CYBER SECURITY AND NETWORKING

Networking Fundamental Concepts

COMPUTER NETWORK

Computer networking refers to interconnected computing devices that can exchange data and share resources with each other. These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies.

BENEFIT OF NETWORK

It enhances communication and availability of information.

It allows for more convenient resource sharing

file sharing

It is highly flexible

It is an inexpensive system

It increases cost efficiency

It boosts storage capacity

Disadvantages of Computer Networking

It lacks independence

It poses security difficulties

It lacks robustness

It allows for more presence of computer viruses and malware

Its light policing usage promotes negative acts

Type of Network

PAN (Personal area Network)

LAN (Local area Network)

CAN (campus area Network)

MAN (Metropolitan area Network)

WAN (wide area Network)

LAN, consists of a computer network at a single site, typically an individual office building. A LAN is very useful for sharing resources, such as data storage and printers. LAN can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables

PAN, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles
and other personal entertainment devices

WAN, occupies a very large area, such as an entire country or the entire world. A
WAN can contain multiple smaller networks, such as LANs or MANs. The Internet is
the best-known example of a public WAN

MAN, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN

What is the mac address ?

A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed.

What is IP address

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network [Statics | Dynamic]

IP Address

IPV4 : IPv4 stands for Internet Protocol Version 4, which is a standard who enables a total range of 4.2 billion addresses. It consists of four segments which are divided by dots

IPV6 : IPv6 stands for Internet Protocol version 6, and it is the newer version of the Internet Protocol (IP). Yet, can you imagine it was around for more than 20 years? It was introduced back in December 1995! The main goal for its creation is to take over and eventually replace the previous protocol – IPv4. The reason is simple. The number of devices that want to connect to the Internet is growing tremendously, and IPv4 is not able to satisfy such needs

Classes Explained with Examples

TCP/IP defines five classes of IP addresses: class A, B, C, D, and E. Each class has range of valid IP addresses. The value of the first octet determines the class. IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes – class D for multicast and class

E for experimental purposes

Class	First octet value	Subnet mask
A	0-127	8
B	128-191	16
C	192-223	24
D	224-239	-
E	240-255	-

A network address identifies the network to which the device belongs. It is the first part of an IP address, and it is used by routers to forward traffic between networks. The network address is determined by the network prefix or subnet mask of the IP address. For example, in the IP address 192.168.0.1 with a subnet mask of 255.255.255.0, the network address is 192.168.0.0.

A host address identifies a specific device on the network. It is the second part of an IP address, and it is used to deliver traffic to a specific device on the network. In the IP address 192.168.0.1, the host address is 1

Pieces of Network

A network card (also called a network adapter, network interface card, or NIC for short) acts as the interface between a computer and a network cable. The purpose of the network card is to prepare, send, and control data on the network.

A network switch connects devices within a network (often a local area network, or LAN) and forwards data packets to and from those devices. Unlike a router, a switch only sends data to the single device it is intended for (which may be another switch, a router, or a user's computer), not to networks of multiple devices

1.Unmanaged Switch: This is a basic switch that does not require any configuration. It's easy to use and inexpensive, but it doesn't offer any advanced features.

2.Managed Switch: This type of switch allows for more control and configuration options, such as VLANs, QoS, and link aggregation. It's typically used in larger networks and is more expensive than an unmanaged switch.

3.Gigabit Ethernet Switch: This switch supports gigabit speeds, which is 10 times faster than Fast Ethernet. It's commonly used in modern networks that require high-speed data transfer.

4.PoE Switch: A Power over Ethernet (PoE) switch provides power to devices over the Ethernet cable, eliminating the need for a separate power supply. It's commonly used to power devices like IP phones, wireless access points, and security cameras.

5.Layer 2 Switch: This type of switch operates at the Data Link Layer (Layer 2) of the OSI model and provides basic switching functionality, such as MAC address learning and forwarding.

6.Layer 3 Switch: A Layer 3 switch adds routing functionality to a Layer 2 switch, allowing it to route traffic between different subnets. It operates at the Network Layer (Layer 3) of the OSI model.

