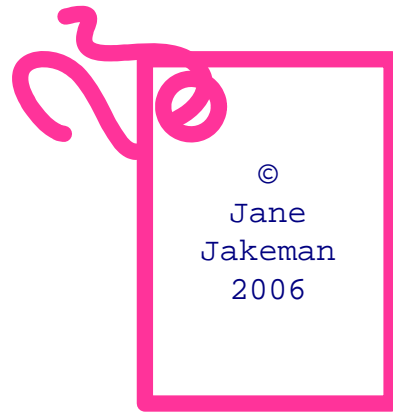


Contents

Original Assignment	Pages (i) to (iv)
Self Evaluation	Page (v)
Task One A	Pages
Task One B	
Task Two	
Task Three	
Task Four	
Task Five	
Task Six	
Appendices	
Appendix (a)	
Appendix (b)	

HARTS AND MINDS



NETWORK AND USER SECURITY

by
Jane Jakeman
6 May 2006

Report / Assignment Check list

Requirement	Student Checked	Tutor Checked
Assignment Front Sheet attached	X	
Assignment briefing notes & marking criteria attached	X	
Front page / Cover sheet	X	
Contents page	X	
Task /Section Dividers used	X	
Introduction to tasks / sections	X	
Headers & footers on all pages (See footnote)	X	
Page numbers are correct and on <u>all</u> pages	X	
All diagrams, charts and drawings have titles and dates	X	
Fonts, line and paragraph spacing meet requirements (See footnote)	X	
Headings with page break and appropriate use of sub headings	X	
Bibliography (& Glossary) included if appropriate		
Appendices included as appropriate and clearly labelled and indexed	X	
Task Time analysis included	X	
Self evaluation included	X	
Hard copy of PowerPoint slides included if assignment involved a presentation		
This tick list included behind assignment front sheet	X	
No polythene pockets used	X	
All items collated and ring bound	X	

Student Self Evaluation of Assignment

Date Completed:16 June 2006

ASSIGNMENT PLANNING**Comments on Time Management**

i.e. comparison of planned time and tasks versus actual time and tasks achieved

This assignment took me longer than planned, an additional 10 hours. This is mainly because of computer issues dealing with screenshots and time taken to learn IP addressing and subnetting.

ASSIGNMENT SELF EVALUATION

I found the class-work extremely helpful with this assignment and appreciated the detailed handouts provided which made it easier to learn about networking. I am quite pleased with the assignment overall and in particular with the IP addressing and subnetting and my knowledge of networking which I now understand.

Things which were difficult and I am not happy about:

My computer couldn't manage a large document with lots of screenshots. I used the computers in Oasis most of the time and particularly to prepare the screenshot part of the assignment, however, even the computers in Oasis 'froze' several times whilst preparing this assignment. I will need to purchase a higher spec. pc for future work.

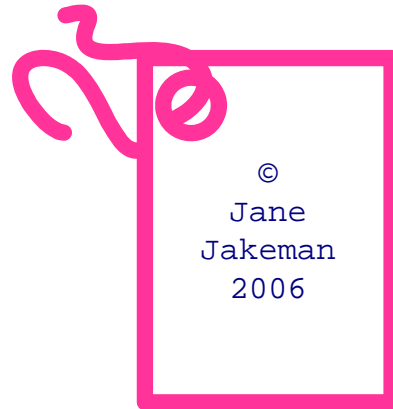
Things I would do differently for the next assessed task:

Try and manage screenshots in a more efficient way.

Any other comments

None

HARTS AND MINDS



TASK ONE A SPREADSHEET

by
Jane Jakeman
6 May 2006

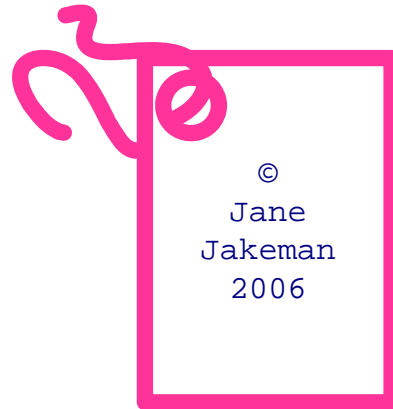
Task One A

Produce a spreadsheet that lists all users with the following information:

- name
- password
- username
- department they are a member of
- their role, staff or manager
- group membership
- shared folder access
- printer access
- application access

Please see Appendix (a) attached - copy spreadsheet.

HARTS AND MINDS

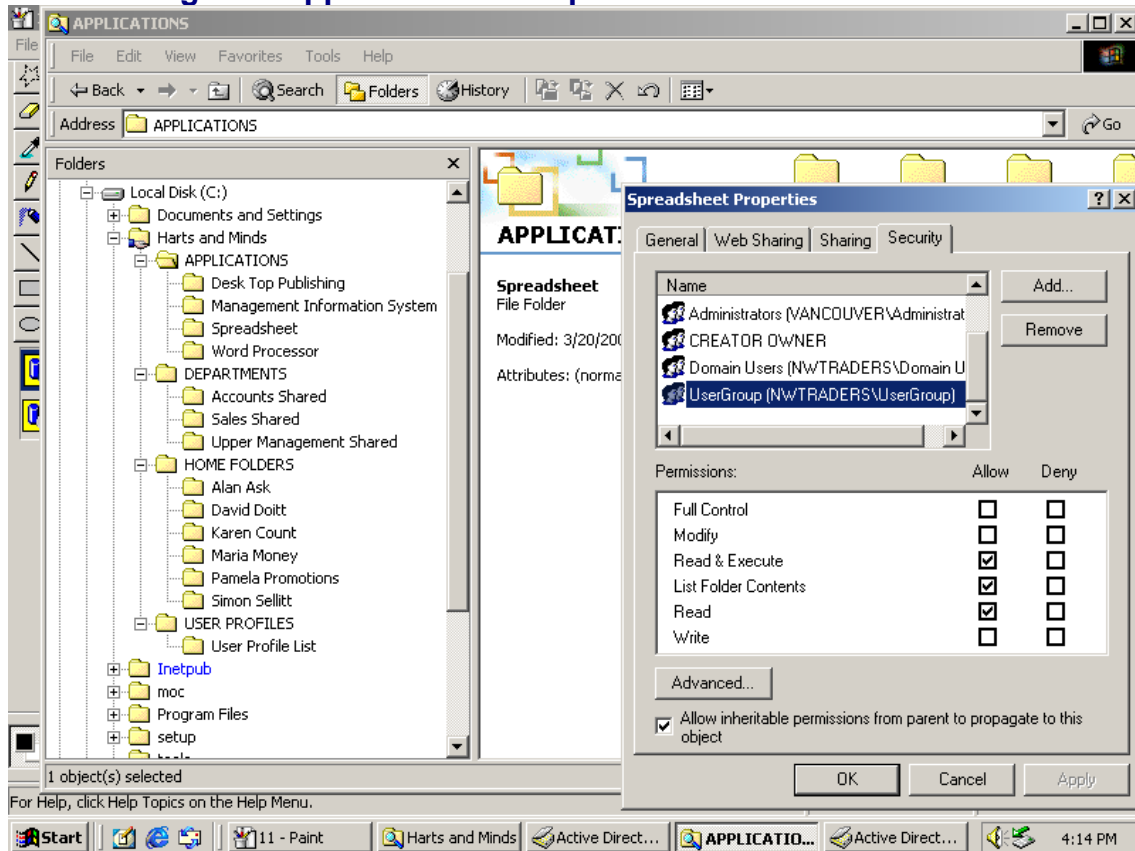


TASK ONE B FOLDER DESIGN

by
Jane Jakeman
6 May 2006

Task One B

Folder design to support network requirements.



The above screenshot shows the Harts and Minds Shared Folder with the necessary sub folders.

Setting Folder Security

- each user will be required to log in to the Harts and Minds Shared Folder.
- once they are logged in each User's rights will be set as determined by Harts and Minds Group Policy

The reason why I have used this design

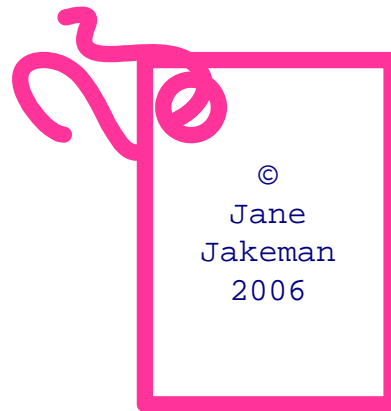
- it follows a similar logical design of Windows file system
- it allows for growth of the company, and of Applications
- it is easy to see at a glance which Applications are available for Users.
- it is easy to add, update and delete User Folders as and when they commence employment, change name, or leave,
- the Profile Folder is clearly marked and will be easy for a new Network Administrator to locate
- grouping Departments under one Folder is clear for users to locate in the computer filing system and makes permissions easier to grant.
- it allows for a new department to be set up, the new department would simply be added as another folder under Departments
- it aids the security of files

Therefore this system generally is easy to follow, easy to identify files, easy to add and delete users and departments and allows for expansion (and contraction) of Harts and Minds as a company.

The reason why the security is set at these levels is to:-

- comply with the Harts and Minds Network Administrator instructions as per the spreadsheet showing users rights and permissions
- reduce the Application Licence cost as much as possible
- prevent one user accidentally accessing and altering another user's work without permission
- appropriate users may access shared folders when they wish to do so or are required to do so
- promotes the company's control of sensitive information
- a User is able to set up their own filing system, within their own folder

HARTS AND MINDS



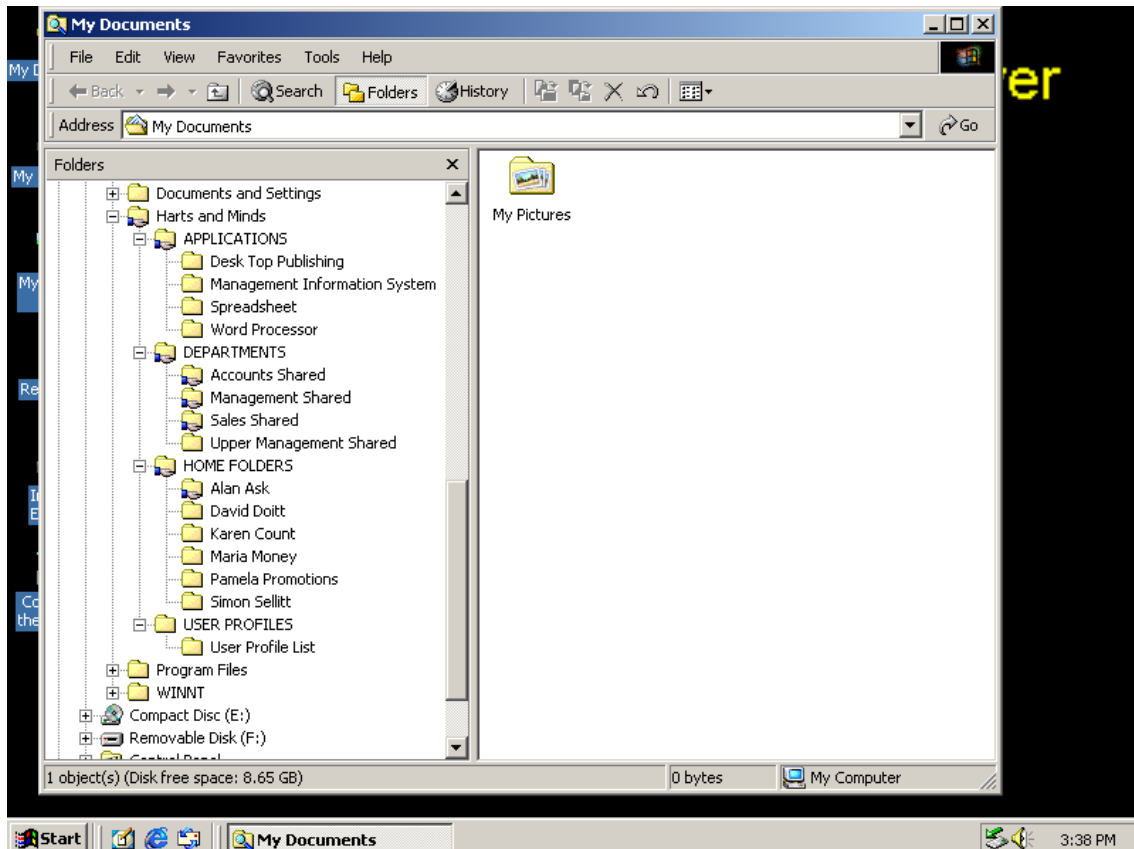
TASK TWO IMPLEMENT DESIGN INSTALL PRINTER

by
Jane Jakeman
6 May 2006

Task Two

On your local machine implement the design for your user and application folders within the root C:/.

