PASS the CompTIA A+ Exam

220-1001 & 220-1002

Hazim Gaber, B.Sc. (ENG), CSSBB, PMP

Published By

HSM Press
HSMG Services & Consulting Inc.
34th Floor
10180 101 ST NW
Edmonton, AB T5J 3S4
Canada
Phone: 1-800-716-8955
www.hsmglobal.ca
books@hsmglobal.ca

The information provided in this book is provided on an “as is” basis. The publisher makes no warranty towards the fitness or accuracy of the information in this book, and cannot be held liable for your reliance upon it.

Foreword

I am delighted to have the opportunity to help you improve your computer hardware & network skills and to obtain the prestigious & internationally-recognized A+ designation.

This book has been organized to make it easier to absorb and understand the information. I have included practical examples where appropriate.

This is a work in progress. If you have any suggestions to improve this book, or if you see any errors, or if you need help, I would be grateful if you contacted me. My e-mail address is hazim@hsmservices.ca

Visit the A+ Page at hsmpress.ca/comptia

Regards,
Hazim

March 2019

Table of Contents

Contents

Part A: Introduction

What is the CompTIA A+?

CompTIA A+ is an entry level credential for IT Professionals to identify issues and solve problems with computer hardware and networks.

CompTIA allows you to do the following

- Support basic IT infrastructure, including endpoint management, advanced device connectivity troubleshooting, and basic networking
- Configure and support PC, mobile and IoT device hardware, including components, connectors and peripherals
- Implement basic data backup and recovery methods and apply data storage and management best practices
- Demonstrate baseline security skills for IT support professionals, including detecting and removing malware, addressing privacy concerns, physical security and device hardening
- Configure device operating systems, including Windows, Mac, Linux, Chrome OS, Android and iOS and administer client-based as well as cloud-based (SaaS) software
- Troubleshoot and problem solve core service and support challenges while applying best practices for documentation, change management, and the use of scripting in IT support

CompTIA overlaps with

- Networking certifications (Cisco CCNA for example)
- Security certifications
- Virtualization certifications (VMWare)
- Storage certifications

CompTIA A+ has changed for 2019. What is new?

- Physical versus logical security concepts and measures
- Social engineering
- Malware detection and removal

- Device hardening for not just PCs but devices in general
- A dramatically different approach in defining competency in operational procedures
- Importance of documentation and using best practices
- Change management
- Basic disaster prevention and recovery
- Privacy concerns, including GDPR and handing PII (Personally Identifying Information)
- Scripting basics
- Use of remote access Networking and device connectivity are broadened
- Cloud and virtualization are now weighed more heavily
- Managing networking and device connectivity includes IoT devices and related protocols
- Includes the concept of Internet appliances and end point management servers
- Added wireless mesh networks to network types

What can you do with a CompTIA A+ Certification?

- Service Desk Analyst
- Help Desk Tech
- Technical Support Specialist
- Field Service Technician
- Associate Network Engineer
- Data Support Technician
- Desktop Support Administrator
- End User Computing Technician
- Help Desk Technician
- System Support Specialist

CompTIA is “vendor neutral”

According to CompTIA: “All CompTIA certification exams are vendor-neutral. This means each exam covers multiple technologies, without confining the candidate to any one platform. Vendor-neutrality is important because it ensures IT professionals can perform important job tasks in any technology environment. IT professionals with vendor-neutral certifications can consider multiple solutions in their approach to problem-solving, making them more flexible and adaptable than those with training in just one technology."

CompTIA A+ consists of two sections, 220-1001 and 220-1002

The Old CompTIA started December 15, 2015 and consisted of two exams: 220-901 and 220-902. The old CompTIA expires in mid 2019.

The New CompTIA is starts January 15, 2019 and consists of 220-1001 and 220-1002. It will be available in English at first, and then several other languages.

CompTIA A+ 220-1001 covers mobile devices, networking technology, hardware, virtualization and cloud computing and network troubleshooting.

CompTIA A+ 220-1002 covers installing and configuring operating systems, expanded security, software troubleshooting and operational procedures.

How do I obtain the A+ Certification?

You must pass the two exams, 220-1001 and 220-1002.

About the Exam

- You can register online to take the exam. The online system will show you the dates and times that are available.
- You may be able to write the exam on a Saturday or Sunday, depending on the Prometric Test Center.
- You may reschedule the exam for free, if you do so at least 30 calendar days before the exam.
- You may reschedule the exam for USD$70, if you do so at least 2 calendar days before the exam.
- You may not reschedule the exam if there are less than 2 calendar days before the exam.

- If you do not show up to the exam or are more than 15 minutes late to the exam, you will not be allowed to write the exam, and will forfeit the entire fee.

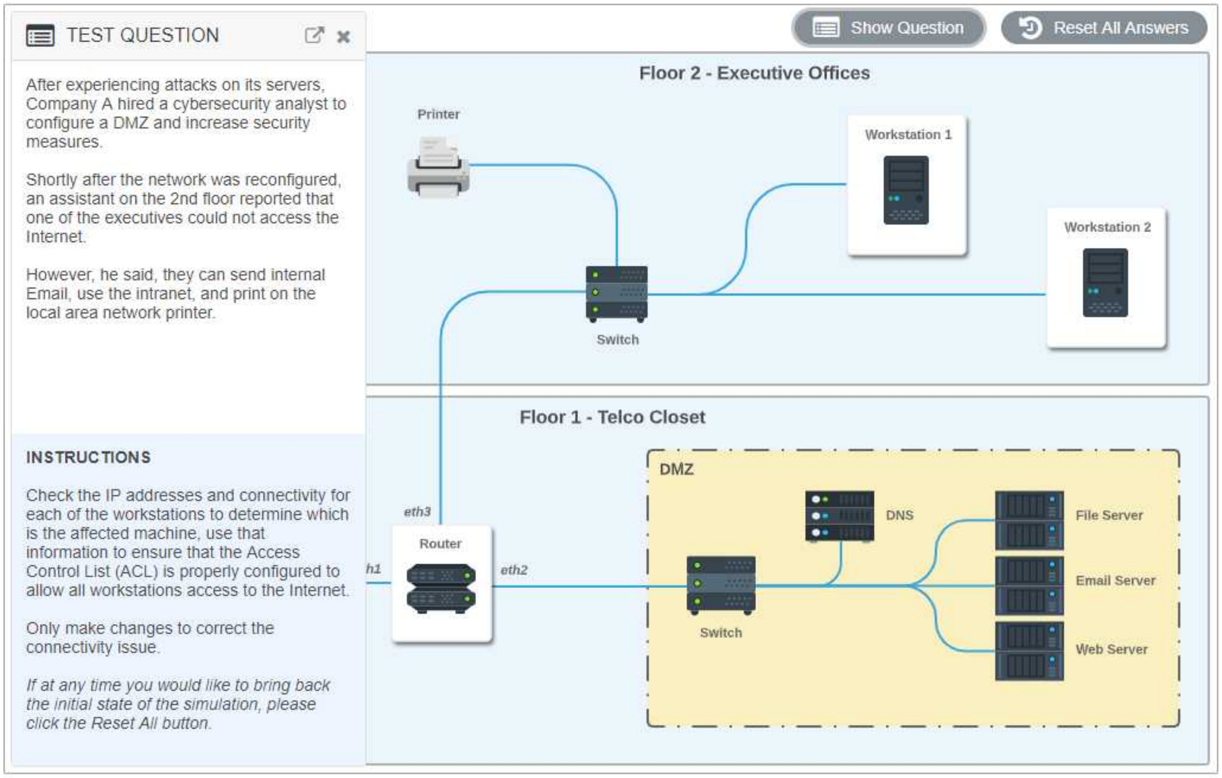
- At the exam center, you are required to show a piece of government-issued photo ID.
- You will be required to empty your pockets and place the contents in a locker.
- If you are wearing eyeglasses, they will be inspected.
- You may be checked with a metal detector.
- You can only bring your photo ID and locker key into the exam room.
- The test center will provide you with scratch paper, a pencil, and a basic calculator.

- While you write the exam, you will be monitored via audio and video surveillance.
- Each exam is up to 90 multiple-choice questions, and you have 90 minutes to complete the exam.
- You can take a break at any time, but the time on the exam will continue to elapse.
- It goes without saying that cheating will not be tolerated!

- You will receive a score between 100 and 900.
- You need a score of 675 to pass the first exam, and 700 to pass the second exam
- You must pass both exams to receive the certification

- The questions are
  - Multiple-choice (single, and multiple responses)
  - Drag & Drop
  - Performance Based (you are provided with a scenario, which you must explore; you are required to correct the issue)

Sample Performance based Question



TEST QUESTION

After experiencing attacks on its servers, Company A hired a cybersecurity analyst to configure a DMZ and increase security measures.

Shortly after the network was reconfigured, an assistant on the 2nd floor reported that one of the executives could not access the Internet.

However, he said, they can send internal Email, use the intranet, and print on the local area network printer.

INSTRUCTIONS

Check the IP addresses and connectivity for each of the workstations to determine which is the affected machine, use that information to ensure that the Access Control List (ACL) is properly configured to allow all workstations access to the Internet.

Only make changes to correct the connectivity issue.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Breakdown of 220-1001

Coverage Amount	Coverage Details
14%	Mobile Devices • Install and configure laptop & components • Compare and contrast characteristics of various types of other mobile devices • Connect and configure accessories and ports of other mobile devices & accessories • Configure basic mobile device network connectivity and application support • Use methods to perform mobile device synchronization
20%	Networks • Compare and contrast TCP and UDP ports, protocols, and their purposes • Compare and contrast common networking hardware devices • Install and configure a basic wired/wireless SOHO network • Compare and contrast wireless networking protocols • Summarize the properties and purposes of services provided by networked hosts • Explain common network configuration concepts • Compare and contrast Internet connection types, network type
27%	Hardware

	• Explain basic cable and connector types, features, and their purposes • Summarize power supply types and features • Select and configure appropriate components & devices for a custom PC configuration to meet customer specifications or needs • Configure SOHO multifunction devices/ printers and settings • Install and maintain various print technologies
12%	Virtualization and Cloud • Compare and contrast cloud computing concepts • Set up and configure client-side virtualization
27%	Networks and Hardware Troubleshooting • Use the best practice methodology to resolve problems • Troubleshoot hard drives and RAID arrays and problems related to motherboards, RAM, power and more • Troubleshoot video, projector, and display issues • Troubleshoot common mobile device issues while adhering to the appropriate procedures • Troubleshoot common wired and wireless network problems

Breakdown of 220-1002

Coverage Amount	Coverage Details
27%	Operating Systems • Compare and contrast common operating system types and their purposes • Compare and contrast features of Microsoft Windows versions • Summarize general OS installation considerations and upgrade methods • Use appropriate Microsoft command line tools • Use Microsoft operating system features and tools • Use Microsoft Windows Control Panel utilities • Summarize application installation and configuration concepts • Configure Microsoft Windows networking on a client/desktop • Use features and tools of the Mac OS and Linux client/desktop operating systems
24%	Security • Summarize the importance of physical security measures • Explain logical security concepts • Compare and contrast wireless security protocols and authentication methods • Given a scenario, detect, remove, and prevent malware using appropriate tools and methods

	• Compare and contrast social engineering, threats, and vulnerabilities • Compare and contrast the differences of basic Microsoft Windows OS security settings • Implement security best practices to secure a workstation • Implement methods for securing mobile devices • Implement appropriate data destruction and disposal methods • Configure security on SOHO wireless and wired networks
26%	Software Troubleshooting • Troubleshoot Microsoft Windows OS problems • Troubleshoot and resolve PC security issues • Use best practice procedures for malware removal • Troubleshoot mobile OS and application issues • Troubleshoot mobile OS and application security issues
23%	Operational Procedures • Compare and contrast best practices associated with types of documentation • Implement basic change management best practices • Implement basic disaster prevention and recovery methods

	• Explain common safety procedures • Explain environmental impacts and appropriate controls • Explain the processes for addressing prohibited content/ activity, and privacy, licensing, and policy concepts • Use proper communication techniques and professionalism • Identify the basics of scripting • Use remote access technologies

Recommended Tools, Hardware & Software

Every job requires tools, and the A+ is no different. You won't need the tools for your exam, but you will need them for your job.

I recommend that you

- Purchase high quality tools that will last a long time. Cheap tools are more expensive in the long term. They break down and cause frustration.
- Ask for advice, read reddit reviews, read reviews on Amazon, and watch YouTube videos until you find the tools that are best for you. Ask me for advice too!

Recommended Tools, Supplies, & Equipment

- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet/Smartphone
- Chromebook
- Windows laptop/Mac laptop/Linux laptop
- Windows desktop/Mac desktop/Linux desktop
- Windows Server with Active Directory and Print Management

- Monitors
- Projectors
- SOHO router/switch
- Access point
- VoIP phone
- Printer - Laser/inkjet - Wireless - 3D printer
- Surge suppressor
- UPS
- VR headset
- Smart devices (IoT devices)

- Motherboards

- RAM
- Hard drives
- Power supplies
- Video cards
- Sounds cards
- Network cards
- Wireless NICs
- Fans/cooling devices/heat sink
- CPUs
- Assorted connectors/cables
- Adapters
- Network cables
- Unterminated network cables/connectors
- AC adapters
- Optical drives
- Screws/stand-offs
- Cases
- Maintenance kit
- Mice/keyboards
- KVM
- Console cable TOOLS
- Screw drivers
- Multimeter
- Wire cutters
- Punchdown tool
- Crimper
- Power supply tester
- Cable stripper
- Standard technician toolkit
- ESD strap
- Thermal paste

- Cable tester
- Cable toner
- Wi-Fi analyzer
- SATA to USB connectors SOFTWARE
- Operating systems - Linux - Chrome OS - Microsoft Windows - Mac OS - Android – iOS
- PE Disk/Live CD
- Antivirus software
- Virtualization software
- Anti-malware
- Driver software

Acronyms Used in This Book

AC	Alternating Current
ACL	Access Control List
ACPI	Advanced Configuration Power Interface
ADF	Automatic Document Feeder
ADSL	Asymmetrical Digital Subscriber Line
AES	Advanced Encryption Standard
AHCI	Advanced Host Controller Interface
AP	Access Point
APIPA	Automatic Private Internet Protocol Addressing
APM	Advanced Power Management
ARP	Address Resolution Protocol
ASR	Automated System Recovery
ATA	Advanced Technology Attachment
ATAPI	Advanced Technology Attachment Packet Interface
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy
A/V	Audio Video
BD-R	Blu-ray Disc Recordable
BIOS	Basic Input/Output System
BD-RE	Blu-ray Disc Rewritable
BNC	Bayonet-Neill-Concelman
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAD	Computer-Aided Design
CAPTCHA	Completely Automated Public Turning Test to tell Computers and Humans Apart
CD	Compact Disc
CD-ROM	Compact Disc-Read-Only Memory

CD-RW	Compact Disc-Rewritable
CDFS	Compact Disc File System
CERT	Computer Emergency Response Team
CFS	Central File System Common File System Command File System
CGA	Computer Graphics and Applications
CIRD	Classless Inter-Domain Routing
CIFS	Common Internet File System
CMOS	Complementary Metal-Oxide Semiconductor
CNR	Communications and Networking Riser
COMX	Communication Port (x=Port Number)
CPU	Central Processing Unit
CRT	Cathode-Ray Tube
DaaS	Data as a Service
DAC	Discretionary Access Control
DB-25	Serial Communications D-Shell Connector, 25 pins
DB-9	Serial Communications D-Shell Connector, 9 pins
DBaaS	Database as a Service
DC	Direct Current
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DDR RAM	Double Data Rate Random Access Memory
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DIN	Deutsche Industrie Norm
DLT	Digital Linear Tape
DLP	Digital Light Processing Data Loss Prevention
DMA	Direct Memory Access

DMZ	Demilitarized Zone
DNS	Domain name Service Domain Name Server
DoS	Denial of Service
DRAM	Dynamic Random Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
DVD-RAM	Digital Versatile Disc-Random Access Memory
DVD-ROM	Digital Versatile Disc-Read Only Memory
DVD-R	Digital Versatile Disc-Recordable
DVD-RW	Digital Versatile Disc-Rewritable
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
ECP	Extended Capabilities Port
EEPROM	Electrically Erasable Programmable Read-Only Memory
EFS	Encrypting File System
EIDE	Enhanced Integrated Drive Electronics
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EPROM	Erasable Programmable Read-Only Memory
EPP	Enhanced Parallel Port
ERD	Emergency Repair Disk
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End User License Agreement
EVGA	Extended Video Graphics Adapter/Array
Ext2	Second Extended File System
exFAT	Extended File Allocation Table
FAT	File Allocation Table

FAT12	12-Bit File Allocation Table
FAT16	16-Bit File Allocation Table
FAT32	32-Bit File Allocation Table
FDD	Floppy Disk Drive
FPM	Fast Page Mode
FSB	Front-Side Bus
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GDDR	Graphics Double Data Rate
GDI	Graphics Device Interface
GUI	Graphical User Interface
GUID	Globally Unique Identifier
GPS	Global Positioning System
GPT	GUID Partition Table
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
HAL	Hardware Abstraction Layer
HAV	Hardware Assisted Virtualization
HCL	Hardware Compatibility List
HDCP	High-Bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High Definition Media Interface
HIPS	Host Intrusion Prevention System
HPFS	High Performance File System
HTML	Hypertext Markup Language
HTPC	Home Theater PC
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IMAP	Internet Mail Access Protocol
IMEI	International Mobile Equipment Identify
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPConfig	Internet Protocol Configuration
IPP	Internet Printing Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
IRQ	Interrupt Request
ISA	Industry Standard Architecture
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
JBOD	Just a Bunch of Disks
KB	Knowledge Base
KVM	Kernel-based Virtual Machine Keyboard-Video-Mouse
LAN	Local Area Network
LBA	Logical Block Addressing
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LPD/LPR	Line Printer Daemon/Line Printer Remote
LPT	Line Printer Terminal
LVD	Low Voltage Differential

MAC	Media Access Control Mandatory Access Control
MAN	Metropolitan Area Network
MAPI	Messaging Application Programming Interface
mATX	Micro Advanced Technology Extended
MAU	Media Access Unit/Media Attachment Unit
MRB	Master Boot Record
MBSA	Microsoft Baseline Security Analyzer
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Product
MicroDIMM	Micro Dual Inline Memory Module
MIDI	Musical Instrument Digital Interface
MIME	Multipurpose Internet Mail Extension
MIMO	Multiple Input Multiple Output
MP3	Moving Picture Experts Group Layer 3 Audio
MP4	Moving Picture Experts Group Layer 4
MPEG	Moving Picture Experts Group
MSConfig	Microsoft Configuration
MSDS	Material Safety Data Sheet
MT-RJ	Mechanical Transfer Registered Jack
MUI	Multilingual User Interface
NaaS	Network as a Service
NAC	Network Access Control
NAS	Network-Attached Storage
NAT	Network Address Translation
NetBIOS	Networked Basic Input/Output System
NetBEUI	Networked Basic Input/Output System Extended User Interface
NFC	Near Field Communication
NFS	Network File System
NIC	Network Interface Card

NiCd	Nickel Cadmium
NiMH	Nickel Metal Hydride
NLX	New Low-profile Extended
NNTP	Network News Transfer Protocol
NTFS	New Technology File System
NTLDR	New Technology Loader
NTP	Network Time Protocol
NTSC	National Transmission Standards Committee
NVMe	Non-Volatile Memory Express
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
OLED	Organic Light Emitting Diode
OS	Operating System
PaaS	Platform as a Service
PAL	Phase Alternating Line
PAN	Personal Area Network
PAT	Port Address Translation
PC	Personal Computer
PCI	Peripheral Component Interconnect Payment Card Industry
PCIe	Peripheral Component Interconnect Express
PCIX	Peripheral Component Interconnect Extended
PCL	Printer Control Language
PCMCIA	Personal Computer Memory Card International Association
PE	Preinstallation Environment
PGA	Pin Grid Array
PGA2	Pin Grid Array 2
PGP	Pretty Good Protection
PII	Personally Identifiable Information
PIN	Personal Identification Number
PHI	Personal Health Information
PKI	Public Key Infrastructure

PnP	Plug and Play
PoE	Power over Ethernet
POP3	Post Office Protocol 3
PoS	Point of Sale
POST	Power-On Self-Test
POTS	Plain Old Telephone Service
PPM	Pages Per Minute
PPP	Point-to-Point Protocol
PPTP	Pont-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PROM	Programmable Read-Only Memory
PS/2	Personal System/2 Connector
PSTN	Public Switched Telephone Network
PSU	Power Supply Unit
PVA	Patterned Vertical Alignment
PVC	Permanent Virtual Circuit
PXE	Preboot Execution Environment
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Server
RAID	Redundant Array of Independent Disks Redundant Array of Inexpensive Disks
RAM	Random Access Memory
Ras	Remote Access Service
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio Frequency Interface
RFID	Radio Frequency Identification
RGB	Red Green Blue
RIP	Routing Information Protocol
RIS	Remote Installation Service
RISC	Reduced Instruction Set Computer
RJ-11	Registered Jack Function 11
RJ-45	Registered Jack Function 45

RMA	Returned Materials Authorization
ROM	Read-Only Memory
RPO	Recovery Point Objective
RTC	Real-Time Clock
RT	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SC	Subscription Channel
SCP	Secure Copy Protection
SCSI	Small Computer System Interface
SCSI ID	Small Computer System Interface Identifier
SD Card	Secure Digital Card
SEC	Single Edge Connector
SFC	System File Checker
SFF	Small Form Factor
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SIMM	Single In-Line Memory Module
SLI	Scalable Link Interface System Level Integration Scanline Interleave Mode
SMART	Self-Monitoring, Analysis and Reporting Technology
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SoDIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SP	Service Pack
SPDIF	Sony-Philips Digital Interface Format
SPGA	Staggered Pin Grid Array

SRAM	Static Random Access Memory
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
SXGA	Super Extended Graphics Array
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDR	Time Domain Reflectometer
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TN	Twisted Nematic
TPM	Trusted Platform Module
UAC	User Account Control
UDF	User Defined Functions Universal Disk Format Universal Data Format
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USMT	User State Migration Tool
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair

UXGA	Ultra Extended Graphics Array
VA	Vertical Alignment
VDC	Volts DC
VDI	Virtual Desktop Infrastructure
VESA	Video Electronics Standards Association
VFAT	Virtual File Allocation Table
VGA	Video Graphics Array
VLAN	Video LAN
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random Access Memory
WAN	Wide Area Network
WAP	Wireless Access Protocol Wireless Access Point
WEP	Wired Equivalent Privacy
WIFI	Wireless Fidelity
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WAP	Wireless Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup
WUXGA	Wide Ultra Extended Graphics Array
WWAN	Wireless Wide Area Network
XGA	Extended Graphics Array
ZIP	Zero-Insertion-Force
ZIP	Zigzag Inline Package

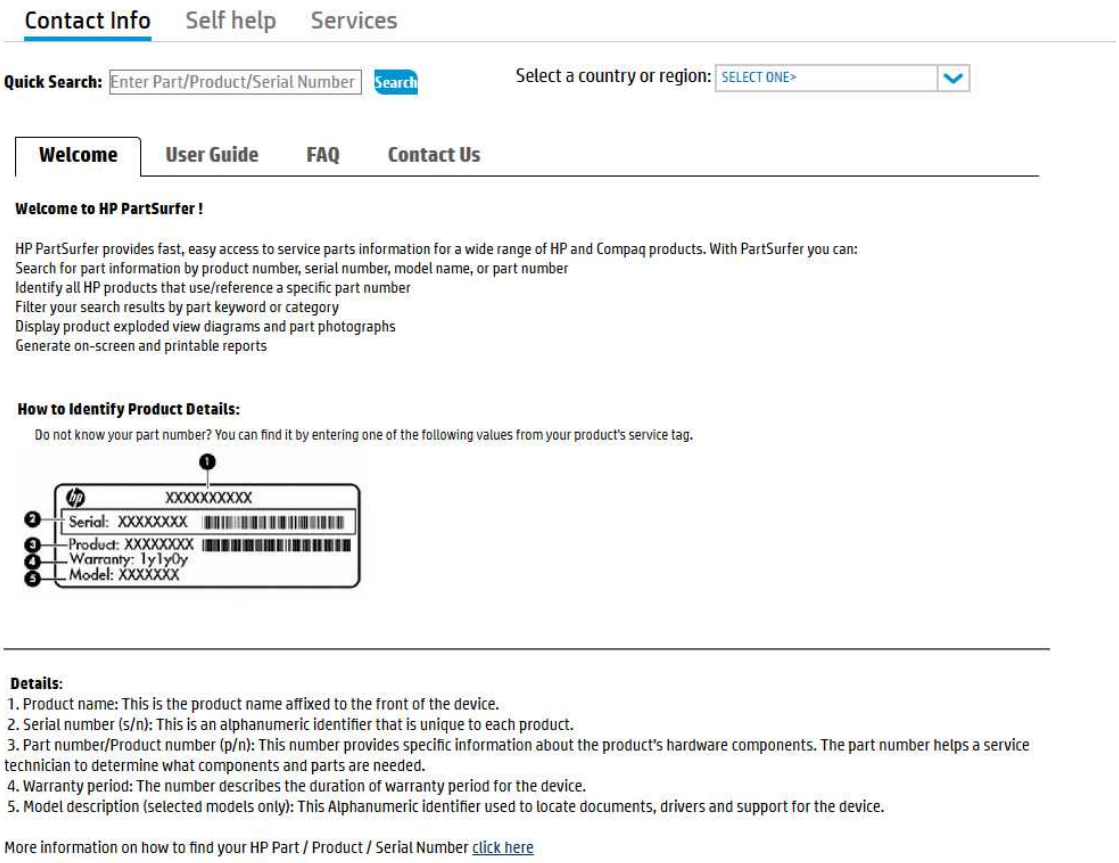
Part B: 220-1001 1.0 Mobile Devices

1.1 Given a scenario, install and configure laptop hardware and components.

- *Hardware/device replacement*
    - *Keyboard*
    - *Hard drive*
        - *SSD vs. hybrid vs. magnetic disk*
        - *1.8in vs. 2.5in*
    - *Memory*
    - *Smart card reader*
    - *Optical drive*
    - *Wireless card/Bluetooth module*
    - *Cellular card*
    - *Video card*
    - *Mini PCIe*
    - *Screen*
    - *DC jack*
    - *Battery*
    - *Touchpad*
    - *Plastics/frames*
    - *Speaker*
    - *System board*
    - *CPU*

Some Quick Tips for Replacing Laptop Components:

1. Safety First! It's a good idea to
    a. Wear an electrostatic wrist strap
    b. Remove the battery
    c. Ensure that the laptop is not plugged in
2. Make sure that the replacement part is compatible with the laptop. You can look up replacement parts from the manufacturer's website. For example, on an HP laptop, you can look up replacement part numbers with HP Part Surfer (http://partsurfer.hp.com/). You can look up parts by serial number or model number.



Welcome to HP PartSurfer !