Router

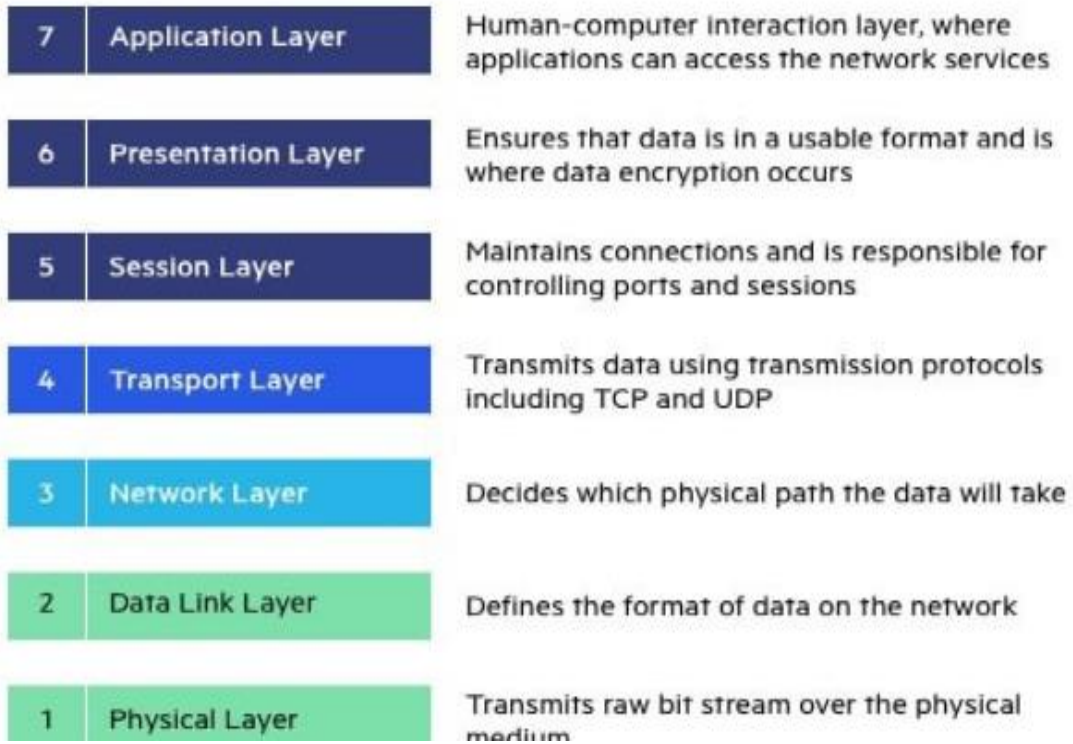
A router is a device that communicates between the internet and the devices in your home that connect to the internet. As its name implies, its “routes” traffic between the devices and the internet.

Wireless access points

Wireless access points (APs or WAPs) are networking devices that allow Wi-Fi devices to connect to a wired network. They form wireless local-area networks (WLANs).

OSI Model

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems



Application Layer: The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users.

Presentation Layer : The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end

Session Layer : The session layer creates communication channels, called sessions, between devices

Transport Layer : The transport layer takes data transferred in the session layer and breaks it into "segments" on the transmitting end.

Network Layer : The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end

Data Link Layer : The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect.

Physical Layer : The physical layer is responsible for the physical cable or wireless connection between network nodes

1.DNS (Domain Name System): This service resolves domain names (e.g. www.example.com) to IP addresses. It translates human-readable domain names into machine-readable IP addresses, allowing devices to access websites and other resources on the internet.

2.DHCP (Dynamic Host Configuration Protocol): This service automatically assigns IP addresses to devices on a network. It eliminates the need for manual IP configuration and helps prevent IP address conflicts.

3.SMTP (Simple Mail Transfer Protocol): This service is used to send and receive email messages between mail servers. It enables email communication across the internet and is a fundamental component of email infrastructure.

4.FTP (File Transfer Protocol): This service is used to transfer files between devices on a network. It's commonly used for sharing files between computers or uploading files to a website.

5.HTTP (Hypertext Transfer Protocol): This service is used to transfer web pages and other resources between web servers and web clients (e.g. web browsers). It's the foundation of the World Wide Web and enables users to access web-based services and content.

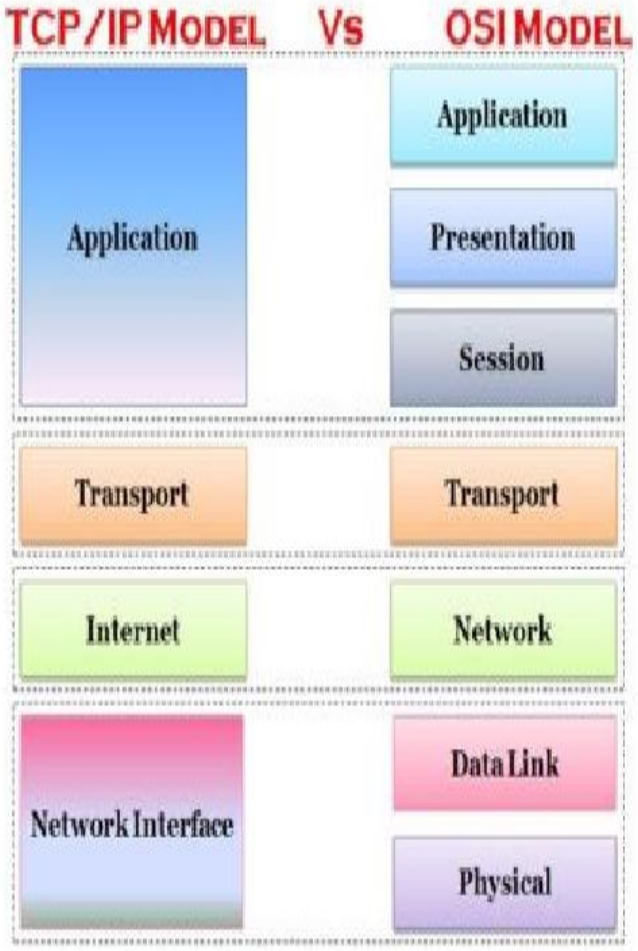
6.SSH (Secure Shell): This service provides secure, encrypted remote access to devices on a network. It's commonly used to remotely manage servers and network devices, and to securely transfer files.

7.NTP (Network Time Protocol): This service synchronizes the time of devices on a network with a central time source. It's important for time-sensitive applications and ensures that all devices on the network have accurate time information.

