How to integrate HP StorageWorks tape libraries into a SAN based backup environment.

Presentation 1 (20 mins) : HP Extended Tape Library Architecture (ETLA)

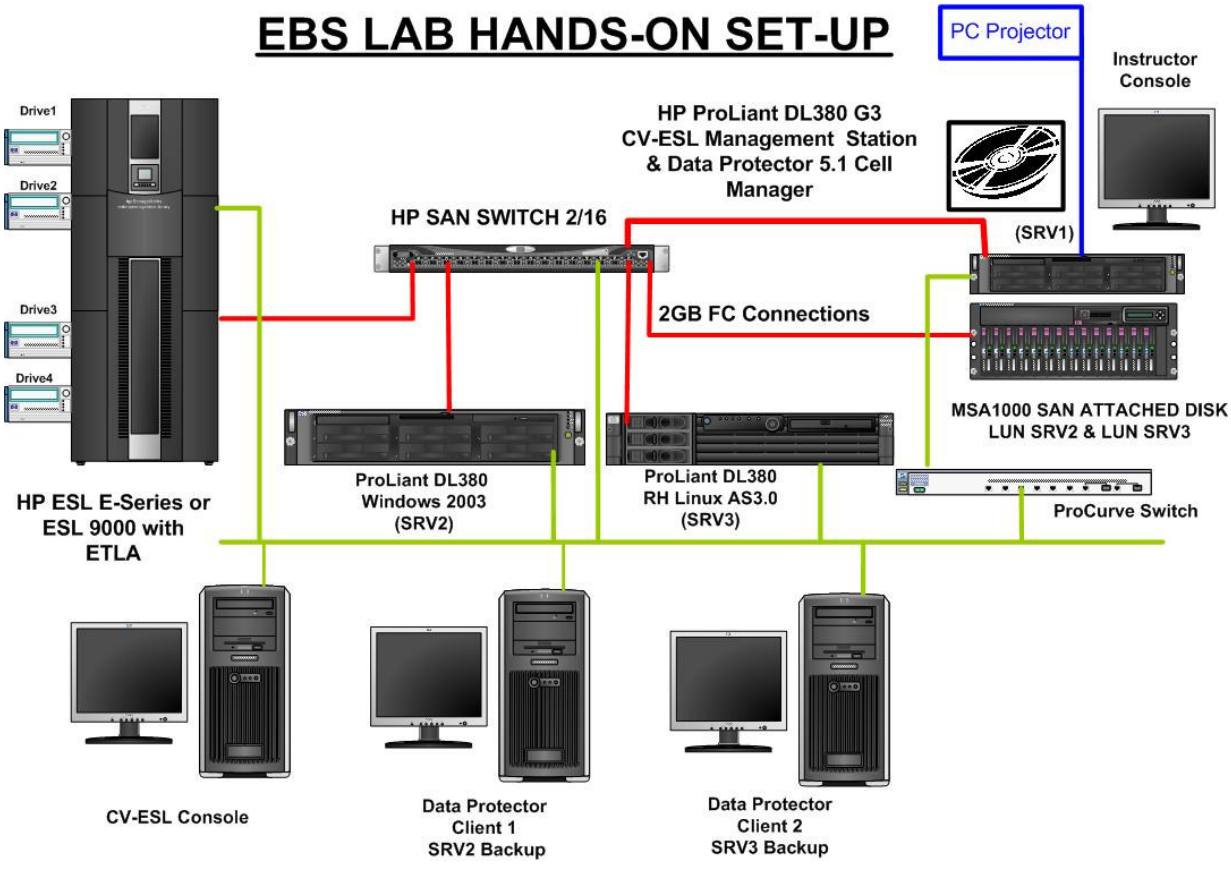
Overall Lab Objective

After completing this lab, you will be able to:-

- Physically configure an HP ESL tape library
  - Diagnose faults and monitor it using HP Command View ESL
  - Install CV-ESL licenses
- Configure the SAN infrastructure to allow specific access patterns from servers in the SAN to access specific tape drives within the Library, using zoning, and implementing HP secure manager.
- Configure HP Data Protector software to run SAN based backups efficiently
  - Configure the library into data protector
  - Create specific media pools for servers to be backed up
  - Run test backups
- Effective Sharing of Tape drives in a SAN
  - Utilize the benefits of HP secure manger to share pools of tape drives
  - Know when to use lock names

Requirements

The lab set-up is as shown below



Introduction

- The whole point of a SAN based tape library is to enable tape drives to be shared by multiple servers. In this case SRV2 will eventually have access to a pool of tape drives Drive1 & Drive2, and SRV3 will have access to a pool of tape drives Drive3 and Drive4.
- The heterogeneous SAN consists of server SRV2 (windows) with an associated Disk area LUN SRV2 (Drive E) on the MSA1000 and server SRV3 (linux) with an associated disk area LUN SRV3 (MSA_LUN) on the MSA 1000.
- Management of the Library is through the Command View ESL management station (SRV1). Workstations can monitor the library by pointing their Web browser at the CV-ESL management station IP address. In this lab only the CV-ESL console has the java applets loaded to enable CV-ESL to run.
- HP Data Protector "cell manager" runs on SRV1 but the Data Protector user interface and backups can be run from either of the 2 data Protector Workstation consoles shown.
- The Lab will initially consist of backing up LUNSRV2 (DriveE) to a tape in the ESL Library and backing up LUNSRV3 (MSA_LUN) to what looks like different tape in the ESL library. Initially these backups will fail because the tape drives will not be allocated to a specific server (or group of servers) – this causes conflicts. HP secure manager will then configure the library so specific tape drives can only be accessed by specific servers, after this the backups will run successfully.
- The Lab is based around 4 drives minimum being available within the Library.

Procedure

Part 1 – Configure the Library

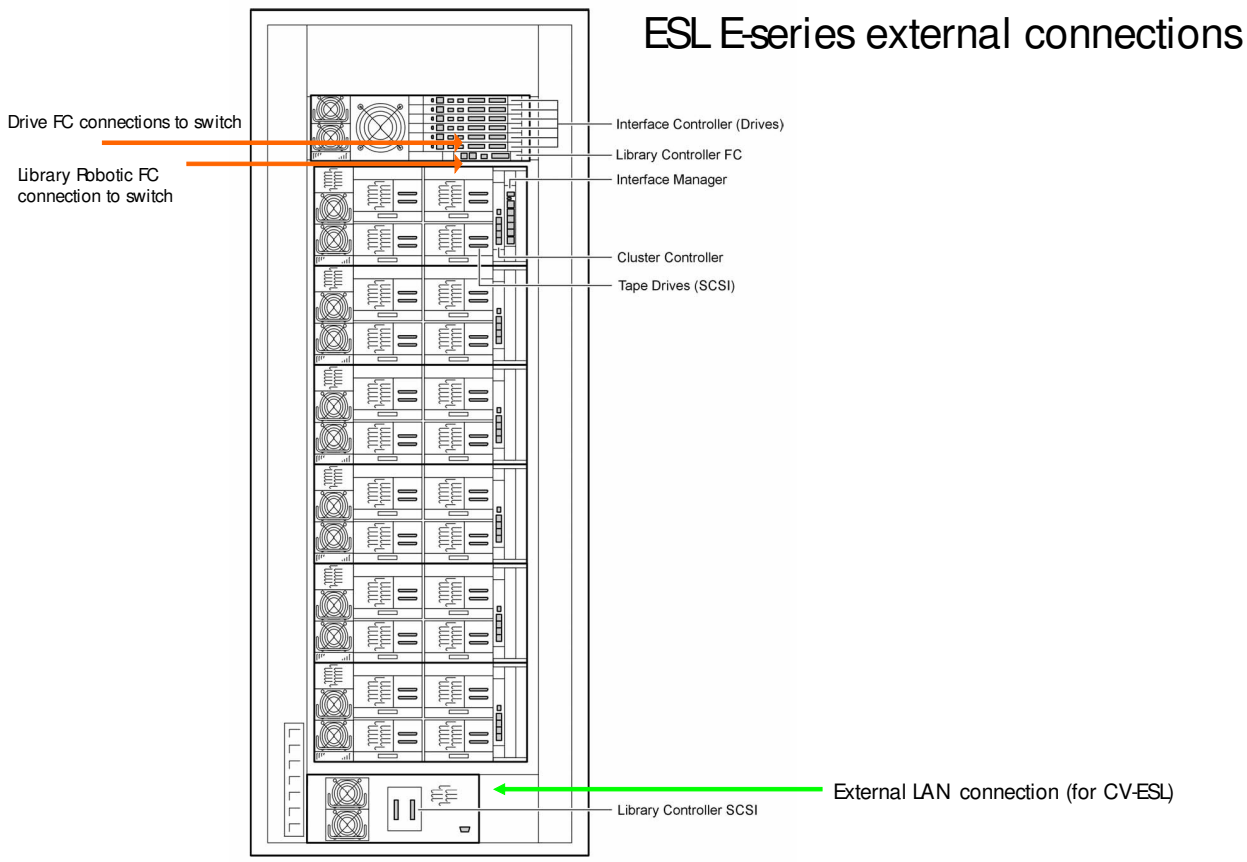
<< IP addresses will be allocated on the day of the Session >>

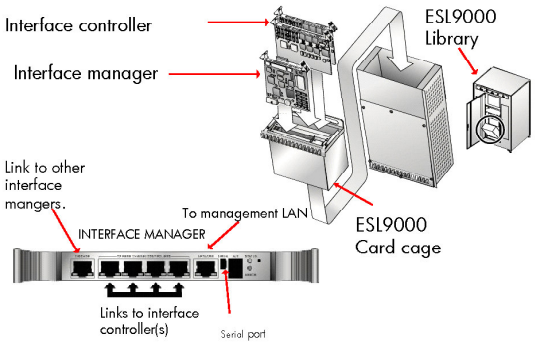
Objectives of this section are:-

- Identify the key library interface components
- Understand the Library Networking Architecture and set the IP Address

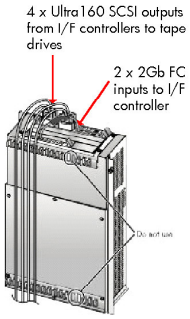
Note: Be careful not to keep power cycling the libraries since it takes around 5-7minute to do a complete inventory and come back online. Only power cycle the library when instructed to do so.

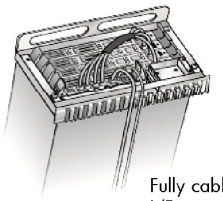
1. Check and understand Library cabling and physical configuration using the diagrams below – this will vary depending on if ESL 9000 or ESL E-series Library is used. An HP NSS technical advocate will be on hand to advise about the physical layout & configuration





ESL 9000 external connections
Robotics control is daisy chained off first drive connection.





Fully cabled
I/F manager
and 4 I/F
controllers

NOW TAKE SOME TIME TO FAMILIARISE YOURSELF WITH THE ARCHITECTURE OF BOTH TYPES OF ESL LIBRARIES

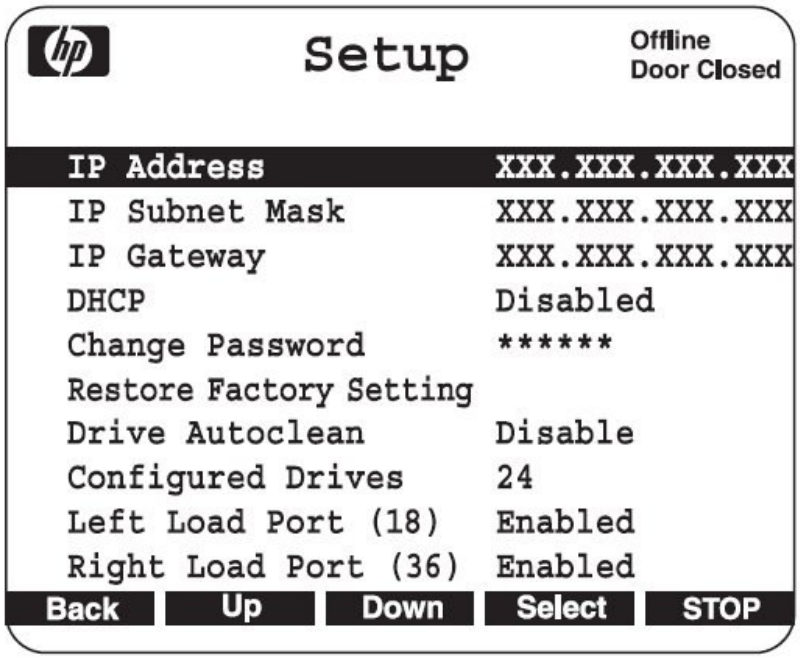
Your instructor will ensure the following areas are understood and discussed.

- Library cabinet controller / robotics controller
- Interface controller cabling to tape drives
- I^2C cabling
- Internal & External LAN cabling
- Additional Serial cables required for Diagnosis (3 different types!)
- Fibre channel cabling considerations

2. Set the Library IP address. On the ESL E-series library the IP address is set from the Operator control panel on the Library. Set IP address of Library to _____ as follows:

   - From the top level *Menu* select *Ops*; the top line will show the cabinet *online.*

- Select *online* and us the up & down buttons until *offline* appears, select *offline*
- The library will prompt you to check if you want to take the library offline answer *YES*
- Go *Back* to the top level menu of the library.



- Select *Setup*
- Key in the password 001122 (wait 10-15 secs for password to be verified)
- The *setup* menu is displayed with IP address highlighted - Press *select* .
- Use UP & DOWN and SELECT buttons to set the IP address to the required value. Repeat for each section of the IP address and then press *select*.
- Go *Back* to the top level menu and select *Ops* again, the cabinet should be shown as *offline* in the top right hand corner of the display. Select *cabinet* and then use up & down to cycle through the options until *reboot* appears. Press *select* – the library will confirm you want to reboot – answer YES.
- The Library will take 5-6 minutes to reboot at the end of the reboot the OCP display should now display the IP address you wish to be used.

If you are using the ESL 9595 Library with HP Extended Tape Library architecture then use the following process to set the Library IP address

- Connect the serial cable supplied onto the serial port of the Interface manager located in the card cage of the ESL 9595
- Using The EVO notebook supplied, connect the serial cable into the COM1 port of the Laptop.
- Open up a Hyper-terminal click **START > Programs > Accessories > Hyperterminal**
- Set the communication settings as follows
    - Port speed 9600
    - Data Bits 8
    - Parity None
    - Stop bits 1
    - Flow control None
    - You may have to hit the return key several times before communication is established.
- At the login prompt use the following information
    - Username: **cliadmin**
    - Password: **clipwd**
- Enter the following command to display the current IP address, along with other current network information
    - *show network ipaddress*
- Set the IP address as indicated by the instructor as follows
    - *Set network ipaddress* < IP address > <subnet mask> <gateway address>

e.g 192.168.0.20 255.255.255.0 192.168.0.100

- Note: Gateway address must not be 0.0.0.0
- Enter *exit* to end the serial session.
- Disconnect the serial cable.

Running Command View ESL to check library status.

Objectives of this section are

- Understand the management station/client architecture of CV-ESL
- Login to CV-ESL using a web browser
- Add a library to CV-ESL
- Within CV-ESL - Select a library and perform Health Checks
- View license status & install a license key.
- Understand how firmware upgrades are performed. (instructor led)
- Understand other CV-ESL functionality

Procedure

> The Library CV-ESL configuration is to be performed at the CV-ESL console by one student with the other 3 students witnessing the configuration

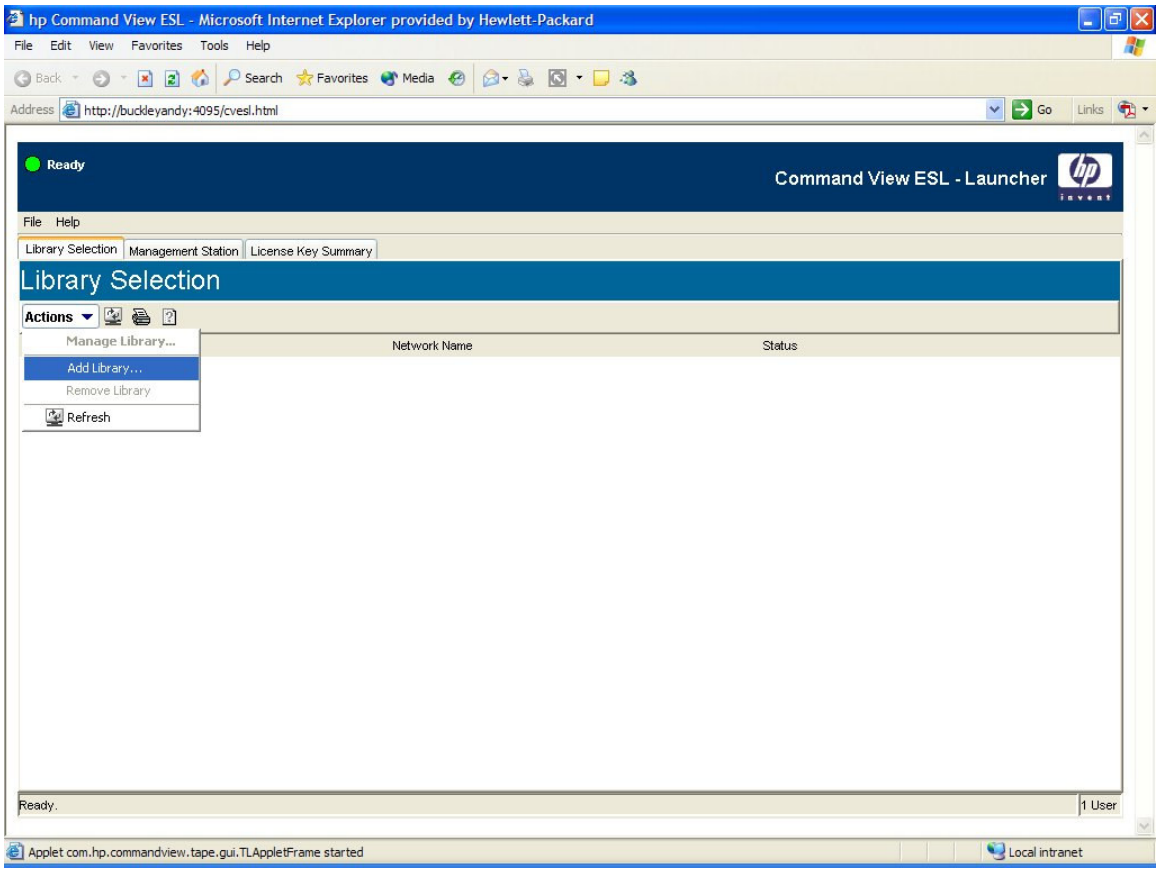
- The Command View ESL software has already been loaded on SRV1 together with the necessary Java plug-in that is required.