HP PartSurfer provides fast, easy access to service parts information for a wide range of HP and Compaq products. With PartSurfer you can:
Search for part information by product number, serial number, model name, or part number
Identify all HP products that use/reference a specific part number
Filter your search results by part keyword or category
Display product exploded view diagrams and part photographs
Generate on-screen and printable reports

How to Identify Product Details:

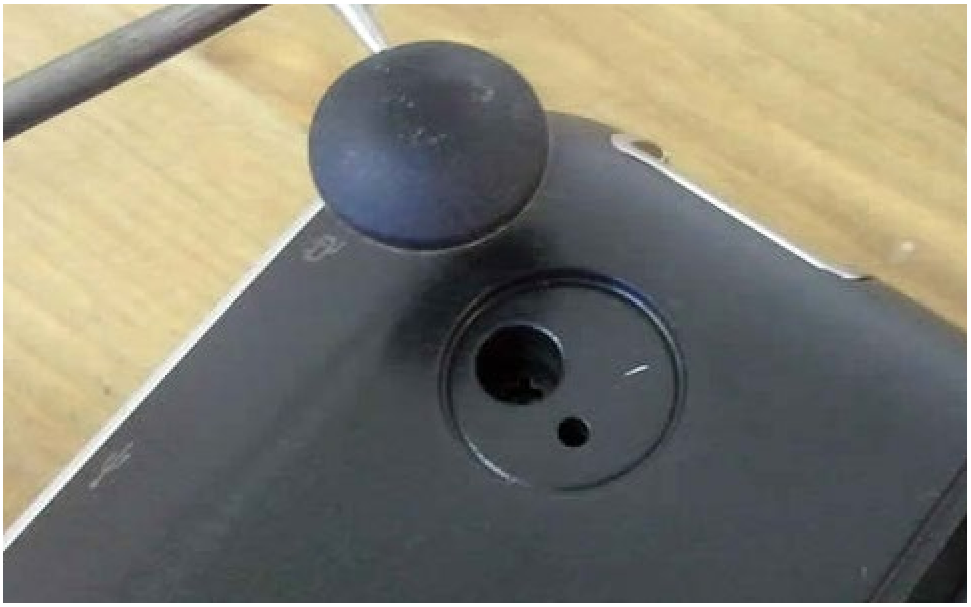
Do not know your part number? You can find it by entering one of the following values from your product's service tag.

Details:
1. Product name: This is the product name affixed to the front of the device.
2. Serial number (s/n): This is an alphanumeric identifier that is unique to each product.
3. Part number/Product number (p/n): This number provides specific information about the product's hardware components. The part number helps a service technician to determine what components and parts are needed.
4. Warranty period: The number describes the duration of warranty period for the device.
5. Model description (selected models only): This Alphanumeric identifier used to locate documents, drivers and support for the device.

More information on how to find your HP Part / Product / Serial Number click here

3. Locate the maintenance manual for your laptop (available online or through the manufacturer). Laptops can be tricky to open. It is always helpful to know how components fit together. Many laptops contain hidden cables or screws.

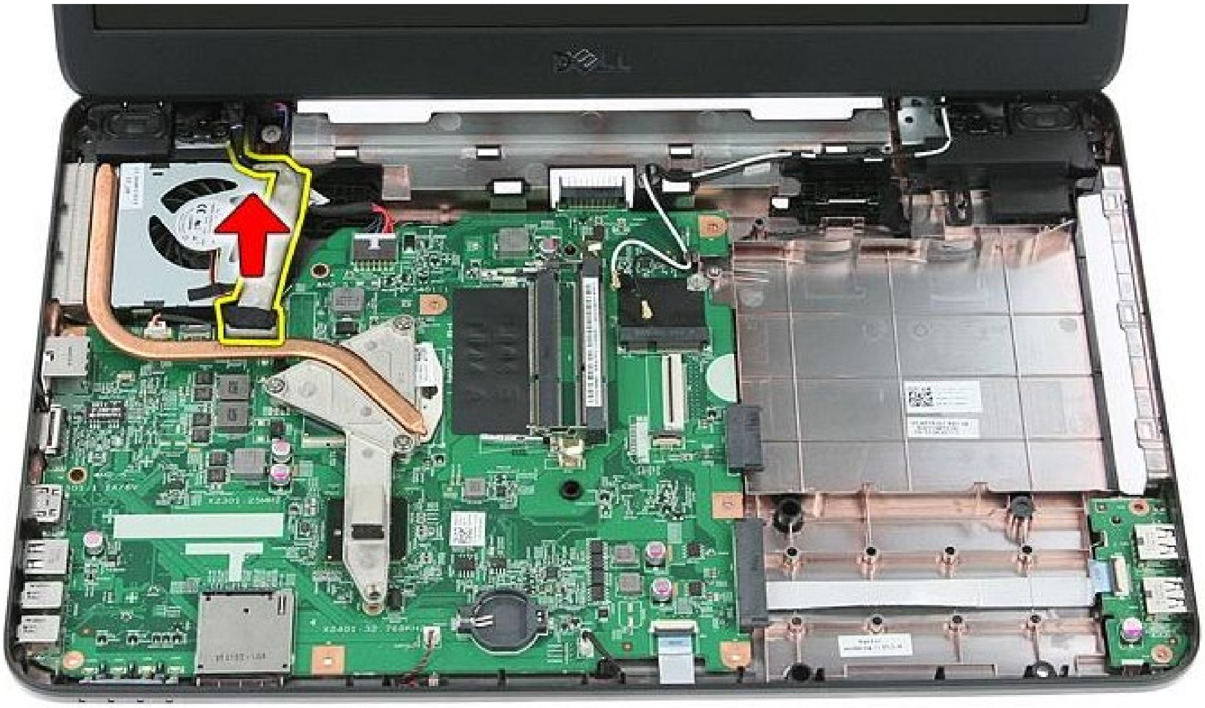
4. Check the warranty status of the laptop. If the laptop is under warranty, you may be able to obtain replacement parts and/or service at no cost.
5. Make sure that you have the correct tools
    a. Screw drivers with different bits (some newer laptops contain small star-shaped screws)
    b. Spudger and guitar picks to remove plastic components
6. Each time you remove a screw, you should label it with the location from where it was removed. A typical laptop will have five to ten different types of screws, and it might be difficult to tell them apart (for example a 2.5mm screw and a 3mm screw). It is important that the screws go back exactly where they came from.
7. Some screws are hidden under stickers or rubber pads, especially on the bottom of the laptop.



8. Increasingly, laptops are designed to be smaller and thinner. Thinner/smaller laptops are more difficult to repair. Take note of the following
    a. Manufacturers of “gaming” laptops are typically repair and upgrade friendly
    b. Other companies (like Apple) will not sell repair parts to third parties. Only aftermarket parts are available. The government may block the import of aftermarket parts.
    c. Other laptop design changes

        i. Having an internal battery (more difficult to change, but also reduces the weight of the laptop)
        ii. Integrating more components into the system board. For example, the MacBook Pro's SSD, Memory, and Processor are soldered into the system board. If any of those components fails, the entire system board will have to be replaced.

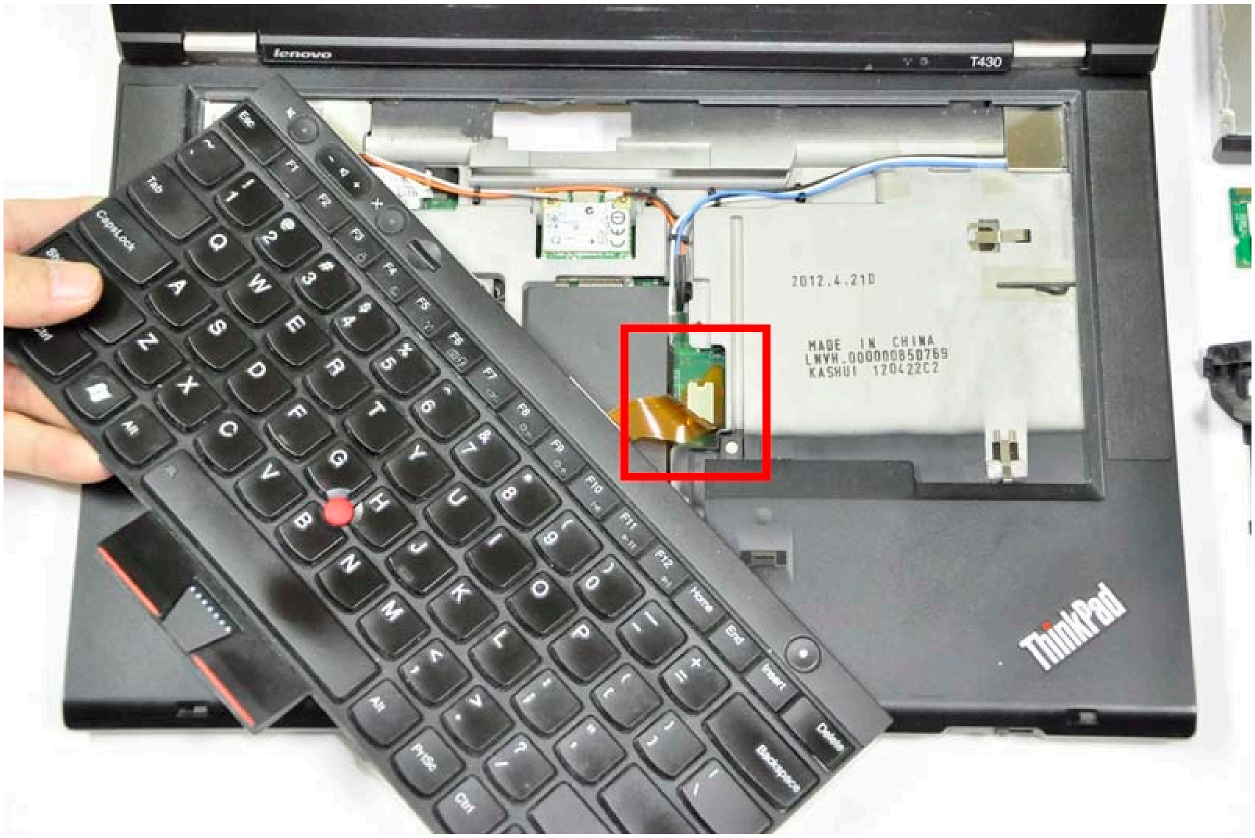
9. Consider whether the laptop is "consumer-grade" or "business-grade".
    a. Examples of consumer grade laptops include the HP Envy
    b. Examples of business-grade laptops include the Lenovo ThinkPad, and the HP EliteBook
    c. Business grade laptops are designed to be easier to repair (they have more accessibility panels and less tools are required)
    d. Many business grade laptops come with 3-year warranties and include on site service. Check the warranty status first.
10. Drivers
    a. In most cases, Windows will automatically detect the new hardware and install the correct driver
    b. It is good to download the correct driver from the manufacturer's website before installation
    c. The component that will cause the most driver issues is the solid-state drive. You should copy the new driver to a USB key before you install a solid-state drive.
11. Determine if the system board is mounted to the top or the bottom of the laptop
    a. If the system board is mounted to the bottom cover
        i. To access the board, you must remove the top cover and keyboard
        ii. Most older model laptops have their system boards mounted to the bottom cover
        iii. You can access some components (CMOS battery, RAM, Wi-Fi card, HDD) from the access panels
        iv. To access the system board, you must remove the keyboard and cover



b. If the system board is mounted to the top cover
    i. To access the system board, you must remove the bottom cover
    ii. You may need to remove other components (HDD, battery, fan) to access the system board

Replacing a Laptop Keyboard

1. Typically, a laptop keyboard has tabs which hold it in place.
2. The keyboard has a sensitive ribbon cable, which connects it to a ZIF connector underneath.
3. Use a spudger or flathead screw driver to lift the keyboard out of the laptop frame.
4. Remove the ribbon cable from the ZIF connector
5. Insert the new keyboard ribbon cable into the ZIF connector
6. Insert the keyboard tabs into the laptop frame and push down to secure it



Replacing a Laptop Hard Drive

There are three types of laptop hard drives

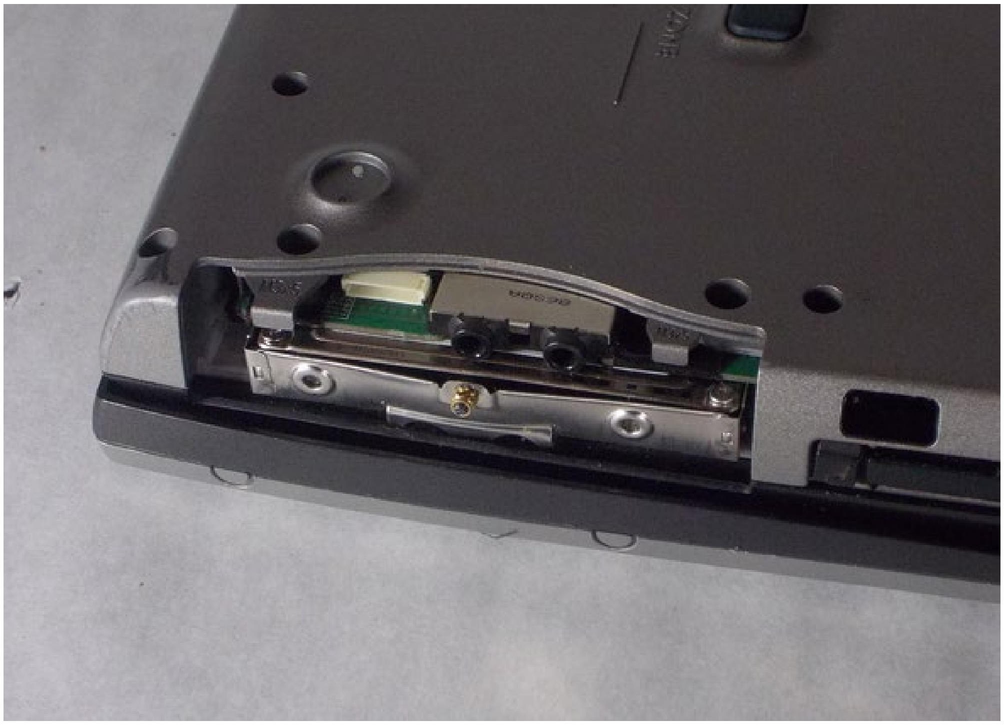
- SSDs
    - An SSD (or Solid-State Drive) contains flash memory.
    - The drive has no moving parts.
    - SSDs operate faster than traditional hard disk drives.
    - SSDs are more expensive.
    - There are several different form-factors of SSDs (discussed later)
- Magnetic Disk
    - A traditional Hard Disk Drive contains glass platters which store the data.
    - The platters rotate at 5400 rpms or more.
    - The drive contains a probe, which stores/reads data on the platters.
    - Magnetic Disks are slower than SSDs.
    - Magnetic disks are less expensive.
    - Laptop magnetic disks only come in a 2.5″ form-factor or a 1.8″ form-factor
- Hybrid
    - A hybrid drive is a magnetic drive with a small amount of flash memory (usually 32GB).
    - Data is stored on the platters.
    - Data that is accessed frequently is stored on the flash memory as well
    - A hybrid drive costs almost the same as a magnetic drive, but offers better performance

Replace a laptop HDD

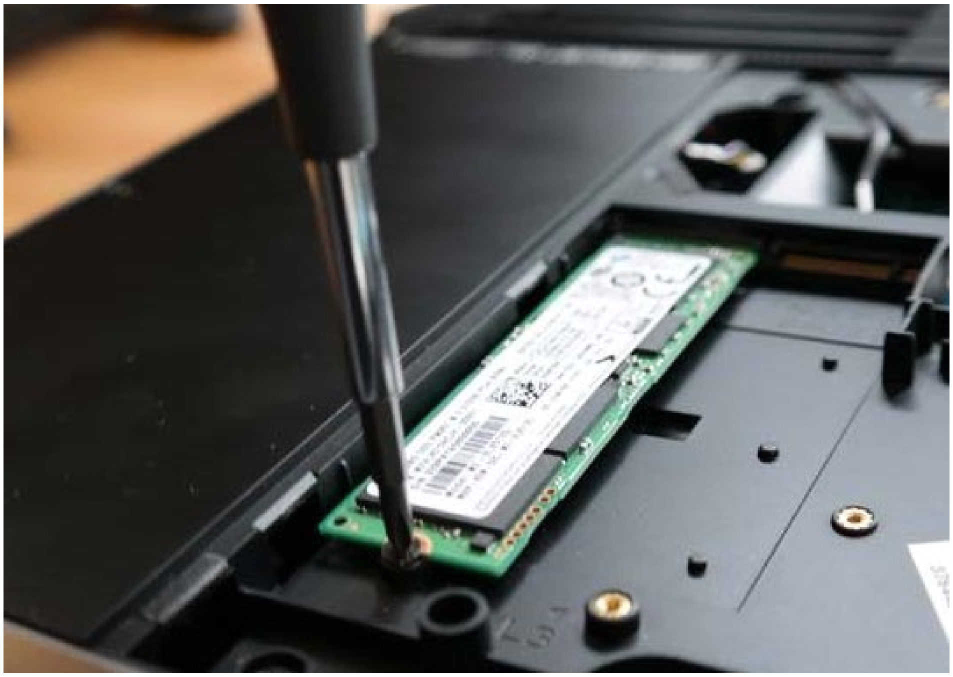
- If the HDD is a 2.5″ form factor
    - On a consumer-grade laptop and some business-grade laptops
        - The HDD is typically located underneath an access panel (may be labelled)
        - Remove the access panel
        - The HDD is sits inside a groove or rubber/metal/plastic bracket
        - Remove the connection cable from the HDD
        - Remove the HDD from the groove and/or bracket

        - Insert the new HDD into the bracket
        - Reconnect the connection cable
        - Close the access panel

    - On some business-grade laptops
        - The HDD might sit inside a slot on the side of the laptop
        - The HDD is secured with a screw
        - Remove the screw and slide out the old HDD
        - Insert the new HDD, and reinsert the screw



- If the SSD is a special form-factor (like an NVMe form-factor)
  - Remove the access panel
  - Remove the screw holding the SSD to the system board
  - Remove the SSD from the slot in the system board
  - Insert the new SSD into the system board
  - Insert the screw
  - Reinstall the access panel

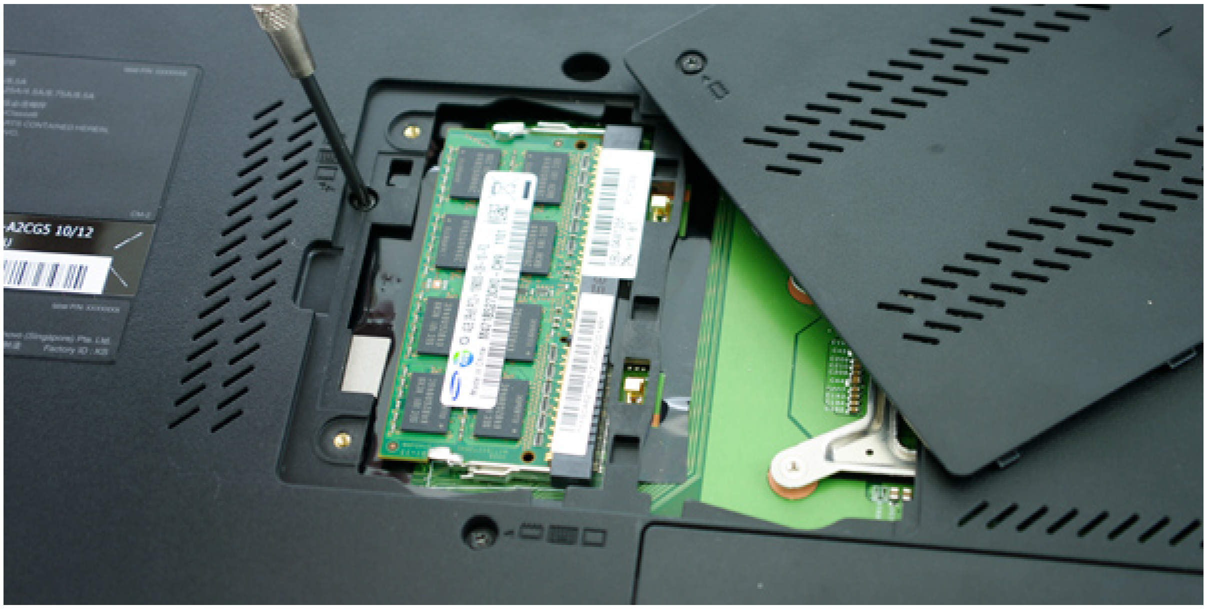


Laptop Hard Disk Drive Sizes

- 1.8″
    - Not common
    - Found in ultralight laptops
    - You can install a 1.8″ drive in a 2.5″ drive bay, with an adapter
- 2.5″
    - Most popular and readily available format
    - Most laptops contain 2.5-inch drives

Replacing Laptop Memory

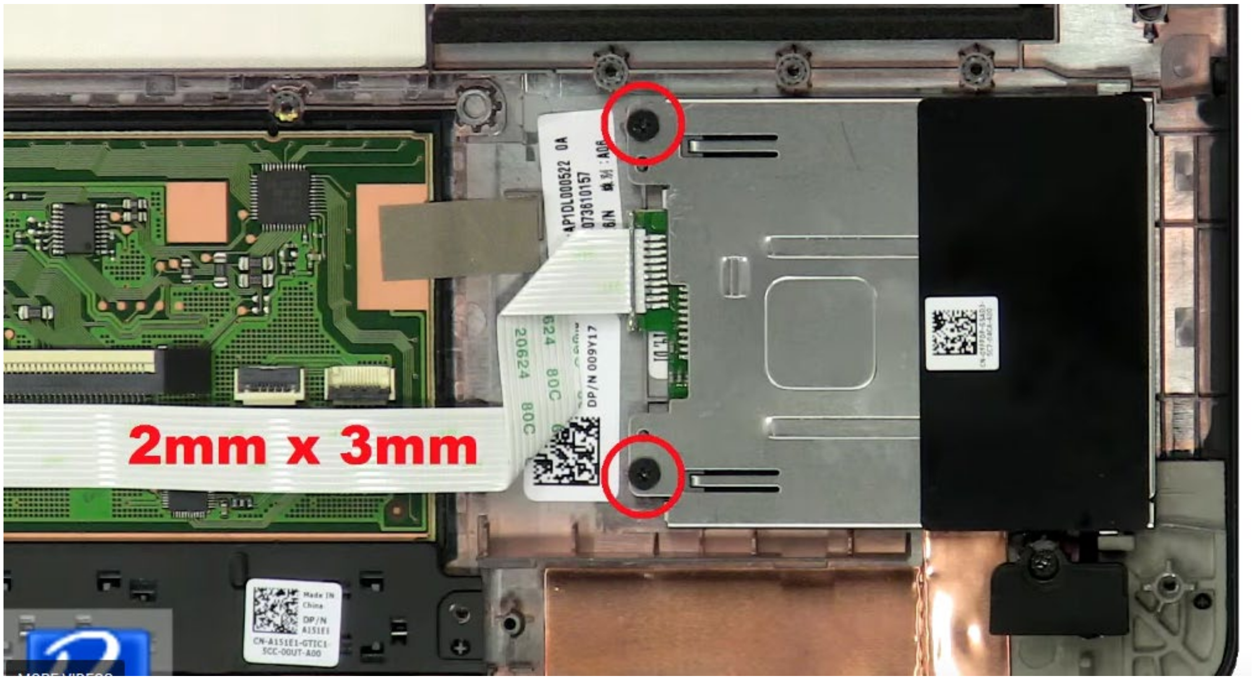
1. Make sure that
   a. Your laptop supports the amount of RAM you plan to add (4GB, 8GB, etc.)
   b. You have the correct number of RAM sticks
   c. You have the correct type of RAM (DDR3, DDR4, etc.)
2. If you're not sure what kind of RAM you require, you can check online
   a. Check with the manufacturer
   b. Check with the RAM retailer
   c. Check the existing computer to see what kind of RAM is installed
3. Remove the access panel from the bottom of the laptop
4. Remove the memory from its connector, by pushing the tabs outward
5. Pull the memory upward
6. Insert the new memory into the connector and push down until it snaps into place
7. Reinstall the access panel



Replacing Laptop Smart Card Reader

1. Determine if the smart card reader can be replaced
    a. If the smart card reader is a separate component, it can be replaced
    b. If the smart card reader is integrated into the system board, then the entire system board will have to be replaced
2. Remove the bottom cover

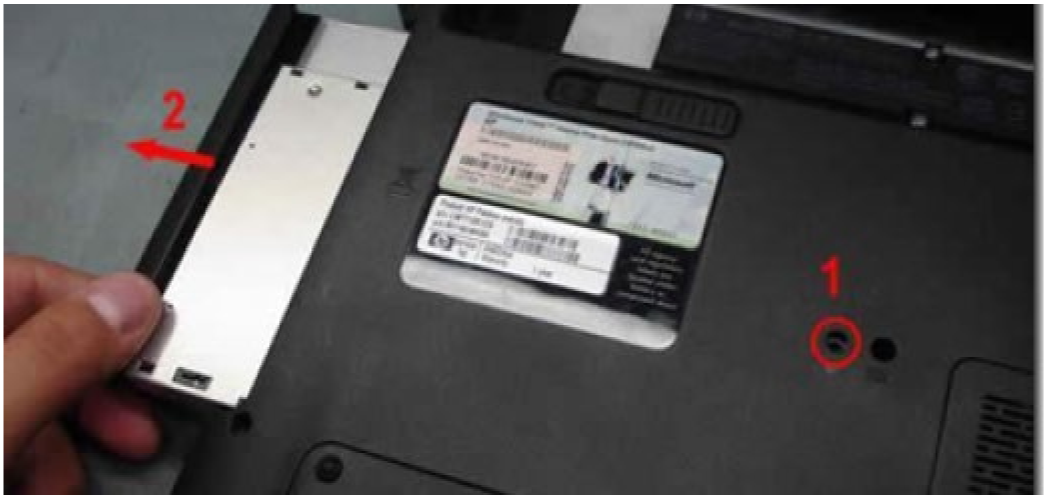
3. Remove any components that are covering the smart card
4. Unplug the smart card reader from its cable
5. Unscrew the smart card reader
6. Remove the smart card reader
7. Install the new smart card reader and insert the screws
8. Plug the new smart card reader into the cable



9. Reinstall any components that were covering the smart card
10. Reinstall the bottom cover

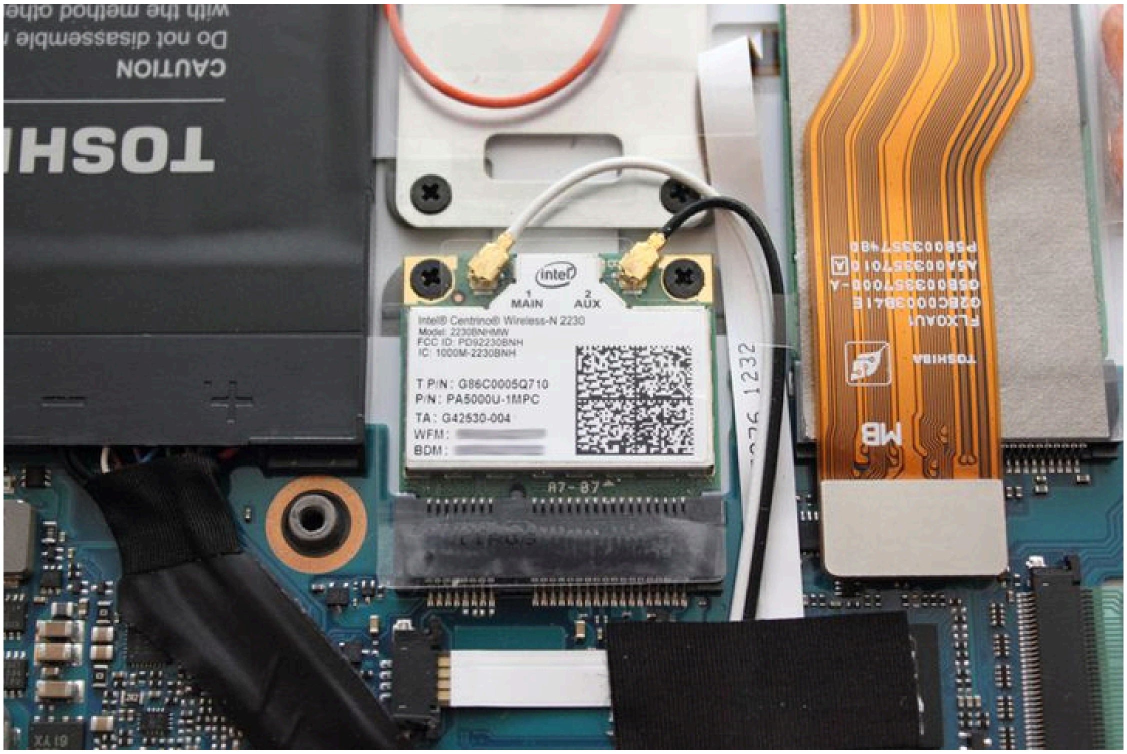
Optical Drive Replacement

1. The optical drive is typically held in by one screw
    a. If the screw is accessible from outside of the laptop, remove the screw
    b. If the screw is accessible from inside the laptop, remove the bottom cover, then remove the screw
2. Slide the drive out of the laptop.
3. Slide the new drive in.
4. Reinsert the screw.
5. Reinstall the bottom panel, if removed
6. The optical drive may have a plastic cover, which may need to be swapped



Wireless Card/Bluetooth Module Replacement

1. Determine if the wireless card is integrated into the system board or if it is a separate component
    a. If it is a separate component, it can be replaced
    b. The wireless card is connected to the system board.
2. Remove
    a. The access panel at the bottom of the laptop or
    b. Remove the bottom cover, depending on where the Wi-Fi card is located
3. Remove the antennas that are connected to the wireless card. There are typically two antennas, but there may be one or three.
4. The wireless card may be held by a couple of screws. Remove the screws.
5. Remove the wireless card from its connector.
6. Install the new wireless card in the connector.
7. Secure the card with screws, if required.
8. Reinstall the antennas.
9. Reinstall the access panel or bottom cover.

