Question

Students are required to choose an Operating system (OS) and study the OS in term of:

- History and development
- File management
- Process management
- Memory management
- Device management
- Network management
- Security

Question 2

From the knowledge gained, the student are requires to draft a new version of OS that include a new name for the OS , LOGO, design principles and so on and prepare for the Report and presentation

1. Deliverable:

   i. A write up/ report (approximately 15-25 pages of the finding.
   ii.Report submission is on week 11th (tutorial session)
2. Presentation
   i.A 15 minutes presentation of the assignment
   ii.Presentation Is on week 13th and week 14th (tutorial session)

1.0 Introduction

The operating system I choose for the assignments is Windows Vista. In this assignment will brief about term of Windows Vista, Such as history and development, file management, process management, memory management, device management, network management and security of the Windows Vista.

Windows Vista introduces the next generation operating system technology and software development platform that will be used by application developers and enterprises worldwide. As part of enhancing the security and user experience of Windows Vista, many new features and been introduced and existing features have been improved.

Windows Vista compatibility is high, and Microsoft is continuously striving to achieve the best possible compatibility solutions for existing applications for Windows Vista. There are several new features that will enable developers to troubleshoot and workaround applications that do not function properly under Windows Vista, such as the Compatibility tab. Users can right-click the shortcut or the EXE.

Additionally, the user can choose Run this program as administrator if the application needs administrator privileges and the user possesses those rights. For more information, see the "User Account Control" section in this document.

2.0 History and development of Windows Vista

The histories of Windows Vista, Vista are Whistler, Longhorn and Blackcomb which are actually real names of places in British Columbia. Both Whistler and Blackcomb are ski resorts while Longhorn is the little bar in between the two ski sites. In Microsoft, the names became code names. Whistler was actually Windows XP, Longhorn was Windows Vista and Blackcomb is yet an unknown higher operating system version. Windows Vista is intended to be an interim system.

Even before Windows XP was released, Microsoft made it known that since May of 2001, they were working on the development of a new operating system. The general excitement became apparent and since the second half of the year 2002, build leaks, both fake and real, crept into the internet. As early as June 2002, there was already some talk that Vista would have improved security features and a more modern look

By the last few months of 2003, the development of Windows Vista suffered a setback when Microsoft realized that they were not making good progress. It seemed as if there was no apparent focus on what the final product should be. The path of Longhorn then had to be properly mapped with the goal of making Vista better.

It somehow became apparent in the middle of 2003 that Longhorn would never make it for an early release. The release was then pushed to the early part of 2005. Some saw this as a sign of Microsoft's commitment to the development of the new system.

The style of Aero finally came into focus in an 1 April 2005 build. Two months after, the name Windows Vista was unveiled. For many, the system name brought the hope of achieving greater ease and clarity.

On 27 July 2005, Windows Vista Beta 1 was released. Beta testers had their first taste of a new user interface, virtual folders, parental controls and networking stacks. Windows Vista Beta 2 followed on 23 May 2006 which was made downloadable for users in the following month. On November 8, 2006, the final build had been made. The final product was finally made available on the market on 30 January 2007.

3.0 File management

A file manager and a file browser is a computer program that provides a user interface to work with file systems. It also referred to as simply a file system. The system that an operating system or program uses to organize and keep track of files.

The most common operations used are create, open, edit, view, print, play, rename, move, copy, delete, attributes, properties, search/find, and permissions. Files are typically displayed in a hierarchy. Some file managers contain features inspired by web browsers, including forward and back navigational buttons.

3.1 Window vista file management

A windows Vista computer has several default folders that can use to display and organize the content of the computer, including files, folder, programs, and drives. Each user is assigned a personal folder, as shown below. (Figure 3.1.1)

