Tepe Services
Network Overhaul
Senior Design Project

Josh Pastura, Mark Tepe, Nick Waldbillig
4/28/2013
Tepe Services Network Overhaul

Mark Tepe, Nick Waldbillig, Josh Pastura

The Faculty of the Department of Information Technology
In Partial Fulfillment of the Requirements for
The Degree of Bachelor of Science
In Information Technology

University of Cincinnati
Department of Information Technology
College of Education, Criminal Justice, and Human Services

April 2013

Josh Pastura ........................................ 4/17/2013 .................. Date
  Josh Pastura

Mark Tepe ........................................ 4/17/2013 .................. Date
  Mark Tepe

Nick Waldbillig ................................. 4/17/2013 .................. Date
  Nick Waldbillig

Russell E. McMahon ......................... 4/16/2013 .................. Date
  Professor Russell McMahon
Table of Contents

I. Introduction
II. Credibility
III. Problem
IV. Overview
V. Proposed Solution
VI. Methodology
VII. User Profiles
VIII. Solution Details
IX. Hardware and Software
X. Budget
XI. Schedule
XII. Problems Encountered
XIII. Future Recommendations
XIV. Conclusion
XV. Works Cited
Introduction

Tepe Services, a landscaping design firm, has an extremely outdated and not fully utilized network. The network has about 25 onsite computers, 15 Scheduling PDA’s, as well as the companies mobile phones. The front office has two computers for scheduling and accounting. The other computers are personal work PC’s, with one being solely for the purpose of the CAD Printer. The network is purely an ad hoc network, there are routers residing in plain sight and anyone who wishes to connect to them can do so without any effort. Currently there is one main router, a D-Link, and then from there the rest of the switches are daisy chained to that.

There are two servers in use at the company. One is a FTP share, with a failover, and the other is their backup system. The issue here is that the FTP has failed along with its fail over, so there is no working file sharing in place. The backup system is of some use, but without active file sharing there has not been any new data to backup.

The computers and network resources are all maintained and administered by the management of the company, who have no IT training or background. If something were to happen then either Mark or Nick would come in to take care of the issue.

Credibility

All three members of the group are seniors in the Information Technology degree program specializing in networking. Each of us has taken all the core networking classes required of us, they are listed as followed:

Routing and Switching which taught us how to setup and configure the networks specifically concerning routers and switches. This class was the main source of information in the configuration of our Cisco 800 series router.
Network Security assisted us in the formation of a safe and secure network for the company as well as more information on the configuration of the router.

System Administration I and II helped us with the configuration of user profiles, the AD, GPO’s and system security.

Network Infrastructure development helped with the setup and configuration of our servers; DHCP, AD, and our firewall server.

Intro to Networking taught us the basics of designing and setting up networks.

On top of our course work the entire group has spent numerous hours through our coops working with systems and networks at several different companies between the three of us.

**Problem**

The main concern of the company is security; there is nothing currently in place to prevent even a disgruntled employee from causing serious damage to the company. The person could very easily delete anything or modify whatever said person chooses to do.
Next, there is no utilization of the file shares, management, or account permissions. The company currently has no GPO’s whatsoever, so security from that standpoint is sorely missed. This was the primary cause of the issues in the past year(s) including the recent security breach involving the email system currently in place. Management has no way of overseeing the users on each computer and what they have access to. There are no logging systems in place so if anything happens, there is no documentation.

If users need to access company resources they must either use the external hard drives or simply email the files to each other. There is no central location for sharing anymore. A sizable chunk of the files are written down now, which only adds to the tediousness of trying to put data together.
The computers on the network as a whole are incredibly outdated; there are some even using home editions of Windows XP that can’t be added to the AD. They are massively behind on updates from Microsoft, and to say that anti-virus is lacking is an understatement.

The network infrastructure is a huge mess. The wiring closet is also doubling as a power tool closet, with easy access to easily disable the entire network with a cement saw. There is no management in place for the infrastructure, at first glance anyone would be hard pressed to figure out what went where and what devices were even attached to the router were a mystery. The network is quite slow at peak hours, and occasionally the network will go down.