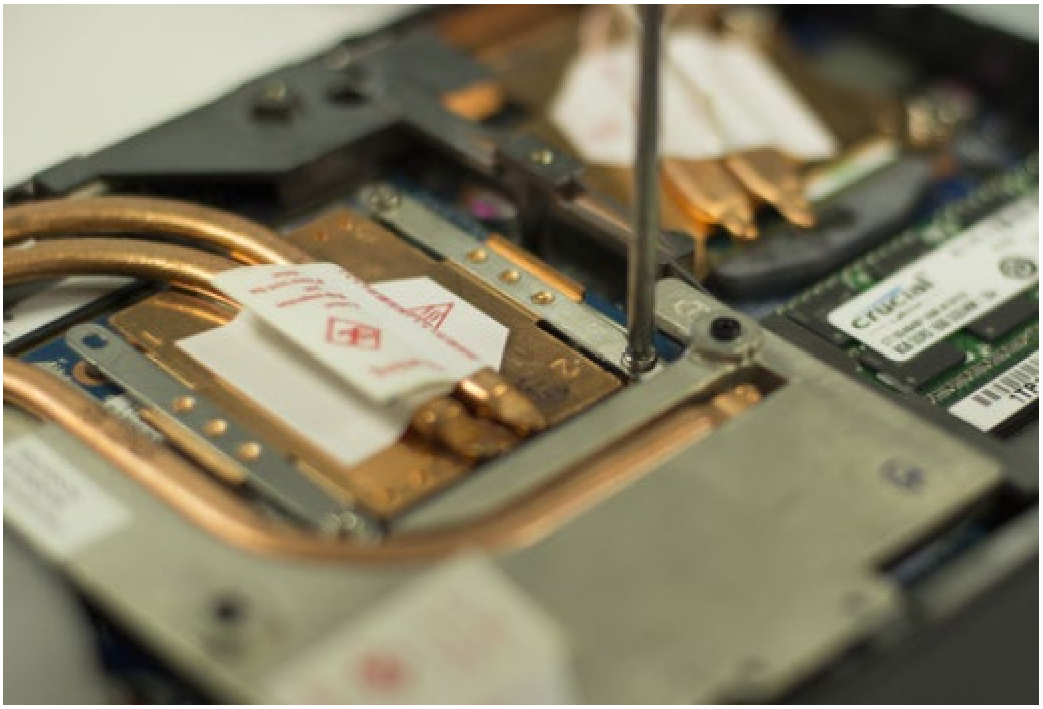


Cellular Card Replacement

1. The cellular card removal/reinstallation is like the wireless card removal/reinstallation
2. Determine if the cellular card is integrated into the system board or if it is a separate component
    a. If it is a separate component, it can be replaced
    b. The cellular card is connected to the system board.
3. Remove
    a. The access panel at the bottom of the laptop or
    b. Remove the bottom cover, depending on where the Wi-Fi card is located
4. Remove the two antennas that are connected to the cellular card.
5. The cellular card may be held by a couple of screws. Remove the screws.
6. Remove the cellular card from its connector.
7. Install the new cellular card in the connector.
8. Secure the card with screws, if required.
9. Reinstall the antennas.
10. Reinstall the access panel or bottom cover.

Video Card Replacement

1. Determine if the laptop has an integrated video chip or a dedicated video chip, and determine if it can be removed
    a. An integrated video chip is part of the system's processor
    b. A dedicated video chip is separate, but many chips are soldered directly onto the system board and can't be removed
    c. Laptops with upgradable GPUs have an MXM module
2. Remove the bottom cover
3. Remove the heat pipes from on top of the chip (they are held in by screws)



4. Remove the GPU chip
5. Clean the thermal paste from the heat pipes
6. Install the new GPU chip, being careful to make sure that it is oriented correctly
7. Apply thermal paste
8. Install the heat pipe and reinsert the screws
9. Reinstall the top cover

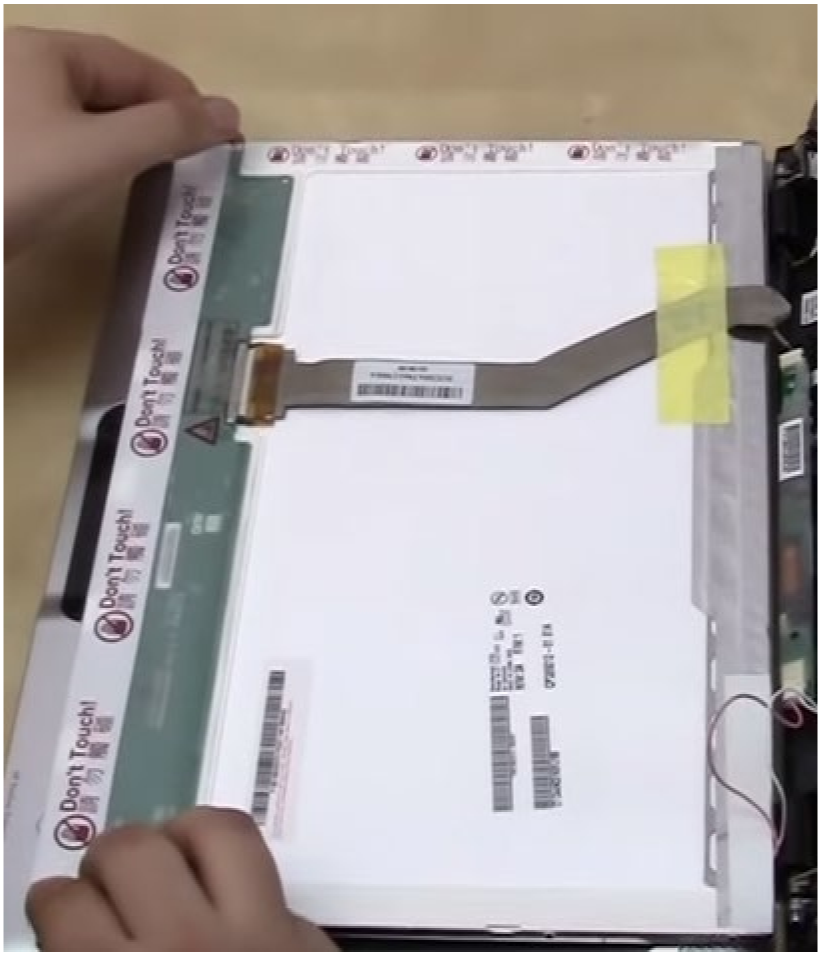
Mini PCIe Replacement

1. Mini PCIe is a card format
2. Mini PCIe is also known as PCIe Mini, PCI Express Mini, Mini-PCI Express or Mini-PCI-e
3. Cards available in the Mini PCIe format include Wi-Fi cards and cellular cards
4. The Mini PCIe card slot is integrated into the system board and can't be replaced separately

Screen Replacement

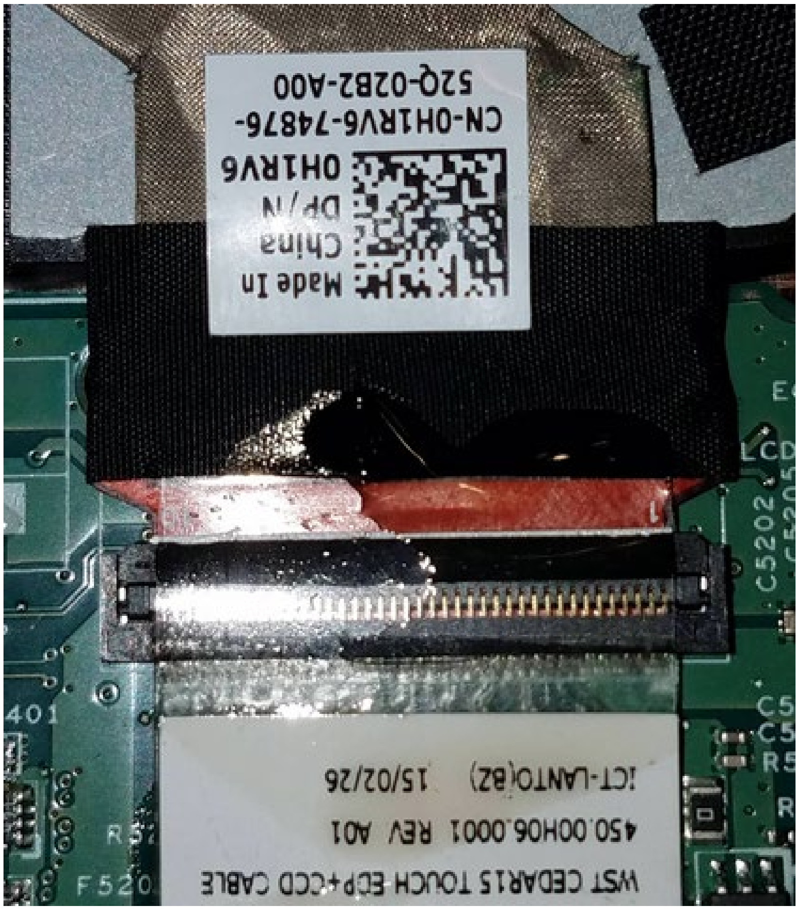
1. Many manufacturers sell a replacement laptop "screen assembly", which is basically the top half of the laptop (screen, bezel, camera, touch digitizer, and hinges). It might be easier to replace the entire assembly, especially if multiple components are damaged
2. Wiring for the screen is routed through the laptop hinge and connects into the system board
3. To replace just the laptop screen
    a. Determine if the screen has a bezel (rectangular plastic that surrounds the screen). This is common on laptops without touch capabilities
4. If the screen has a bezel
    a. Remove the bezel (rectangular plastic that surrounds the screen

    b. Remove the screen from the top assembly. You may need to remove screws that hold it in place.



   c. Disconnect the ribbon cables from the screen
   d. Connect the cables to the new screen
   e. Reinstall the new screen
   f. Reinstall the bezel

5. If the screen does not have a bezel (certain models of laptops), or if you also need to replace the video cable
   a. You may need to remove the bottom cover
   b. Disconnect the cable from the motherboard

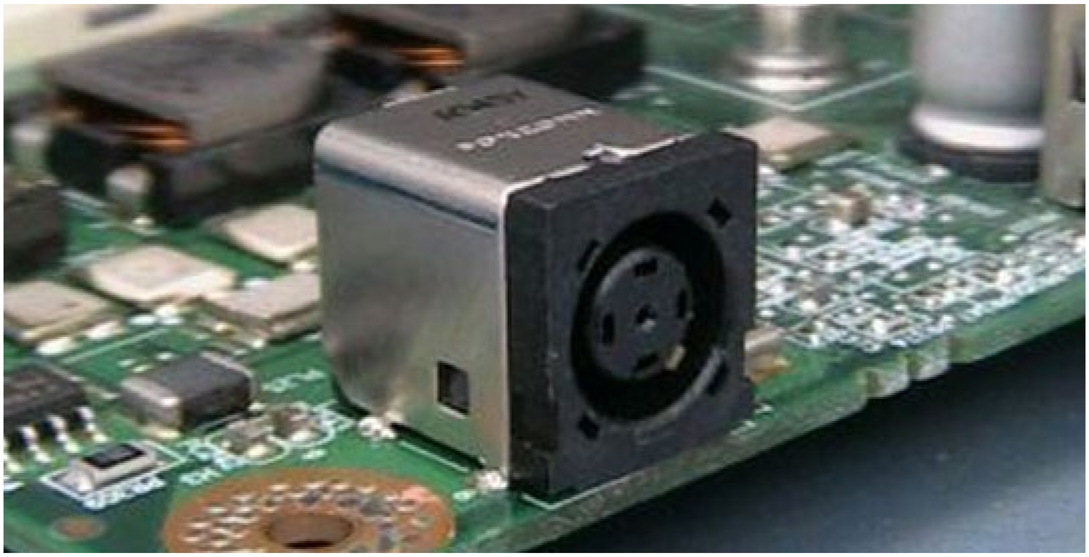


   c. Route the cable through the hinge
   d. You may need to pry the top cover from the screen
   e. Unscrew the existing screen
   f. Install the new screen
   g. Reroute the cable through the hinge
   h. Connect the cable to the motherboard
   i. Reinstall the bottom cover

6. If the laptop has touch capabilities
   a. The LCD screen will have a glass digitizer on top of it
   b. The glass may crack easily
   c. The glass digitizer may be screwed to the screen, or it may be glued to the LCD
      i. If it is glued, you may need to use a heat gun to melt the glue in order to remove it

DC Jack Replacement

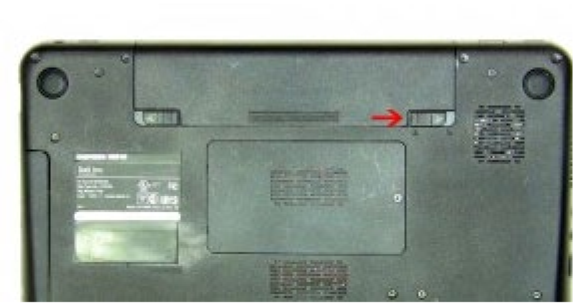
1. The DC jack is part of the system board



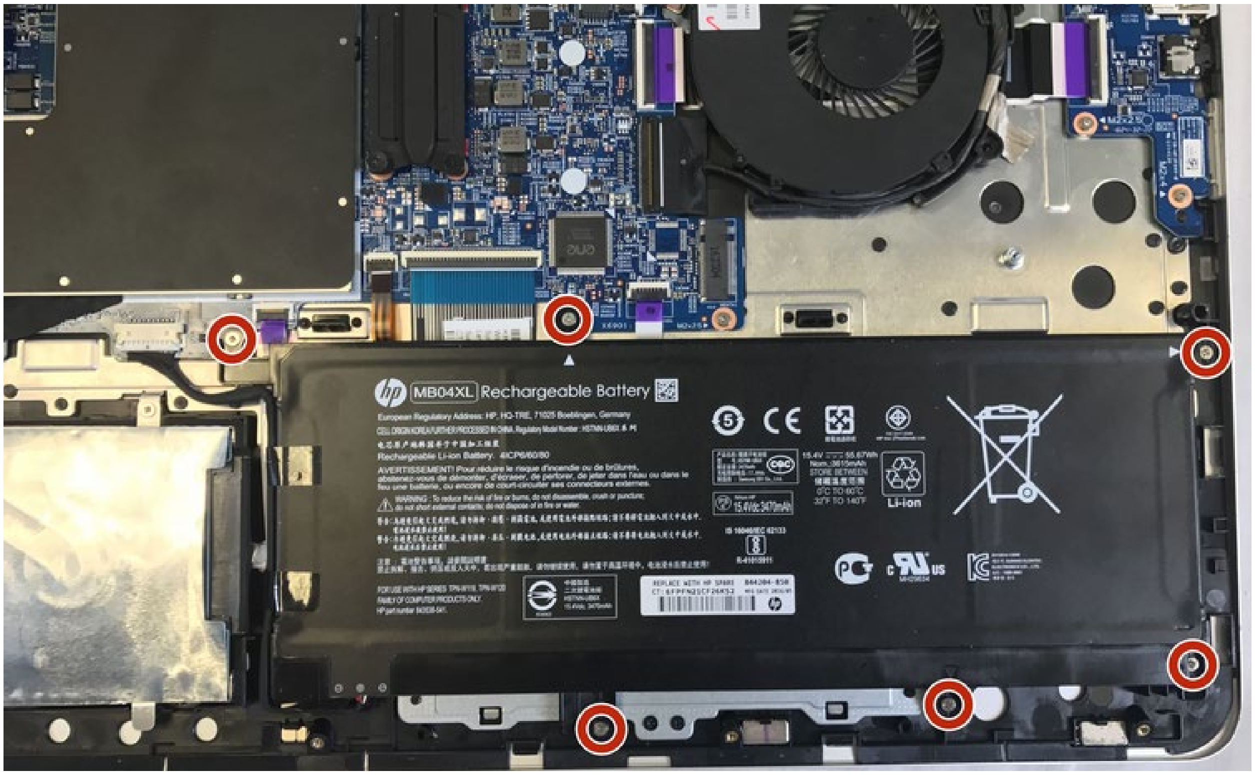
2. You can either
    a. Desolder and resolder the DC jack
    b. Replace the entire system board (most likely option)
3. To access the DC jack
    a. Remove the bottom cover
    b. Remove all the components on the system board (including the processor, memory, Wi-Fi cards)
    c. Remove all the connection cables from the system board
    d. Unscrew the system board from the laptop
    e. Desolder the DC jack
    f. Resolder a new DC jack
    g. Reinstall the system board
    h. Reinstall the connection cables
    i. Reinstall the system board components (including the processor, memory, Wi-Fi cards)
    j. Reinstall the bottom cover

Battery Replacement

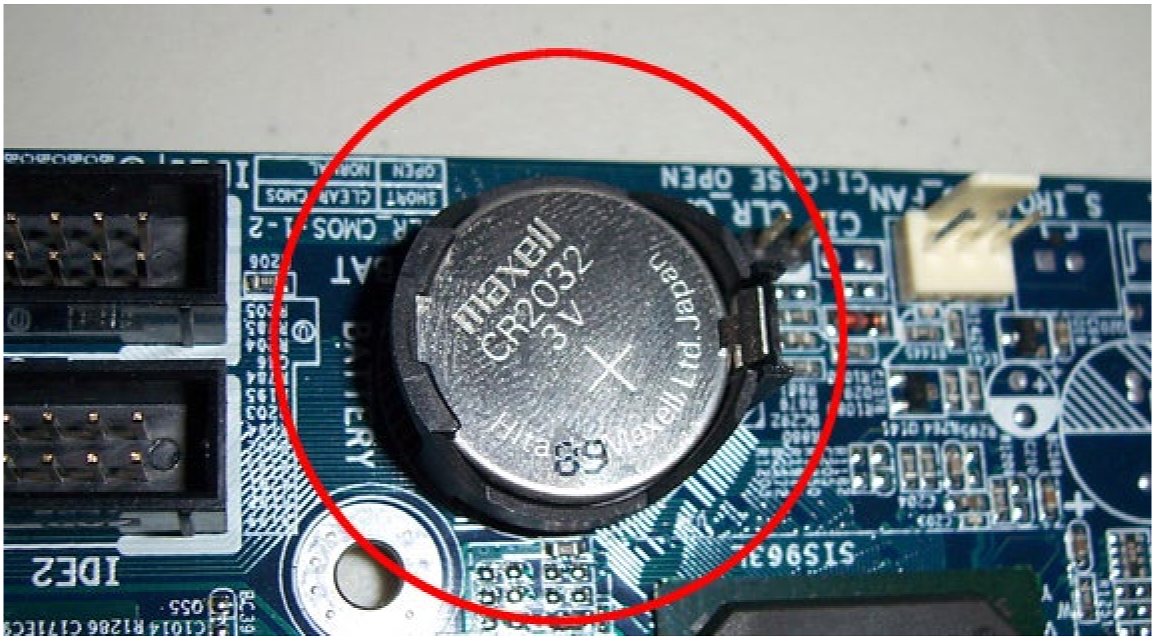
1. Determine if the battery is external or internal, or if you are replacing the CMOS battery
2. For an external battery
    a. The external battery will have two tabs (one to lock the battery in place, and one to release the battery)
    b. Slide the locking tab to the unlock position
    c. Slide the release tab to release the battery
    d. Remove the battery
    e. Install the new battery
    f. Slide the locking tab to the lock position



3. For an internal battery
    a. Remove the bottom cover
    b. Disconnect the battery cable from the system board
    c. The battery may be held in by adhesive or screws. Remove the adhesive or screws.
    d. Install the new battery. Reinstall the screws or peel the covering on the adhesive
    e. Connect the battery cable to the system board
    f. Reinstall the bottom cover

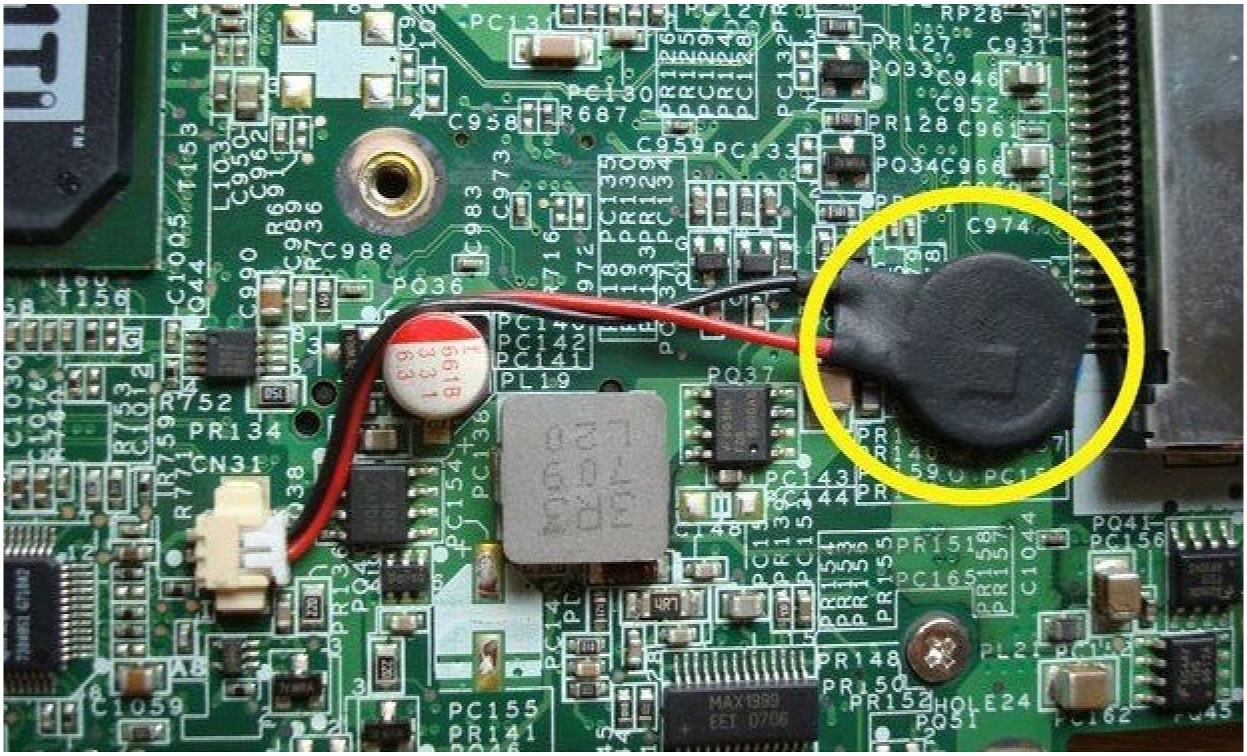


4. For a CMOS battery
    a. CMOS battery allows the computer to store BIOS settings and clock settings
    b. The CMOS battery is the size of a quarter
    c. Remove the bottom cover or access panel
    d. The CMOS battery is either
        i. Installed in a bracket
            1. Remove the battery from the bracket
            2. Install the new battery in the bracket



ii. Glued to the inside of the laptop and connected via a cable to the system board

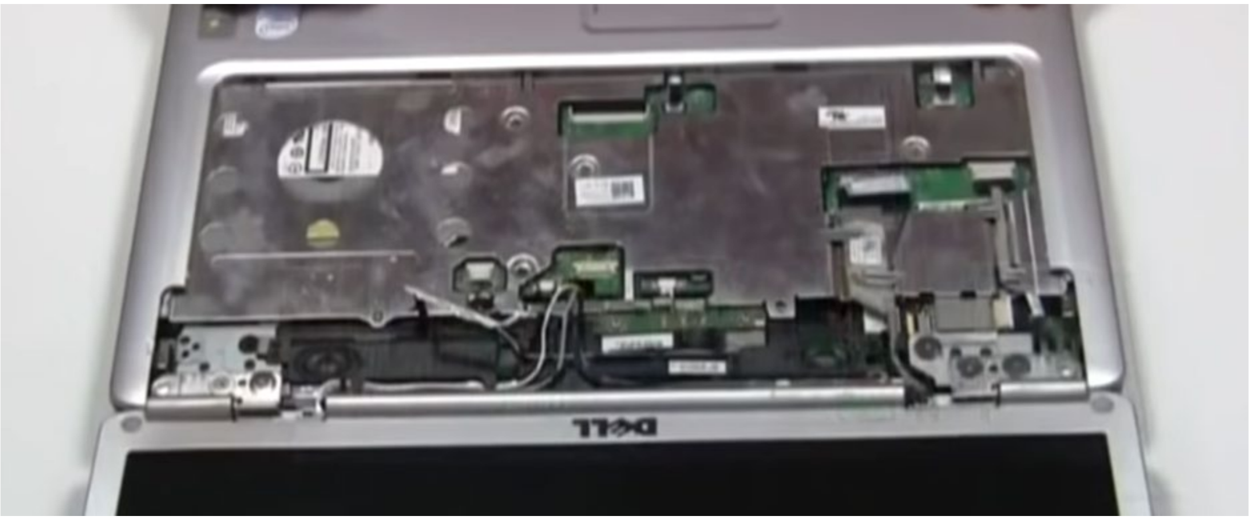
   1. Remove the battery from the laptop
   2. Remove the connector from the system board
   3. Install the new battery
   4. Install the new connector to the system board



