The Office Network

Section Four

Infrastructure builds stability

Introduction

GENERAL

In this section we look at the pre-planned work environment. What you do before you move in is just as important as after you have all the equipment in place. By this I mean taking the time to have the cabling installed correctly, planning your network topology, providing a secure place for data resources and developing a strategy for troubleshooting problems. Along with all that, this environment will be built for scalability and centralized administration.

Once you expand beyond the five user network, it becomes cost effective to look at the server option to balance the administrative load and ensure a structured, well planned growth process that will keep you on track as your business booms. All of the stuff you learned in the previous sections will be the foundation for what you do here. The key is to understand what is necessaries for the server to provide. Paying too much for server software could be damaging to the bottom line. Not centralizing the right administrative tasks could make the workload unbearable.

Our scenario covers office networks from five to twenty-five desktops (or laptops). We limit the scalability to twenty-five so that we can limit the amount of servers to one. This helps us to see the growing responsibility for a server solution and when it is wise to add another server to the mix. Modern server hardware has great potential but you must understand when your placing too much of your business into one resource (like putting all of your eggs in one basket). Balancing your TCO[87] with a well defined DRP[88] will make your network work for and not against you.

[87] Total Cost of Ownership

Planning and Development

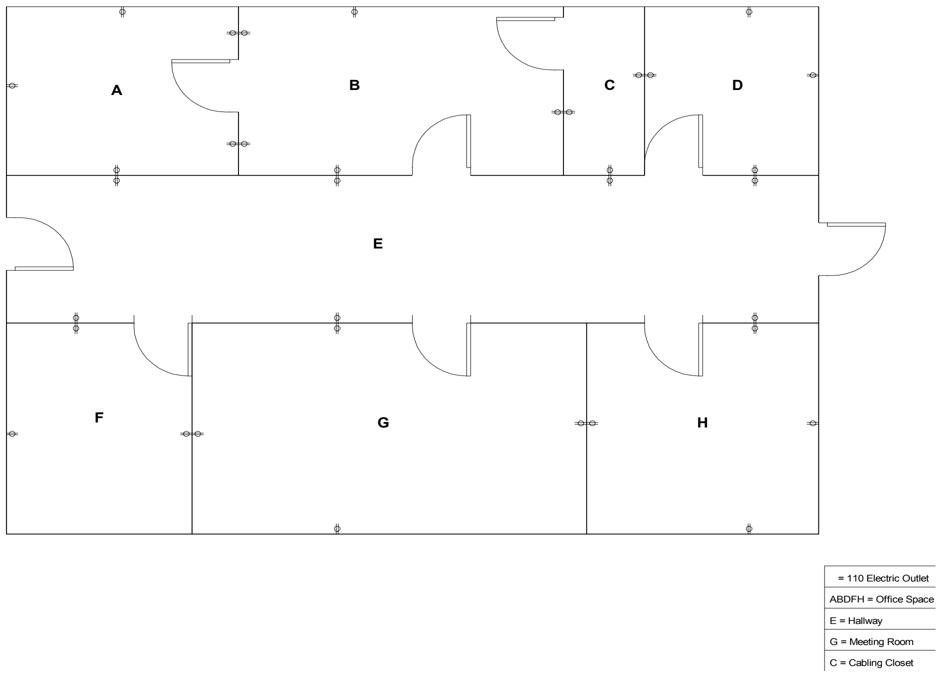
THE WALK THROUGH

Your initial walk through of the office space should help you to establish the topology and conditioning of your network. As we discussed earlier, you can install either a wireless or wired network topology -- cost and security will help you to make the decision. You may wish to combine both wired and wireless. As you walk through check to see if their have been previous network installations -- if so then you may wish to replicate the cabling layout using the same port holes and maybe (but I don't suggest it) the pre-laid cable itself. I always recommend that you have new cable installed mainly to ensure that there are no hidden problems. When people vacate their office space, they are usually not very careful with the cabling they leave behind.

ELECTRICITY

Check the power outlets using a power strip that tests grounding -- if your outlet does not have proper grounding your computer equipment could be damaged. Note any problems that you find. Talk to the landlord and obtain a layout of electrical circuits (usually they are 20 or 40 amp circuits that include several rooms). Since each computer (monitor and all) take up about 2.0 amps you will not want to have more then 9 - 18 computers per circuit. If you add a printer or other peripheral to the mix be sure to subtract those amps as well. If you can create a diagram of what rooms are on what circuits, that will help to quickly resolve power issues.

FIGURE 4 - 1. **Floor Plan**



[88] Disaster Recovery Plan

In our office each room is labeled by alphabet. The following Circuit Plan is given:

- **Circuit 1** = A, B, C (20 Amps)
- **Circuit 2** = D, E (20 Amps)
- **Circuit 3** = F, G, H (40 Amps)

With this is mind, it becomes apparent that you can have twice as much equipment on circuit 3 then any other circuit. It would be wise to plan for that before you install equipment. You should also take in any site code information (such as limitations on extension cords, etc.). Remember that lighting, space heaters, printers, even electrical pencil sharpeners should be considered when planning the use of electrical circuitry and your network.

Look for a secure place to locate your sensitive hardware (such as server and storage). Pick a place where it would be difficult to break in but with good ventilation. In our floor plan we have chosen room "B" for this purpose. Room "C" will be used for our wiring closet.

THE CABLING CLOSET CONFIGURATION

Since 100BaseT provides significantly greater bandwidth (and is fairly inexpensive), it has become a standard for small and large network installations. Try to locate a central closet space (that can be locked) to place your patch panels, router and switches. This closet space should have reasonable ventilation and an empty wall.

FIGURE 4 - 2. Back Wall of Wiring Closet

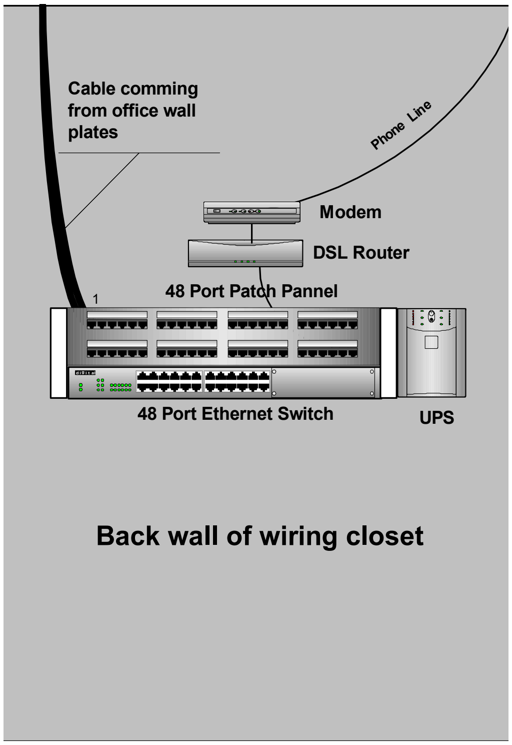
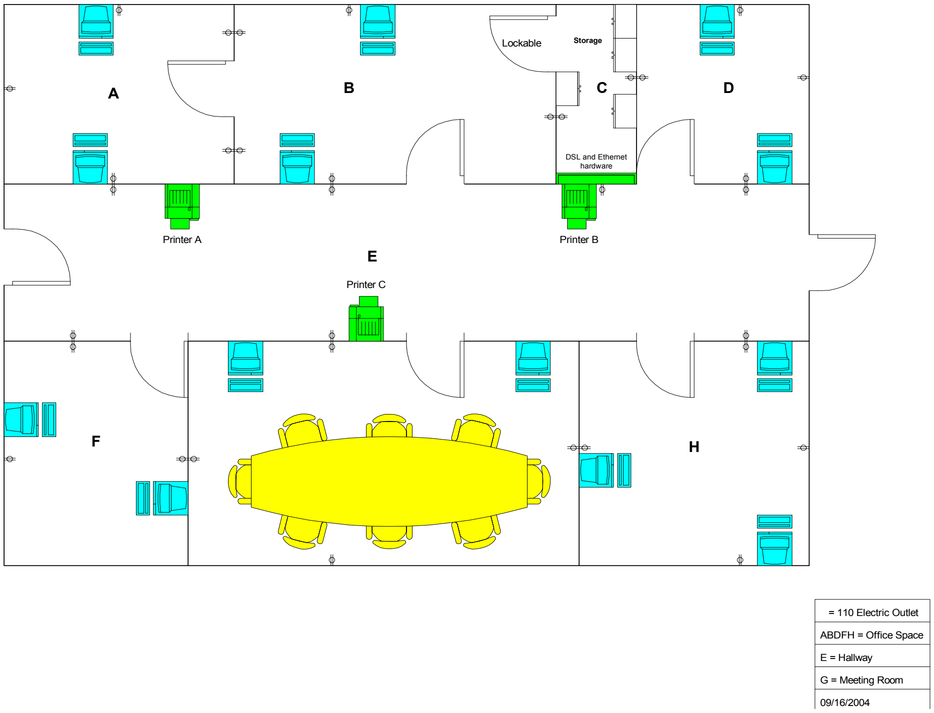


Figure 4 -2 displays what you might see in a well laid out cable closet. The DSL modem, router and ethernet switch get their power through a UPS which conditions electricity while providing emergency power to all devices. All of the cables from each of the offices will merge into the patch panel (ports 1 through 40). Ports 41 through 48 should be reserved for special connections (such as router, server, and printer patch panel connections). In this example we are setting our initial scalability for up to 40 office ports and 8 special connections.

Look for a false ceiling (that is the logical place to run the network cabling). Check to make sure there are no show stoppers (such as physical firewalls that won't allow you to run cabling).

