architecture with the addition of a high availability server (HA). The cluster server environment will generate incremental replication by scheduled tasking. This data will replicate to the high availability server every thirty minutes located at the disaster recovery site. Diagram 1.4 illustrates the flow analysis for the clusters and replication across the networks.

**1.4 Network Replication**



Failover to the EPIC high availability server will not me seamless. The virtual IP address will have to be changed thus resolving to the original DNS value. Upon new resolution, the EPIC EMR will be out of a degraded state therefore providing availability by adding the layer.

iSite, PathNet, EPIC, and the DMZ will utilize LDAP integration for centralized administration. This will provide efficient management of groups and users across the domains. Active directory and management of LDAP will be done on the domain controllers. Group policies will manage user desktop appearance and user profile types. Deployment of software will be done by Microsoft System Center Configuration Manager (SCCM). Unattended installs driven by .vbs scripts will be the standard deployment strategy. SCCM will enable inventory reporting for hardware and software versions. These reports can be utilized to forecast project implementations and manage deployments over network segments.

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 range within the system stability index. The chart can be analyzed and provisions can be qualified. 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 on the system and log a ticket with the support center.

Access control lists (ACLs) will be managed by the domain controller nodes (DC). iSite, PathNet, and EPIC will have policies and procedures related to their environment defining resources usage, access, and management. The ACLs will provide documentation for referral during crisis or catastrophe. Data backups will occur as daily incremental and weekly full backups. This will be the standard process for all systems.

Maintenance plans will be created for all SQL databases they will incorporate back up processes, re-indexing, and housekeeping. These tasks will be scheduled for various times which are not during peak hours. SCCM resources will deploy and maintain application patches and profile settings. Software deployment will be executed as an unattended installer for version upgrades and new systems. Microsoft deployment for the clinics, Physician’s practices, and research facility will comprise of downstream WSUS servers as a parent child relationship with the upstream WSUS server. Replica mode between the upstream and downstream servers will enable synchronization and approval from the upstream WSUS server. The main upstream WSUS server will be located in the data center with a redundant counterpart on the class C network.

All client computers will have the documents folder pointed at the Distributed File Systems (DFS) share. This allows the users to have a network storage capacity and ensures the integrity of their data. Distributed File Systems (DFS) role will be integrated into the domain controllers. DFS namespaces will incorporate domain-based shares with path mapping associated to the user’s Active Directory account by log on scripting. All users will inherit an H: drive linked to the My Documents folder. This ensures data redundancy as the My Document directories are default paths for saving documents. Some users will have additional DFS shares associated to their log on script thus providing containers with common information shared across groups and organizational units (OUs). The DFS shares will have a backup retention period of 30 days; this ensures data integrity especially for the common DFS shares. Network File Systems (NFS) protocols will be implemented to govern the DFS design moreover managing the EPIC UNIX backbone as well.

File Server Resource Manager (FSRM) will manage the storage resources for the HP 3 PAR SAN. These tools will help zone the volumes and manage quotas for folders. Reports can be generated for refining resource allocation which will optimize storage resources and expansion for the annual 3 PAR storage magazines’ budget.

Windows Search Service (WSS) server role will be implemented on the DFS servers. Indexing management of folders and directories will be evaluated and organized when queried. Results will be cached which permit fast access to the data retrieved. This process will be run at the Local System account starting automatically for all users.

BranchCache will be executed for wide area network (WAN) optimization. This directly affects the DMZ users, contents from the WAN will be cached for the branch offices including the clinics, Physician’s offices, and the research facility. Once one workstation requested the WAN content it will be cached and available for all other branch workstation.

**Secur**i**ty**

Security begins with effective account policies. A GPO linked to the domain will enforce Kerberos settings, account lockout policies, and password policies. The group policies will be applied to the organizational unit and in some cases just a group within the organizational unit. Audit policies will review the account policies by triggers. Local policies and right consignments will provide the user no more or no less than they need to perform their job. Local policies for security will incorporate a standardized approach for logon, user desktop, interactive login, and browser based restrictions. Windows provides a firewall and allows advanced security for configuring inbound and outbound rules. The rules can be deployed to the containers globally or locally. Network list and manager polices will be installed to ensure network stability and deter attacks. Unidentified network policies will block unknown networks and network nodes. Identified networks will be blessed and identification of the location will be catalogued. Permission to the identified networks can be managed group policy edits.

Restriction for applications and control of the application will be identified and managed. Public Key Policies will perform tasks such as automatic certificate enrollment, generate certificate trust lists, administer data recovery agents, and form trust relationships with the certificate authority. Software restriction management will occur to block unapproved software. All new software will be a part of a process called change control. A committee will meet every week to evaluate and approve new software. All other components will be blocked on the domain. Application control policies will inherit AppLocker policies. The software restriction policies and AppLocker policies will work in tandem across the network. The use of BitLocker for laptops and workstations will be a standard as well. The network images will have BitLocker built in thus ensuring encryption for hardware.

The security architecture will encompass public key infrastructure (PKI) certificate assignments. Active directory will be integrated with Microsoft System Center Configuration Manager (SCCM) and become the certificate authority. Client computing will connect to Internet resources by means of PKI coupled it IPSEC technology for point to point communications. SCCM will generate self-signed certificates for an alternative to the PKI certificates due to availability constraints.

