mThree Alumni Training

Introduction to Computer Fundamentals and Windows

ALUMNI
BY MTHREE CONSULTING

Introduction to Computer Fundamentals and Windows

In this course, we look at various computer fundamentals as well as basic concepts related to managing Windows-based systems and networks.

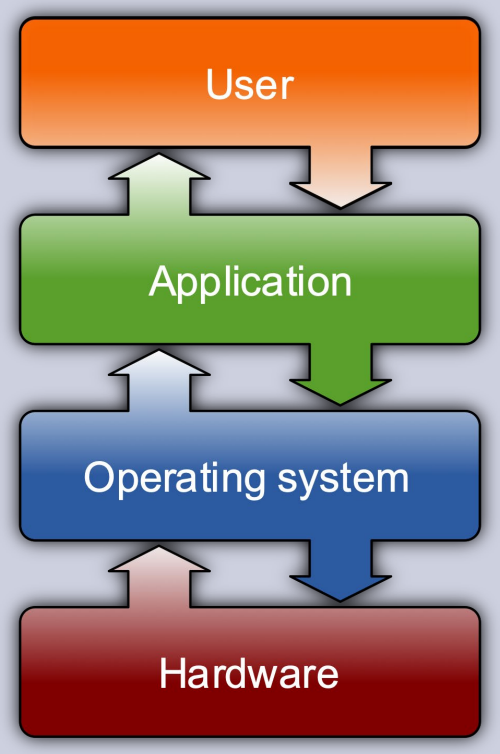
What is an OS?

- An operating system (OS) is the software that manages computer hardware and software resources and provides common services for applications installed on a computer.

- For hardware functions such as input, output, and memory allocation, the operating system acts as an intermediary between application software and the computer hardware.

The OS manages a computer's hardware resources, including:

- Input devices such as a keyboard, mouse, scanner, camera, or microphone.
- Output devices such as display monitors, speakers, and printers.
- Network devices such as modems, routers, and network connections.
- Storage devices such as internal and external drives.

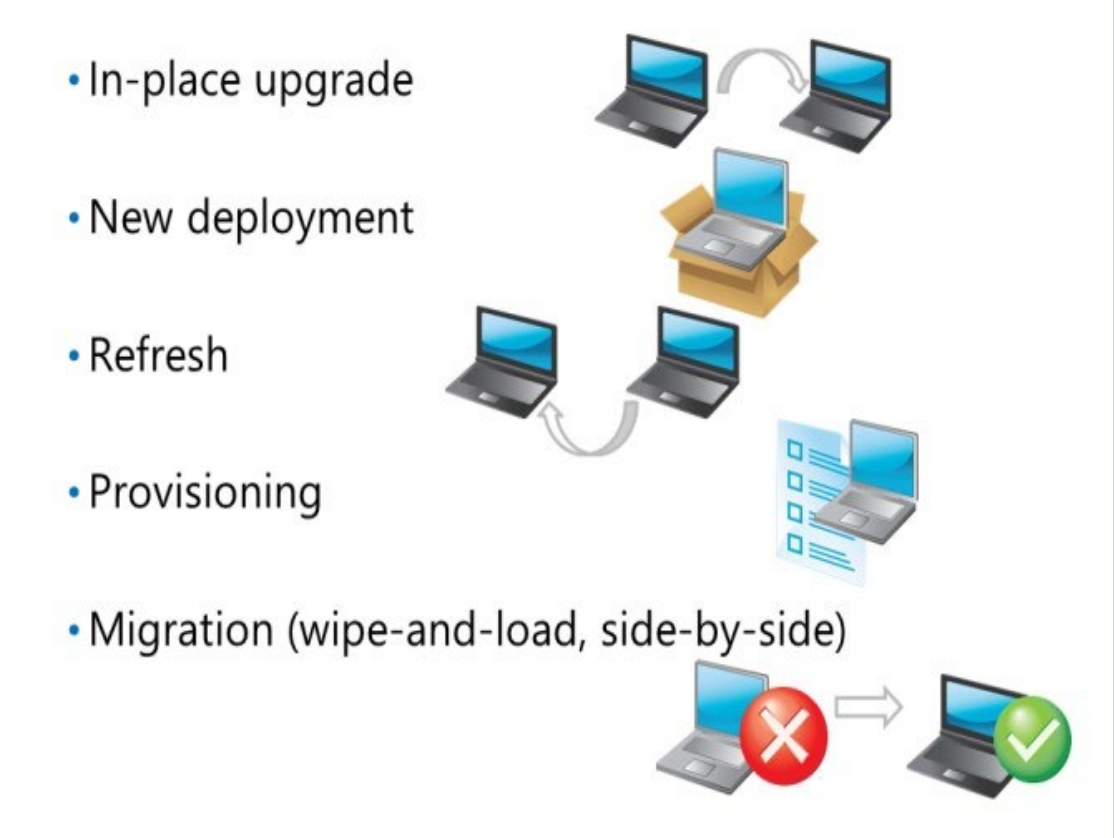


OS Installation

Here we can see the various types of installation we can have for operating systems.

You will have experienced some of these on your personal computers.

How this is managed in banks will usually be run by a systems admin team.



File Systems

mthree

Each disk must be formatted with a filesystem. Some file systems are optimized for large files, others for network files etc. Sometimes we need to upgrade to a new version of a filesystem for performance/stability reasons.

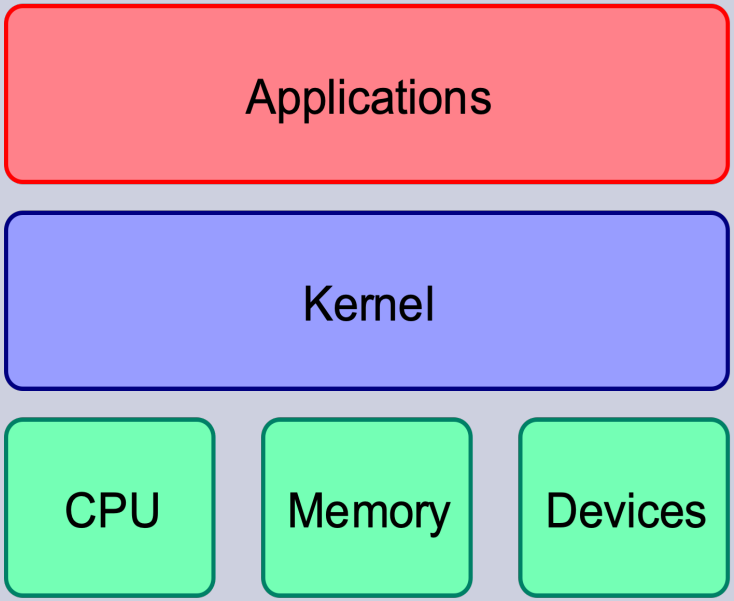
Maintaining Integrity	Scanning filesystem for corruptions, recovers lost or broken data
Access Control	Define access policies for users and programs
Utilities	Maintaining and providing common interface for editing and manipulating the filesystem

Linux and Windows use different systems:

- **Common local file systems:** Windows: NTFS; OS/2 & MAC: HFS and HFS+ HPFS, APFS; Unix/Linux: ext4,xfs; CD/DVD: ISO 9660; Vmware: VMFS
- **Network Filesystems:** Linux: NFS; Windows: CIFS (SMB); Web: FTP

What is the Kernel?

- The kernel is the core of a computer's operating system, with complete control over everything in the system.
- Kernel is the third program loaded on start-up after BIOS, BootLoader
- The kernel is responsible for low-level tasks such as disk/network management, task management and memory management.
- The interface is a low-level abstraction layer: when a process makes a request, it is called a system call.