FIGURE 4 - 3. **Floor space with equipment**



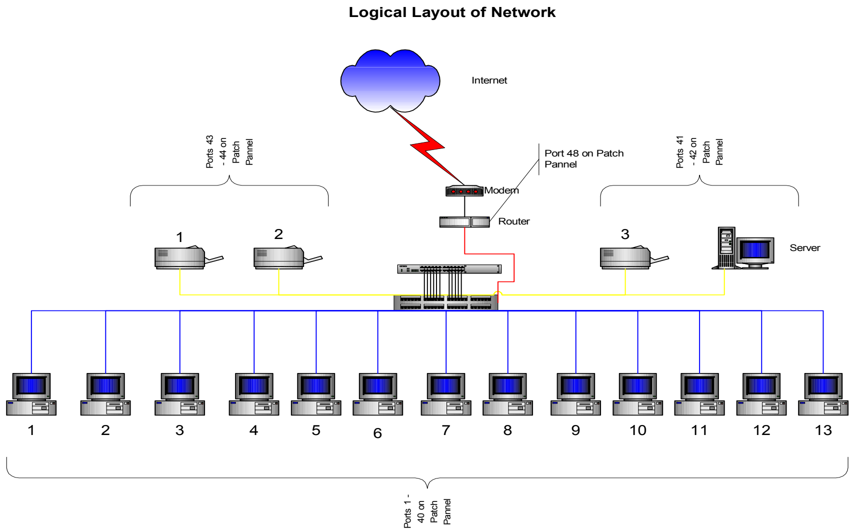
As we look at the layout in figure 4 - 3, we have thirteen workstations, three printer and one router connection equaling seventeen ports. It is a good policy to have at least two ethernet ports associated with every desktop work area (or in this case twenty-three ports). This lets users bring in their laptops and work with more then one computer if need be. If we set up eight ethernet ports for the conference room (mounted underneath the table for easy access) we end up with a total of thirty-five ports accounted for. This leaves us with thirteen open ports for expansion.

Rooms B and C have been set aside for network administration and computer support. There should be additional Ethernet ports installed for building and repairing workstations, adding servers and testing new technologies. It would be advantageous to add four to five additional Ethernet ports for this purpose.

NETWORK TOPOLOGY

Network topology should best reflect the physical layout of the network and its' users.

FIGURE 4 - 4. **Network Topology**


Logical Layout of Network
Internet
Ports 43 - 44 on Patch Pannel
Port 48 on Patch Pannel
Ports 41 - 42 on Patch Pannel
Modem
Router
1
2
3
Server
1
2
3
4
5
6
7
8
9
10
11
12
13
Ports 1 - 40 on Patch Pannel

To help in the troubleshooting process patch cables have been color coded as follows:

- **Red** - Port 48 (critical connection for Internet connection)
- **Yellow** - Ports 41 - 47 (special connections for shared devices)
- **Blue** - Ports 1- 40 (general purpose connections for workstations and laptops)

Using this color coding for patch cables helps to troubleshoot connections by establishing the level of importance for connections. If you disconnect the red patch cable all access to the Internet will be lost. If you disconnect a yellow patch cable everyone will loose connection to a shared device. And if you disconnect a blue cable a single device (workstation or laptop) looses connection to the network. Simple things like this help to quickly resolve problems when the going gets tough.

There are two patch cables associated with each connection:

1. Workstation to wall plate
2. Patch Panel to switch

The workstation patch cord is usually 10 to 15 feet in length while the patch panel patch cable should be 1 - 3 feet in length. All patch cables associated with a particular connection should follow the same color code. All Patch cables associated with patch ports 1 - 40 should be blue, while special ports should be either yellow or red. It is fine to use whatever color scheme you find works best for you as long as you are consistent.

FIGURE 4 - 5. The Cable Connection

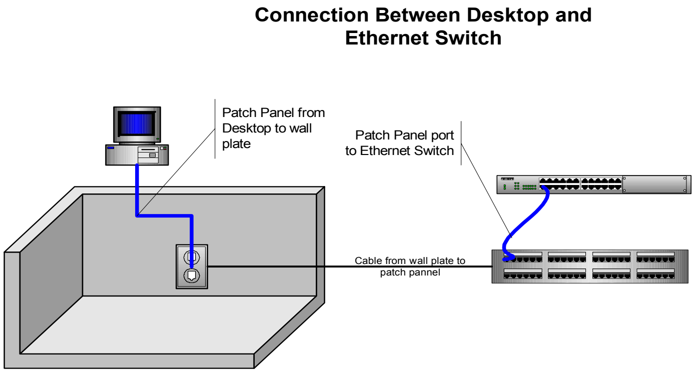

Connection Between Desktop and Ethernet Switch
Patch Panel from Desktop to wall plate
Patch Panel port to Ethernet Switch
Cable from wall plate to patch pannel

Figure 4 - 5 represents the cable configuration for a workstation on port 1.

BETWEEN THE PATCH CABLES

Have professionals install the cables between wall plate and patch panel. The amount of time running cable between rooms through the false ceilings and hollow walls is dirty hard work. You must not tweak cabling (bind or twist) or else it will have problems. Each connection must be tested with expensive equipment (cable testers) to ensure that it is working correctly. Finally the best reason to have someone else do the job is so that you can hold them accountable for if it's not done right. Always get a list of prior customers to make sure that there is a history of good work -- a bad cabling job is hard to troubleshoot and even more difficult to get fixed.

You want to make sure that there is a labeling strategy that is easy to understand and scalable in case your business grows. If you are on a single floor of a multi-floor building, use this as a standard to build off of.

The standard I will use in figure 4-6 is as follows:

- **Room 100 (special connections)**

  Wall Plate = 100-1, 100-2, 100-3, 100-4, 100-5, 100-6

  Patch Panel = 41, 42, 43, 44, 45, 46
- **Room 101**

  Wall Plate = 101-1, 101-2, 101-3, 101-4

  Patch Panel = 1,2,3,4
- **Room 102**

  Wall Plate = 102-1, 102-2, 102-3, 102-4, 102-5, 102-6, 102-7, 102-8, 102-9, 102-10, 102.11, 102-12

  Patch Panel - 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
- **Room 103**

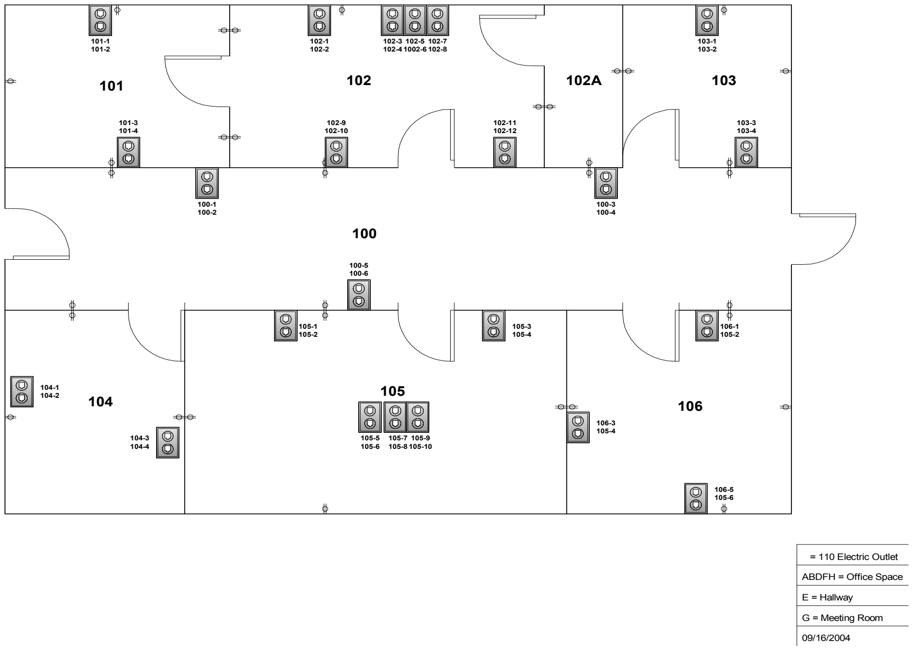
  Wall Plate = 103-1, 103-2, 103-3, 103-4

  Patch Panel = 17, 18, 19, 20

- **Room 104**
  Wall Plate = 104-1, 104-2, 104-3, 104-4
  Patch Panel = 21, 22, 23, 24
- **Room 105**
  Wall Plate = 105-1, 105-2, 105-3, 105-4, 105-6, 105-7, 105-8, 105-9, 105-10
  Patch Panel = 25, 26, 27, 28, 29, 30, 31, 32, 33, 34
- **Room 106**
  Wall Plate = 106-1, 106-2, 106-3, 106-4, 106-5, 106-6
  Patch Panel = 35, 36, 37, 38, 39, 40

Here is our example again.

FIGURE 4 - 6. Wall Plate Labeling



If at all possible, make diagrams and keep them available when you need to troubleshoot your network -- the more information the less confusion. Most of the time you can obtain diagrams of the office space from your landlord -- make copies of these and draw what you plan to do on those copies. Labeling is away the right first step but having diagrams will help to understand the labeling when your network begins to get large and the labeling becomes more complicated.

The patch panel ports would have the same labeling as their companion wall plate ports.