The wireless access points in place have no security other than a password, and pose a huge security risk to the entire network. The access points are plugged directly into the main router (which is directly connected to the ISP). There is no subnet for the wireless, and it is not split between a customer wireless access and employee access either even though there is an option to do so.

There is no backup solution currently in place as the backup server failed sometime in the past, the company was not sure when. So none of the computers have any backup solutions and the only form of backup they have really is old fashioned writing stuff down. This affects every employee and the management here because if the employee loses any important information there is no easy form of recovering that data.
Tepe Services has finally recognized that in order to continuing growing as a business they need to have a fully functioning network that can run on its own for the most part. Currently their wiring closet is just that, a closet. There is no added security or management in place around their network devices and anyone is free to tamper with them at any time. The servers they have currently have failed and are taking up space more than anything else. The workstations are so outdated that, even by adding in some security into the environment, these machines would still have issues with being infected by malware and viruses. Below is a diagram of the previous network setup.
Figure C: Attached above is the old network setup.

Overview

The remainder of this final report outlines in detail how the project was completed. The report includes the following sections: Proposed Solution, User Profiles, Solution Details, Hardware and Software, Budget, Schedule, and the Conclusion.

Proposed Solution

Our proposed solution for Tepe Services was to first plan what hardware and software will need to be bought. Second is to setup and configure all of the hardware that was purchased. Third, the pre-existing network that is currently in place will be completely torn out and replaced. After the breakdown we will install all hardware and software and
begin updating the network. From there the new AD, GPO’s, DHCP, and firewall servers will be implemented and make sure they work correctly with the network. Afterwards all PC’s will be connected to the network and then follow up with troubleshooting, training, documentation, and implementing whatever changes management decides they want done.

The group came up with this idea through discussions with management at Tepe, and discussion amongst us based on prior classwork and work completed through our coops.

**Methodology**

The design requirements allowed us to create a “big picture” approach so that we knew what the company expected from the group and what they wanted to be accomplished. With this approach it allowed us to be flexible with the implementation of the new network by not focusing all the little details too much but we still knew where we needed to go with the project.

Testing was a huge part of this project for us, because there was quite a bit of trial and error with the implementation of the network. The group has never taken on a project like this before and while the setup and configuration went fairly smooth, some things were not accounted for such as, all of the software that would need to be reconfigured that was previously in place to work with the new network. This required hours and hours of fine tuning and tweaking little things in order for the network to be completely in place and all software up and running properly.
User Profiles

Tepe Services users consist of administrators, sales, accounting, CAD, office receptionists, guests/clients. An acceptable network solution will have to fulfill each of these users.

The first user group that needs to be addressed with this network system is the administrators group. The administrators will consist of the owners Mark Tepe and Gregg Tepe. They will need to have access to the servers monitoring tools to see how the company is utilizing the network traffic throughout the week. This group should have access to all of the server shares including the accounting files and all of the backups from the employee’s workstations. They will also have access to the usage monitoring tool, which will allow them to see how employees are making use of company time. The administrative group will be managing the network, they will have to outsource if they have any issues. They will be able to view logs and make sure everything is running smoothly as far as user access rights and etc. The whole point of this group is to make sure that the company is getting the most out of employee’s time and to make sure that the network is running up to speed. This group will have to be given training in order to get the full use out of their privileges.

The second group will be the sales team group. This group will consist of most of the office employees that handle sales for lighting, landscape and sprinkler. They will
need access to applications such as Microsoft Office Suite (Word, PowerPoint, and Excel). This group will also have their own Sales Share that will contain all of the invoicing, proposals and other client data needed for the employees to fulfill their job daily. Wireless access or wired access will be setup so that the sales group can log in using their laptop or desktop anywhere in the office and still connect into these shares. Remote access will be setup to allow the sales team to access from home if need be. The on-site employees have little to no experience regarding IT fields. They are familiar with the basics to get their job done; such as using file shares and the network printers. Improvements to be made for them would be making sure network speeds are up to par, making sure there is little to no network downtime, and increasing the speed of their computers as well.

The off-site employees will only need to have access to the VPN’s as well as the scheduling software that they will access through their mobile phones and PDA’s. For these users the network must be up at all times and have no drop in connectivity. The must also be able to access the Wi-Fi points throughout the company’s grounds as well via their laptops.