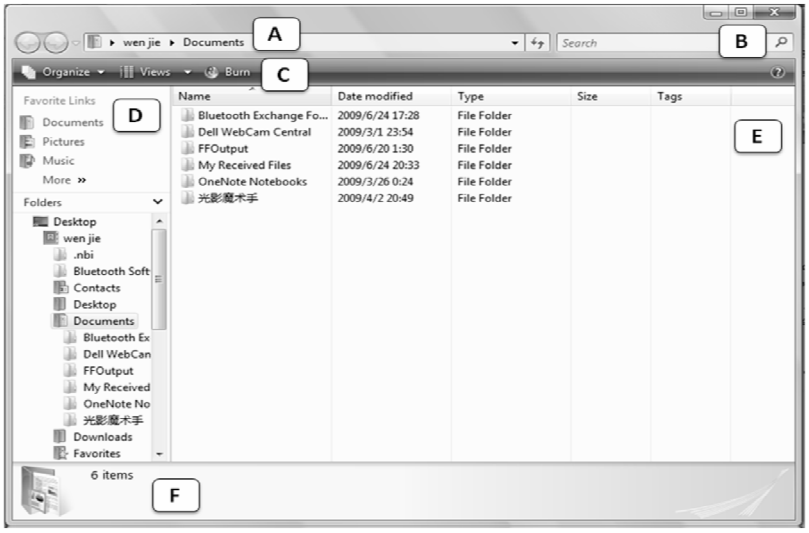


Figure 3.1.1

A. Address bar -Show current location in computer's folder hierarchy.

B. Search box -Provides a way to search for content. Enter the search words and click the search button.

C. Command bar -Contains buttons and menus for working with files and folders. The buttons change depending on current selection.

D. Navigation pane -Contains favourites links and the Folder list. Use the Navigation pane to move through the folder hierarchy.

E. List pane -Display the contents of the selected folder.

F. Detail pane -Display detailed information for the selected file, folder or program.

3.2 Windows Vista File System

Windows Vista interface comes in two flavours such as basic user interface or the Aero, Microsoft's "best-designed, highest-performing desktop experience". In order to use the Aero interface, the user needs a PC with a compatible graphics adapter and also the Premium or Business edition of Vista software.

The file system support Microsoft windows for the first personal computers used a file system called FAT16, which was introduced way back in 1981 with MS-DOS. It handled files on a floppy drive and could only handle short file names. This was upgraded to FAT32 which was introduced in Windows95. Then came NTFS, the "New Technology File System" which was a super hit and stayed the course for almost a decade in WINNT, WIN 2000, XP as well as other versions of the Operating system.

NTFS has been outsmarted by a newer file system called the Transactional File system which has been introduced in Windows Vista. This new file system uses a database type of approach to everything that takes place on the computer.

3.3 New Technology File System (NTFS) on windows vista

Windows Vista introduced Transactional NTFS, NTFS symbolic links, partition shrinking and self-healing functionality though these features owe more to additional functionality of the operating system than the file system itself.

Transactional NTFS (TxF) they should have called it TNT, but let us remember, those are computer geeks that play with this part of the operating system, everything to them sounds like Fx because they want to become socially acceptable like pharmacists who have the Rx sound, The name probably comes from the database world, and what it means also comes from there, This means that if the transaction was not complete, user can roll back and get back the old file.

Transactional NTFS logs every call to every file, and maintains a record of all changed files, Now when something goes wrong with that file, vista can restore a previous version of the file back to the minute the shadow copy of the system was created (Windows takes that shadow copy when boot up the computer)

So, up to a limited number of reboots, user can have versions of every file, and then user can restore the needed one.

Now to restore a file to a previous version, user take the properties of that file where user will find a tab called Previous Versions, in the same way this can be done to a file, or even a drive (from their properties)

3.4 The new Vista file system works on the following (ACID) transaction principles:

Atomicity – In a transaction involving two or more discrete pieces of information, either all of the pieces are committed or none are.

Consistency – A transaction either creates a new and valid state of data, or if any failure occurs, returns all data to its state before the transaction started.

Isolation – A transaction in process and not yet committed must remain isolated from any other transaction.

Durability – Committed data is saved by the system such that, even in the event of a failure and system restart, the data is available in its correct state.

4.0 Process management

A process is a program in execution. It is a unit of work within the system. Program is a passive entity, process is an active entity. Process management is a process that contains its own independent virtual address space with both code and data, protected from other processes.

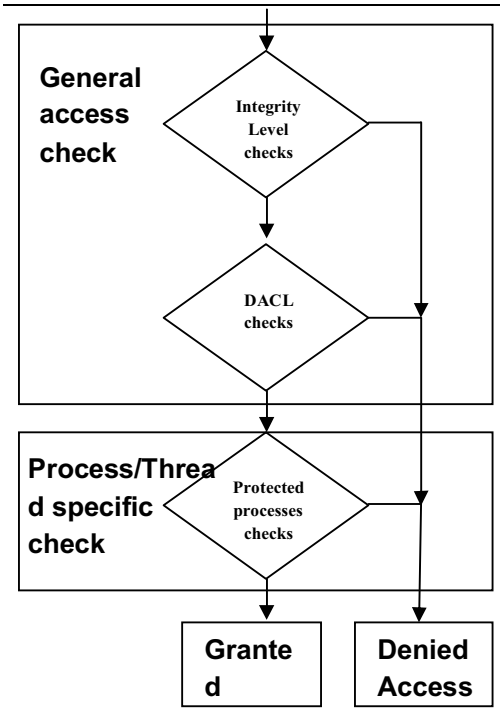
Each process, in turn, contains one or more independently executing threads. A thread running within a process can create new threads, create new independent processes, and manage communication and synchronization between the objects.