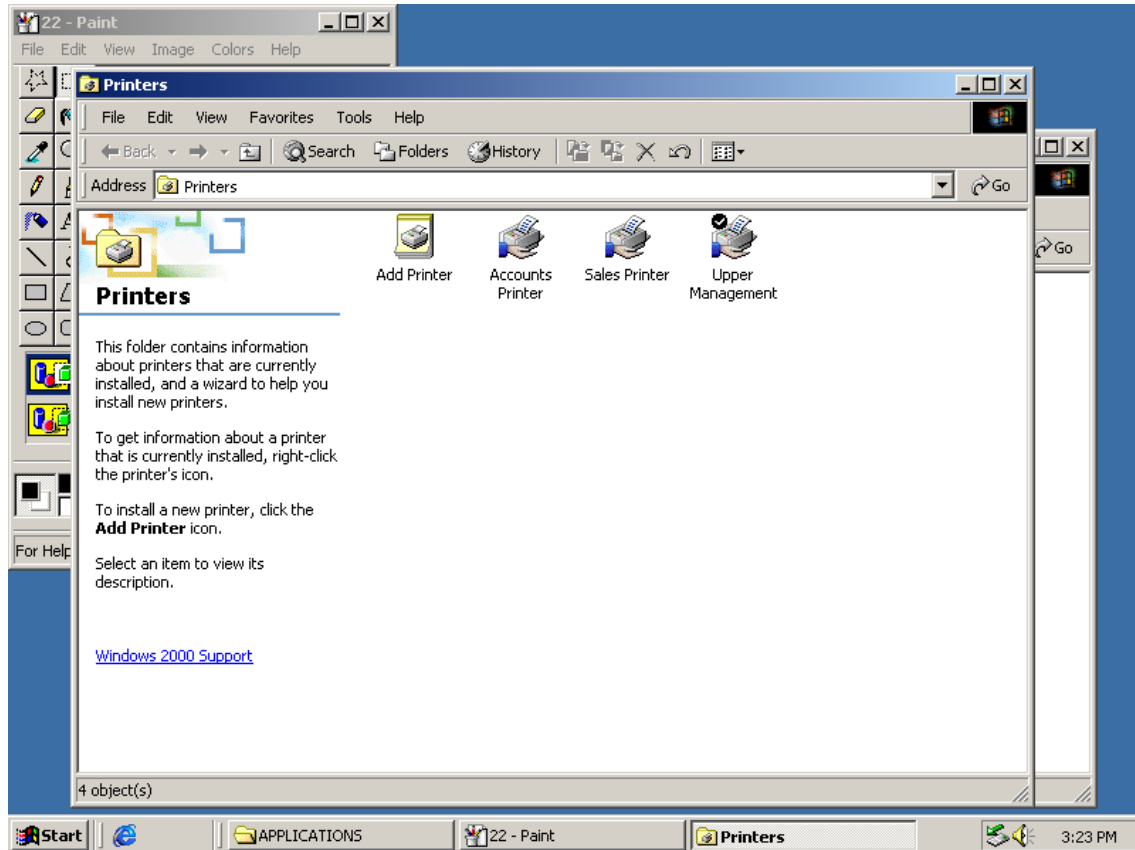
The screenshot below shows the folder design in the process of user rights being set up. The 'hand' underneath each folder denotes that sharing is allowed.



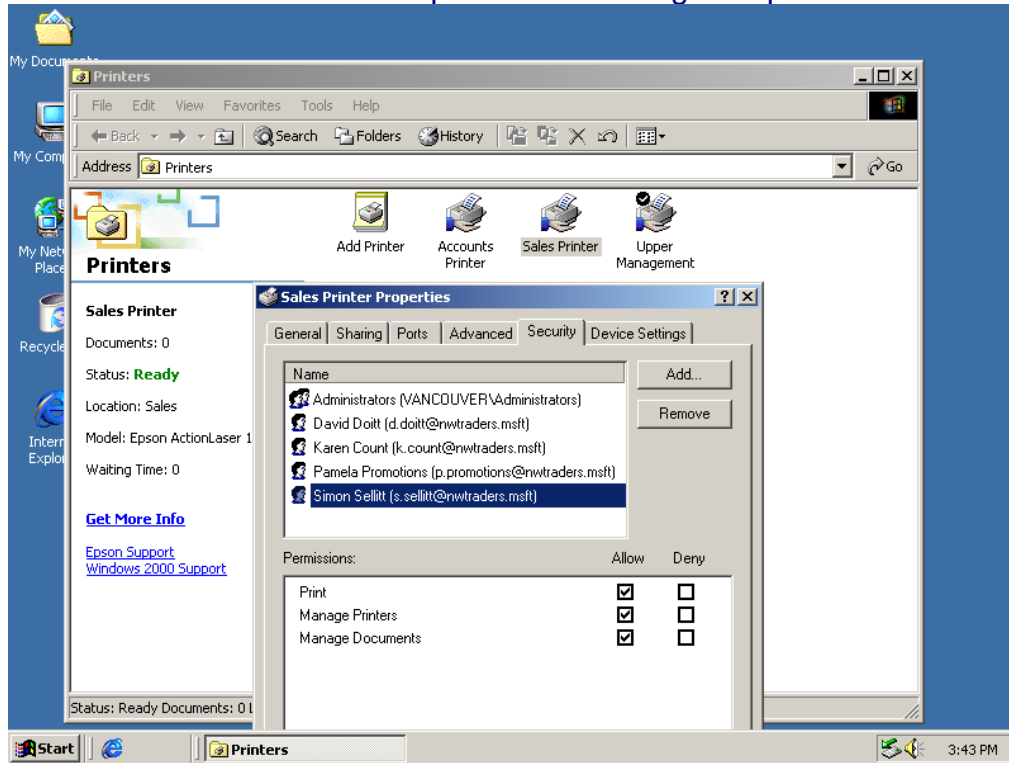
In the screenshot above, under HOME FOLDERS Alan Ask's Home Folder has accidentally be implemented for sharing. This showed up later in testing and was amended so that only Alan Ask could access his Home Folder.

Install a printer for each department

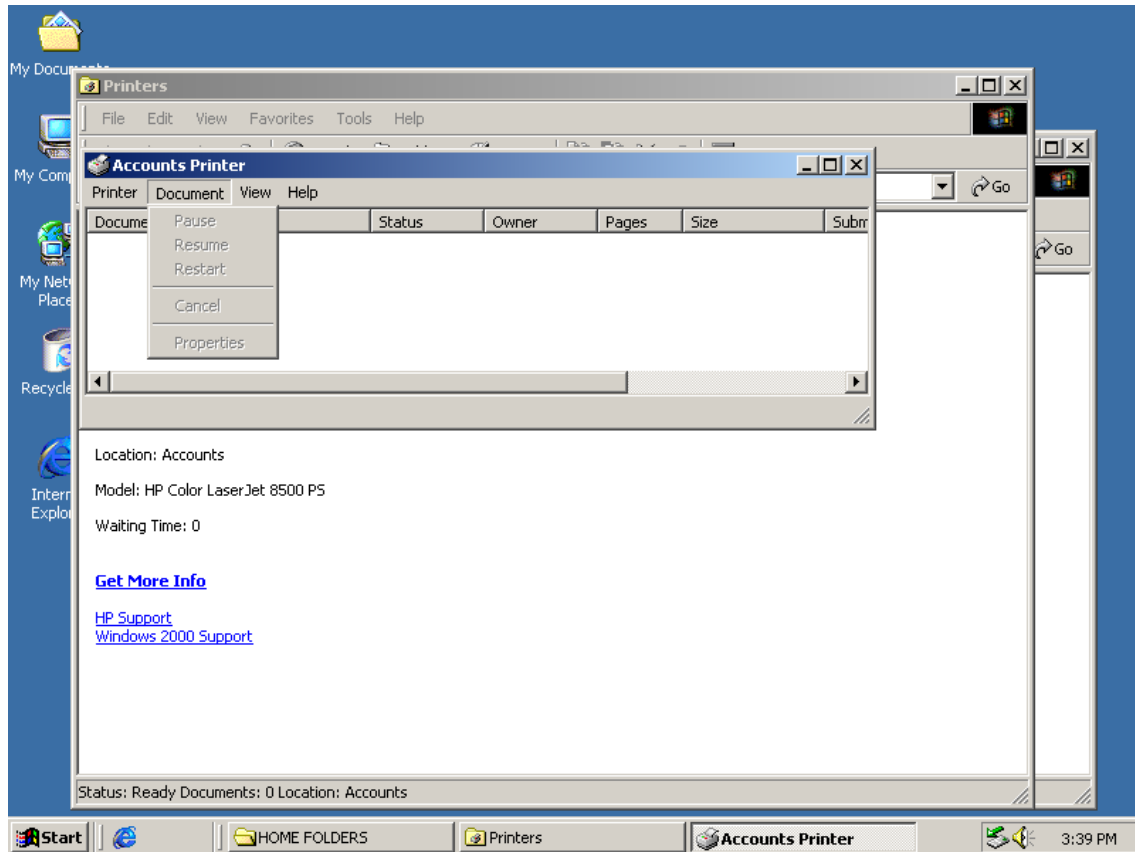
As the screenshot below shows, a printer has been added for each department. The tick means that the Upper Management printer in this instance is the default printer. Each user's settings are directed to their department's printer as a default.



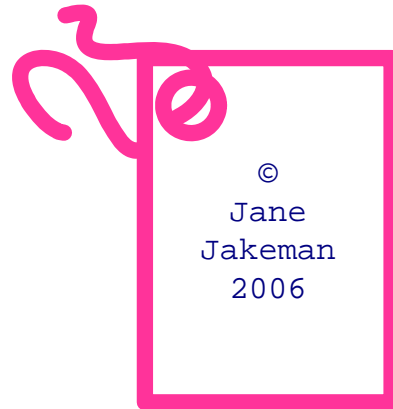
The screenshot below shows permissions being set up:



The screenshot below would normally show the print que, unless a User was not allowed access. In this exercise, although network printers were selected, the Menu is greyed out, meaning there is no access to these Menu items. In this instance it is because the printers do not really exist, in an actual situation it may be because the person does not have access to that particular Menu item of the printer, i.e. they may not be allowed to manage the document que, or cancel documents that are in the que to print.