The customers will have basic Wi-Fi access which will be on its own subnet so that it is not touching the internal network of the company. These users will have no other needs than that access, so the project is not catering to the customer too much here.

The accounting user group will have access to an accounting share that will have a full archive of all of the accounting history from previous years. This group will have remote access denied since this information is very confidential and the owners don’t want this data leaving the office externally. This user group will have permission to
access the accounting software that will be running on the application server. This accounting will have monitoring tools running to log every event on the users accessing this account.

The receptionists will need to have access to the scheduling software and accounting software. They need to have their rights restricted so that anything that could cause damage to the company, whether it be by accident or on purpose, would be prevented. These users also need to have the most up-to-date machines so that the likelihood of their machines being compromised is very small. The office receptionist’s user group will be similar to the sales user group. This group will have access to the Microsoft Office Suite, Office Share that will have files that they need to complete their tasks, and access to Hindsite Software for scheduling technicians for clients.

The CAD user group is for the designers using auto CAD for computer-aided drawings of landscaping and lighting designs. This group is only using one application and it is Autodesk’s AutoCAD 2007 application. Our solution will give them permissions to use this application as well as to save and backup all of their existing work to the network attached server.
Solution Details

Our solution will replace the routers, so that the company can have better security over-all with improved speeds. Switches will be added to the network for scalability and ease of management as well as an improvement to security. An IDS (Snort) will be put in place so that management will be aware at all times of what is going on in the network. Active Directory will be put in place as well as group policies for a more secure internal infrastructure and to prevent disgruntled employees from further damaging the company. Physical security will be repaired or replaced depending on the system currently in place (locks, security cameras, etc.). The current network closets will be re-wired with CAT6 cabling by group to give added speed to the network. Tepe Services also needs consolidation of their customer databases so they can cross-sell better. Our group will build them a new customer database that will include all the customers from all of their
current applications into one system. During the project, our team will be looking into other side projects to further enhance the network and make it more useable.

**Servers**

The first goal of the overhaul is to deploy four new servers. One will be running pfSense, which is an open sourced firewall with many add-ons that you can integrate directly into the software such as Snort and also Squid. The group is using Snort on the server as our IDS, which will monitor the network for any intrusions and other nuances. Squid will be put in place as our Web filtering device which will also allow for logging.

The company decided to go with an open source solution mainly for budgeting reasons but also since pfSense is incredibly versatile, there are many features that have been put into this software that allows for quite a bit of control and management.

The second server will be running Windows Server 2012 which will be our Domain Controller. This box will be running Active Directory which will be implemented here so that the company is easier to manage, scale, and secure. DNS will also be running DNS and DHCP to help with managing the addressing scheme the group agreed upon. The DC will also have a management tool for Gregg Tepe so that he can manage the network without having to outsource.
Figure E: Pictured above is the Windows Server 2012.

The third server will be our application server. This server will be running VMware EXSI which will allow for the administrative staff to easily manage resources for the applications and reduce conflicts as well.

EXSI is currently working and has 2 servers which will be soon expanded to 3.
Figure F: Pictured above is the EXSI Server.

Server Backups

For backup to the servers a 4TB NAS will be put in place, on site at the company’s office. There is a backup and recovery feature which is built into WS 2012, and the group will put those backups on the NAS that will be used and taken advantage of. Another form of backup that is being utilized is Carbonite; the group purchased the package to allow all computers on the network to have specific folders backed-up at specific times throughout the week for our online/off-site backup.

Our backup plan is that the onsite backup will have all files backed up locally to the NAS device. Carbonite will be our offsite and main form of backup in case of any kind of disaster at the company office building (fire, floods, etc.). All information will be backed up except for client/customer personal information so there will not be any credit card information being saved on the companies end.
**Printing**

The company already has quite a few network printers, some of which are top of the line so the group will be integrating these printers with the printing services offered through windows server as well. This will allow for us to choose which printers users are allowed to print from each pc.

**Switches**

The company has purchased a 48 port switch which will act as our main switch. Four VLANs will be configured and implemented for increased security and ease of management. The first VLAN will be only for our servers. The second will be for internal employees. The third and fourth VLANs will be set up as internal and guest Wi-Fi respectively.

