

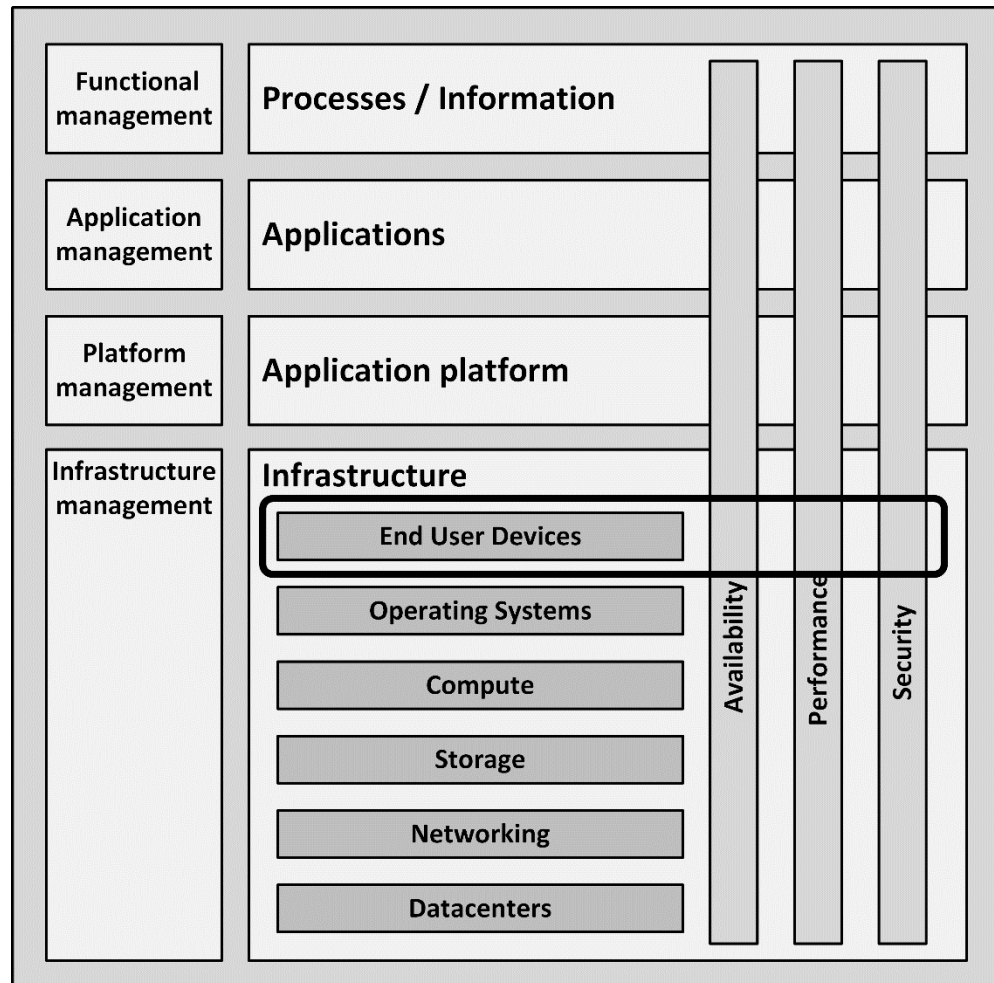
IT Infrastructure Architecture

Infrastructure Building Blocks
and Concepts

End user devices

Introduction

- Humans interact with applications using end user devices
- Typical end user devices are:
 - Desktop PCs
 - Laptops
 - Virtual desktops
 - Mobile devices like phones and tablets
 - Printers



History

- The first end user devices were teletypes
- Teletypes were electromechanical typewriters
 - Provided a user interface to early mainframes
 - Sending typed data to the computer and printing the response



History

- Electronic terminals replaced the teletypes
- Terminals provided a monitor screen instead of printed paper
 - Allowing full screen editing and instant output
- Terminals were “dumb”
 - Did not have their own processing power
 - Relayed typed-in commands to the mainframe computer and the mainframe computer sent data back to the terminal to be displayed
- Terminals were used for decades to interact with mainframe and midrange computers

History - PC

- In 1981, IBM introduced the Personal Computer (PC)
- The IBM PC became the de facto end user device in many office environments
 - Office workers had full control over their own computer for the first time