HARTS AND MINDS

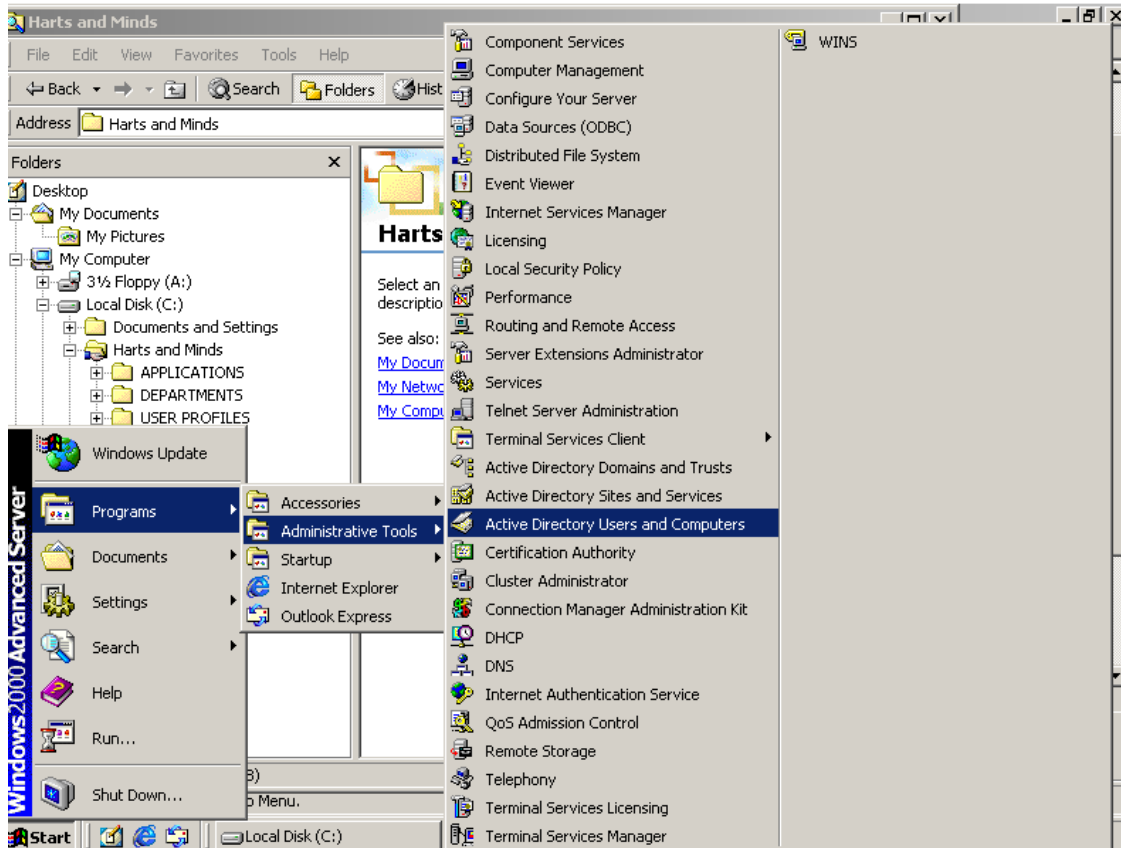


TASK THREE ACTIVE DIRECTORY

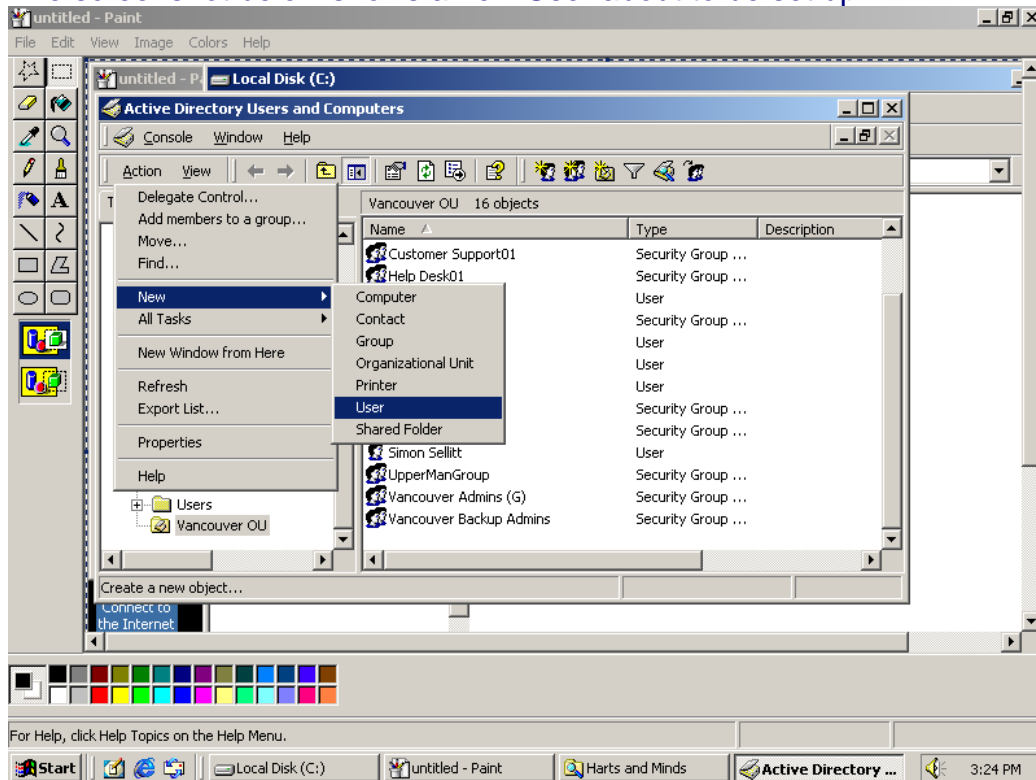
by
Jane Jakeman
6 May 2006

Task Three

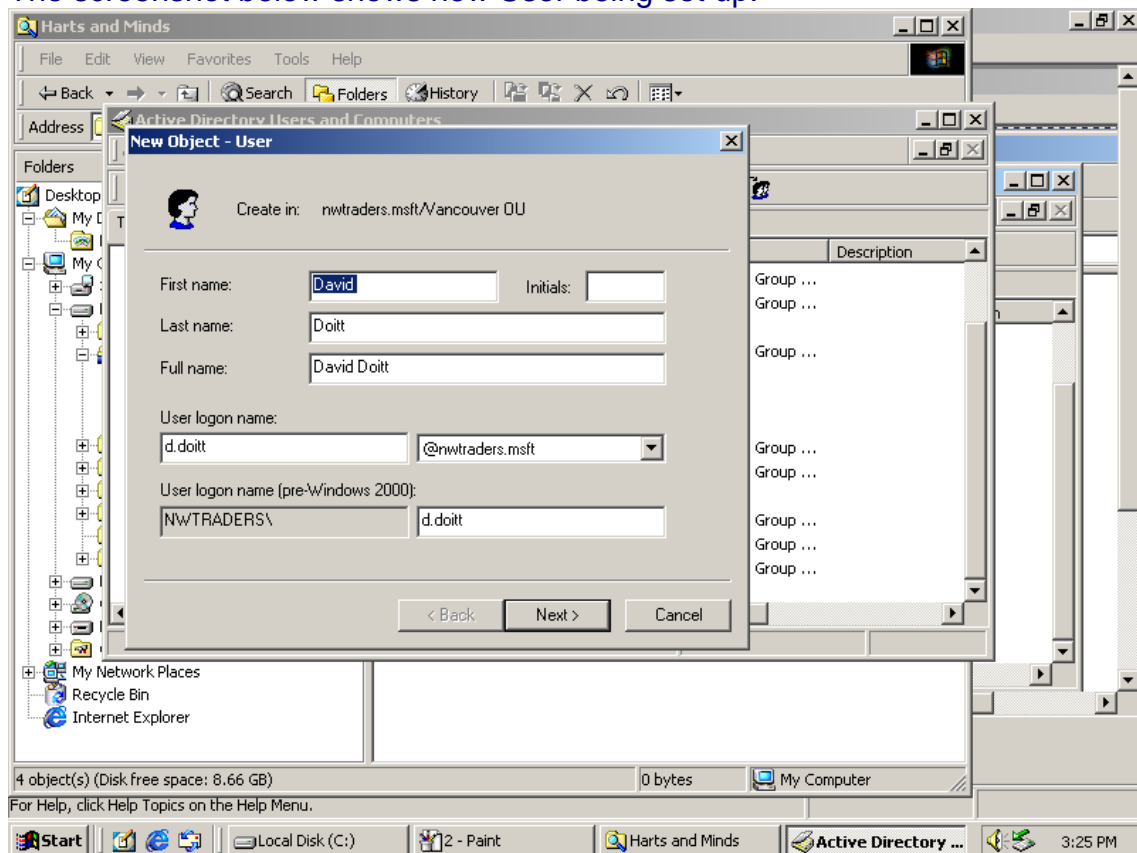
Within Active Directory implement your design, your user accounts, security groups and configure any membership required.



The screenshot below shows a new User about to be set up:

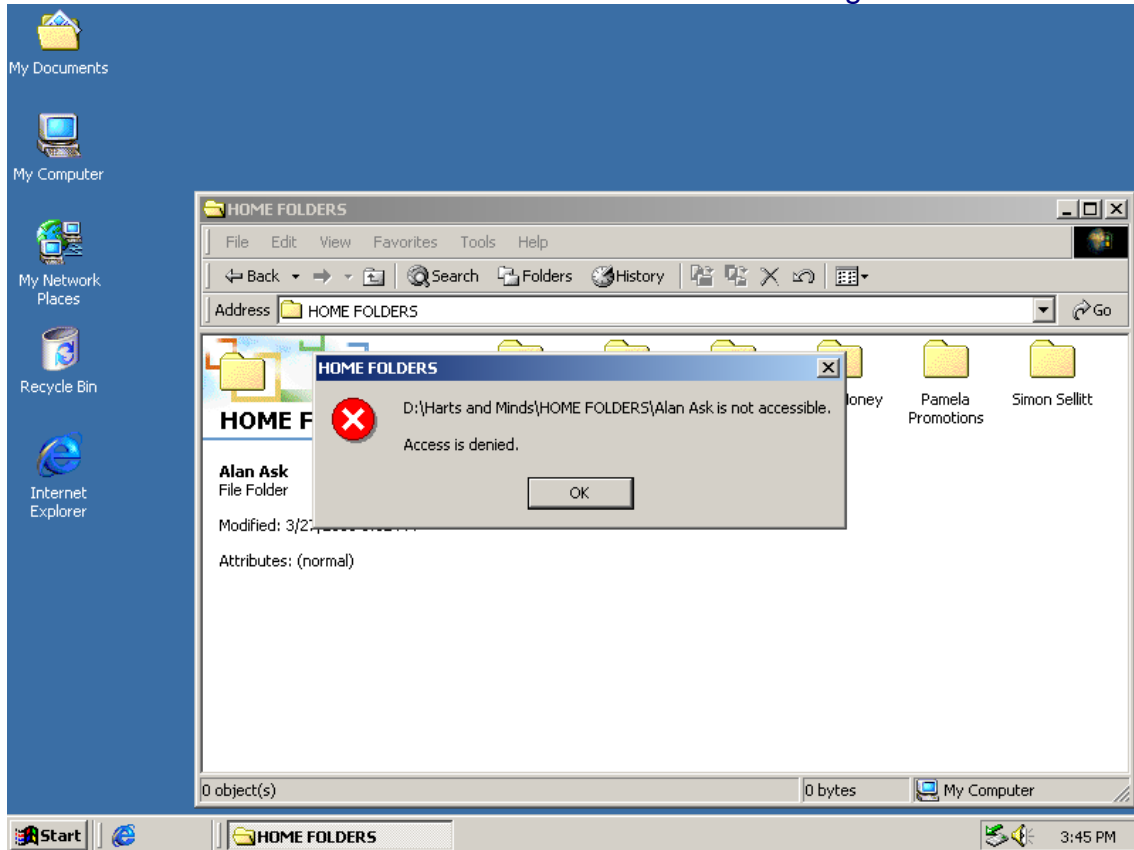


The screenshot below shows new User being set up:

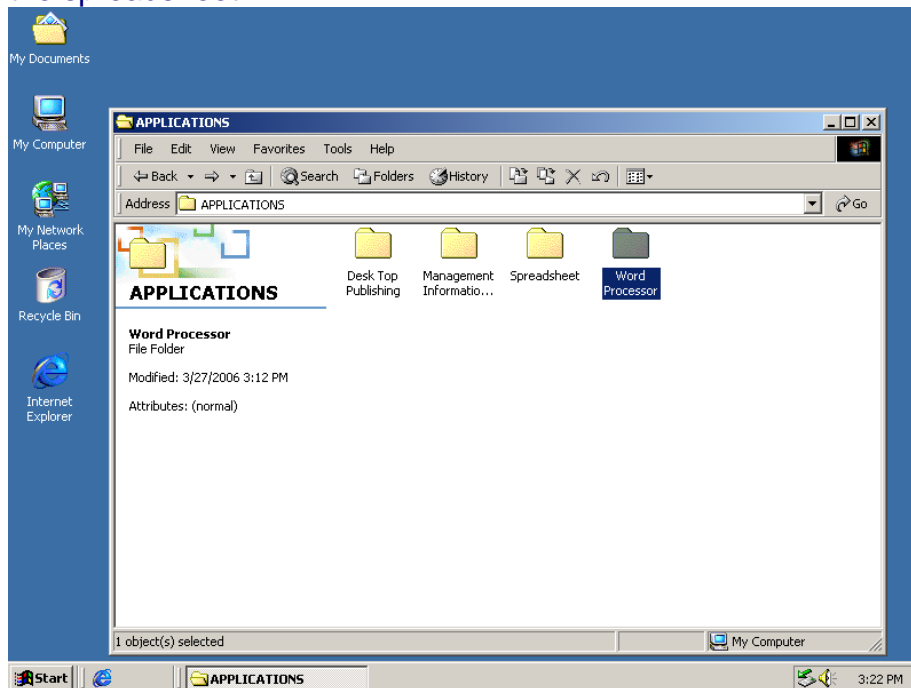


In the file system implement the security requirements for the home folders, profile folders and application folders that are required.

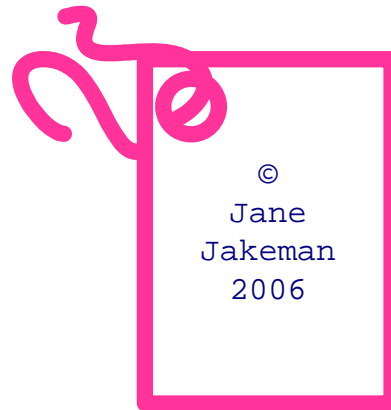
The screenshot below shows that access is denied to Alan Ask's Home Folder. This is because when testing, I logged in as a different user, not Alan Ask, and tried to access his Home Folder and this is the error message I received.



The screenshot below shows the Applications in a separate folder and relevant permissions were set up with each user or each group whether or not they could access some or all of the Applications dependent upon what is stated in the spreadsheet.



HARTS AND MINDS



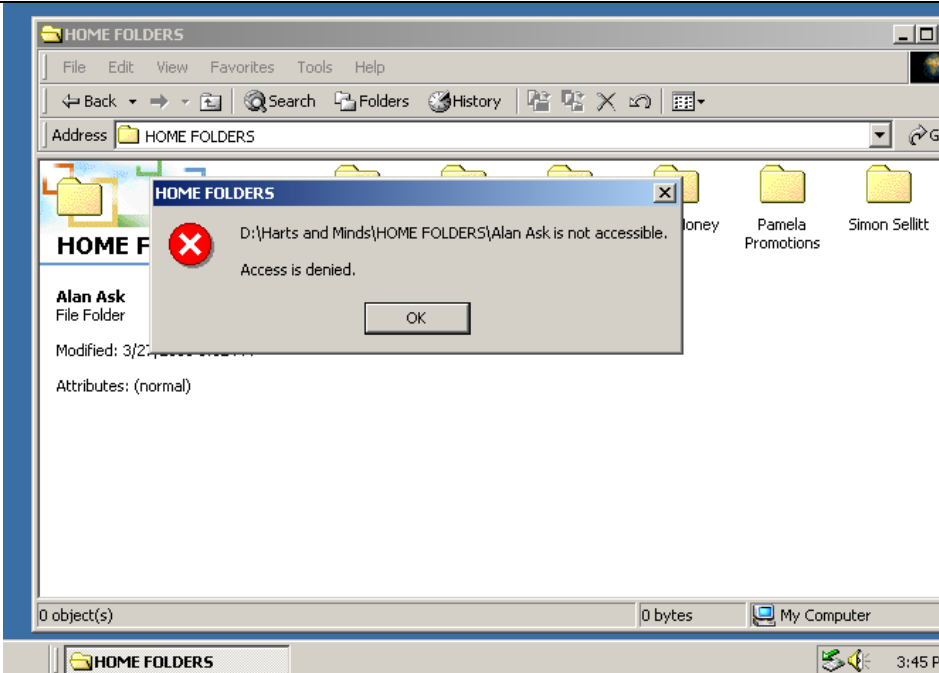
TASK FOUR TEST PLAN

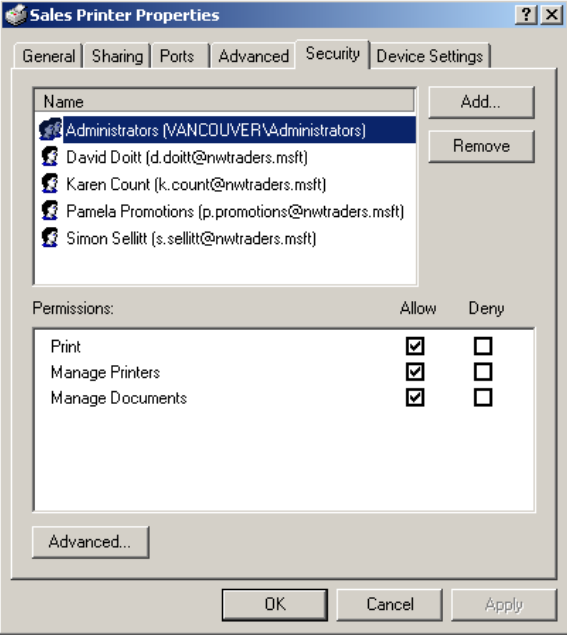
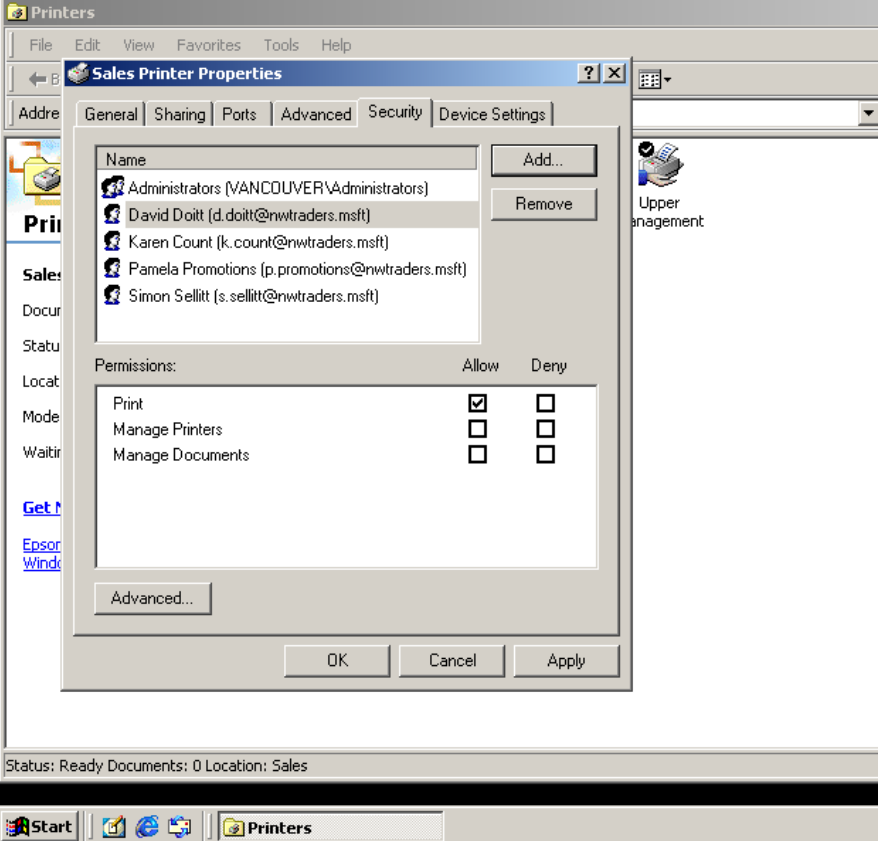
by
Jane Jakeman
6 May 2006

Task Four

Test Plan

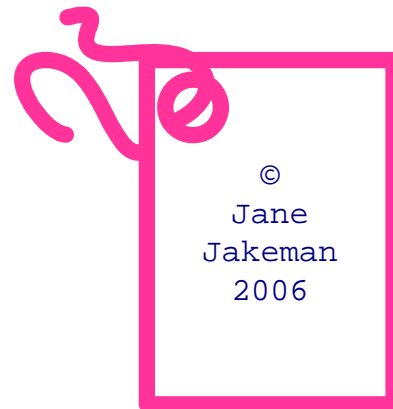
Testing was carried out whilst under development and some errors were found. These were corrected at development stage and once development was complete, the written test plan was then conducted and all was found to be working as expected.

<p>Can a User login with the wrong password?</p>	<p>No</p>
<p>Can a User login with their correct password</p>	<p>Yes</p>
<p>Can all Users access their home folder?</p>	<p>All users can access their Home Folder.</p>
<p>Can Users access other users home folders? No.</p>	

<p>Can users access correct printer?</p> <p>Yes</p>	
<p>Can users print to their own department printers?</p> <p>Yes</p>	
<p>Do Managers have full control over their department printer? I.e. can they manage the print que?</p>	<p>Tested ok</p>

Upper management print to all printers	Tested ok
Users access only applications entitled to	Tested ok
Enter a new User to a Security Group	Permissions tested ok
Password change requested at first User use	Tested ok