Advantages of OSI Model

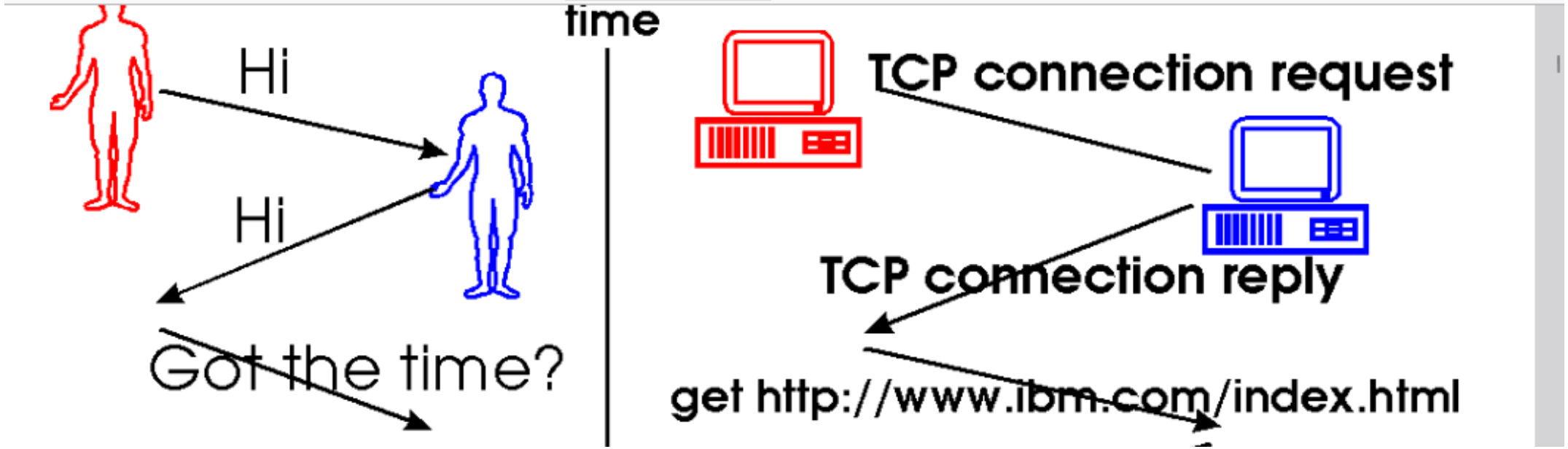
- ✓ The OSI model helps users and operators of computer networks:
- ✓ Determine the required hardware and software to build their network.
- ✓ Understand and communicate the process followed by components communicating across a network.

  Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer



TCP/IP Model: Layers & Protocol

The TCP/IP model is a part of the Internet Protocol Suite. This model acts as a communication protocol for computer networks and connects hosts on the Internet. It is a concise version of the OSI Model and comprises four layers in its structure



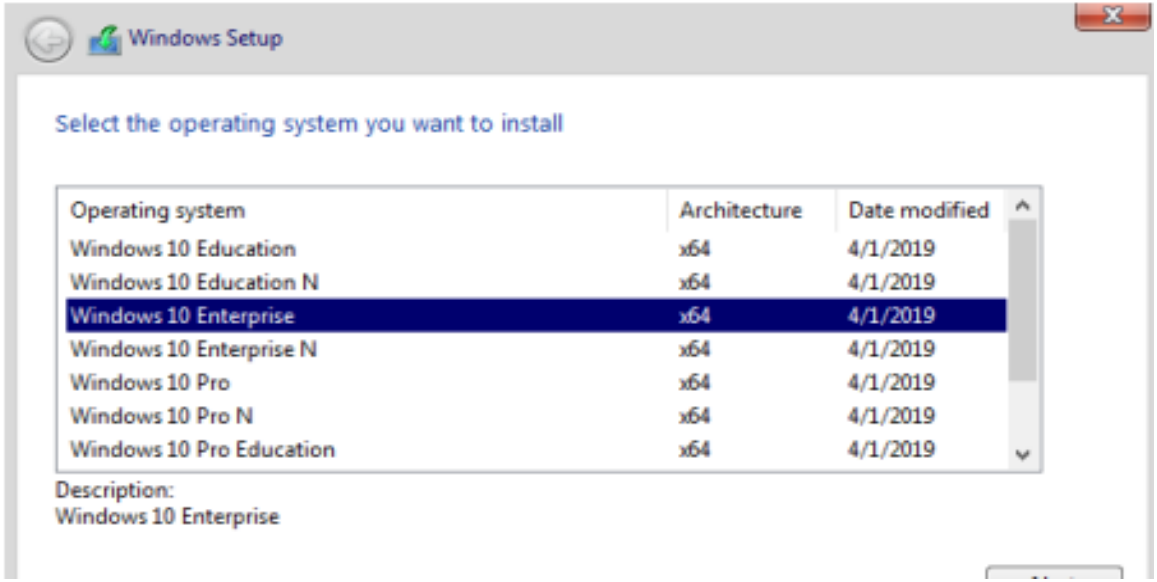
A human protocol and a computer network protocol

Fundamentals of Windows and Linux Operating system

Understanding Windows 10 editions and capabilities

Windows 10 editions available for home users, enterprise users, and education users

Before you deploy Windows 10 in your environment, you must select the most suitable edition for your environment



Edition	Consumer	Availability
Windows 10 Home	Individual/home use	Everybody
Windows 10 Pro	Small and medium-sized businesses, advanced users	Everybody
Windows 10 Enterprise	Large enterprises	Only available to Volume Licensing customers
Windows 10 Enterprise LTSB	Large enterprises	Only available to Volume Licensing customers
Windows 10 Education	School staff, administrators, teachers, and students	Only available through academic Volume Licensing

Installation method

- ✓ **Installation media**: When you buy a self-customized gaming PC with different hardware components, you will use a DVD or USB with a Windows 10 ISO file on it and boot the computer from your installation media.