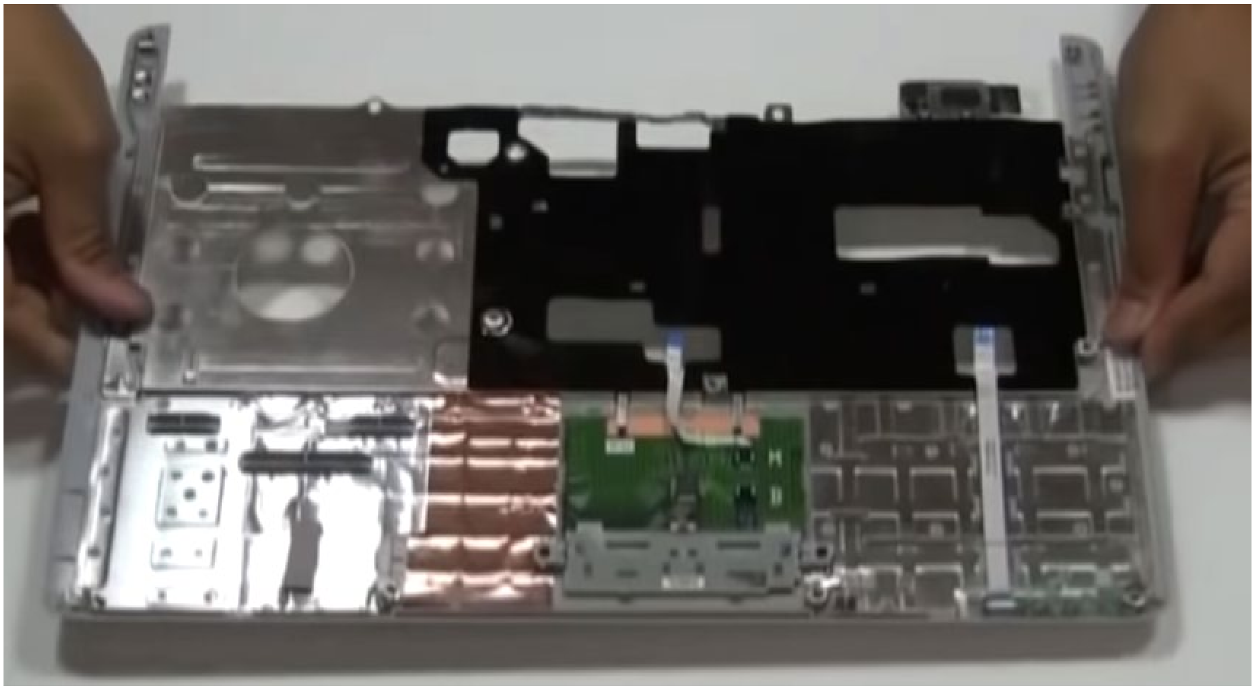
e. Reinstall the bottom cover or access panel

Touchpad Replacement

1. The touchpad is secured to the bottom inside of the keyboard cover
2. To remove the keyboard cover, you must remove the bottom cover
3. Remove the screw or screws holding the keyboard cover
4. Remove the keyboard
5. Remove the keyboard cover
6. The touchpad is connected to the system board by a ribbon cable



7. Remove the touchpad from the bottom of the keyboard cover



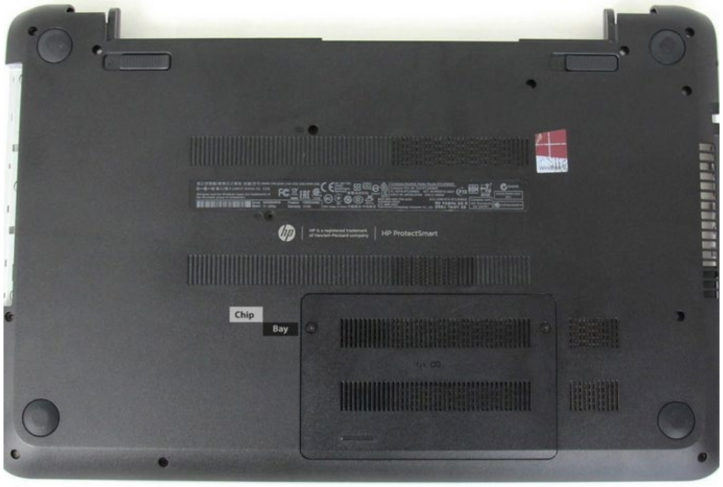
8. Insert the new touchpad into the keyboard cover
9. Insert the touchpad cable into the system board
10. Install the keyboard cover
11. Install the keyboard
12. Reinstall the keyboard cover screws
13. Reinstall the bottom cover

Plastics/Frames Replacement

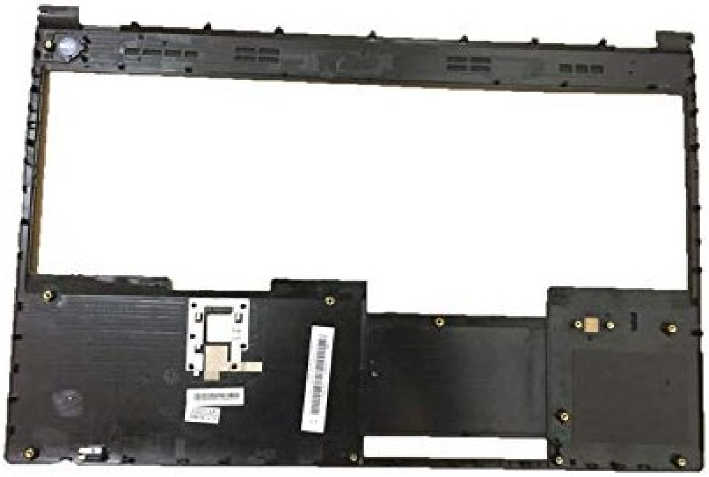
1. Remove the plastic component
2. Remove any components connected to the plastic
3. Install components on the new plastic
4. Reinstall the new plastic
5. A laptop will have several plastic components
    a. The bezel covering the screen

    b. The top cover, which covers the screen

c. The bottom cover



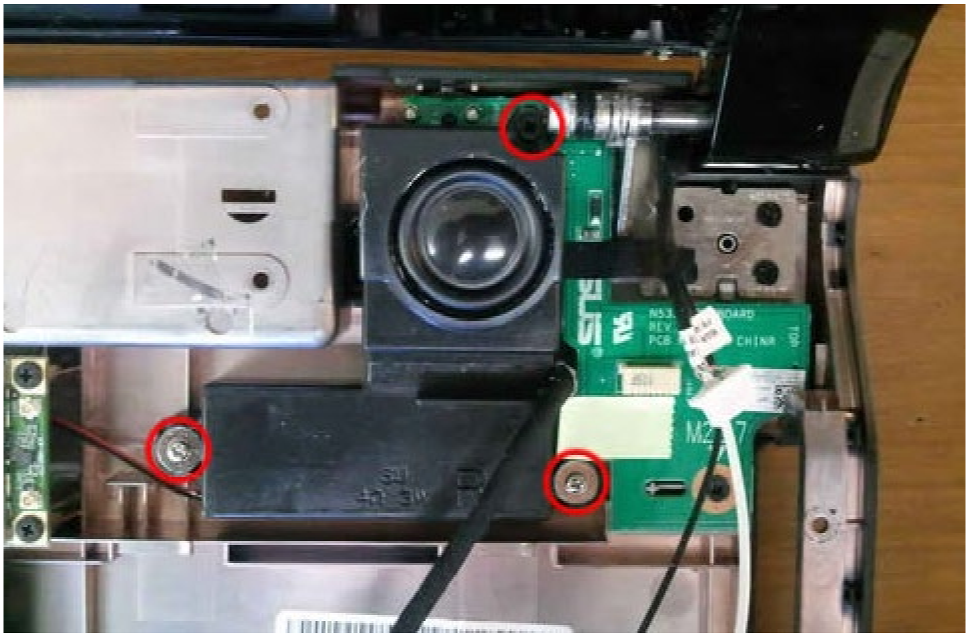
d. The cover where the keyboard fits (the keyboard cover)
    i. Note that this may or may not contain the keyboard, depending on the style of the laptop



e. Multiple access panels that insert into the bottom cover

Speaker Replacement

1. Determine the number and location of the speakers you must replace. A high-end laptop may have multiple speakers, and may even have a subwoofer
2. Typically
   - Remove the bottom cover
   - Remove the old speaker by removing the screws holding it
   - Remove connecting cable
   - Install new speaker and connecting cable
   - Reinstall the bottom cover
3. In some laptops, you may need to remove the keyboard and keyboard cover to access the speakers

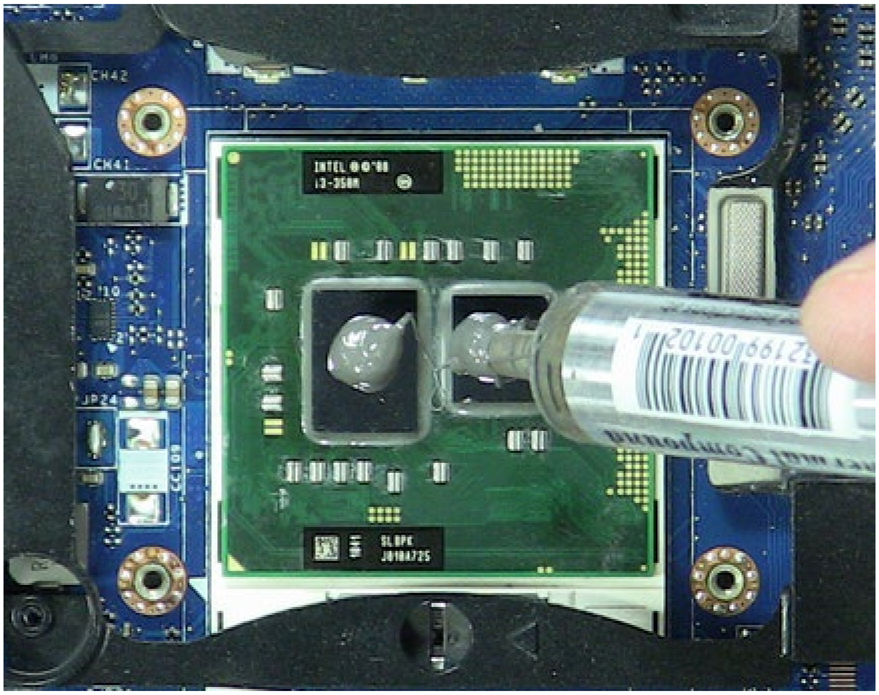


System Board Replacement

1. Determine if the system board is mounted to the top cover or to the bottom cover
2. Remove access panels
3. Remove bottom cover or top cover
4. Remove additional components (HDD, battery, etc.) if necessary
5. Remove components from system board (RAM, processor, Wi-Fi card, battery)
6. Remove all connection cables
7. Unscrew system board from laptop
8. Install new system board
9. Reinstall all connection cables
10. Reinstall all components
11. Reinstall additional components (HDD, battery, etc.) if necessary
12. Reinstall covers
13. Configure BIOS
    a. May need to record system serial number on new system board
    b. Configure system date/time
    c. Configure additional BIOS settings

CPU Replacement

1. Determine if the CPU is can be replaced
    a. Most laptop CPUs are not replaceable. They are soldered to the system board. The entire board must be replaced.
2. Remove bottom cover or access panel
3. Remove fan assembly or heat pipes that cover the CPU.
4. Remove old CPU
5. Remove thermal paste from heat pipe
6. Add thermal paste to new CPU, if required



7. Reinstall CPU
8. Reinstall screw or fan
9. Reinstall bottom cover

1.2 Given a scenario, install components within the display of a laptop.

- *Types*
  - *LCD*
  - *OLED*
- *Wi-Fi antenna connector/placement*
- *Webcam*
- *Microphone*
- *Inverter*
- *Digitizer/touchscreen*

Laptop Display Components

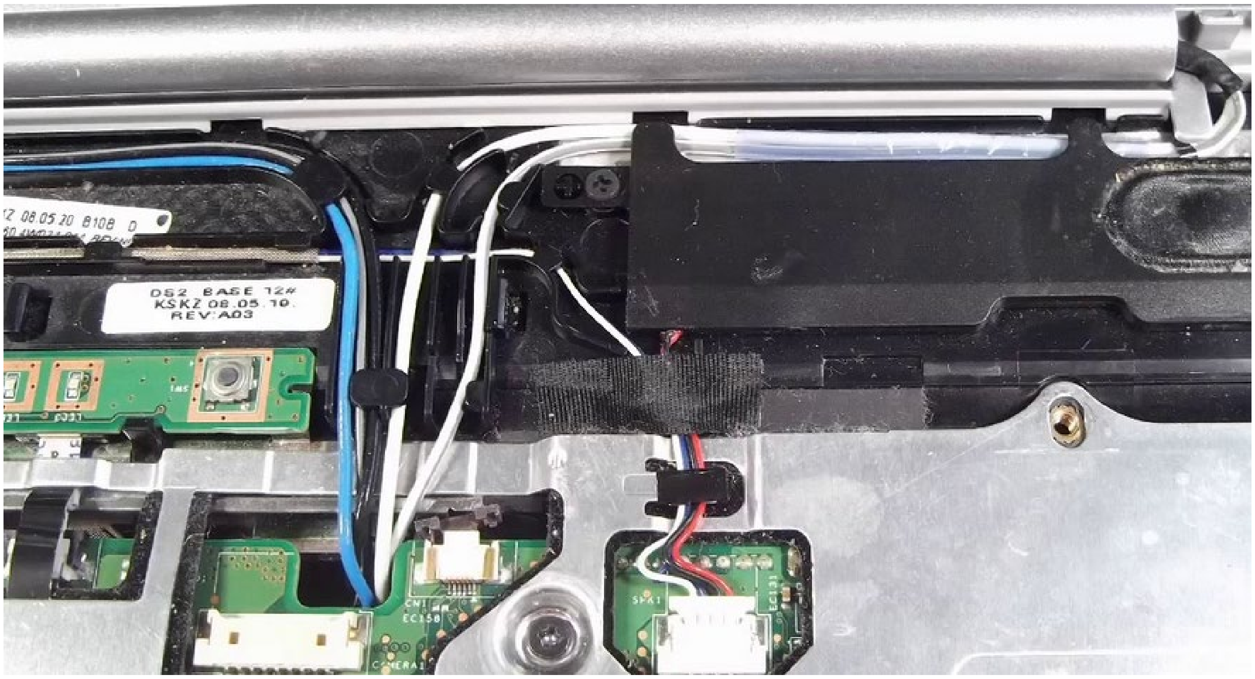
1. Many manufacturers sell a replacement laptop “screen assembly”, which is basically the top half of the laptop (screen, bezel, camera, touch digitizer, and hinges). It might be easier to replace the entire assembly, especially if multiple components are damaged
2. Wiring for the screen is routed through the laptop hinge and connects into the system board
3. To replace just the laptop screen.
    a. Determine if the screen has a bezel (rectangular plastic that surrounds the screen). This is common on laptops without touch capabilities

Types of Screens

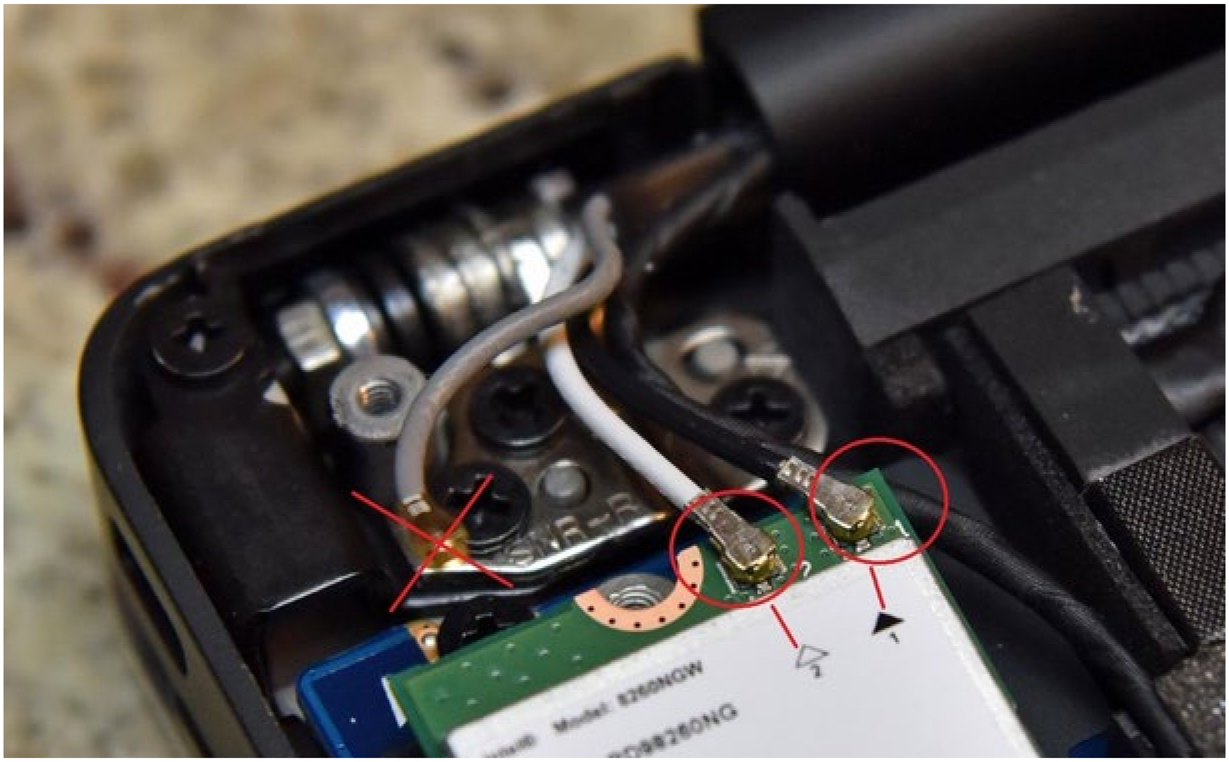
- There are two types of laptop screens: LCDs and OLEDs
- LCD
    - Liquid Crystal Display
    - Also known as TN or IPS
    - Requires a backlight to stay bright
    - If the backlight fails, the screen will look dim
- OLED
    - Organic Light Emitting Diode
    - No backlight required
    - An OLED screen can display a wider range of colors because it doesn’t have a backlight that interferes with the colors
    - Can be thinner and lighter

Wi-Fi Antenna Connector

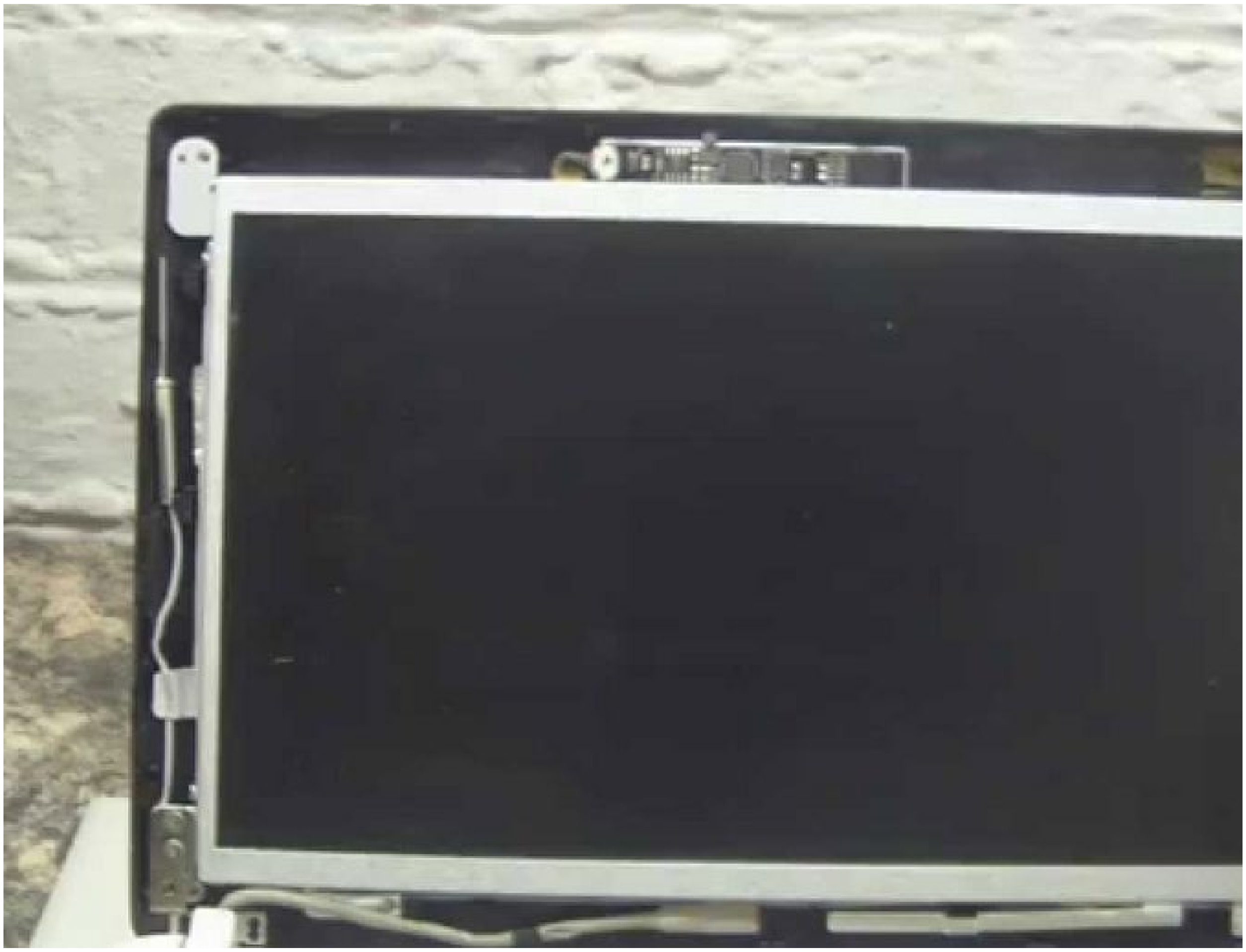
- The laptop antennas starts at the Wi-Fi card and are routed through the laptop hinges and into the screen assembly



- Remove the laptop bottom access panel
- Disconnect the antenna from the Wi-Fi card



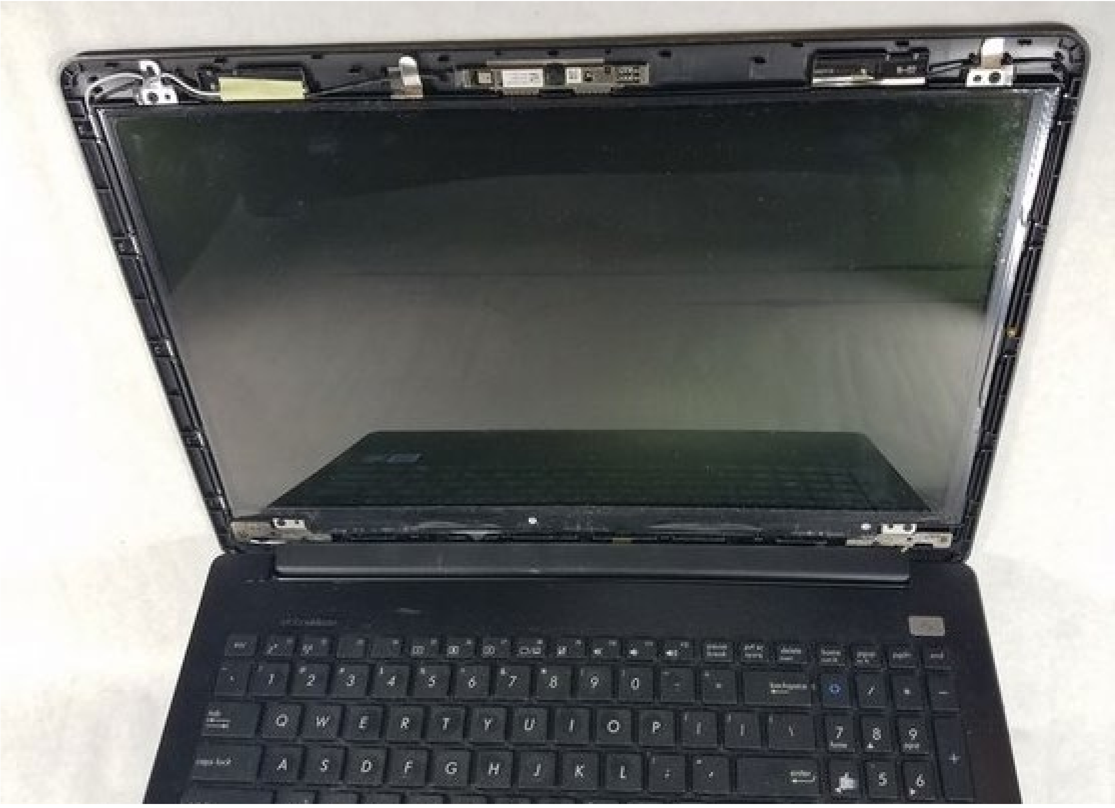
- Remove the bottom or top cover
- Remove the screen bezel
- Remove the antenna cable



- Reinstall the antenna
- Route the antenna through the hinge
- Connect the antenna to the Wi-Fi card
- Reinstall the bezel and covers

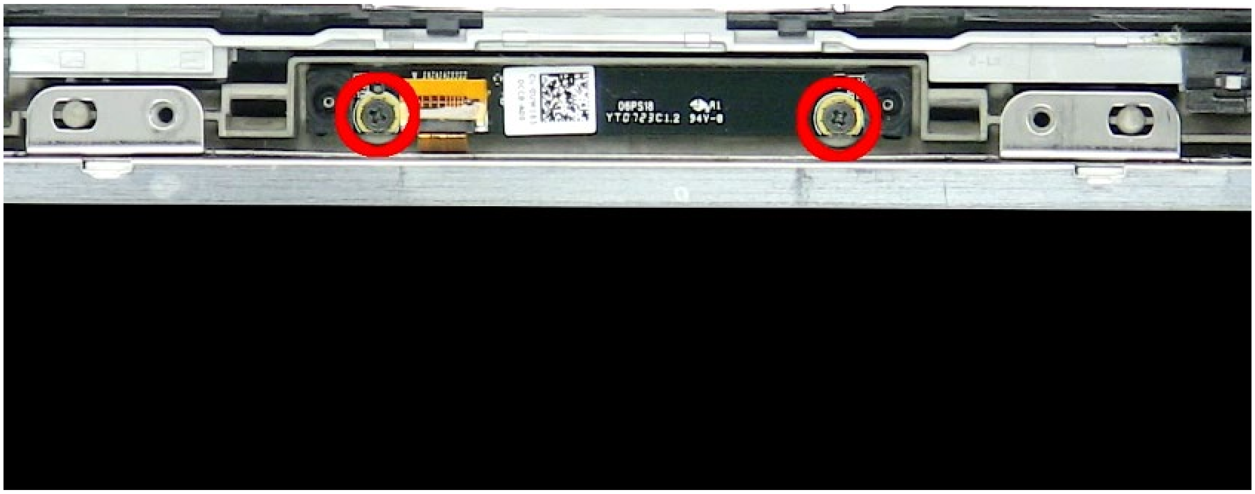
Webcam

- Webcam replacement follows similar steps to Wi-Fi antenna replacement
- Typically, the webcam sits at the top of the screen and is part of a circuit board that contains the microphone
- The webcam cable is routed through the hinge and connects to the system board
- Remove the top or bottom cover and access panels
- Remove the bezel
- Remove the web cam cable
- Remove the web cam from the top. You may have to remove some screws.
- Install the new camera.
- Route the cable through the hinge and into the system board.
- Reinstall the bezel and covers.