HARTS AND MINDS



TASK FIVE STEP-BY-STEP GUIDE TO A NEW ADMINISTRATOR

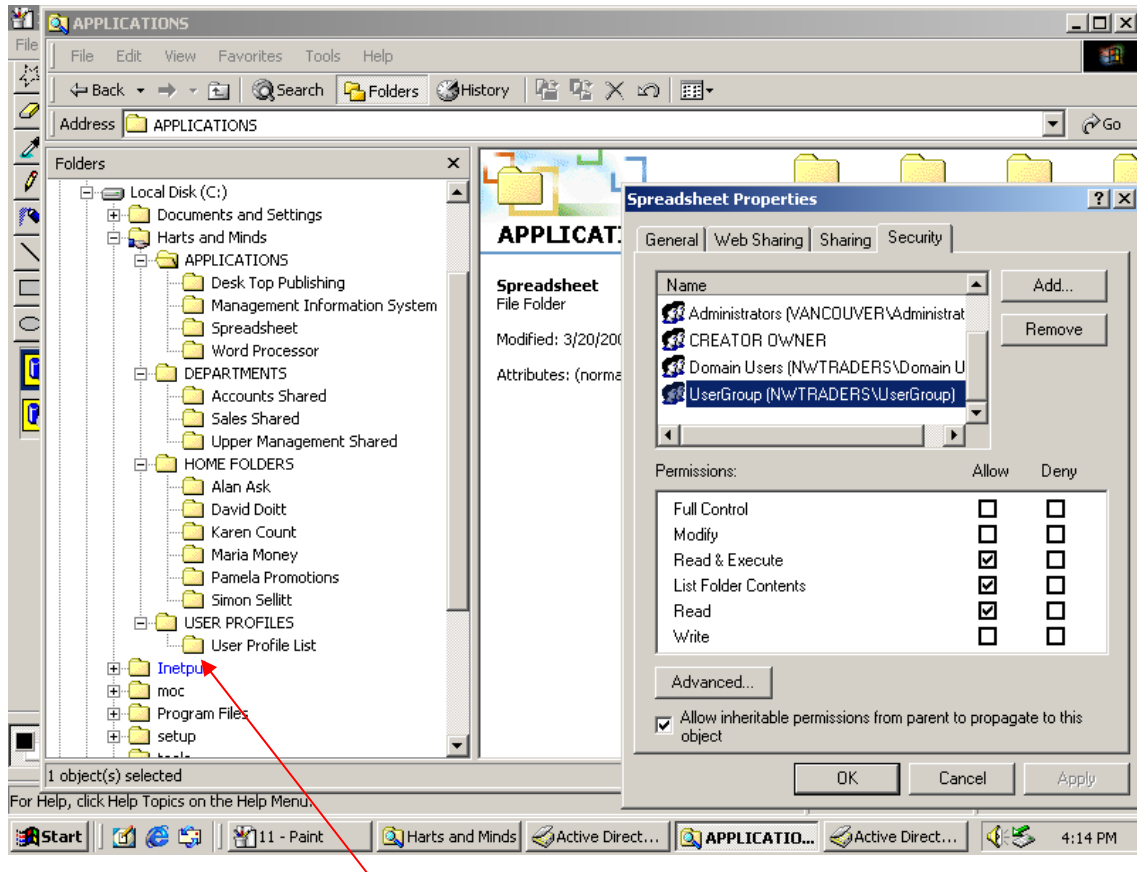
by
Jane Jakeman
6 May 2006

Task Five

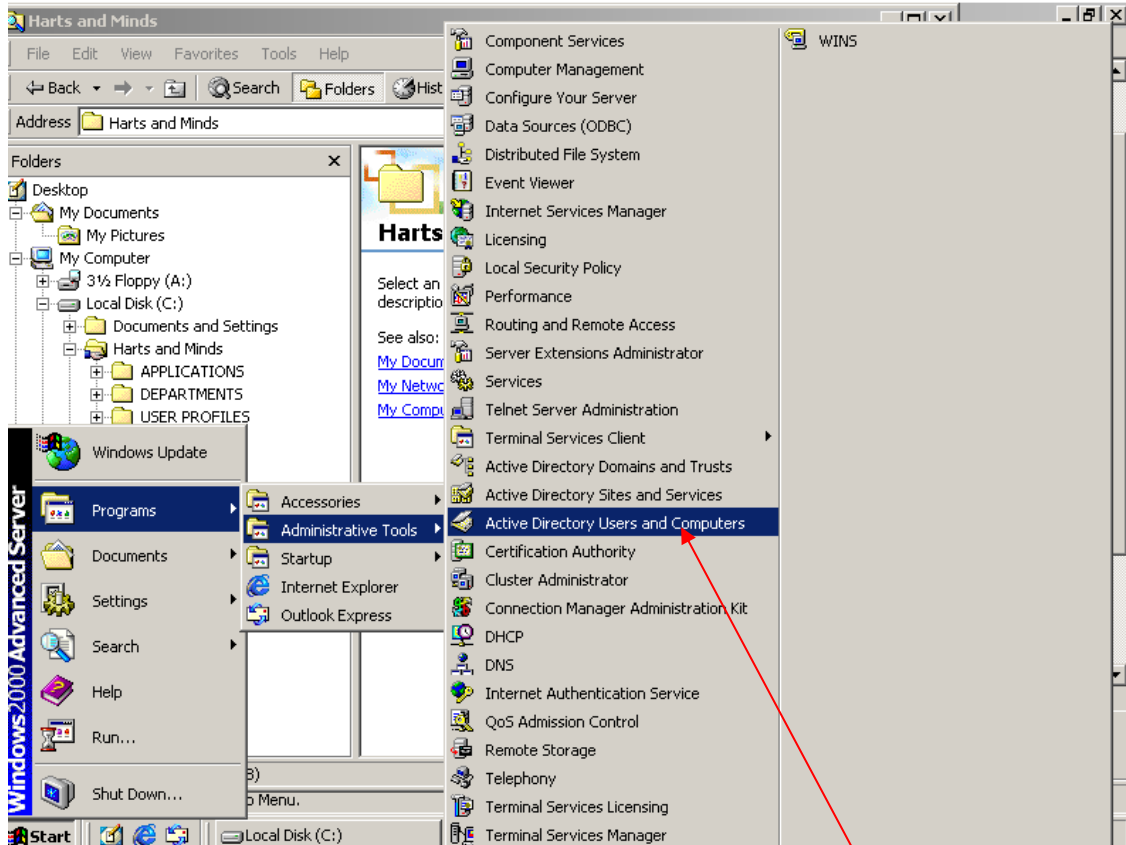
Step-by-step guide

Step 1

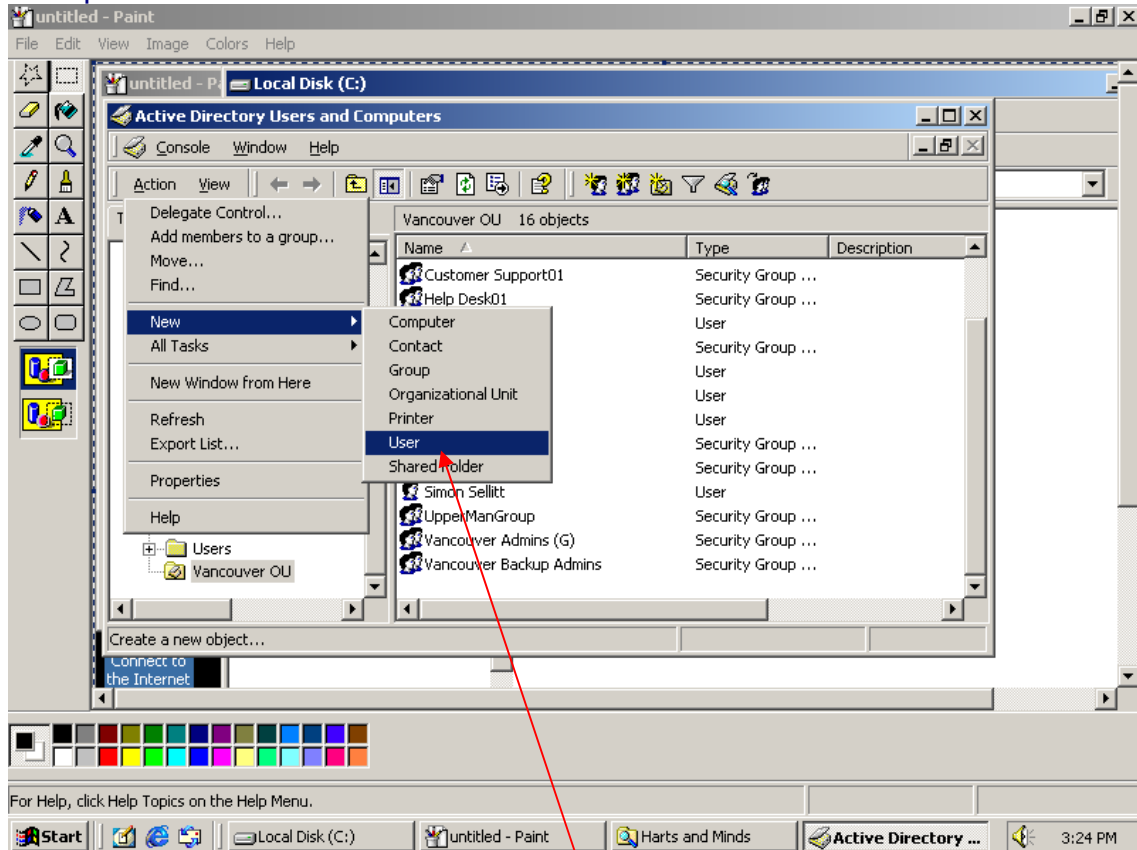
Print a copy of User Profile List which is located at C://Harts and Minds/USER PROFILE/User Profile List.doc



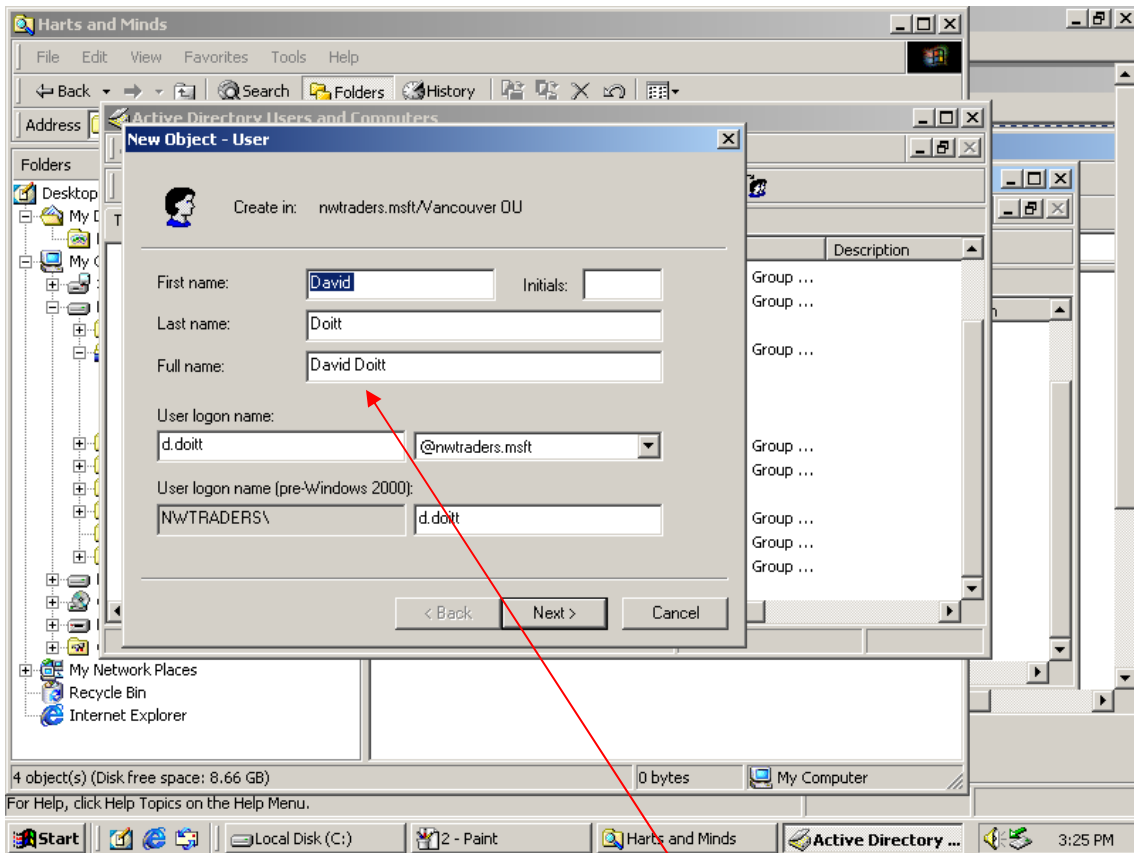
Set up the permissions by using Active Directory