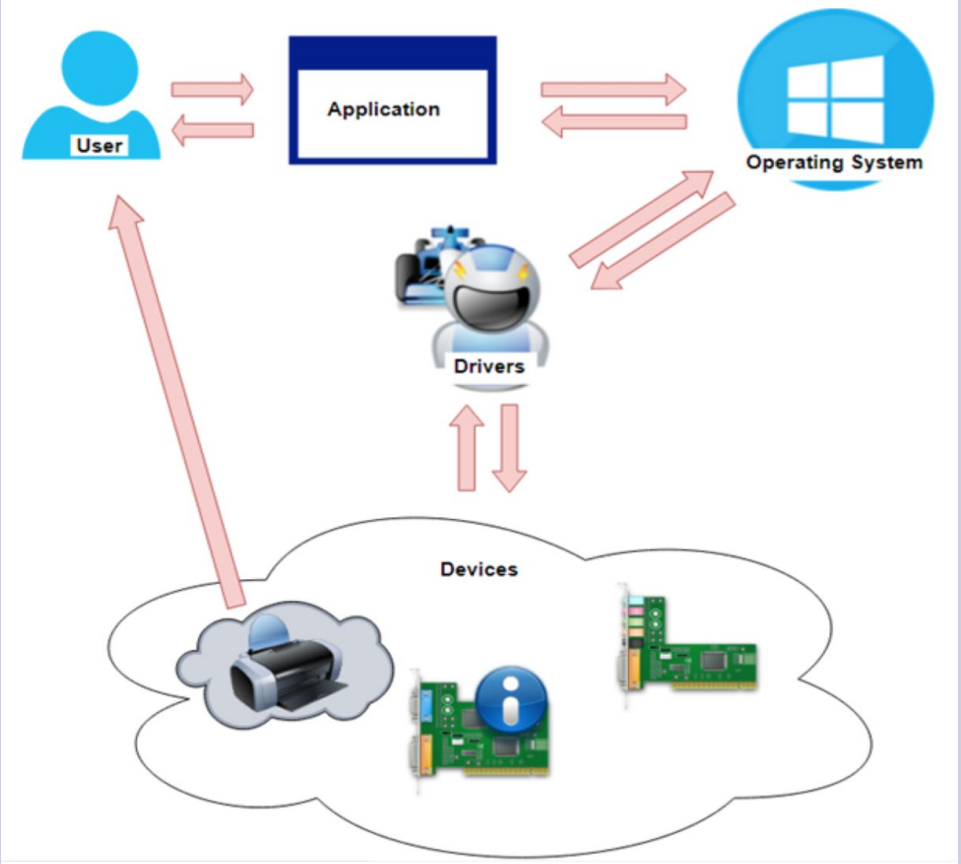


Device Drivers

Applications must use a driver to access a device.

A device driver is a software program that controls a particular type of hardware device that is attached to a computer. For example, if you get a new printer, you will usually have to install a driver for that printer.

Drivers often have configuration/monitoring tools that load in the notification area (on the task bar just to the left of the clock). Other drivers are generally invisible to the user, but they can be managed using Windows Device Manager.



System Services

A system service is software loaded into memory that works in the background for a specific process.

Some services load at startup and some load as required or manually.

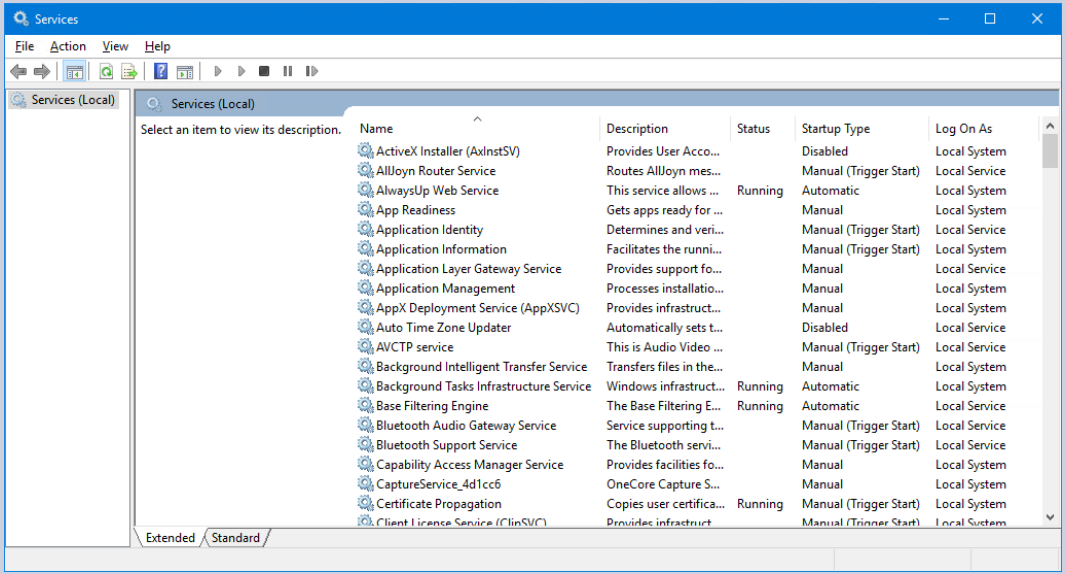
System Service	Service needed to run the OS
Network Service	Service for the network devices and dependent components
User Service	Services which user operations depend on

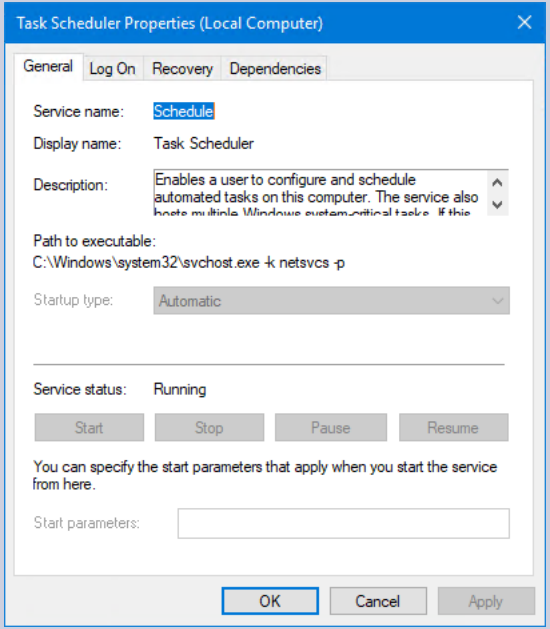
There is a service control process to watch over all services.

Some services depend on other services to work.

Windows Services

We can view the services list in the Windows Services tool.





Windows Registry

The Windows Registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows OS.

When a program is installed, a new subkey containing settings such as location, version, how to start are all added to the registry.