The demilitarized zone will deliver access by Internet connections and HTTPS enabled interfacing ran through port 443. SCCM Management Point (MP) will enable client communication. Management point is the interface between the remote clients and the servers. Symantec cloud services will be deployed between the DMZ and the remote sites. This utility will control traffic, email, provide URL filtering and Anti-Virus while communicating with the Symantec Endpoint Protection Proxy within the DMZ. Remote (mobile) users will have access to advertised programs provided by the Citrix server. An RSA token and web portal will be the vessel for access.  
 Symantec Endpoint will manage traffic, Email, virus protection, and system quarantines. The client application will be deployed and updated from centralized servers on each network. Access to the Symantec Endpoint servers will be restricted to a group of domain administrators. Operating systems will be updated to ensure minimal treats for both servers and client computers. Network and host-based intrusion detection systems will monitor traffic and identify suspicious events. SCCM servers will reside on both networks. Their responsibilities will be to manage PKI, deploy updates, and deploy unattended software installations across segments of the network.

**Backup Strategy**

Replication between the main datacenter and the disaster recovery site will ensure high availibilty. Scheduled backups for the database servers are aligned with the best practices concerning the technologies. Multiple layers of redundancy will exist. The servers will have the data partition attached to the 3 PAR SAN which has a RAID and is replicated to the DR. The last layer involves Symantec Netbackups. All servers will have critical partitions replicated and stored for 30 days. In summation Microsoft SQL maintenance plans, SAN redundancy, and Netbackups will reinforce the architecture.

**UNIX and Linux File Systems**

UNIX file systems are known as UFS (Berkeley Fast File System) which utilizes iNode (index node) to encapsulate Meta data for file description. The iNode defines a single file and can be considered somewhat obsolete. iNodes advancements consists of blocking by cylinder groups which separates the iNode data blocks into segments moreover negating fragmentation for large disk partitions.

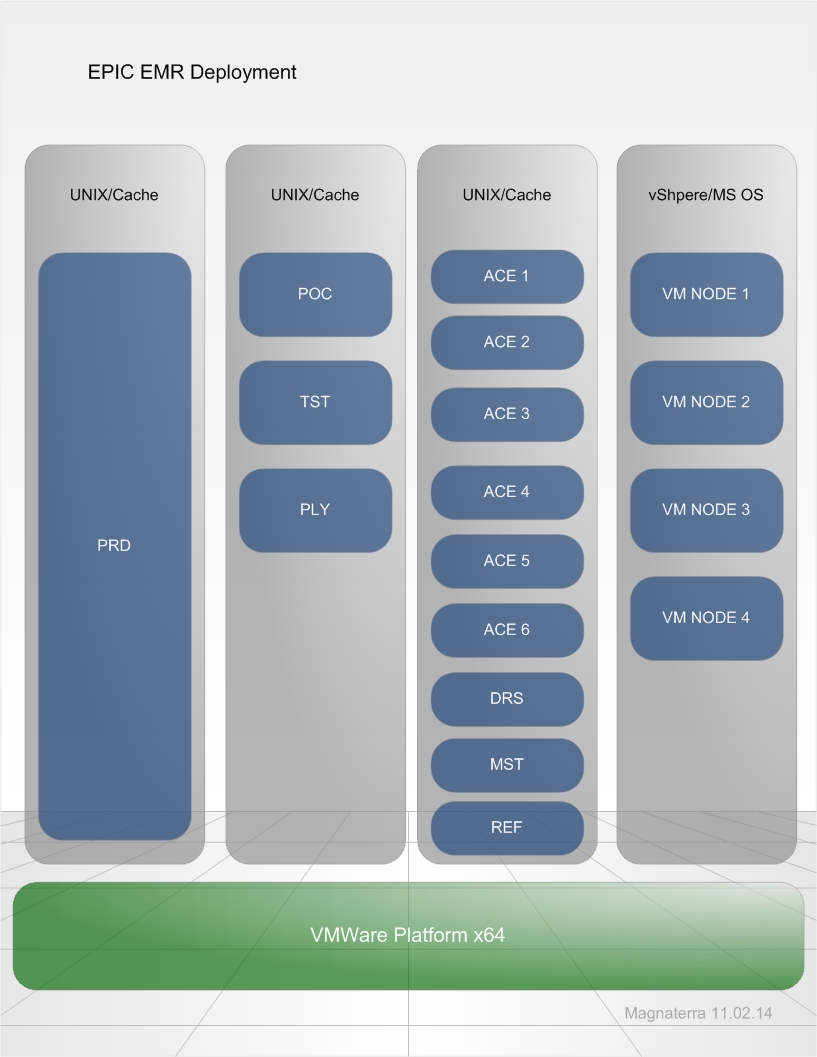
Linux file system is ext2 (second extender file system) is known as a journaling file system and manages flash storage effectively. The ext2 file system is built from UFS concepts thus linking the technology between UNIX and Linux file systems. Linux provides access control list know as POSIX ACLs promoting scalable administration for system files. Ext2 is split into block much like UFS. They too are segmented into cylinder groups designed to minimize fragmentation. iNode integrates with the ACLs allowing the permissions to be applied to the blocked data.

**UNIX – EPIC Deployment**

The EPIC EMR will utilize VMWare vSphere 5 to encompass the virtual nodes for the EPIC system. The system backbone consists of UNIX and Cache married to Windows. The Cache database engine will run on UNIX divided by the various EPIC build environments. System mnemonics functions upon a UNIX and Cache platform in the following layers: POC, PLY, TST, and PROD. POC, TST, and PLY builds are segmented from PROD to ensure federation yet separate the environments. Figure 1.5 illustrates the model for deployment. Each module equates to a separate virtual server.

The virtual servers are replicated to the disaster recovery site moreover providing redundancy. Storage for the virtual machines derives from the HP 3 PAR SAN. All virtual servers reside between twelve host servers. The host servers can provide migration by means of vMotion. If a host server fails the virtual nodes simply migrated to a healthy host server negating service interruption thus generating an additional layer of redundancy. Each storage partition will be thin provisioned and live on a separate virtual SCSI adapter.