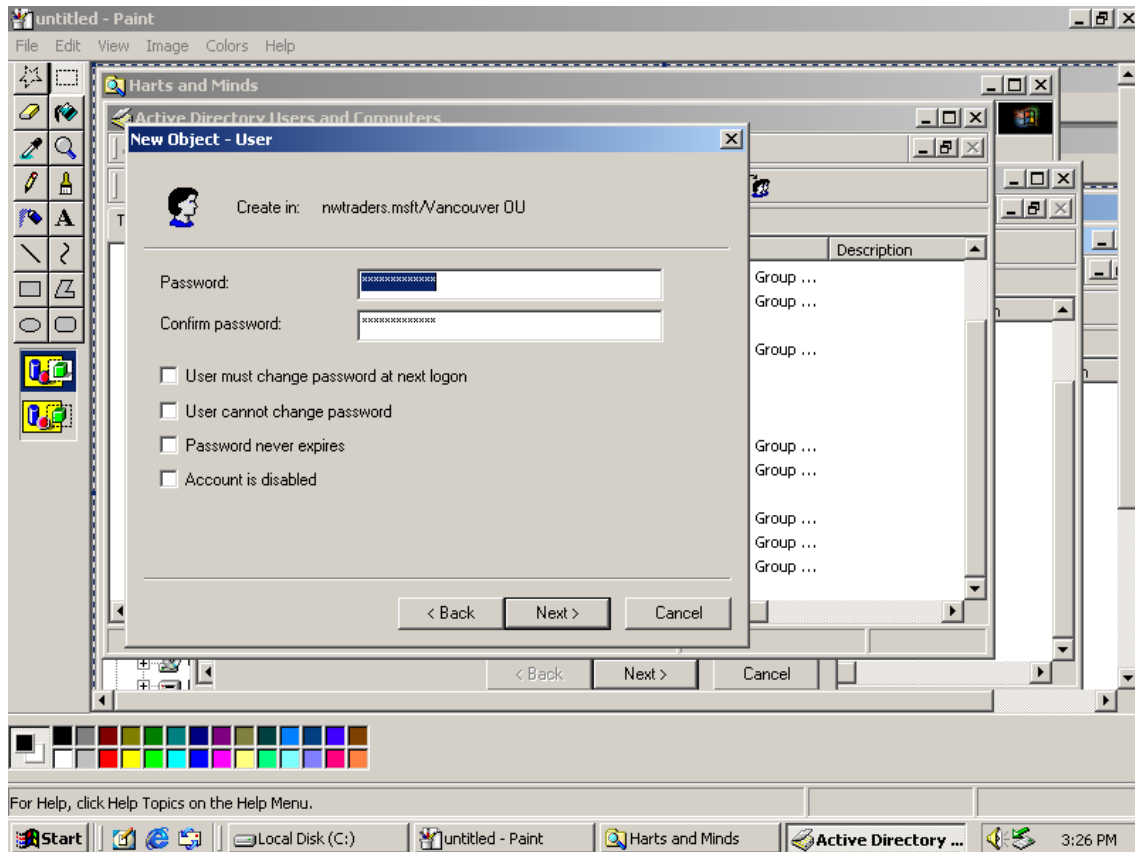
Set up each new user



For example, this is a new user being set up network. Complete all the fields with the correct information as taken from the spreadsheet.

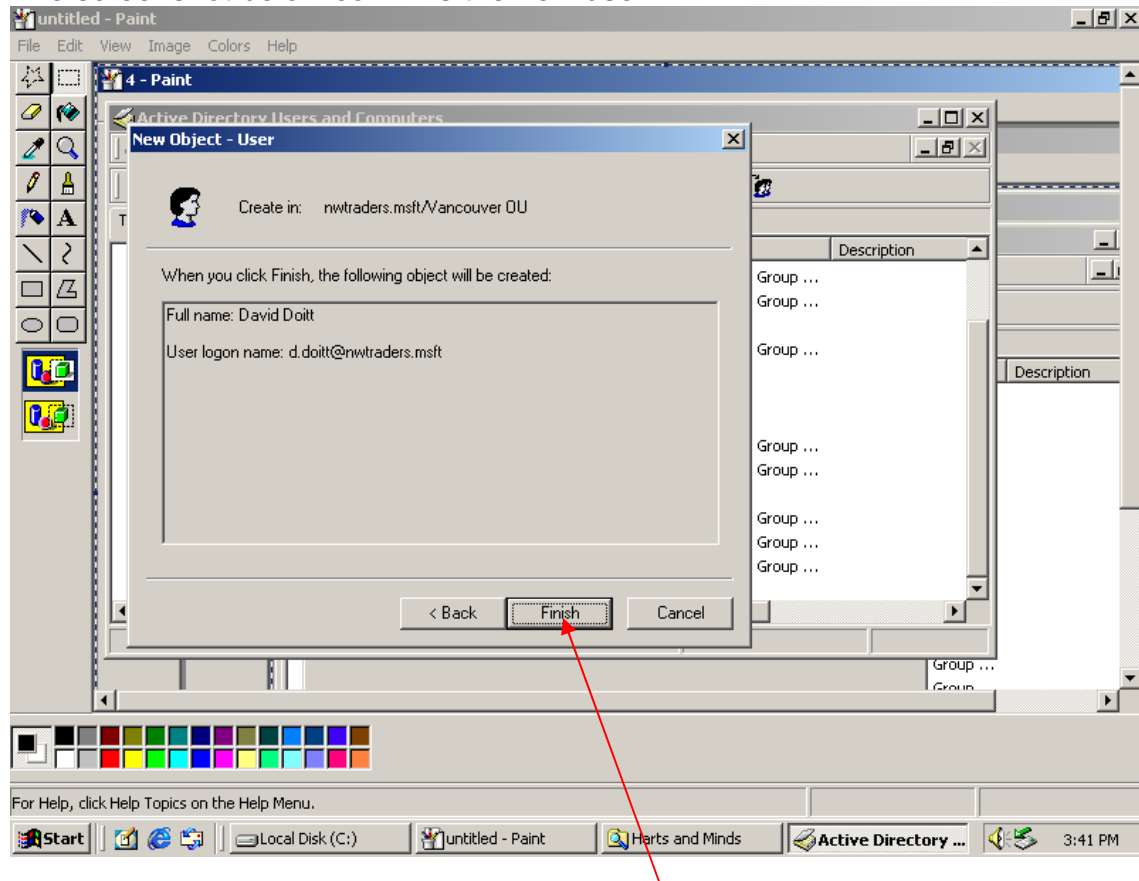


Continue to complete the fields

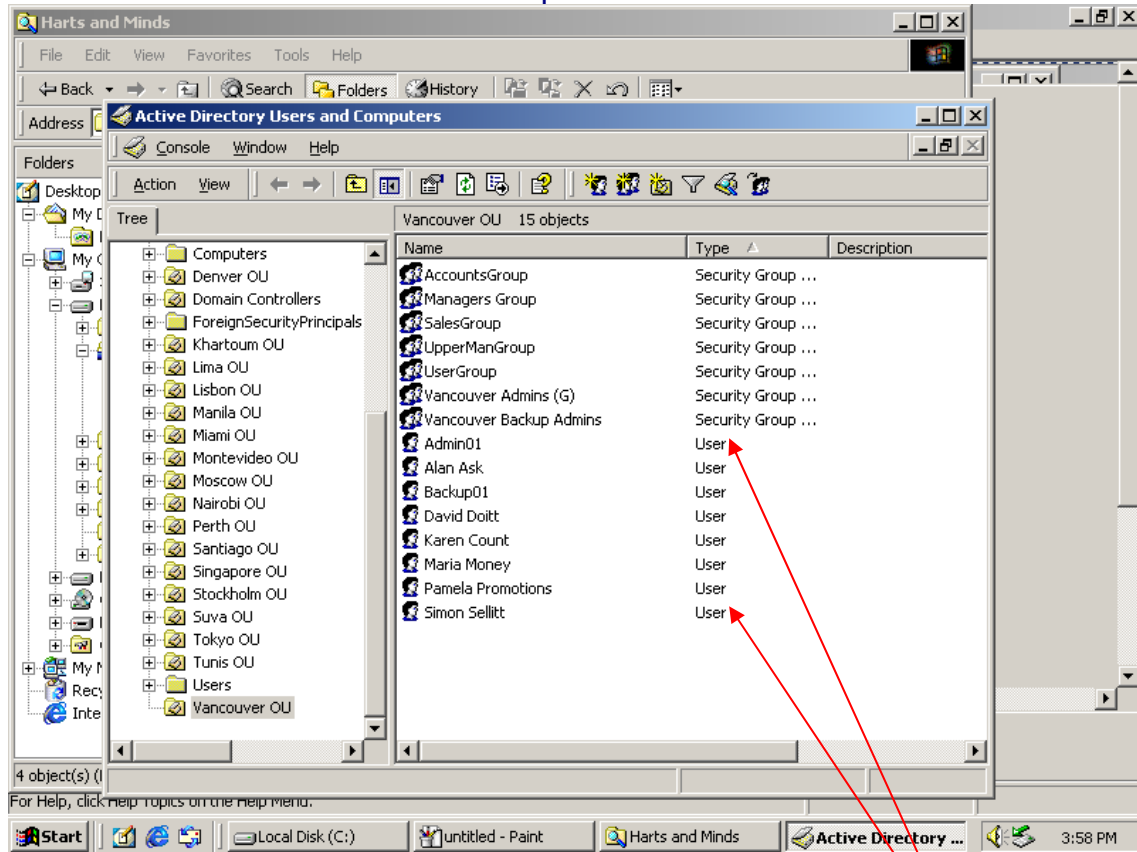


In the screenshot above, select “User must change password at next logon” (which is Harts and Minds network policy).

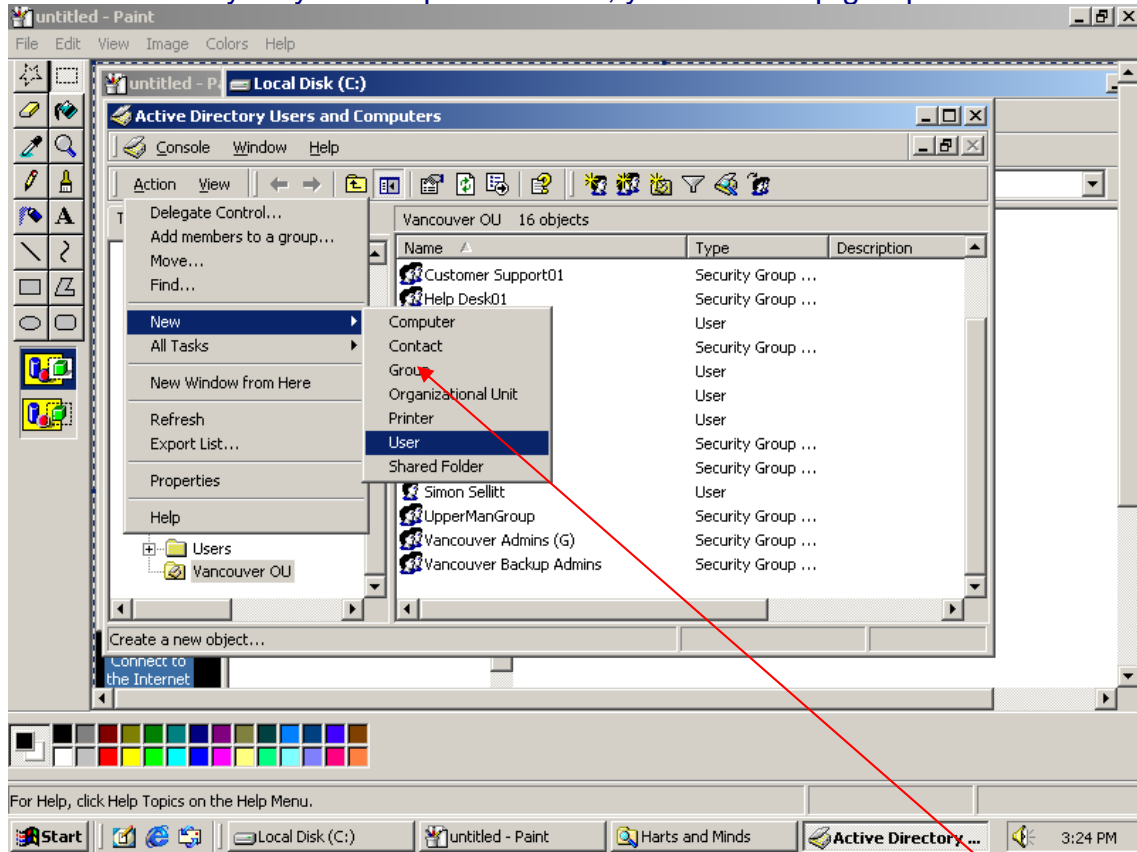
The screenshot below confirms the new user