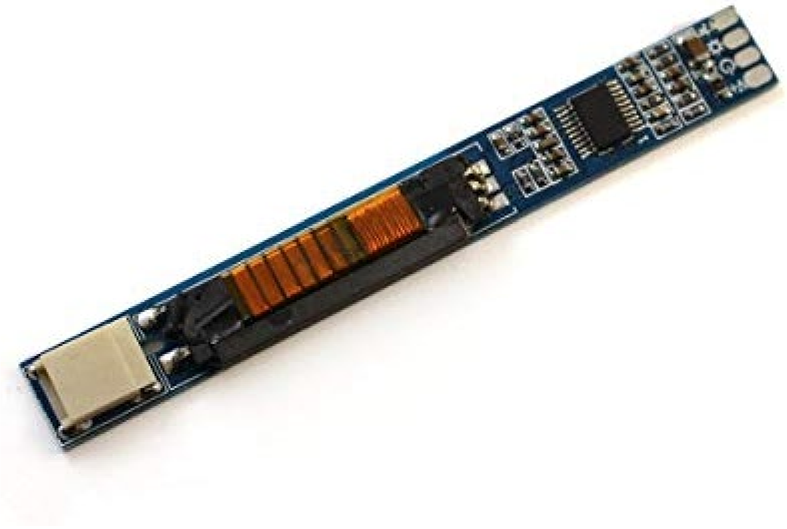
Microphone

- The laptop microphone and webcam are connected to the same circuit board
- Follow the steps for replacing the webcam

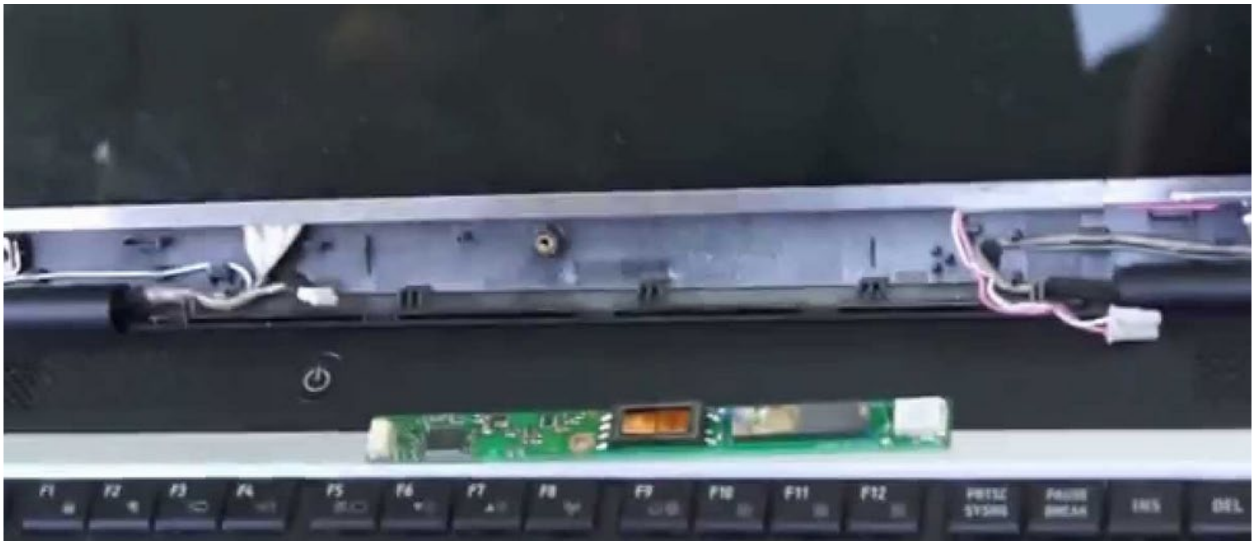


Inverter

- Provides backlight for LCD



- Only found on LCD screens, not OLED screens
- Determine if the inverter is part of the LCD, or if it can be replaced separately
- The inverter is located underneath the LCD, or at the bottom of the LCD



- To replace the Inverter
    - Remove the bezel
    - Remove the cables connecting the inverter to the system board and to the LCD

- Unscrew the inverter from the laptop
- Install the new inverter
- Reconnect the cables to the inverter
- Reinstall the bezel

Digitizer

- The digitizer is a pane of glass that covers the laptop screen and provides touch capabilities
- It is connected via a cable to the system board
- Laptops with touch have a more solid feeling screen
- An impact to the laptop could crack the digitizer
- Determine if the digitizer can be removed
    - Some digitizers are glued to the LCD/OLED panel, in which case the entire screen (LCD and digitizer) must be replaced
    - You can melt the glue with a heat gun
        - If you're not careful, you could damage the LCD/OLED panel
        - You could also crack the glass
- Laptops with digitizers typically don't have bezels
- To replace the digitizer
    - Remove the top or bottom cover
    - Remove the screws which may be covered by stickers, or remove the screen with a spudger
    - Disconnect the digitizer cable from the system board
    - If the digitizer and LCD are glued together, it's possible to remove the glue by melting it with a heat gun
    - Install the new digitizer
    - Reconnect the digitizer cable to the system board
    - Install the LCD assembly
    - Reinstall the top or bottom cover

1.3 Given a scenario, use appropriate laptop features.

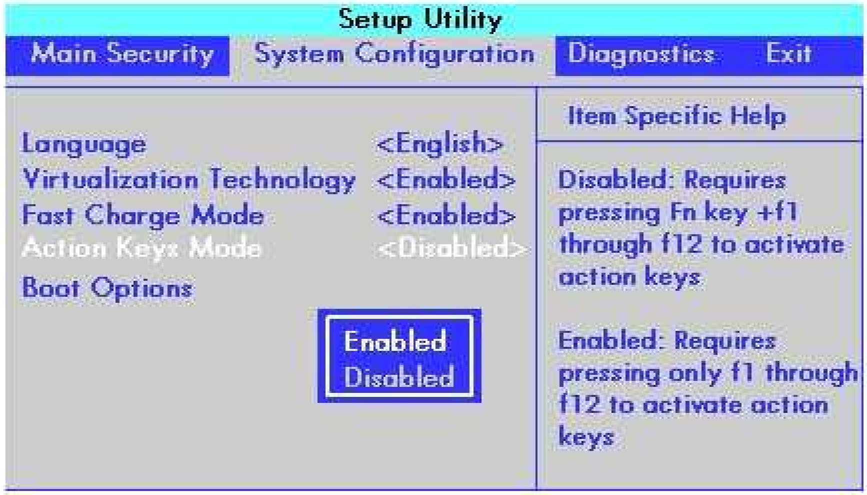
- *Special function keys*
    - *Dual displays*
    - *Wireless (on/off)*
    - *Cellular (on/off)*
    - *Volume settings*
    - *Screen brightness*
    - *Bluetooth (on/off)*
    - *Keyboard backlight*
    - *Touchpad (on/off)*
    - *Screen orientation*
    - *Media options (fast forward/rewind)*
    - *GPS (on/off)*
    - *Airplane mode*
- *Docking station*
- *Port replicator*
- *Physical laptop lock and cable lock*
- *Rotating/removable screens*

Special Function Keys

The special function keys are located at the top of the keyboard and are labelled F1 to F12. Each Function key is labelled with a logo for what it does (differs from laptop to laptop). The most common functions are listed in the table below, but your laptop may have other functions.

To activate a special function key

- Hold down the “fn” key while pressing the key
- To activate the ley without having to press “fn”, you must toggle a setting in the BIOS. The setting is called “Action Keys Mode:

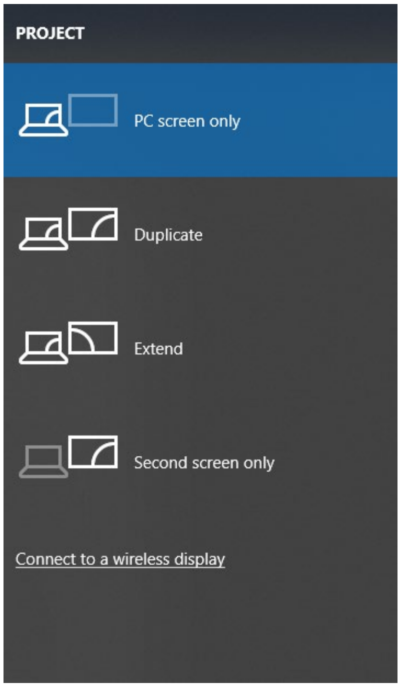


Setup Utility

Main Security   System Configuration   Diagnostics   Exit

		Item Specific Help
Language	<English>	
Virtualization Technology	<Enabled>	Disabled: Requires pressing Fn key +f1 through f12 to activate action keys
Fast Charge Mode	<Enabled>	
Action Keys Mode	<Disabled>	
Boot Options		Enabled: Requires pressing only f1 through f12 to activate action keys

Enabled
Disabled

Dual Displays	Allow you to project laptop screen to external display (connected via cable or wireless – Chromecast, Surface, etc.) The Dual Displays menu appears. Pressing the button again toggles through the different menu options.  PROJECT PC screen only Duplicate Extend Second screen only Connect to a wireless display The options are: • PC Screen Only: display only on PC Screen • Duplicate: display identical content on second screen • Extend: display different content on second screen, equivalent to having a second monitor • Second screen only: display content on second screen, turns the laptop screen off

	Choose the "Connect to a wireless display" link to connect to a wireless display
Wireless	Toggle Wi-Fi on or off
Cellular	Turn cellular data on or off (for laptops with cellular capabilities)
Volume	Adjust volume up or down (2 buttons)
Screen brightness	Turn screen brightness up or down (2 buttons)
Bluetooth	Toggle Bluetooth on or off
Touchpad	Toggle touchpad on or off (good for when you're using a mouse)
Screen Orientation	Change screen orientation from landscape to portrait A tablet can automatically detect the correct screen orientation A tablet will have the option to toggle automatic rotation (you may want to fix the orientation)
Media Options	Fast Forward, Rewind, Pause, etc. These features are good for when you're watching a movie on a DVD or Blu-Ray They may also work with third-party applications, such as VLC Media Player

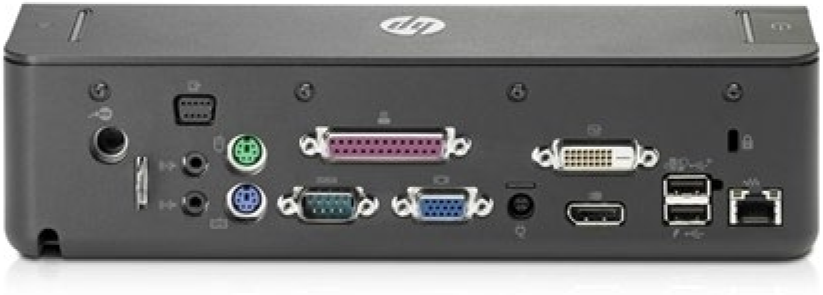
GPS	Toggle GPS on or off (for laptops equipped with GPS)
Airplane Mode	Toggle airplane mode on or off Airplane mode will deactivate Wi-Fi, GPS, Cellular, and Bluetooth If you're on an airplane with Wi-Fi, you can still connect to the airplane's Wi-Fi when on airplane mode
Help	Launch Windows help, or possibly launch the help menu inside an application that you're running
Keyboard Backlight	Toggle keyboard backlight on or off (for laptops with keyboard backlights)

Docking Station vs Port Replicator

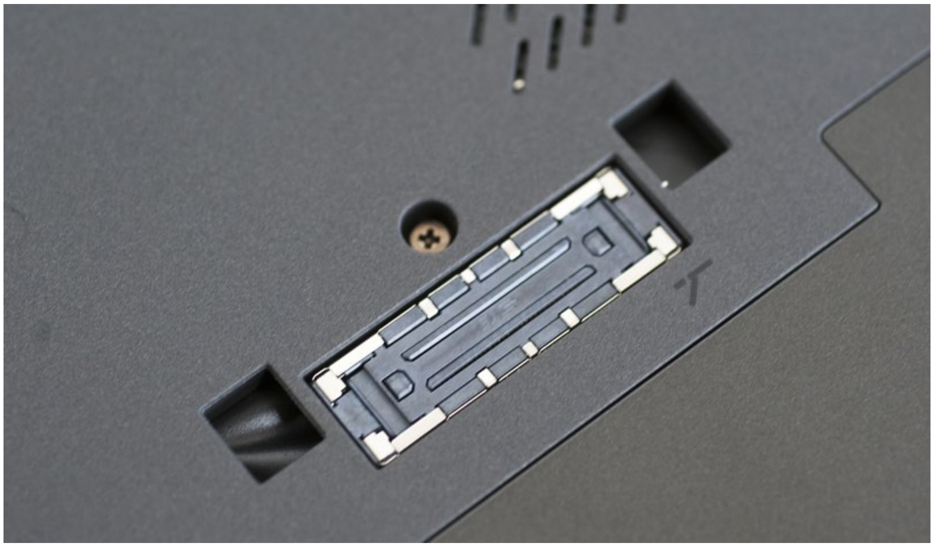
- A user with a laptop may take it home or on the road. When the user gets back to the office, they connect their laptop to the docking station, and can use all of their peripherals.
- A docking station allows a user to connect their laptop to many devices at the same time
- It is ideal for an office worker who wants to connect external monitors, ethernet, and USB devices such as mice, keyboards and printers, but wants to avoid the hassle of connecting each device manually
- Only "business-grade" laptops have docking ports
- The bottom of the laptop contains a docking port
- The laptop sits on top of the docking station
- The docking station may have
    - A button to power the laptop on or off
    - A button to eject the laptop from the dock
    - A button to lock/unlock the laptop in the dock
- A docking station is typically proprietary to the manufacturer, although aftermarket docking stations exist. A docking station may work with multiple models of laptops made by the same manufacturer
- Older docking stations can have optional slots to add memory, hard disk drives, and PCI cards, which the laptop can take advantage of when it is connected. These are not popular.
- Disadvantages
    - Some of the docks' ports contain pins that are easily damaged if the laptop isn't inserted correctly
    - Dock may take up too much space on the desk

Older models of docking stations look like this

Back of Dock

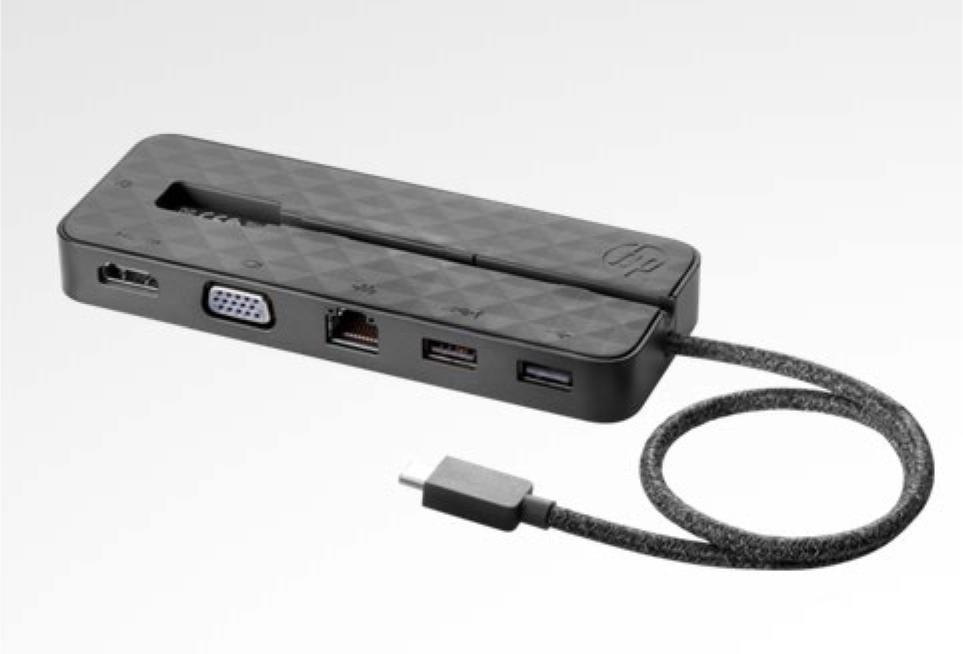


Docking port on bottom of laptop



Newer docking stations use USB-C

- The user connects the USB-C cable to the laptop
- All data and power are transmitted through the USB-C cable
- Some docking stations require two connections to the laptop (one for USB-C and one for power)
- Most laptops with USB-C ports (even consumer-grade laptops) can function with the newer docking stations

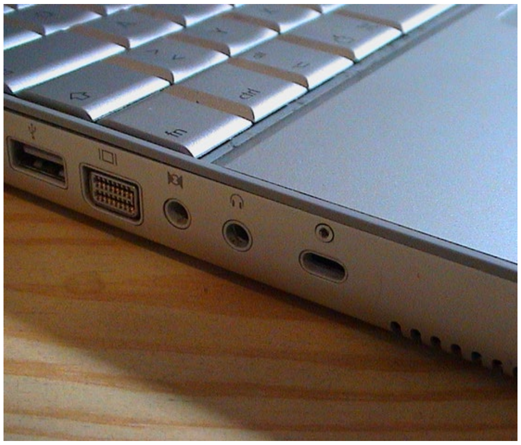


What’s the difference between a port replicator and a docking station?

- Technically a port replicator includes the same ports that are on the laptop
- A docking station includes additional ports that aren’t found on the laptop (for example a serial port)
- A docking station may have additional hardware support

Cable Lock

- A cable lock allows you to lock your laptop to a desk so that it can't be stolen
- Most laptops and monitors have a cable lock port. The port on the right is a cable lock port. It looks almost like a USB-C port.



- You wrap the cable around a secure object like a desk and then insert the lock mechanism into the lock port

- It's easy to cut the cable with a pair of bolt cutters
- Good physical security is important, in combination with other security practices
  - Encrypt your laptop data
  - Lock your screen when you are away from your desk
  - Don't leave your laptop unattended if possible

Rotating Screens

- A rotating screen allows you to convert your laptop into a tablet

- Laptops with rotating screens are not popular
- Consider the Microsoft Surface Pro Tablet
  - You can fold the screen over so that it becomes a tablet
  - The keyboard connects to the screen via a magnetic connector
  - You can detach the keyboard portion from the laptop (some models)

6:18
Sunday, June 18

1.4 Compare and contrast characteristics of various types of other mobile devices.

- *Tablets*
- *Smartphones*
- *Wearable technology devices*
    - *Smart watches*
    - *Fitness monitors*
    - *VR/AR headsets*
- *E-readers*
- *GPS*

Tablet

- Size
    - A tablet is larger than a smartphone and all glass, with a few buttons (such as power, home, and volume)
    - Average 7″ x 5″ size
- Interaction
    - You must use the touch interface to interact with the tablet (or can use a stylus)
- Operating System
    - Some tablets run a full version of an operating system (for example Microsoft Surface, HP Elite Pad)
    - Other tablets run only limited versions of an operating system (For example Apple iPad), where you can only install and operate a limited set of applications
    - Android operating system is common for tablets
- Peripherals
    - Tablet may contain a camera, speakers, and a microphone
    - Tablet may have no external ports or only a few external ports (for ethernet, USB, HDMI, or mini-HDMI)
- Repair
    - Some tablets contain replaceable components (Microsoft Surface) and some don't.
- Connectivity
    - Tablets connect to the internet via Wi-Fi, or cellular. Tablets may have Bluetooth capabilities.
    - Some tablets have optional docking stations
    - Tablets are battery powered

Smartphone

- Size
    - A smartphone (cellular telephone) is smaller than a tablet
    - Average 6” x 3” in size
- Interaction
    - Interact with phone via touchscreen or stylus (larger phones such as Samsung Galaxy Note)
    - Few phones have keyboards, such as Blackberry Key2
    - Allows you to place and receive phone calls, and SMS messages (typically can’t be performed by a tablet)
    - Smartphone may have additional features, such as a web browser, or e-mail
    - Smart phones contain many sensors for light, vibration, GPS, pedometers, etc.
- Operating System
    - Apple iOS (iPhone)
    - Android (Samsung Galaxy, Google Pixel). Android is customized to each smartphone manufacturer and cell service provider
    - Proprietary operating systems (Boeing phone, CAT phone, other military-grade phones)
- Peripherals
    - Some smartphones have styluses
    - Phone will typically have one USB port and one headphone jack
    - Some phones don’t have headphone jacks
    - Peripherals can include headphones, credit card readers, and external cameras
- Repair
    - Difficult to repair a smartphone due to lack of cooperation from manufacturers
    - Many repair shops offer same day service for batteries and cracked screens
- Connectivity
    - Smartphone will have a SIM card which allows it to authenticate with the cellular network
    - Some smartphones have the ability to insert two SIM cards and/or SD Cards (for additional memory)

- A smartphone will have a cellular modem and can also connect to Wi-Fi

Wearable Technology – Watches

- Size
  - Size of a wrist watch
- Interaction
  - Smart watches can display limited data such as SMS messages and photos
  - Interact with screen or buttons on side of watch
  - Smart watch may contain other sensors such as GPS, heart rate, and pedometer
  - Examples include Apple Watch, some Fossil watches
  - Many watch manufacturers have introduced internet-connected watch models
- Operating System
  - May run iOS, Android (with limited features), or proprietary operating system
- Peripherals
  - Typically, none
- Repair
  - Difficult to repair
  - Some repair shops or manufacturer may be able to repair the watch
- Connectivity
  - Typically pairs via smartphone over Bluetooth
  - Requires smartphone to be connected, and may require installation of app on smartphone
  - May have a USB port for charging and/or firmware updates
- A smart watch will typically pair with a smartphone and can't operate independently

Wearable Technology – Health Monitors

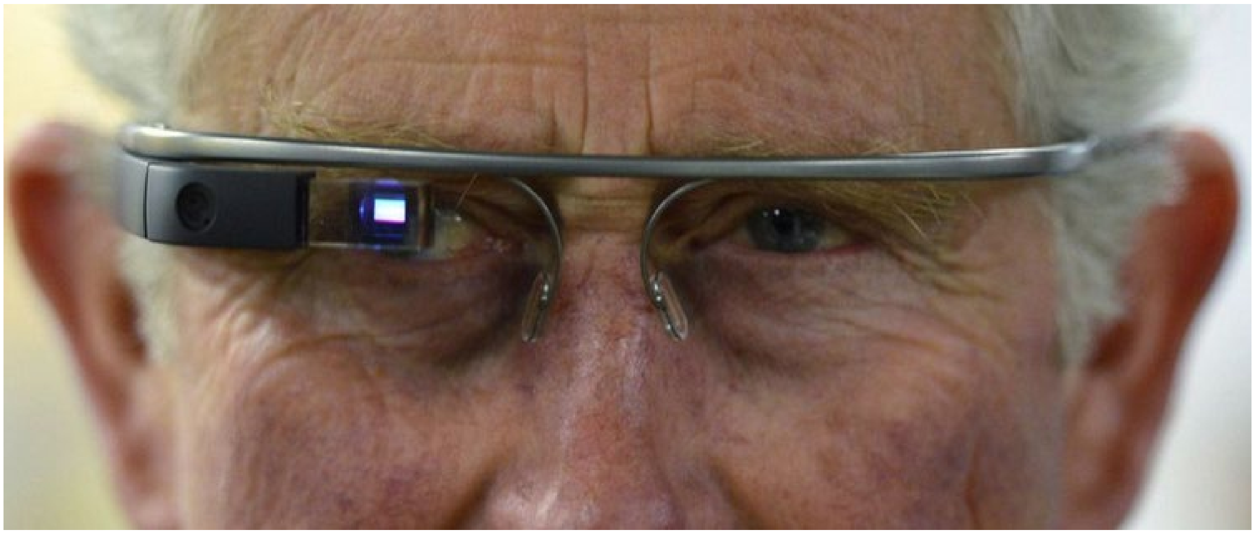
- Size
    - Size of a wrist watch
- Interaction
    - May have a screen and buttons to interact with
    - May contain other sensors such as GPS, heart rate, and pedometer
    - Updates may be available regularly, which can add functionality
    - Possible to download apps directly to health monitor, including apps released by third party developers
    - Example includes the Fitbit, which has the appearance of a wrist watch

- Operating System
    - May run Android (with limited features) or proprietary operating system
- Peripherals
    - Typically, none
- Repair
    - Difficult to repair
    - Some repair shops or manufacturer may be able to assist
- Connectivity
    - Typically pairs via smartphone over Bluetooth

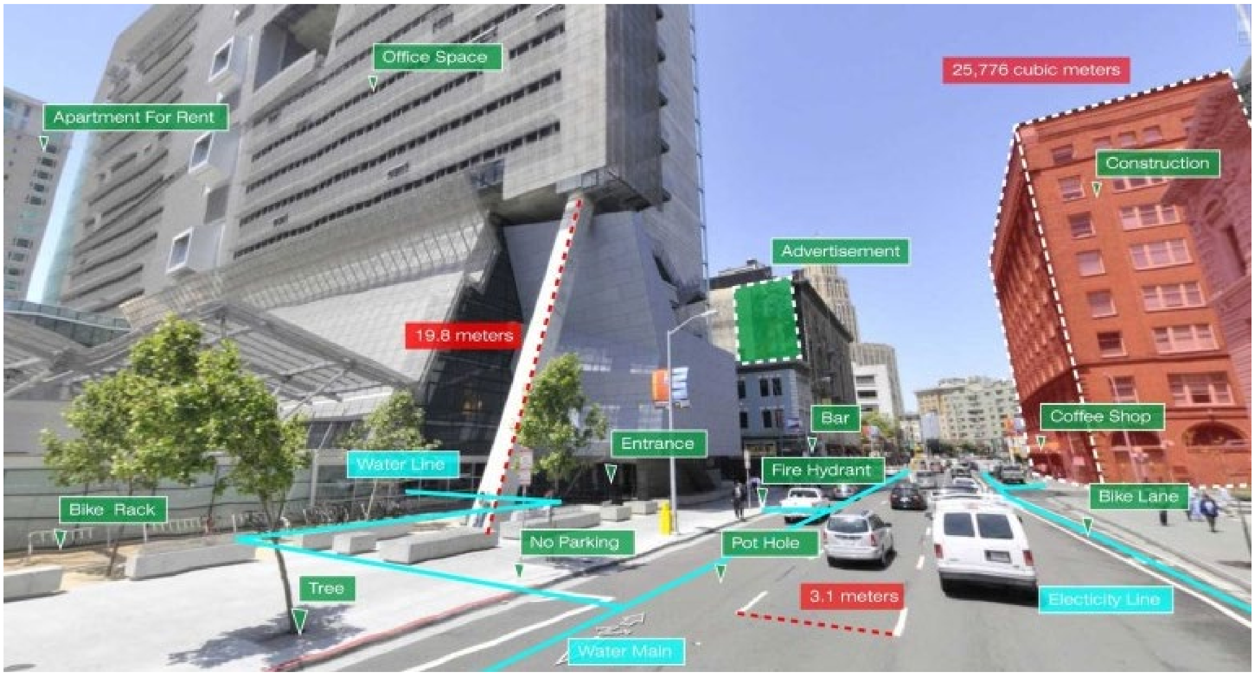
- Requires smartphone to be connected, and may require installation of app on smartphone
- May have a USB port for charging and/or firmware updates
- May require payment of monthly fee for continued use