Through the creating and managing processes, applications can have multiple, performing computations, concurrent tasks processing files, or communicating with other networked systems. It is even possible to exploit multiple processors to speed processing.

4.1 Protected processes in Windows Vista

Windows Vista operating system introduces a new type of process, called a protected process, to enhance support for digital rights management functionality in Windows Vista. Protected processes exist alongside normal processes in Windows Vista.

The access to the processes is restricted regardless of actual access control lists and assigned integrity levels. Only limited subset of operations is allowed, such as termination, suspending, resuming, retrieving process image name and synchronization. Whenever a process is opened system performs following access checks. (Figure 4.1.1)



1. Access control checks according to integrity levels
2. Standard access control for DACL
3. Protected process checks

(Figure 4.1.1)

4.2 Processes and protected processes

The primary difference between a typical process and a protected process is the level of access that other processes in the system can obtain to protected processes. In versions of Microsoft Windows earlier than Windows Vista, the process model allows a parent process to acquire a handle to and manipulate the state of any child process that it creates. Likewise, processes that users created with sufficient privileges can access and manipulate the state of all processes on the system. This behaviour remains true for typical processes. However, the level of access to protected processes and threads within those processes is significantly more constrained.

Any application can attempt to create a protected process. However, due to the restrictions of running inside a protected process, the operating system requires that these processes be specially signed. In Windows Vista, Protected Media Path (PMP) uses the protected process infrastructure to provide increased protection for high-value media content. Developers can leverage protected processes by using the Media Foundation API

5.0 Memory management

Memory management is the activity of managing computer memory. In the context of programming languages it means providing means of storing individual objects in a memory space provided by the underlying system. Usually, a memory management system allocates small objects in one or more big contiguous memory spaces while also holding its book-keeping data structures there.

Memory management can be manual, where the programmer explicitly calls allocation or deal location routines or automatic where the system automatically determines which objects are no longer accessible by the program and safely removes them.

5.1 Memory management in Microsoft Window

Memory management in Microsoft Windows operating systems has evolved into a rich and sophisticated architecture, capable of scaling from the tiny embedded platforms (where Windows executes from ROM) all the way up to the multi-terabyte NUMA configurations, taking full advantage of all capabilities of existing and future hardware designs.

With each release of Windows, memory management supports many new features and capabilities. Advances in algorithms and techniques yield a rich and sophisticated code base, which is maintained as a single code base for all platforms and SKUs.

Memory management improvements in Windows Vista focused on areas such as dynamic system address space, enhanced NUMA and large system or page support, advanced video model support, I/O and section access, and robustness and diagnosis ability

5.2 NUMA (Non uniform memory access)

NUMA is a computer memory design used in multiprocessor where the memory access time depends on the memory location relative to a processor. Under NUMA, a processor can access its own local memory faster than non-local memory that is memory local to another processor or memory shared between processors.

NUMA provides separate memory for each processor, avoiding the performance hit when several processor attempt to address the same memory. For the problem involving spread data (common for servers and similar application) NUMA can improve the performance over a single shared memory by a factor of roughly the number of processors (or separate memory bank).

For this to work NUMA system include additional hardware or software to move data between banks. NUMA is not entirely new to windows but vista is designed to handle and support it better.

5.3 Super Fetch

One of the key enhancements to the Windows Vista memory management system is a new feature called Super Fetch. It is a new technology with Vista, SuperFetch is an intelligent memory management mechanism that attempts to keep most-often used memory pages in memory. However, it goes beyond a simple last-used algorithm. SuperFetch understands which applications are most often used (and even when certain applications are accessed), and preloads these applications into memory to make their invocation faster.