- On the allocated Command View ESL console in the Session Room start the Web Browser and enter the following url in the address field

  http://<hostname (SRV1)> :4095

  This will point the browser to the CV-ESL management station

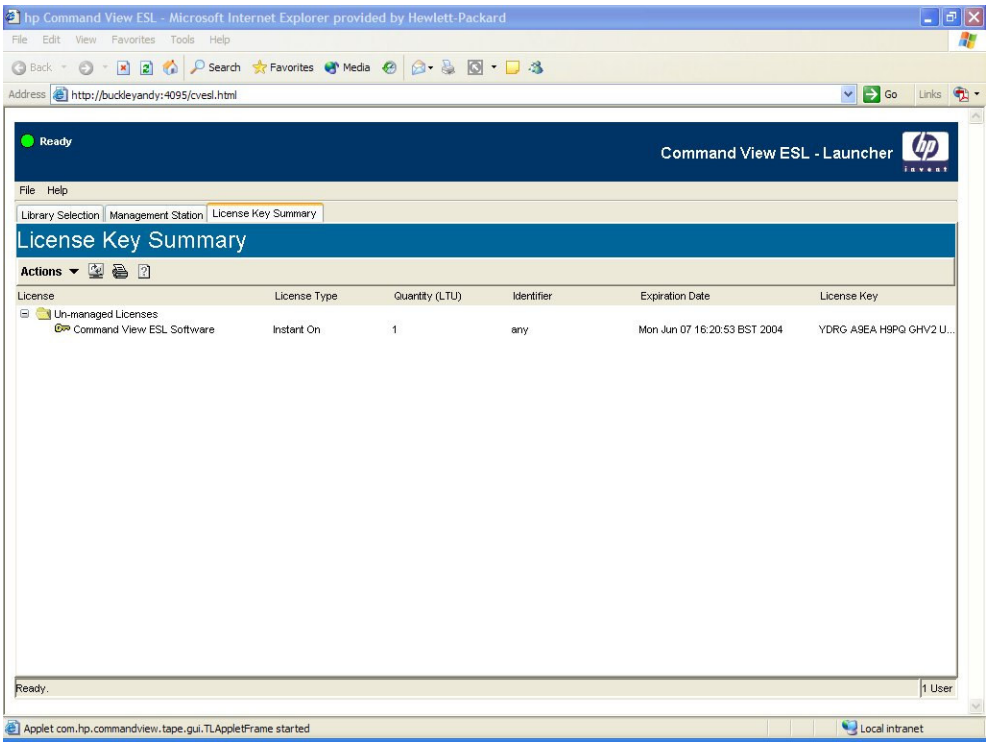
  A screen similar to the one below will appear.



- Select Add Library from the Actions drop down list and in the dialog box enter the IP address of Library.

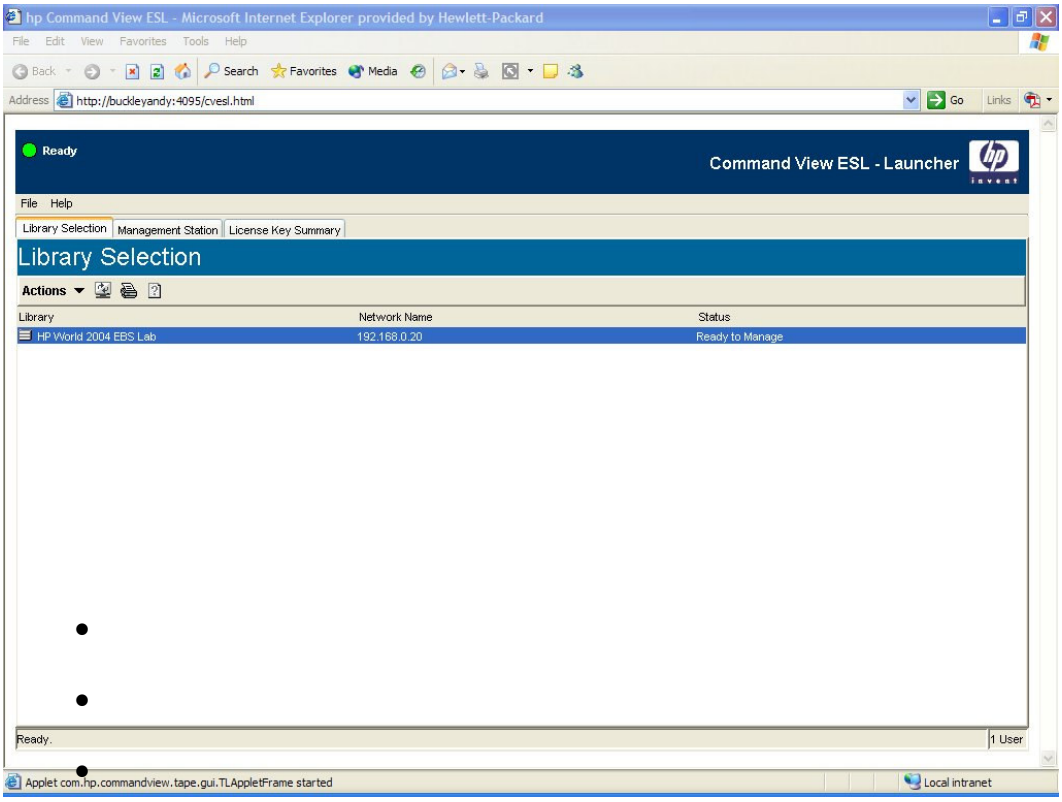
  Note: multiple libraries can be added to CV-ESL in the same way

- Also at this time click on License key summary tab and witness that there are no permanent licenses applied, only the instant-on license as shown below



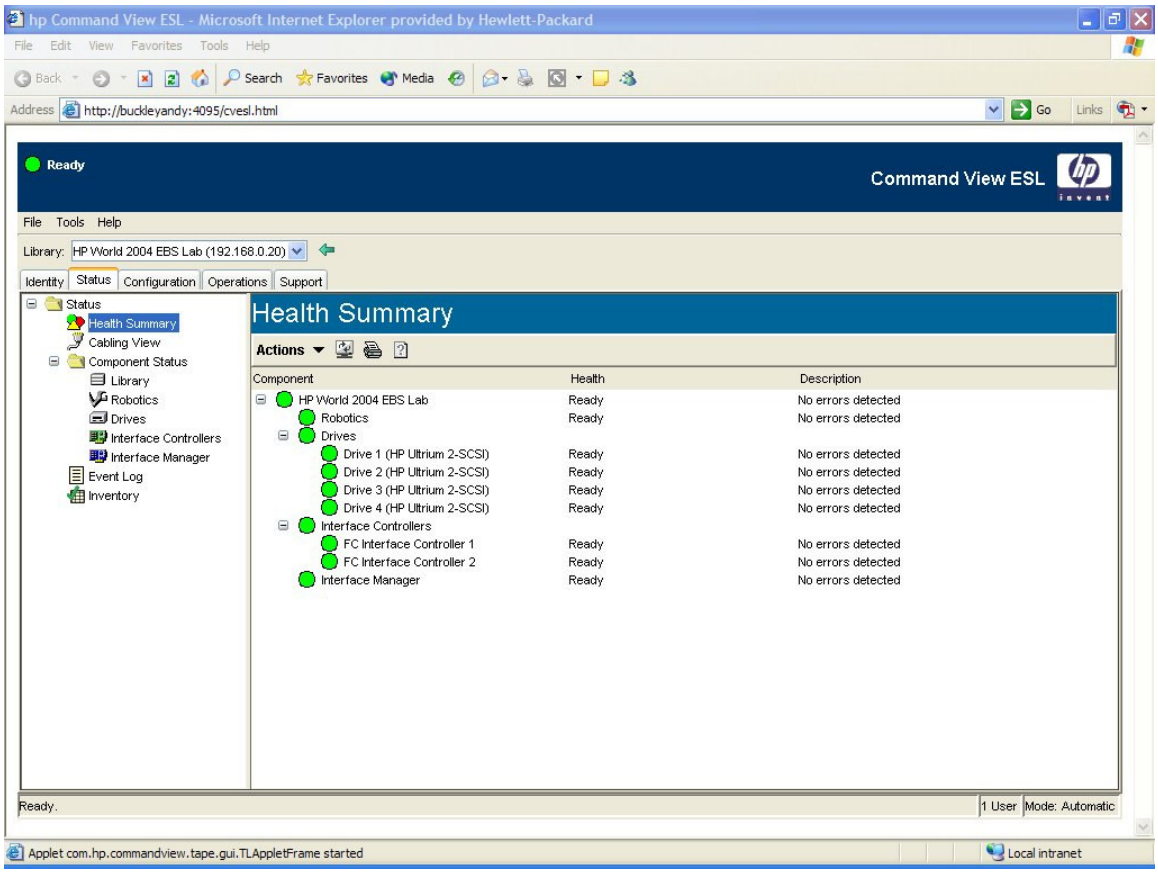
Return to the generic CV-ESL launch window.

- The library should now become available to manage, double click on the Library entry to manage the library (as shown below)



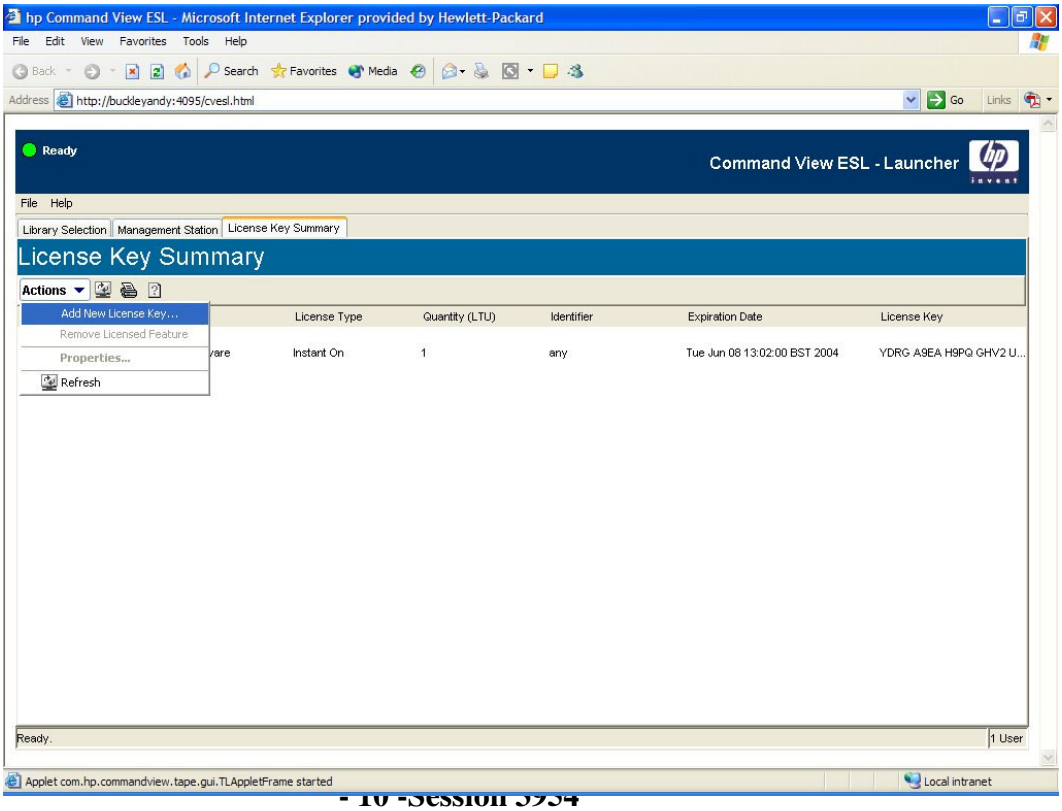
- When the management screen appears, click on the health summary section on the left hand side.

Note: Remember to keep hitting the *refresh* feature under *Actions* to ensure you are viewing the latest status information.



Installing License Keys

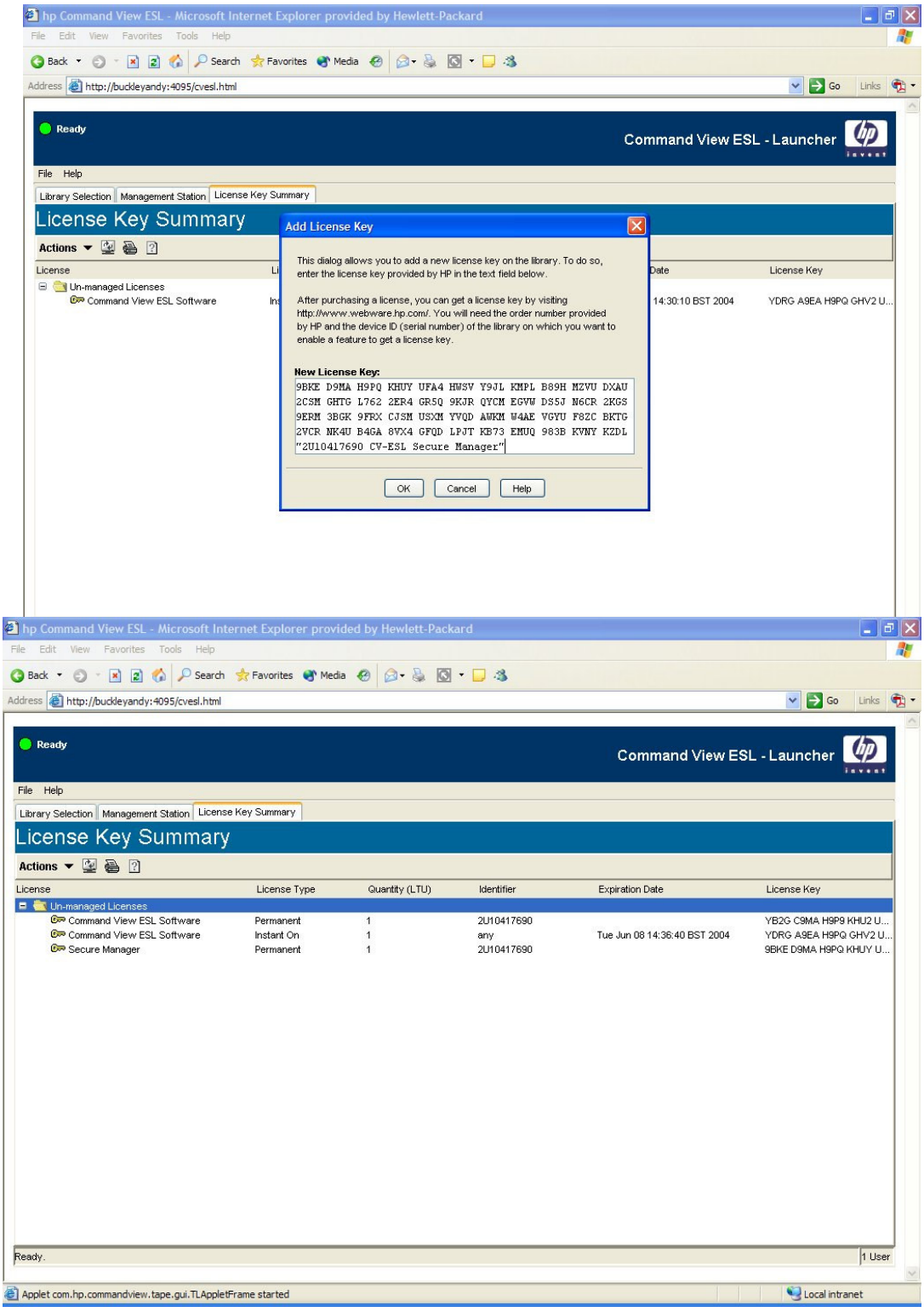
Go back to the launch screen by clicking the ⇐ icon on the top line of the CV-ESL screen
Click on license key summary tab, and then on ACTIONS



The license keys are shown as icons on your CV-ESL console desktop as

- Command View permanent License.dat
- Secure Manager License.dat

Open the license keys with the Notepad utility and then copy (right click mouse and select copy) the data stream to the clipboard, then use <control> V to paste it into the license key screen as shown below.



When both licenses have been loaded in this manner you should end up with the license summary screen shown above.
Take some time to look at other CV-ESL features such as Inventory and setting Library ownership by using the right hand tree structures appropriately..