Wearable Technology – VR

- Size
  - Size of a pair of large goggles or a helmet
- Interaction
  - Virtual Reality technology allows you to see a new world, for example, allows you to feel like you are inside a 3D environment (example is Oculus Rift)
  - Augmented Reality technology allows you to see your existing environment, but presents enhanced data (example is Google Glass)



  - You wear the device and it displays video
  - Augmented Reality devices will have sensors, cameras, and GPS locators to understand where you are and display relevant data
  - Virtual Reality devices will connect with a server or computer and display relevant video content. May also have sensors to identify the direction and speed of your movement in order to display a more realistic environment.
  - May contain eye tracking sensors that understand where the user is looking.
  - Good for medical and military training

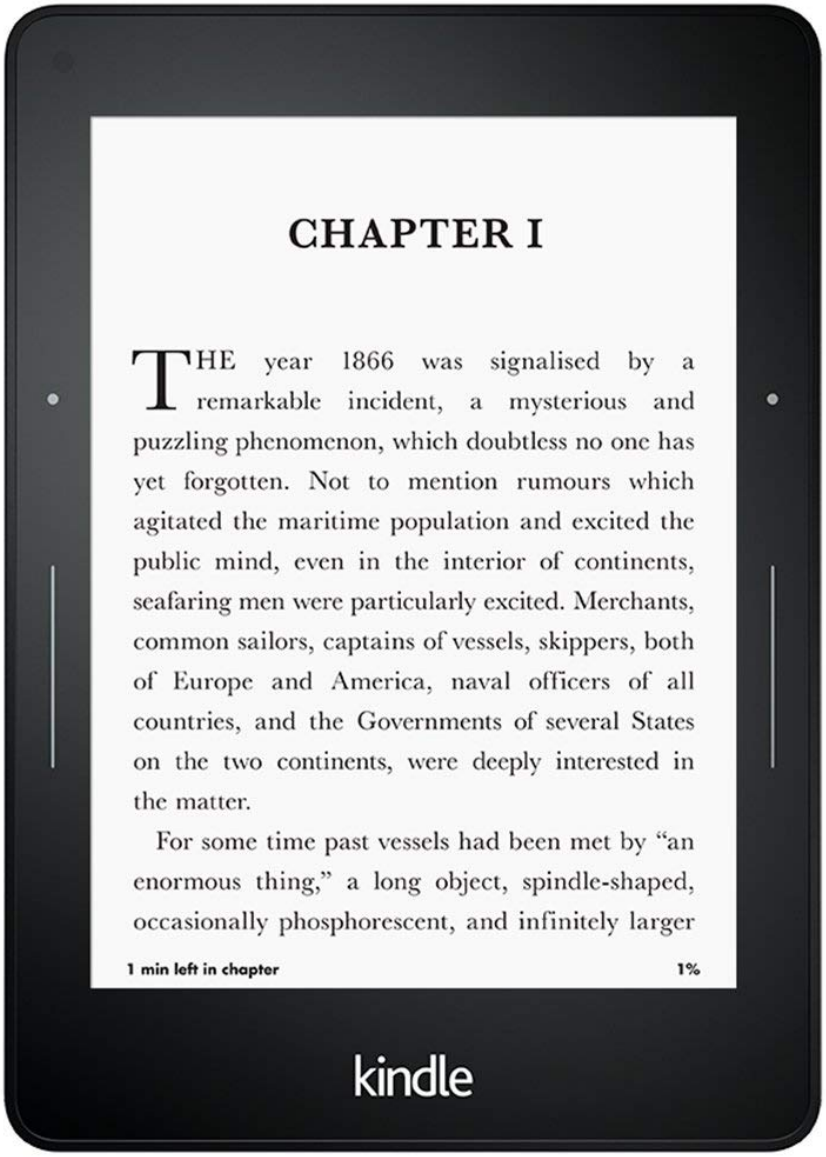


- Operating System
  - Android or proprietary operating system
- Peripherals
  - Typically, none
- Repair
  - Difficult to repair
  - Some repair shops or manufacturer may be able to assist
- Connectivity
  - May have a USB port for charging and/or firmware updates
  - Oculus Rift has multiple connectors
    - Headset requires HDMI and USB 3.0 connection to computer
    - Also required to connect two camera sensors to computer

oculus

E-Reader

- Size
    - Size of a tablet
- Interaction
    - Typically, a touch screen with some buttons to flip pages and scroll
    - Many e-readers have a special screen that mimics printed paper
    - Can read eBooks
    - E-reader may have DRM so that you can’t share or copy eBooks
    - E-reader may have additional functions such as ability to highlight text, ability to browse the web or a dictionary
    - E-reader will read eBooks in the proprietary format made by its manufacturer (For example Kindle e-reader only reads eBooks from the Kindle store, and in PDF format)
    - Many e-reader manufacturers offer apps for the smartphone, tablet, and computer as well
- Operating System
    - Android or proprietary operating system
- Peripherals
    - Typically, none
- Repair
    - Difficult to repair
    - Some repair shops or manufacturer may be able to assist
- Connectivity
    - May have a USB port for charging
    - Can connect to Wi-Fi or cellular network



CHAPTER I

THE year 1866 was signalised by a remarkable incident, a mysterious and puzzling phenomenon, which doubtless no one has yet forgotten. Not to mention rumours which agitated the maritime population and excited the public mind, even in the interior of continents, seafaring men were particularly excited. Merchants, common sailors, captains of vessels, skippers, both of Europe and America, naval officers of all countries, and the Governments of several States on the two continents, were deeply interested in the matter.

For some time past vessels had been met by "an enormous thing," a long object, spindle-shaped, occasionally phosphorescent, and infinitely larger

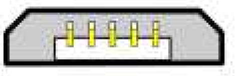
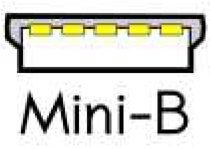
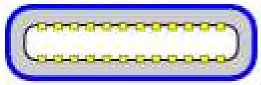
1 min left in chapter 1%

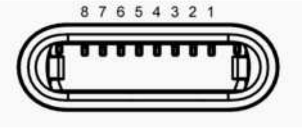
1.5 Given a scenario, connect and configure accessories and ports of other mobile devices.

- *Connection types*
    - *Wired*
        - *Micro-USB/Mini-USB/USB-C*
        - *Lightning*
        - *Tethering*
        - *Proprietary vendor-specific ports (communication/power)*
    - *Wireless*
        - *NFC*
        - *Bluetooth*
        - *IR*
        - *Hotspot*
- *Accessories*
    - *Headsets*
    - *Speakers*
    - *Game pads*
    - *Extra battery packs/battery chargers*
    - *Protective covers/waterproofing*
    - *Credit card readers*
    - *Memory/MicroSD*

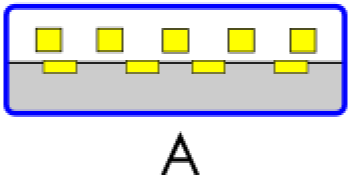
Connection Types for a Mobile Device – Wired

Note that there are many more types of USB connectors (Type A vs Type B connectors, and USB 1.0/2.0 vs 3.0 connectors). We will look at these in more detail in a later section.

Micro-USB (Type B)  	Most common format Allows you to connect the mobile device to a computer (to transfer data and power) or to a power outlet (to transfer power)
Mini-USB (Type B)  	Less common format Allows you to connect the mobile device to a computer (to transfer data and power) or to a power outlet (to transfer power)
USB-C  	New format for connecting mobile devices Allows you to connect the mobile device to a computer (to transfer data and power) or to a power outlet (to transfer power) USB-C connector is symmetrical USB-C is USB 3.0

Lightning  	Apple devices use lightning connection, which is proprietary Allows you to connect the mobile device to a computer (to transfer data and power) or to a power outlet (to transfer power) Lightning connector is symmetrical
Tethering	Uses a USB cable, Bluetooth, or a Wi-Fi connection to connect the mobile device to a computer Useful for transferring data to/from the computer Useful for providing an internet connection to a computer or to other mobile devices (the mobile device acts as an internet router/modem/wireless access point)
Proprietary vendor-specific ports 	Older mobile devices (prior to 2010) may use proprietary connectors The connector may only provide power or may provide connection to a computer There are dozens, if not hundreds of different proprietary connectors from the early-to-late 2000s May need to search online (eBay or Amazon) to find these adapters

The standard USB connector is Type-A



You can purchase a cable in any of the above models that is Type B, USB-C, Lightning, etc. on one side, and Type A on the other.

Connect the Type A side to a computer (to transfer data) or to a power adapter (to charge the mobile device).

Connection Types for a Mobile Device – Wireless

NFC	Near-Field Communication Uses an electromagnetic signal generated by a loop antenna inside the mobile device NFC Devices work together automatically Uses • Contactless payments/Mobile payments (your mobile device can act as a credit card or a debit card) • Key card (your mobile device can act as a key card in an office building or hotel) • Sharing data between mobile devices • Range of 4cm (maximum)
Bluetooth	Uses radio waves to connect peripherals and transfer data Devices must "pair" with each other before any data can transfer Uses • Connect to a headset • Connect to vehicle audio system • Transfer files • Range of 100m
IR	Infrared

	Uses invisible light to transfer data between devices The devices must be aligned so that their IR transmitter/receiver have a clear line of sight Uses • Transfer data between devices IR was popular around 2010, but currently few mobile devices have IR capabilities
Hotspot	Mobile device broadcasts a Wi-Fi signal (acts like a wireless access point) Other devices can connect to it Uses • Provide a wireless internet connection to a laptop, phone, tablet, or other device • Useful when travelling with a laptop and unable to find an internet connection Range of 100m, but depends on power mobile device and interference from walls, buildings, and other obstruction

Phone Accessories

A wide range of phone accessories are available

Phone accessories connect via

- USB/lighting (very common)
- Bluetooth (very common)
- Headphone jack (common for headphones, and less common for other devices)
- Internet (Wi-Fi/cellular data) (phone and device share data through an external server)

A wireless accessory will usually contain a USB port for charging, or will contain batteries

Headset 	Phone headset • "Over the ears" headsets are adjustable, and may or may not contain a microphone (first two photos) • "Ear buds" style headsets fit into ears and have replaceable buds. They may or may not contain a microphone embedded into the wire. Headsets • Wired (headphone jack) or wireless (Bluetooth) connectivity • Bluetooth offer higher quality audio than the headphone jack • Headsets can be noise cancelling • Typically, don't require a power source or battery • Price ranges between $10 and $1000 Examples are Bose, Skull Candy, Beats Audio, Sennheiser

Speaker 	An external speaker - Can connect to the headphone jack or over Bluetooth - Will play audio sent by phone - May contain a USB port for charging - Prices range from $20 to $1000 Example is the Beats Pill
Game Pad 	A gamepad - Can play games on a phone or tablet - Provides additional controls not available on the phone - May contain a bracket to secure the phone in place - Connects over Bluetooth or USB - Prices range from $20 to $150

Extra battery 	Older phones have replaceable batteries, newer phones do not There are two options for increasing battery capacity • An external case containing a battery. The phone fits into the case, and the case connects to the phone's USB port. The case supplies power to the phone. This becomes a relatively permanent part of the phone. An example is the Apple Smart Battery Case (first photo) • A power bank device connects to the USB port and charges the battery. A typical power bank device has capacity to charge a phone twice. The power bank device can be charged via USB (second photo). • Costs around $40
Protective Cover/Waterproofing	Phone cases • Many models and styles are available from practical to stylish, and in a wide variety of colors • A phone case will be custom to a particular phone model • Contains cut-outs for the phone's cameras and sensors • Phone cases can be soft or hard • Protects phone from damage when it is dropped

	• May provide waterproofing • Example of a protective case is the Otter box • Another option is to coat the screen with a protective coating or a screen protector, which prevents scratches. • Cases cost between $10 and $50, but high-end designer cases may cost thousands of dollars • Screen protectors cost about $10
Credit Card Reader 	Credit Card Reader • Allows cell phone user to accept mobile payments (alternative to carrying a credit card machine) • Most popular is Square • Credit card reader connects to the phone's headphone jack, USB port, or via Bluetooth • Linked to a smartphone app • A more advanced reader contains a screen and a keypad (for entering a PIN)
Memory Cards	Memory card • Increases memory of phone • Size ranges between 4GB and 512GB • MicroSD and MicroSDXC are the most common formats

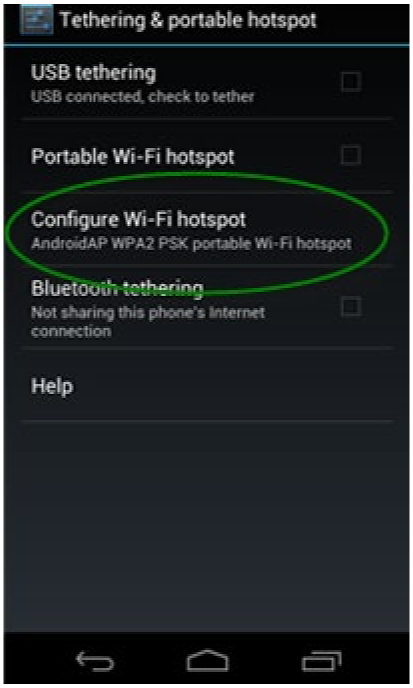
	Some phones have space for memory cards, including an SD card or a Micro SD card You can increase the memory of the phone up to 1TB Some phones do not have the ability to add a memory card (like Apple iPhone)

1.6 Given a scenario, configure basic mobile device network connectivity and application support.

- *Wireless/cellular data network (enable/disable)*
  - *Hotspot*
  - *Tethering*
  - *Airplane mode*
- *Bluetooth*
  - *Enable Bluetooth*
  - *Enable pairing*
  - *Find a device for pairing*
  - *Enter the appropriate pin code*
  - *Test connectivity*
- *Corporate and ISP email configuration*
  - *POP3*
  - *IMAP*
  - *Port and SSL settings*
  - *S/MIME*
- *Integrated commercial provider email configuration*
  - *iCloud*
  - *Google/Inbox*
  - *Exchange Online*
  - *Yahoo*
- *PRI updates/PRL updates/baseband updates*
- *Radio firmware*
- *IMEI vs. IMSI*
- *VPN*

How to configure a wireless/cellular data network

- Cellular network
    - The cellular data network settings are usually obtained automatically from the SIM card/cellular network
    - If not, access the Cellular options from the phone's option menu
    - Options to configure are the APN name, and a few other settings. You can obtain the correct settings from the carrier.
- Airplane Mode
    - You can select "Airplane Mode" from the options to turn off all external communication (Wi-Fi, NFC, Bluetooth, and Cellular)
    - You can enable or disable cellular data (when disabled, you may make and receive phone calls and SMS messages only). This is useful when roaming and will incur additional charges.
- Tethering/Hotspot
    - Tethering allows you to connect your phone to another phone or computer via USB or Bluetooth for the purposes of sharing data
    - A Hotspot allows you to connect your phone to another phone or computer via Wi-Fi for the purposes of sharing an internet connection
    - Go to Options and choose the USB tethering or Configure Wi-Fi hotspot option



Tethering & portable hotspot

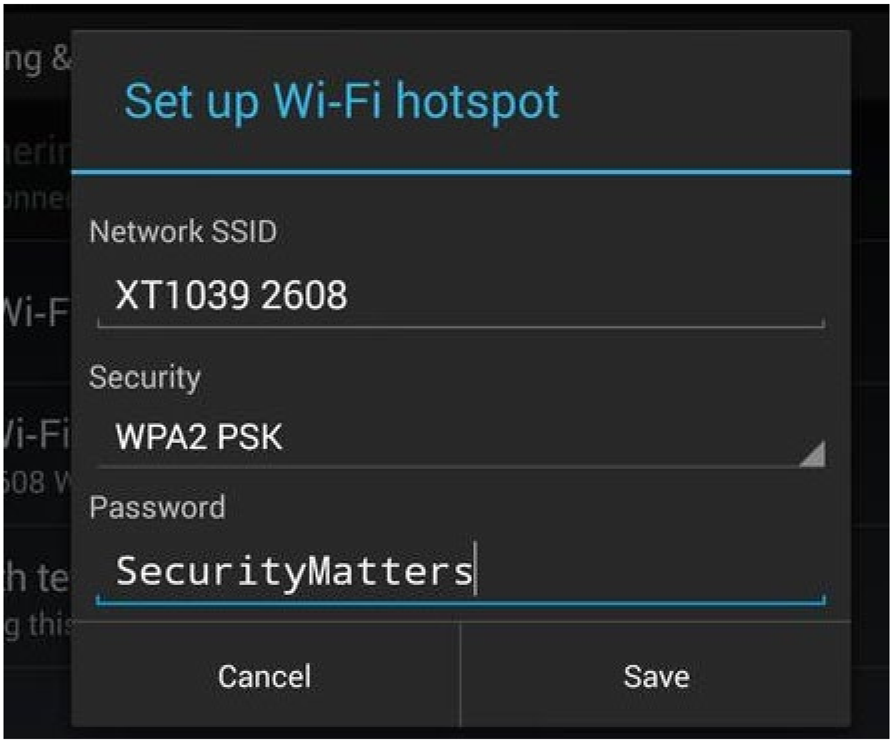
USB tethering
USB connected, check to tether □

Portable Wi-Fi hotspot □

Configure Wi-Fi hotspot
AndroidAP WPA2 PSK portable Wi-Fi hotspot

Bluetooth tethering
Not sharing this phone's internet connection □

Help



Set up Wi-Fi hotspot

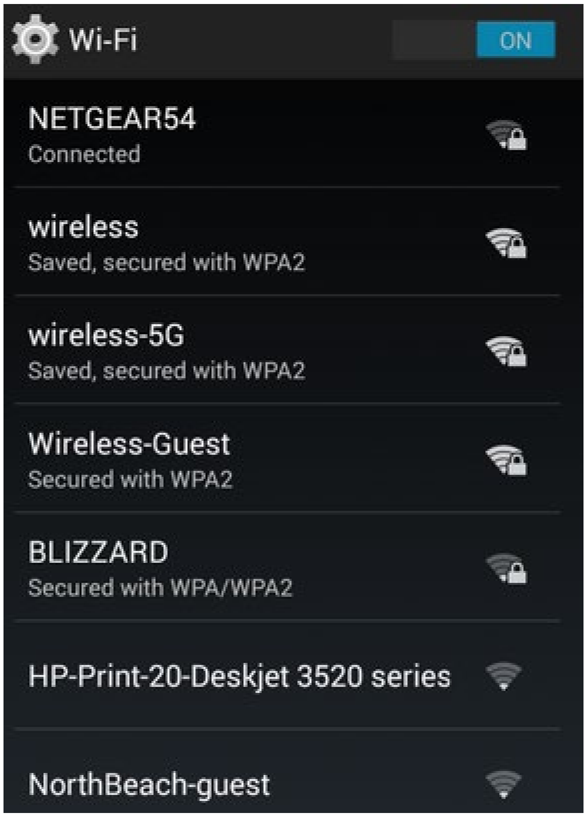
Network SSID: XT1039 2608

Security: WPA2 PSK

Password: SecurityMatters

- You can select the following options
  - SSID name
  - Security type
  - Password

        - Devices that are blocked from connecting
    - The SSID and password are generated randomly by default, but you can change them to something that you will remember.
- Wi-Fi
    - Go to Options and choose Wi-Fi
    - Choose the correct SSID
    - The phone will attempt to connect. You will need to enter the password or username/password combination for the SSID
    - If you're attempting to connect to a hidden SSID, you must enter the SSID/password manually
    - The Wi-Fi menu shows you the signal strength of each Wi-Fi network
    - Some phones aren't compatible with 2.4 GHz or 5 GHz networks



NETGEAR54
Connected

wireless
Saved, secured with WPA2

wireless-5G
Saved, secured with WPA2

Wireless-Guest
Secured with WPA2

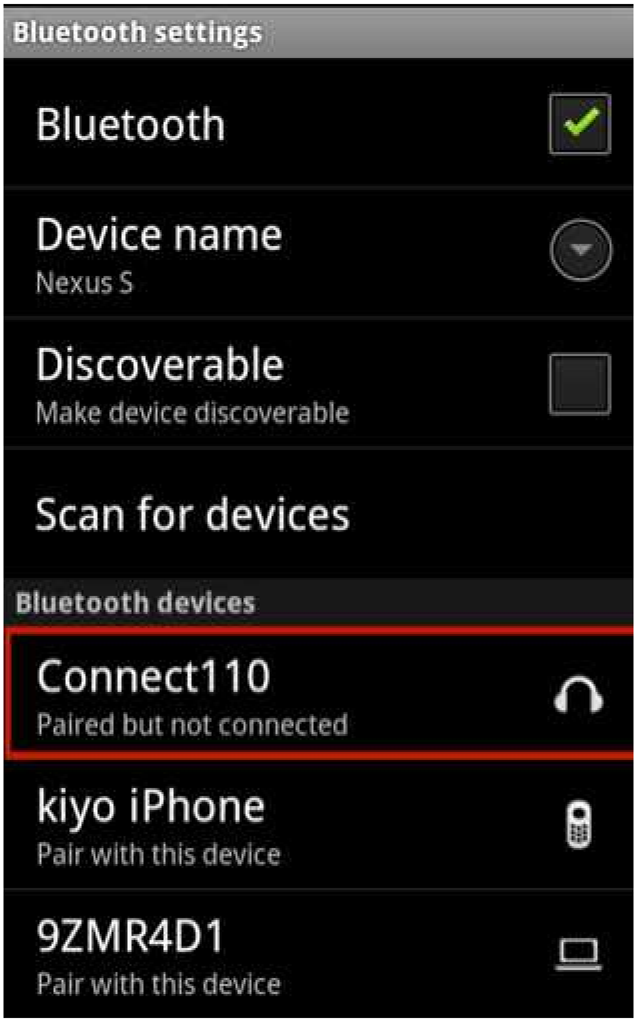
BLIZZARD
Secured with WPA/WPA2

HP-Print-20-Deskjet 3520 series

NorthBeach-guest

Bluetooth

- Select Bluetooth from the options menu
- The Bluetooth menu shows you a list of paired Bluetooth devices
- To add a new device
    - Choose “Scan for devices” on the phone
    - Choose “Scan for devices” on the device that you want to pair with (or put the device in pairing mode by pressing the Bluetooth button on it)
    - The phone will show you a list of detected devices
    - Choose the device that you want to pair with
    - You may be required to enter a password (the device that you’re attempting to pair with will provide you with a password)
    - The devices will connect together
    - You may need to configure additional settings, depending on the type of device



Bluetooth settings

Bluetooth ☑

Device name
Nexus S

Discoverable ☐
Make device discoverable

Scan for devices

Bluetooth devices

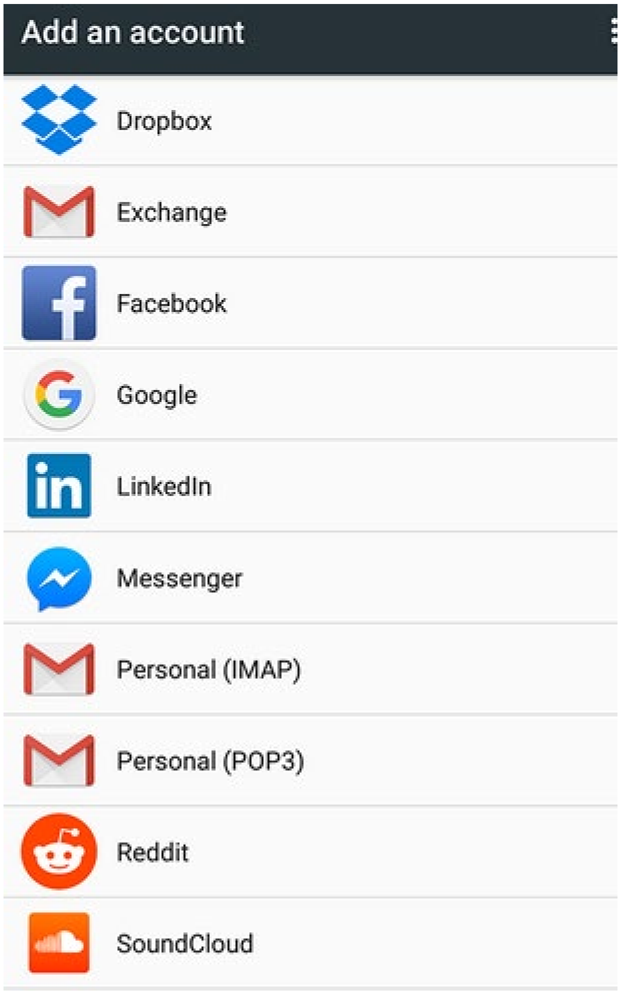
Connect110
Paired but not connected

kiyo iPhone
Pair with this device

9ZMR4D1
Pair with this device

E-mail Configuration

- Android and iOS operating systems have default "Mail" apps
- To set up an e-mail account
  - Choose Accounts from the Options menu
  - Choose the type of account



  - You must enter your username/password
  - The phone will automatically detect the additional settings
  - If detection fails, you may be prompted to enter the settings manually (username, password, e-mail server address, etc.)
- You may choose to use another type of app (Outlook, Gmail) to access your e-mail
- Use another app
  - Install the e-mail app

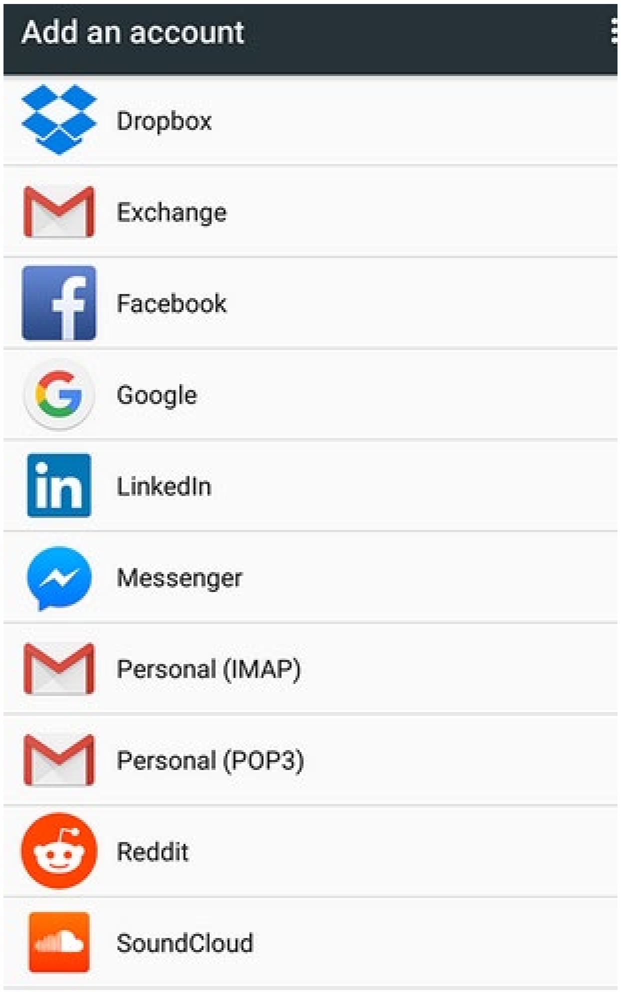
  - Add a new account inside the app
  - Enter username/password
  - App will attempt to detect settings automatically
  - If detection fails, you may be prompted to enter your settings manually
  - You can obtain the correct settings from your e-mail provider