History - PC

- IBM developed the PC in about a year
 - The PC was built using "off-the-shelf" parts from a variety of manufacturers
 - Based on an open architecture
 - Enabling other manufacturers to produce and sell peripheral components and compatible software without having to purchase licenses
- IBM sold an IBM PC Technical Reference Manual
 - Complete circuit diagrams
 - A listing of the ROM BIOS source code

History - PC

- Many parties copied the PC
 - PC clones or IBM-compatible PCs
- Built with:
 - The same architecture
 - The same chipset as the IBM PC
 - Reversed-engineered BIOS software
- This allowed clones to run unmodified IBM software
- One of the first and most successful companies building clones was Compaq, which would later become part of HP
- All of the IBM PC software was developed by third parties
 - Microsoft provided the DOS operating system and office tools like Word and Excel

History - Apple

- IBM was already a large manufacturer of computers before the introduction of the PC
- Apple was founded by two hobbyists
- In 1984, Apple introduced the Apple Macintosh
 - The first commercially successful personal computer to feature a mouse and a GUI rather than a command line interface
 - Designed to be used by consumers, and not as an office tool

History

- Both the Mac and the PC evolved over time to become much faster
 - Color video screens and sound boards became the norm
 - Laptops became the most used form factor
- The introduction of tablets and smartphones made the end user experience truly mobile

End user devices building blocks

Desktop PCs and laptops

- Over the years, PCs have become very powerful
 - Can run complex software
 - Store relatively large amounts of data
- Many organizations are searching for more cost-effective and simple solutions, because of:
 - The complexity of the PC itself
 - The very advanced operating systems
 - The amount of locally installed software
 - The performance, availability, and security issues related to all of these aspects

Desktop PCs and laptops

- People are attached to their PCs
- The term personal computer is still correct
 - Most users feel their PC is their personal tool that systems managers should not tamper with
 - This is why the adoption of alternatives like thin clients has never been very successful

Laptops

- Most laptops are as powerful as desktop PCs
- They are more "personal" than desktops
 - Users can take them home or use them on the road
- Laptops have some disadvantages compared to desktop PCs:
 - Laptops frequently get lost or stolen
 - Laptops break more easily than desktops
 - They are more vulnerable to drops, bumps, coffee spills, etc.
 - The chance of illegal or malicious software being installed on the laptop is higher than on a desktop PC in the office
 - Most laptops are taken home every night,

Mobile devices

- Mobile devices in the context of this course are devices that connect to the IT infrastructure using wireless public or off-site Wi-Fi networks
- Typical mobile devices are:
 - Smartphones and tablets
 - Cars
 - Smart watches
 - Music players
 - Digital cameras
- Computing power of mobile devices is getting comparable to desktop and laptop computers

Mobile devices

- Specific properties:
 - Connect to the IT infrastructure using public networks
 - UMTS or LTE technology
 - Low bandwidth connectivity
 - Fluctuating connection speed
 - Low reliability of connections
 - Small form factor (screen, keyboard)
 - Applications' user interfaces must be re-engineered to handle these smaller sizes

Bring Your Own Device (BYOD)

- Most organizations use standard PCs or laptops with a limited set of business software
- Users at home have access to:
 - Fast, sexy laptops of the brand they like
 - Tablets and smart phones that allow them to run thousands of highly attractive apps
 - Fast broadband internet connections that are often faster than the shared network in the office
- A concept called Bring Your Own Device (BYOD) allows people to bring personally owned – typically mobile – devices to the office
 - Can be used to access the organization's applications and data, as well as their personal applications and data

Bring Your Own Device (BYOD)

- The BYOD concept creates a conflict of interests:
 - To optimize stability of the organization's infrastructure and security, systems managers need to fully control the end user device
 - The owners of the devices want full freedom
 - The user paid for the device (they brought their *own* device), it will not be acceptable to:
 - Have systems managers erase the device (including all family photos or purchased music) in case of an incident
 - Have personal data visible to the systems managers

Bring Your Own Device (BYOD)

- Virtualization techniques can be used to create isolated environments:
 - One virtual machine with access to the organization's data and applications and is fully managed by the organization's systems managers.
 - Managed using Mobile Device Management (MDM) software to monitor, maintain and secure virtual machines on mobile devices
 - When needed, the virtual machine can be remotely wiped to remove all sensitive data
 - One virtual machine that is owned and managed by the end user. This machine runs whatever applications the user wants
- Both virtual machines use the same underlying hardware like network connectivity, touch screen, GPS, compass, and the sound system

