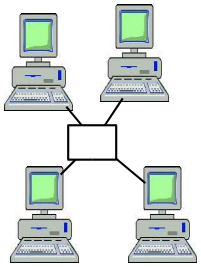
A workshop for ICCM
Tim Young
6/5/2004

Windows 101:

Summary: *This session covers the basics of using windows in a networked environment. How do windows computers communicate, and how should you set them up for the following configurations (and what do they mean): peer-to-peer, client-server (NT4), Client-server (Active Directory). In short, what do you need to know about what goes on in a small windows network.*

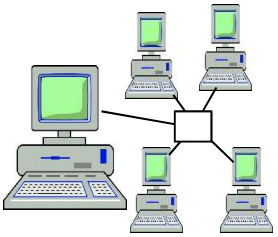
Why Network & what does Windows networking give you?

Since this is a 101 course we will assume very limited knowledge of networking. The first question is "what is networking and what does it give you?"



Peer to Peer

Windows networking allows files, printers, and some applications to be shared across multiple computers. One good use of networking allows you to have one computer with a good tape backup to backup all the important files from the other computers. You can have one printer and print to it from all the computers in the room. It allows you to have multiple entering data into one database (if the database allows for it to be used in a networked environment). It allows you to share one Internet connection.



Client / Server

If you have a network server, you can have more security on the network, enforce specific "rules", and speed up many aspects of the network. Servers can also provide many different types of functionality, from shared email to web content filtering and virus checking. This windows 101 session will mainly talk about how to network windows and what the various types of networking give you.

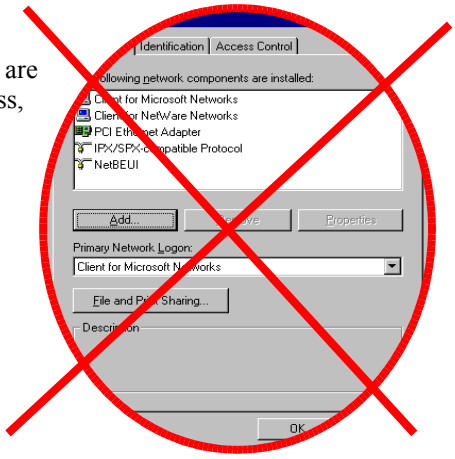
Accounts, logins, profiles, and groups.

If you have a server it allows you to set up logins for individuals and enforce the passwords for those logins. Under Windows 9x, you can have a login prompt, press [esc], and have access to the desktop. If you have a domain server and if the client is set up properly, then users cannot log onto the workstation (in graphical mode) without a password.

You can set up groups of users, and using the "group profiles" or "group policies" (depending on the version of Windows and Windows server) you can have certain restrictions to those groups. On systems using NTFS you can set file permissions per group or user (rejecting people from one group or allowing from another).

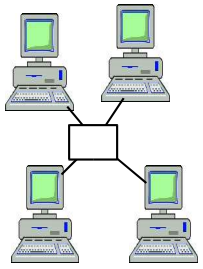
Networking Fundimentals:

Whether you use peer-to-peer networking or client/server networking, there are some network fundamentals. We will not get into the details in this 101 class, but suffice it to say that it is simplest to use TCP/IP for the "Network Protocol." Other protocols that are available, but you should not use, are: NetBEUI, IPX/SPX.



TCP/IP is what you will need to use if you ever surf the Internet, and after you have a small number of machines on your network, it turns out to be more efficient. In the long run, it is best to simply choose TCP/IP as the protocol. It is very important that every computer has the same "default protocol" set. If you have different default protocols, you will have a lot of problems.

Peer to Peer Networking:



Peer to Peer

Most people starting a Windows network begin with peer to peer networking. This simply means that there is no dedicated server that runs the special server software (Windows Server, Linux Samba Server, etc). Peer-to-peer means that all the computers are at the same level.

Because there are some tasks that do need a hierarchy, the peer-to-peer network contains an electoral system where the computers actually elect their temporary leader, named the browsemaster.

Broadcast packets: Most TCP/IP connections are from one computer to one other computer. If the destination computer hears a packet for itself on the network, it processes it. If it hears a packet destined for another computer, it ignores it. The "broadcast" packet is data that is sent to all computers, or to a computer that the source computer does not know who it is for. It is just sent out there in the hopes that someone will respond.

In Peer-to-Peer networking, a lot of broadcasting is necessary. This makes for a lot of traffic on the network that is not needed. If you have a "switch" (Not a hub), broadcasts are easy to see as all the lights flash simultaneously. The more often this happens, the slower your network will function.

Broadcast packets only go to the local network. It falls outside the scope of this 101 session to cover the scenarios where broadcasts fail because of, routers, VPNs, and subnets. If broadcast packets seem not to be getting through (computers do not appear on browse-lists), you can research the WINS server. For non-active directory networks.

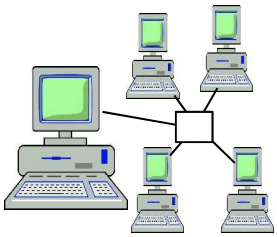
The "*Browse Master*" is the computer that holds the list of computers that show up in the network neighborhood. When a computer first turns on, it sends out a broadcast packet asking where the browse master is. It then registers itself with the browse master. Then, any time someone clicks on the network-neighborhood (or "My Network Places") the computer asks the browse-master for the list of computers.