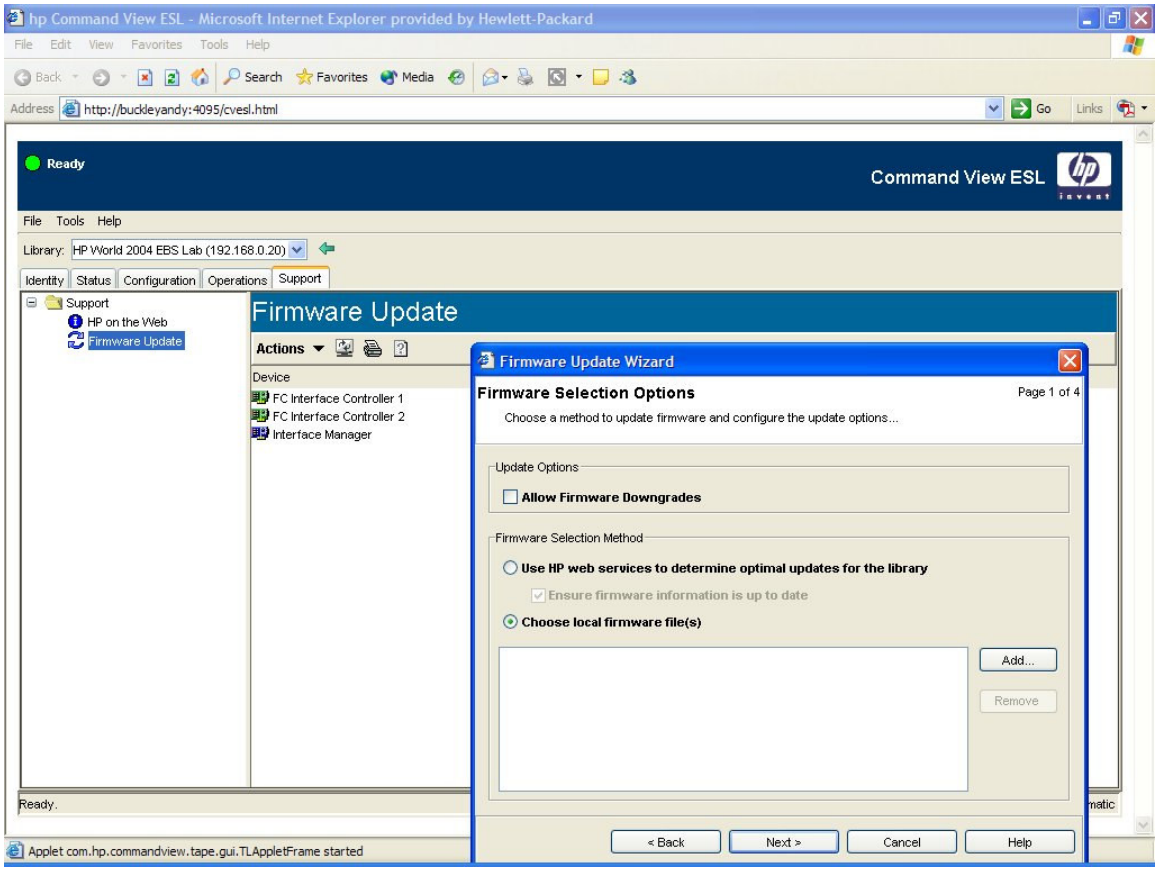
Upgrading Firmware
< this is not part of the lab and is for reference only>

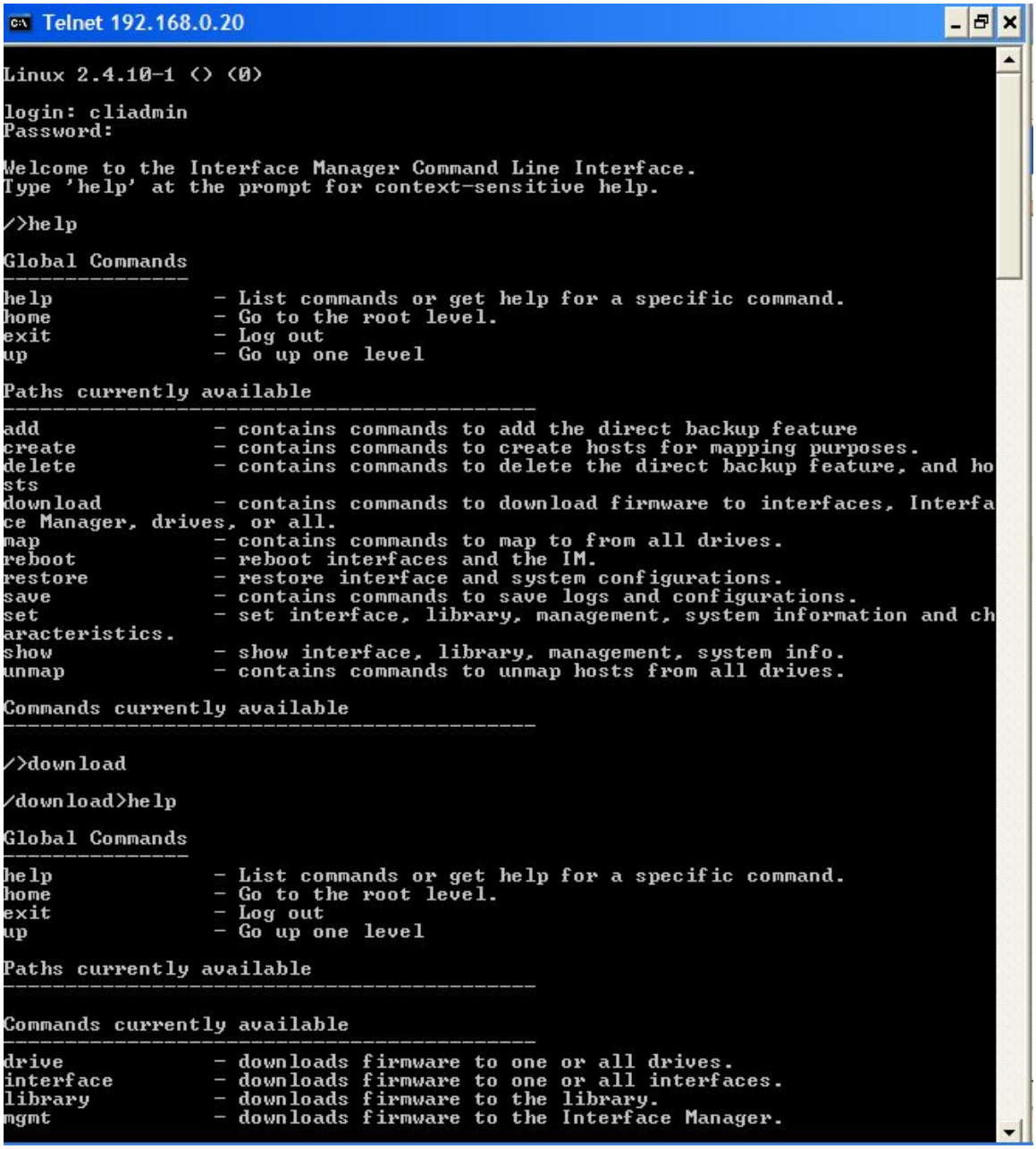
The preferred method of upgrading firmware in the ESL & ESL E-series libraries with HP extended Tape Library Architecture is as follows:

- For the Interface manager and Interface controllers – use the CV-ESL firmware upgrade Wizard (shown below)
- For the Cabinet controller (Library Robotics) and Tape Drives you must first
    - Set up an ftp session with the interface manger (using the Library IP address)
    - ftp the .frm* files for the drive or robotics firmware onto the Library IP Address
    - Run a telnet session with the Interface manager and use the firmware upgrade utility from the Interface manager Command Line prompts (shown below)

  * frm is the required file suffix for firmware files.

FW source files available via http://www.hp.com/support then key in the Product name of your Library and it will direct you to the FW download site. If you have an internet connection on the management server running CV-ESL you will be directed to the FW download site directly.





Note: Login: cliadmin

Password: clipwd

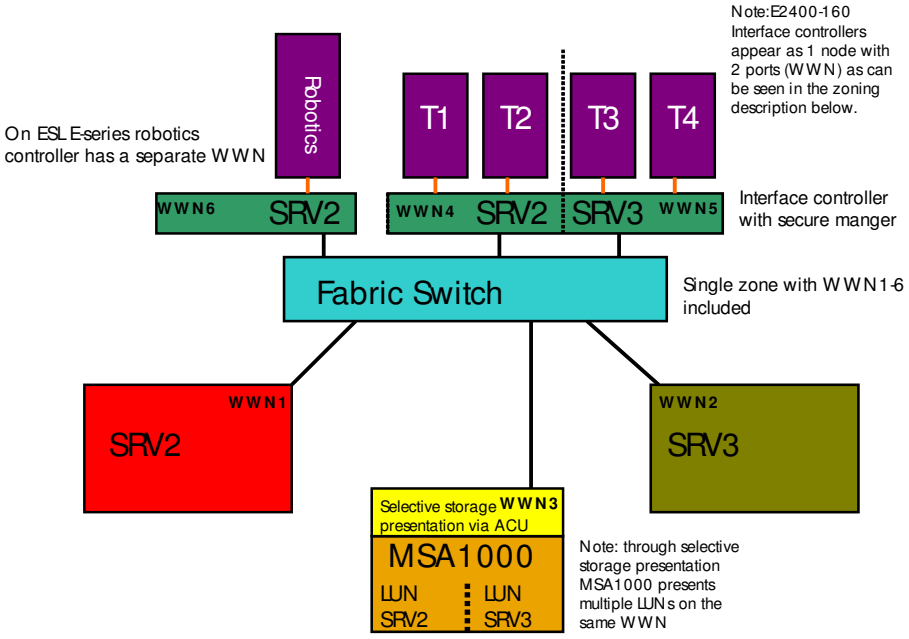
Presentation 2 (20 mins) : SAN Backup – Best Practices

Part 2 – Configure the SAN Fabric

Objectives of this section are:

- Understand what components to include in a backup zone
- View the Fabric switch zoning that is in place
- Display LUN masking features for tape in HP Secure manager

SAN configuration - Overview



The above diagram shows the SAN configuration, the two LUNs on the MSA1000 are presented into the SAN by means of the Select Storage Presentation using the Array control utility (ACU). The diagram shows the components of the SAN which possess World Wide names (WWN). A simple way of ensuring SAN integrity is to create a zone within the Fabric switch that only contains the server and storage components you want, and will not accept addition rogue servers or devices being plugged into the Fabric. For this reason in this Lab the switch consists of a single zone which contains WWN 1- 6 ONLY. This is shown configured in the screenshot below.
The main reason for attaching a tape library to a SAN is to share the resource with multiple servers. In a typical configuration the library robotics is controlled from one server (in HP Data Protector this is the 'Cell Manager') and groups of tape drives are allocated to servers either as a dedicated or 'shared' resource. Only one host server can write to a tape drive at any one time.

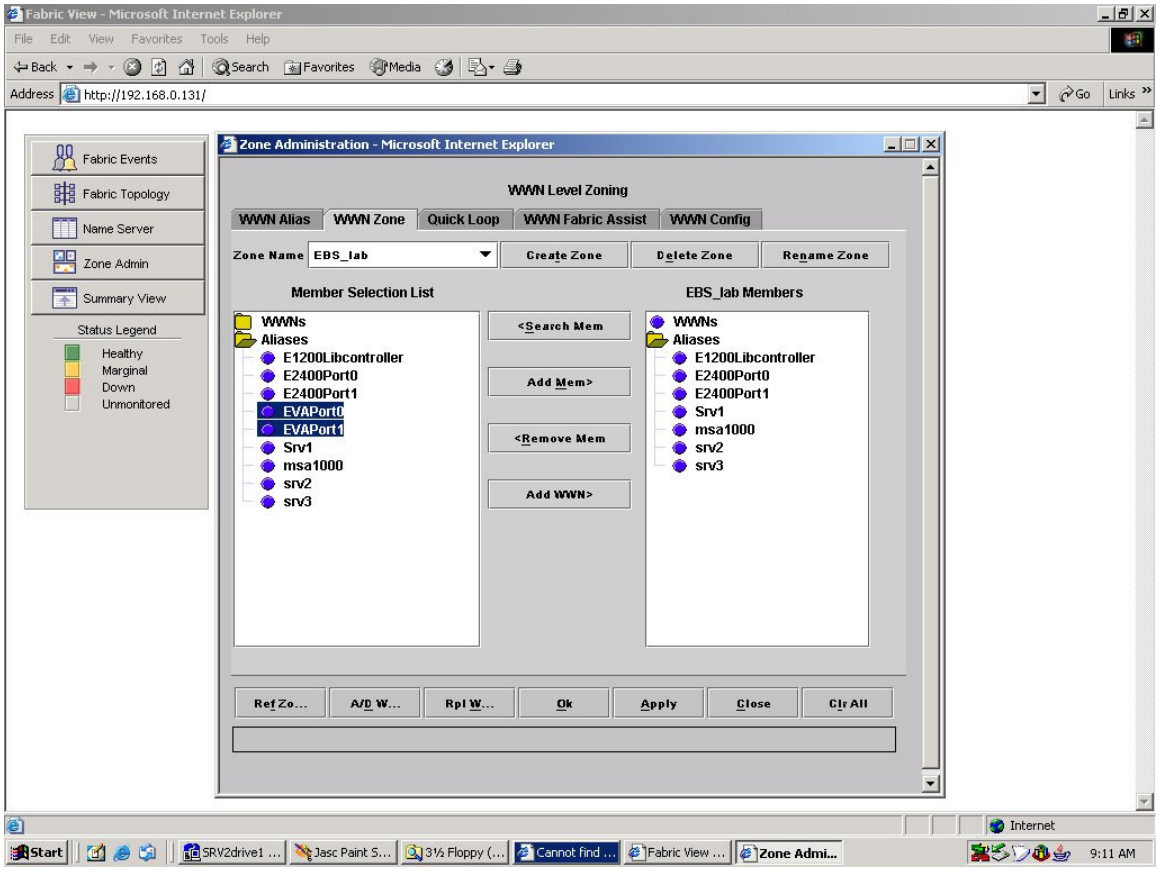
Controlled access can be achieved by several methods.:

1. Use zoning at the SAN level to allocate the robotics and or drives to servers. Because this uses World Wide Names (WWNs) allocation of individual drives LUNs is not possible.

2. Use HP Advanced Secure Manager to 'map' drives or robotics to individual host servers. This is similar to LUN the masking feature deployed in disk array technology.

3. Use the "lock names feature" in the backup application (HP DataProtector in this case). This provides no protection for shared drives outside of the application. For example a user on one server could be using HP Data Protector to perform a backup. A user on another server could execute an operating system utility such as tar on a LINUX server with access to the same tape drive. At best the one of the servers would show the drive as 'not ready' and in the worst case the backup job could fail in a totally unpredictable manner.

This lab will focus on the use of HP Advanced Secure Manager to allocate specific LUNs to individual servers. The lab will also use tape drive 'lock names' within DataProtector to demonstrate how resources can be shared at an application level. The lab does not involve changing any of the zone configuration. Disk and tape are all within the same zone.



You may view the zoning by pointing your browser at the San switch IP address. (IP address will be allocated at Session time)
Note in the above example:

- how "alias" names have been created instead of WWN to allow easier identification

- Other equipment not in the EBS_lab zone are the EVAPort0 & EVAPort1

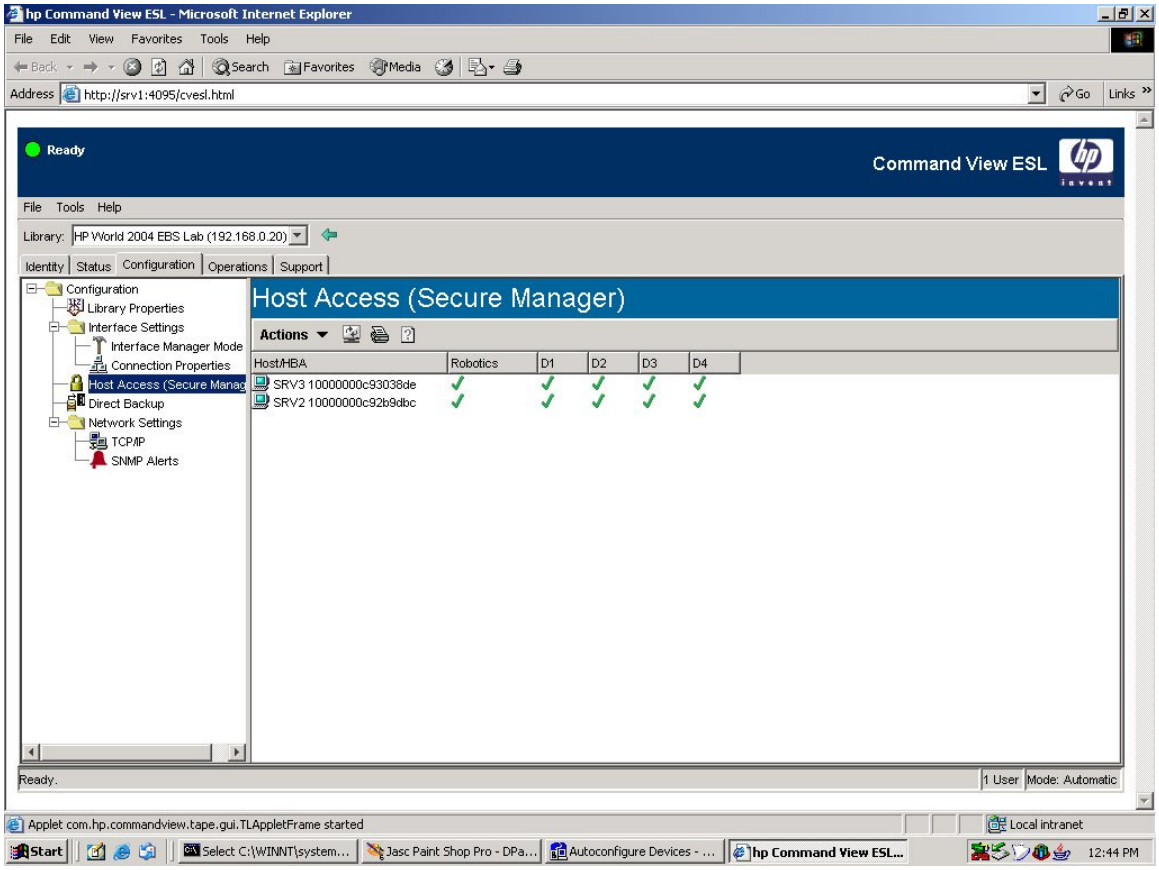
Configuring secure manager

On the CV-ESL console go to the configuration tab and note the following…

Note: in the bottom right hand of the CV-ESL screens there is text that says *Mode:Automatic*, this says the library is operating with the Interface manager in Automatic mode (the HP recommended mode) in this mode all the mappings to allow host access to the tape drives are produced automatically. The maps can be viewed using the serial interface to the interface controllers. The interface manager can also be configured to operate in manual mode, but then the user is responsible for creating (and maintaining) all the maps within the interface controllers, and this can be prone to errors.