- ✓ **System image**: A system image also refers to a golden image. It is typically a file that contains a snapshot, which can be referred as a capture image, of a generic computer with the OS installed, including drivers, specific configurations, and perhaps some applications, such as Microsoft Office and Adobe Reader.

- ✓ There are various tools available for creating and deploying images, such as System Center Configuration Manager (SCCM) and Microsoft Deployment Toolkit(MDT). A system image is the preferred method and is used for medium- and large-sized enterprise organizations. These kinds of deployments are faster and more automated than installing from a DVD or USB.

Windows Autopilot: If the computer already has Windows 10 pre-installed, then Windows Autopilot can be used to carry out a new deployment. Windows Autopilot allows administrators to apply organization-specific configurations and some types of applications

Clean Installation process

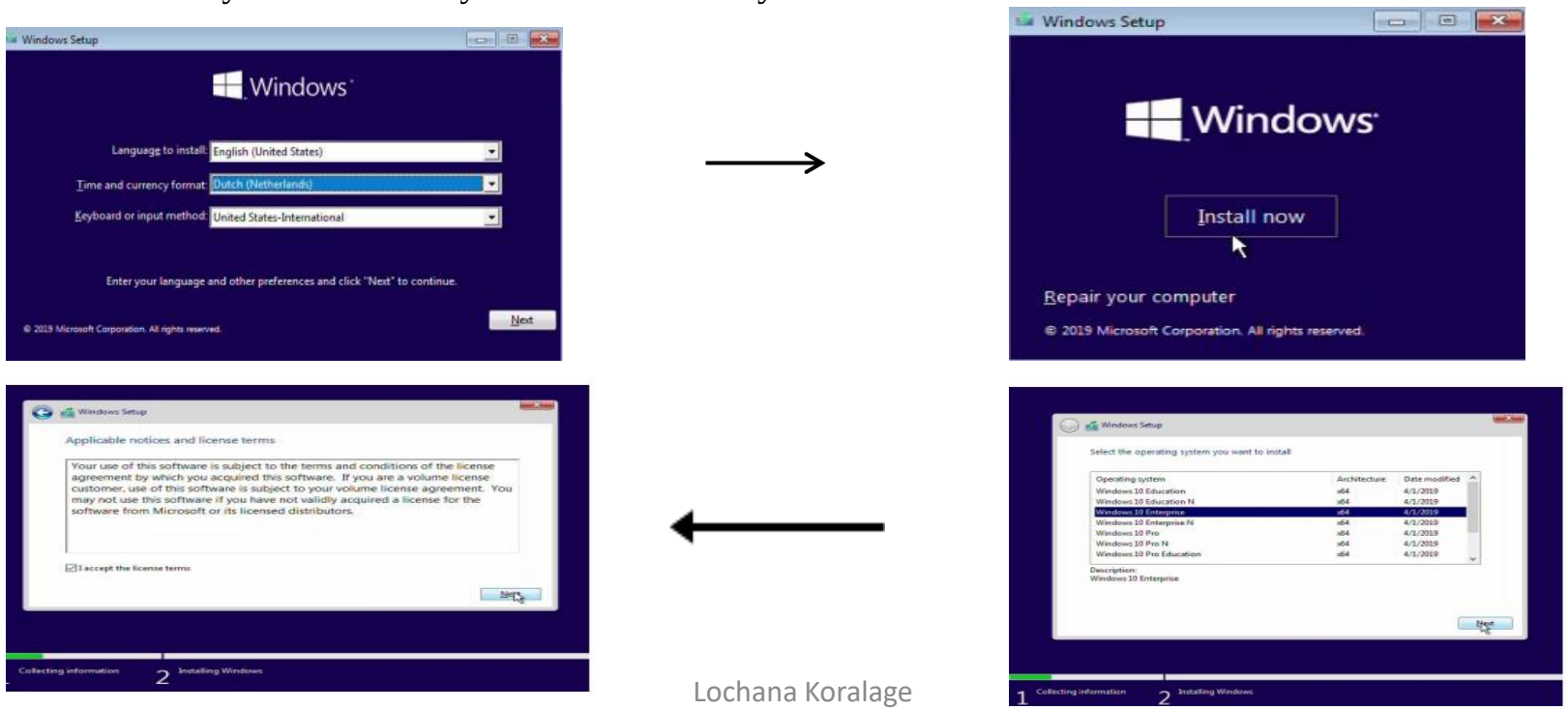
A clean installation process refers to the process of installing an operating system or software on a computer or device by erasing all the data and files that are currently on the device. A clean installation is often done to start fresh with a clean slate, removing any system or software issues that may have been caused by previous installations or use.

Clean installations can be done for various reasons

Upgrading to a newer version of the operating system or software.

•Resolving persistent system or software issues that are not easily fixable through other means.