**Wireless**

The wireless network that is currently in place will be scrapped. The group will be securing the wireless so that it is less of a security risk. The first step is separating the Wi-Fi so that there is an employee wireless network as well as a guest connection. These will be on separate subnets that are off the main subnet for the network. These will then be separated into two different VLANs.

It was agreed upon to do this so that if a guest connects to the wireless, they will not be able to see the internal network and see what is going on. The employee wireless will be separated as well so that if there are any malicious users or apps on the machines the employees are using it will not compromise the internal network. The wireless will also take advantage of WPA2 encryption for further security.
**Router**

For our network router are using a Cisco 881 Series router which will be the main (and only) router for the network. This will allow for routing of traffic between the several VLANs that will be implemented.

**VPN**

To allow for remote access the group will be setting up a VPN connection so that employees can securely and quickly connect to their machines without compromising the network or being a drain on the network as well. The VPN users will be on the private subnet which was created for the internal employee Wi-Fi access.

**Anti-Virus Software**

It has not been agreed upon on what to choose for a business grade anti-virus solution yet, but most likely be using a free or open sourced AV for budgeting reasons. This AV will be installed across all machines so that everyone is on the same starting ground for protection.

**Operating Systems**

Our group will be updating the network as needed so that all machines will be on the AD. There are a total of 8 machines that need new upgrades to Windows 7 Professional since they are currently on Windows XP Home Edition. Windows Home Edition operating system cannot be added to the domain controllers on our network, this is why the workstations must be upgraded. The company will be upgraded from 8 workstations to 15 workstations, and once the new building is complete there will be 5 more workstations added to the network as well, all will be running Windows 7.

**Security**
Over a dozen new security cameras have been purchased, that have been placed throughout the building per the instructions of management. There were a few cameras that were previously in place that needed to be repaired and have new cable run.

**Pre-existing Software**

There were several pieces of pre-existing software that needed to be brought over from the old network and integrated into the new network to make sure that it functioned as it did previously and without any issues. The first piece of software was Hindsite, which is on 7 workstations in the building. The purpose of this software is to control sprinkler systems remotely and was integral to the company’s service they provided to customers after a system was put in place.

Timesummit Exaktime is the company’s time tracking system for W2 employee’s so that they can perform payroll easier. They use a box that is connected directly to the network that allows employees to swipe their badge to clock-in/out. This box has its own statically set IP address that caused some issues for us when implementing the new network because there was no way of figuring out what that IP was set to be since there was no documentation and could not test through pinging because the box did not allow for pings. In the end, the box ended up having to be reset completely and be reconfigured for the new network.

AutoCAD 2007 needed to be reconfigured for the media workstation in the office which has access to the industrial printer for blueprints. QuickBooks enterprise also needed to be reinstalled and reconfigured on the accountant’s new machine as well. The
final piece of software, another accounting program which was needed, was MYOB 2006 which was specifically designed with landscaping companies in mind.

**Documentation and Training**

We have documented our project from the ground up. The group will be documenting the network address scheme, the VLAN configurations as well as the switch and router configurations. There is documentation for the server configurations, wireless, backups, and anti-virus configurations along with all licensing documentation.

Training will be provided for all employees, so that they are aware of what they can and cannot do. Management will receive special training for use of the management system that will be put in place.

The goal here is to allow the company to not have to worry about the technical aspect of the business so that they may focus solely on the business aspect as well as allow them to run much more efficiently. Below is a diagram of the proposed solution that our team is going to deploy for Tepe Services.
Figure G: Attached above is the proposed network solution.

Hardware and Software

This is a list of hardware and software that is needed to implement this network solution for Tepe Services. Please note that additional research might change the list below to provide a better solution.

This project will consist of enterprise grade servers, routers, switches, IDS, IPS, firewalls and software.
Figure H: Pictured above is the new router/switch closet.

Figure I: Picture below is the new router/server rack.
For our storage server, our group has chosen to go with enterprise Qnap NAS. This was chosen over other products such as FreeNas due to a few reasons; hardware costs – if going the route of more expensive products, there would have had to of been budget cuts for other hardware that needed to be purchased. Second it’s incredibly light. It only takes up 64 MB once installed. Third, it works great with Active Directory. For our users and groups it was decided upon to use Active Directory because a solid database system that would allow authentication, a directory, policies, and several other windows components. Our network devices (routers and switches) it was decided upon to go with Cisco products simply because of stability reasons, the network has to be self-sufficient and reliable products are needed for that.