A screen similar to that below should appear. Note how it shows the HBA WWN of SRV2 and SRV3 on the "y" axis and the Robotics and Drives along the "x"axis.

For the time being leave the configuration such that both hosts can access the robotics and all the drives (this is the default configuration without the advanced secure manager license key enabled)



Part 3 – Running Backups

This part of the Lab assumes a familiarity with backup application concepts.

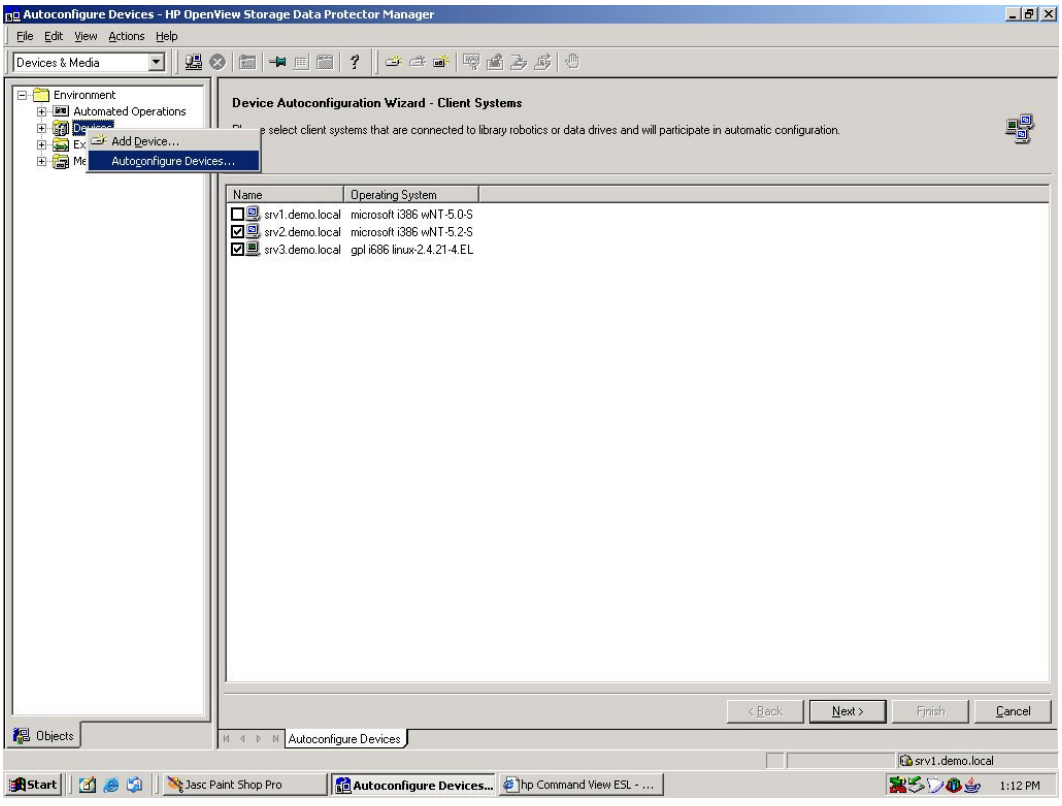
Objectives of this section are:

- Familiarization with HP Data Protector user interface
- Configure the tape library into HP data Protector & assign robotics control
- Perform a library inventory
- Set up media pools for SRV2 & SRV3
- Define a backup job to send data from LUN SRV2 To Tape 1 and to send data from LUN SRV3 to Tape 3 to simply test the backup infrastructure. We will also note that from both SRV2 and SRV3 all 4 tape drives are available to us for backup.

Configure Library into HP Data Protector

Note: ***This initial configuration should be performed from only ONE of the Data Protector Client stations.***

Start up data protector from your Client station and select the *Devices and Media* drop down box as shown below:



Right click the *devices* extension in the tree structure displayed in the left hand pane.
Click *Autoconfigure Devices*

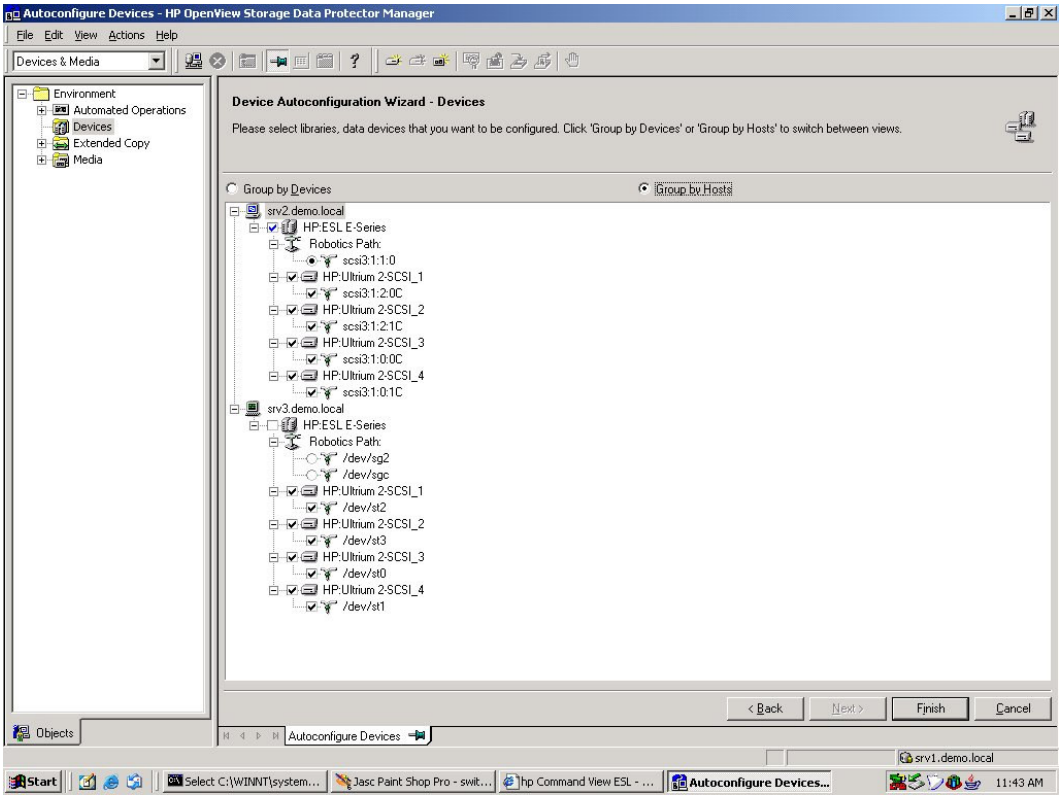
Data Protector then asks which servers you would like to protect using the device you are about to configure, checkbox *srv2* and *srv3*, then click *next* to continue.
Data Protector will now autodiscover devices connected to the SAN.
It will find an ESL Library, *Click* + to expand the components of the ESL library it has found.
Check the "*Group by Hosts*" box to enable the correct display format.

Note: How both SRV2 and SRV3 see the robotics and all the tape drives

We could at this stage simply use Data Protector to allocate certain tape drives to be only used by certain servers, by checking the appropriate boxes, for example HP Ultrium2-SCSI_1 we could tick the box for this only to be accessible to SRV2.

But this would not be a robust solution since at any time other servers added to the SAN or a server performing a device scan could interfere with the tape drives during a backup causing the backup to fail. We need to segregate the tape drives at a hardware level not at a software level. Instead we will allow both servers access to all tape drives and use HP secure manager later to segregate the drives at a hardware level. It is strongly recommended that only 1 server in your San is allocated to control the robotics.
So *tick* the boxes as shown below to allow SRV2 to control the robotics and all 4 tape drives to be visible to both servers.

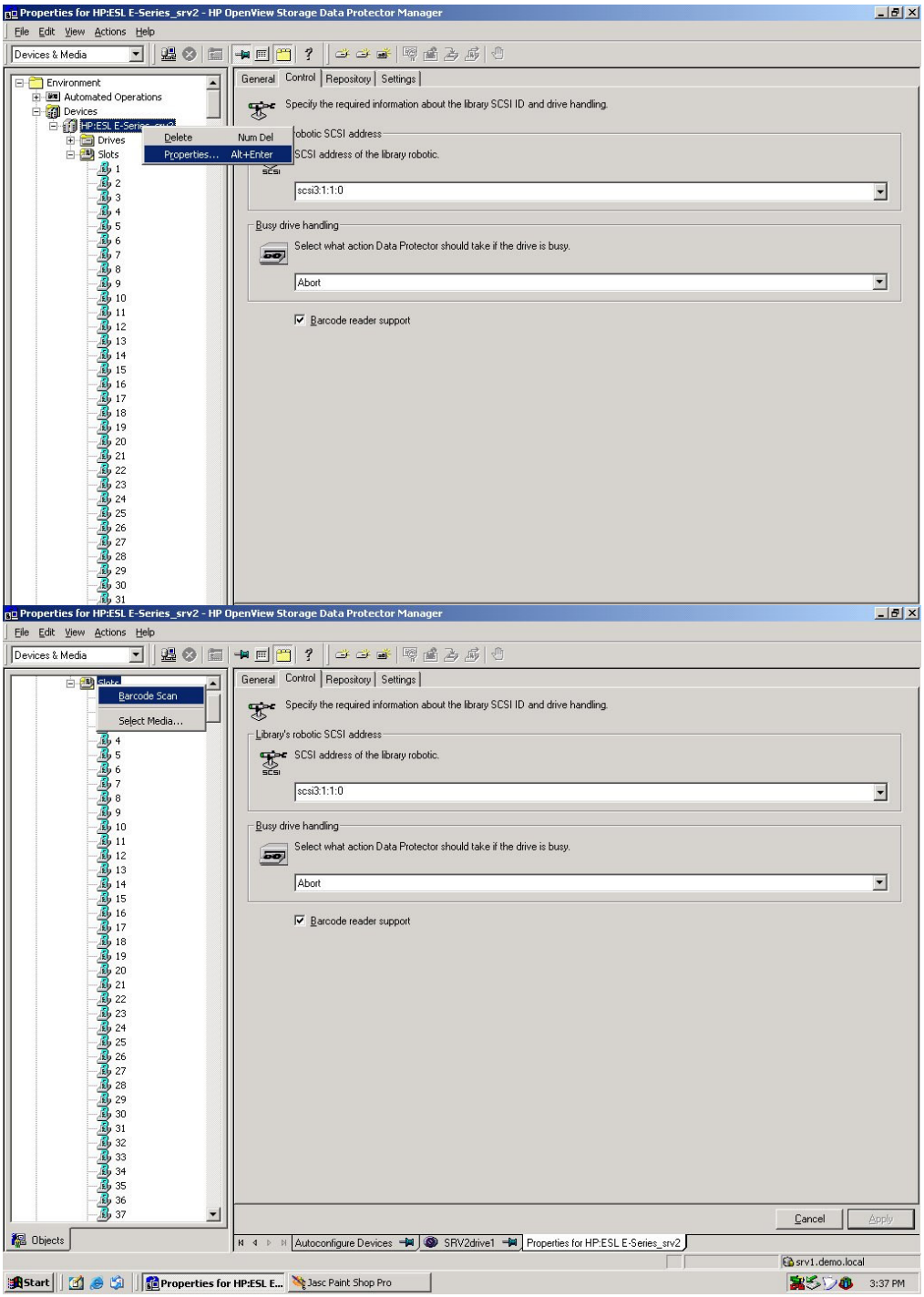
Note: How Data Protector also shows the Windows path and Linux device file associated with each component.



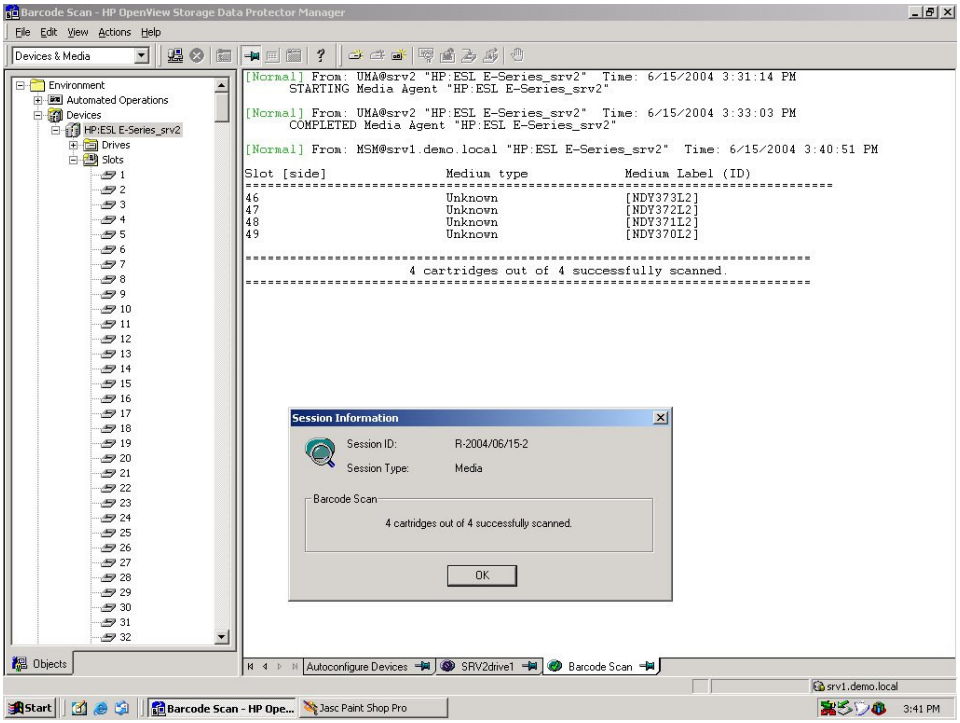
Before we can use the library for Backups we have to

- Enable bar code scanning
- Inventory the library to data protector knows in which slots the media resides
- Define media pools for SRV2 and SRV3
- Allocate Media pools to specific drive types
- Format the media for use by Data Protector

Under *devices* in the tree structure right click *properties,* select the *control* tab and checkmark the *barcode reader support* box. Click on *Apply.*
Now we need to allow HP data Protector to do an Inventory of what media is where in the Library



Right Click *slots* in the tree structure under *Devices and media* as shown above and select *Barcode scan.* A job will start which scans all the media in the library.
Note: This can take 4-5 minutes



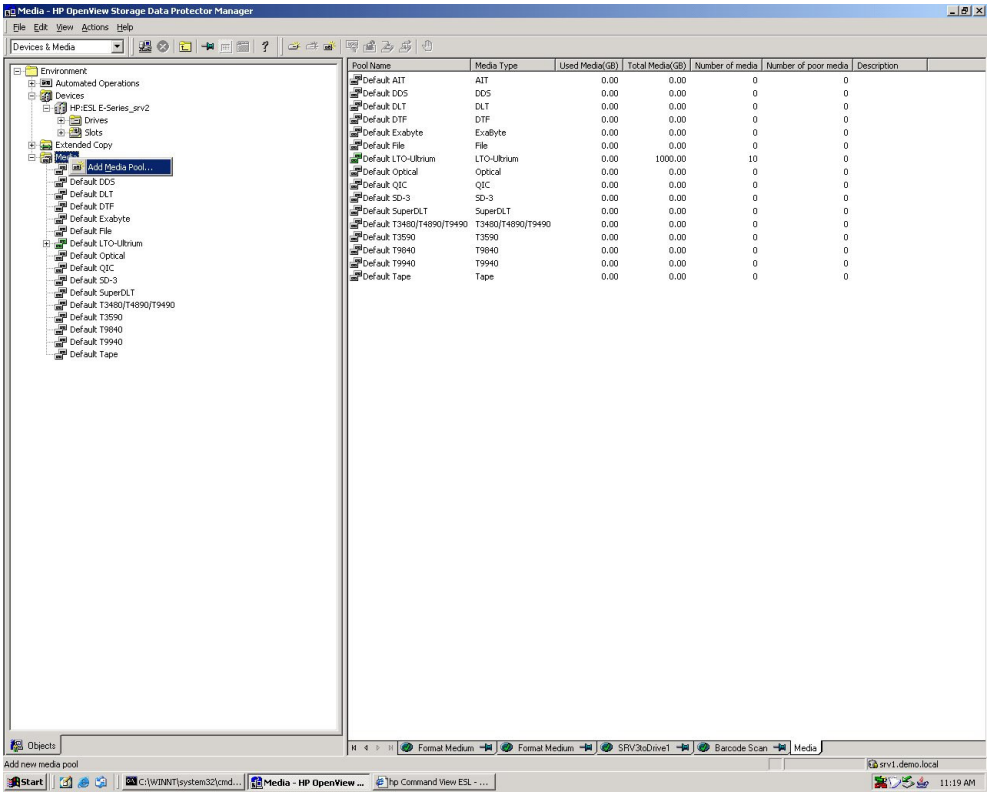
In the example shown 4 pieces of barcodes media were detected in the Library.

SEPARATE INTO 2 GROUPS – ONE GROUP ON DP CLIENT 1 (SRV2 Windows Backups) AND THE SECOND GROUP ON DP CLIENT 2 (SRV3 Linux Backups).