TABLE 1. Patch Panel Labels

101-1	101-2	101-3	101-4	102-1	102-2	102-3	102-4	102-5	102-6	102-7	102-8	102-9	102-10	102-11	102-12	103-1	103-2	103-3	103-4	104-1	104-2	104-3	104-4
X		X		X								X		X		X		X		X		X	
105-1	105-2	105-3	105-4	105-5	105-6	105-7	105-8	105-9	105-10	106-1	106-2	106-3	106-4	106-5	106-6	100-1	100-2	100-3	100-4	100-5	100-6		Router
X		X								X		X		X		X		X		X			X

The “X” in each of the boxes represents ports that will have live connections (workstations will be connect on those locations). As you can see there is a lot of open (available) ports, but all (excluding one) of the patch panel ports are wired to wall plates or to the router. You should label each end of each patch cable connected to the patch panel as well -- so that you can follow the connection to the Ethernet switch.

Planning the labeling of ports is as important as labeling the ports. Each system administrator has their own way of looking at the distribution of resources. Coming up with a labeling scheme that will work for the current system administrator as well as their replacement will help to keep things going even when the members of the team change. Having all of this well documented is not just a good idea -- it’s essential to the wellbeing of your business future.

PHONES

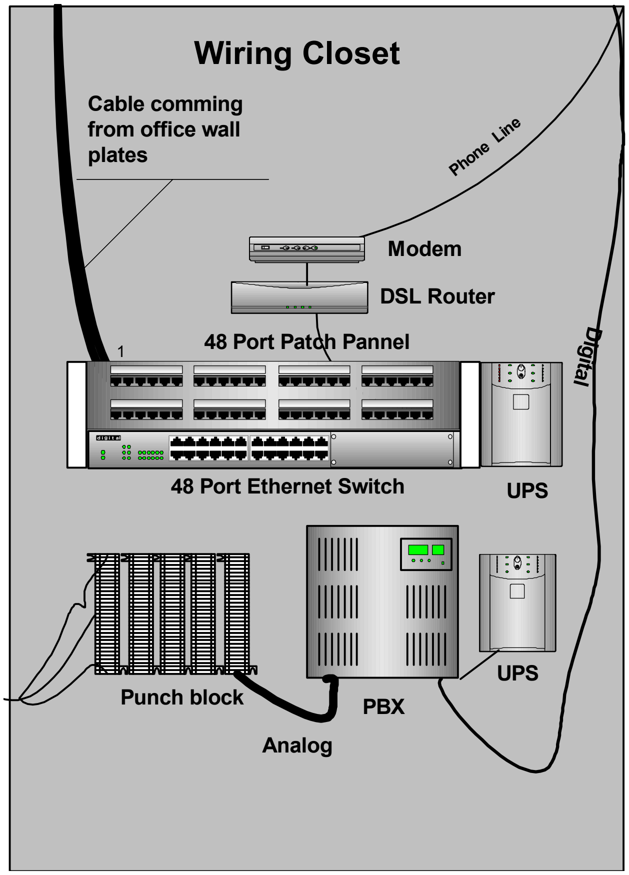
Phone lines are either analog or digital. Analog phones are also known as POTS (Plain Old Telephone System) the kind you find in the average home. The connection is usually RJ11. Analog lines are required for facsimiles, modems, etc. It is a good idea to limit the amount of analog lines to a minimum so that you can get the most cost effective digital line possible.

Digital phone lines are usually part of a PBX[89]. These lines use RJ45 connectors, programmable phones and a menuing system. The cost of phone lines are reduced when groups are bundled together through a PBX. Usually a phone contractor leases, sells or provides a service contract that includes the PBX hardware, phones and digital phone connection. Many times small businesses Buy T1 lines and split them so that they provide both Internet access and phone line services. This part of the networking scheme

[89] A PBX (private branch exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

gets complicated quickly and cost a lot. If you are not experienced in “provisioning[90]” a PBX you should find a third party to help you generate the contract between you and the phone company.

FIGURE 4 - 7. **PBX and Punchdown Block**



The PBX converts digital signals from a T1 or fractional T1 line to a standard punchdown block commonly used for standard phone lines. From the punch block the lines are ran to wall plates much the same as the network cable. Since the PBX lines use the same CAT 5 cabling as your computer network it is often the case that both lines are ran at the same time to wall plates next to the network wall plates. Phone wall plates should be labeled much the same way as the network wall plates. The PBX offers all of the frills that modern phone lines provide - menuing, call routing, messaging, and voice

[90] In general, provisioning means “providing”. In telecommunications terminology, provisioning means providing a product or service, such as wiring or bandwidth. The term has a number of varied meanings when used in telecommunications: 1) Providing telecommunications service to a user, including everything necessary to set up the service, such as equipment, wiring, and transmission. 2) Used as a synonym for *configuring*, as in “Telecommunications lines must be correctly provisioned to work with the customer's equipment and enabled for various options the customer has chosen.”

mail. You should always gauge the type of PBX you plan to use by the potential size your business can grow in the location your in. If at all possible try to get a contract that provides the equipment as a service (purchasing a PXBX is expensive and looses its' value quickly. An alternative to the PBX is voice over IP. This requires an expensive switch and some extra hardware -- for our little network this would not be cost effective.

THE SERVER

What makes a computer a server?

- Multi-processor capability
- Improved capacity for high-speed RAM
- High-end storage (usually a set of SCSI RAID devices)
- Backup Device (tape drive)
- Redundant power
- Server specific operating system

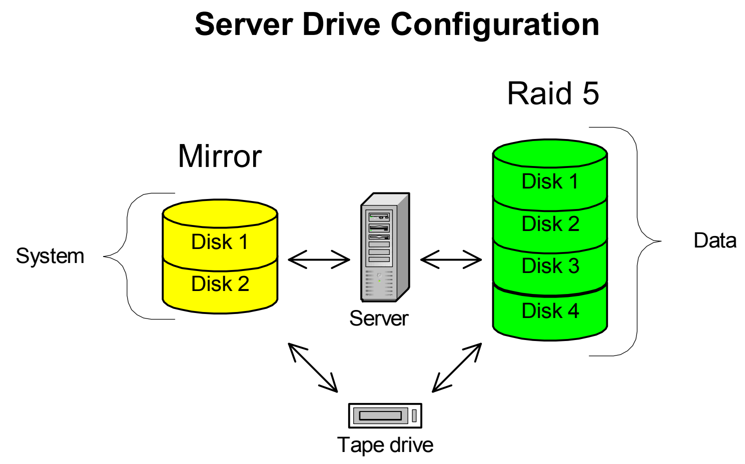
The key is to have a computer that can handle multiple users well. Servers share resources, and those resources require power. Server software vendors often provide guidelines as to what is necessaries for hardware to meet the needs of a network.you should take what they suggest and add a little to be on the safe side. You need to define what is going to be shared and how many people will access those shared resources and then go to the vendor's web site and get an idea of what will meet your office needs.

In our example office environment we have chosen to use networked printers (printers that have an Ethernet device installed) so that we can maximize availability of printing services and minimize the dependency of printing on any one computer. As we have seen in previous sections, printing takes up a lot of resources and can effect the performance of the print server (which world either be the server itself or another workstation). This also frees up the printers to be located liberally throughout the office space.

I believe that a servers first responsibility is to provide centralized authentication and account management. Secondly, it should act to either manage or provide access to data storage. Thirdly, a server should act to simplify shared security (such as antivirus management and Intranet services). Only after all of the other functions should the server be required to provide print queue services.

Along with all of the other resources offered by the server, a forwarded DNS database would be used to offer a local naming resolution in case Internet access fails. When proposing a network strategy it is vital to look at many possibilities. Since the Internet access is just one of the single resources that could fail and cause potential havoc for your local network, it is imperative to have a local repository for some of the most necessary resources (in this case DNS) so that the network continues operation even when the Internet is down.

FIGURE 4 - 8. **Drive Settings**



PRE-DEFINE DISK CONFIGURATION

Before you can build OS and application settings, you need to build the hardware configuration. You should try to separate system files from applications and data. Figure 4-8 represents a common server configuration where the system drive is mirrored so that when a drive failure occurs you have little to no immediate downtime. You also build a larger disk set (also know as volume) for applications and user data (using a RAID 5 configuration). Both system and data volumes can be backed up by the tape backup resource. While it may not be imperative to back up system files it is essential that you back up user data and application settings -- these are files that will be almost impossible to restore any other way. Hardware RAID is also essential. My experience with software raid has not been totally positive while I have never had problems with hardware raid.

HOT SWAP

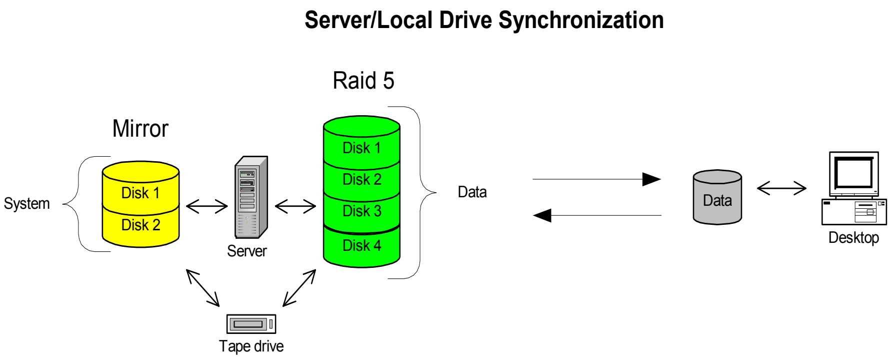
It is best to have what is known as "hot swappable[91]" hard drives so that you can replace drives without having to shut the computer down. This helps to limit unscheduled down time and possible network panic. People are more willing to appreciate scheduled downtime as opposed to an emergency condition -- this enforces a sense of confidence in network operations. Every time someone looses confidence in your network administration, you gain a potential advisories when it comes time to ask for additional funding. Keeping your down time to a minimum is the key to building goodwill throughout your company.