Printers

- Printers are used in almost all organizations to provide paper output
- Most used printer types are:
 - Laser printers
 - Inkjet printers
 - Multi-Functional Printers
 - Specialized printers like:
 - Dot matrix printers
 - Line printers
 - Plotters
 - Thermal printers

Laser printers

- A laser printer rapidly produces high quality text and graphics on plain sheets of paper
 - Using ink powder, called toner
- In color printers four toners are used, one for each basic color
 - Cyan
 - Magenta
 - Yellow
 - Black
- Each color is put on paper separately



Laser printers

- The image is produced using a photoreceptive drum
- The drum is electrically charged using high voltages
- The drum is lightened with a laser beam, which eliminates the electrostatic charge on all places, except the image
- The electrostatic charge left on the drum attracts toner that transfers the image on paper
- A fuser then heats the toner to burn it on paper

Inkjet printers

- Inkjet printers create text and graphics by propelling droplets of ink onto paper through high print head resolution
- Benefits with respect to laser printers:
 - No warm up time
 - Use much less energy
 - Relatively cheap
 - Produce high quality printouts, usually in color
- Some professional inkjet printers provide wide format printing, with a print width ranging from 75 cm to 5 m
 - They can be used for instance to create advertising billboards

Multi-Functional Printers (MFPs)

- A Multi-Function Printer (MFP) is an office device that acts as a:
 - Printer
 - Scanner
 - Photocopier
 - Fax machine
- Provides centralized document management and production in an office setting



Multi-Functional Printers (MFPs)

- Printing on demand
 - Printing only starts when a user is authenticated to the printer
 - No printed paper with possibly sensitive text is left on the MFP waiting to be collected
- MFPs contain:
 - Memory
 - Processors
 - Storage, such as a hard disk drive or flash memory
 - An operating system
- An MFP should be handled like a computer
 - Patches must be installed
 - The hard drive should be erased before repair

Specialized printers - Dot Matrix printers

- In dot matrix printers, characters are drawn out of a matrix of dots
 - Each dot is produced by a tiny metal rod driven forward by a tiny electromagnet
 - The moving portion of the printer is called the print head
- Prints one line of text at a time, character-by-character
- Noisy during operation as a result of the hammer-like mechanism in the print head
- Uses continuous fanfold paper rather than cut-sheets

ystem where a
ld allow us to
mercial supplier.



Specialized printers - Dot Matrix printers

- From the 1970s until the 1990s, dot matrix printers were by far the most common type of printer used with personal computers
- Dot matrix printers:
 - Can print on multi-part stationery or make carbon-copies, used for instance for printing invoices
 - Have one of the lowest printing costs per page
 - Use continuous paper rather than individual sheets
- Dot matrix printers are very reliable work horses and are therefore still in use in many places

Specialized printers - Line printers

- Line printers are high speed printers that print one complete line of text at once
 - 600 to 1200 lines per minute
- Multiple technologies:
 - Spinning drums
 - Chains
 - Bandsthat contain the character set
Small hammers are used to push the paper to the passing characters at exactly the right moment, putting the characters on paper