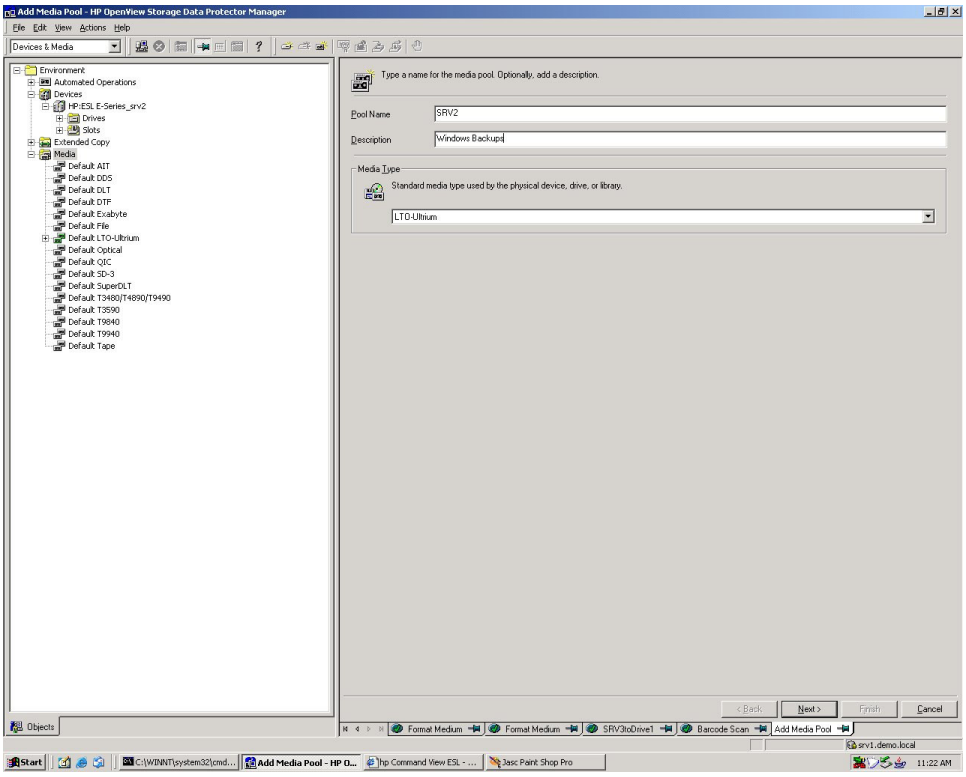
AWAIT INSTRUCTIONS FROM THE INSTRUCTOR AS TO WHAT MEDIA TO ALLOCATE INTO YOUR MEDIA POOLS

On DP Client 1 machine

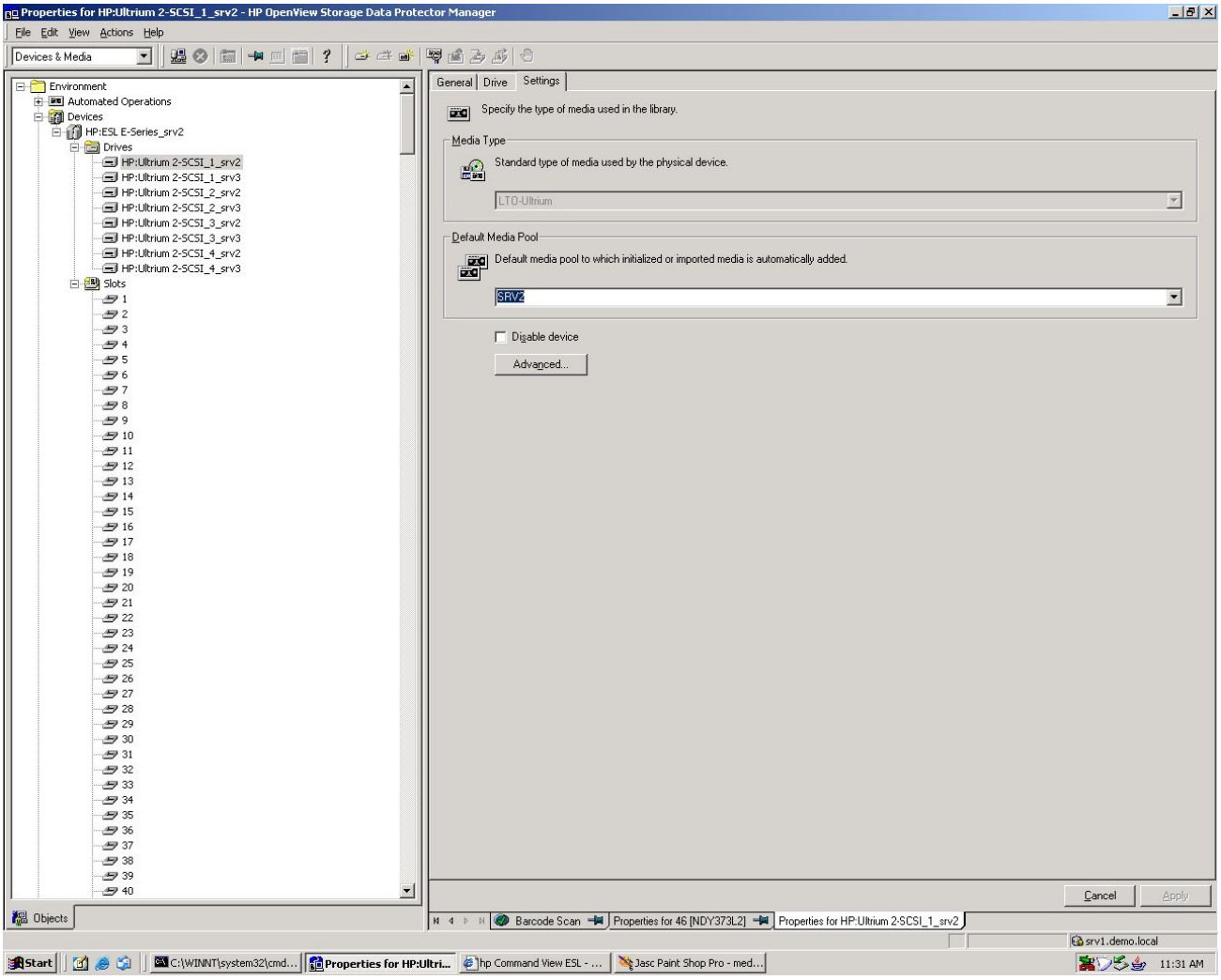
expand + Media in the left hand pane tree structure
Right *Click* Media and Click *Add Media Pool* (as shown below)



We will now add 2 nominated (defined by the instructor) pieces of media to the media pool you are about to create.
When the Add media pool screen appears
Name: media Pool type SRV2 and add the Description “Windows Backups”
Media type is LTO-Ultrium Click *next*
Use the default entries for the next 2 screens click *next* after each screen and *Finish* to Finish



We must finally assign these media pools to be used by specific drives; proceed as follows
Expand + *Drives* to display all the drives available.
Select each of the _srv2 drives (4 in all) in turn
Right click on each drive and click on *properties*
Go to the *settings* tab
Change default media pool from LTO-Ultrium to SRV2 from the drop down list and click *Apply*



Repeat for remaining 3 drives.

On DP Client 2 machine

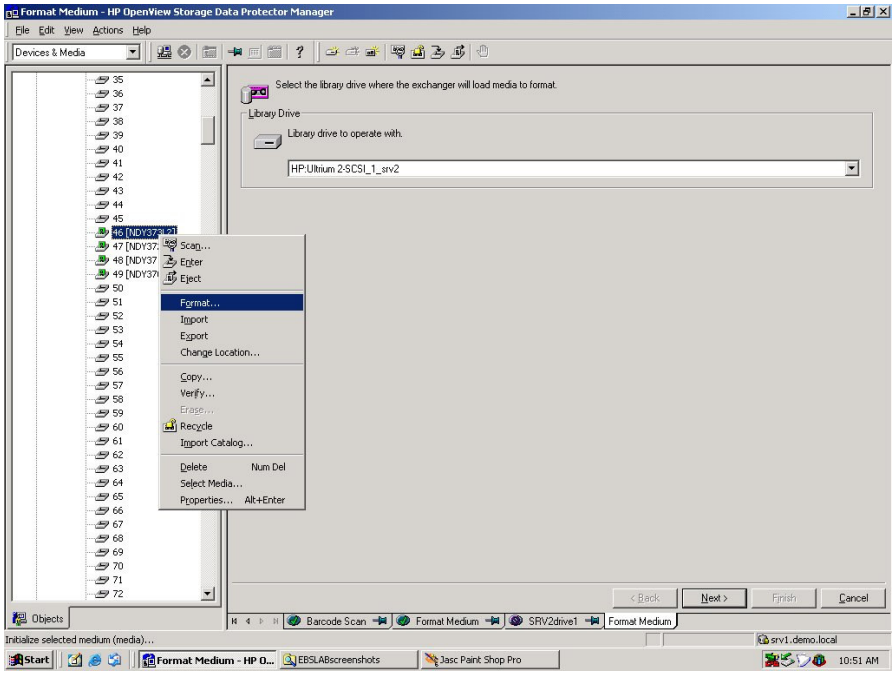
Repeat the process defined above to create a media pool for the Linux Backups
Call it : SRV3
Description: Linux Backups
Type: LTO-Ultrium

Assign media pool SRV3 to be used by specific drives. proceed as follows

Expand + *Drives* to display all the drives available.
Select each of the _srv3 drives (4 in all) in turn
Right click on each drive and click on *properties*
Go to the *settings* tab
Change default media pool from LTO-Ultrium to SRV3 from the drop down list and click *Apply*
Repeat for remaining 3 drives.

ON BOTH DP CLIENT 1 AND DP CLIENT 2 MACHINES FORMAT THE MEDIA WHICH HAS BEEN ASSIGNED TO YOU USING TAPE DRIVES 1 & 2 (for SRV2) AND TAPE DRIVES 3 & 4 (for SRV3)

Now we need to format this media so that Data Protector can identify it.

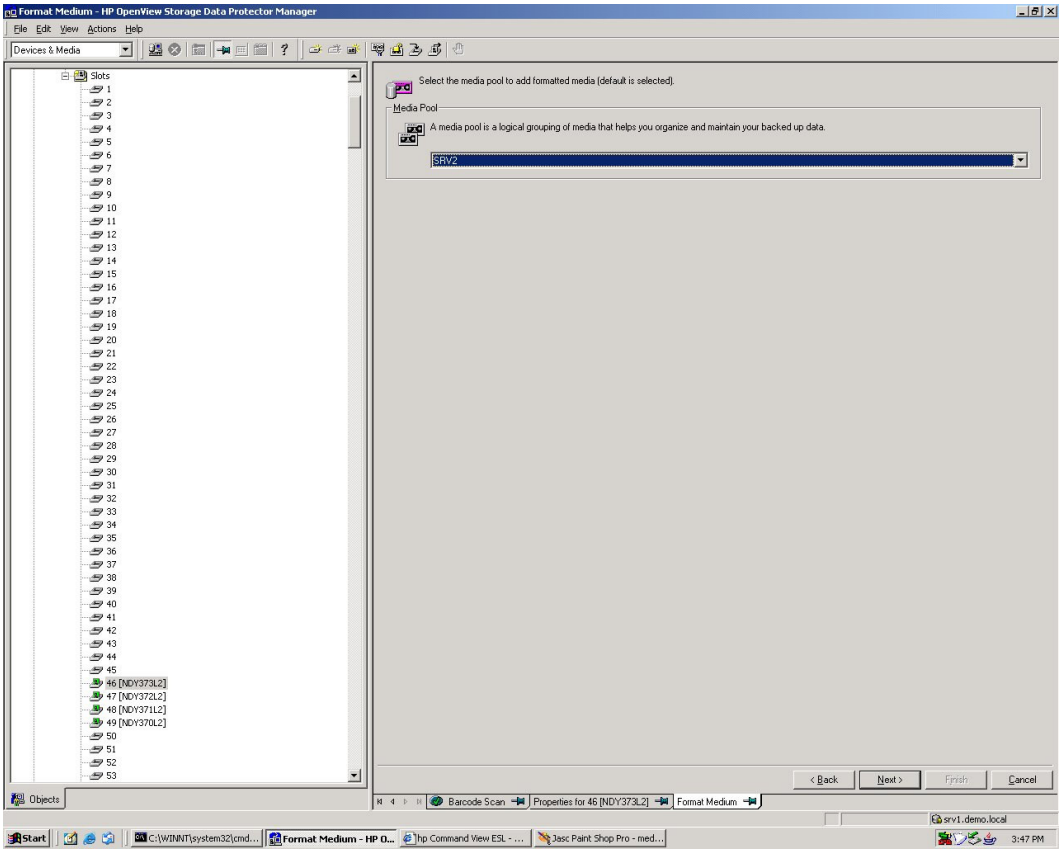


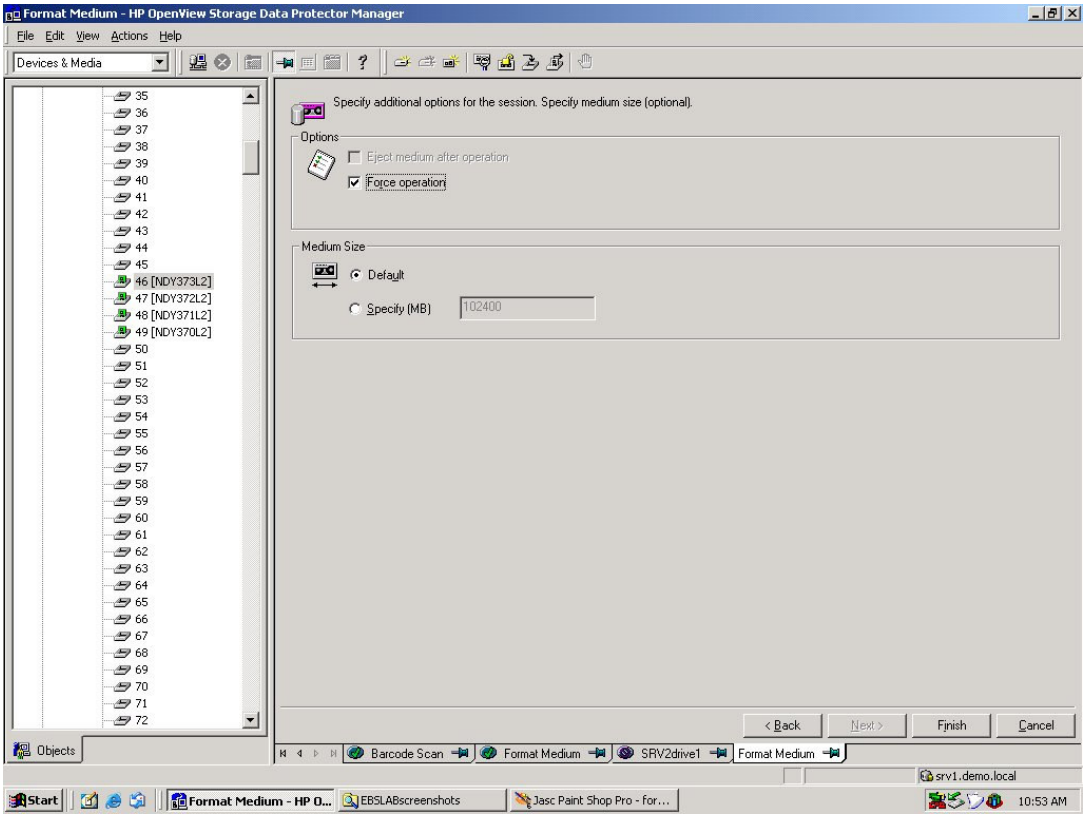
DP Client 1 use Media References _____ (to be assigned at each Lab)

DP Client 2 use Media references _____ (to be assigned at each Lab)

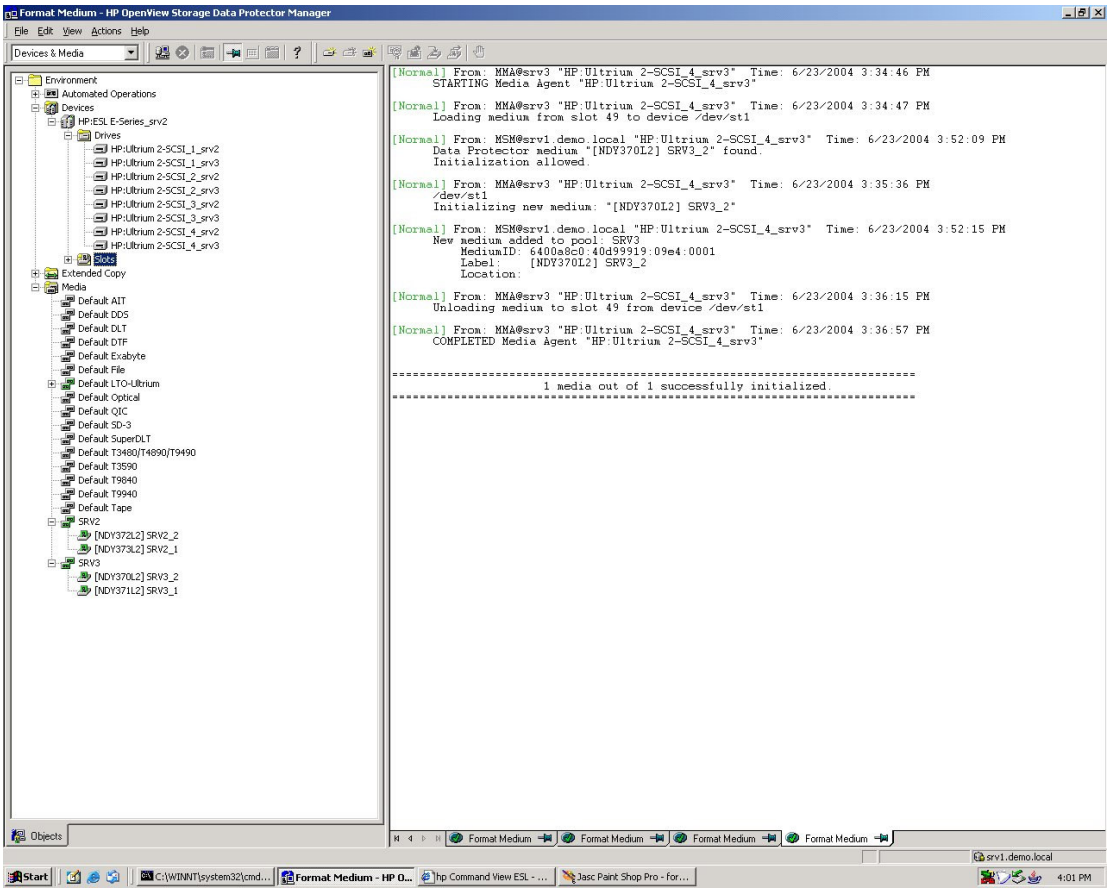
Under *Devices & media* select slots in the tree directory and expand the + sign, a list of all the slots in the library is displayed along with if they contain media and what the media barcode is. Right *click* a piece of media you wish to format and which the instructor has indicated is assigned to you.
You will see the drop down list click *Format*. There now follows a series of screens, the first screen asks you to select which tape drive in the library is to format the media.
DP Client 1 users should use drive HP Ultrium2-SCSI_1_srv2 to format media
DP Client 2 users should use drive HP Ultrium2-SCSI_3_srv3 to format media

Click *Next* and the second formatting screen will appear , here you must allocate which media pool the formatted media is to be placed into, so for DP Client 1 this should be the SRV2 media pool and for DP Client 2 this should be the SRV3 media pool as shown below.