[91] A hot swap is the replacement of a hard drive, CD-ROM drive, power supply, or other device with a similar device while the computer system using it remains in operation. The replacement can be because of a device failure or, for storage devices, to substitute other data.Hot swapping works by providing a rack or enclosure for the device that provides an appearance to the computer's bus or I/O controller that the device is still there while it's being removed and replaced with another device. A hot swap arrangement is sometimes provided where multiple devices are shared on a local area network. Hot swap arrangements are sold for both SCSI and IDE hard drives. Hot swap versions of a redundant array of independent devices (RAID) are also available.

SYNCHRONIZATION

Having users synchronize their local data folders with a server folder is yet another move towards securing their data. This process keeps data on both server and workstation. If the network is down (for any reason) the user can continue working on their data. When the network is available again, changes made in data from the workstation is up dated to the server folder. If the user has a laptop and travels, this allows that person to work on data while away and when they connect to the server data it updated automatically.

FIGURE 4 - 9. User Data Synchronization



The more convenient you can make the synchronization of data the better. The more processes you put in place to secure data the better you will look when disaster strikes.

It is just as important to protect against hardware failure as it is for user mischief. Unhappy users can take their displeasure out on important data. Having tape backups and keeping them in a secure place helps to protect against the disgruntled worker. It makes sense to put your backup tapes in a fire proof safe (better yet somewhere off site). When you run your back up process make sure no one can be logged onto the server so that no files are left out of the backup process -- an open file will not be backed up.

Locking out user account access in the evening ensures that all files will be closed when the backup occurs. You should be careful when locking out administrator accounts for any reason -- you never know when you'll need it. Always have an alternative administrator account as a backup account for when you find the need (keep an eye on both accounts).

I suggest that you lock out user accounts between the hours of 1:00 am through 4:00 am unless your business practices can not support that schedule. Night time is the preferred time for hackers to break in. If they can get in when no one is around they can do the most damage.

You may wish to disable Internet access during this time as well, but you should always leave a back door (a secure modem on a workstation somewhere that no one knows about) so that you can log in remotely and start things back up if an emergency requires. Limit knowledge of any backdoors to your boss and do your best to maintain that secrete. Also practice emergency operations occasionally so that the process is dependable.

SERVER SOFTWARE INSTALLATION

Unfortunately, new network administrators are quick to use defaults when installing an operating system. They don't want to forget anything important. The problem with this is that in installing the default settings, you open your server to attack. Default settings for a server always install more then you need and open ports (remember ports?) that are not required. The rule of thumb is to only install those resources you need for a server to to its job. You should also limit any applications that are installed to only those applications that manage the shared environment.

Applications

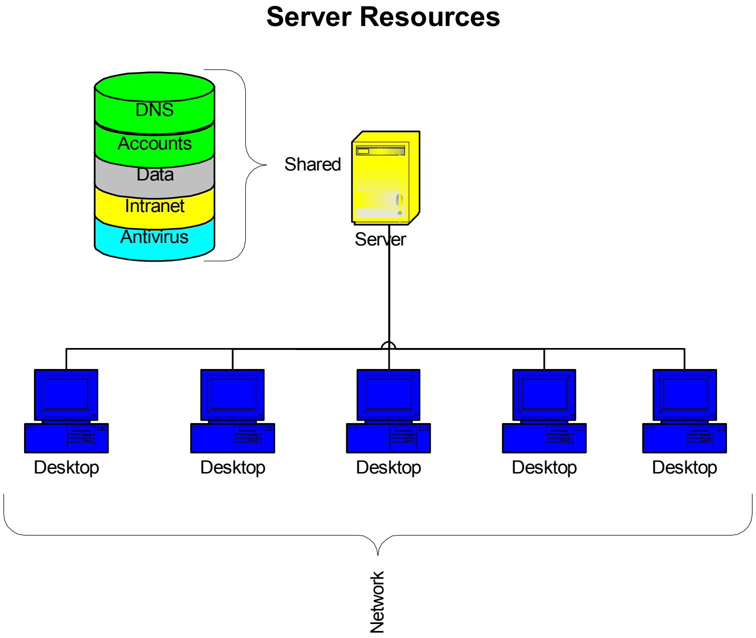
- DO NOT LOAD OFFICE APPLICATIONS on the server!
- Don't use a server as a workstation.
- Limit server utilities to a minimum.

Security

- Don't leave a server in an open access room
- Don't give users administrative access to the server.
- Remove anonymous access (FTP, etc.)
- Force user authentication to gain access to server resources.
- Lock the desktop when you are not using the server.

SERVICES

FIGURE 4 - 10. **Local Services**



Services are applications that run within the confines of the operating system and enhance its versatility. For instance the DNS service allows a server the ability to resolve local and/or remote computer names. Account management is a built in service that allows the administrator of the network to create and manage user accounts. Disk sharing is also a built in function of any server (and workstation). Web serving is an added function (service) of most server operating systems. Finally (for this example) antivirus software is an added (third party) service that must be purchased separately from the operating system. The more services you have running, the more your system is made available. Always keep the number of services to a minimal.

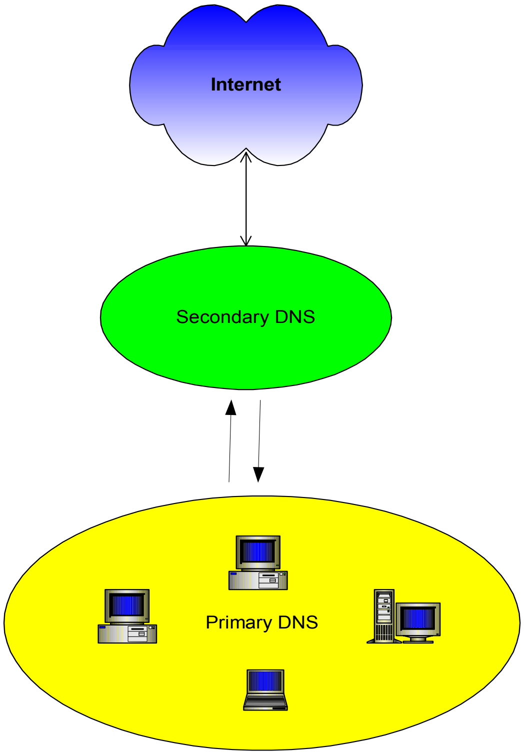
DNS

In figure 4 - 11 there is a definite separation of name resolution:

- **Internal** - local workstations resolve their host names quickly because there is a smaller search parameter (only the local network workstations and devices).
- **External** - resolves Internet host names only when required.

This process promotes speed and security by defining communication based on local and external boundaries - less data traffic between the primary DNS (a slower communication media (DSL)) and secondary DNS a (larger communication media (Ethernet or 100BaseT)). Basic planning such as this will become more and more important as the network grows.

FIGURE 4 - 11. **Primary/Secondary DNS**



DHCP

DHCP is offered through the router. A secondary (local) DNS can be setup to provide primary name resolution with ISP DNS as a secondary source. DHCP can incorporate both DNS sources automatically so that a hiarchy of host searching can enhance internal network performance. This speeds local name resolution while offering Internet name resolution when required. The end result is a fine-tuned local environment that supports external resources.

IP ADDRESSING

Speaking of DHCP, it becomes important to set limits for the scope of DHCP in our office network so that we can define static[92] IP addresses. Shared devices such as servers, printers and routers work best with static IP addresses so that they can be located quickly and without ambiguity. DNS make a static addresses mandatory for the server providing that service. To keep with our office network design the following DHCP scope would help to further tighten local network performance and also increase security by means of limiting dynamic distribution of IP Addresses.

Lets look at subnetting a little closer:

There are three types of IP network addresses:

- **Class A** - Large - 16,000,000+ computers
- **Class B** - Medium - 65,536 computers
- **Class C** - Small - 254 computers

The subnet mask is used to limit the search for hosts by the set of numbers assigned to a particular IP Class.

TABLE 2.

Address Class	Dotted Decimal Notation Ranges
A (/8 prefixes)	**1**.*nnn.nnn.nnn* through **126**.*nnn.nnn.nnn*
B (/16 prefixes)	**128.0**.*nnn.nnn* through **191.255**.*nnn.nnn*
C (/24 prefixes)	**192.0.0**.*nnn* through **223.255.255**.*nnn*

An IP address is divided into four Octets[93] (nnn.nnn.nnn.nnn) whereas the network number is defined by a class:

- **Class A** - 255.0.0.0 - 11111111**.00000000.00000000.00000000**
- **Class B** - 255.255.0.0 - 11111111.11111111.**00000000.00000000**
- **Class C** - 255.255.255.0 - 11111111.11111111.11111111.**00000000**

[92] In general, *dynamic* means *energetic, capable of action and/or change*, or *forceful*, while *static* means *stationary* or *fixed*. In computer terminology, *dynamic* usually means *capable of action and/or change*, while *static* means *fixed*.

[93] In computers, an octet (from the Latin *octo* or "eight") is a sequence of eight bits. An octet is thus an eight-bit byte. Since a byte is not eight bits in all computer systems, *octet* provides a non ambiguous term.

Class A networks (where 1- 128 is the network and nnn.nnn.1 would be the host number) will search a larger number of computers (16,000,000+) to locate a specific computer. Further, there can be more computers in that network unaccounted for (possibly not authorized to be part of that network). Class A networks are usually broken down into smaller (more manageable) networks so that the search time is decreased -- we will talk about this later.

Class B networks (where 128.nnn - 191.nnn would be the network number and nnn.nn1 would be the host number) will search a smaller number of computers (65,000) to locate a specific computer. Still a large number but more manageable. This environment would be found in branches of larger networks or medium size businesses.