6.0 Device management

Managing the inputs and outputs of various devices / peripherals ,it controls peripheral devices by sending those commands in their own proprietary language .Device management also was a critical functions of Operating Systems. With the help of device drivers, the OS controls flow of information with the necessary allocation of system resources to ensure correct input and output.

The software routine that knows how to deal with each device is called a "driver," and the operating system requires drivers for the peripherals attached to the computer. When a new peripheral is added, that device's driver is installed into the operating system.

6.1 Device management of Windows Vista

Device Management fully supports Windows Vista in native mode, providing complete systems management functionality for this platform and a seamless user experience. Window vista using Device drive Signing and staging, that can increase the security of the computers by allowing users to install only those device drivers that user approve.

Windows Vista includes several features that allow an administrator to make device driver installation easier for users. User have the ability to stage driver packages in a protected area of a user's computer called the driver store. A standard user, without any special privileges or permissions, can install a driver package that is in the driver store. User can also configure client computers to automatically search an administrator-specified list of folders (and their subfolders) when a new device is attached to the computer. These folders can be local to the computer or hosted on a network share.

When a device driver is accessible in this manner, Windows will not need to prompt the user to insert media. These features improve the user experience and reduce help desk support costs by allowing standard users to install approved driver packages without requiring additional permissions or the assistance of an administrator. These features also increase the security of the computers by ensuring that standard users can only install those driver packages which user authorize and trust.

6.2 Advantage of Device drivers signing and staging in Windows Vista

- **Improved security**

  Before Windows Vista standard users could not install device drivers without assistance from an administrator. Users often logged on with user accounts that were members of the Administrator's group. The rights associated with Administrator group membership allows a user to carry out required tasks, but they also allow the user to carry out actions that can compromise security or configure the computer so that it does not run correctly.

- **Better user experience**

  A driver package that is staged in the driver store works automatically when the user plugs in the device. Alternatively, driver packages placed on a shared network folder can be discovered whenever the operating system detects a new hardware device. In both cases, the user is not prompted before installation.

  With Windows Vista user can allow standard users to install approved device drivers without compromising computer security or requiring help desk assistance.

- **Reduced support costs-**

  Users can only install devices that organization has tested and is prepared to support. Therefore maintain the security of the computer while simultaneously reducing the demands on helpdesk.

7.0 Network management

Network management refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance and reliability.

Security : Ensuring that the network is protected from unauthorized users.

Performance : Eliminating bottlenecks in the network.

Reliability : Making sure the network is available to users and responding to hardware and software malfunctions.

7.1 Function of the network management

The network management functions provide the ability to manage user accounts and network resources. Many of the capabilities provided by the network management functions are not provided by other networking functions.

However, if the capabilities are provided by another set of functions, the documentation for the network management functions will refer to other functions that can use for the same task.

7.2 Network management on Windows Vista

There are many types of threats, when users accessing wireless networks that are not as they seem, unhealthy guest PCs connecting to a corporate network, and unmanaged resources attempting to access resources they shouldn't have access to. It's enough to keep a network administrator busy all day and worrying all night. Windows Vista can help with all of these scenarios, with enhanced network security features that are comprehensive yet easy to configure.

The networking features in Windows Vista have been designed to support high levels of manageability to help reduce the cost of deploying wireless networks and network security policies, as well as to provide quality of service for applications and users. Windows Vista uses Group Policy or command-line scripting via the Network Shell (NETSH) extensively to manage network features, so user don't need to learn or deploy a new management tool, and user can take advantage of existing investment in Active Directory and the Organizational Unit (OU) structure that have already created.

Deployment and management of network security rules are combining firewall and IPSec policies. It made easier within a single wizard-driven Microsoft Management Console (MMC) snap-in called Windows Firewall with Advanced Security or command-line scripting via NETSH.

The new snap-in provides a simple way to deploy inbound or outbound filtering and connection security rules that limit access by specific users, computers, or applications while providing a granular level of administrative control. IPSec can request or require authentication by user, computer, or health certificate (integrating with Network Access Protection) to provide a scenario-based security policy. The snap-in makes the creation of server or domain isolation rules easy and, since it is Group Policy-based.

7.3 Network securing of the Windows Vista

There are many types of threats, when users accessing wireless networks that are not as they seem, unhealthy guest PCs connecting to a corporate network, and unmanaged resources attempting to access resources they shouldn't have access to. It's enough to keep a network administrator busy all day and worrying all night. Windows Vista can help with all of these scenarios, with enhanced network security features that are comprehensive yet easy to configure.