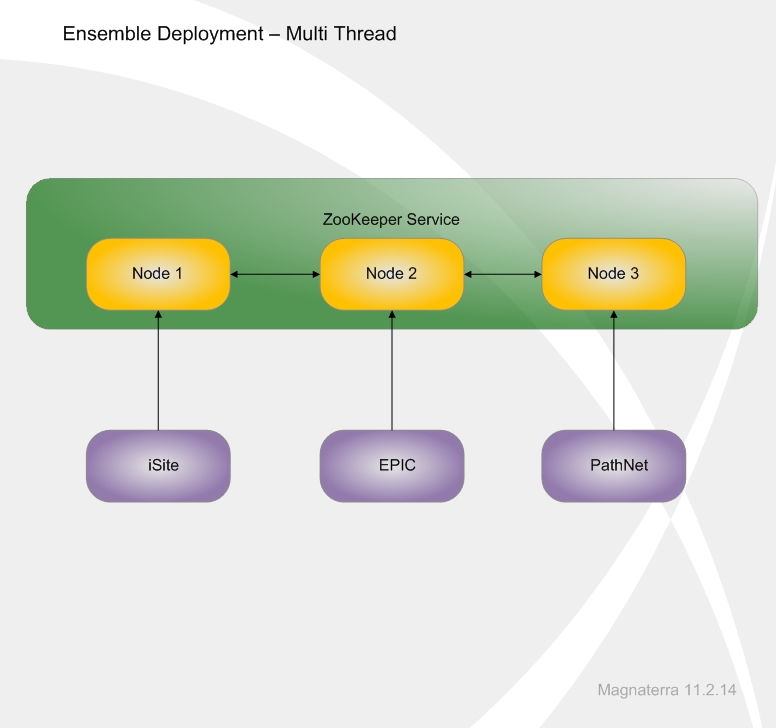
**1.5 EPIC Deployment**



**UNIX – Ensemble Deployment**

The interface engine which provides the “hand shake” between EPIC, iSite, and PathNet will be a UNIX deployment. The environment will be a virtual build farmed similar to EPIC. The Ensemble servers will be UNIX with a Cache database engine. This will incorporate an Apache web server design negating a client on a Windows node (known as the ZooKeeper service). Figure 1.6 projects the flow analysis. This allows zNodes (based on iNodes) to function in a parent child capacity hence optimizing directories by relationships. The Ensemble client will reside upon a Windows client OS for management of the database. The HP 3 PAR SAN will be attached to the virtual nodes thus providing redundancy and high availability. Replication will occur to the disaster recover site accordingly providing high availability.

**1.6 Ensemble Server – Server Architecture**



**UNIX Design**

The marriage between VMWare, Microsoft, Cache, and UNIX enables normalization between the multiple databases. Most database management will be driven by Windows clients therefore generating the portals for administration. Utilizing virtualization permits multiple layers of redundancy for the critical systems. High availability due to vMotion and disaster recovery alignment reinforces the architecture for both by redundancy and geographical diversity.

Driving these systems from the UNIX platform supplements low overhead and allows the environment to be scalable for the efficiencies associated to the file systems and the directory services. Hierarchy construction for data nodes directories allows associations “think of znodes (ZooKeeper data nodes) as files in a traditional UNIX-like system, except that they can have child nodes” (Grover, 2013).

**Windows – UNIX**

Windows security manages users by Security Identifiers (SID). The SID is a unique identifier which never changes and cannot be reused. UNIX provides users a User Identification Number (UID). Some flexibility is available as this is not a dynamic process. The UID is manually selected by the system administrator and can be reassigned.

Windows authentication is password based; the password and SID are contained together within the Security Accounts Manager (SAM). This is a database for hashed passwords; LM-hash and NT-native. UNIX utilizes a system which sees the UID then acknowledges the relationship. Once the password is entered the encryption occurs by comparing the string in the NIS database. This style can be compromise as the file is readable for everyone thus providing a backdoor for intrusion.

Windows Access Control Lists (ACLs) are object orientated whereas all database objects have an ACL. Access Control Entries drive the lists by group association. The group container association allows the permissions to be set globally. UNIX manages access control within the UFS by indexing every file and directory then comparing the UID for ownership. Group membership by default can read and execute, additional permission must be denoted.

**UNIX Implementation**

UNIX systems security must be managed efficiently to ensure stability. Non-interactive accounts can be the vessel for intrusion, the login shell must be disabled and equate to a null value. This allows accounts to be available yet secure. Anonymous FTP activity can be an inlet for attacks as well. Additional security controls can be deployed to counter access points. A sandbox can be designed to contain and secure the UNIX architectures. User group design and ACL alignment must be an executed effectively; disabling the administrator account can help security after the initial deployment.