Class C networks (where 192.nnn.nnn - 223.nnn.nnn would be the network number and nn1 would be the host number) will search an even smaller number of computers (254) to find a specific computer on the network. Currently we are using a Class C license (192.168.1.n).

SUPERNET

The key is to minimize the search to a reasonable size (allowing for growth of the business) so that computers can communicate with each other in the quickest manner. We can reduce the search path even smaller by dividing our class C network into a supernet[94].

In a class C license the subnet mask would normally be 255.255.255.0 (leaving the search scope to 254 possible computers in the local network). Since we have limited our network to 48 computers so why not refine the subnet mask (and network search scope). If we set the subnet mask to 255.255.255.*192* we limit the search scope to *64* hosts (*please see table 3) - which increases network performance and reduces the number of local IP addresses. If we set our DHCP scope (limiting the amount of dynamic IP addresses to 40 - the number of possible hosts ports available on the switch) we can use the rest of the IP addresses in our subnet for static addresses.

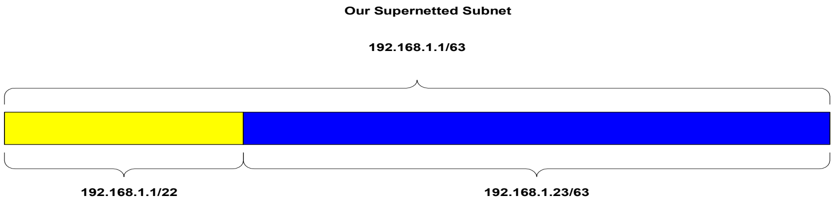
Our local network becomes

- **Subnet range** - 192.168.1.*1* - 192.168.1.*64* (IP addresses in the local network)
- **Static addresses** - 192.168.1.*1* - 192.168.1.*22* (IP addresses for servers, printers and the router)
- **Dynamic Addresses** - 192.168.1.*23* - 192.168.1.*64* (IP addresses for workstations on the network)

[94] Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. The original Internet Protocol (IP) defines IP addresses in four major classes of address structure, Classes A through D. Each class allocates one portion of the 32-bit Internet address format to a network address and the remaining portion to the specific host machines within the network. Using supernetting, the network address 192.168.2.0/24 and an adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23. The “23” at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses. Supernetting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.

Figure 4-12 graphically represents our supernetted subnet.

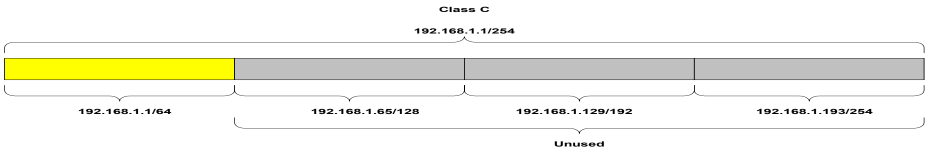
FIGURE 4 - 12. **Supernetted Subnet**



There are four supernets in our class C subnet (see figure 4-13):

- 192.168.1.1/64 (used by our network)
- 192.168.1.65/128 (unused)
- 192.168.1.128/192 (unused)
- 192.168.1.193/254 (unused)

FIGURE 4 - 13. **Available IP Addresses**



If someone sets a static IP address outside of the 192.168.1.1/64 (say 192.168.1.68), that IP address will not see the other IP addresses. This has advantages in that if you have an accounting system that you do not wish others to see or touch, you can put that workstation outside of the common supernet address scope. This protects you data from inside attack.

If you want to supernet your network here is a table that may help:

TABLE 3. **Supernet Cheat sheet**

CIDR prefix-length	Dotted-Decimal	Number of Individual Addresses	Number of Classful Networks
/13	255.248.0. 0	512,000	8 - B or 2048 - C
/14	255.252.0.0	256,000	4 - B or 1024 - C
/15	255.254.0.0	128,000	2 - B or 512 - C
/16	255.255.0.0	64,000	1 - B or 256 - C
/17	255.255.128.0	32,000	128 - C
/18	255.255.192.0	16,000	64 - C
/19	255.255.224.0	8,000	32 - C

TABLE 3. Supernet Cheat sheet

CIDR prefix-length	Dotted-Decimal	Number of Individual Addresses	Number of Classful Networks
/20	255.255.240.0	4,000	16 - C
/21	255.255.248.0	2,000	8 - C
/22	255.255.252.0	1,000	4 - C
/23	255.255.254.0	512	2 - C
/24	255.255.255.0	256	1 - C
/25	255.255.255.128	128	1/2 - C
***/26**	**255.255.255.192**	**64**	**1/4 - C**
/27	255.255.255.224	32	1/8- C

SUMMARY

While all of this can be a little bit much for the beginner, taking things slowly and setting up a list of things to do (and finishing each item one at a time), the planning and development phase can be accomplished. Knowing that as each item is done, you will not have to go back and do it again -- that moves you one step closer to completion. Here is the list of things to do:

1. Assess the office environment (get floor plans and draw on copies of the floor plans)

   - power (make sure you don't overload the circuits)

   - lighting (make sure that the lighting is good enough for your people to work in)

   - location of resources (printers, server, switch, router, PBX)
2. Stage where the wiring closet will be and how many ports will be needed (always double the amount).
3. Contract the cabling between wall plates and patch panel. (get three or more quotes from outside sources and have the contractors test each port completely and in front of you).
4. Contract the installation, servicing and maintenance of the PBX (keep a few POTS lines for one modem and any faxes and get a third party to act as a consultant in evaluating potential telephone companies).
5. Have a naming and color coding strategy for ports and resources.
6. Define the services you'll provide with your server and network appliances.
7. Separate local data traffic from remote by establishing an internal DNS.
8. Create an IP strategy

   - Supernet your internal IP scope.

   - Define your static (shared devices such as printers, servers, router, etc.) and dynamic (workstation and laptops) IP ranges.
9. Document everything (save any diagrams, receipts, contracts, e-mail, etc.).

Maybe number nine should be at the end of each line in this list. It is so easy to loose documents and the ones you misplace are always the ones you need most.

Administration

GENERAL

Even though our network is small, it has the functions and design of a larger network. Along with the physical and logical network design (as described in the planning and design phase) must come the administrative strategy that will help to maintain security and stability. This strategy must look to the future and include growth (both in personnel and in services). There are several main areas of responsibility:

- Software installation
- Licensing management
- System inventory
- Procurement/repair
- Account administration
- Security
- Resource scaling
- Documentation
- Infrastructure management
- Training
- Disaster recovery
- File system management

SOFTWARE DISTRIBUTION

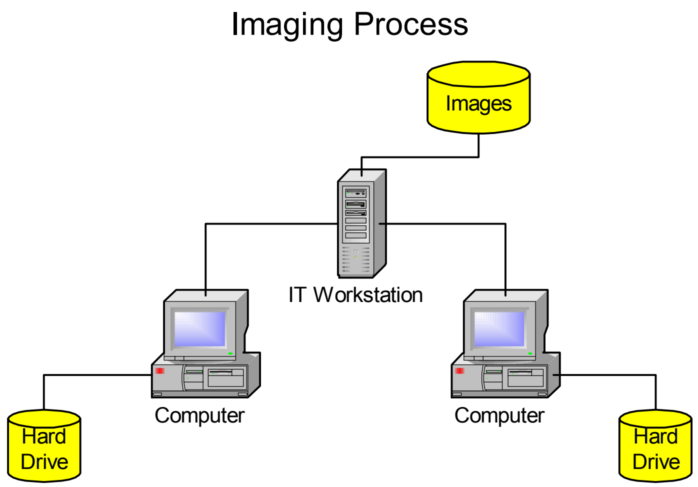
The installation and distribution of software for workstations and servers is one of the more complex duties of an administrator. You are essentially between a rock and a hard place because you're responsible for keeping things running effectively but you don't usually have the authority to say no when someone requests software that may make their systems less stable. You are also required to keep users from installing software off a web site until testing it with your workstation software configuration. Setting up guidelines and posting them on the Intranet[95], keeping your network community informed is a never ending process - but one that pays off again and again.

Usually the network administrator creates a workstation with all of the software that everyone will need. This workstation is tested to make sure that everything works well with the network. This workstation is then imaged using special software that takes a snapshot of the files on that computer and replicates it on other computers.

Every time a computer is upgraded, an image of that workstation is made so that no data is lost. a copy of that image is placed on the new computer and data files extracted. While there are other ways to do this process, imaging a hard drive is a cost effective method for small businesses. We will look at other options that are more dynamic and cost effective for larger network installations. What you should be concerned with here is that images are made and standards are enforced as best they can be.

[95] An intranet is a private network that is contained within an enterprise. The main purpose of an intranet is to share company information and computing resources among employees.

FIGURE 4 - 14. **Imaging Station**



The imaging process takes a file from the image server (source) and expands it onto the new workstation (target). This process is fairly easy to learn and inexpensive to impliment. The time line to image a workstation depends on the bandwidth available and the size of the image being transferred.

LICENSING

Licensing software can be time consuming and difficult when software is purchased through other department budgets. It is to your advantage to require all software purchases to go through the network administrator -- this gives you time to test the application and ensure that it works like it should. It also gives you the opportunity to build custom installation packages that brand your companies information on the software so that if someone takes the software off site it will carry the company ownership with it.

Never give out original software distribution disks (they never come back). Build a software packaging library to install from and lock up the originals. If you believe that the installation can be done by others, post the installation off the Intranet web page and point users to that location.