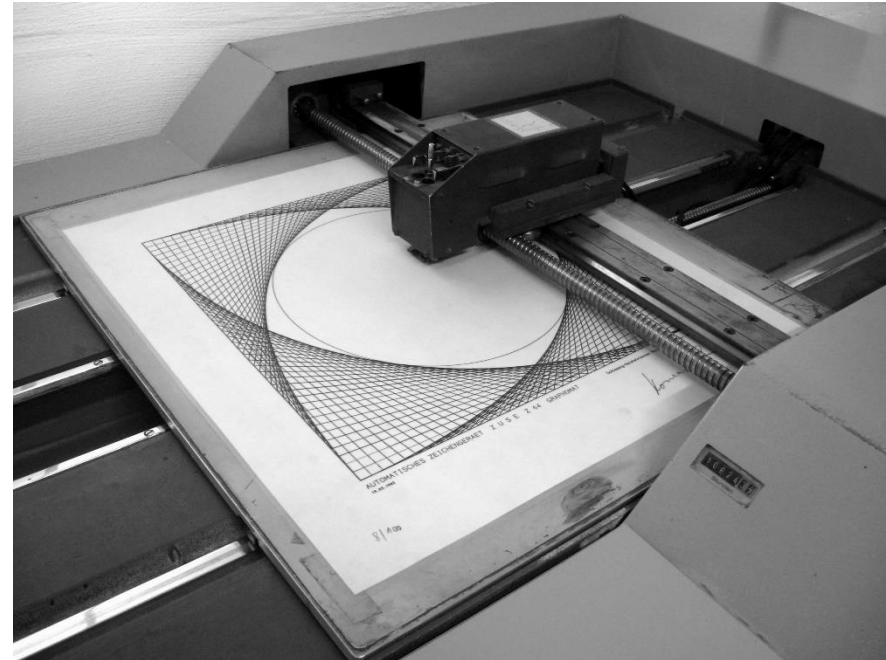


Specialized printers - Line printers

- Line printers are especially well-suited to shop floors and industrial environments
- They use continuous fanfold paper rather than cut-sheets
- Line printers are physically more durable than laser printers
- Their consumables are both less costly and less harmful to the environment

Specialized printers - Plotters

- A plotter is a specialized printer that draws vector graphics using a pen
- Mainly used in computer-aided design, for creating blueprints
- Either the pen moves, or the paper
- Plotters can draw high quality complex line art, including text
- They are slow because of the mechanical movement of the pen and paper
- Most plotters have been replaced by large-format inkjet printers



Specialized printers - Thermal printers

- A thermal printer produces a printed image by selectively heating thermal paper when the paper passes over the thermal print head
 - Thermal paper is impregnated with a chemical that changes color when exposed to heat
- Thermal printers are
 - Quiet
 - Fast
 - Small
 - Low power
- Ideal for portable and retail applications like point of sale terminals and voucher printers
- Drawback: the image disappears exposed to sunlight or heat