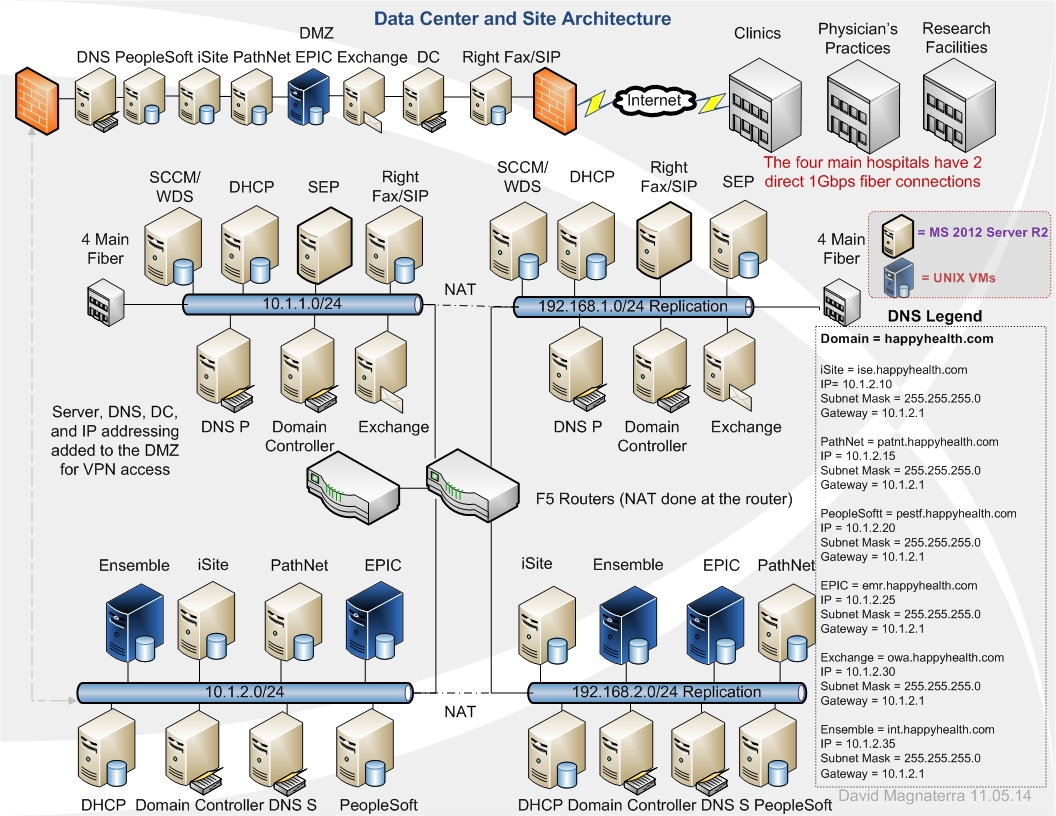
After security is established the testing will occur. Multiple dry-runs will take place; one by one problematic variables will be eliminated. Upon the final dry-run production UNIX and Cache builds will become populated by the data from the former HIS. The migration of information can transpire in increments. After 50% of information is populated for EPIC the interfaces between the servers concerning HL7 will begin feeding to the downstream systems.

**Operating Systems and Hardware**

The base workstations incorporate Windows 7 Enterprise addition. The operating systems will interact with the monitor/s, perphials, and in many caces a microphone for physician dictation. The operating system driver set will function with the monitor/s and perphials from the built in drivers. The speech microphone will have drivers installed from the vendor website thus ensuring updated interfaces. Printing consiste of network only print servers. All printing will be laser jet fuser based modules. Drivers will be located on the IT DFS share, the installation will be completed by the desktop support team.

Atypical workstations will have additional driver integrations. The Radiologist’s diagnostic workstation must incorporate BARCO MX7400 GPU boards.This relationship with the operating system involves specialized configuations. The diagnostic reading workstation have four three megapixel monitors and two companion monitors. Interfacing the custom drivers with iSite comprises balanceing the display properties with the operating syatem and the display setting in the application. The images need to follow hanging protocols to emulate preceding light boxes. The two BARCO MX 7400 card will connect the four DVI-D ports to the diagnostic monitors (three megapixel monitors). The two display ports will connect the companion monitors.

**1.7 Network Diagram – All Nodes**



The network nodes illustrated in figure 1.7 protrey the relation ship between the external sites, the DMZ, and the disaster recovery site. Incremental replication occurs for all critical systems to the disaster recovery site. There is translation between the class A and class C networks. The F5 router has a redundant counterpart which allows a failover feature. The four main hospital are connected to both the main datacenter and the disaster recovery site. The servers DNS can resolve to the class C IP addresses upon failure. DNS internal placement will consist of primary to secondary nodes. The main datacenter will entertain one primary and on secondary node per network. One WINS node will be placed into each network for NetBIOS resolutions. The CNAME alias will be the record type utilized for all DNS nodes. The DNS resolver will query both the CNAME record and regular resource record. This allows local or remote naming resolutions. Upon network failure, the IP schema can be “flipped” to the stable network e.g. ise.happhealth.com has a native network address of 10.1.2.10. If the 10.1.2.x network fails simply have ise.happhealth.com resolve to 192.168.1.10 thus providing redundancy.

The Class A IP addressing will be the native or default values. The Class C addressing will only resolve upon network failure. The IP and DNS matching are comprised of the following redundant linkage:

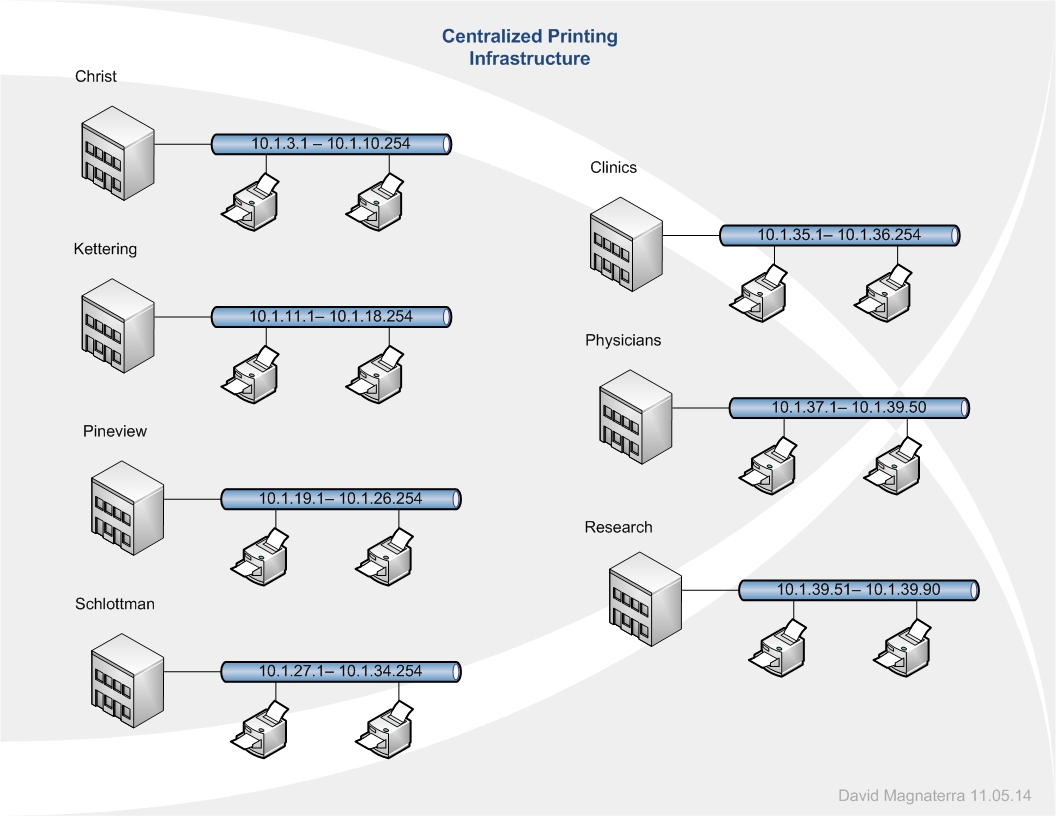
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DNS | IP | IP | Subnet Mask | Subnet Mask | Gateway | Gateway |
| ise.happyhealth.com | 10.1.2.10 | 192.168.1.10 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| patnt.happyhealth.com | 10.1.2.15 | 192.168.1.15 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| pestf.happyhealth.com | 10.1.2.20 | 192.168.1.20 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| emr.happyhealth.com | 10.1.2.25 | 192.168.1.25 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| owa.happyhealth.com | 10.1.2.30 | 192.168.1.30 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |
| int.happyhealth.com | 10.1.2.35 | 192.168.1.35 | 255.255.255.0 | 255.255.255.0 | 10.1.2.1 | 192.168.1.1 |

**Printing Infrastructure**

Printing infrastructure will centralize printing throughout the departments and floors. Different floors will utilize different segments of the network. Each floor or department incorporates two HP Color Laser Jet 3600n printer servers. Both local and remote users will have access to the print servers; the printer management interface will be accessible by toggling the printer IP address in the IE browser. This architecture encompasses a tier system shown below.

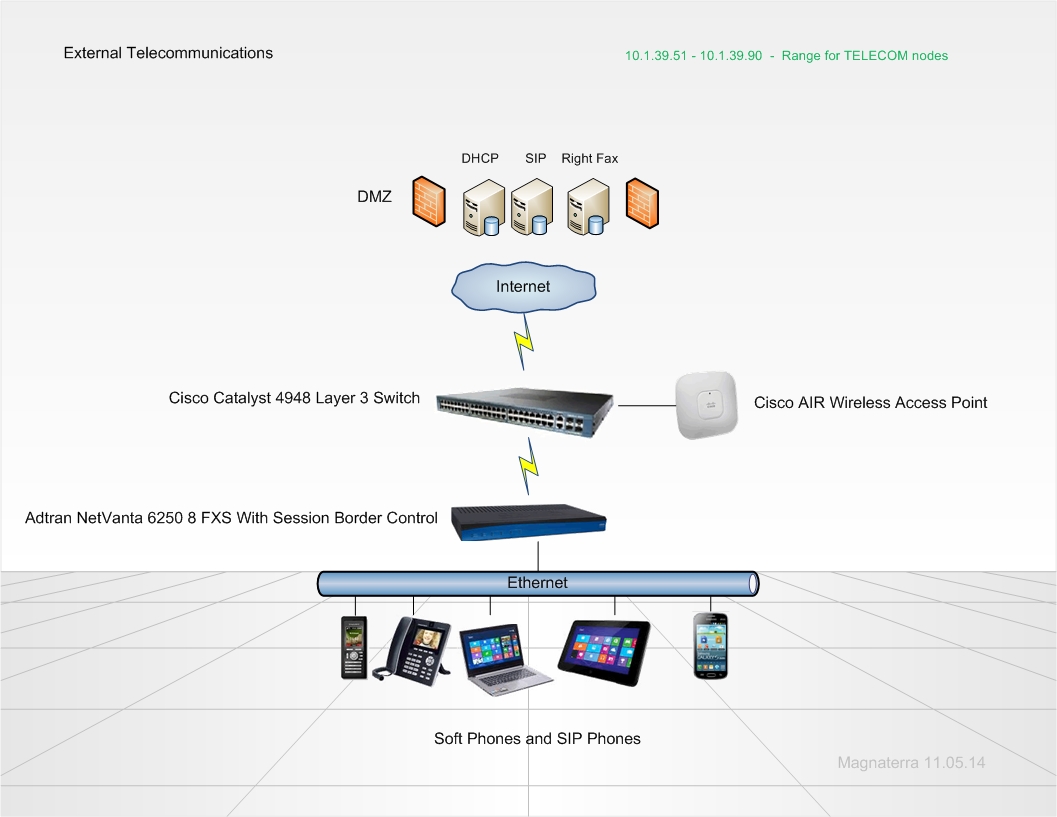
All printing will be done by means of Laser Jet. No printers will be locally attached to a workstation. Client workstations connect to the print servers throughout the network. Mobile devices can attach to the print server over the wireless infrastructure and acquire multiple printer servers "the benefit of this system, known as ‘peer-to-peer’ printing, is that no additional infrastructure is needed, and consequently less maintenance"(Axis, 2014). Each site will utilize DHCP reservations for the printers thus generating an IP address which will not change due to lease. Diagram 1.8 projects the IP range associated to the printer infrastructure across the domain.

