

PROJECT OBJECTIVE:

To set up a multiple master domain consisting of six domains. Each domain will consist at a minimum, one (1) PDC, one (1) BDC, and two NT workstations.

Intro on IP Scheme:

Before getting started on trusts, relationships, and permissions, it may be wise to take time to restructure the IP Scheme for USX. There are two types of IP addressing: Public and Private. Public IP's are used for direct connections to the internet, routers, web servers, ISA, etc. that need to be available to the public for external use. The Private IP addressing scheme is used for internal IP addressing of companies for communication throughout the internal network of a company. There are 4 private IP networks available and reserved through ICANN. These are:

10.0.0.0 through 10.255.255.255 which is a class A network

172.16.0.0 through 172.31.255.255 which is a class B network

192.168.0.0 through 192.168.255.255 which is a class C network

and then there is the 169.254.0.0 network which is the APIPA network and is used by individual machines that are set up for DHCP but are no longer receiving DHCP configurations.

These are the only IP's that can be used for internal purposes.

Private IP networks can stretch all across the country through routers using public IP's. The one thing to take note is that although in different domains and in different cities, no two machines can have the same private IP address. This is where subnetting comes in. A company that needs up to a thousand networks with many in each site and needs tens of thousands of users in each subnet would need to develop a unique IP scheme for their company. The most common network would be the 10.0.0.0 network because it can hold the largest number of networks and subnets. An example of large scale subnetting with the appropriate routing can be found later in this packet. Once the private network has been subnetted, each network can only talk to each other through routers with DNS pointing them in the right direction. Super netting should never be used on private networks and can only be used correctly on public class C networks. The only way for a private network to be subnetted and to communicate with other networks without routing is through supernetting, because you can overlap networks. This is something that should never be done except in extreme circumstances. This should only be done in class C public addressing where you purchase blocks of class C networks from ICANN and need them to function as one.

For class purposes, we have no methods of routing unless our machines have two NIC's and then we can turn 2000 boxes into routers. Because of this, every machine must be on the same network and can not have the same IP addresses in order for complete communication and trust relationships to function correctly.

IP Scheme

Because the default gateway for the class is 192.168.0.1 we will use the class C private network with the default subnet mask. Any other subnet mask greater than the 24 bit default will be partitioning the network into pieces eliminating all communication between networks. Subnetting will also remove the default gateway from the valid network range. Any subnet mask less than 24 bits would be called supernetting and serves us no purpose but confusion.

To simplify the locations of all IP's, it would be best to distribute IP's to groups in ranges starting with 10 while matching up the row number to the section of IP's

A good IP scheme would be the following:

Hedquarters

Anglum	192.168.0.11
Briskey	192.168.0.12
Frazier	192.168.0.13
Zipfel	192.168.0.14
Thoma	192.168.0.15

Los Angeles

Slak	192.168.0.41
Poniatowski	192.168.0.42
Miller	192.168.0.43
Martin	192.168.0.44
Uhrin	192.168.0.45

Dallas

Bitters	192.168.0.21
Matuch	192.168.0.22
Starzynski	192.168.0.23
Wilkerson	192.168.0.24
Trusedale	192.168.0.25

Baton Rouge

Medich	192.168.0.51
McGill	192.168.0.52
Taylor	192.168.0.53
Wallat	192.168.0.54
Baldwin	192.168.0.55

New York

Hatok	192.168.0.31
McConnell	192.168.0.32
Wolfe	192.168.0.33
Cresswell	192.168.0.34
Falba	192.168.0.35

Seattle

Devine	192.168.0.61
Casey	192.168.0.62
George	192.168.0.63
Jensen	192.168.0.64

We will be using a 192.168.0.0 Class C Private IP Addressing Scheme

The subnet mask will be 255.255.255.0. This provides us with 254 networks and 254 hosts per network.

The CIDR (classless internet domain routing) Scheme will be 192.168.0.0/24

We will only be using the first network and everyone will be on the same network.

Currently there is no method of domain resolution and we have been depending on the MASTER_BROWER services for NetBIOS resolution. There is a Master browser for every workgroup and domain. This service does an ok job of providing resolution, however it is very unreliable. This is because when machines go offline or come online there are elections and constant broadcasts to update the browse list of who in the domain is where. This can become a problem especially when each domain is depending on each other. Whenever a 2000 machine is on a workgroup or domain, it automatically seizes the master browser ownership of any other machine on that domain or workgroup. Because of this, it can sometimes take up to 15 minutes for browse list to be accurately updated and stabilized on one machine. After your domain is stabilized, you then may have to wait longer for other domains to stabilize and for their browsing master to synchronize with your browsing master to gain an up to date list. This process is very inefficient and time consuming. The correct way to provide resolution is through DNS and WINS. DNS and WINS services on 2000 provide zone transfers very efficiently unlike NT.