The Registry contains keys and values:

- Registry keys are container objects similar to folders and the values are non- container objects similar to files
- Keys may contain values and subkeys
- Keys are referenced with a syntax similar to Windows path names (backslashes indicate hierarchy levels)
- Keys must have a case insensitive name without backslashes

Windows Registry

mthree

Here are some examples of keys:

Command	Comments
HKEY_LOCAL_MACHINE or HKLM	Local machine specific configuration data
HKEY_CURRENT_CONFIG or HKCC	Contains information gathered at runtime; information stored in this key is not permanently stored on disk but rather regenerated at boot time
HKEY_CLASSES_ROOT or HKCR	Contains information about registered applications such as file associations and OLE object class and user data
HKEY_CURRENT_USER or HKCU	Stores settings that are specific to the current logged in user
HKEY_PERFORMANCE_DATA (Not visible)	This key provides runtime information into performance data provided by either the NT Kernel itself or running system drivers and programs
HKEY_USERS or HKU	Keys for each user profile actively loaded on the machine

Windows Registry

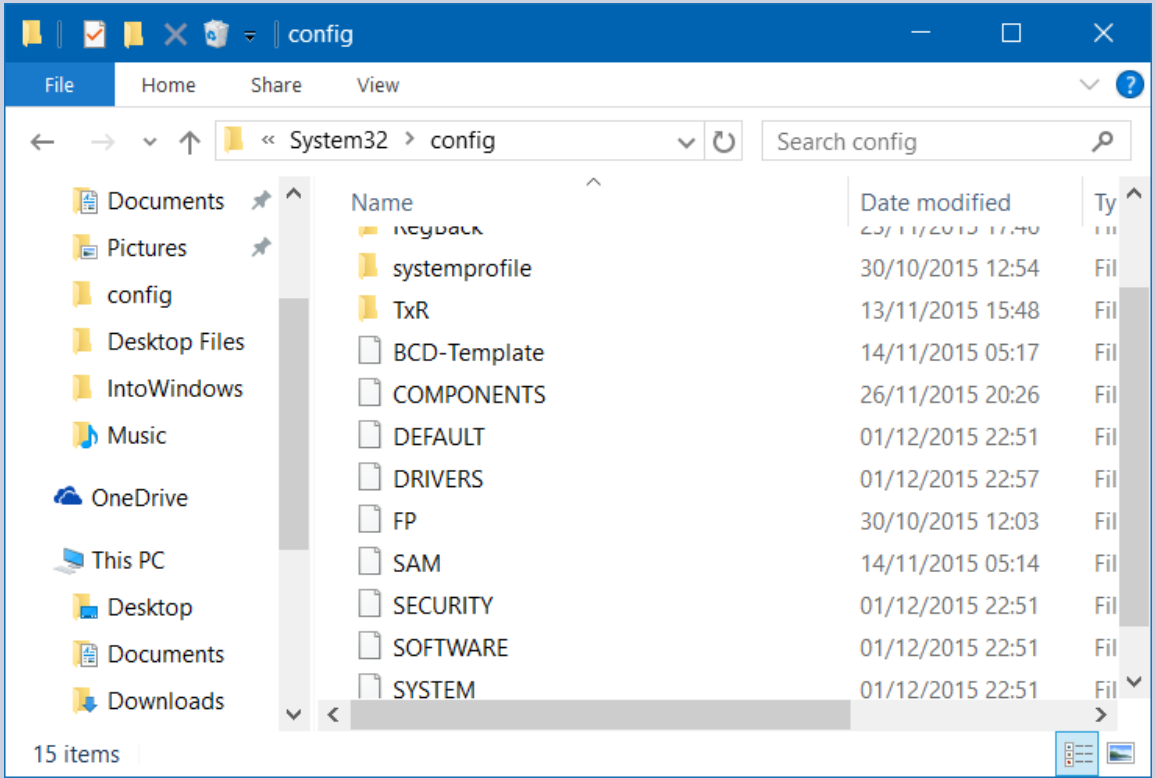
mthree

The registry is not a single file. Instead, it is a set of files referred to as *hives*. Each hive has a specific purpose.

Registry Hives	Supporting Files
HKEY_LOCAL_MACHINE\Software	Software, Software.log, and Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, and System.sav
HKEY_LOCAL_MACHINE\SAM	Sm, Sam.log, and Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, and Security.sav
HKEY_USERS\DEFAULT	Default, Default.log, and Default.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, and Ntuser.dat.log

Windows Registry

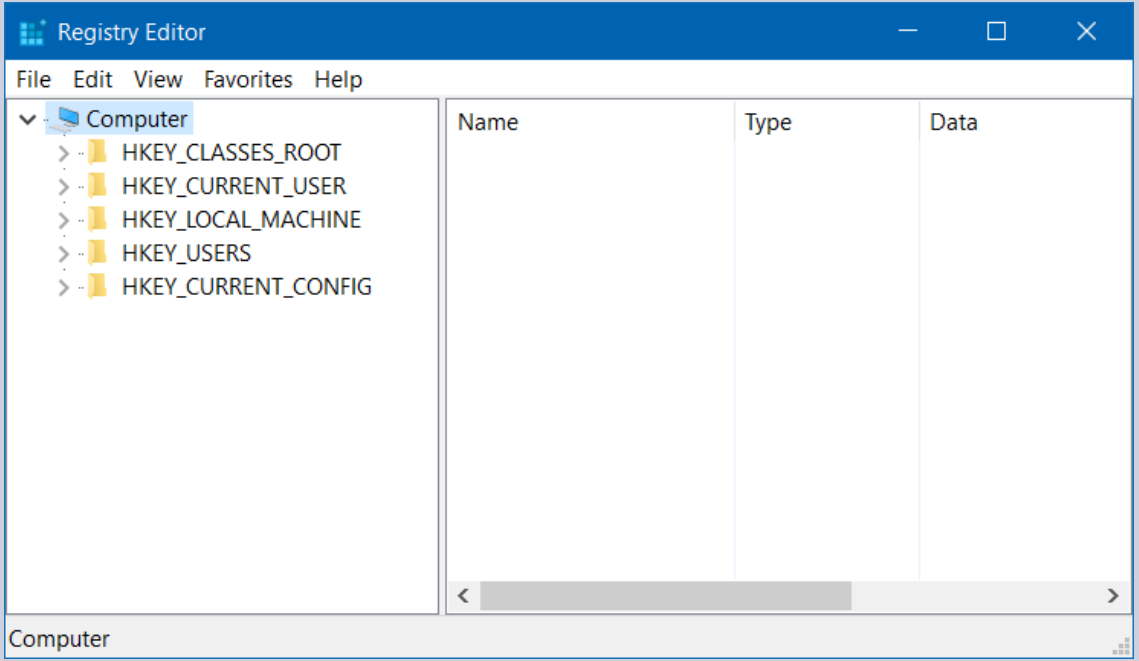
Registry hives are located in Windows\System32\Config folder.



Registry Editor

Regedit.exe : Enables manipulation of the registry database

Registry Editor enables users to manually edit the Registry to make necessary changes to the operating system.



Users

A user account is a name bound to a security id (SID)

Computers do NOT care about the name – they care about SID

Every user has a Unique Identifier (Unique ID) and Security Identifier (SID)

There cannot be duplicate usernames within a system (Local or Domain)

Local User Accounts :

Local accounts are stored and managed on the computer or system.