For the servers, it was decided purely based on an economic standpoint – Dell was chosen over HP due to the fact that HP servers are noticeably more expensive and the users don’t get much more than what they would by going with Dell. For our Web filtering device the company chose to go with Barracuda so that Tepe Services could better manage its employee’s use of company hours. The group will be working with management so that the filter can block everything that they feel should be filtered out, as well as trying to prevent malware/viruses/spyware from being accessed.

For security the company was looking between Cisco Firewalls and pfSense (an open sourced firewall/router). In the end it was decided upon to go with pfSense simply because of all the options it allows for us to take advantage. Some examples being; stateful firewall, Nat, Dynamic DNS, load balancing, etc.
For backups, tape backups will be used for the primary server, which will be running our AD. For all user data the company is going to push all data to the 4 TB NAS. The NAS has been set to do weekly backups of user data and Daily backups of AD, which are subject to change.

**Budget**

The budget below is for our hardware and software needs to complete our project. The two owners of Tepe Services approved the budget on October 25. The budget included $12,000.00 for the completion of the project. The table below shows the estimated costs of the project by the retailers. Please note that the grand total amount is far less than the budgeted amount of $12,000.00, which will give us some room for unexpected changes, or problems that might occur during the installation.

<table>
<thead>
<tr>
<th>Components</th>
<th>Quantity</th>
<th>Unit price</th>
<th>Total Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Server PowerEdge R1I</td>
<td>1</td>
<td>$1,600</td>
<td>$1,600</td>
</tr>
<tr>
<td>HP Server ProLiant G5 (Used)</td>
<td>2</td>
<td>$690</td>
<td>$690</td>
</tr>
<tr>
<td>Cisco 800 Series Router</td>
<td>1</td>
<td>$340.00</td>
<td>$340.00</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>1</td>
<td>$110</td>
<td>$110</td>
</tr>
<tr>
<td>Dell PowerConnect 2748 Switch</td>
<td>1</td>
<td>$230</td>
<td>$230</td>
</tr>
<tr>
<td>Qnap NAS 4TB</td>
<td>1</td>
<td>$960</td>
<td>$960</td>
</tr>
<tr>
<td>Surveillance cameras &amp; DVI</td>
<td>1</td>
<td>$780</td>
<td>$780</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>2</td>
<td>$730</td>
<td>$1,460</td>
</tr>
<tr>
<td>15 Windows CALS</td>
<td>15</td>
<td>$39</td>
<td>$585</td>
</tr>
<tr>
<td>Windows 7 Upgrades</td>
<td>5</td>
<td>$95</td>
<td>$475</td>
</tr>
<tr>
<td>Windows Office</td>
<td>4</td>
<td>$279</td>
<td>$1,116</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td></td>
<td></td>
<td><strong>$8,346</strong></td>
</tr>
</tbody>
</table>

*Figure J: Attached above is the budget.*
Schedule

The only time constraint that our team will be facing when deploying our network solution to Tepe Services is that they start to get very busy in April so most of the heavy work such as deploying the servers and network switches will have to be finished by that time. They will need to have access to the application server at that time so they can view all of their scheduling appointments and so that there service techs can view these appointments remotely. Below is a grant chart that has a clear plan on when different phases of the project are going to be deployed at the company’s office.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Q2, 2019</th>
<th>Q3, 2019</th>
<th>Q4, 2019</th>
<th>Q4, 2019</th>
<th>Q1, 2020</th>
<th>Q1, 2020</th>
<th>Q2, 2020</th>
<th>Q2, 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Prepare for Proposal/Presentation</td>
<td>June</td>
<td>July</td>
<td>August</td>
<td>September</td>
<td>November</td>
<td>December</td>
<td>January</td>
<td>February</td>
</tr>
<tr>
<td>1</td>
<td>Research/configure for network devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Order hardware &amp; software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Begin writing database application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Re-wire the entire building with CAT5 ethernet wiring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Route/Order Hardware &amp; Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Install Primary and Secondary Domain Controllers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Install &amp; Configure DHCP, AD, DNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Configure file shares</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Install Edge Router with Cisco Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Install switches and setup VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Configure NAP Device for employee storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Join computers to new Domain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Configure print server and printer drivers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Configure firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Lay wire for security surveillance cameras</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Beta test client database application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Install surveillance cameras</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Deploy database applications using AD for workstations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Add new jack to office rooms for network wiring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Setup wireless access points</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Setup employee &amp; guest wireless access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Install and setup bar codes with .390</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Setup VPI/verification access with edge router</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Setup weekly backup on NAS device</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Prepare administrator/maintaining tools on management server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Prepare access policies with legal team</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Train office employees on how to use new network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Prepare final report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure J: Attached above is the project timeline.