This screenshot shows all users set up

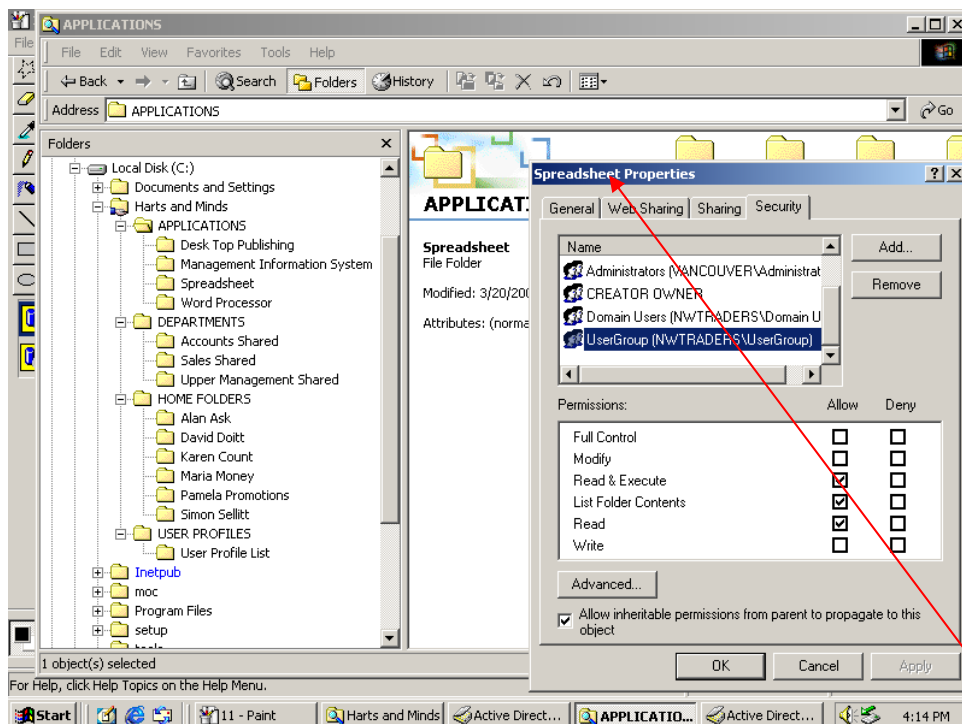


In the same way as you set up a new user, you can set up groups



Select "Group" instead of "User" in the above screenshot and then make a group for each department, putting each user in the correct department.

The screenshot below shows the User Group being given rights to Spreadsheet.

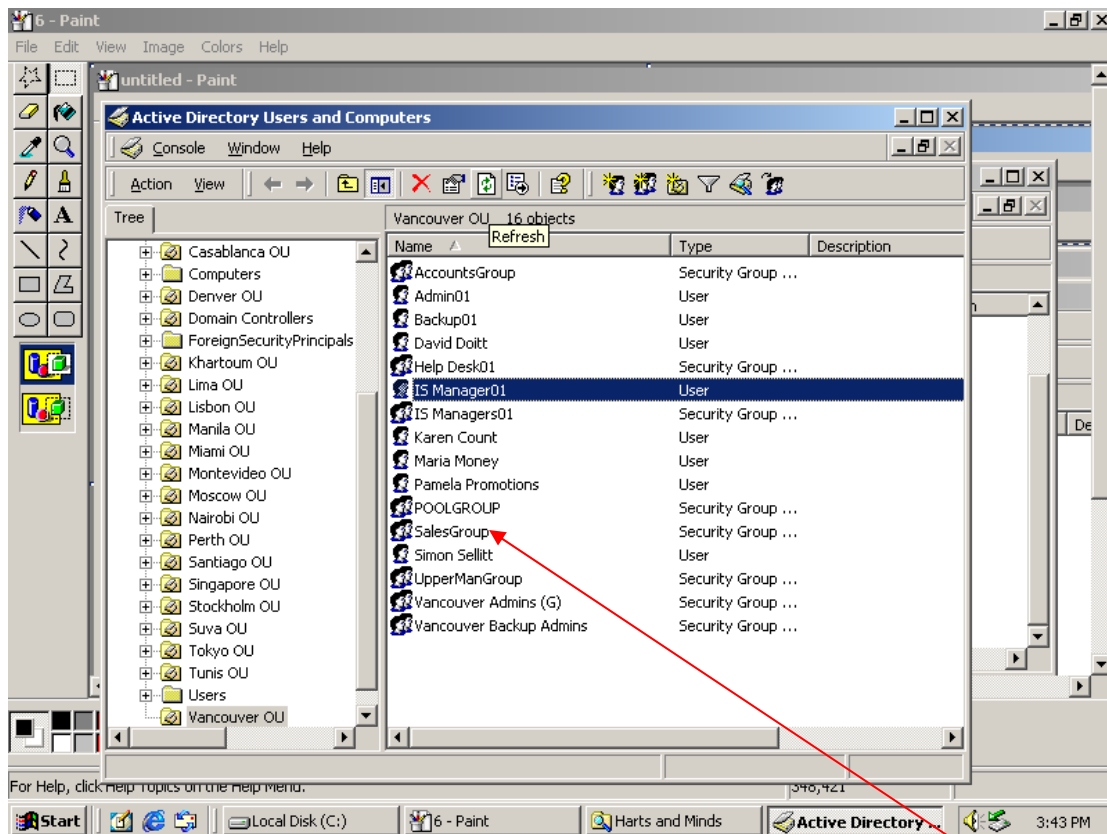


The screenshot above shows all Users have access to spreadsheet.

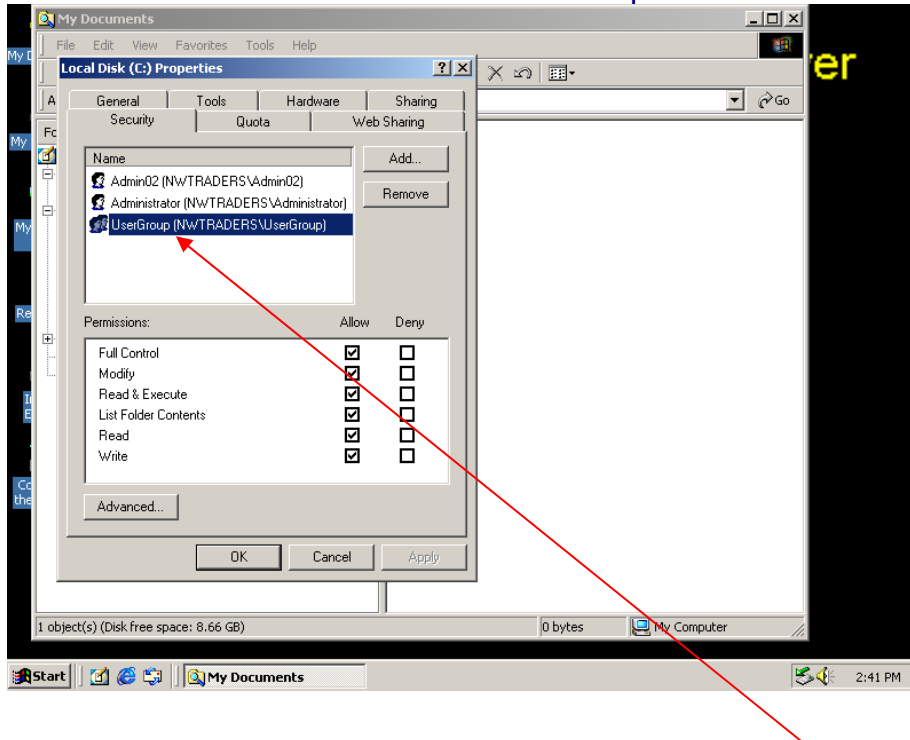
Our system works by:

The User Profile Spreadsheet shows that all users have access to spreadsheet. Therefore by putting all users into a users group, it is quicker to give spreadsheet access to the user group rather than individually to each user.

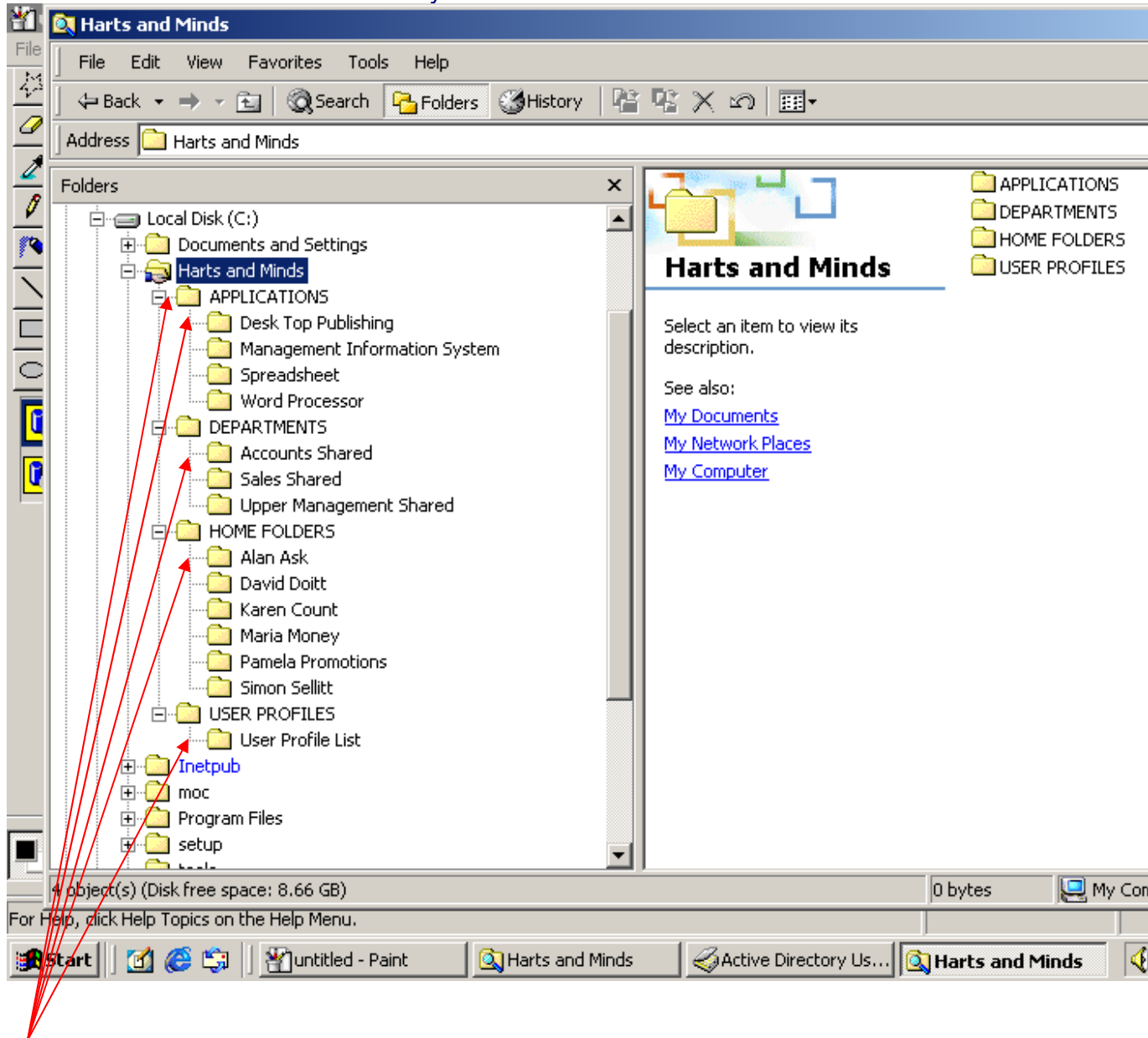
In the same way, each department is set up as a group and this makes it more efficient to set up permissions for a group instead of several individual users.