Network (Domain) User Accounts:

Network accounts are stored and managed on a centralized system, in a directory or database

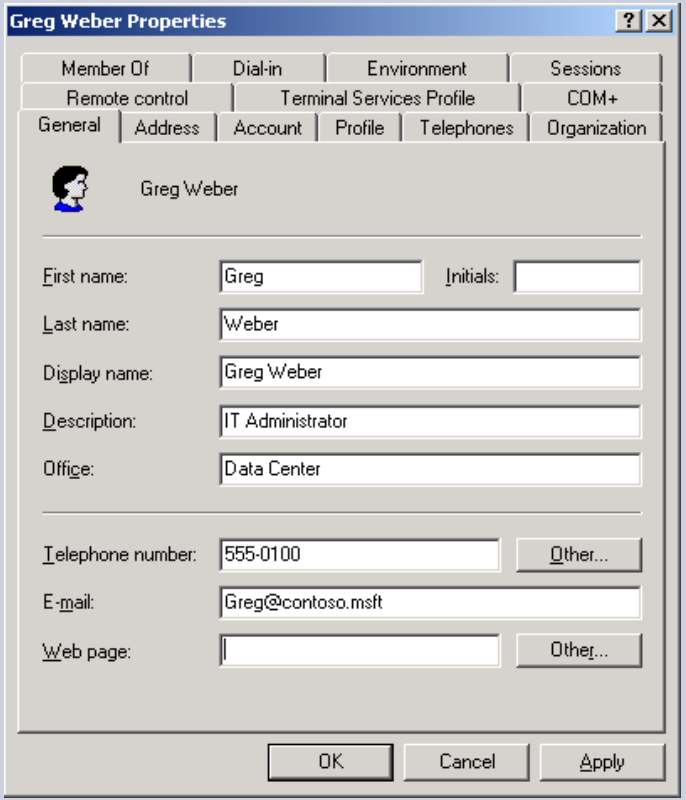
Names Associated with Domain User Accounts

Name	Comments
User Logon Name	Tadams
Pre-Windows 2000 logon name	contoso\Tadams
User principal logon name	contoso\Tadams
LDAP distinguished name	CN=terry adams,ou=sales,dc=contoso,dc=msft
LDAP relative distinguished name	CN=terry adams

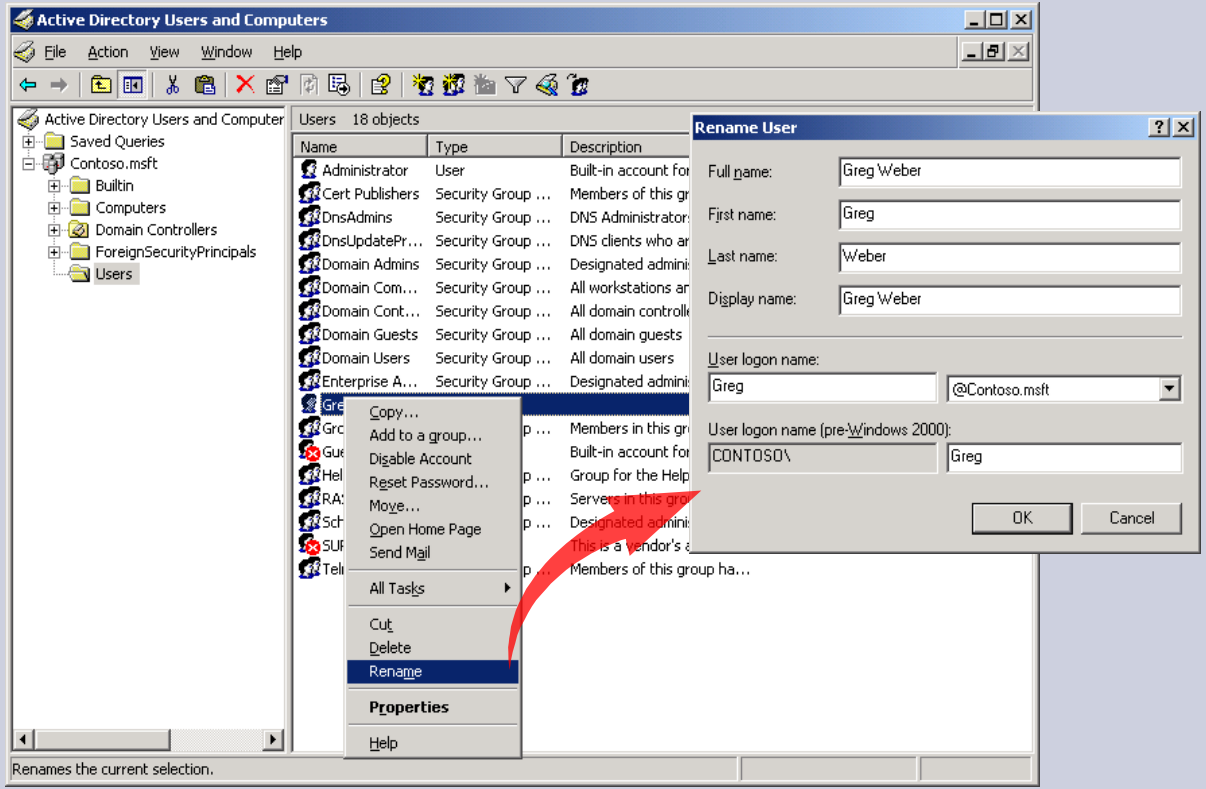
Properties Associated with User Accounts

Here is a typical set of values associated with a user

This is from the properties dialogue box for the user



Properties Associated with User Accounts



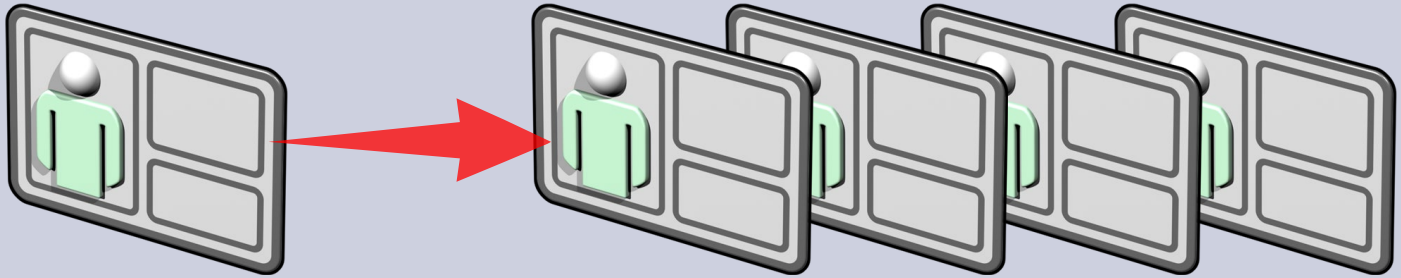
Renaming the user does not change the SID

User Account Template

mthree

Most admin systems use a template user account with properties meeting common user requirements.

A template makes creating user accounts with standardized configurations more efficient.



What Properties are in a Template

Tab	Properties Copied
Address	All properties except street name
Account	All properties except logon name
Profile	All properties except profile path and home folder reflect new user's logon
Organization	All properties except title
Member Of	All properties

User Groups

Groups simplify administration by enabling you to assign permissions for resources

Groups are characterized by scope and type – and should be named appropriately

Group Type: Security

Used to assign user rights and permissions

Can be used as an email distribution list

Naming conventions:
- Incorporate the scope in the group name
- Should reflect the group ownership
- Use a descriptor to identify the assigned permissions