You can use the IP address of 192.168.0.24 as your DNS and WINS servers, however to participate in name resolution, please provide Cory with your computer names and IP addresses. When using DNS and WINS, 2000 queries DNS first then WINS to resolve NETBIOS names. NT on the other hand queries WINS and then DNS. This is because NT is built around NETBIOS names in which WINS is based on. 2000 on the other hand is build on FQDN's (Fully qualified domain names) which is full DNS name space. By resolving through these services, each computer no longer has to send out broadcasts to find the computer it is looking for. It simply queries the database.

Static IP's will always have to be mapped in DNS and WINS because the addresses are not provided dynamically. When the IP configuration is provided automatically and with scope options, all DNS, WINS, gateways, and the many other configurations are provided to the client automatically. The DNS and WINS databases are also updated automatically when a computer comes online or goes offline. This dynamic effect is only provided through 2000 and is streamlined in Active Directory which makes all transfers secure.

One thing to consider while picking domain names and computer names is that Active directory does not allow underscores. The difference between NT and Active directory, is that NT uses a flat hierarchy name space while Active directory uses a DNS hierarchy name space which does not consider an underscore as a valid character.

You only have to be concerned with the underscore being an invalid character if you plan on upgrading to active directory. If you plan on upgrading then you do not want to create a domain with underscores, but use the hyphen instead. When installing 2000 you will be presented with a warning when using an underscore. You can simply continue and ignore this error only if you don't plan on using active directory.

Domains:

1. Headquarters
2. New_York
3. Los_Angeles
4. Dallas
5. Seattle
6. Baton_Rouge

Two way trusts should be set up between every domain

There are four divisions in each domain listed below.

HR	Operations
Finance	Production

Each division will consist of one (1) manager and ten (10) staff members

In each domain the following global groups will exist:

MANAGERS HR_staff Finance_staff Operations_staff Production_staff

In each domain the following local groups will exist:

HR Finance Operations Production

Add each staff member to the global group for their division and the division manager

Add each manager to the global Managers group

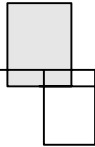
After complete two way trusts are set up between each domain, global groups can be added to local groups

Add each domains global division group to your corresponding local division group. Do this for each division local group on your domain.

Each domain will have a data folder with the following 4 division folders that will be shared appropriately:

HR Finance Operations Production

Each division folder will have subfolders with data files in the appropriate subfolder.



Each division share will have share permission of full control for the everyone group with no other group listed.

NTFS and share permission are least restrictive on user access with the exception of deny, which overrides all permissions.

NTFS determines a users file access, and the combination of share and NTFS permission with most restrictive access determines remote access.

Because NTFS permissions are essentially granting users access, the share permission should only be used in rare circumstances.

NTFS Permissions for the HR division folder:

Managers	R
HR_staff	RWX
HR	R
"division manager"	RWXD

NTFS Permissions for the Finance division folder:

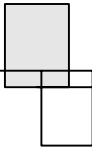
Managers	R
Finance_staff	RWX
Finance	R
"division manager"	RWXD

NTFS Permissions for the Operations division folder:

Managers	R
Operations_staff	RWX
Operations	R
"division manager"	RWXD
HR_staff	R
Finance_staff	R
Production_staff	R

NTFS Permissions for the Production division folder:

Managers	R
Production_staff	RWX
Production	R
"division manager"	RWXD
HR_staff	R
Finance_staff	R
Operations_staff	R



IP Addressing Scheme: 10.0.0.0/13

NEW YORK

Routers 10.24.0.1 to 10.24.0.254
Servers 10.25.0.0 to 10.25.0.254
Workstations 10.26.0.0 to 10.31.0.254

BOSTON

Routers 10.32.0.1 to 10.32.0.254
Servers 10.33.0.0 to 10.33.0.254
Workstations 10.34.0.0 to 10.39.0.254

PITTSBURGH

Routers 10.40.0.1 to 10.40.0.254
Servers 10.41.0.0 to 10.41.0.254
Workstations 10.42.0.0 to 10.47.0.254

CHICAGO

Routers 10.48.0.1 to 10.48.0.254
Servers 10.49.0.0 to 10.49.0.254
Workstations 10.50.0.0 to 10.50.0.254