•Removing malware or other security threats that may have infected the system.



Upgrading Windows 10

Performing an in-place upgrade

During an in-place upgrade, all user applications, hardware devi
settings, data, files, and other configuration information are reta
An in-place upgrade consists of four phases that occur throughc
upgrade process:

1. System check
2. Installing Windows 10 with Windows Preinstallation Environ
(WinPE)
3. First startup
4. Installing the OS and a second startup

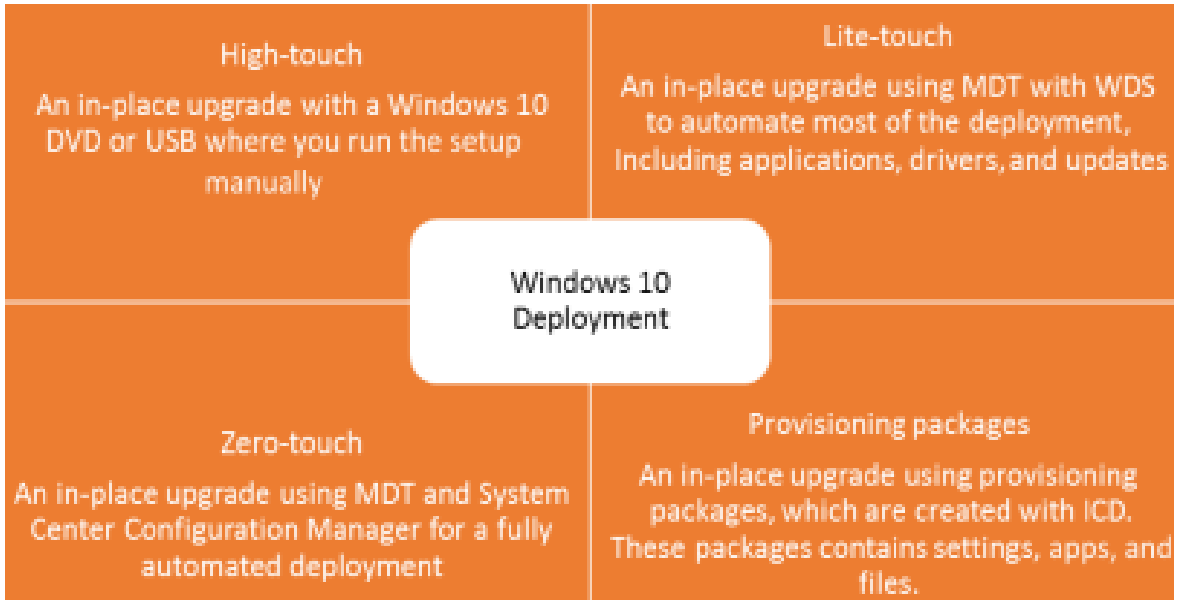
Upgrade paths to Windows 10

		Windows 10 Home	Windows 10 Pro	Windows 10 Education	Windows 10 Enterprise
Windows 7	Home	✓	✓	✓	
	Professional		✓	✓	
	Ultimate		✓	✓	✓
	Enterprise			✓	✓
Windows 8.1	Connected	✓	✓	✓	
	Pro		✓	✓	✓
	Enterprise			✓	✓
Windows 10	Home		✓	✓	
	Pro			✓	
	Enterprise			✓	

Questions

1. You want to deploy AppLocker and Windows Defender Credential Guard on your school's network. Can you install the Windows 10 Education version?
2. Can you buy Windows 10 Enterprise in a computer store?
3. You have a 32-bit version of Windows 10. Is it possible to install the Hyper-V feature?
4. Is it possible to boot and install Windows 10 from a DVD?

Selecting the right tools for upgrading



Zero-touch installation (ZTI) is a deployment method used to automate the installation and configuration of software and operating systems on a large number of devices. ZTI is designed to reduce the need for human intervention during the installation process, allowing for faster and more consistent deployment across an organization's devices.

High-touch deployment method This type of deployment strategy is time-consuming. However, it can be ideal for small organizations with less than 100 computers and no IT staff. For this, you need to go to each computer and manually start the Windows 10 installation from a Digital Video Disc (DVD) or Universal Serial Bus (USB), which requires you to provide an answer for each prompt during the setup stage

lite-touch deployment method

This type of deployment strategy is ideal for medium-sized organizations with between 200 and 500 computers. In most cases, this deployment type uses the Microsoft Deployment Toolkit (MDT) in combination with Windows Deployment Services (WDS). MDT automates most of the installation of Windows 10 together with installing applications, device drivers, and updates

Provisioning packages are a collection of settings and configuration files that can be used to automate the setup and configuration of devices running Windows 10 or later operating systems. These packages are designed to simplify the process of deploying and configuring devices in enterprise environments by allowing IT administrators to create and apply custom configurations to one or more devices at the same time.

More information : https://www.youtube.com/watch?v=ivqvYlQirNo

file systems

FAT (File Allocation Table): A simple file system used by older versions of Windows and some removable storage devices. It is limited in terms of file size and does not provide robust security features.

NTFS (New Technology File System): A file system used by modern versions of Windows that provides improved performance, scalability, and security compared to FAT. It supports larger file sizes, better data protection, and access control.