Problems Encountered

The first problem that was encountered was that in order to implement the new network, the entire building needed to have new wiring installed from the ISP closet to
the server room which was solved by running the wiring through the ceiling between the two rooms.

The next problem encountered was that we could not actively work on the network until at least 4-5 pm each day since the business was still running, if any changes to the network that would not allow the business to continue the next day, all changes must be reverted and the network restored and figure out a solution the next time we came in.

There were conflicts between the firewall server and the built-in firewall that configured on the cisco router we purchased. In order to get around this, ACL’s were created on the router to allow for certain traffic to get through unfiltered and then from there the firewall would filter the rest of the traffic.

There were issues with the clock-in system since the IP address on the box was set statically and there was no documentation on how to access the box to find out what the address was, so it had to completely reset and add it to the domain that way.

When management decided they wanted to have a monitoring tool put in place, it had conflicts with the cisco router where management could not see the usage statistics for some users but others it worked perfectly fine, in order to fix this we created a new ACL that would allow port forwarding on port 80.

While ordering the new hardware, there were issues with delivering it to the company. Some products were delayed several weeks for build time. Some were sent to the company and were faulty and had to be sent back and wait for another to be shipped to the company.
The firewall, pFense, and the Web filtering service, Squid, did not function well together at the beginning of the setup for some reason. The only solution was to keep uninstalling and reinstalling Squid in order for it to function properly and log/block traffic to websites.

EXSI was troublesome simply because it does not like legacy hardware and took a while to be configured around that and setup correctly. Some of the older hardware simply had to be upgraded in order to it to function with EXSI.

**Future Recommendations**

If this project were to be done all over again from scratch, the first thing that should be done is get all the information needed about the network first. User groups, software, hardware, figure out what’s in place currently that needs to be configured to work with the new network.

Due to time constraints, there was simply not enough time to do everything, but if there was more time, a database would be implemented for the company so that they could properly store all of their client information and contracts so that they could better manage their accounts. Secondly, upgrade all of the machines on the network to new PC’s but that was a money/time issue as well.

The plan for this project is the continuation of support and upgrading the network and helping them to scale the network for the upcoming expansion to the business that would allow for more office space, so that will need to be added onto the network.
Conclusion

The current network at Tepe Services was so crippled from the individual workstations to the old Novell servers, that this project will help grow the company in the future. The team believes with the number of solutions that our team will be addressing and with the added risk of problems arising when deploying this environment makes this a great senior design project. The real world problems that are being addressed for this company makes it even more valuable because they wouldn’t be able to afford to hire a network consultant since there isn’t a budget for it. Our team will complete this project and learn so much more hands on that will help us achieve jobs in the networking field using this experience from this project.

Some of the things learned from this project were that project management aspect was absolutely essential to successfully complete this assignment. If all relevant information had been properly gathered all of the information that was needed for the project at the beginning as well as proper risk analysis the group would have been better off and there would have not been so many errors while implementing the network with the pre-existing software.

This project helped us all around in terms of skills with network infrastructure, software deployment, security, and design. It also helped with system administration tasks as well as all of the network and system work that needed to be done. This project was the culmination of every core IT class, and then some, which tied everything together into one real world application so that we could actually see and learn how complete a project of this scope. By allowing our team to rebuild a network of this size from the ground up
gave us the real world experience to learn from our mistakes and progress forward. We would like to say thank you to Tepe Services for allowing us to take a chance with us.
Works Cited


