Post Wrap up on USX Project

Some problems with this project were:
NTFS permission vs. Share permissions
Correct Usage of Security groups
Computer accounts not in domain
IP addresses reset
Use of DNS, WINS, and Browsing master

NTFS Permissions
Numerous people seem to misunderstand the differences between share and NTFS permissions and when they are to be used. NTFS permissions are the basis of your file security. It is used to control who has access to your system, whether it is locally or remotely. Remember NTFS permissions can only be used on a NTFS volume. Sometimes you will come across volumes that are FAT and not NTFS and therefore don't support file level security. If this is the case you would be using the share permissions because the NTFS permissions do not exist. If you are able, you should convert this volume to NTFS. Because you would normally be using NTFS, you would not even use share permissions except under certain circumstances. For example you had a user named Joe. This user needed access to some files shared out. However for security reasons you only want him to access these files on the data server locally and you do not want him to have access remotely. In this case you would still be using NTFS permissions like you always should, and your share permissions would be at its default of full control to everyone. The only difference in this case is that you would simply add the user Joe to the share permissions and deny him access. You would use the deny access exception because it is much easier than removing the everyone group and trying to constantly match up the share permissions identically with the NTFS security permissions. Joe can now access the share files locally and not remotely like the rest of his group. If you try to do things the other way around and remove his NTFS permissions, then Joe would not be able to log on locally or remotely. This is what most people have been doing. If you don't grand a group or user NTFS permissions, then they wouldn't be able to access the files locally or remotely. So by rule of thumb, always use NTFS permissions to grant users access and never the share permissions unless for exceptions. Also by default there are several system groups and accounts by default on every file and folder on the NTFS volume. When editing these permissions be sure not to remove the essential groups and accounts like administrator and domain admins. Also everyone would not be of best choice here because it grants everyone access. And authenticated users means all users with accounts that have been granted access. When testing access make sure you are not an administrator because you should always have full control.
After you understand NTFS and know to always use NTFS permissions and to forget about the share permissions you can then trouble shoot why remote users can not gain access. Because NT does a lame job of identifying your domain groups from another domain groups you have to make sure the domain group you are looking at in your NTFS permissions tab is your domains group and not another domains group because the names will look identical. Windows 2000 solves this problem by putting in parenthesis the

domain the group comes from. There are many methods and ways to apply NTFS permissions to grand a user access to files. The correct way to apply NTFS permission for the USX project is on page 5 of the last packet. If you apply security permissions straight from the list you will have perfect user access. The only addition that needs to be added to this list is just based on personal preference. Because each class member was normally logging on with their own username is was affective to add each domain admins group to each division folder. This is assuming that each member of the class was a domain admin of their domain. This allowed each group to test each others permissions based on their personal user account. This can be related to the real world, because say in another domain a user comes up to you saying they can't access resources in another domain that they should. Well it would be useful if you had access to those same resources as well. The project also required staff members to have RWX. IF you notice in the NTFS tab, this is ADD and read. This means the user can read the file, and make new files. This does not give the user right to modify the file or delete the file. However by default the creator and owner account is also in the NTFS tab. This allows only the user that created the file to re access it, edit it and save it. This is good security measures because you don't want all staff members to be able to edit any file they want or to delete anything they want. You only want the owner to be able to work on their own file and not everyone. It would be a security breach if everyone in payroll had access to the payroll and could change their pay. In other words only the owner can edit that file, but everyone else could add files to the payroll directory.

Correct usage of Security groups

If you have forgotten the rule of thumb for correct usage of security groups, remember Users should be placed in global groups and then the global groups can be placed in local groups. Some domains were adding other domain's global groups into their own global groups. Although this can be done, this is also a security breach if other domains are supposed to have lesser access. If your groups are supposed to have read and add or change, you don't want another domain to have those same permissions if they are only supposed to have read. Some were even trying to add local groups to local groups, and that can't be done. The correct method is to make local groups on your domain and add remote global groups to your local groups. Some domains were even adding other domains groups into their own domain admins groups. This is a major security breach because you would never grant other users and even other administrators global access to your domain. Only the administrators of the domain should have global access to your domain. The correct method of group placement without any security breaches is found on page 4 of the last packet.

Computer accounts not in domain

The project called for an appropriate naming of the server on which the data shares are located on. If your server name had to be changed, then you may have broken from the domain if you didn't prep. The easiest method is to first add a computer account in the PDC and the sync the domain. Next you can rename the server you want to rename from its networking properties. When you restart, the server will automatically find the new

computer account in the domain and act as if nothing happened. You can then remove the old computer account from the PDC after the domain has synchronized and no longer sees the server. There are other methods of doing this, but this seems to be the easiest. If you don't do any steps, then your server will be broken from the domain and won't be able to log into the domain or access resources.