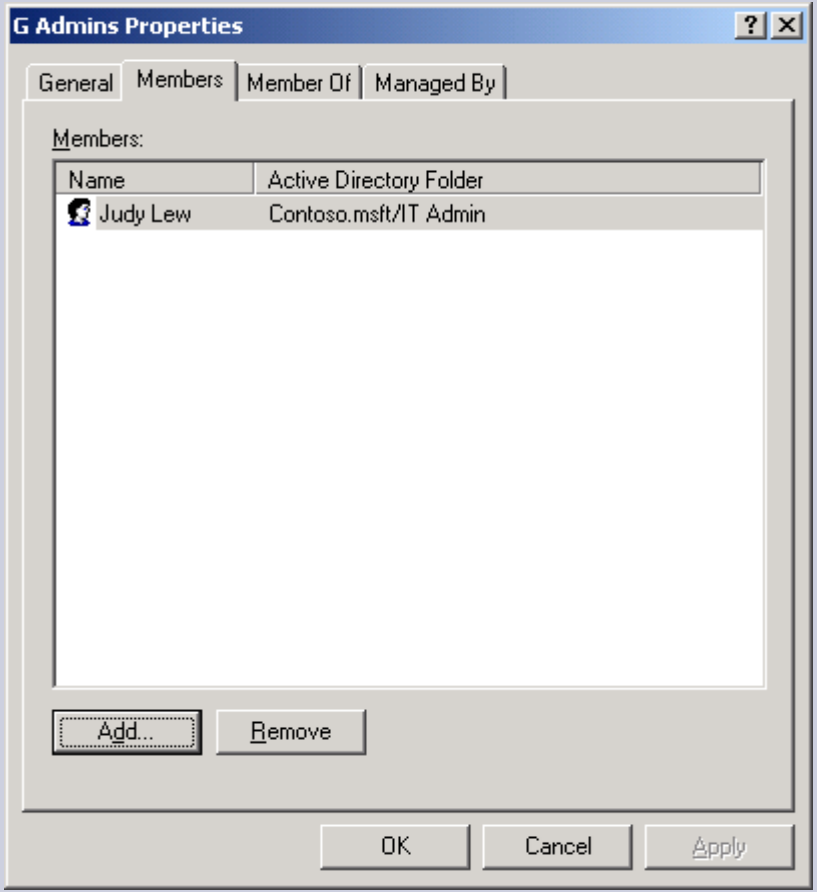
Group Type: Distribution

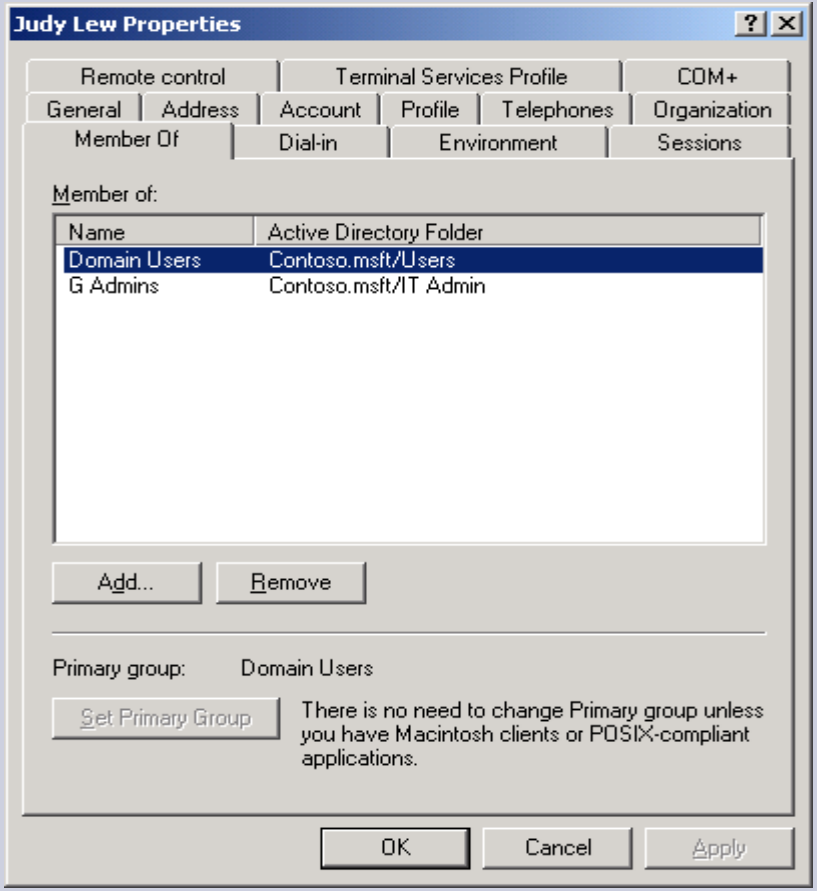
Can be used only with email distributions

Cannot be used to assign permissions

Naming conventions:
- Use short alias names
- Do not include a user's alias name in the display name
- Allow a max of five co-owners for a single distribution group