**1.8 Centralized Printing**

****

Print queues reside in the windows operating system. The print spooler services handle the jobs for print servers with a single process moreover segmenting the service per server. Drivers associated to the networked printer will reside on the client workstation providing the interface between the hardware and the operating system "one server has a driver version 26.232 the other has version 26.234, in theory the client will download the latest driver and use it for both printers, in practice the results may be less predictable - the worst case being a driver download every time the user prints" (SS64, 2014). Communication starts at the physical layer; the NIC card communicates to the network switch then the print server acknowledges the request. Upon acknowledgment, the print process queues then moves to the spooler for execution. All administration occurs by access to the print server from the client IE browser. Credentials are passed when the administrator logs into the operating system. The printer is toggled using the IP address in the IE browser.

**1.9 Remote Faxing and Telecommunications – SIP Technology**



Session initiation protocol (SIP) will manage multiple media types thus generating a scalable architecture for faxing, 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.

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 negating modems. Ethernet protocols manage the throughput for all types of communication across the network therefore standardizing the infrastructure components across the wide area network (WAN). 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.

**IP Design**

The replication at the data center to the disaster recovery data center will incorporate parallel IP v6 functionality. The servers in the IP v4 scope will be manually configured to provide stability between network nodes. The interface identifiers for IP v6 will rely upon current IP v4 router configurations as the naming schema thus enabling seamless conversion between the two versions. The second phase of testing will integrate the nodes within the DMZ. This will be the testing ground for IP v6 deployment in the future; the following table illustrates the DR data center subnet mapping.

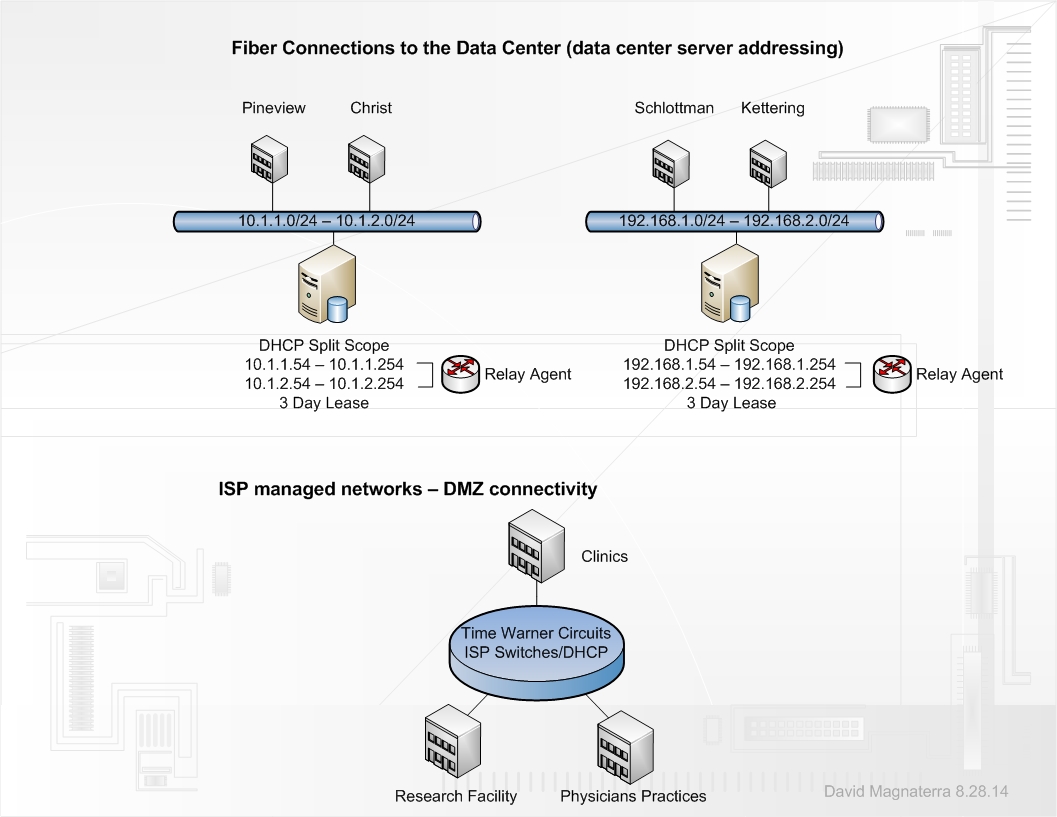
|  |  |
| --- | --- |
| IP v4 | IP v6 |
| 192.168.1.0/24 | 2001:db8:3c4d:1::/64 |
| 192.168.2.0/24 | 2001:db8:3c4d:2::/64 |

The tangible differences between the two addressing types begin with the IP v4 bit strings. IP v4 allows 32 bit whereas IP v6 employs 128 bit capacities. The class structure for IP v4 consists of A, B, C, and D primarily. IP v6 entails hexadecimal digits signifying 4 bits. This far supersede IP v4 total amount of addresses. IP v4 has a maximum of 4,294,967,296 addresses available; IP v6 allows 79,228,162,514,264,337,593,543,950,336 total addresses. Testing the new addressing must be complete due to the imminent execution of the new IP system. The main differences between the two are the allocation, life, mask, prefix and the method of address resolution protocol (ARP). IP v4 standards are quite logical yet have constraints however IP v6 endless capabilities prove relatively complicated.

