Networking Essay, Research Paper

For my independent study, I have created a network in my house. A network by definition are more than one computer that are linked together electronically via a protocol (common language) so the computers can communicate and share resources. This network improves the day-to-day life by adding value and usefulness to the computers. The processes and ideas that I have learned thru this experience can be applied directly into today’s rich electronic business environment.

Identifying the needs of the user is the first step for building a well-designed Network. A professional installation was needed to maintain the aesthetics of the rental house. Most of the wires are run in the attic and then down plastic conduit attached to the wall. The conduit is run all the way to the wall boxes where the Ethernet ports are located. Every wire is clearly labeled and included in an easy to read schematic of the house. This way future tenants will have the ability to utilize the network. Next, every room needed to have access to the network. In order to minimize the overall use of wires, hubs were placed in strategic locations. An 8-port 10/100-megabit auto-sensing hub is located in the computer room and a 5 port 10-megabit in the sound room. There, needed to be docking stations, so laptop users or visiting computers could easily plug into the network and utilize the pre-existing monitor, keyboard, and mouse. These are the basic needs that have been put into the design of the network.

Each computer setup is unique with certain strengths and weaknesses. The network takes advantage of the strengths of each individual computer and makes them available to all users. A network essentially expands the capabilities of each computer by increasing functionality thru resource sharing. In the house, there are a total of four computers and two laptops. Processing speed and an abundance of ram is not essential for a server with such low traffic. Thus the most antiquated computer was elected for this function. Between all the computers, we have several extra pieces of hardware such as a zip drive, CDRW, DVD ROM, scanner, and multiple printers. Each piece of hardware is dispersed between the computers.

There were several immediate efficiencies that occurred when the network went operational. The zip drive is located on the server while the CDRW is located on one of the individual workstations. Previously, if the need arose to burn some information stored on the zip disk to a CD, the individual computers were practically worthless for this task. However, with the network, one can map a network drive on the computer with the CDRW to the zip drive on the server. This allows information to be efficiently transferred from the zip drive to a CD. In addition, the server also has a scanner attached to it. The problem is that the server is too slow to handle sophisticated photo editing software. Now an image can be scanned on to the server and then a faster computer can be used to edit it. There are 3 different printers, each varies in quality, speed, and maintenance costs. The most expensive one is reserved for only making color photos, and the other two are used for everyday printing, one of which is much faster and has more reliable paper feeding. A user can easily choose a printer depending on their needs. This network takes full advantage of each computer through resource sharing which ads tremendous value for its users.

In Business it is important in any network to be able to restrict access to individuals private files or directories. Security would demand that not all users would be allowed access to highly confidential information. There is other information that would be made available to other users on a read only basis. The same is true of the users in my network. Microsoft developed NT to be very secure. Most of this security is devoted to protecting network resources and the filing system (NTFS). The administrator decides who gets access to which resources by setting up users and user groups. Each person is asked to choose a user name and password. Then the administrator identifies the needs and privileges of each individual user. Next the administrator grants users either full access, modify, change, read only, or no access at all to directories and resources on the network. In the house each roommate, trusted friend, and guest is given a user name and rights to the resources he/she needs. Roommates, as a profile group, have access to the Server’s C drive, which contains the core o/s. They are also given access to all directories on the D or storage drive except for the individual User and private directories. The User’s Folder has a directory for each user to store personal files on the Server. The read and write rights are given only to that user, so the data in that directory is secure. A Guest account is set up for anybody to use. This account is given minimal access to resources with no ability to adjust system settings or cause adverse affects.

There were four operating systems to deal with on this project. Two laptops and one of the PC’s use windows 98 while another pc runs 2000 Advanced server, and the server uses NT 4.0 SP 6 with a dual boot of Linux Red Hat 7.0. Microsoft developed windows 98 for the home user and did not include adequate security with the FAT32 filing system. When a user logs onto a machine utilizing the windows 98 o/s, they have access to all the information on that computer and have the ability delete, change, or modify directories. In any event the server still secures the rest of the network and only grants access to the pre-determined resources. The NT and 2000 machines can be set up to allow different levels of users access inside that machine, and also restrict rights to others on the network. On these operating systems A guest account would be denied most write privileges so they couldn’t accidentally delete important files. It is a security flaw in the network that cannot be fixed without upgrading the operating systems on machines that run windows 98.

Most businesses store their vital records in the form of digital data. Keeping this data secure is a key issue. Many problems may arise that can cause the loss or corruption of data. A virus attack, system crash, hardware failure, or a natural disaster are just a few potential problems that could cause loss of information and in turn devastate a company. It is imperative for a business to consider these possibilities and make sure they back up their data.

As college students living in the technology age, we too have lots of important data stored on our computers. This information ranges from term papers to financial records that would be devastating if lost. This is even a bigger worry with laptops as they go thru the daily rigors and abuse of being transported and connected to many different networks. It only takes one bad bump (over 14 to 17 G’s of force) to break a hard drive arm and/or data reading heads to render it useless. Possible virus threat, accidentally transmitted thru email, could corrupt a hard drive and render the O.S. useless and trash the hard drive. For all the above reasons we needed to put a system in place to back up all of our information. One of the benefits of the network is that backing up data is both fast and convenient. For example, the users in my network back up their data onto their user directory located on the server. Once a month, the user directory is burnt onto a CD. This back up is then stored in a fireproof lockbox, where it is guaranteed to be safe. Getting into the habit of such practices is imperative for today’s I.T. professional.

Connecting a network to the Internet can bring tremendous improvements in productivity, but not without posing major security issues. A network always has to be on the defense, making sure the information and systems that lie within are protected. Anybody can hack right into an unprotected network with just a little bit of knowledge. Once inside, a hacker can access confidential information, read, write, install a virus, or delete whatever he/she sees fit. In order to prevent such attacks over the Internet, a firewall needs to be installed. A firewall is powerful defensive software that blocks unauthorized intruders from entering a network. There are many ways to configure a firewall. Generally, a firewall locks down all ports except for ports being managed by secure communication programs, such as email. It also does not allow in coming request from the Internet for network resources. Sybergate Personal Firewall has been installed on the network to protect it from outside attacks. Once configured, I tested it at http://scan.sygatetech.com. It scans all the ports and tries some Trojans to ensure that the network is protected.

Overall I view the project as being successful. The network is up and running and all the users are able to be more productive. The ability to access all the different peripherals is a real money saver for the budget conscious college student. Personally I found the setting up of the security features and the installation of the software to be the most rewarding part of the experience. My next step in my ongoing process to improve the network is to install and configure Apache. This gives a unique opportunity to see first hand how Unix manages a network as compared to Windows. I have learned marketable job skills that I intend on applying in the interview process. I am even now considering becoming a network specialist as a career.