On the last screen it is recommended to check the *force operation* box, since this allows the overwrite of previously formatted HP Data Protector tapes. Click *Finish.* Your format should now start a dialog window and complete successfully.



Note how media Pools SRV2 and SRV3 now contain HP Data Protector formatted media.

SESSSION BREAK 15 MINS

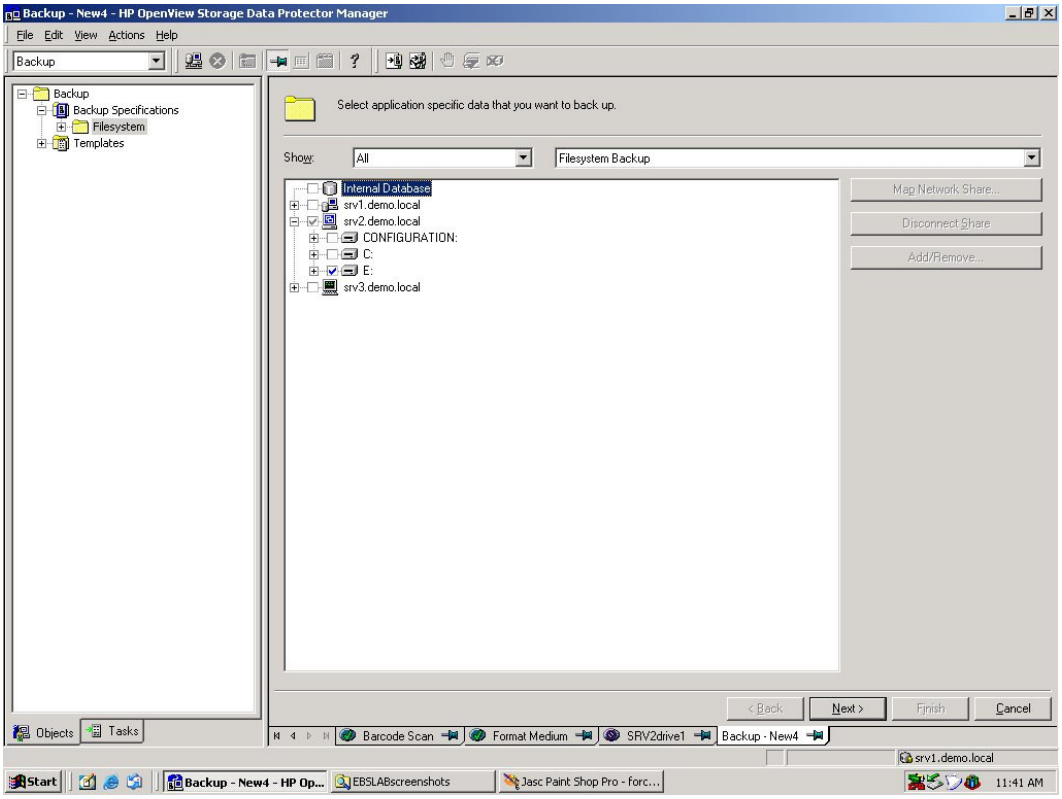
Define a backup job to send data from LUN SRV2 (E drive) to Tape 1 and to send data from LUN SRV3 (MSA_LUN) to Tape 3 to simply test the backup infrastructure.

On the DP Client 1 console…
Select *Backup* from the top line drop down list on the Data Protector Opening screen

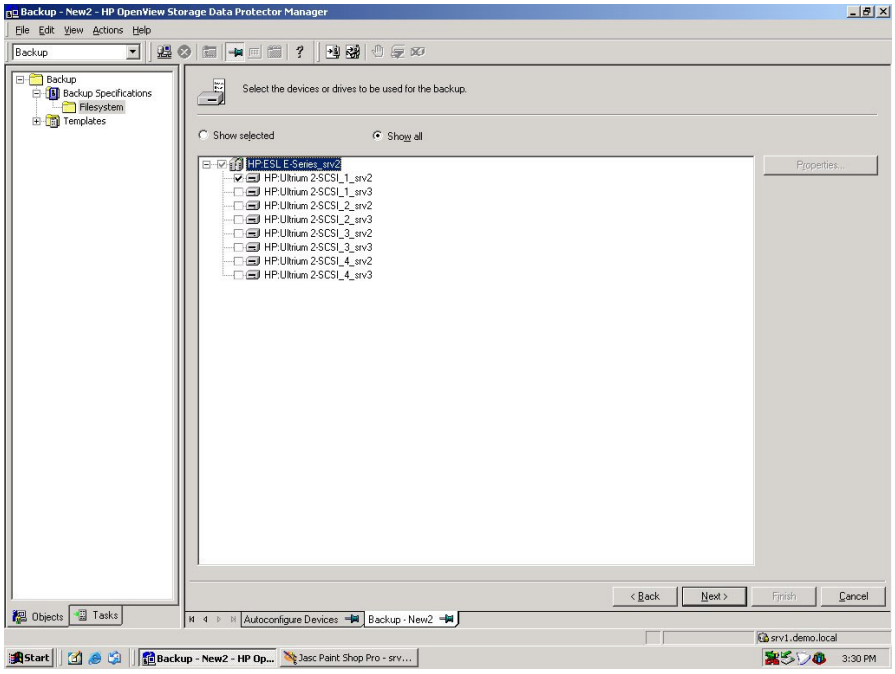
Right click on Filesystem in the directory tree structure in the left hand pane.

"Add Backup" will appear, click on *"Add Backup"* and a new window will appear.
The new window consists of a series of templates for constructing backup jobs
Select *"Blank Filesystem Template"*
Click *OK*

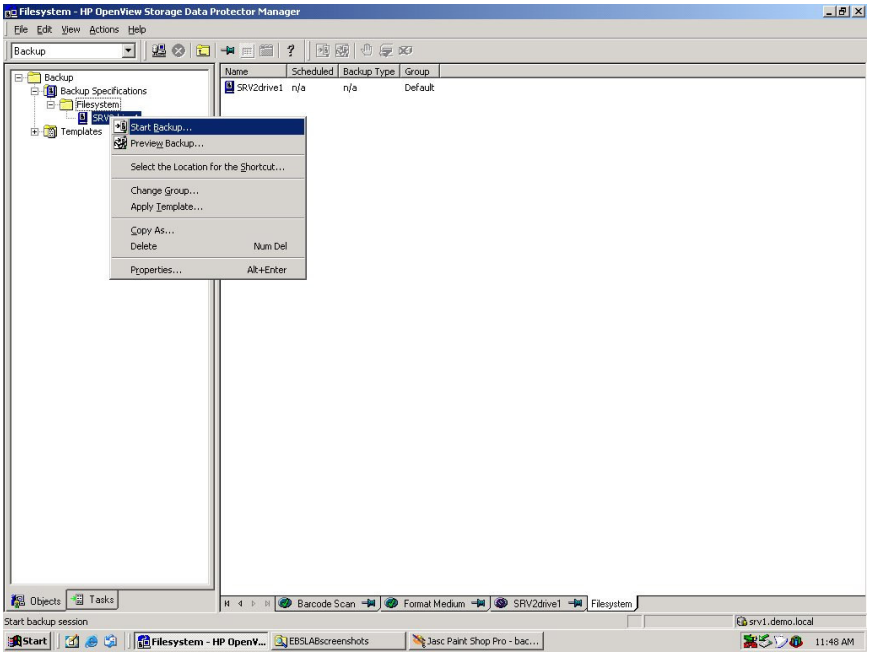
The data source screen appears, expand the + under srv2, tick the *E* drive box as shown below (this will backup the total contents of the E drive)



Click *Next>*
Now we will select which tape drive to use for the backup
Tick HP-Ultrium 2-SCSI_1_srv2 as shown below



Click *Next*>
The Backup Options page will appear
Under *"protection"* select *"none"* from the drop down list. This will enable this test tape to be overwritten time after time.
Click *Next*>
This is the scheduling page, we intend to run the jobs manually so please just Click *Next*>
The last screen is the Backup Summary screen
Click *Next*>
Save the filesystem backup as *SRV2drive1*.
You are now ready to run the backup
Open up the + filesystem backups structure as shown below, select SRV2drive 1 right click, on the drop down menu click *"start backup"*



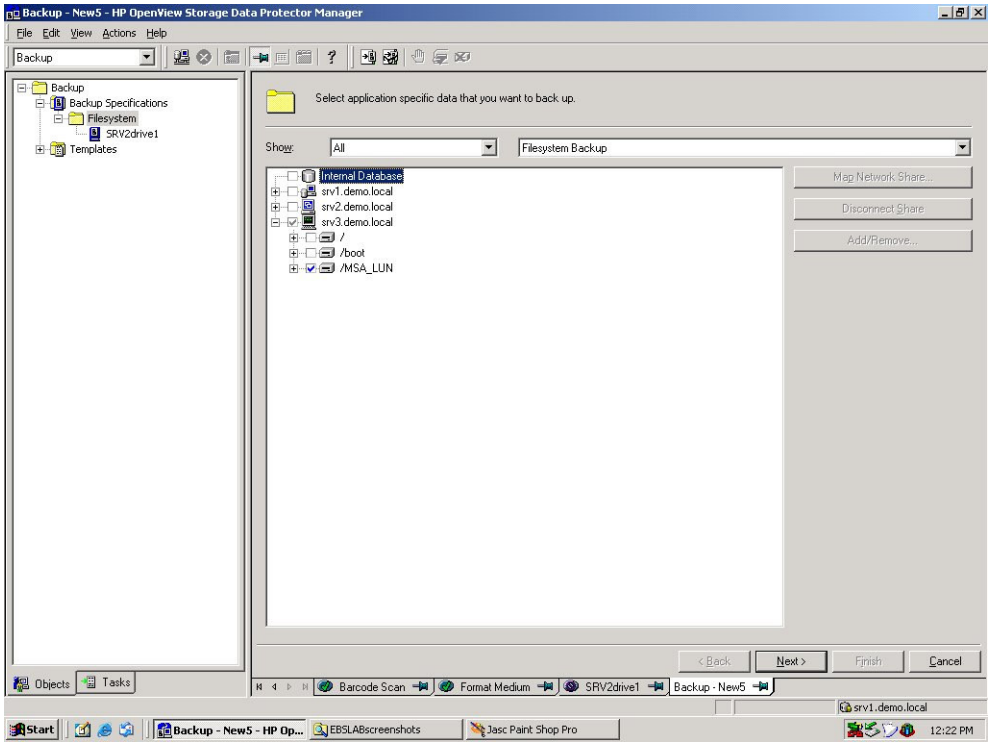
A dialog screen will start telling you the disk and media agents have started and logging the backup progress – the backup should complete successfully.

On the DP Client 2 console…
Select *Backup* from the top line drop down list on the Data Protector Opening screen

Right click on Filesystem in the directory tree structure in the left hand pane.

"Add Backup" will appear, click on *"Add Backup"* and a new window will appear.
The new window consists of a series of templates for constructing backup jobs
Select *"Blank Filesystem Template"*
Click *OK*

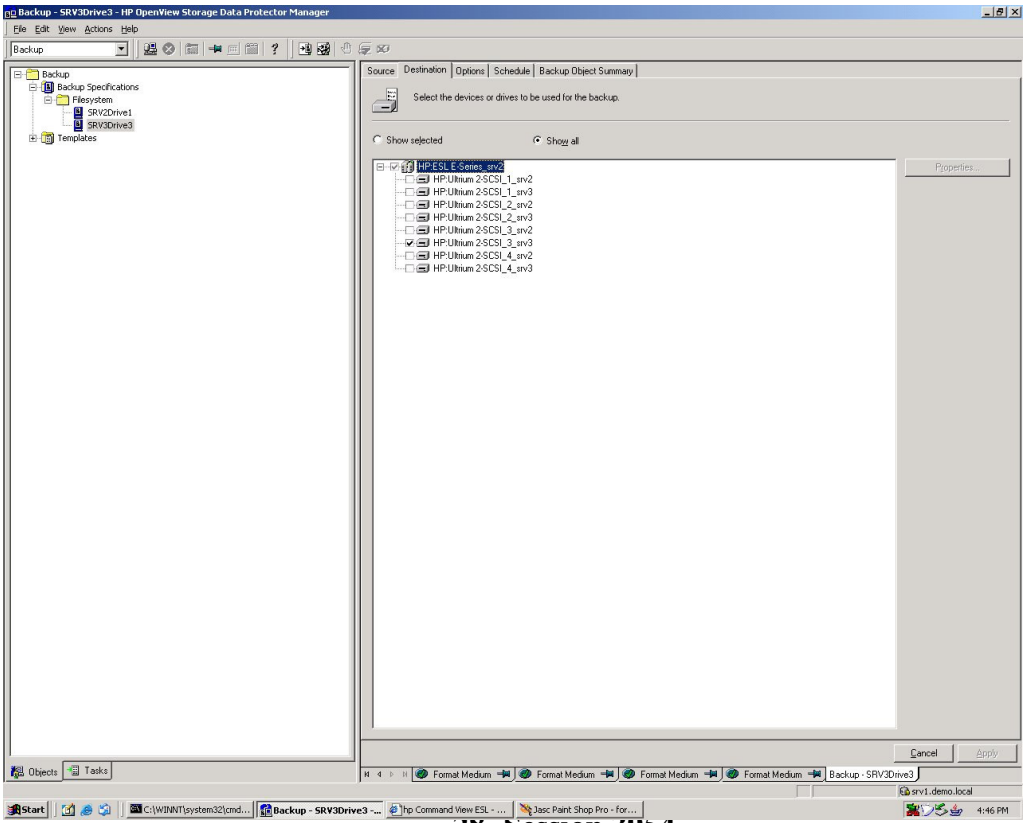
The data source screen appears, expand the + under srv3, tick the MSA_LUN drive box as shown below (this will backup the total contents of the LUN allocated to SRV3 on the MSA1000).



Click *Next>*

Now we will select which tape drive to use for the backup

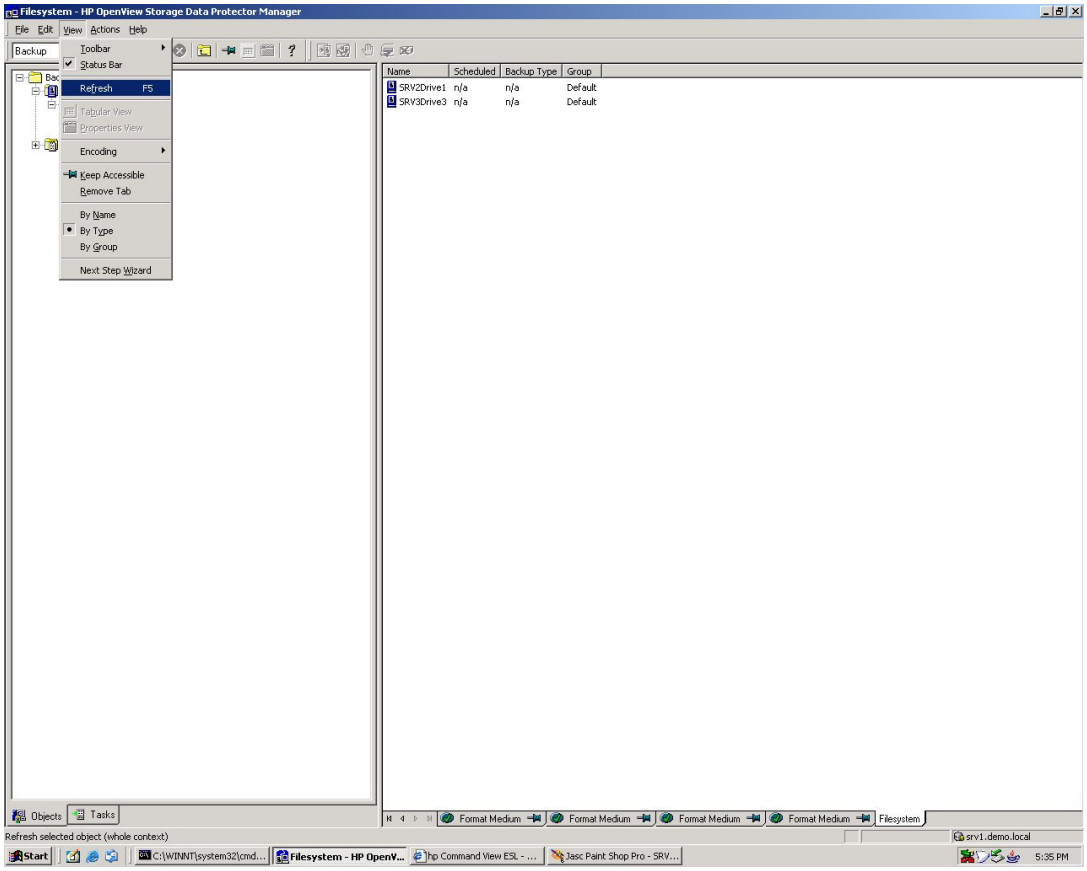
Tick HP-Ultrium 2-SCSI_3_srv3 as shown below



Click *Next*>
The Backup Options page will appear
Under *"protection"* select *"none"* from the drop down list. This will enable this test tape to be overwritten time after time.
Click *Next*>
This is the scheduling page, we intend to run the jobs manually so please just..
Click *Next*>
The last screen is the Backup Summary screen
Click *Next*>
Save the filesystem backup as *SRV3drive3.*
You are now ready to run the backup
Open up the + filesystem backups structure as shown below, select SRV3drive 1 right click, on the drop down menu click *"start backup"*

The backup should complete successfully.