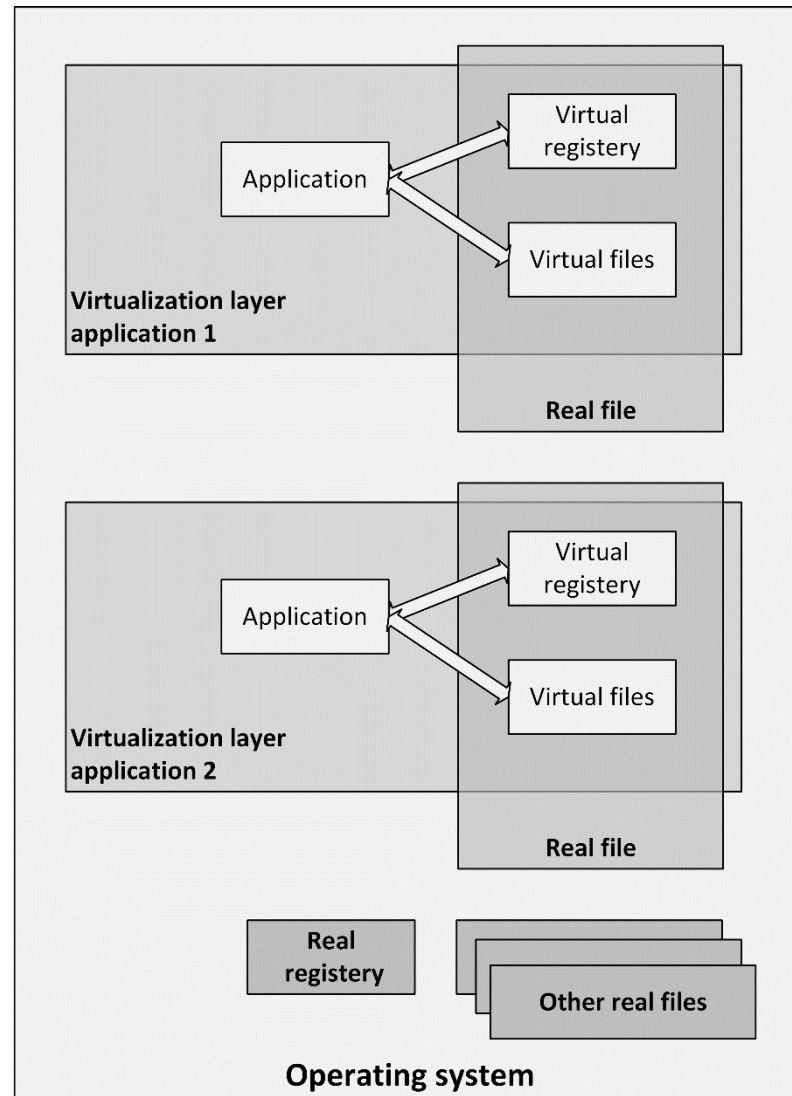
Desktop virtualization

- Virtualization technologies for end user devices:
 - Application virtualization
 - Run applications on an underlying virtualized operating system
 - Virtualized PCs based on:
 - Server Based Computing (SBC)
 - Virtual Desktop Infrastructure (VDI)

Application virtualization

- Application virtualization is typically implemented in a Windows-based environment
- The term application virtualization is a bit misleading:
 - The application itself is not virtualized
 - The operating system resources the application uses are virtualized
- Application virtualization isolates applications from some resources of the underlying operating system and from other applications
 - The application virtualization layer provides the application with virtualized parts of the runtime environment normally provided by the operating system
 - The application assumes it is directly interfacing with the operating system

Application virtualization

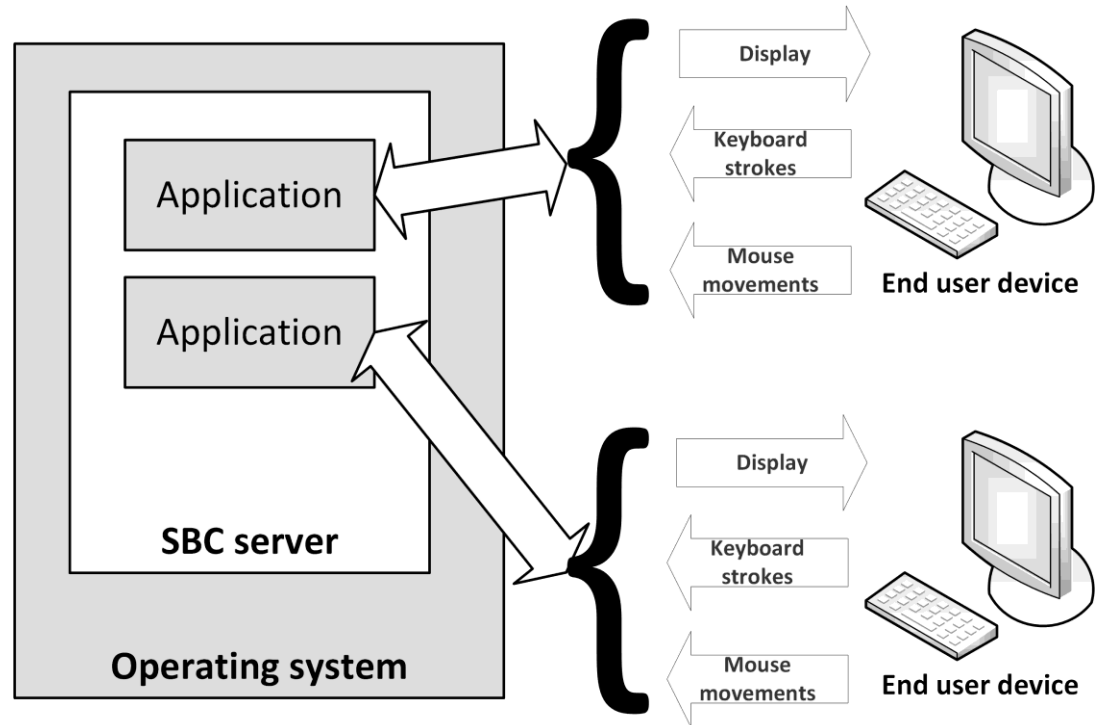


Application virtualization

- The application virtualization layer:
 - Proxies all requests to the operating system
 - Intercepts all file and registry operations
 - These are transparently redirected to a virtualized location, often a single real file
- The application is working with one file, not many files and registry entries spread throughout the system
 - It becomes easy to run the application on a different computer
 - Previously incompatible applications or application versions can be run side-by-side
- Examples:
 - Microsoft App-V
 - VMware ThinApp