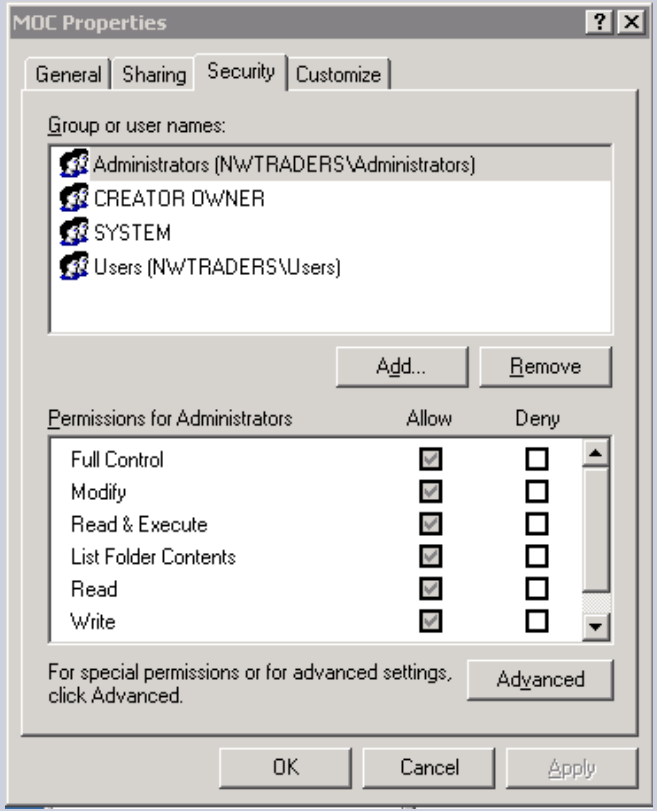
Adding or Removing members from a group



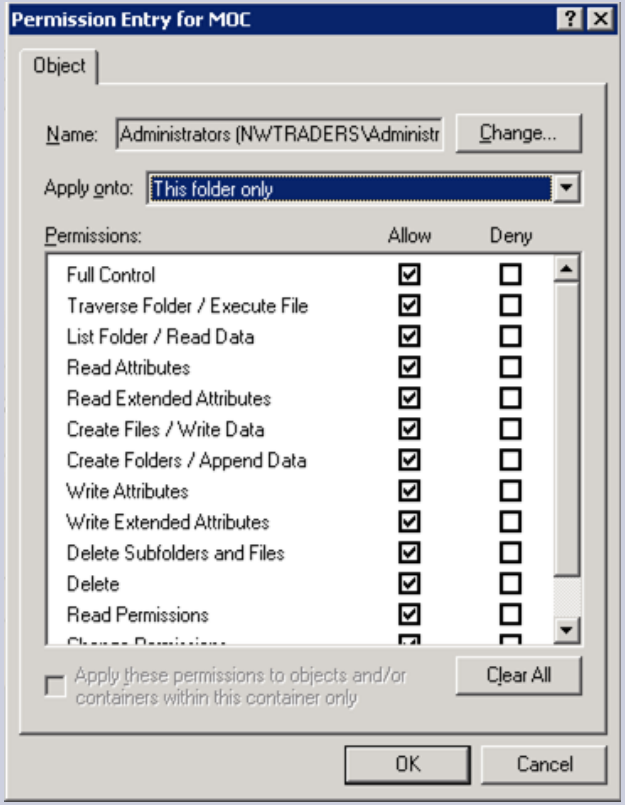


File and Folder Permissions

Standard Permissions



Special Permissions



Permissions and User/Security Mappings

mthree

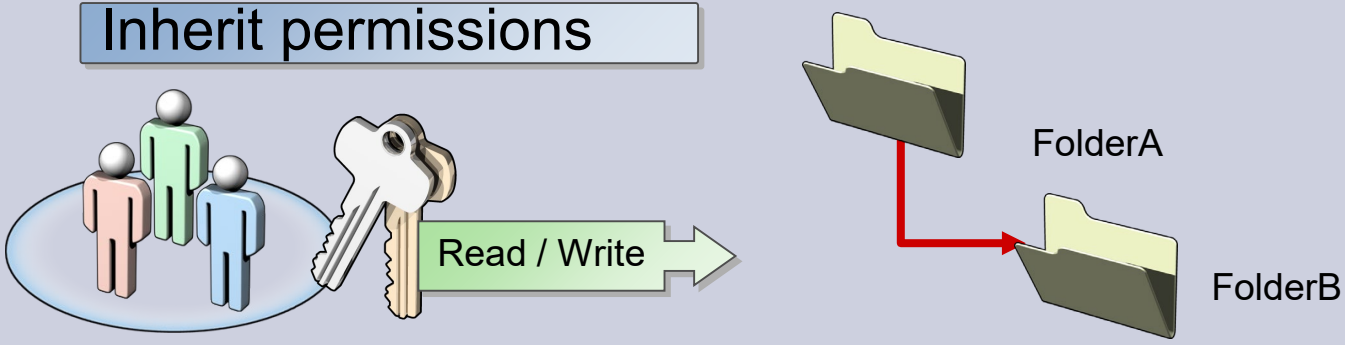
For NTFS – permissions are cumulative; file permissions overwrite folder; deny overrides everything and the creator is automatically the owner.

Users	Security Mapping
Administrator	The sole owner of all the objects within the system / domain
Single User Name (User)	A user with predefined file/folder & system access
Single Group Name (Group)	A group with predefined file/folder & system access
Authenticated Users	Users already authenticated to use a system (via password or other token)
Other System Users	Pre-defined system users
Everyone	All defined users along with the rest of the world

Security Inheritance

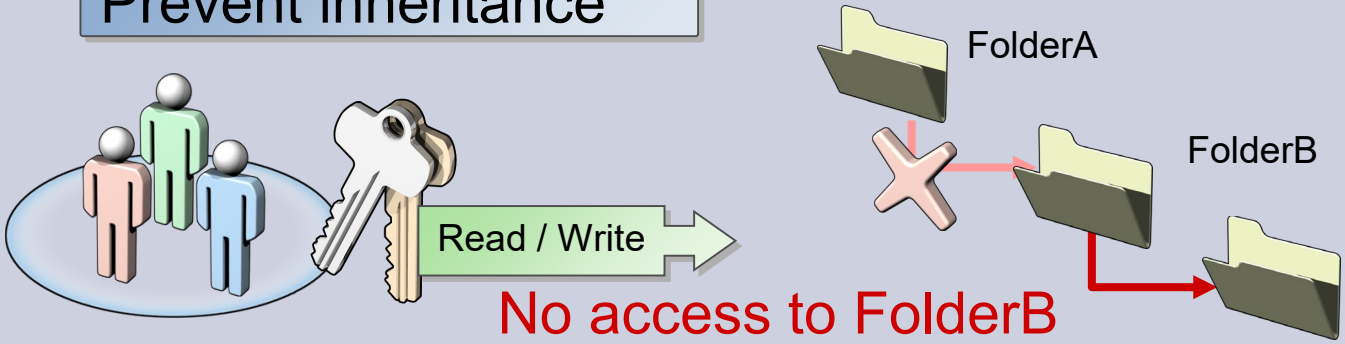
mthree

Inherit permissions



Access to FolderB

Prevent inheritance



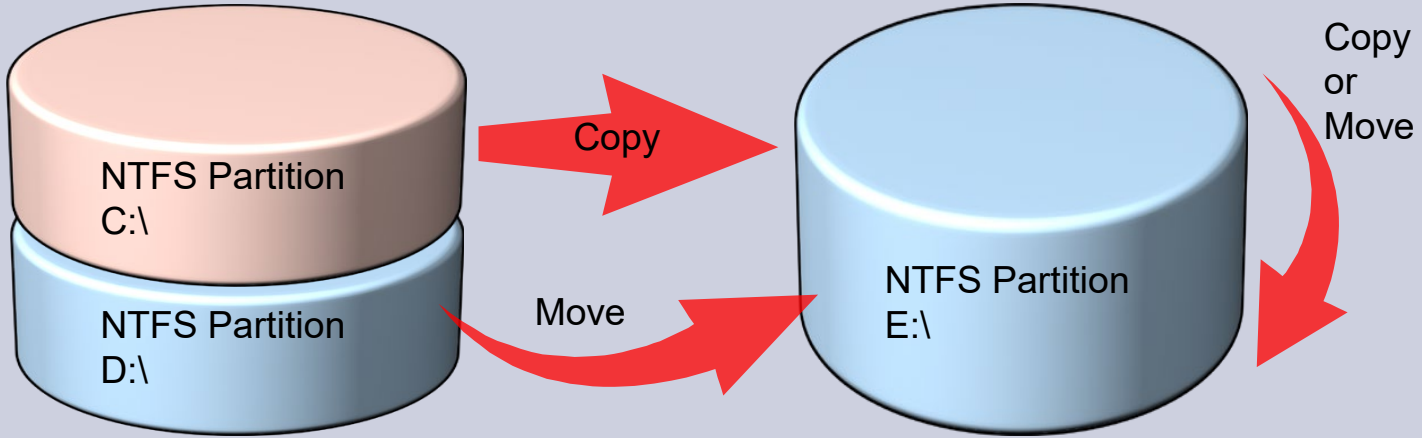
No access to FolderB

Copy vs Moving Files

When you copy files and folders, they inherit the permissions of the destination folder

When you move files and folders within the same partition, they retain their permissions

When you move files and folders to a different partition, they inherit the permissions of the destination folder



You can only share folders and default permissions will be everyone on read

Copy or moving a shared folder will stop it being shared

Shared Folders

mthree

Shared folders should use authenticated groups and only share with the appropriate level of permission.

If shared in larger environments, always use groups to grant access rather than individual users

Permission	Description
Read (Default, applied to the everyone group)	• Allows you to view data in files and attributes • Allows you to view file names and subfolder names • Allows you to run program files
Change (includes all read permissions)	• Allows you to view data in files and attributes • Allows you to view file names and subfolder names • Allows you to run program files
Full control (contains all read and change permissions)	• Allows you to change NTFS file and folder permissions

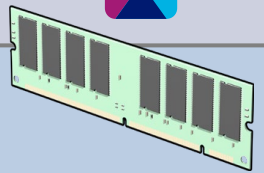
Windows Command Line

Some basic Windows CLI commands

Command	Description
dir	List the directory (folder) system.
cd pathname	Change directory (folder) in the file system.
cd \	Move to the root folder of the file system.
cd ..	Move one level up (one folder) in the file system.
copy	Copy a file to another folder.
move	Move a file to another folder.
type filename	Type a file.
mkdir or md	Creates a new directory (folder).
rmdir or rd	Removes a directory (folder).
cls	Clears the CLI window.
exit	Closes the CLI window.
help command	Shows the manual for a given command.