- E-mail communication protocols
  - POP3
    - The server receives e-mail messages and holds them
    - Your phone/device will download the messages from the server
    - Once downloaded, the server deletes the messages
  - IMAP
    - The server "syncs" with the phone and possibly other devices, if you have multiple devices to access the same e-mail account
    - When an item is created by or deleted on the phone/device, it is created on or deleted by the server
    - The server syncs e-mails, contacts, and calendar items
  - Port and SSL Settings
    - Port and SSL Settings are automatically detected by the e-mail app. If detection fails, you must enter them in manually.
    - The e-mail provider may have specific port settings for authentication. You must specify the port in use (common ports are 25 and 587, although an e-mail provider may use a non-standard port)
    - The e-mail provider use SSL (Secure Sockets Layer), TLS (Transport Layer Security), or no security. You must specify the type of security in use
  - SMTP
    - Simple Mail Transfer Protocol
    - Protocol for sending messages only
    - You must authenticate with the SMTP server to send messages

    - Your SMTP username/password may be the same as your POP3 or IMAP account username/password
- S/MIME
    - Secure/Multipurpose Internet Mail Extensions
    - Not actually an e-mail protocol
    - Standard for public key encryption
    - Allows an e-mail client to encrypt e-mail data
- Microsoft Exchange
    - Not mentioned in the outline, but very common in the corporate world
    - Similar to IMAP
    - Allows e-mail, contacts, and calendars to sync with the server
    - Provides advanced features such as a global address directory, automatic e-mail replies, photographs/job titles of recipients, conference room bookings, etc.
    - Also integrates with Active Directory

Commercial Email Provider Configuration

- iCloud
    - Proprietary service offered by Apple for iOS users
    - Must pay a fee to use, and must pay additional fees depending on storage capacity used
    - iCloud allows you to back-up and sync your photos, passwords, documents and settings across multiple Apple devices
    - iCloud provides you with an optional @icloud e-mail account
    - iCloud account allows you to manage your phone
    - Users are prompted to set up an iCloud account or log in to an iCloud account when setting up a new iCloud device
- Google/Inbox
    - A Google account can be used to manage an Android phone
    - Can add account from Settings/Accounts page (choose Google account)



  - Corporate Google Accounts (Google Apps for Business) can be used to manage corporate devices, prevent theft, remotely wipe phones, prevent unauthorized app installation, etc.
  - Google account will sync data, photos, messages, and settings. Account can also detect stolen devices and provide GPS coordinates of missing phones
- Exchange Online
  - Part of Office 365, and sold by Microsoft (pay per user per month)
    - Multiple options available depending on needs of organization
  - Functions on any phone (iOS or Android)
  - An administrator will create the Exchange account
  - Can set up the account in Outlook for Android/iOS or in the Accounts page on Android/iOS
  - Enter username/password, and the phone will automatically detect additional settings

    - Exchange will sync more data than IMAP, including corporate address book and away messages
    - Exchange works with Skype (allows you to send messages and make calls)
- Yahoo
    - Create a new Yahoo e-mail account on the Yahoo website
    - Set up the Yahoo account on the phone like any other account (as IMAP or POP3)
    - Yahoo mail is not a popular option among corporate or personal users

PRI Updates/PRL Updates/Baseband Updates

- Updates
  - The phone contains software/hardware including a processor, memory, RAM, etc.
  - The phone also contains a hardware radio for communicating with the cell tower
  - The phone manufacturer will regularly release updates for the phone's operating system and/or hardware
  - The phone will automatically check for updates and prompt you to download/install them
    - Typically, download updates when connected to Wi-Fi and install them when you aren't using the phone
- PRI Updates
  - Primary Rate Interface
  - Provides communication between the phone and the phone's hardware radio
  - The communication program requires software updates
- PRL Updates
  - Preferred Roaming List
  - Contains a list of radio frequencies that the phone can broadcast on
  - When you travel with a phone to a different network, or when the carrier upgrades their network, the phone will automatically download a new list
  - Sometimes a manual update is necessary. You can manually obtain an update by dialing a specific number. For example, on a Verizon network, dial *228.
- Baseband Updates
  - Chip that controls GSM and 3G/4G/5G phone radio waves
  - The software that runs on the baseband chip is separate from the software that runs on the phone (Android or iOS)
  - Software updates are made available, which improve stability and battery life

Radio Firmware

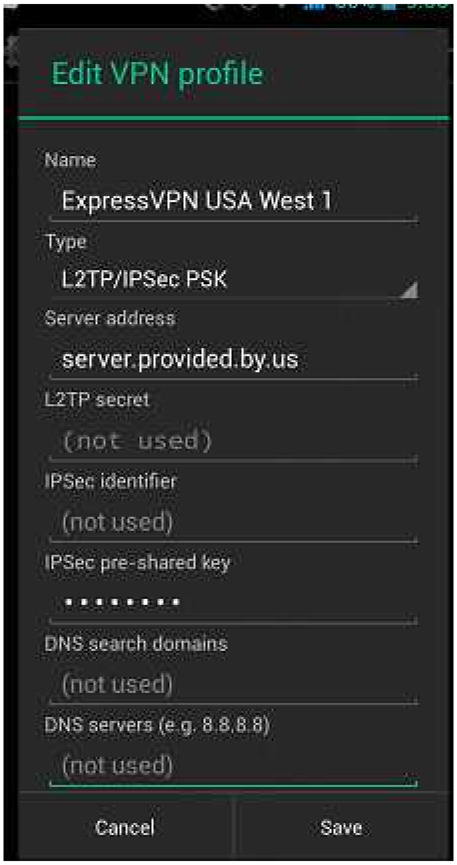
- The firmware works with the operating system to control Wi-Fi, GPS, NFC, and other types of connectivity
- Phone manufacturers release new versions of the firmware, which improve connectivity and battery life
- You can manually download a firmware update and install it. Connect the phone to a computer and run the firmware update utility.
- In many newer phones, the Firmware is controlled by the Operating System

IMEI vs. IMSI

- IMEI
  - International Mobile Equipment Identity
  - Unique 15-digit number for identifying a phone
  - When a phone connects to a cellular network, it shares its IMEI number
  - The cellular network uses the IMEI to uniquely identify each phone, and can block stolen phones
- IMSI
  - International Mobile Subscriber Identity
  - Unique 15-digit number that identifies a SIM card
  - The SIM is inserted into the phone
  - When the phone connects to the cellular network, it shares the IMSI number on the SIM
  - The SIM is lined to a mobile phone subscriber
  - The cellular provider uses the IMSI to bill the correct subscriber for the usage

VPN

- A VPN is a Virtual Private Network
- A VPN allows a device to connect to a corporate network, even if it is not physically present on the network
- Allows users who travel or work from home to access resources on the corporate network
- VPN creates a tunnel between the device and the corporate network and routes all traffic through the tunnel
- You can set up a VPN connection on a cellular phone or tablet
- You can create the VPN in the Settings menu
    - o Choose VPN from settings
    - o You can create multiple VPN connections
    - o Enter the correct details for the VPN



Name
ExpressVPN USA West 1

Type
L2TP/IPSec PSK

Server address
server.provided.by.us

L2TP secret
(not used)

IPSec identifier
(not used)

IPSec pre-shared key
••••••••

DNS search domains
(not used)

DNS servers (e.g. 8.8.8.8)
(not used)

- You can install a separate VPN application

1.7 Given a scenario, use methods to perform mobile device synchronization.

- *Synchronization methods*
    - *Synchronize to the cloud*
    - *Synchronize to the desktop*
    - *Synchronize to the automobile*
- *Types of data to synchronize*
    - *Contacts*
    - *Applications*
    - *Email*
    - *Pictures*
    - *Music*
    - *Videos*
    - *Calendar*
    - *Bookmarks*
    - *Documents*
    - *Location data*
    - *Social media data*
    - *E-books*
    - *Passwords*
- *Mutual authentication for multiple services (SSO)*
- *Software requirements to install the application on the PC*
- *Connection types to enable synchronization*

Synchronization Methods

- We set up synchronization settings in the previous sections (examples include iCloud account, Google account, Microsoft Exchange, Bluetooth connection)
- Once the settings are in place, the phone will connect and sync with the cloud/desktop/automobile automatically, provided it is connected to the internet/desktop/automobile
- Cloud
  - Sync e-mail, contacts, photos, passwords, or complete back-up of the phone
- Desktop
  - Sync all files and data
  - Both the phone and the Desktop can sync with the cloud
  - Desktop and phone sync over a local network, internet, or USB connection
  - E-mail usually syncs between the phone and the server, and then between the server and other user devices (tablet, other phones, desktops)
  - Can use a third-party application to sync phone (examples include Wondershare, SyncMate)
- Automobile
  - Sync contacts, recent calls received and made, possibly GPS location or updates.
  - For safety reasons, very few items sync with the vehicle except those that can be accessed hands free.

Types of Data to Synchronize

- There are many types of data that can sync
  - Contacts
  - Applications
  - Email
  - Pictures
  - Music
  - Videos
  - Calendar
  - Bookmarks
  - Documents
  - Location data (typically turned off by default)
  - Social media data
  - E-books
  - Passwords (passwords are typically encrypted before being synced; can only be viewed on the original device)
- It's possible to select the types of data that can be synced or not synced
- Data can be synced with one application provider or with multiple providers. Some examples:
  - Facebook app may only sync with Facebook servers, and only back up Facebook data
  - E-mail data syncs with e-mail provider
  - Photos sync with Google Photos app

Mutual Authentication for Multiple Services (SSO)

- Single Sign On allows a user to log on once with an authentication server
- The authentication server provides a token to authenticate the user across multiple services (avoids having the user log in multiple times)
- Single Sign On uses Lightweight Directory Access Protocol
- Many different providers offer Single Sign On
    - Google
    - Microsoft (Active Directory)
    - Some social media providers
- For example, a user could log in to their Windows computer via Windows Authentication
    - Windows would automatically sign them into their e-mail (Outlook), Skype, procurement software, HR software, etc.
    - Each of the other software applications authenticates through the same Windows credentials
    - The user only logs in once, and the Microsoft Active Directory server authorizes them to access all of the other resources

Software Requirements to Install the Application on the PC

- There are three scenarios
    - A phone sync app
        - Examples include iTunes and Wondershare
        - This app requires a recent version of Windows or OSX
        - It communicates with the phone either via USB or the network
        - A user can back up all phone data (subject to the security restrictions on the phone)
    - A phone app with a Windows or OSX version
        - Examples include iMessage and WhatsApp
        - You can download a Windows version of WhatsApp, which syncs with the WhatsApp app on your phone and send/receive messages from both the PC and the phone
        - This app type only syncs data related to the app
    - A web-based service
        - Examples include Facebook, Twitter, LinkedIn
        - The data accessed through the phone app can also be accessed through a web site (web browser)
        - This app type only syncs data related to the app
        - Does not back up any data to the user's computer
- Can use an Android emulator (like Bluestacks) to run Android apps on a PC or Mac

Connection Types to Enable Synchronization

- Typical synchronization connection
    - Phone connects to internet and syncs data with server
    - Other devices (other phones, tablets, desktop) connect to server and download/sync data over the internet
- Alternative synchronization connection
    - Connect phone directly to the PC over USB, or over a local network (the PC and phone locate each other on the local network)
    - The two devices share data directly
- Print from iOS and Android through a wireless connection to a local printer or Google Cloud print

Part C: 220-1001 2.0 Networking

2.1 Compare and contrast TCP and UDP ports, protocols, and their purposes.

- *Ports and protocols*
    - *21 – FTP*
    - *22 – SSH*
    - *23 – Telnet*
    - *25 – SMTP*
    - *53 – DNS*
    - *80 – HTTP*
    - *110 – POP3*
    - *143 – IMAP*
    - *443 – HTTPS*
    - *3389 – RDP*
    - *137-139 – NetBIOS/NetBT*
    - *445 – SMB/CIFS*
    - *427 – SLP*
    - *548 – AFP*
    - *67/68 – DHCP*
    - *389 – LDAP*
    - *161/162 – SNMP*
- *TCP vs. UDP*

What is a Port and Protocol?

Protocol

- Formal standard/policy for two or more network-enabled devices to communicate with each other
- May include a set of commands that the two parties/devices can issue to each other
- All devices using the protocol understand each other
- For example, HTTP (Hyper Text Transfer Protocol) allows a web server to share website data with a web browser.
    - The web browser understands HTTP and knows which commands it should issue to the web server
    - The web server understands HTTP and understands the commands received from the web browser. It understands what the commands mean and responds appropriately to deliver website data to the browser.

Port

- A network device/computer server may receive data from multiple network sources
- The device may have several applications operating on it, each of which offers a different service (for example e-mail server, web server, DNS server)
- An application that offers a service will listen on/bind to a port or set of ports
- The operating system will forward traffic to the correct application based on the port that it is listening on
- Port numbers range from 1 to 65535
- The port number is appended to the IP address
- For example, HTTP (website) traffic is typically sent/received on Port 80
- If a web server has an IP address of 192.168.0.1, and the port is 80, then the full address is 192.168.0.1:80
- The web server software listens on port 80
- Traffic that is received on port 80 is forwarded to the web server. Traffic received on other ports is forwarded to other applications
- Many of the lower number ports (1 to 500) are reserved for specific applications, but an application can use a non-standard port to communicate

Common Ports and Their Typical Protocol

Port Number/Name	Use
21/FTP	File Transfer Protocol Used to transfer large files over a network
22/SSH	Secure Shell Used to communicate securely with a server, especially UNIX servers. Can provide remote control of a server.
23/Telnet	Telnet Like SSH, but does not contain any security Older protocol that is no longer popular due to lack of security
25/SMTP	Simple Mail Transfer Protocol Used to communicate with an e-mail server (for sending e-mail only) Can be secure or insecure, depending on whether client encrypts data
53/DNS	Domain Name Server Translates Domain Names/Hostnames to IP addresses (necessary to locate network resource)
80/HTTP	Hyper Text Transfer Protocol Used to transmit web site data (insecure)
443/HTTPS	Hyper Text Transfer Protocol-Secure Used to transmit web site data (secure)

3389/RDP	Remote Desktop Protocol Allows you to remotely connect to a Windows server or computer via a Graphical User Interface
137-139/NetBIOS/NetBT	NetBIOS/NetBT Allows computers to communicate with each other over a network Provides name services (provides each computer with a unique hostname), and communications
445/SMB/CIFS	Server Message Block/Common Internet File System Allows computers on a network to share files and printers
427/SLP	Service Location Protocol Allows computers to find services on a local network A device will broadcast a URL containing the location of a service over SLP Other devices can connect to the URL over SLP to use the service
548/AFP	Apple Filing Protocol Allows Apple devices to share files
67/68/DHCP	Dynamic Host Configuration Protocol Allows a device to request a dynamic IP from a DHCP server Allows a DHCP server to dynamically assign IP addresses to other devices

389/LDAP	Lightweight Directory Access Protocol Allows users to access different directories Directories include e-mail directories, users, phone numbers, printers, and services
161/162/SNMP	Simple Network Management Protocol Allows a user to collect and manage data about managed network devices, including routers, switches, servers, and printers

Difference Between TCP and UDP

An application will send data to another computer (for example, a web server needs to send a website to a visitor). The application is not concerned with the details of how the data is sent or received. TCP/UDP handles the transmission details.

TCP

- Transmission Control Protocol
- TCP
    - The sender and recipient establish a "connection"
    - The sender breaks the data up into "packets".
    - Each packet is numbered.
    - The packets are sent over the network or internet.
    - During transmission some packets might get lost. These are known as "dropped packets". The packets won't necessarily arrive in the order that they were sent.
    - Errors are okay, because
        - The recipient receives the packets and puts them in the correct order
        - The recipient acknowledges receipt of each packet
        - The recipient requests that the sender resend missing packets
- Most internet traffic is TCP (FTP, HTTP, etc.)
- TCP is slower but reduces data loss. When data integrity is important, TCP is better. For example, if we download an Excel spreadsheet, we can wait a few seconds/minutes for the file to download, but missing part of an Excel spreadsheet would be unacceptable, therefore FTP is TCP.

UDP

- User Datagram Protocol
- UDP
    - Just like TCP, except that
        - No connection is created
        - Packets aren't numbered (they won't necessarily arrive in the correct order)

        - The recipient does not acknowledge receipt of any packets. Lost packets are not resent.

- Used in Voice Over IP systems, online games, etc.
- UDP requires a better-quality connection to perform reliably
- UDP is faster but risks data loss. For example, in a phone conversation, we need to hear what the other person is saying in real time. We don't have time to break up the conversation and reassemble it. It is a reasonable trade-off if we miss a few seconds of the conversation.

2.2 Compare and contrast common networking hardware devices.

- *Routers*
- *Switches*
  - *Managed*
  - *Unmanaged*
- *Access points*
- *Cloud-based network controller*
- *Firewall*
- *Network interface card*
- *Repeater*
- *Hub*
- *Cable/DSL modem*
- *Bridge*
- *Patch panel*
- *Power over Ethernet (PoE)*
  - *Injectors*
  - *Switch*
- *Ethernet over Power*

Network Equipment

- Remember that a network device could have multiple functions
- A typical home router can be a modem, router, switch, firewall, and access point, all in one
- For the purposes of the A+, consider only Small Office/Home Office network equipment

Router

- Forwards data traffic between two networks (between a Local Area Network and a Wide Area Network)
- The router contains a routing table or routing policy
- When the router receives data, it reads the destination IP address of the data
- It looks up the IP address in the routing table to determine the correct destination
- It sends the data to the correct destination

Switch

- Connects multiple devices over a local network
- A switch reduces traffic collisions (compared to a HUB) because multiple devices can communicate at the same time.
- Can connect multiple switches together to increase the number of available ports
- A switch maintains a table of connected devices
    - Each time a switch receives data on a port, it identifies the source MAC address (the sender's MAC address)
    - It records the source MAC address and port in a table
    - When the switch receives data that it must forward, it looks up the destination MAC address in the table, and forwards the data to the appropriate port
    - If the destination MAC address is not found in the table, then the switch broadcasts the data across all the ports
- There are two types of switches
    - A managed switch allows you to change settings on a per-port basis. Settings that can be modified include VLANs, PoE status, port name, and security rules
    - An unmanaged switch does not allow you make any changes.
- A switch can have ethernet or fiber connections
- Some switches provide PoE (power over ethernet) and some don't

Access Points

- Allows a Wi-Fi device to connect to an Ethernet network
- The Access Point broadcasts an SSID
- Each Access Point connects to a switch over ethernet
- Access Points are typically powered via PoE, but could also be powered by DC adapters
- Each Access Point can be configured independently, or multiple access points can receive their configuration from a controller
  - Access points can work together to adjust their broadcast channel and power, in order to avoid overlap
- An Access Point can have different antenna shapes so that it can adequately cover different areas (conference room, football stadium, parking lot)

CISCO SYSTEMS
PEEL HERE
Position the access point on a flat surface and grasp it with both hands.
Cable access notch and arrow
Remove this label from cover after installation
47-16829-01 Rev A0
Gently push the cover outward until it stops as shown in the illustration above.

Cloud Based Network Controller

- A Cloud Based Network Controller allows an administrator to configure and administer a network from a web-based application
- Known as "software defined networking" or "zero touch provisioning"
- How it works
    - Cloud-based network devices (Routers, Switches, Firewalls, and Access Points) are connected and installed like in a traditional network
    - Network administrator uses controller to create broad, general rules for how the network will function, including
        - VPNs and Wide Area Networks
        - Wi-Fi SSIDs and authentication
        - Firewall Settings
    - Devices automatically connect to the controller over the internet
    - Controller pushes a configuration onto each device automatically
    - Controller pushes regular firmware updates onto the devices
    - Administrator can monitor network activity from cloud
    - Cloud devices can work together
- Key advantages
    - Easier to configure and maintain network
    - Specific network skills and knowledge not required
    - Cloud devices can share intrusion data for more advanced protection
    - Devices automatically work together to implement network policy
- Key disadvantage
    - Requires payment of a monthly/yearly license fee to continue using network equipment
    - Requires devices to connect to the internet to receive their configuration
- Example is Cisco Meraki

Firewall

- Monitors and controls network traffic
- A firewall contains a set of rules that determine which traffic is permitted and which traffic is not permitted
- Rules can permit/block traffic based on
  - Source IP Address/Port
  - Destination IP Address/Port
  - Time of Day
  - Application Type
  - User
  - Combination of the above rules
- Most firewalls come with a set of default rules
- Additional specific rules can be programmed
- Some firewalls have heuristics (advanced threat detection) based on artificial intelligence
- A Whitelist is a list of parameters that are automatically permitted. Traffic that doesn't meet the parameters on the whitelist is automatically blocked.
- A Blacklist is a list of parameters that are automatically blocked. Traffic that doesn't meet the parameters on the blacklist is automatically permitted.
- Cloud connected firewalls can download new rules from the internet automatically, based on newly-detected threats.
- Examples are Cisco ASA, and FortiGate.

Network Interface Card (NIC)

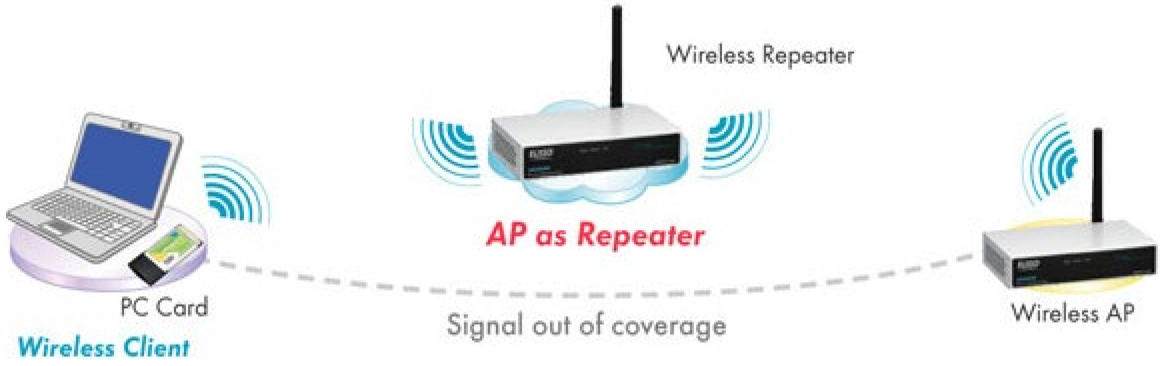
- Allows a device to connect to the ethernet network
- There are two types of NICs: Copper & Fiber
- Copper NIC
    - A Network Interface will operate at a particular speed, and at a particular duplex setting
    - Speed
        - A NIC will operate at one or more of the following speeds: 10Mbits/s 100Mbits/s, 1000Mbits/s, 10Gbit/s
        - Older NICs operate at only 10Mbits/s or 100Mbits/s (known as 10/100)
        - Newer NICs operate at 10/100/1000
        - Only high-end NICs for servers can operate at 10Gbit/s
    - Duplex
        - A NIC can operate as "half-duplex:" or "full-duplex"
        - Half-duplex uses two pairs of wire in an ethernet cable
        - Full-duplex uses four pars of wire in the ethernet cable
    - When a connection is established between a NIC and a Switch/Router, the two devices will negotiate a speed and duplex setting
    - NIC Form Factor
        - Most motherboards contain a soldered NIC chip (most common for laptops and desktops). A consumer-grade NIC will have one port.
        - NICs are also available as separate PCI cards. A NIC intended for use in a server may have several ports.

        - USB to Ethernet adapter. Can create an ethernet port for a laptop or other device that doesn't have a NIC.

- Fiber NIC
    - Like Copper NIC, except that it accepts a fiber optic cable
    - Speed
        - Operates at 100Mbits/s, 1000Mbits/s, 10Gb/s
        - Some can also operate at 40Gb/s or 100Gb/s
    - Most commonly installed on servers and storage appliances
    - The Fiber NIC will be a separate PCI card

Repeater

- Extends the range of a Wi-Fi network
- It's not always possible to install an ethernet cable to a location where an Access Point is required (ethernet cables have a maximum operating length of 300 ft)
- A repeater can be installed instead
- The repeater "repeats" signals from an Access Point
- Requires a power source
- Mesh Network
  - Can connect multiple access points in a mesh network where some APs don't have a connection to the switch; they repeat data to APs that do
- Disadvantages
  - Adding too many APs can cause latency because data must travel through multiple APs before reaching the switch (it takes longer for data to reach the switch)
  - AP that is physically connected to the switch is responsible for handling all the traffic. It may become overloaded.



Hub

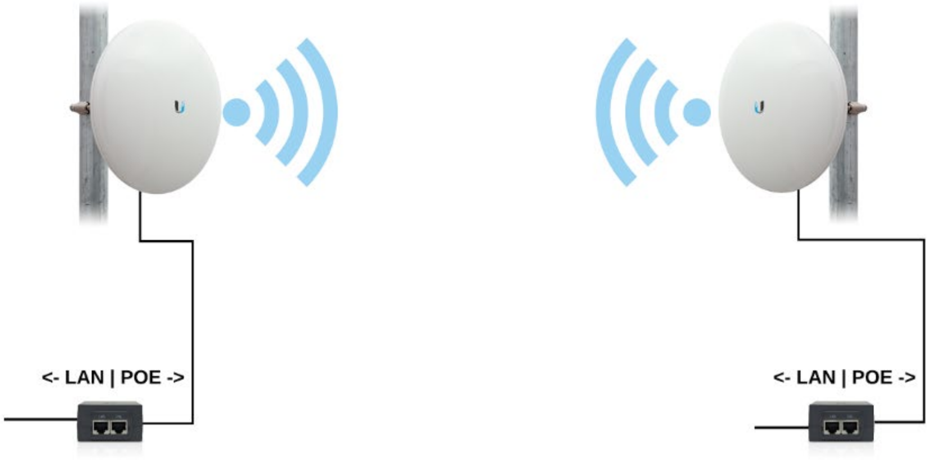
- Also known as an ethernet hub, active hub, network hub, repeater hub, or multiport repeater
- Hubs are mostly obsolete and should be replaced by switches
- When a hub receives traffic (a data packet) it will broadcast the packet on all its ports
    - All devices connected to the hub receive the packet, even if it's not addressed to them
- Disadvantages
    - Hubs have no management and don't keep track of which devices are connected to which ports
    - A hub only allows one device to communicate at a time

Cable/DSL Modem

- Converts Cable or DSL connection to ethernet (Cable or DSL connection is an analog signal and must be converted into a digital signal)
- A modem is typically supplied by an Internet Service Provider
- Small network
  - In smaller networks (like home networks), the modem may act as a router, switch, wireless access point, and/or firewall
  - Most ISPs will supply modem/router/access point combinations for their residential customers
  - A modem can be simply a modem, with no other functions (example Speedtouch modem)
- Large network
  - In larger networks, the modem is "bridged" so that it acts as a modem only
  - All other configuration features of the modem become inaccessible
  - Customer supplies separate router, switch, firewall, and access point

Bridge

- Connects two networks so that they act as one network
- A bridge is different from a router, which connects two separate networks in a way that keeps them distinct
- Bridge functions
  - A bridge will pass routing, DHCP, and other services between the two network segments
  - Records the address of each network device and the side of the bridge that it is connected to
  - Forwards data to the correct side of the bridge based on its destination address
- Examples of bridges
  - Wireless bridge can receive a Wi-Fi signal and convert it into an ethernet (wired) signal. Can connect a Wi-Fi bridge to a NIC or switch and provide it with network access in an area where no ethernet port is available
  - Can use two long-range point-to-point Wi-Fi antennas to connect two networks together in an area where installing a cable is not possible. An example is a Ubiquiti NanoStation.