Note: In order to see the full list of backup jobs from DP Client 1 and DP Client 2 machines, it may be necessary from time to time to *Refresh* the screens.



Under *View* on the top level menu of HP Data Protector Click *Refresh* or Function Key F5.

Part 4 – Tape Drive Sharing

Objectives
In this section we will

- Demonstrate multiple servers accessing the same tape drive
- Understand differences between zoning and LUN masking
- Implement LUN masking using HP Secure manager
- Use of lock names at an application level to share tape drives.
- Understand the nuances of specifying tape drives which are not available to the server via the SAN fabric.

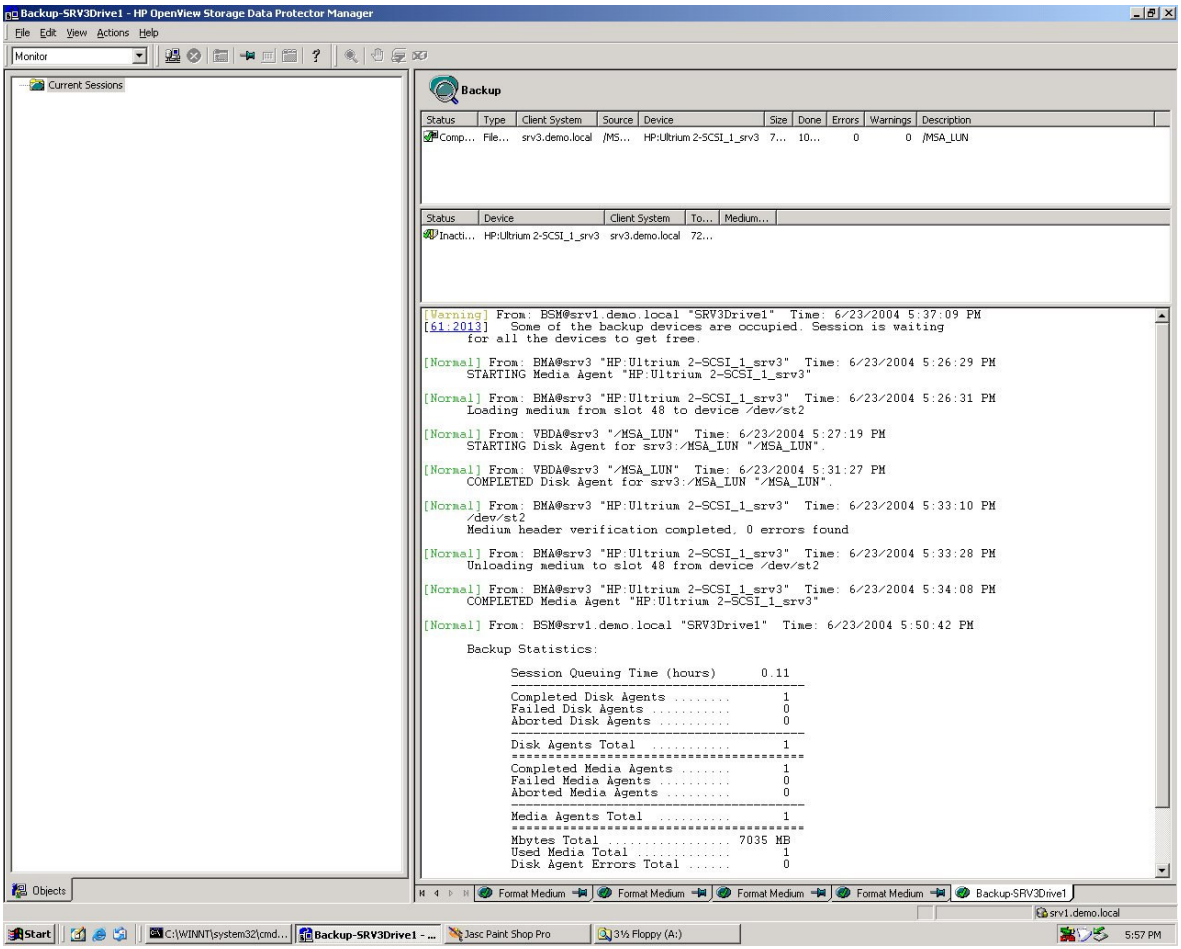
Procedure

- We will try sending data to the same tape drive from SRV2 & SRV3 and note the issues that this causes due to the fact there is no LUN masking currently deployed in the interface controllers.
- We will the implement LUN masking and note how Tape drives 1 & 2 now only are presented to SRV2 and Tape drives 3 & 4 are now only presented to SRV3.
- We will run a backup from SRV2 to Tape 3 with some unexpected results.

On DP Client2 copy the Filesystem template SRV3Drive3 and re-edit the Destination tape drive to be HP-Ultrium2-SCSI_1_srv3. (This is the same physical tape drive as used in Filesystem SRV2 backup)
Save this Backup job as SRV3Drive1

BOTH GROUPS MUST NOW CO-ORDINATE ACTIVITIES
FROM DP CLIENT 1 RUN SRV2Drive1 BACKUP JOB
FROM DP CLIENT 2 RUN SRV3Drive 1 BACKUP JOB
START THESE JOBS SIMULTANEOUSLY

One of the backups will stall as shown below because one system has got access to the drive before the other.
The backups think they are using different devices when in actual fact they are using the same physical device.
This could be damaging if a system took the drive for long periods of time – some systems may never get backed up within the backup window.



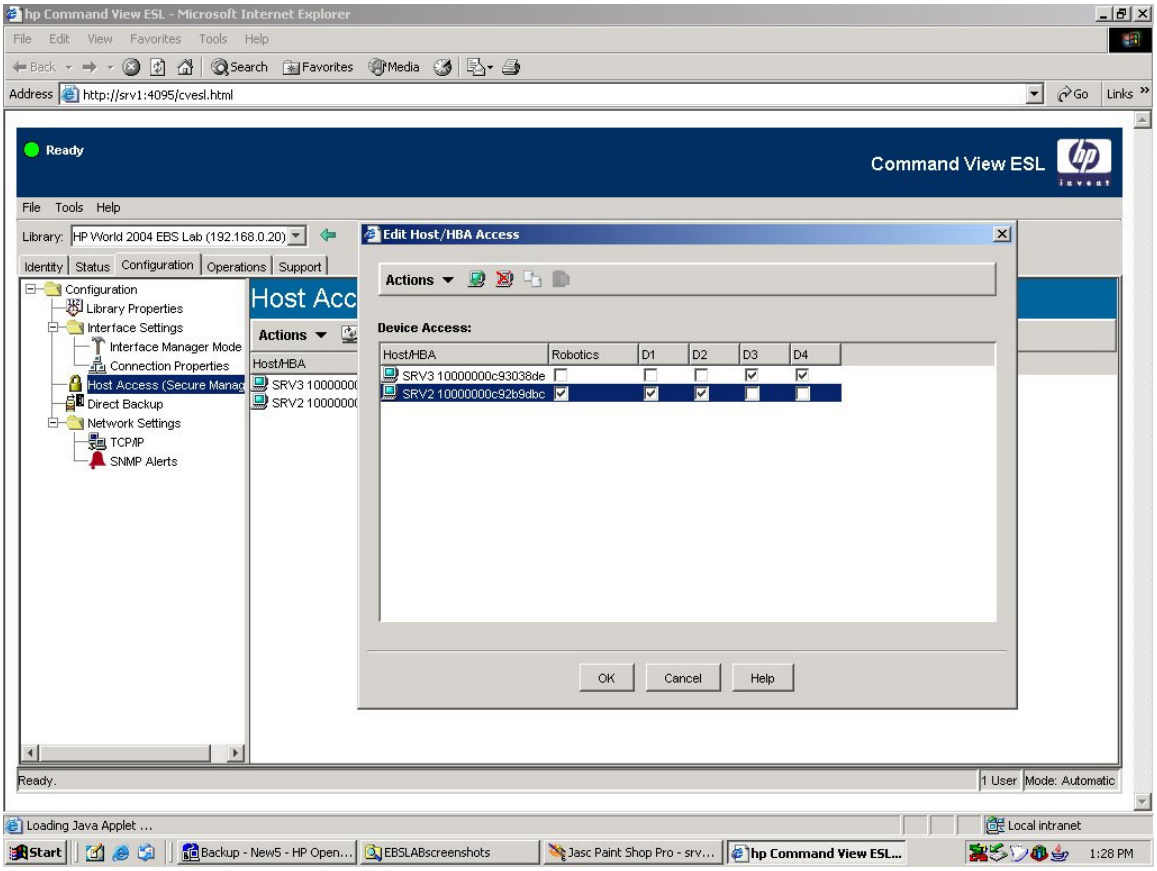
How can we correct this?

Configure HP secure Manager

Go to the Command View ESL console and select the configuration tab, display the secure manager settings.

Click *Actions* to edit the Host HBA settings

Now “tick” SRV2 to allow SRV2 to have access to the robotics, Tape 1 and Tape 2
“tick” SRV3 to allow SRV3 to have access to Tape 3 and Tape 4 as shown below

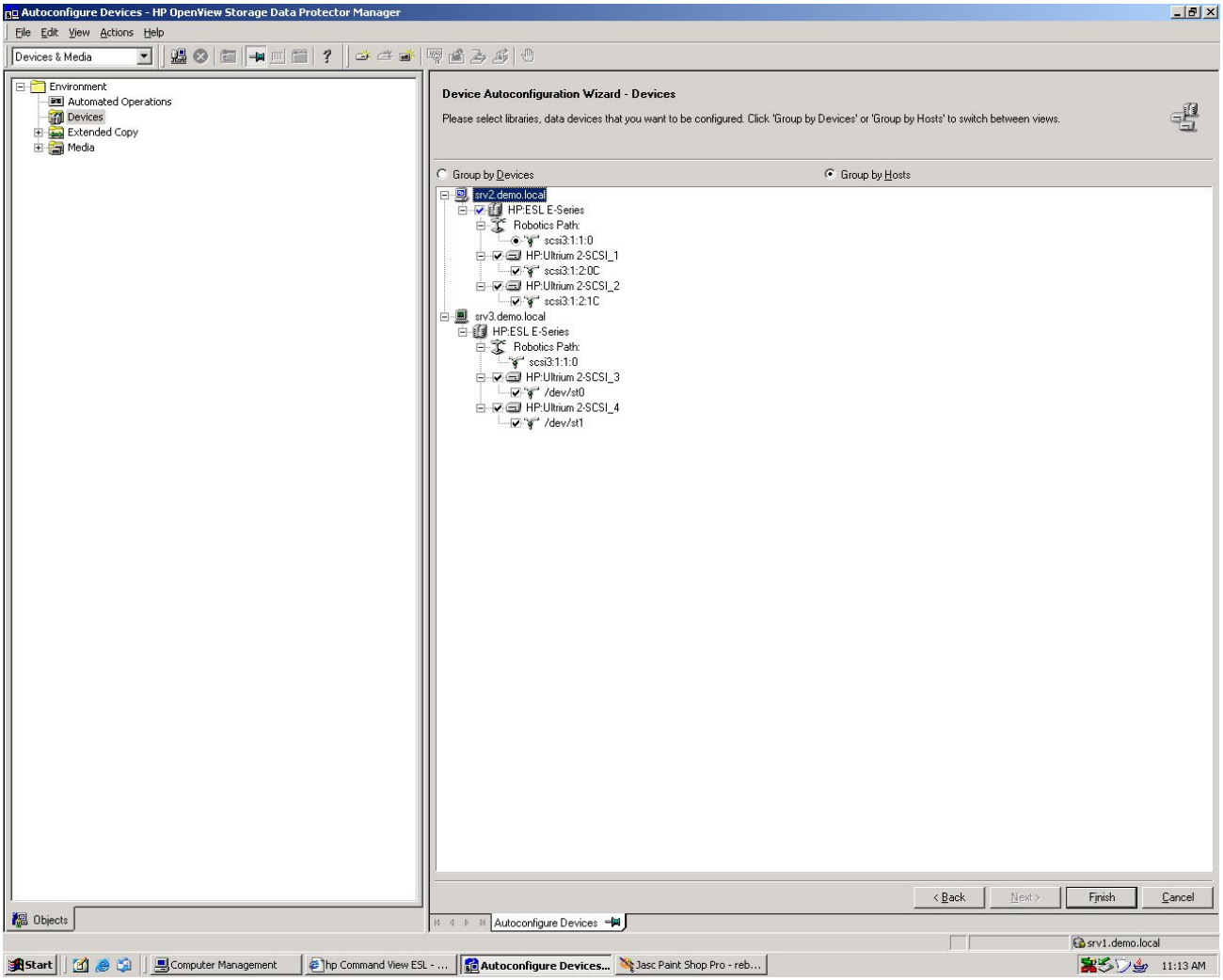


Click *OK*

Because this process involves re-booting of the interface controllers to accept the new "storage presentation" there may be a 1-2min wait at this stage

ON DP CLIENT 1 STATION ONLY – DELETE & THEN AUTO-CONFIGURE THE LIBRARY AGAIN SO THE NEW INTERFACE CONTROLLER SETTINGS WILL BE USED

To show the effect of this change, go into Data protector on DP Client 1and delete the Library configuration (right click *devices* and then click *delete*) , then Auto-configure the library again. This time a display similar to that shown below should appear.



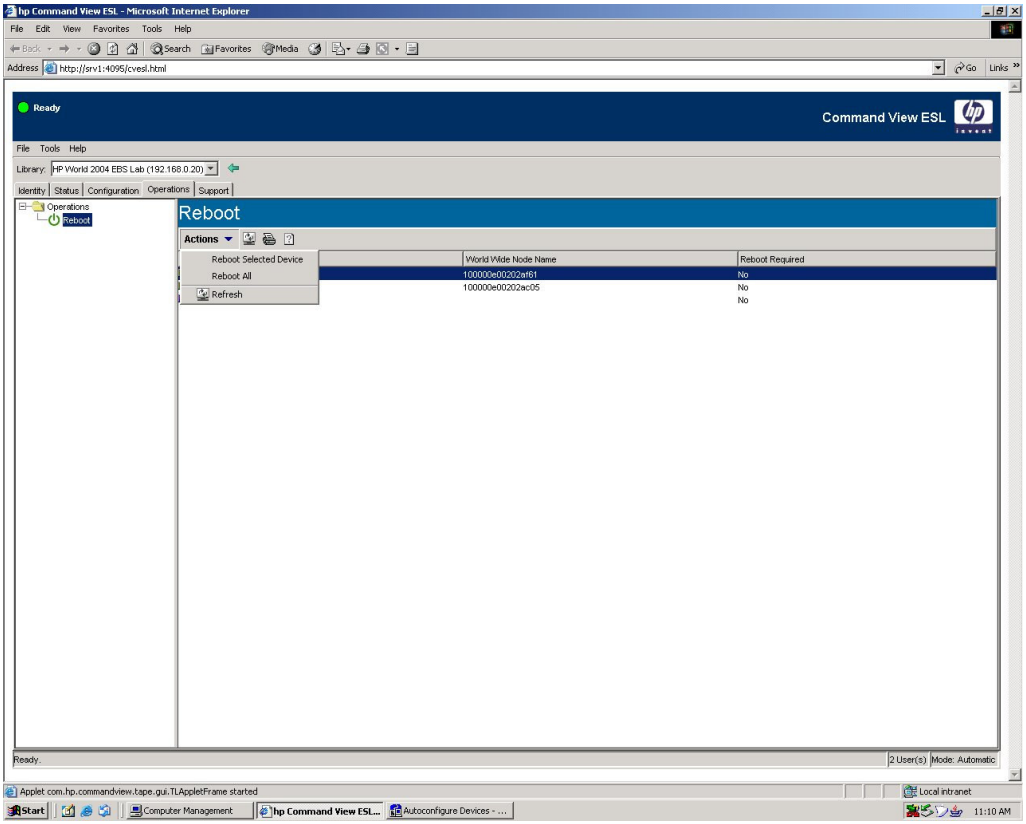
Note: you must still tick the checkbox to confirm you wish this connection to be used by HP data Protector.

Note: SRV2 now sees only Robotics, Drive 1 and Drive 2
SRV3 now sees only Drive 3 and Drive 4 (as detected by HP Data Protector)
This mimics precisely the selective storage presentation performed by using HP secure manager. This is done at a hardware fibre channel protocol level, so devices are not seen by servers who have no rights to access them.

After you have finished the auto-configuration, you must enable the barcode reader support and perform a barcode scan as you did previously before the library can be used.

Note: it may be that Windows does not automatically detect the Library after rebooting the interface controllers following applying the secure manager configuration. If this happens

a) Try going into *manage computer*, *device manager* and re-*scan for hardware*.
b) Using CV-ESL as shown below reboot the library controller as shown below



On DP Client 1

Copy the Filesystem backup template *SRV2Drive1*, edit it to select the destination of the backup to be Drive 3
Save as "*SRV2toDrive3"*
Start the backup.