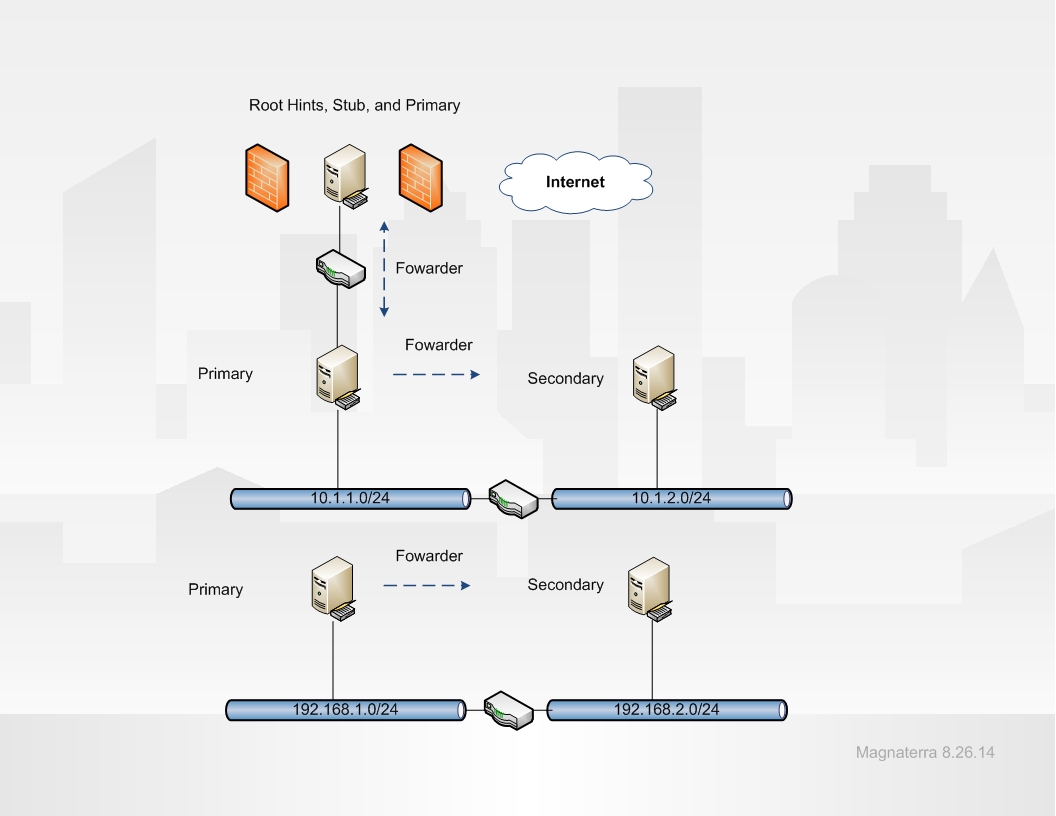
The DHCP configurations will be administered within Microsoft Windows Server 2012. The DHCP servers will provide leases and reservations for static IP addressing. The MAC address will be programed into the reservation which will provide the static IP configurations necessary for servers, printers, and radiology modalities. Polices for vendor class, user class, MAC addresses, client identifiers, and relay agents will be defined. The outside facilities are controlled by ISP third party IP addressing. We have identified ranges and classes to the ISP for these facilities. Stability can be compromised due to the third-party component. Switch and circuit failures will stop connectivity to the DMZ resources. Redundancy has been evaluated for failover protocols. The failover process has been tested with the ISP.

The DHCP scope will incorporate three networks. The first two networks will have two subnets for the DHCP pool of addresses. Between the subnets a DHCP relay agent will manage the requests by utilizing a DHCPREQUEST broadcast message. The DHCP relay agent will enable the DHCPREQUEST message to leave the subnet and route the message to the DHCP server. Routers and layer three switches will enable broadcast messages to facilitate the messaging. The DHCP scope will be divided evenly between subnets to ensure address availability. The third network will comprise the clinics, physician’s practices, and the research facility. Layer three switches will manage the external sites with Time Warner circuits. The DHCP and routing will be administered once authenticated into the DMZ. Address ranges 10.1.35.1 through 10.1.39.90 will have reservations assigned within the DHCP pool. The external sites will tunnel through the Internet and reach the DMZ therefore accessing the hosted applications and resources. This alternative enables a cost effective solution for support and subtracts network overhead. The table below projects the IP ranges which are dedicated to the sites across the network. The scope of subnets will be routed/forwarded by relay agents.