The native Wi-Fi architecture in Windows Vista has wide support for the latest security protocols, including Wi-Fi Protected Access (WPA) 2 Enterprise and Personal, PEAP-TLS, and PEAP-MS-CHAP v2 (Protected Extensible Authentication Protocol with Transport Layer Security and with Microsoft Challenge Handshake Authentication Protocol).

This broad support ensures interoperability between Windows Vista and almost any wireless infrastructure. The capabilities of the wireless network card are examined by Windows Vista and the most secure protocol is chosen by default when connecting to or creating wireless networks. Using the EAP-HOST framework, Windows Vista is able to support custom authentication mechanisms defined by a hardware vendor or by an organization.

Windows Vista includes many improvements to the behaviour of the wireless client to mitigate common wireless attacks. The client will automatically connect only to networks the user has explicitly requested or identified as preferred networks, and will not automatically connect to ad hoc networks.

The client also provides a warning if the user is about to initiate a connection to an unsecured network. Additionally, the client will actively probe for fewer preferred networks and only if instructed to do so by the user, making it more difficult for attackers to identify what network the client is trying to connect to and create a rogue network with the same name.

7.4 Window Vista native wireless client supports a single sign-on (SSO)

The Windows Vista native wireless client supports a single sign-on (SSO) feature, which executes Layer 2 network authentication at the appropriate time given the network security configuration, while at the same time integrating with the user's Windows logon experience. Once a single sign-on profile is configured, network logon will precede the Windows logo. This feature enables scenarios such as Group Policy updates, logon scripts and wireless bootstraps, which require network connectivity prior to user logon.

Windows Firewall with Advanced Security brings a new level of network security to the Windows platform, providing support for both inbound and outbound filtering as well as Windows Service Hardening. If the firewall detects a Windows service behaving abnormally as defined by the Windows Service Hardening network rules, the firewall will block it. Windows Firewall with Advanced Security also supports Authenticated Bypass, which enables certain computers authenticated with IPsec to bypass firewall rules for such tasks as remote management.

8.0 Security

Security is an issue that very important to all computer user. Microsoft is making fundamental investments in technology to help make user more secure. Efforts include using a security development lifecycle to develop more secure software and providing technology innovation in the platform to provide layered defense, or defense-in-depth.

The Operating systems provide password protection to keep unauthorized users out of the system. Some operating systems also maintain activity logs and accounting of the user's time for billing purposes. They also provide backup and recovery routines for starting over in the event of a system failure.

Windows Vista includes many security features and improvements to protect client computers from the latest generation of threats, including worms, viruses, and other malicious software.

8.1 Security of the Windows Vista

Windows Vista stands as the most secure Windows operating system to date. Considerable effort was made to improve the security of the system in comparison to Window XP. In particular, Internet Explorer 7 offers greater personal information protection, less overall vulnerability and less susceptibility to infections and the so called defence-in-depth feature s like User account Control and Internet Explorer Protection Mode help to reduce the risk and severity of potential security breaches.

The security setting of Windows Vista also help individual users and organizations using the system to reduce the time they need to spend installing updates and reviewing the security setting of their systems and operating protocol.

When Window Vista was launched, Microsoft offered up a number of new security technologies integrated into the system. Specifically, they looked to address several issues that had affected previous windows operating system. In many respects, the improved security of the window system was a primary goal for the designers of the vista system.

8.2 The most notable development for the Windows Vista

- **User Account Control**

  User Account Control (UAC) is a Windows Vista feature which prevents unauthorized changes and helps keeping malware out of the system by a method called Mandatory Integrity Control (MIC). MIC prevents processes to write to objects with higher integrity levels unless authorized by a computer administrator. This Admin Approval Mode (AAM) starts when a program or Vista needs permission to continue, and when unidentified application wants access to the system. UAC implements the principle of the least privilege in that all users including administrators only have standard privileges unless an operation requires administrative permissions and thus starts AAM.

- **BitLocker Drive Encryption**

  BitLocker Drive Encryption encrypts volumes on local hard disk including the Vista system drive to protect system and data. User can work with the encrypted Vista normally, but if somebody alters the BIOS, changes startup files or when BitLocker Drive Encryption detects another anomaly which could pose a security risk Windows will not start until unlocked with the recovery password from user. BitLocker Drive Encryption is particularly useful if user laptop gets lost or stolen ,even if the hard disk is inserted in another computer all encrypted content remains secure. BitLocker Drive Encryption is restricted to Windows Vista Ultimate and Enterprise editions, which also fully support Encrypting File System (EFS) to encrypt individual files.