Monitoring Performance - Memory

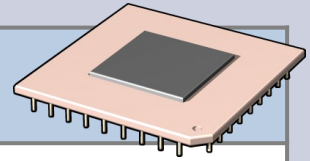
mthree



Memory counter	Acceptable average range	Desired value	Action
Pages/sec	Below 5	Low	Find the process that is causing paging Add RAM
Available Bytes	Minimum of 5% (Desktop) / 50% (Server) of total memory	High	Find the process that is using RAM Add RAM
Committed Bytes	Less than physical RAM	Low	Find the process that is using RAM Add RAM
Pool Nonpaged Bytes	Remain steady, no increase	Not applicable	Check for memory leak in application

Monitoring Performance - CPU

mthree



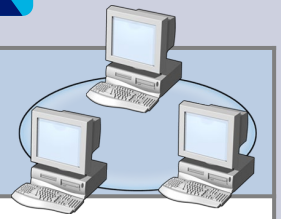
Processor counter	Acceptable average range	Desired value	Action
% Processor Time	Less than 85%/50%	Low	Find process using excessive processor time Upgrade or add another processor
System: Processor Queue Length	Less than 2	Low	Upgrade or add additional processor
Server Work Queues: Queue Length	Less than four	Low	Find process using excessive processor time Upgrade or add another processor
Interrupts/sec	Depends on processor	Low	Find controller card generating interrupts

Monitoring Performance - Disks

mthree

Physical disk counter	Acceptable average range	Desired value	Action
% Disk Time	Under 90%	Low	Monitor to see if paging is occurring Upgrade disk subsystem
Current Disk Queue Length	0–3	Low	Upgrade disk subsystem
Avg. Disk Bytes/Transfer	Baseline or higher	High	Upgrade disk subsystem
Disk Bytes/sec	Baseline or higher	High	Upgrade disk subsystem

Monitoring Performance - Networks



Network interface counter	Acceptable average range	Desire high or low value	Action
Network Utilization (in Task Manager)	Generally lower than 30%	Low	Upgrade network adapter or physical network
Network Interface: Bytes Sent/sec	Baseline or higher	High	Upgrade network adapter or physical network
Network Interface: Bytes Total/sec	Baseline or higher	High	Perform further analysis to determine cause of problem Upgrade or add another adapter.
Server: Bytes Received/Sec	Less than 50% of the capacity of the bandwidth of the network card	NA	Upgrade network adapter or physical network

Performance – General Counters

Subsystem	Counter	Threshold
Memory	• Monitor page faults • Monitor available RAM • Monitor committed bytes	• Over 5 per second • 4 MB or less of RAM • More than physical RAM
CPU	• % Processor time, % Privileged Time, % User Time • System: Processor Queue Length • Server Work Queues: Queue Length	• Above 85% • Above 2 • Above 2
Disk	• % Disk Time • Current Disk Queue Length	• If more than 90%, check for excessive paging • Greater than 3
Network	• Server: Bytes Total/sec, Network Interface: Bytes Total/sec	• Higher than the baseline number

Windows Power Management

mthree

You have the option to control the power management of your server (and indeed your own computer). In a production environment the systems admin team will likely be responsible for this.

The power management option can be found in:

```
Control panel > power options > change plan settings > change
advanced power settings >
```

- Noisy
- Slow
- Hot
- Sleep

Browser Maintenance

Being able to control your browser settings is also important.

Chrome

- Settings under Privacy and Security allow you to clear cached browsing data and cookies

Microsoft Edge

- Settings under Privacy & Security allow you to clear browsing data and choose what to clear

Internet Explorer

- You can delete your browsing history through Internet options under the general tab

Always be aware of what you are deleting before you do it.

Single Sign On (SSO)

Most big companies implement a single sign on (SSO) system, which allows users to log onto multiple independent systems with the same username and password.

This usually works in partnership with LDAP (Lightweight Directory Access Protocol)

Benefits:

- Mitigate risk on 3rd party sites
- Reduce password fatigue and time spent re-entering passwords
- Reduce IT costs for helpdesk calls on password issues

Concerns:

- As single sign on allows access to everything, if misused it is a big security problem
- If there is an issue impacting SSO services – everything gets locked out (effectively a denial of service)

Using Windows CLI

mthree

You can use the command prompt in Windows to do additional things.

Command	Explanation
echo %DATE% %TIME% %COMPUTERNAME% %PATH%	Print out environment variables
dir|sort	dir lists your directories; The sort option sorts the results
dir|clip	The clip option copies the result to the clipboard
dir|findstr es	findstr allows you to find a string in the output
cd	This will tell you the current directory
dir /?	This lists all the options you can use with dir
copy	Copy a directory or file
del	Delete recursively
type	Read content of text files
rd	Remove directory
ren	Equivalent to a move command

Using Windows CLI (continued)

mthree

Command	Explanation
ipconfig	Displays all current TCP/IP network configuration and domain name system (DNS) settings
netstat	Displays network connections for TCP, routing tables and a number of network interface and protocol statistics
ping <address>	Allows you to test the network connectivity to an address
notepad	This will start the app notepad

Batch files (.BAT)

mthree

Batch files are scripts – a series of commands to be executed by the command line interpreter (and stored in a plain text file).

It can have extensions: .bat, .cmd, .btm

.bat	This was the first filename extension used by Microsoft Runs with all versions of Windows and DOS
.cmd	Used for batch files in Windows NT and IBMs OS/2
.btm	Extension used by 4DOS, 4OS2, 4NT and Take command Usually faster as the script is loaded entirely before execution rather than line by line

An example hello world batch script:

```
@echo OFF
ECHO Hello World!
PAUSE
```

Task Manager

The Windows Task Manager provides information about computer performance and running software. You also get information on CPU load, commit charge, I/O details, logged in users and windows services.

It can also be used to set process priorities, processor affinity, start and stop services and terminate processes.

You can open Task Manager using Ctrl+Al+Del or by right-clicking the Start button or task bar.

View	Comments
Summary Mode	This simply shows the processes running – the more details hyperlink will open the below views
Processes and Details	Showing all processes on the system – the delete key can be used to terminate processes CPU and memory consumption is also shown
Performance	Overall statistics on the systems performance
App History	Shows resource usage information about applications
Startup	Manages the software that start with the windows shell
Users	Will show all the current users logged on to the system
Details	Further details on processes running
Services	Shows your services view

Disk Management

Managing disk space is extremely important.

Windows allows you to look at your disk management through the storage application.

Tools available:

- Disk cleanup
- Compression of drives
- Content indexing
- Optimization

Device Manager

The device manager allows you to view and control hardware attached to the computer.