APFS (Apple File System): A file system used by Apple's macOS operating system. It provides improved performance, encryption, and crash protection compared to previous file systems used by macOS.

ext4 (Fourth Extended File System): A file system used by Linux-based operating systems. It supports larger file sizes, journaling for faster file system recovery, and improved performance compared to older Linux file systems.

exFAT (Extended File Allocation Table): A file system designed for use with flash drives and other removable storage devices. It supports large file sizes and is compatible with both Windows and macOS.

CMD (Command Prompt) is a command-line interpreter that allows users to execute various commands to perform tasks in Windows. Here are some commonly used CMD commands

cd: Changes the current directory.

- ✓ md: Creates a new directory.
- ✓ del: Deletes one or more files.
- ✓ type: Displays the contents of a text file.
- ✓ echo: Displays messages or turns command echoing on or off.
- ✓ tasklist: Displays a list of currently running processes.
- ✓ taskkill: Terminates one or more processes.
- ✓ netstat: Displays network statistics and active connections.
- ✓ ipconfig: Displays network configuration information.
- ✓ ping: Tests network connectivity to a specified host.
- ✓ tracert: Traces the route taken by packets over a network.
- ✓ systeminfo: Displays system information.
- ✓ shutdown: Shuts down or restarts the computer.
- ✓ format: Formats a disk or drive.
- ✓ chkdsk: Checks a disk for errors and attempts to repair them

dir: Displays the contents of the current directory..

•**dir**: displays the contents of the current directory.

•**cd:** changes the current directory. For example, cd C:\Users changes the current directory to the "Users" folder on the C: drive.

•**md**: creates a new directory. For example, md Documents creates a new directory named "Documents" in the current directory.

•**type**: displays the contents of a file. For example, type myfile.txt displays the contents of the file "myfile.txt".

•**copy**: copies a file from one location to another. For example, copy myfile.txt C:\Users\Loch\Documents copies the file "myfile.txt" to the "Documents" folder in the “loch" folder on the C: drive.

•**del**: deletes a file. For example, del myfile.txt deletes the file "myfile.txt".

•**ping**: tests the connection between your computer and another computer or website. For example, ping google.com tests the connection to the Google website.

•**ipconfig**: displays the network settings for your computer. For example, ipconfig /all displays detailed network information, including IP addresses, DNS se**tasklist**rvers, and more.

•: displays a list of running processes. For example, tasklist /svc displays a list of running processes and the services they are associated with.

•shutdown: shuts down the computer. For example, shutdown /s shuts down the computer immediately

Batch Scripts are stored in simple text files containing lines with commands that get executed in sequence, one after the other. Scripting is a way by which one can alleviate this necessity by automating these command sequences in order to make one's life at the shell easier and more productive

```
@echo off
set name=Lochana
echo Hello %name%!
Pause
```

set command is used to create a variable called name and assign it the value "Lochana"

The echo command is used to print out a greeting message that includes the value of the name variable. The %name% syntax is used to reference the variable's value.

Comment :

```
@echo off
Rem This program just displays Hello World
set message=Hello World
echo %message%
```

In a batch script, comments can be created using the REM command

String

```
set first_name=John
set last_name=Doe
set full_name=%first_name% %last_name%
echo %full_name%
set command
```

In a batch script, strings are sequences of characters enclosed in quotes. They can be used to store text and manipulate it in various ways

In batch scripting, an **empty string** is a string that contains no characters. You can create an empty string variable by using the set command

```
@echo off

set message="Hello, world!"
echo %message%

set message=""
if "%message%"=="" (
  echo Message is empty
) else (
  echo Message is not empty
)

set message="Goodbye!"
echo %message%

pause
```

In batch scripting, **string interpolation** is the process of substituting variables or expressions into a string

```
set name=John
set message=Hello, %name%!
echo %message%
```

String concatenation is the process of combining two or more strings into a single string. In batch scripting, you can use the set command and the + operator to concatenate strings.

```
set str1=Hello
set str2=World
set message=%str1% %str2%!
echo %message%
```

In batch scripting, you can use the set command and the call command to determine the length of a string

Batch Script - String length

```
@echo off

set string=Hello, world!

REM Determine the length of the string
call :strlen result "%string%"
echo The length of the string is %result%

pause
goto :eof

REM The :strlen subroutine
:strlen
setlocal EnableDelayedExpansion
set "str=!%~2!"
set "len=0"
for /L %%A in (12,-1,0) do (
  set /a "len |= 1<<%%A"
  for %%B in (!len!) do if "!str:~%%B,1!"=="" set /a "len &= ~(1<<%%A)"
)
endlocal & set "%~1=%len%"
exit /b
```

Batch Script - toInt

In batch scripting, you can use the set /a command to convert a string to an integer. The /a option tells set to evaluate the string as an arithmetic expression.

```
@echo off
set string=42
set /a integer=%string%
echo The integer is %integer%.
Pause
```

Batch Script – Remove

In batch scripting, you can use the %variable: search=replace% syntax to replace all occurrences of a substring in a string variable with a new substring.

```
@echo off
set string=Hello, world!
set substring=, world!
echo The original string is %string%.
REM Remove the substring
set string=%string:%substring%=
echo The modified string is %string%.
pause
```

Batch Script – Arrays ?

Batch scripts do not have built-in support for arrays, but you can simulate them using variables with numeric suffixes.

```
@echo off

set fruits[0]=apple
set fruits[1]=banana
set fruits[2]=cherry

echo The second fruit is %fruits[1]%.

Pause
```

Batch Script - Decision Making

The if statement in a batch script is used to make decisions based on conditions.