IP address reset

On a couple machines running windows 2000 the IP addresses were reset. This was because the machines were moved and the computer saw a new network card. When a 2000 machine finds its network card is replaced it automatically configures the network card with a new connection because each connection is bonded to its network card. Because of this you will notice all the setting for your connection have been reset. This isn't really a problem until you try to put the same IP address back in. When attempting to do this, windows prompts you with a warning telling you that there is already a connection with that IP address. Although you may not see any other connections, the connection is in fact on the machine but hidden until the old network card is restored. When the warning comes up simply hit NO and continue on your way and it will use the settings you provided. This is simply a warning protecting you from using two network cards with the same IP address. You will mainly find this on 2000 pro with removable drives. It isn't very common on 2000 server because 2000 server doesn't like to have its hardware switched on it. When using 2000 pro, you can swap drives on similar and sometimes dissimilar machines as long as the processor and chip set are higher or equal to its previous hardware. On 2000 Server, this isn't the case. Server has security features that prevent this and also because of its services running. A 2000 server can be swapped only if the hardware is virtually identical. Pro doesn't care and will auto detect anything as long as the manufacture was competent in providing Microsoft with a driver for the hardware. You normally don't have this trouble with NT because it can't tell the difference between hardware because it is not plug and play.

WINS, DNS, and the Master Browser

The last packet was a little bit unclear in explaining this. The only reason why DNS and WINS was used in the USX project is to get some people thinking in terms of resolution so these services aren't totally new later on. WINS and DNS do not have to be present for a NT domain to exist. However because 70 percent of network traffic is based on broadcasts, it is wise to use DNS and WINS. There is nothing yet to prevent the broadcasting of the master browser, although 2000 has had great improvements. The difference in DNS and WINS in NT is that DNS is used mainly when connecting to the internet and referrals and WINS is for NetBIOS name resolution. When crossing subnets, you would still need to use DNS and WINS because you can't broadcast through networks. 2000 unlike NT requires DNS for its active directory, but does not even use WINS unless NT or 9x systems are needed. I will explain how browsing and these services are used.

When you want to connect to a computer you have two ways. You can either do a direct connect through start run, or IE 4 and above. This method bypasses the Master browser and you are essentially trying to directly connect to the computer. To do this you need to know the IP address. IF you have WINS (NT or 9x machine) or DNS(2000 machine) addresses statically or dynamically entered into your networking properties, then your computer contacts that server and requests for the IP address of the machine you are trying to contact. Once you have the IP address you can then connect to the computer. If like in this lab, where most people didn't map DNS or WINS, when trying to connect to a machine your computer would essentially broadcast for the machine you are trying to connect to. This machine would eventually send you back its IP address and then you could connect to it. This is why it sometimes takes a while to connect to another machine especially if the network is experiencing heavy traffic. All these broadcasts add to this traffic. The use of WINS and DNS speeds up your machines ability to resolve host names by queering a database instead of broadcasting the network and also cuts network traffic.

When not trying to directly connect you would simply browse to find the computer and then connect. This method is referring to the use of Network Neighborhood in NT or 9x or Windows networking in 2000 found through my network places, you are essentially browsing for the Master Browser. You are then retrieving the browse list which is what you see, a list of domains or workgroups and computer in each. First you see your own workgroup or domain. You can then switch to another domain or workgroup. This list is provided by the Master browser in that domain or workgroup and then transferred to your master browser's browse list. This isn't very effective when servers are going on and off line frequently because elections can occur and the browse list can be full of bad mappings or stale or be non existent. This is why most people were having trouble seeing their computers and other domains in the Network Neighborhood. It takes several minutes for this browse list to stabilize and synchronize with each other. This is a major part of excessive and unneeded broadcasting. After you can actually see the computer you are trying to access you can click on it. Once you click on it you are essentially trying to directly connect and the steps above would now apply as if you were connecting from start run or IE.
2000 somewhat eliminates the problem of browsing by providing the active directory through windows networking in something called the directory. Unlike browsing, this directory is provided by the active directory and does not take up network bandwidth from broadcasting. Also this list is always up to date and you never have to wait on it like with network neighborhood through browsing. You simply go through the directory and access the resources you want. You do have to publish all resources in active directory for anybody to access these resources. You now don't have to browse for resources eliminating excess bandwidth, and because 2000 runs on DNS, as soon as you click on the resource, the IP address is provided by the DNS which is integrated into active directory and you are taken straight to the resource with out any browsing or waiting.