There is an element of pride built into each computer. If the computer believes it is more capable of being the browse-master, it "forces an election." All the computers look deep down inside themselves and pull up a "random number" that somewhat represents themselves. They take into consideration their operating system and a few other factors, and then add an element of the random. This is their vote for themselves. They broadcast this out, the votes are tallied, and the one that voted themselves the highest becomes the new browse master. The browse master's first task is to ask for a census, making a current list of computers on the network.

Occasionally the computer that is the browse-master will be turned off as someone exits the office. The rest of the computers will not notice this immediately, but if you click on the network-neighborhood nothing appears for a moment. The computers will notice that their elected leader has vanished, so they will elect a new one, and then each computer will register itself with the new browse-master when the census is called for.

Note: *If you have a browse list that grows and shrinks, with some computers appearing and disappearing, it is usually because you have some computers that are set up with different "default protocols." These computers can participate in elections, just like any other computer, but when it wins the election, it proceeds to change the language to their personal "default." It would be like the USA electing a president who spoke English and French, and then having every communication from him being in French. When the census comes, those that do not speak French do not participate in it, and therefore do not appear in the browse-list.*

Client-Server networking:



Client / Server

There are two main types of Microsoft networking. All Windows computers can function in both worlds, but the computers work best under the leadership they were created to serve under. The switchover came with Windows 2000 and Active Directory. If you have an NT-server (NT3.5, NT4, etc) you definitely use the old style of leadership. Newer servers (2000, XP, 2003) can serve with either style of leadership, you can enable or disable the various services that are needed for the types of leadership.

Non-Active-Directory

Client-server networking on a non -active-directory network means that there is a master server that knows how to "stuff the ballot-box." The server always wins elections. You do still need to configure your clients not to hold elections; the democratic spirit is so ingrained into each computer that it will hold elections whether you have a defined server or not. The server will always win the election, but the clients will regularly force an election even though they will be thoroughly and resoundingly whipped. Since servers get to vote for themselves, they simply vote an order of magnitude higher than the poor clients can achieve, and the servers win hands-down.

So just because you have a server on the network does not mean all the electoral traffic gets removed.

You can, however, have multiple servers on the system. This can cause some problems with other services, but the servers usually vote between themselves for the honor of being the browse-master.

Active-Directory:

Once networks started growing very large, the electoral process with many computers is very "noisy." Microsoft designed "Active Directory" which uses a very different method of managing the computers and services on a network. It is based off standard Internet services that are modified for the specific uses of a Local Area Network. Active Directory is much more complex than the broadcasting and electoral method, and has a lot of room for error; but a well-configured network will run much more smoothly even if it is large. If you do not have an Active Directory Server, then you cannot use Active Directory.

LDAP

Much of the information kept by Active Directory is served using LDAP (A standard Internet service). But most people never need to know it is there, as most of the administration of the LDAP server is done through windows graphical interfaces that do not say anything about "LDAP." If you get into in-depth administration, you will come across this. But for the sake of simple windows networking, all you need to know is that LDAP exists on an Active Directory server.

DDNS (Dynamic DNS):

Instead of using broadcast packets to find the other servers on the network, Active Directory clients update a master list. This list is updated and accessed through DNS. But this list is more complex than the simple browse-list. Not only does it contain the various computers, but it also lists the various network services that those computers provide.

The server that holds the DNS is assigned that role when it is first set up (You can have a backup server if you have a need for that level of reliability).

Win95/98/ME and domain logins

The earlier versions of windows required multiple steps to force authentication from a server. You needed to:

Use "Client for Microsoft Networks" instead of "Windows Logon" as the primary network logon.
Check "log onto a windows domain" in the properties for "client for Microsoft Networks"
Under the network Access Control, choose "user level access control" and list the domain.

Windows 2000/XP Pro – Joining the domain
The NT based systems, once you join the domain, the computer is set up to work under that domain. Any user from the domain can log in on that computer. (It is possible to limit specific logons to that computer, but it is done from the server side.)

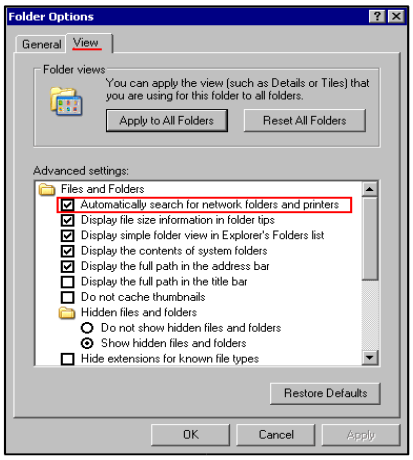
Setting up Active Directory:
Windows servers have a good "Active Directory Installation Wizard" that will walk you through the process of configuring a domain. The issue of primary importance is that you have a properly configured DNS server for that domain. See:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/enterprise/proddocs/en-us/sag_DNS_Chk_new_forest.asp

Upgrading or adding servers:
The process of upgrading is non trivial. There are tools and processes to do this but they lie far outside the bounds of this workshop.