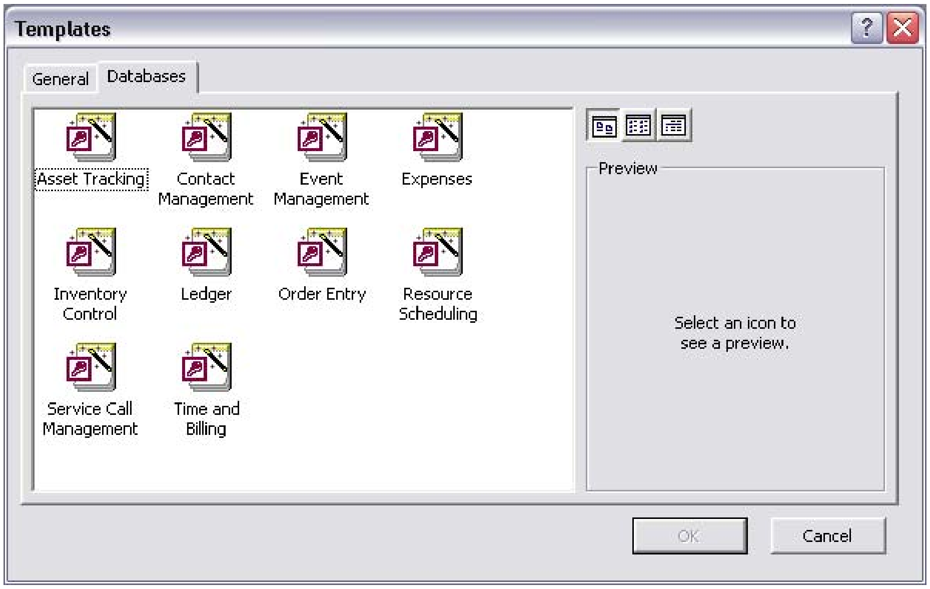
Register all software in the name of the business and never use personal information (such as a user name or home address). People move from business to business and when they leave you don't want their name associated with company assets.

Buy site licenses when you can. Purchase packs of software and be sure to find the lowest price. Take the time to look up several vendors and make sure you get some support level with them. While everyone is going to expect you to know everything there is about all the applications on their desktop, you and I know that is impossible. Having a support line helps to give you the edge when a question pops up about software you don't have an answer for.

SYSTEM INVENTORY

Keeping track of hardware should start at the building of the network. There needs to be some recording of hardware/software which can keep up with purchases. Many pieces of the network are mobile (such as laptops, PDAs or pocket PCs) and can end up lost quickly. If you have no audit trail for these items then their loss will go unaddressed. There are companies out there that sell barcode stickers which can work with a barcode reader that supports Excell, Access, SQL and other applications which can store and track your inventory. In fact, many Office Suites offer an inventory template that can integrate with barcodes and do an excellent job of providing up-to-date information on what and where.

FIGURE 4 - 15. **Microsoft Access Wizards**



If you start at the beginning of your network to track items, you also grow the process for maintaining inventory. Too often inventory is considered an annual event that requires long hours of hunting down items and verifying their still available. Having an up-to-date list complimented by an easily portable barcode reader and a process for verifying inventory can greatly reduce the “search and verify” process.

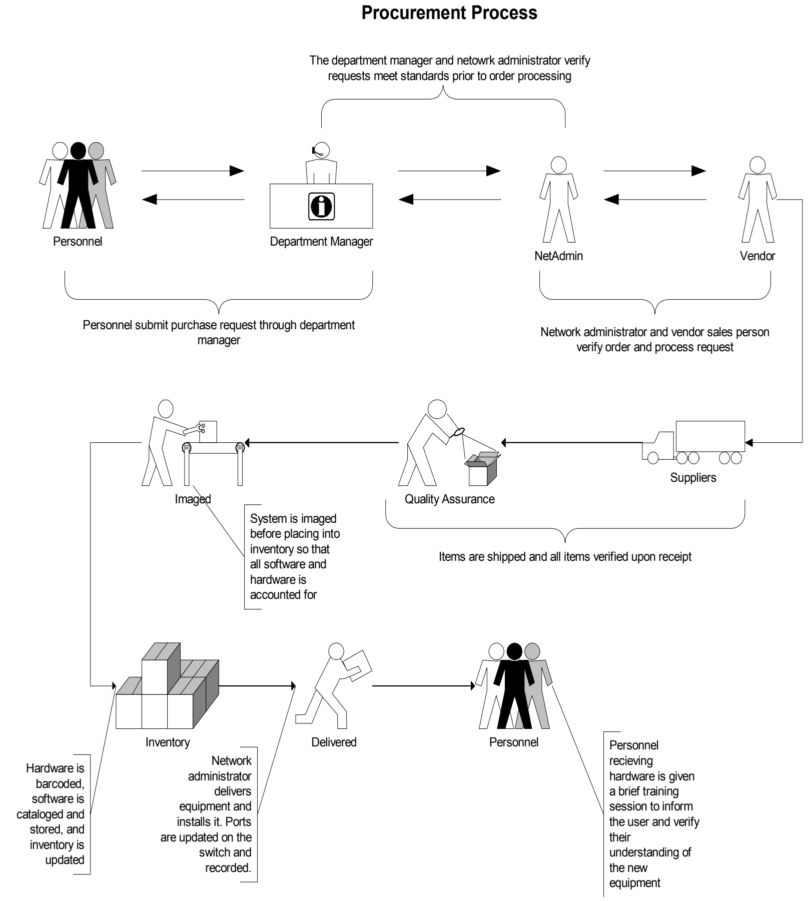
Items that can not be barcoded (such as software and internal upgrades i.e.; CPUs, hard drives, etc., should be controlled in other ways. Original software should never leave the IT library (only duplicates that are pre-packaged and stamped with the company’s information). Hardware additions can be associated with in the inventory database as part of a pre-barcoded item.

Everyone has a process for inventory that differs from everyone else. The key is to make sure that whatever database you use, that data can be imported into most other database applications. When it comes time to change the application you use for inventorying, you will be able to do so quickly and without loss of data.

PROCUREMENT AND REPAIR

As I said earlier, all network asset purchases should go through the network administrator so that standards can be maintained.

FIGURE 4 - 16. **Procurement Flowchart**


Procurement Process
The department manager and netowrk administrator verify requests meet standards prior to order processing
Personnel
Department Manager
NetAdmin
Vendor
Personnel submit purchase request through department manager
Network administrator and vendor sales person verify order and process request
Imaged
Quality Assurance
Suppliers
System is imaged before placing into inventory so that all software and hardware is accounted for
Items are shipped and all items verified upon receipt
Inventory
Delivered
Personnel
Hardware is barcoded, software is cataloged and stored, and inventory is updated
Network administrator delivers equipment and installs it. Ports are updated on the switch and recorded.
Personnel recieving hardware is given a brief training session to inform the user and verify their understanding of the new equipment

Having a well defined process (and sticking to it) will help to ensure that all hardware follows a testing and approval processes that minimize incompatibility. Publishing the process on the Intranet and educating personnel as to that process will ensure that everyone gets what they want when they want it. As a network administrator, you need to be aware of the time it takes to get products in.

You should also query department managers to get information ahead of time regarding new personnel and try to have the hardware and resources in place for their first day at work. There is nothing more motivating for a new employee then having everything ready for them on their first day -- it shows that you respect their value to the company and builds goodwill that you may need later.

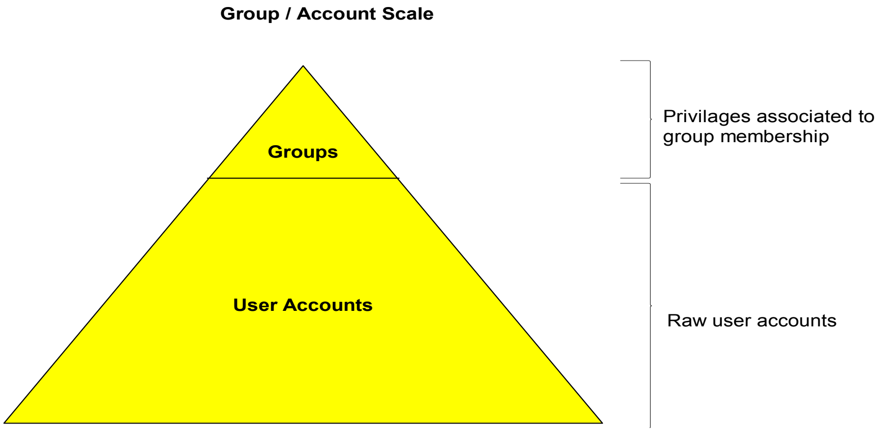
Always spend time with each recipient of new equipment and show them what you know about how it works. Taking the time to train personnel is a win/win situation for both you and the person receiving the new equipment.

ACCOUNTS

The most important parts of administration is the creation and management of accounts. Accounts are the keys to the palace. Making sure that the right key goes to the right person is crucial to the security of your network.

Part of making sure that the right privileges go to the right account is in setting the privileges through group settings and then assigning users to those groups. Also using login script account name variables to assign server folders and enforcing good password policies go hand in hand with group policies.

FIGURE 4 - 17. Groups and Users



GROUPS

As you can see in figure 4-17, it is much easier to manage the smaller number of groups then individual users. This also makes it easier to focus on where the problem is when troubleshooting a privilege problem.