Here's the basic syntax of an if statement:

```
@echo off

set /p name=Enter your name:

if "%name%"=="John" (
    echo Hello, John!
)
pause
```

```
@echo off

set /p name=Enter your name:

if "%name%"=="John" (
    echo Hello, John!
) else (
    echo Nice to meet you, %name%.
)

pause
```

Batch Script - Operators

Batch scripts support a variety of operators that can be used in if statements and other expressions. Here's a summary of the operators available in batch scripts:

Arithmetic operators: + (addition), - (subtraction), * (multiplication), / (division), % (modulus)

Comparison operators: == (equal to), neq (not equal to), lss (less than), leq (less than or equal to), gtr (greater than), geq (greater than or equal to)

Logical operators: & (bitwise AND), | (bitwise OR), ^ (bitwise XOR), && (logical AND), || (logical OR), ! (logical NOT)

```
@echo off
if %age% leq 18 (
    echo You are not old enough to vote.
) else (
    echo You are old enough to vote.
)
Pause
```

set /p age=Enter your age: if statement with **the leq comparison operator to check whether the value of the age variable is less than or equal to 18**. If it is, the script outputs a message indicating that the user is not old enough to vote. Otherwise, the script outputs a message indicating that the user is old enough to vote.

Batch Script - Network

Display IP Address: To display the IP address of the computer, we can use the following batch script:

```
@echo off
ipconfig | findstr /i "IPv4"
Pause
```

Set IP Address:

To set the IP address of the computer, we can use the netsh command. The following batch script will set the IP address, subnet mask, and default gateway:

```
@echo off
netsh interface ipv4 set address name="Local Area Connection" static 192.168.0.2 255.255.255.0 192.168.0.1
Pause
```

Example

```
@echo off

set /p num1=Enter the first number:
set /p num2=Enter the second number:

set /a result=%num1%+%num2%

echo The result is %result%
```

set /p command prompts the user to enter two numbers, which are then stored in the variables num1 and num2. The set /a command performs the addition operation on the two numbers and stores the result in the variable result. Finally, the echo command displays the result to the user.

Registry ? The Windows Registry is a hierarchical database that stores configuration settings and options for the Microsoft Windows operating system. It contains information and settings for hardware, software, users, and preferences.

The registry is organized into keys, subkeys, and values, which are similar to folders, subfolders, and files in a file system. Each key and value in the registry corresponds to a specific aspect of the operating system or installed applications.

The registry is a critical component of Windows, and any changes made to it can have a significant impact on the performance and stability of the operating system.

The registry can be accessed and modified using the Registry Editor (regedit.exe) that comes with Windows. However, modifying the registry manually can be complex and risky, especially for novice users. Batch scripts can automate registry-related tasks and make the process more efficient and less error-prone.

Read Registry Value

```
@echo off
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion" /v ProductName
pause
```

PowerShell is a command-line shell and scripting language developed by Microsoft. It is designed to automate tasks and manage system configurations in Windows and can also be used for tasks such as debugging, testing, and data analysis.

Working with the Commands in PowerShell

Accessible | simple and complex | automation scalable management | access information

Why Learn PowerShell : Most Microsoft products use it | cannot do all the administration | many gui are PowerShell front ends |automation and security | Network management|

Get-ChildItem C:\Windows : This command is used to list the files and folders in a specified directory.

Set-ExecutionPolicy RemoteSigned : This command is used to set the execution policy for PowerShell scripts

New-Item -ItemType Directory -Path C:\Test : New-Item: This command is used to create a new item, such as a file or folder.

Get-Process: This command is used to list the running processes on the system

Start-Process notepad.exe

New-Item -ItemType Directory -Path "C:\MyNewFolder“ : To Create the New Folder using PowerShell

Remove-Item -Path "C:\MyFolder" –Recurse : To delete a folder using PowerShell

New-Item -ItemType File -Path "C:\MyNewFile.txt“ : To create a new file using PowerShell

In the following scenarios, how should you use PowerShell commands?

- ✓ Make a text file with your name in the file name.
- ✓ change the locations
- ✓ Make a new desktop folder.
- ✓ duplicates in your file
- ✓ Previews file delete
- ✓ duplicate in your folder now C drive

SET-DATA AND TIME

Set-Date cmdlet is used to set System Date :Get-Date

set-date -Date (Get-Date).AddDays(1)

What is File I/O ?

PowerShell provides several cmdlets to perform file input/output (I/O) operations. Here are some of the commonly used file I/O cmdlets in PowerShell

Get-Content: This cmdlet is used to read the content of a file. :

Get-Content C:\myfile.txt

Set-Content: This cmdlet is used to write content to a file

Set-Content C:\newfile.txt "This is some text."

Add-Content: This cmdlet is used to append content to a file. :

Add-Content C:\myfile.txt "This is some additional text.“

Copy-Item: This cmdlet is used to copy files from one location to another.

Copy-Item C:\myfile.txt C:\myotherdir\myfile.txt

Move-Item: This cmdlet is used to move files from one location to another. Move-

Item **C:\myfile.txt C:\myotherdir\myfile.txt**

6 .Remove-Item: This cmdlet is used to delete files from the system

Remove-Item C:\myfile.txt

Cmdlets

Cmdlets in PowerShell are small, task-oriented commands that are used to perform specific operations.

common categories of PowerShell cmdlets:

1.Active Directory Cmdlets: These cmdlets are used to manage users, groups, and other objects in Active Directory.