If you were using peer-to-peer XP or 2000 computers and wish to create a new domain, there are some serious issues you should be aware of. The domain users, even if they are named the same as the previous users, will be different than the users on the computers. Thus, a user named "Tim" that has 2 years of files on his desktop, when he logs in as the domain user "Tim", those files may be inaccessible. The user's settings will also disappear, and there can be some heinous file permission issues. It is honestly simplest, if you have a small enough network, to either reinstall the operating system and software, or uninstall all the user software. Then Join the domain, and then install everything. Once this happens, the correct permissions will be set up for the individual packages, directories, and shared folders. There are other fairly complex ways to handle the situation, but nothing simple.

Particulars:
Win9x computers do not participate in most of an Active Directory environment. They can function but do not receive the full benefit. It is best to use Windows 2000 or XP Pro. Microsoft does have patches for Win98 to allow it to participate better in the domain. These are on the Windows 2000 server and 2003 server CD. And on the Internet here:
http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp

Windows XP does do some broadcasting to find services on other computers. By default it will probe all the computers on the network to see all folders and printers that are shared. On a large network this is very annoying and can cause a lot of traffic. It is easy to disable this by opening "folder options" from the explorer window, and going to "view." You can then uncheck the "automatically search for network folders and printers"



XP Pro vs. XP Home.
http://www.microsoft.com/windowsxp/pro/howtobuy/choosing2.asp
http://www.winsupersite.com/showcase/windowsxp_home_pro.asp
XP Home is not a managed operating system. Most of the tools that are used for making the system administrator's job easier are not in the Home version. XP Home does not have support for Active Directory, but behaves reasonably well in a peer-to-peer network.

http://support.microsoft.com/?id=314882
"For Windows XP Professional, the maximum number of other computers that are permitted to simultaneously connect over the network is ten. This limit includes all transports and resource sharing protocols combined. For Windows XP Home Edition, the maximum number of other computers that are permitted to simultaneously connect over the network is five."

Windows 95/98/ME had a simultaneous connection limit of 100.

Checklist:

Specific clients on various systems

For all computers all types of networking:

Default protocol: Make sure the default protocol is TCP/IP

TCP/IP addresses set: Make sure all the addresses are in the same subnet

I recommend 192.168.0.x Where x is a digit starting at 20 and counting up

If you use Internet Connection Sharing or a firewall that has DHCP installed on it, you do not need to manually set the DHCP address. You can use the "automatically assign an address" option.

Netmask:

Usually this is 255.255.255.0

If someone uses an address like: 10.0.x.x they might use 255.255.0.0 If you use the recommended TCP/IP address, just use 255.255.255.0.

Gateway:

The gateway computer is the IP address of the computer that connects to the Internet. If you use Internet Connection Sharing this will be automatically set for you if the clients are set to "get the IP address automatically"

Computer Name

This needs to be distinct for each computer.

Workgroup / Domain

This should be the same for each computer unless the network gets fairly big.

Enable "file and print sharing" (Win9x)

Peer-to-peer networks:

If all the computers are in the same workgroup and adhere to the above defaults, you should have good peer-to-peer networking.

Note: *You should never have the c:\windows directory shared (or the c:\ directory for that matter). This is one of the favorite ways for viruses to propagate. It is best to simply have a shared folder, not a shared drive.*

Client-Server networks:

Win9x

- Use "Client for Microsoft Networks" instead of "Windows Logon" as the primary network logon.
- Check "log onto a windows domain" in the properties for "client for Microsoft Networks"
- Under the network Access Control, choose "user level access control" and list the domain.
- Install the Active Directory hotfix if connecting to an AD network.

Win NT, 2000, XP

- Set up the server
- Join the domain

Note: *You should never have the c:\windows directory shared (or the c:\ directory for that matter). This is one of the favorite ways for viruses to propagate. It is best to simply have a shared folder, not a shared drive.*

Note on TCP/IP:
If you are setting up TCP/IP on a peer to peer network, you have a few options available to you. If you have no shared connection to the Internet, you can set the IP addresses by hand. For many reasons that I will not expound upon, I recommend using the IP address range from 192.168.0.1 – 192.168.0.254 This range has the subnet mask of 255.255.255.0 The computer with the IP address ending in 1 or 254 is usually used as the "gateway" when you do have an Internet connection, so you should not use those. I usually recommend starting at IP address 20 and counting up.

You can also turn on Internet Connection Sharing on a computer (Windows 98, ME, 2000, XP) Part of the Internet Connection Sharing system is a DHCP server that will automatically assign IP addresses to the computers. You can do this even if you do not share one connection to the Internet, but it does help if you want to allow all your computers to dial out through the same phone connection.
Note: *You should only have one computer with Internet connection sharing enabled, otherwise you will have significant problems!*

Or you can purchase a small DSL firewall/router for $40 and use the DHCP service on it to give the IP addresses to your computers. This is probably the simplest option that has the most flexibility.