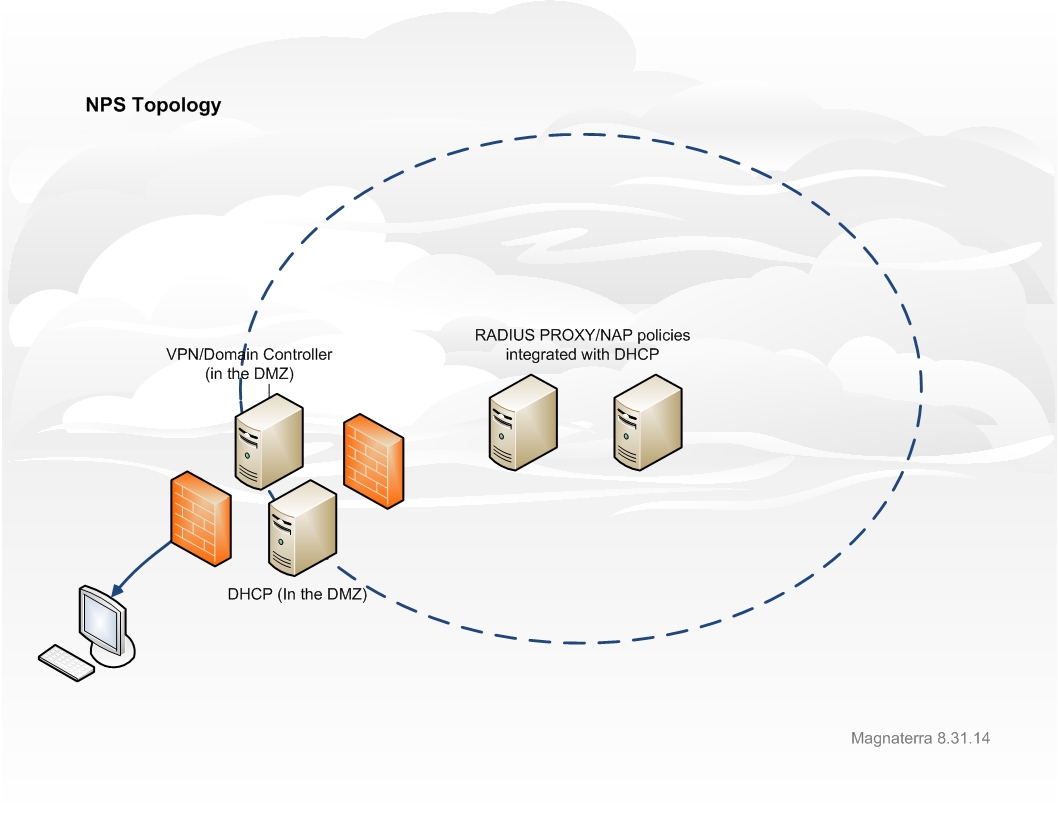
|  |  |  |
| --- | --- | --- |
| Site | Scope Subnet | Lease Period |
| Christ | 10.1.3.1 - 10.1.10.254 | **7 Days** |
| Kettering | 10.1.11.1 - 10.1.18.254 | **7 Days** |
| Pineview | 10.1.19.1 - 10.1.26.254 | **7 Days** |
| Schlottman | 10.1.27.1 - 10.1.34.254 | **7 Days** |
| Clinics | 10.1.35.1 - 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 DHCP servers will be a split scope and use two independent DHCP servers which share responsibility for each scope. The class A network will have one split scope and the class C network will have one split scope. This provides a layer of redundancy and negates a single point of failure. Address assignment will be split by fifty percent of addresses on each server. DHCP failover will be configured in the Windows Server 2012 server management console. This configuration provides DHCP up time continuous availability, it also enables dynamic lease expansion to the node if the DHCP server is not reachable. Communication between the two split scope DHCP servers executes lease replication thus qualifying management of subnets for the compromised DHCP server.



The configurations in Windows Server 2012 will entail an extension of resources into the DMZ. A root server will be incorporated into the DNS node within the DMZ. Within the server management console external forwarding will be done internally. Internal conditional forwarding will occur from the primary DNS servers to the secondary DNS servers. Each DNS server will have a stub interface built to refer requests. The diagram above projects the design for the flow of replication. Dynamic updates within zones will be enabled because the DNS topology is a primary to secondary interaction across the network. The interfaces listening for the DNS request will be set manually to provide security from DNS poisoning.

****

The DMZ plays a large part in the protection topology. Adding the NPS role allows scalable administration for access "NPS is a RADIUS-compatible server designed to provide authentication and authorization for remote clients, and it acts as the "health evaluation server" for Network Access Protection" (Rouse, 2012). VPN services will reside on the domain controller located in the DMZ. DHCP integration with NAP also will reside in the DMZ for VPN access. A RADIUS proxy provides the authentication for the all users. The configuration will be DTS compliant; the proxy will house the remote server groups as the RADIUS will incorporate the proxy as a RADIUS client. RADIUS accounting will be attached to a SQL database with an ODBC connection. Diagram 1.6 Illustrates the topology.

NAP configurations involve DHCP as the gateway. The network access protection will be enabled on the scope. Scope options will be configured to limit access to the nodes which do not operate within the defined parameters. VPN connectivity with NAP employs EAP security for connections. Non-compliant clients will be filtered and access will be limited. These windows configuration will be implemented for VPN and standard DHCP access. VPN access will deliver synonymous NAP configurations; the only difference is the DMZ firewall configurations. NAP governs the remote desktop gateway as well. The health check of the client querying the gateway will have policy enforcement and group association concerning the remote desktop users. If NAP is unavailable restricted access will be applied. Active Directory account access and Exchange email will be provided, DFS shares will be offline until NAP is available.

**References**

Axis. (2014). Network printing infrastructure. Retrieved November 2014, from <http://www.axis.com/products/print_servers/about/printing_infrastructure.htm>

Krypted. (2012). Managing DNS In Windows Server 2012. Retrieved October 2014, from <http://krypted.com/windows-server/managing-dns-in-windows-server-2012/>

Grover, Mark. (2013). ZooKeeper fundamentals, deployment, and applications. Retrieved November, 2014, from <http://www.ibm.com/developerworks/library/bd-zookeeper/>

Lavapie, Rolly. (2012). Step-by-Step Guide for Windows Deployment Services. Retrieved October, 2014, from <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&cad=rja&uact=8&ved=0CCYQFjAB&url=http%3A%2F%2Fwww.smashwords.com%2Fbooks%2Fdownload%2F216962%2F1%2Flatest%2F0%2F0%2Fstep-by-step-guide-for-windows-deployment-services.pdf&ei=EBr6U5T1I5KnyASg1IGoCw&usg=AFQjCNFtoENSyG-TvtBok9Glni2c7efVnw&bvm=bv.73612305,d.aWw>

Spector, Lincoln. (2009). 7 Backup Strategies for Your Data, Multimedia, and System Files. Retrieved October, 2014, from <http://www.pcworld.com/article/170688/7_backup_strategies.html>

SS64. (2014). Managing DNS In Windows Server 2012. Retrieved November 2014, from <http://krypted.com/windows-server/managing-dns-in-windows-server-2012/>