- **Windows Resource Protection**

  Windows Resource Protection (WRP) is a property of Windows Vista which protects executables, critical system files and folders as well as parts of the Registry from modifications unless invoked by the Trusted Installer, a Vista security entity which is more privileged than administrators and local system account. Thus, the successor of Windows File Protection does not even let administrators make changes to these objects by default; if required WRP lets user override the access control list entries of protected objects on an individual bases though.

- **Services Hardening**

  Until Windows Vista services often ran as LocalSystem with excessive privileges. Windows services in Vista are now configured to run with the least privilege to accomplish their purpose, so as to be less attractive targets for writers of malicious software. On top of that does Vista make use of service isolation by means of limiting access to a particular service's resources to those services whose Security IDs are present in the resource's access control entries, usually the particular service's SID only.

  Also, user applications and Windows services can no longer share the same session in Windows Vista: Session 0 is now exclusively used by Windows services with no interactive processes. Last but not least do Windows services have a firewall policy associated so that the Windows Vista firewall prevents or restricts network access of services which have no network functionality by design.

- **Windows Firewall with Advanced Security**

  The Windows Vista firewall basic configurations can again be made in Control Panel, but to view or configure the advanced security options user have to open a MMC snap-in, or type firewall in Start Search. User can set rules for incoming and outgoing connections in three profiles depending whether user use Vista at home, at workplace or in public places. In addition to that can user apply rules based on connection type, e.g. server-to-server or tunnel, and configure a variety of monitoring options. On top of that has the IPSec (Internet Protocol Security) protocol suite for IP-based encryption and authentication been integrated in the firewall. In short, the Windows Vista firewall with advanced security is a full-fledged host-based firewall.

- **Windows Defender Integration**

  Windows Defender, Microsoft's anti-spyware removal tool, has been integrated into Vista, too. Windows Defender does not replace anti-virus software but is effective against other unwanted and potentially unwanted software. The software protects system in both, real-time when accessing objects, as well as trough periodic scans of entire system. Windows Defender also includes Software Explorer, a tool to inspect and configure security-relevant properties of user's Vista computer including auto start programs for example.

- **Internet Explorer Protected Mode**

  Internet Explorer in Windows Vista by default runs in protected mode with an integrity level lower than that of a standard user. This permits user to browse with an additional layer of protection against drive-by downloads (applications that install without user intervention, just by visiting a web site) and alterations of system files and computer configuration through a vulnerability in Internet Explorer. Applications may write to virtual temporary files of low integrity, but access to normal-integrity objects is only possible utilizing an intermediary security process.

- **Network Access Protection**

  Network Access Protection (NAP) checks whether Vista-based computers connecting to a LAN or corporate network have the required security software, such as anti-virus software, installed and, equally important, if their security software is up to date. Computers not meeting the NAP requirements can be blocked, restricted or automatically updated. Thus, Network Access Protection particularly aims at preventing viruses and malware from entering the IT-infrastructure trough mobile or remote Windows Vista computers.

- **Anti-Phishing**

  Windows Mail, which replaces Outlook Express as default email client in Windows in Vista, has an integrated phishing filter which analyzes incoming mails for deceptive links and URLs known as bogus Web sites. Vista's Internet Explorer phishing filter goes beyond Windows Mail's method of comparing URLs to a locally stored blacklist, and permits user's browser to check the current Web address on the fly with Microsoft's online database of blacklisted sites. A method to report a fraudulent web address is also included in Vista's Internet Explorer of course.

- **Parental Controls**

  Windows Vista Parental Controls lets user restrict the web sites and user kids can visit based on Web address, content and age group-rating. With Windows Vista user will be also in a position to allow or deny children to download files from the Internet. Parental Controls furthermore provides the option to give the nod or block specific programs, set time limits for offspring's use of the Vista computer, and control which kind of games they can play. In addition to that can view an activity report about computer usage of each user that specify.

Reference

http://technet.microsoft.com/en-us/library/cc766437(WS.10).aspx

http://www.sharewareconnection.com/network-management-suite.htm

http://www.brighthub.com/computing/smb-security/articles/33211.aspx

http://www.microsoft.com/windows/windows-vista/compare-editions/business.aspx

http://www.windows-vista-update.com/Windows_Vista_Security.html