Here you can:

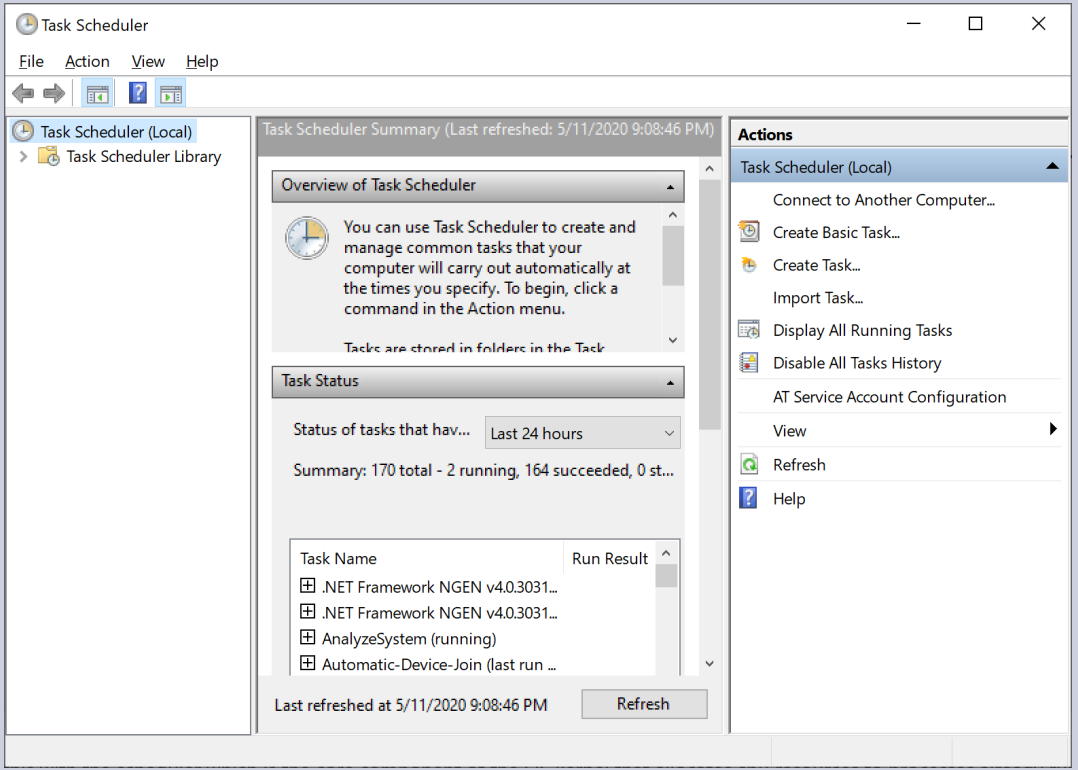
- Supply or update device drivers
- Enable or disable devices
- Tell Windows to ignore malfunctioning devices
- View other technical properties

Useful tool when troubleshooting issues with any of your devices.

Task Scheduler

The scheduler provides the ability to schedule the launch of programs and scripts at predefined times or after time intervals.

The view here shows you the wizard you can use to create tasks and view the tasks that are currently scheduled on the server



Subnet Masks, Gateways

- Every device has an IP Address(Static vs DHCP)
- Every IP address is on a network
- A network is an IP address range, constructed from the IP address and the subnet mask(2 notations):

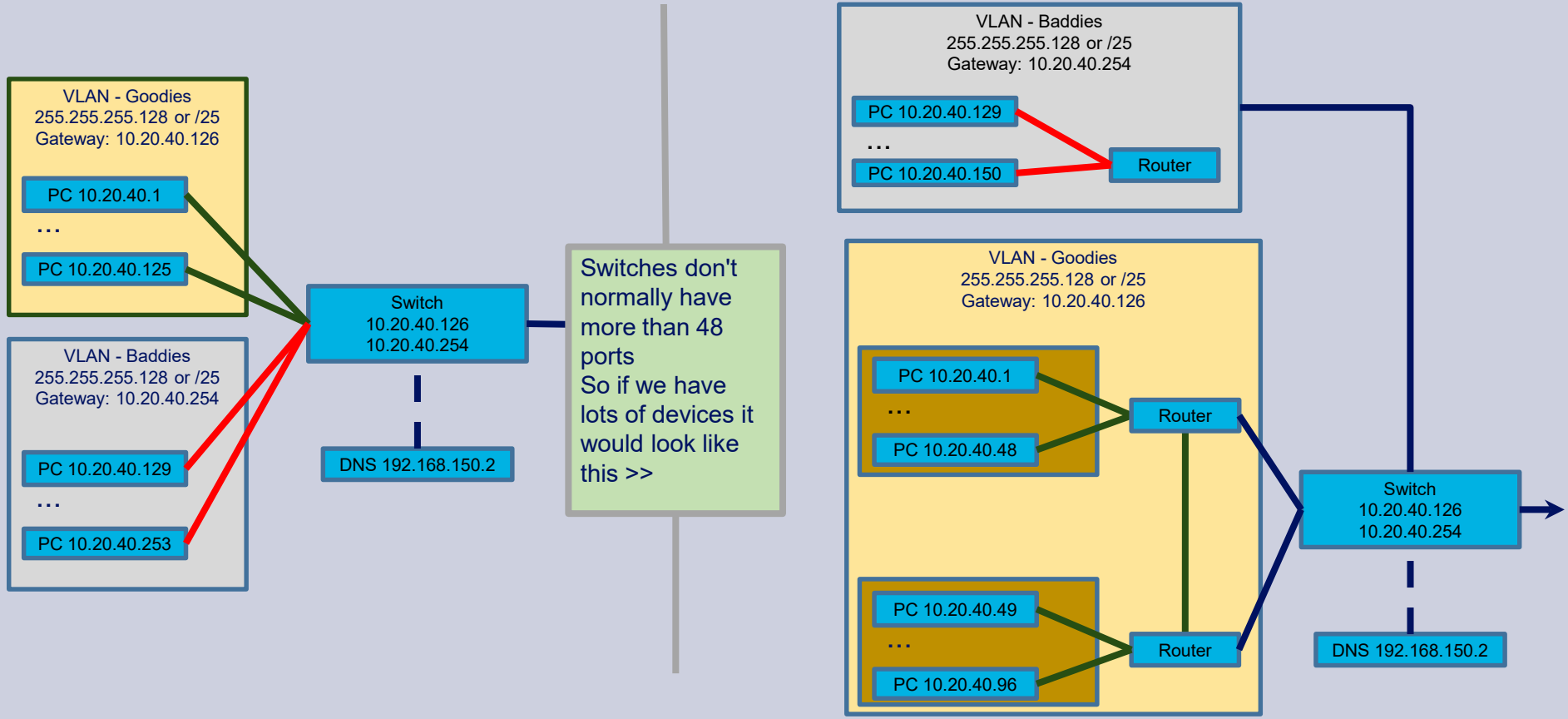
IP:10.20.40.53 SubnetMask:255.255.255.0
IP:10.20.40.53/24
→ Network Range:10.20.40.1 to 10.20.40.254 Training Network

IP:10.20.40.53 SubnetMask:255.255.255.128
IP:10.20.40.53/25
→ Network Range:10.20.40.1 to 10.20.40.126 Dev Network

IP:10.20.40.153 SubnetMask:255.255.255.128
IP:10.20.40.153/25
→ Network Range:10.20.40.129 to 10.20.40.254 UAT Network

- All devices on a network can talk to each other
- Any messages destined for outside the network need to be directed via the 'Default Gateway'
  - 10.20.40.53 can send messages directly to 10.20.40.52
  - 10.20.40.153 can send messages directly to 10.20.40.152
  - For 10.20.40.53 to send a message to 10.20.40.153 or 8.8.8.8 it will be directed at the 'Default Gateway'
  - Gateways must be on the same network. For /24 the gateway is 10.20.40.254. For /25 there would need to be two gateways
  - Networks can be virtual or physical. A single switch could host multiple virtual networks, or there may be multiple physical switches involved

VLANs, Gateways, Routers, Switches, DNS



Firewall

A firewall disables some network connections (filters network traffic) based on:

- Incoming/Outgoing
- Protocol (TCP/UDP, etc.)
- IP Address
- Port
- Intelligent rules that detect suspicious activity
- MAC
- User

Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Types:

- Local (Host-Based) – all computers have one, e.g., Windows Defender firewall
- Remote (Network) – all networks have at least one