BOISE

Routers 10.56.0.1 to 10.56.0.254
Servers 10.57.0.0 to 10.57.0.254
Workstations 10.58.0.0 to 10.63.0.254

GREAT FALLS

Routers 10.64.0.1 to 10.64.0.254
Servers 10.65.0.0 to 10.65.0.254
Workstations 10.66.0.0 to 10.66.0.254

SPRINGFIELD

Routers 10.72.0.1 to 10.72.0.254
Servers 10.73.0.0 to 10.73.0.254
Workstations 10.74.0.0 to 10.79.0.254

SEATTLE

Routers 10.80.0.1 to 10.80.0.254
Servers 10.81.0.0 to 10.81.0.254
Workstations 10.82.0.0 to 10.87.0.254

HEADQUARTERS

Routers 10.16.0.1 to 10.16.0.254
Servers 10.17.0.0 to 10.17.0.254
Workstations 10.18.0.0 to 10.23.0.254

ATLANTA

Routers 10.88.0.1 to 10.88.0.254
Servers 10.89.0.0 to 10.89.0.254
Workstations 10.90.0.0 to 10.95.0.254

ORLANDO

Routers 10.96.0.1 to 10.96.0.254
Servers 10.97.0.0 to 10.97.0.254
Workstations 10.98.0.0 to 10.103.0.254

TAMPA

Routers 10.104.0.1 to 10.104.0.254
Servers 10.105.0.0 to 10.105.0.254
Workstations 10.106.0.0 to 10.111.0.254

NEW ORLEANS

Routers 10.112.0.1 to 10.112.0.254
Servers 10.113.0.0 to 10.113.0.254
Workstations 10.114.0.0 to 10.119.0.254

HOUSTON

Routers 10.120.0.1 to 10.120.0.254
Servers 10.121.0.0 to 10.121.0.254
Workstations 10.122.0.0 to 10.127.0.254

PHOENIX

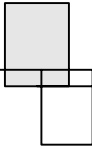
Routers 10.128.0.1 to 10.128.0.254
Servers 10.129.0.0 to 10.129.0.254
Workstations 10.130.0.0 to 10.135.0.254

LOS ANGELES

Routers 10.136.0.1 to 10.136.0.254
Servers 10.137.0.0 to 10.137.0.254
Workstations 10.138.0.0 to 10.143.0.254

SAN DIEGO

Routers 10.144.0.1 to 10.144.0.254
Servers 10.145.0.0 to 10.145.0.254
Workstations 10.146.0.0 to 10.151.0.254



Cisco Layout:

E = goes to a Switch - or - connects to another Switch (Ethernet Ports)
S = goes to a Router - or - connects to another Router (Serial Line Interfaces)

HEADQUARTERS

S0	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
<u>S0 New York</u>				<u>S0 Boise</u>				<u>S0 Atlanta</u>				<u>S0 Houston</u>				
E0 - Training				E0 - Training				E0 - Training				E0 - Training				
E1 - Sales				E1 - Sales				E1 - Sales				E1 - Sales				
E2 - Marketing				E2 - Marketing				E2 - Marketing				E2 - Marketing				
E3 - IT				E3 - IT				E3 - IT				E3 - IT				
<u>S0 Boston</u>				<u>S0 Great Falls</u>				<u>S0 Orlando</u>				<u>S0 Phoenix</u>				
E0 - Training				E0 - Training				E0 - Training				E0 - Training				
E1 - Sales				E1 - Sales				E1 - Sales				E1 - Sales				
E2 - Marketing				E2 - Marketing				E2 - Marketing				E2 - Marketing				
E3 - IT				E3 - IT				E3 - IT				E3 - IT				
<u>S0 Pittsburgh</u>				<u>S0 Springfield</u>				<u>S0 Tampa</u>				<u>S0 Los Angeles</u>				
E0 - Training				E0 - Training				E0 - Training				E0 - Training				
E1 - Sales				E1 - Sales				E1 - Sales				E1 - Sales				
E2 - Marketing				E2 - Marketing				E2 - Marketing				E2 - Marketing				
E3 - IT				E3 - IT				E3 - IT				E3 - IT				
<u>S0 Chicago</u>				<u>S0 Seattle</u>				<u>S0 New Orleans</u>				<u>S0 San Diego</u>				
E0 - Training				E0 - Training				E0 - Training				E0 - Training				
E1 - Sales				E1 - Sales				E1 - Sales				E1 - Sales				
E2 - Marketing				E2 - Marketing				E2 - Marketing				E2 - Marketing				
E3 - IT				E3 - IT				E3 - IT				E3 - IT				