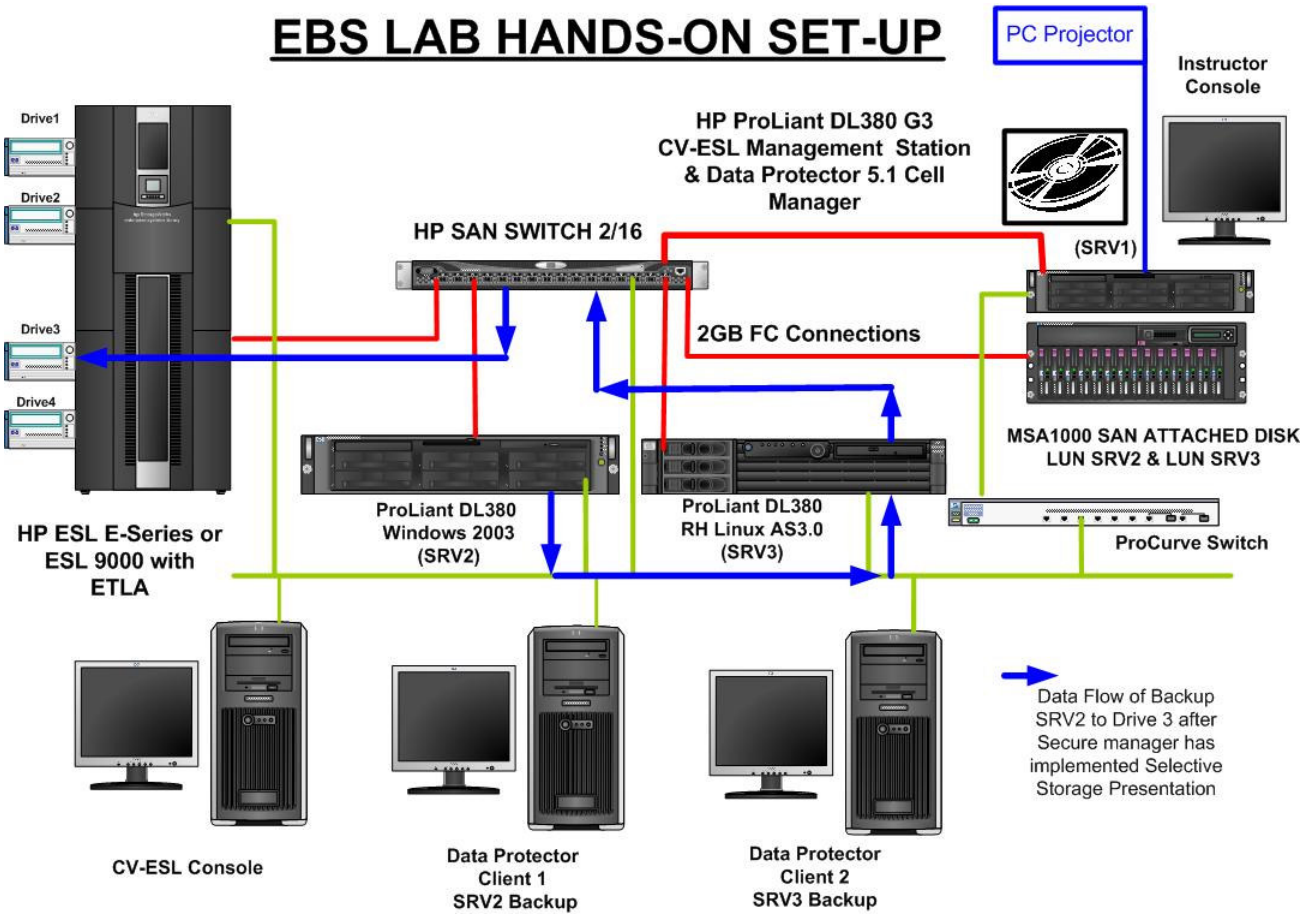
The backup runs successfully – Why?

On DP Client 2

Copy the Filesystem backup *SRV3Drive3*, edit it to select the destination of the backup to be Drive 1
Save as "*SRV3toDrive1"*

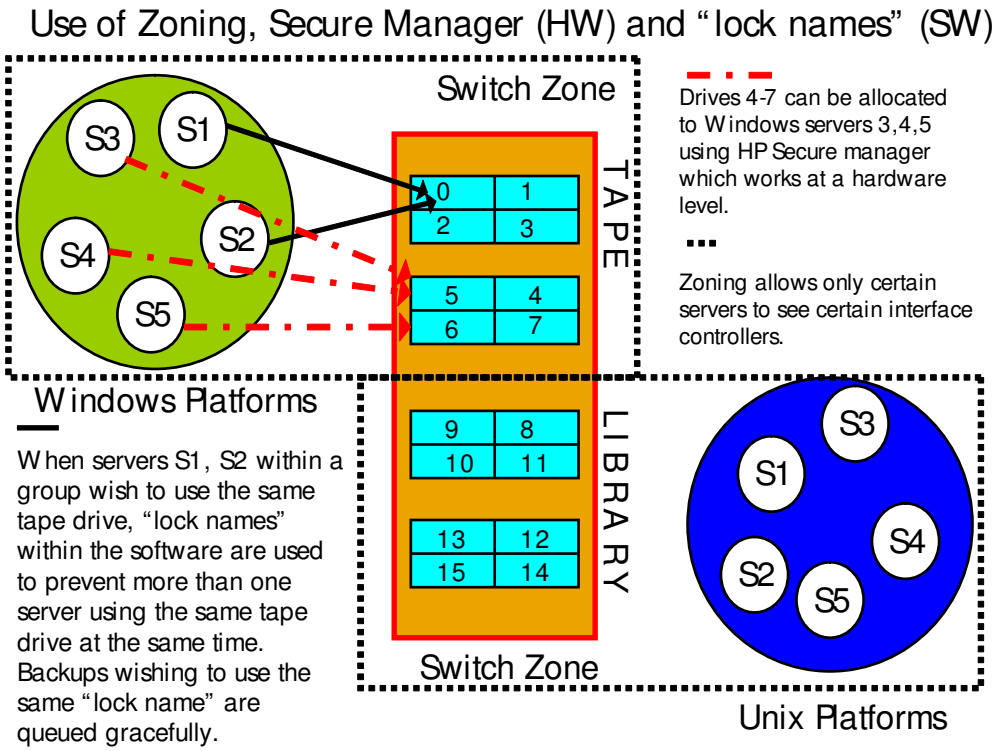
The backup runs successfully – Why?

The answer is because the backup is now being performed over the Network. Data Protector when attempting to backup SRV2 still has visibility of Drive 3 in the Enterprise, even though Tape Drive 3 can no longer be accessed directly by SRV2, instead Data Protector routes the data over the Network to SRV3 (which does have local access to Drive 3) and SRV3 then pushes the data onto Drive 3. This is not what we wanted because the network backup is slower and this backup consumes processing bandwidth on SRV3, but this illustrates a good point in terms of the capabilities of Enterprise backup software such as HP Data Protector. The data path is shown in the diagram below. The same is true of the backup job from SRV3 to Drive 1.



And finally……..

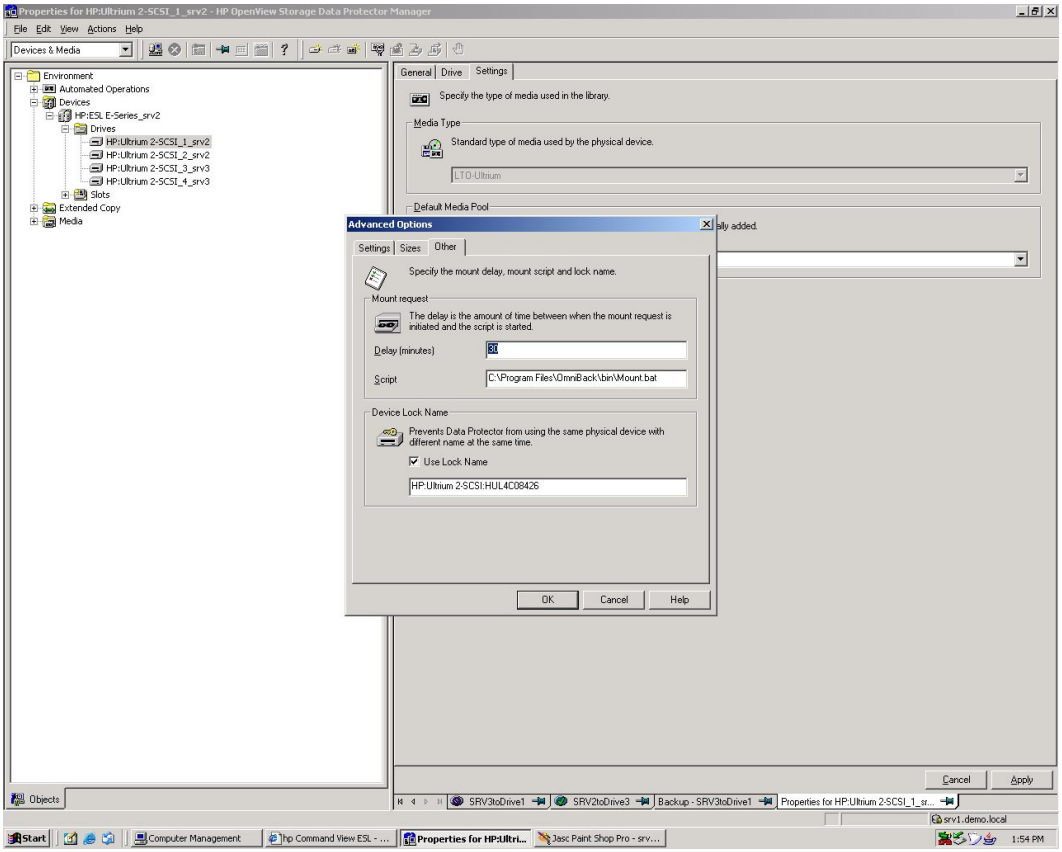
Within ISV Backup Applications there is a concept called “lock names” which allows tape drives in a shared “pool” to be used without disruption from other hosts trying to access them at the same time. The concept is explained below.



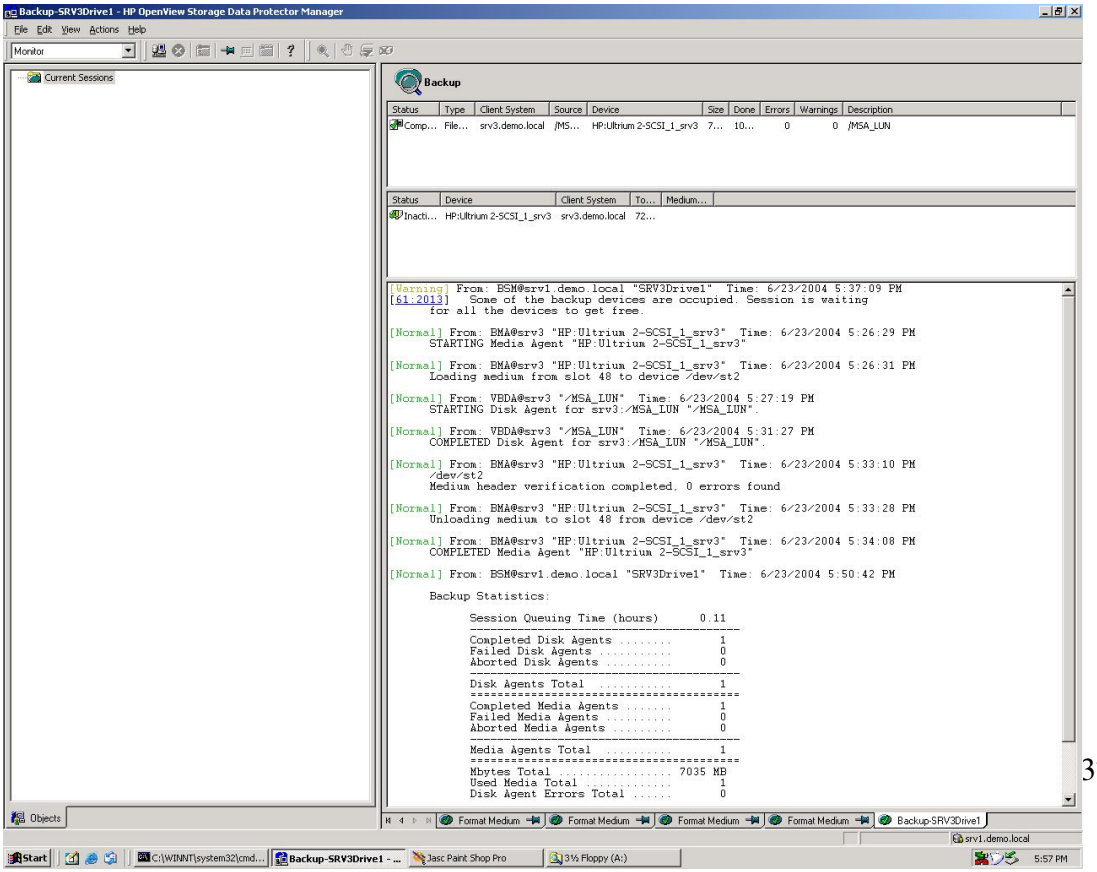
In the above example Windows server 1 and Windows server 2 may both have backup jobs which wish to use Tape Drive 0, and Tape Drive 0 may appear as a different drive name to server 1 and server 2, hence there is distinct possibility that both servers could try to send data to the same tape physical drive at the same time (though using different drive names). So as default in HP Data Protector "lock names" are assigned which are unique to the physical tape drive (and are generally based on the tape drive physical serial number).

Lock names

On the *devices and media* drop down list
Select as *HP Ultrium2-SCSI_1_srv2* in the devices list.
Right *Click* the tape drive name
Click *Properties*
Click the *Settings* tab
Click the *Advanced* radio button
Click the *"Other"* tab
The screen below shows the "lock name" for tape drive HP Ultrium2-SCSI_1_srv2
Note this lock name. Note how it includes the tape drive Serial #.
You may change the lock name at this stage if you wish.

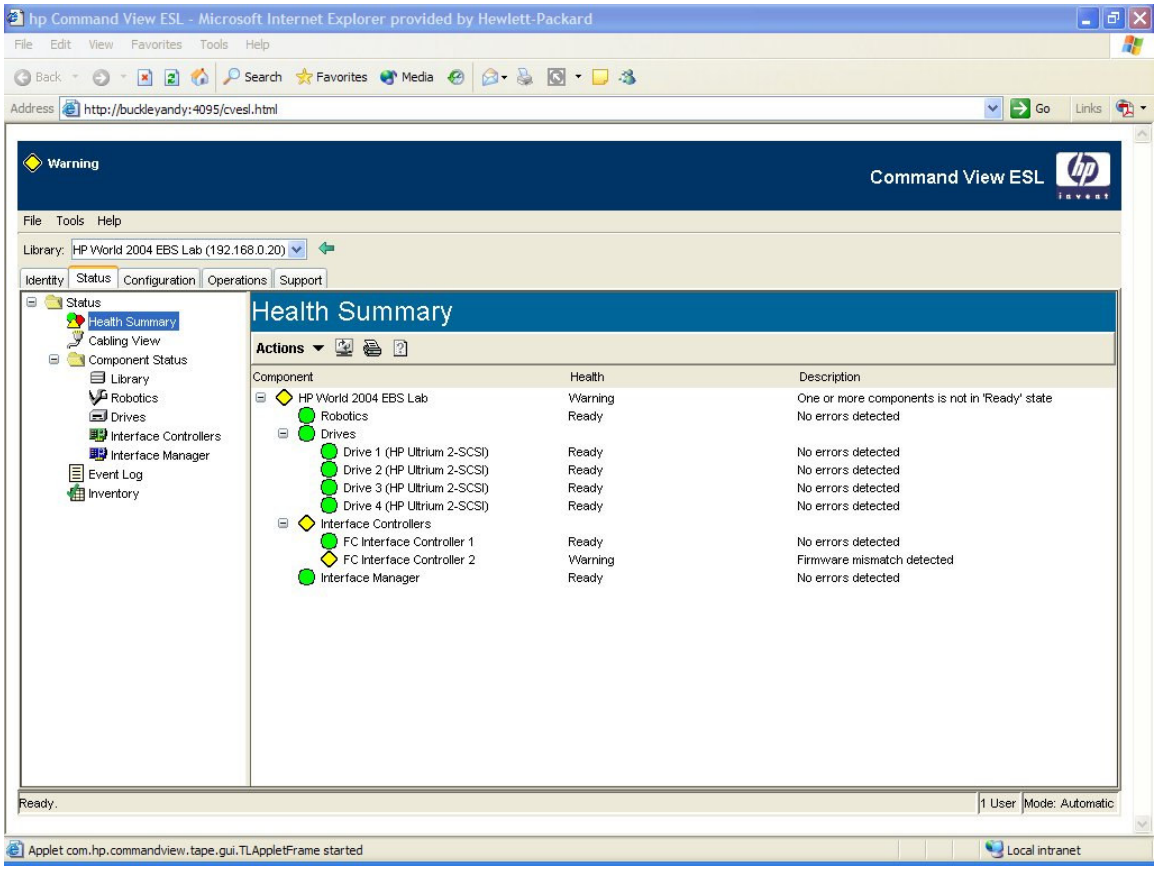


In the example shown above, should Windows Server1 and Windows Server 2 try to access tape drive0 at the same time, one of them will gain control first and the backup will proceed, the other server will wait patiently because it realises the device lock name is in use (locked). In HP Data Protector this situation is reported to the user as “waiting for devices to get free” as shown below:



If time permits……..

The instructor will now introduce a series of faults onto the Libraries and the students must use CV-ESL and their architecture knowledge to diagnose and correct the failures. For example



In the example shown above a "firmware mismatch" on Interface controller 2 is caused by the Interface manager having a different record of the firmware on the interface controller than is actually implemented on the interface controller. The solution to this would be to upgrade the firmware in controller 2 again but this time it should be done through the interface manager via CV-ESL.

Other failures may include:-

- Tape Drives or robotics unavailable
- Library Internal LAN communications (may require use of serial cables to access components such as interface controllers and interface managers) – ask the instructor about these techniques.
- Expired or End of Life media

End of Lab