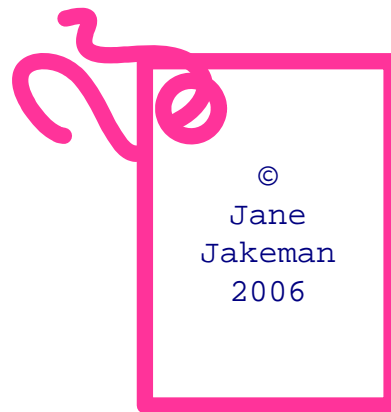
The screenshot below shows the User Group



This screenshot shows the Folder system:



HARTS AND MINDS



REPORT

RIGHTS AND RESPONSIBILITIES OF:-

- A NETWORK MANAGER
 - A NETWORK USER
-

by
Jane Jakeman
6 May 2006

Rights and responsibilities of a Network Manager

Building security

A Network Manager needs to ensure:

- that the building housing the equipment is safe and secure from events such as theft and building damage, i.e. water leaks. Most companies will operate an alarm system as well as keep expensive and important servers in a locked room.

Hardware

A Network Manager is likely to be responsible for:

- Investigating new hardware options. For example there may be hardware available that will save (x) hours per week for (x) number of employees and it may be cost effective to purchase this new hardware.
- Request budget or funding for replacing hardware
- Purchase new hardware
- Install hardware and any necessary drivers
- Investigate phone line options and costs and quality of service
- Arrange for maintenance of existing hardware
- Monitor items of hardware and their location and security coding

Software

A Network Manager will:

- investigate new software options
- request budget or funding for new software
- purchase software
- install software
- update software
- manage licences and payment of licencing
- organise training for existing/new software

Network

A Network Manager will:

- manage Health & Safety, for example, educate users on the Health & Safety that applies to them
- assess network hardware capability
- upgrade network hardware such as cables, routers etc.
- manage network security such as anti-virus software, firewall, spyware blocker
- manage internet access for users and groups
- set up users and groups
- set up users and groups security
- manage the Folder system
- install new hardware, ranging from new pc's, printers, network cards, etc
- manage the IP addressing and any subnetwork
- maintain a user profile list and keep it up –to-date by adding, updating and deleting, for example, if a user is on a short-term contract, then set

their use to the end date of their contract. Or if a user leaves the company, remove the user details from the network and update the user profile list

- manage the finances of the network, say for example leased telephone lines
- make recommendations on upgrading the network
- troubleshoot any problems
- manage any intranet

Users

A Network Manager will:

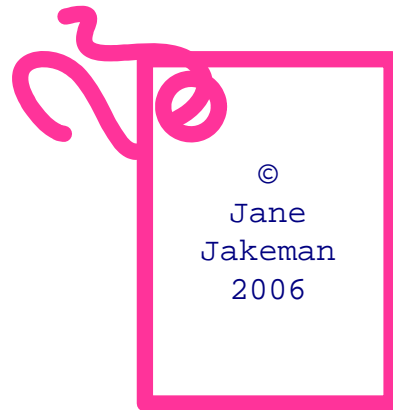
- install new users to the network, setting all their correct permissions
- organise training for users, for example, how to use the company email
- prepare and update when necessary a 'Code of Conduct' for the user to follow
- provide support to users
- operate a 'Helpdesk' for users to call
- maintain a 'log' showing details of issues raised and time taken to resolve

Rights and responsibilities of a Network User

A User will:

- keep their password safe and change their password when requested
- not use the Internet for their own personal use
- not eat or drink near computer hardware
- follow Health & Safety requirements such as taking a break from the screen every 45 minutes
- report any errors or problems with their system
- attend Training as requested by Network Manager
- check their email on a regular basis
- turn their computer off at the end of the working day
- not relocate their computer
- not use their own peripherals

HARTS AND MINDS



TASK SIX IP ADDRESSING DESIGN

by
Jane Jakeman
6 May 2006

Task Six

Design an IP Addressing Scheme for a Network.

Question 1.

What is the minimum number of bits you can borrow that will allow the network to be subnetted to support the network as it is configured at this time?

The IP address of 132.64.0.0 is a Class 'B' address because the binary number commences with 10. (A Class 'A' address commences with binary 0, whilst a Class 'C' address commences with binary 11).

There are 3 networks, being Marketing, Sales and Management. We need to borrow enough bits to subnet 3 times. Three bits will provide six subnets as shown below:

128	64	32	16	8	4	2	1
0	0	0	For network address				
0	0	1	subnet 1				
0	1	0	subnet 2				
0	1	1	subnet 3				
1	0	0	subnet 4				
1	0	1	subnet 5				
1	1	0	subnet 6				
1	1	1	For network broadcast				

(Two bits would only provide 2 subnets and therefore would not be practicable in this instance).

The network address is 132.64.0.0. **The new subnet mask will be 255.255.224.0.** 224 is the total of 128 + 64 + 32 (being 3 bits borrowed) as shown highlighted in yellow below:

128	64	32	16	8	4	2	1
0	0	0	For network address				
0	0	1	for subnet 1				
0	1	0	for subnet 2				
0	1	1	for subnet 3				
1	0	0	for subnet 4				
1	0	1	for subnet 5				
1	1	0	for subnet 6				
1	1	1	For network broadcast				

The number of subnets will be six. This is because **zeros** are used for the network address and **ones** are used for network broadcast address. The remaining 1's and 0's can be displayed in six different ways, making 6 different subnets.

The number of hosts per subnet are calculated by:

- counting the remaining bits – in this case there are 5 bits remaining from the third octet and eight bits remaining from the fourth octet totalling 13.
- calculating the different combinations of the 1’s and 0’s whilst not counting any 1’s or 0’s that will be used for network address or broadcast address.
- using the formula $2^n - 2$. (n = number of bits, in this case, 13). This is because binary is in base 2, and $- 2$ will deal with removing the count of 1’s and 0’s used for the network broadcast address and network address.

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
For network address	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
subnet 1	0	0	1													
subnet 2	0	1	0													
subnet 3	0	1	1													
subnet 4	1	0	0													
subnet 5	1	0	1													
subnet 6	1	1	0													
For network broadcast	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Third Octet								Fourth Octet							

The cells in blue indicate the hosts. Therefore the number of hosts are $2^{13} - 2$ which equals **8190 hosts per subnet.**

The range of IP addresses per subnet are calculated in the table below

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	Decimal
For network address	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
subnet 1 first host address	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	32.1
subnet 1 last host address	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	63.254
subnet 2 first host address	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	64.1
subnet 2 last host address	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	95.254
subnet 3 first host address	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	96.1
subnet 3 last host address	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	127.254
subnet 4 first host address	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	128.1
subnet 4 last host address	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	0	159.254
subnet 5 first host address	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	160.1
subnet 5 last host address	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	191.254
subnet 6 first host address	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	192.1
subnet 6 last host address	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0	223.254
For network broadcast	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Third Octet								Fourth Octet								

By taking the decimal calculation of the third and fourth octet, and placing the first two octets in front of the calculation, the actual range of addresses is:

subnet 1 first host address	132.64.	32.1
subnet 1 last host address	132.64.	63.254
subnet 2 first host address	132.64.	64.1
subnet 2 last host address	132.64.	95.254

subnet 3 first host address	132.64.	96.1
subnet 3 last host address	132.64.	127.254
subnet 4 first host address	132.64.	128.1
subnet 4 last host address	132.64.	159.254
subnet 5 first host address	132.64.	160.1
subnet 5 last host address	132.64.	191.254
subnet 6 first host address	132.64.	192.1
subnet 6 last host address	132.64.	223.254

The broadcast addresses are calculated by displaying all 1's in the host section of the subnet. The change from 0 to 1 is highlighted in green:

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	Decimal	Broadcast Address
For network address	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
subnet 1 first host address	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	32.1	
subnet 1 last host address	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	63.254	132.64.63.255
subnet 2 first host address	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	64.1	
subnet 2 last host address	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	95.254	132.64.95.255
subnet 3 first host address	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	96.1	
subnet 3 last host address	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	127.254	132.64.127.255
subnet 4 first host address	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	128.1	
subnet 4 last host address	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	159.254	132.64.159.255
subnet 5 first host address	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	160.1	
subnet 5 last host address	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	191.254	132.64.191.255
subnet 6 first host address	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	192.1	
subnet 6 last host address	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	223.254	132.64.223.255
For network broadcast	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		

Third Octet
Fourth Octet

Question 2

How many bits would you need to borrow to allow some growth in the number of hosts at each campus and to allow the company to add extra subnets?

1. Work out the number of hosts required on each subnetwork
2. Work out the number of subnetworks required

This table has been calculated using the formula $2^{(\text{number of bits})} - 2$ and will provide a simple way to design this IP addressing scheme:

CLASS B IP ADDRESS			
Bits borrowed	No of subnets	Bits remaining	No of hosts
2	2	14	16,382
3	6	13	8,190
4	14	12	4,094
5	30	11	2,046
6	62	10	1,022
7	126	9	510
8	254	8	254
9	510	7	126
10	1,022	6	62
11	2,046	5	30
12	4,094	4	14
13	8,190	3	6
14	16,382	2	2

The specification states that some growth is required in the number of hosts. Therefore I have selected 62 subnets and 1,022 hosts as the most appropriate IP addressing scheme for this company network.

CLASS B IP ADDRESS			
Bits borrowed	No of subnets	Bits remaining	No of hosts
2	2	14	16,382
3	6	13	8,190
4	14	12	4,094
5	30	11	2,046
6	62	10	1,022
7	126	9	510
8	254	8	254
9	510	7	126
10	1,022	6	62
11	2,046	5	30
12	4,094	4	14
13	8,190	3	6
14	16,382	2	2

Therefore the number of bits borrowed would be 6.

The subnet mask would calculate to 252 (128+64+32+16+8+4), making the subnet mask address 255.255.252.0

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1
For network address	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The number of subnets would be $2^6 - 2$ which equals 62.

The number of hosts per subnet will be $2^{(no\ of\ bits\ remaining)} - 2$, which is $2^{10} - 2$ which equals 1022.

	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	Decimal
For network address	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
subnet 1 first host address	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	4.1
subnet 1 last host address	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	7.254
subnet 2 first host address	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	8.1
subnet 2 last host address	0	0	0	0	1	0	1	1	1	1	1	1	1	1	1	0	11.254
subnet 3 first host address	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	12.1
subnet 3 last host address	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	0	15.254

The range of IP address per subnet will be calculated as follows:

.....and so on thru all 62 subnets ending in 132.64.248.1 to 132.64.251.254

.... and showing the broadcast address and the full IP address below:

Decimal	Broadcast Address	Range of IP addresses		
4.1		subnet 1	132.64.	4.1
7.254	132.64.7.255		132.64.	7.254
8.1		subnet 2	132.64.	8.1
11.254	132.64.11.255		132.64.	11.254
12.1		subnet 3	132.64.	12.1
15.254	132.64.15.255		132.64.	15.254

.....and so on thru all 62 subnets, last subnet broadcast address being 132.64.251.255.