2.Networking Cmdlets: These cmdlets are used to manage network adapters, configure network settings, and troubleshoot network issues.

3.File Management Cmdlets: These cmdlets are used to manage files and directories, copy and move files, and perform other file-related operations.

4.Process and Service Cmdlets: These cmdlets are used to manage processes and services running on the system.

5.Registry Cmdlets: These cmdlets are used to manage the Windows Registry, including creating, modifying, and deleting registry keys and values.

6.Security Cmdlets: These cmdlets are used to manage security-related tasks, such as managing certificates and setting security policies.

7.PowerShell Utility Cmdlets: These cmdlets are used to perform various utility tasks, such as formatting and converting data, managing variables, and running scripts.

Object-Oriented: PowerShell is built on the .NET framework and is an object-oriented language. This means that PowerShell scripts can work with objects, such as files, folders, and registry keys, rather than just strings of text

Pipelining: PowerShell allows you to pipe the output of one command to another command, allowing you to chain together commands to perform complex operations. This makes it easier to write concise, efficient scripts that perform multiple tasks.

Modules: PowerShell includes a wide range of modules that provide additional functionality, such as working with Active Directory, managing network settings, and working with Microsoft Office products. You can also create your own modules to extend PowerShell's functionality.

Cmdlets: PowerShell includes a large number of built-in cmdlets that perform common tasks, such as working with files, managing processes, and querying the registry. You can also create your own cmdlets to perform custom tasks.

Variables: PowerShell allows you to use variables to store data, making it easier to reuse data throughout your script. You can also use variables to pass data between functions and cmdlets.

Functions: PowerShell allows you to define your own functions to perform custom tasks. Functions are reusable and can be called from within other functions, cmdlets, and scripts.

Error Handling: PowerShell includes robust error handling capabilities, allowing you to catch and handle errors that occur during script execution. You can also use try/catch blocks to handle specific types of errors.

Script Debugging: PowerShell includes a debugging feature that allows you to step through your script line by line, inspect variables, and set breakpoints. This makes it easier to troubleshoot and fix errors in your scripts.

Powershell - Special Variables

PSVersionTable - This variable contains information about the PowerShell version that is currently running, such as the version number, build number, and release date.

$PSScriptRoot - This variable contains the path to the directory that contains the currently executing PowerShell script.

$MyInvocation - This variable contains information about the current invocation of the script or command, such as the command line arguments and the name of the script or command.

$_ - This variable represents the current object in the pipeline. It is used as a placeholder variable in many PowerShell commands and scripts.

$args - This variable contains an array of the command line arguments that were passed to the script or command.

$Error - This variable contains an array of the most recent errors that occurred in the current PowerShell session.

$Host - This variable provides access to the current PowerShell host application, such as the PowerShell console or the PowerShell Integrated Scripting Environment (ISE).

Powershell - Operators

Arithmetic Operators:

```
# Addition
$x = 5
$y = 3
$result = $x + $y
Write-Output $result    # Output: 8

# Exponentiation
$x = 5
$y = 3
$result = $x ** $y
Write-Output $result
```

Addition (+):

Subtraction

Multiplication

Division (/):

Exponentiation

Comparison Operators:

```
# And
$x = 5
$y = 3
$result = ($x -gt 3) -and ($y -lt 10)
Write-Output $result    # Output: True

# Not
$x = 5
$result = -not ($x -gt 3)
Write-Output $result    # Output: False
```

Equal to (-eq): Returns True if the first value or object is equal to the second

Not equal to (-ne): Returns True if the first value or object is not equal to the second

Greater than (-gt): Returns True if the first value or object is greater than the second

Less than (-lt): Returns True if the first value or object is less than the second

Greater than or equal to (-ge): Returns True if the first value or object is greater than or equal to the second

Less than or equal to (-le): Returns True if the first value or object is less than or equal to the second

Logical Operators:

```
# And
$x = 5
$y = 3
$result = ($x -gt 3) -and ($y -lt 10)
Write-Output $result    # Output: True

# Not
$x = 5
$result = -not ($x -gt 3)
Write-Output $result    # Output: False
```

And (-and): Returns True if both expressions are True

Or (-or): Returns True if at least one expression is True

Not (-not): Returns True if the expression is False, and vice versa

For Loop:

A For loop is used when you know how many times you want to execute the block of code. It uses a counter variable to keep track of the number of iterations

```
for ($i = 1; $i -le 5; $i++) {
    Write-Output "The value of i is $i"
}
```

ForEach Loop:

A ForEach loop is used when you want to loop through a collection of items

```
$colors = @("red", "green", "blue")
foreach ($color in $colors) {
    Write-Output "The color is $color"
}
```

Do-While Loop:

A Do-While loop is similar to a While loop, but it will always execute the block of code at least once, even if the condition is false.

```
$i = 1

do {
    Write-Output "The value of i is $i"
    $i++
} while ($i -le 5)
```

While Loop:

A While loop is used when you want to execute the block of code repeatedly until a certain condition is no longer true

```
$i = 1
while ($i -le 5) {
    Write-Output "The value of i is $i"
    $i++
}
```