Server Based Computing

- Server Based Computing (SBC) is a concept where applications and/or desktops run on remote servers
- They relay their virtual display to the user's device
- Keyboard and mouse information is processed by the application on the server
- The resulting display changes are sent back to the user device



Server Based Computing

- The user's device runs a lightweight application (a thin client) that:
 - Displays the video output from the server
 - Fetches the keyboard strokes from the client
 - Fetches mouse movements from the client
 - Sends client input back to the application on the remote server
- SBC requires a limited amount of network bandwidth:
 - Only changed display information is sent to the end user device
 - Only keyboard strokes and mouse movements are sent to the server

Server Based Computing

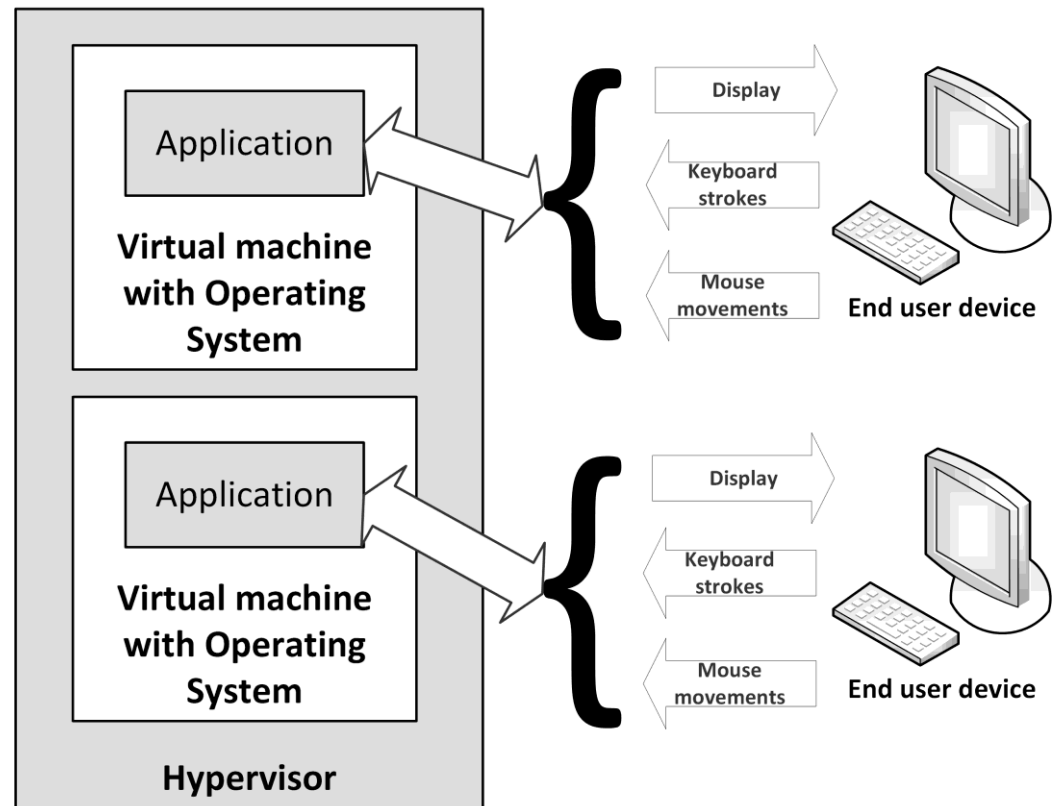
- SBC is typically implemented in a Windows based environment
- SBC products:
 - Windows Remote Desktop Service (RDS, formerly known as Windows Terminal Services)
 - Citrix XenApp (formerly known as MetaFrame Presentation Server)
- RDS is part of the Windows operating system
- XenApp provides more functionality than RDS, but is a separate product

Server Based Computing

- Advantages of SBC:
 - Maintenance (like applying patches and upgrades) can be done at the server level
 - The changes are available instantly to all users
 - Application configurations are the same for all users
- Disadvantages:
 - Graphical properties of the SBC server are used instead of that of the client end user device
 - Limitations on the desktop experience (slow response or keyboard lag) are mostly due to network latency or the configuration of the remote desktop

Virtual Desktop Infrastructure (VDI)