Here is a list of some group names that might be used:

- Administrators
- Accounting
- Everyone
- Managers
- Marketing
- Remote Users

There are obviously more groups you can generate that would be tailored to your business. Groups should not be limited to the organizational structure. You should look at resources and try to control those resources through groups (such as remote access). An account can belong to more then one group, but it is always preferred to nest groups instead of users. In other words, a user (by default) should only belong to one main group but that group should belong to other groups as needed. You should look at groups in two ways:

1. Organizations within the business
2. Resources within the business

Administrator Group

Only network administrators should be added to the administrator group -- this will reduce the potential for people to abuse their authority. NO ONE should get administrator access to either the server or their workstation. Giving non-administrators administrative access opens the door for unauthorized software, broken applications and lethal viruses. You should be prepared to act quickly to every software request that is made so that people don't build displeasure with their limited access to their workstation. You should explain to your users this policy and why it is so important.

Accounting

Only those personnel who are authorized by the accounting department should be a member. This group manages confidential information that should have a higher level of security then most other groups. HR would be another group with the same security requirements.

Everyone

The everyone group is there so that you can push privileges globally. You add other groups to this group. Every time you create a group you add that group to this group. By nesting groups like this you reduce the work you will have to do in maintaining individual accounts. If company policy dictates that everyone should have access to the Intranet Main web page you set those rights with this group.

Managers

As the name says, managers should be placed in this group. You may wish to have file shares that only managers can access. By setting access via this group all members are given the correct privileges.

Marketing (Department name goes here)

All department member (in this case marketing) are added to this group so that they have access to resources only their department requires.

Remote Users

Adding users to this group should allow those members to access network resources from home or elsewhere. You should always limit member to this account for security.

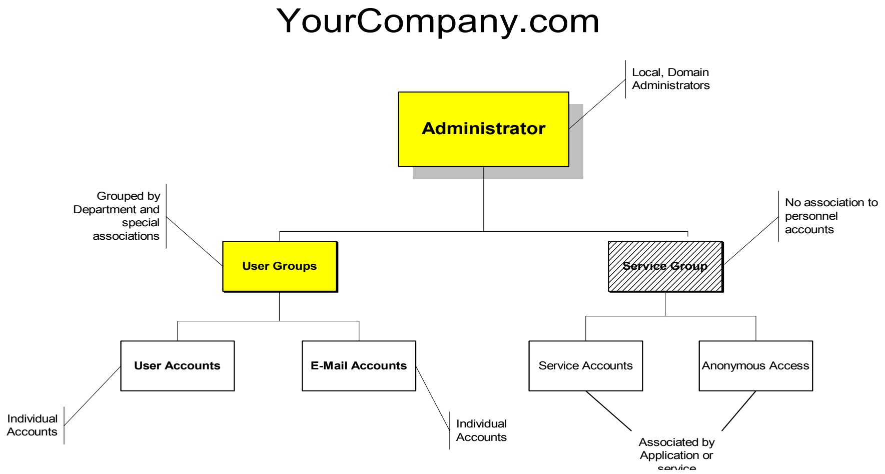
SERVICE ACCOUNTS

Other groups (not associated with users or hardware resources) should be defined so that you can control services and their account management. As stated earlier, services are additions to the operating system that add functionality. Some services require special accounts to operate across the network. Setting up a group for service accounts helps you to keep track of all of the service accounts you need to run your business.

Service accounts must have password changes just as user accounts should. Your job is to keep track of all of the services that require special accounts and be prepared to alter any instance related to passwords that may exist on servers, routers and computers.

ACCOUNT HIARCHY

FIGURE 4 - 18. **Basic Account Structure**



It becomes clear that:

- User accounts are given privileges through groups.
- Groups have unique privileges not shared by other groups.
- Groups can be nested so that users share privileges from more then a single group.
- The administrator group is at the top of the food chain and should only contain users who are responsible for the management of the network.
- Service accounts can be placed into groups as well, but should never be associated with either user or system.

What we haven't discussed is how these accounts apply to workstations. Once a workstation is added to a domain (either Windows, Novell or Apple) it can authenticate account information from the server account database. In doing so, domain accounts can have access to any machine on the network (or be limited to a particular machine). This gives the network administrator great leverage with resources so that when it becomes necessaries, people can be assigned new equipment without added configuration.

Workstations cache[96] account information from previous logins, so if a person takes their computer with them (say a laptop) they can still login using the domain account.

[96] A cache (pronounced CASH) is a place to store something temporarily. The files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser (for example, Internet Explorer). When you return to a page you've recently looked at, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic.

FIGURE 4 - 19.

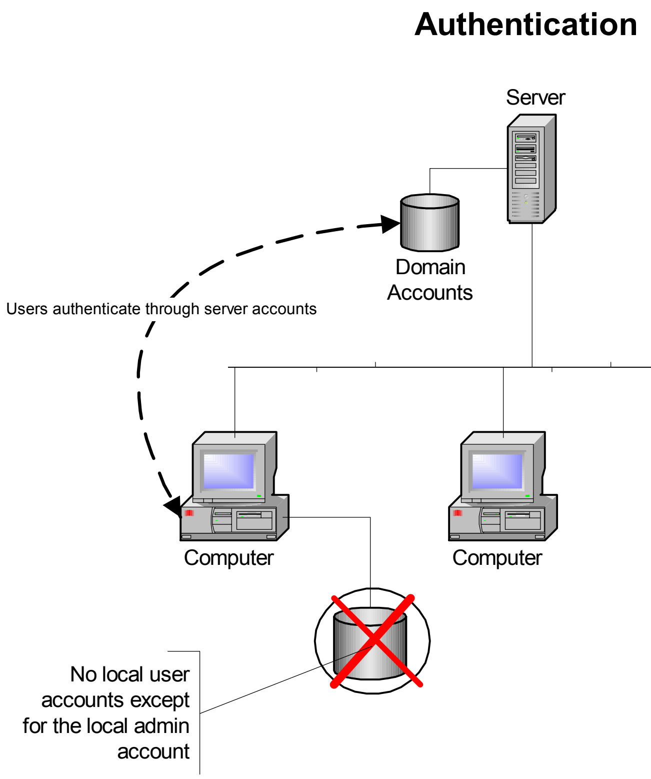

Authentication
Server
Domain Accounts
Users authenticate through server accounts
Computer
Computer
Computer
No local user accounts except for the local admin account

Figure 4-19 represents the connection between the server account database and the workstation. Note that the workstation does not allow for the local accounts database to be accessed.

E-MAIL

I have chosen to outsource[97] E-mail and Internet web services for one simple reason -- lack of assets. The trouble of maintaining an E-mail server as well as the security for a web server would not be cost effective in our network scenario. Outsourcing helps to bring in a well developed communication strategy without emptying the bank.

Besides the usual accounts that your users will have you should have the following additional E-mail accounts generated and linked to the appropriate personnel:

- **Department@yourcompany.com** - accounts for each of your departments (i.e. *Marketing*@yourcompany.com)
- **HelpDesk@yourcompany.com** - to receive problem issues (internally)

[97] Outsourcing is an arrangement in which one company provides services for another company that could also be or usually have been provided in-house. Outsourcing is a trend that is becoming more common in information technology and other industries for services that have usually been regarded as intrinsic to managing a business.

- **Employment@yourcompany.com** - to receive employment requests, resume's.
- **President@yourcompany.com** - to get information from outside directed towards the upper management.
- **Support@yourcompany.com** - to receive problem issues (externally)
- **Webmaster@yourcompany.com** - to receive outside communications regarding your web presence.

There are three common e-mail syntaxes used in business (you should pick one and keep it as the standard for all personnel e-mail accounts:

1. First letter of the first name followed by the last name (**FLast**@yourcompany.com).
2. Firstname followed by the first letter of your last name (**FirstL**@yourcompany.com)
3. First and last name separated by a period (**First.Last**@yourcompany.com)

For simplicity, user accounts on the network are usually the same as their e-mail account name. While this is a common practice it does expose your account naming principles to the world and could invite hackers to try and break passwords associated with those accounts. Further, giving the full names of your employees as their E-mail address also exposes employees to potentially dangerous situations. I would suggest that the E-mail address not follow the syntax of the user account nor expose your employee's full name. You should make sure that each account gets 50 - 100 Mbps for their mailbox.

SECURITY

You can see that we have already looked at many security issues:

- limiting router access
- restricting administrator accounts
- supernetting

We have also defined both physical and logical security measures to be taken:

- locking up the server and router hardware
- backing up data and keeping copies off site
- restricting access to original software installation media
- maintaining current inventory

We have also touched lightly on antivirus software and external access to internal assets.Antivirus software should be keep current and never disabled for any reason. A virus can spread quickly and destroy data -- something you just can't afford to let happen. Limit access from the outside to the most minimum resources and have the router log everything that happens on those exposed resources. There needs to be further security measures which define access to folders and data. There needs to be well defined protections against unauthorized access (internal and external) through either ports or stealing an account's password. One of the most successful methods to break into a network is through social engineering. This refers to the method of getting someone to freely give up their password to someone they don't know (or someone they barely know).

The scenario goes like this:

> Someone calls your office and tells you that they work in the IT department. They explain that there has been a break-in on the network and that your account has been breached. They want to verify that you can still logon with your old password so they ask you for your password as verification.

What's wrong with this picture? Administrators can not usually tell what your password was -- you must give them that information. Secondly, an administrator would never ask for your password over the phone -- they would ask for permission to change your password if they needed access through your account. You wouldn't believe how well this type of attack works. Keeping people aware of their security responsibilities -- most people don't take security as seriously as they should.

Try to get people to lock their screens when they walk away from their computers. Break-ins have been very successful by walking up to computers that were left with their accounts open and available.

Limit the installation of spyware (instant messaging, webshots, special plug-ins that interactively communicate with workstations through the internet). These tools may be fine for home use but they don't belong in an office.