- Virtual Desktop Infrastructure (VDI) is a similar concept as SBC
- In VDI, user applications run in their own virtual machine
- The hypervisor's primary task is to distribute available hardware resources between VDI machines on a physical machine



Virtual Desktop Infrastructure (VDI)

- With VDI, each user has exclusive use of the operating system, CPU, and RAM
 - SBC users share these resources
 - VDI enables applications and operating systems to run next to each other in complete isolation without interference
- VDI tends not to scale well in terms of CPU resources and storage IOPS
 - Each client uses an entire virtual machine
 - A 'Logon storm' occurs when many virtualized systems boot up at the same time
 - Logon storms can partly be prevented by pre-starting a predefined number of virtual machines at configured time slots

Thin clients

- VDI and SBC both enable the hosting of desktops on central server farms and use the same protocols to deliver the output of application screens to users
- Thin clients communicate with the SBC or VDI server
 - Hardware:
 - Lightweight computers, inexpensive, have no moving parts or local disk drives
 - Have no configuration; can be used directly after plugging them into the network
 - Easy to replace when one fails
 - No regular upgrades or systems management needed
 - Software:
 - Applications running in a normal client operating system
 - Runs on mobile devices like tablets and smartphones

PXE boot

- The Preboot eXecution Environment (PXE) allows desktop PCs or thin clients to boot from an operating system disk image stored on the network instead of from a local hard disk
 - This allows for diskless thin clients
 - The BIOS tries to locate a PXE boot server on the network
- For PXE to work, the PC always needs a network connection
 - Not suitable for mobile devices like laptops
- Implementing a high performing TFTP server is crucial for fast start-up times

End user devices availability

Reliability

- End user devices' hardware is much less reliable than hardware installed in the datacentre
 - To keep the cost low
 - Designed to last only 3 to 5 years
- Mobile devices like laptops or tablets can get physically damaged quite easily
 - Leading to hardware failures
 - Typical failures are hard disk crashes in laptops or screen cracks in tablets
- A failing end user device immediately leads to downtime for a user
 - Loss of availability of business functions to the end user

Backup of end user devices

- Backup of local disks is very important
 - Most of the work worldwide is first saved to a local disk on an end user device
 - Automated synchronization of local data to a server can be implemented
 - For end users, it should be impossible to disable this synchronization function
- End user devices should be protected from random installs of potential bad software by end users

End user devices performance

End user device performance

- Performance of end user devices is in most cases not a big issue
- PCs and laptops:
 - Adding more RAM increases the performance more than choosing a faster CPU
 - A faster disk – preferably an SSD disk – can positively affect the performance
- Most data processed on a PC or laptop is transferred using the network
 - Make sure enough bandwidth is available for each end user device

End user device performance

- Ensure software running on mobile devices is capable of handling low bandwidth and unreliable connectivity
 - End user devices are often used with public wireless networks (like public Wi-Fi, or 3G)
 - Technologies like Server Based Computing can help to make mitigate the effect of low bandwidth

End user devices security

End user device security

- Securing end user devices is quite a challenge
 - They are not located in a locked down datacentre
 - They are spread around offices, homes and client locations
- Some tips:
 - Provide users with laptop cable locks to physically lock the laptop to an unmovable object to prevent theft.
 - If end user devices are at the end-of-life, or when they need repair, fully erase the hard disk first
 - Malware protection software like a virus scanner needs to be installed on each device
 - Laptops and PCs can contain a large amount of (business critical) data – encrypt the full hard disk!

Mobile device management

- Mobile device management (MDM) can be used to monitor, maintain and secure devices that are not regularly connected to the organization's network
- When a mobile device is stolen, MDM enables systems management to remotely erase the device's content
- Software to locate the stolen device can be installed to help law enforcement locating the device and arresting the thief

End user authorizations and awareness

- End users should not be able to remove important software or alter system files or log files
 - They should not have the administrator password of their device
 - When users need to install software, they could be given the right to do so, without giving them the administrator password of their device
- BIOS passwords can be used on laptops and desktops to further increase security
 - BIOS setting should be applied to prevent booting from USB sticks or DVD drives
- Users need to be aware of common security guidelines including:
 - The possibility of social engineering
 - Using strong passwords
 - Knowing how to handle sensitive data