Offer training to promote safe computing and invite everyone. Keep people up to date with notifications of potential virus outbreaks or web attacks -- if you don't keep people interested they will forget to play it safe.

SCALING RESOURCES

Put the infrastructure in place which will meet the needs of a full office even though you have empty space. By putting the infrastructure in place you are building for the future and making it easier for new employees to come on-line quickly. Make sure that you leave added resources to expand outside of your office space. If the need to expand should arise, you will be prepared to expand without disrupting the workers you already have. Buy equipment that is well accepted as a standard - don't just buy hardware because it was cheap. Don't buy end-of-life equipment or software, you'll be stuck with something you can not support or get rid of.

Build a budget and forecast growth. Start looking at the cost of an individual using those resources along with what it takes to provide those service (hardware, software, network provisioning and support). Always add 10% to the final number (so that you can cover changes in pricing).

Use the following as a benchmark:

- Cost of an individual port = Port (cost of switch divided by the number of ports)
- Cost of having the cables run = Cable (total cost of the installation divided by the number of connections).
- Cost of server resources = Server (total cost of the server and software divided by the number of people using the server).
- Cost of Internet connection hardware and services = Internet (total monthly bill divided by the number of people accessing the Internet).
- Cost of E-mail accounts = E-Mail (total monthly bill of E-mail accounts divided by the number of people with e-mail accounts).

- Cost of electricity to run the equipment = Electricity (total monthly electrical bill divided by the number of people in the company).
- Cost of workstation and applications = Workstation (total cost of purchasing workstations and laptops for all people using them in the company).
- Cost of web presence = WebPage (monthly cost of contracting the web service provided).

Add all of the individual components:

Port + Cable + Server + Workstation + = One Time Expense

Internet + E-Mail + Electricity + WebPage = Monthly Expense

One Time Expense + (Monthly Expense x 12) = Individual

Project your budget growth by multiplying “Individual” with the projected growth of the company and you build a baseline for expected costs to be uncured. If you add more resources to the equation, you should apply the same concept to that piece of equipment.

Example:

1. The cost of an individual is $3,500.00 (add 10%) = $3,850.00
2. Multiply the Individual by the projected number of personnel and you have a baseline for your projected budget.

You should look at adding resources outside of the Individual calculation as projects and they should be calculated individually.

DOCUMENTATION

You need to keep track of as much information as you can about your network and correspondence that takes place regarding it. Not just receipts and contracts, but all we have covered in this section of the book. Organize your information and keep it in electronic form.

While it is great to have hard copies of everything, electronic versions offer you the ability to merge information and get metrics about how your doing. Scanning receipts and contracts will help you to build and organize your information further. Never get rid of E-mail, store it for future use -- many times I’m questioned about E-mail I received a long time ago and when I can pull it up quickly, I can respond in an educated way. There is nothing worse then not having the data you need to respond. Don’t forget to archive data -- I put it into CDs and date them accordingly.

Publishing a “State of the Network” monthly e-mail to your fellow employees helps everyone to be aware of that’s going on. Post metrics on the Intranet IT web page so that everyone can see what you are doing. People are interested in what the network administrator is up to and they can get a true appreciation of how hard your working to keep them working.

INFRASTRUCTURE MANAGEMENT

Managing the performance of your network hardware should be a daily duty, in that you should scan log files, test bandwidth and inspect switch and router indicator lights. I tend to do this in the morning before people arrive so that I can be on top of any problems related to connectivity before everyone else. Notifying people of potential problems will show everyone that you are on the ball and concerned about keeping things running smoothly. Mondays are especially important when it comes time to look for potential problems - most of your connectivity issues happen after a weekend or long holiday.

Here is a list of things to look for:

- Switch - amber (or red) lights where there should be green lights.
- Router - No blinking lights
- Patch Panel -Loose or tightly pulled cables
- Printers off line
- No access to server resources
- No access to the Internet
- No access to E-Mail
- Backup logs are empty

While these things seem obvious, if you are not looking for them someone else will be sure to let you know there is a problem. Be pro-active and be the first to find the problem. Inform others that you are working on the problem and let everyone know when a solution is in place.

TRAINING

Offer Training

Offer training that helps everyone to understand what they need to do to get the network to work better for them. So many times network administrators create training and present it for people who already have a technical background. Keep things simple and offer information that is directly related to what the participants do with their workstations and the network.

Educate Yourself

To keep yourself up to date:

- Attend off-site technical classes and seminars
- Go to conventions when available (and affordable)
- Subscribe to on-line technical help (such as Tech Republic)
- Subscribe to free industry magazines
- Make friends with other network administrators in other companies

Networking is a never ending cycle of re-training. Keeping up with new techniques and ideas will easily fill your free time (if you ever get free time). Be aware of the bias that each magazine or technical course/seminar places on the information you get - everyone has an angle. Don’t get hooked on any one vendor to solve all of your technical issues. As the market sways from one vendor to another, take the time to question everything and move slowly once your mind is made up - slow and steady wins the race.

DISASTER RECOVERY

Tape backups, sychronization, RAID, everything should be in place for disaster recovery up to this point. The one thing missing is a plan for recovery. We have the tools set and are keeping up with our backups but what happens when the disaster happens?

The disaster recovery plan should be posted in the network administrators office for everyone to see. It should be a list of bullet points that clearly motions people through the process. You should be able to follow the steps even when others around you are panicing. Having everyone trained to follow the steps is the key to recovering from disaster.

Disaster - Steps to Recovery

- **User Side**

1. Don't panic!
2. Stop what your doing.
3. Call the Network Administrator.
4. Define the problem.
5. Explain what data may be compromised.

- **Network Administrator Side**

6. Is it life threatening? (call appropriate authorities immediately)
7. If its network related localize the problem (if it's virus disconnect any network resources immediately)
8. Does it affect more then one person?
9. Is it hardware that can be replaced?
10. Is it data that can be restored from tape?
11. Is there synchronized data that could be recovered?
12. Is it software related and what can be done quickly to recover the application?

Following these steps and finding the solution can be quick and effective only if there is good communication between the person having the disaster and the network administrator. There has to be a comfort level where trust has been established. Many times a person is not willing to tell you what happened because they believe it might get them in trouble or make them look bad - as the administrator you must assure them that neither will happen. Further you must follow through by not posting information (or talking to anyone) regarding the event other then what happened and how it was resolved. Trust is a two way street.

FILE SYSTEM MANAGEMENT

Defining a strategy for file sharing must incorporate two things:

1. Hiarchial folder structure with appropriate security.
2. Front-end for posting sharable material.

The most common hiarchial folder structure comes with each operating system. Linking folders on the server with folders on each of the workstations (synchronizing folders) so that user data is stored in both places helps to take care of the secure data each person is individually responsible for. Departments need to share data as well (with their members and the company).

FIGURE 4 - 20. **Folder Structure**

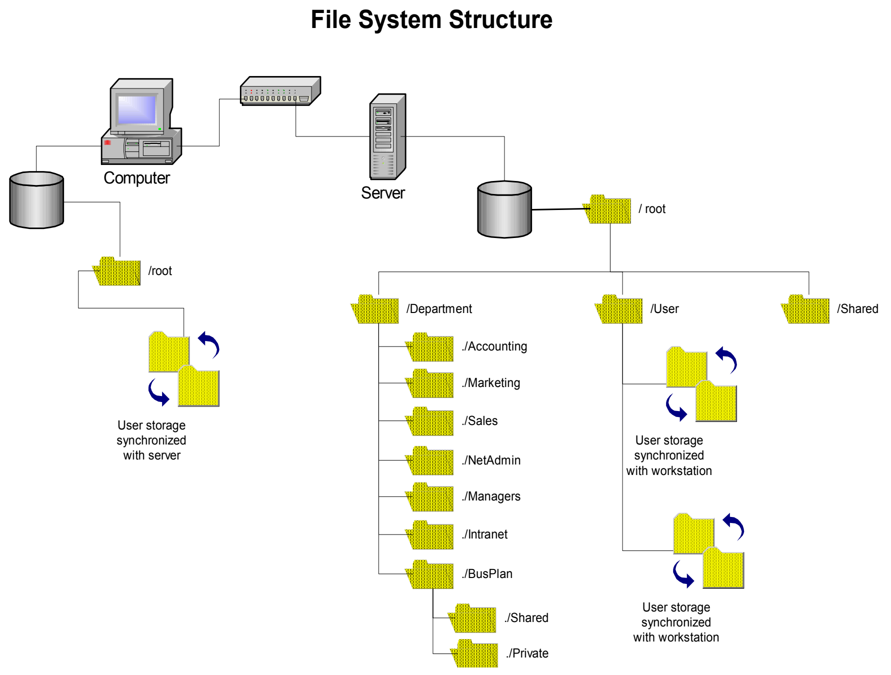


Figure 4-20 diagrams the folder layout for shared files.

- The users home folder (or “My Docs” on a Microsoft Windows system) would be sychronized with a data folder on the server (/user/username).
- Department folders would also be mapped to the workstation so that people can save their departmental data (/department/marketing).
- In the department folder on the server you would find two sub folders (shared and private).
- The shared folder content would be linked to the Intranet web page associated with the department.
- The private folder would only be excisable by members of that department.
- The “\shared” folder would be used for all data common to the company in general.
- Management would share a separate folder for confidential files that are common for all managers.

The concept is to keep it as simple as possible and link any data to be shared through the Intranet web pages.

SUMMARY

Obviously administration of the LAN has grown and started to get complicated. The goal is to document everything, build goodwill with employees through keeping them informed and moving quickly to keep data had inventory out there for people to use. Train and be trained as often as you can and build your disaster plan to inform and resolve with shared expectations for success. Work with and not against people.