Patch Panel

- Ethernet cables/fiber optic cables terminate from a patch panel (in the back of the panel) to a network jack (in a wall, typically)
- The patch panel and wall jacks should be labelled so that they can be identified
- A patch cable is connected from the front of patch panel to the switch (or other appropriate network device)
- Good security practice is to patch in only the ports that are in use
- There are many models of patch panels (Copper and Fiber)
    - Copper Patch Panels
        - Manufactured to Cat5e, Cat6, or Cat6A standards
        - 12-port, 24-port or 48-port are common sizes
        - 24-port and 48-port panels fit into standard network racks; 12-port patch panels can be wall-mounted
    - Fiber Optic Patch Panels
        - Less common
        - Typically used to connect multiple server rooms together
        - Can be rack-mounted or wall-mounted
    - Other types of patch panels
        - BIX, 110-block, 66-block for copper phone wiring
        - Coaxial patch panels

Patch Panel - Copper

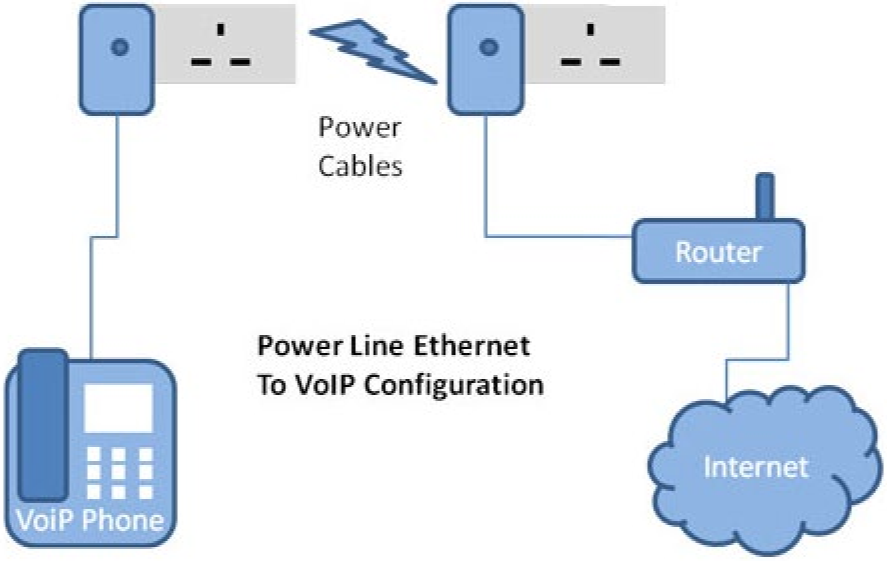
Wall Jack - Copper

PoE

- Power over Ethernet
- Allows us to transmit power and data over an ethernet cable simultaneously
- Provides power to APs, VoIP Phones, IP Cameras, etc.
- A PoE device may accept power from an AC-DC adapter instead of through PoE
- There are two ways to transmit PoE: from a switch or over a power injector
- Switch
    - A PoE-capable switch will provide PoE, different switches have different wattage capacities
    - It's important to select a switch with enough wattage for the devices that you are connecting
    - Some switches may support PoE on only some ports
    - A switch can automatically detect if a connected device requires power, and then supply PoE
    - You can toggle the power on a switch port, if it is a managed switch
        - Useful for remotely rebooting connected devices such as APs and cameras, if they crash
- Power Injector
    - Power injector sits between the switch and the device requiring power
    - Power injector requires a normal power outlet
    - Good for when there is no PoE switch and a PoE device needs to be powered
    - A power injector can only power one device
    - If you have many PoE devices, a PoE switch is better than multiple power injectors

Ethernet Over Power

- Uses two adapters to transmit ethernet over a high-voltage electrical system
- Connect one adapter to the network and to a power outlet; connect the other adapter to a power outlet and to a device requiring network access
- Good for houses or other building where it is not practical/possible to install ethernet cable
- Can also provide PoE



2.3 Given a scenario, install and configure a basic wired/wireless SOHO network.

- *Router/switch functionality*
- *Access point settings*
- *IP addressing*
- *NIC configuration*
    - *Wired*
    - *Wireless*
- *End-user device configuration*
- *IoT device configuration*
    - *Thermostat*
    - *Light switches*
    - *Security cameras*
    - *Door locks*
    - *Voice-enabled, smart speaker/digital assistant*
- *Cable/DSL modem configuration*
- *Firewall settings*
    - *DMZ*
    - *Port forwarding*
    - *NAT*
    - *UPnP*
    - *Whitelist/blacklist*
    - *MAC filtering*
- *QoS*
- *Wireless settings*
    - *Encryption*
    - *Channels*
    - *QoS*

Basic Router Configuration

- Power on the router/switch
- Connect the router's WAN port to the ISPs modem
- Configure the name of the router
- Configure the WAN IP address of the router based on details from the ISP, including
  - DHCP or Static
  - If static, add IP address, gateway address, subnet mask, DNS server addresses
- Configure IP address for router
- Configure size/class of network
- Configure DHCP
  - Provide a range of addresses that will be part of DHCP pool
  - Configure DHCP reservations based on MAC address if necessary
- Configure remote management if needed

Basic Switch Configuration

- Connect switch to router’s LAN port via ethernet cable
- Power on switch
- Configure switch name
- Configure switch IP address for management
- Configure security rules for switch
- For each port
    - Configure VLANs handled by port
    - Configure port name/description
    - Configure port security
    - Configure PoE
    - Shutdown unused ports

Access Point Settings

- Install antennas if necessary
- Mount Access Point to wall/ceiling, or another appropriate place
- Connect Access Point to switch
- Connect Access Point to Power Injector or AC/DC adapter if switch does not support PoE
- Configure settings
    - Configure SSIDs (may have multiple SSIDs)
    - Select security type (WPA, WPA2, WPA Enterprise) for each SSID
    - Decide if the SSID will be hidden
    - Select password, or connect AP to authentication server
    - Configure security such as whitelists, blacklists, or MAC address filtering
    - Configure guest Wi-Fi, if necessary
- Configure power settings
    - Choose between 2.4GHz and 5GHz or both
    - Choose channel
    - Choose broadcast power
    - In a larger system, the APs may automatically adjust their channel and/or broadcast power

IP Addressing

- IPv4 addresses range from 0.0.0.0 to 255.255.255.255
- IP addresses are assigned in blocks to different Internet Service Providers. For example, AT&T has been assigned the IP addresses 12.0.0.0 to 12.255.255.255. An ISP can assign one or more IP addresses to their customers. These are known as public IP addresses.
- Three ranges of IP addresses are reserved for internal networks. These are known as private IP addresses. When setting up an internet network, you have a choice of three IP address schemes (IPv4)

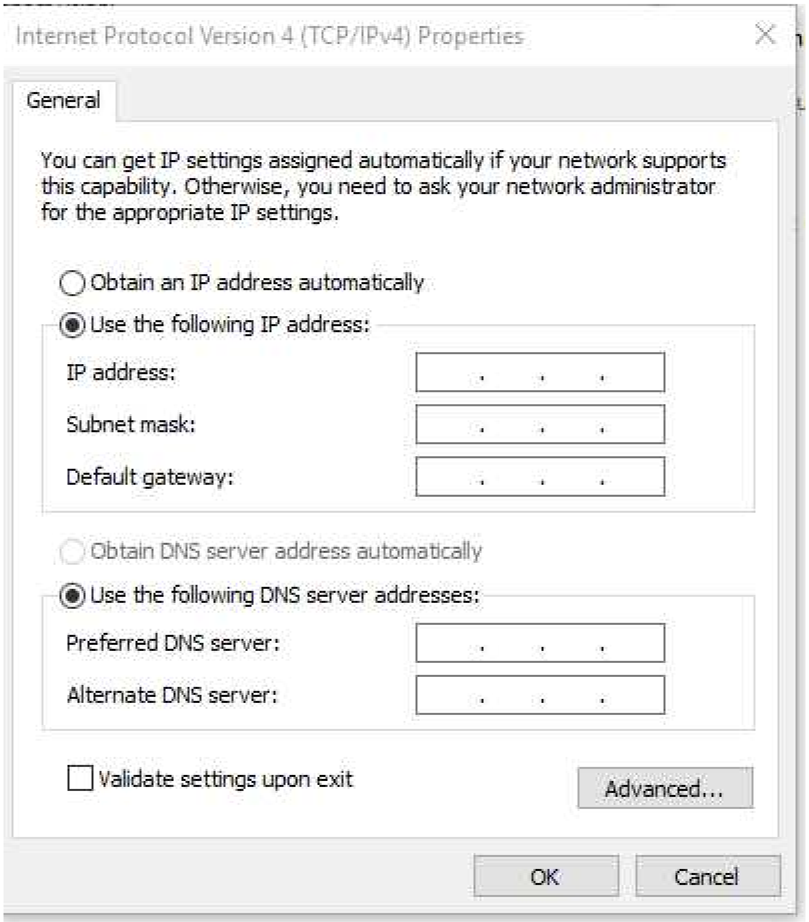
Class A	Range of IP addresses: 10.0.0.0 - 10.255.255.255 Most common for corporate networks
Class B	Range of IP addresses: 172.16.0.0 - 172.31.255.255
Class C	Range of IP addresses: 192.168.0.0 - 192.168.255.255 Most common for home networks

- You must choose the following
  - Class of network
  - Subnet mask. The subnet mask determines the number of IP addresses in the network (255.255.255.0 is a common mask and limits the network to 255 IP addresses)
  - Address of the gateway (router). Configure the address on the router.
- DHCP IP Addresses
  - DHCP = Dynamic Host Configuration Protocol
  - DHCP means that when a device joins the network, a DHCP server automatically assigns it an IP address (DHCP server also provides the device with the network's gateway IP address, subnet mask, and DNS server IP addresses)
  - When you configure the network, decide which devices, if any, will have DHCP
  - Configure a DHCP server (a router can function as a DHCP server, but so can a Windows server)

    - Choose the range of addresses that will be used for DHCP
    - User devices such as laptops, desktops, and IP phones should be DHCP
    - If a specific device should be assigned the same IP address over DHCP, set up a DHCP reservation
- Static IP Addresses
    - Permanent devices such as printers, servers, IP cameras, and access points should have static IP addresses
    - A static IP address can be set over a DHCP reservation or programmed as a static IP address directly into the device
- IPv4 vs IPv6
    - IPv6 addresses are longer, but follow the same concepts as IPv4
    - IPv6 was introduced because the world is running out of IPv4 addresses
    - IPv6 addresses follow a hierarchical routing scheme

End User Device Configuration

- Ethernet vs Wi-Fi
  - If the device is ethernet, connecting an ethernet cable between the switch and the device's NIC should automatically establish the connection
  - If the device is Wi-Fi, select the correct Wi-Fi SSID from the list, enter the correct password, username/password combination, or certificate. If the network is hidden, enter the hidden SSID and then the password.
- DHCP vs Static
  - If the device is DHCP, make sure that the network settings are set to DHCP
  - If the device is static, manually configure the static IP address in the network properties (don't forget to configure the subnet mask gateway, and DNS servers)



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

IoT Device Configuration

- Tens of thousands of IoT devices are available on the market; this is not an exhaustive list
- There are two main configuration parameters for an IoT device
    - Network connection (static vs DHCP, and ethernet vs Wi-Fi)
    - Other parameters specific to the device (thermometer temperature, camera recording time, etc.)
- Network connection
    - There are several ways that a network connection can be configured, depending on the device
    - Read the manual
    - Ethernet-connected device
        - Includes PoE devices such as cameras
        - Connect the camera to the network and allow it to power on
        - Device will automatically obtain an IP address over DHCP, or it might be configured with a static IP address
        - Use a network scanner or check the router's status page to determine IP address assigned to device.
        - Go to the IP address in a web browser to access the device's configuration page
        - Find the network settings page and change IP address to static. Why? Easier to locate and connect to the device in the future, set up port forwarding, and connect the device to other systems.
    - Wi-Fi device with user interface/touchpad
        - Access settings menu from device's screen
        - Select correct Wi-Fi SSID and insert password
        - Allow device to connect to Wi-Fi
        - Change IP address to static
    - Wi-Fi device with no user interface – USB
        - Power on device
        - Connect device to computer via USB and run software setup wizard
        - Wizard will copy correct Wi-Fi/IP address settings to device

        - Allow device to connect to Wi-Fi
        - Device will begin operating
    - Wi-Fi device with no user interface – ad hoc Wi-Fi
        - When you power up the device for the first time, it will broadcast a unique SSID (as a Wi-Fi network)
        - Connect to the SSID from a computer
        - Browse to the configuration page via a web browser or run a software setup wizard
        - Wizard will copy Wi-Fi/IP address/configuration settings
        - Disconnect from device and allow it to connect to network
- Other Configurations
    - Once a device is connected to the network/cloud, there are three ways to configure it
        - Visit the IP address of the device in a web browser to access configuration page
        - User interface (screen/buttons) if device has one
        - Cloud website / app, if device connects to cloud
- Other parameters
    - Thermostat
        - Example includes Nest thermostat
        - Configure temperatures and schedules
    - Light Switch
        - Example includes Leviton light switches
        - Configure schedule for turning lights on/off, and LED colors
    - Security Camera
        - Example includes Ring.com cameras
        - Configure recording time, sensitivity, alerts for when camera detects motion
    - Door Lock
        - Example includes Yale lock
        - Configure password, keys, authorized users, schedules
    - Digital Assistant
        - Example includes Amazon Alexa

- Configure name, authorized users
- Digital Assistants typically have artificial intelligence and record all interactions, so that they can become smarter over time

Cable/DSL Modem Configuration

- Typically, a modem automatically downloads its configuration from the ISP
- If the modem fails, you can perform a factory reset on the modem
- Modem with additional functions (router, switch, AP) can be configured as per those settings (already discussed)

Firewall Settings

- DMZ
    - Demilitarized zone
    - Allows an internal network device (such as a web server or e-mail server) to access the internet
    - Devices in the DMZ are considered less secure than the internal network and have only limited connectivity to devices in the internal network
    - Configuration options
        - Name of DMZ (can have multiple DMZs)
        - IP address range of DMZ
        - DHCP reservations/range of DMZ
        - Configure rules for allowing traffic to access devices on the DMZ (but not the LAN)
- Port Forwarding
    - Not recommended (use a VPN instead)
    - Traffic received on a specific port can be forwarded to a specific internal IP address and port
    - Advantage
        - Allows us to access internal device from outside the network
    - Disadvantage
        - Exposes internal devices to the internet.
    - For example,
        - Network's public IP address is 201.201.201.201
        - Server on LAN has private IP address of 192.192.192.192
        - We want to use RDP (port 3389) to connect to the server from outside the network. Inside the network, we can connect to the server via 192.192.192.192:3389 (our internal network can find the server).
        - Outside the network, we must type 201.201.201.201:3389, but if the network has many devices, the router won't know that it should send the traffic to the server.
        - We set up a port forwarding rule like this:

            - Source Port: 3389
            - Destination Port: 3389
            - Destination IP: 192.192.192.192
        - Now the router knows that traffic coming in on port 3389 (regardless of the source IP) should be directed to 192.192.192.192, port 3389.
        - If you can't avoid using port forwarding, you should set up a rule for denying access except to specific, known IP addresses.
- NAT
    - Network Address Translation
    - The router separates the external (public) network from the internal (private) network
    - The router will be assigned a public IP address on the public (WAN) interface (its connection with the modem)
        - You may need to statically assign this address in the router
    - The router will be assigned a private IP address on the private interface (its connection with the switch)
        - You may need to statically assign this address in the router
    - The router receives traffic (data packets) from private devices on the network, destined for the internet, and receives traffic (data packets) from the internet, destined for devices on the LAN
    - The router will convert the source address/destination address before forwarding packets between internal/external networks
    - For example
        - Our router has a public IP of 100.100.100.1 and a private IP of 192.192.192.1
        - A device on our internal network has a private IP of 192.192.192.2
        - The device on our network wants to communicate with a device on the internet (which has a public IP address of 100.100.100.2)
        - The device creates a data packet and addresses it as follows
            - Source: 192.192.192.2
            - Destination: 100.100.100.2

        - The device realizes that the destination isn't on the local network. Therefore, it sends the packet to the router, and the router sends it to the internet device at 100.100.100.2
        - The router changes the packet's address to the following before sending it over the internet:
            - Source: 100.100.100.1
            - Destination: 100.100.100.2
        - The device at 100.100.100.2 receives the packet
        - The device at 100.100.100.2 wants to reply. It only knows the address of the router; therefore, it creates a packet with the following details:
            - Source: 100.100.100.2
            - Destination: 100.100.100.1
        - The router at 100.100.100.1 receives the packet and changes it to the following:
            - Source: 100.100.100.2
            - Destination: 192.192.192.2
        - The router forwards the packet to the internal device at 192.192.192.2
    - Why do we bother with NAT?
        - The internet has a limited number of public IP addresses. We may have thousands of devices on our internal network. An ISP doesn't have enough addresses to assign a public IP address to each of our devices. Instead, they assign a single public IP to our router. All the devices on our network must share the same public IP.
        - Even if we could assign a public IP address to each device, we don't want to expose the many devices on our network directly to the internet. We prefer a private IP for each device.
        - Therefore, NAT allows multiple devices to access the internet through a single IP address
- UPnP
    - Like port forwarding
    - Allows different port numbers to be used between the internal and external networks
    - Good for when we have multiple internal services that function on the same port

- For example,
  - Server 1 has an internal IP of 192.192.192.1, and is accessible over RDP on port 3389
  - Server 2 has an internal IP of 192.192.192.2, and is accessible over RDP on port 3389
  - Internally, we can access both servers by going to either 192.192.192.1:3389 or 192.192.192.2:3389
  - We have one public IP of 200.200.200.200
  - If we set up port forwarding of 3389, we can only forward to one internal destination. What if we want to access both servers?
  - We set up the following
    - Rule #1
      - Source Port: 3389
      - Destination Port: 3389
      - Destination IP : 192.192.192.1
    - Rule #2
      - Source Port: 3390
      - Destination Port: 3389
      - Destination IP: 192.192.192.2
  - From outside the network, we can connect the following now:
    - 200.200.200.200:3389 connects us to 192.192.192.1:3389
    - 200.200.200.200:3390 connects us to 192.192.192.2:3389

- Whitelist/Blacklist
  - Allows us to override firewall rules
  - Traffic from addresses on the whitelist is allowed
  - Traffic from addresses on the blacklist is denied
- MAC Filtering
  - Allows us to filter traffic by MAC address
  - Traffic entering the network via the internet will not have a MAC address (MAC address data is not shared across networks), only IP addresses
  - We can create a whitelist of authorized devices by MAC address

    - Devices are blocked from connecting to the internal network if their MAC address isn't on the list
- A MAC address can be spoofed

QoS

- Quality of Service
- Allows us to prioritize specific types of traffic on the network to avoid poor quality transmission
- The quality of a network transmission is measured in the following areas
    - Packet loss: data sent over a network is broken up into chunks called packets. The percentage of packets that don't arrive at their destination is called packet loss.
    - Bit rate: the speed of the connection (how much data/second we can receive)
    - Latency: the amount of time it takes a packet to travel from the source to the destination. If the time is long, there could be a noticeable delay in the signal, especially for VoIP or Video conferencing.
    - Jitter: whether the packets arrive in the correct order. In a VoIP signal, if the packets don't arrive in the correct order, then the conversation will not be in the correct order.
- We should prioritize the following types of traffic
    - Streaming media
    - Voice Over IP
    - Video Conferencing
    - Critical systems such as industrial control systems and medical systems

Wireless Settings

- Mentioned earlier
- Configure encryption type on the Access Point

WEP	Wired Equivalent Privacy Uses a 40-bit password key Easily broken and not acceptable for security
WPA	Wi-Fi Protected Access – First Version Obsolete Was developed as a temporary replacement for WEP (when security problems were discovered) and quickly replaced by WPA2
WPA2	Wi-Fi Protected Access – Second Version Current Wi-Fi security in use in most organizations Uses a Four-way handshake and password to secure the connection. Wireless device and access point automatically complete handshake.
WPA3	Wi-Fi Protected Access – Third Version New standard being implemented in newer wireless devices Uses a 128-bit key (a password)
WPA2 Enterprise	Wi-Fi Protected Access – Second Version – Enterprise

	Requires a username and password Access Point must connect to an authentication server to verify user's credentials
Wi-Fi Protected Setup (WPS)	Wi-Fi Protected Setup (WPS) Allows devices with no user interface (such as printers and IoT devices) to connect to Wi-Fi Not secure WPA3 will solve issues created by WPS

- Configure Channel
    - 2.4GHz
        - When we say that a Wi-Fi network is 2.4GHz, that means that the frequency of the Wi-Fi signal is 2.4GHz
        - If two nearby networks broadcast at the same frequency, the signals will interfere, and nobody will be able to connect
        - To solve this problem, we divide the 2.4GHz spectrum into 11 channels: each channel is 22MHz wide, spaced 5MHz apart.
        - Therefore, a 2.4GHz network can broadcast on 2.412GHz, 2.417GHz, 2.422GHz, etc.
        - It's not important to know all the channels and their exact range. It's important to know that there are 11 channels.
        - If two neighboring networks choose different channels, they will each broadcast on a slightly different frequency – different enough that their signals won't interfere.
        - We can manually select the channel that we want to broadcast on
            - We should survey the neighboring networks to see what channels they are broadcasting on and select a different channel from all of them
        - If we have multiple access points in a building and their signals overlap, we should cover select a different channel for each of them

  - 5GHz
    - The channel concept applies to 5GHz networks as well
    - A 5GHz spectrum is divided into 23 channels, each is 20MHz wide
    - A 5GHz spectrum can broadcast on 5.150GHz, 5.1570GHz, etc.
    - There are more regulations for the 5GHz network and some countries do not allow some frequencies (they could interfere with weather radar and other systems)

- Two Access Points on the same network, but installed close to each other and operating on the same channel would block each other's signal
  - If we have neighboring access points, we should configure different channels for each one
  - We could also reduce the broadcast power to ensure that the access point signals don't overlap
- More advanced access points (such as Meraki) can detect interference & neighboring access points, and automatically adjust their channels and broadcast power
- Configure QoS
  - Some Wi-Fi devices allow you to prioritize traffic between the Access Point and the Switch

2.4 Compare and contrast wireless networking protocols.

- *802.11a*
- *802.11b*
- *802.11g*
- *802.11n*
- *802.11ac*
- *Frequencies*
    - *2.4Ghz*
    - *5Ghz*
- *Channels*
    - *1–11*
- *Bluetooth*
- *NFC*
- *RFID*
- *Zigbee*
- *Z-Wave*
- *3G*
- *4G*
- *5G*
- *LTE*

Wi-Fi Network Standards

- All 802.11 Wi-Fi protocols are regulated by IEEE (Institute of Electrical and Electronics Engineers)
- Considered a "one-to-many" connection
- It's important to understand that a wireless antenna can only communicate with one device at a time
  - To communicate with multiple devices at the same time, the access point must cycle between the devices
  - This is known as time division multiplexing
  - The access point sends data to one device, pauses, sends data to the next device, pauses, sends data to the third device, pauses, etc. until it has sent data to all the devices. The it starts sending data to the first device.
  - To send data to multiple devices at the same time, an access point must have multiple antennas. This is known as Multiple Input, Multiple Output.
- An access point or client (computer, phone, Wi-Fi adapter) may support multiple standards
- The standards are backwards compatible (for example, an 802.11ac device will work with an 802.11a device)

802.11a	1999 Standard Supports up to 54 Mbps in the 5GHz range
802.11b	1999 Standard Supports up to 11 Mbps in the 2.4GHz range
802.11g	2003 Standard Up to 54 Mbps in the 2.4GHz range
802.11n	2009 Standard Supports multiple-input, multiple-output (MIMO) – a device with multiple antennas Up to 72.2 Mbps with one send and one receive antenna

	Up to 450 Mbps with three send and three receive antennas
802.11ac	2014 Standard Supports multiple-input, multiple-output (MIMO) Up to 433 Mbps per antenna, or 1.3Gbps with three antennas

Frequencies

- Only two frequencies are permitted for Wi-Fi communication – 2.4Ghz and 5Ghz
- The range of a Wi-Fi signal is 50 to 300 ft
- The range is affected by signal interference (noise) from neighboring networks
- Different wall types can block or reduce the signal (glass, concrete, steel will block signals more than drywall)
- 2.4Ghz
  - 11 Channels
  - Longer range and less vulnerable to noise
  - Slower speeds
  - Older devices use 2.4Ghz
- 5Ghz
  - 23 Channels
  - Shorter range and more vulnerable to noise because walls and concrete absorb the signals easily
  - Faster speeds

Bluetooth

- One-to-one connection
- Uses radio waves to connect peripherals and transfer data
- Devices must “pair” with each other before any data can transfer
- Typically found in mobile devices
- Maximum range is 100m

NFC

- Near Field Communication
- One-to-one connection
- Typically found in mobile devices and used for contactless payment
- Range of 4cm

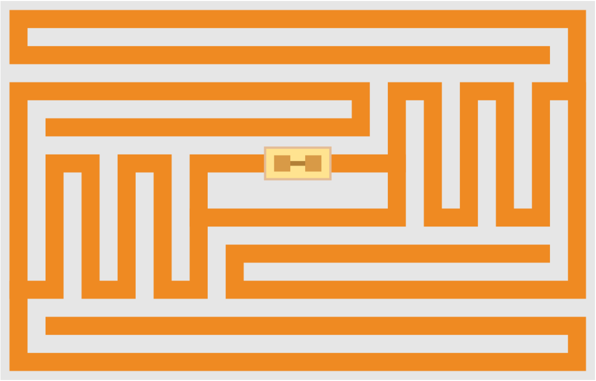
RFID

- Radio Frequency ID
- RFID has two components – a tag and a sensor
- The tag is attached to the item that we want to track or identify. The sensor detects the tag.
- There are two types of tags – active, and passive
  - An active tag contains a battery and broadcasts a signal. The sensor can pick up the signal.
  - A passive tag contains a wire loop. When the tag is near a sensor, an electric signal from the sensor activates the wire loop, and the sensor and the tag can communicate.
- Passive tags are cheaper than active tags
- A tag can be "read only", where the data contained on it can't be changed
- A tag may be combined with a barcode.
- RFID has a range of 1000 ft
- Cost of tags ranges from $0.10 for passive tags to $100 for active tags used in sensitive applications
- Uses of RFID
  - Inventory tracking. Manufacturers can tag products in their warehouses. They will be able to identify the quantity and location of each item in the warehouse.
  - Retail electronic article surveillance. Retailers will tag each product in their stores. They will install sensors at the exit. The tags are removed at the point of sale. If an individual attempts to leave the store with a tagged item, the sensor at the exit will detect the tag and sound an alarm.
  - Access control. Tags can be placed inside ID badges and vehicles. A sensor connected to a door lock or gate can provide access when detecting an authorized ID badge or vehicle.
  - Passports. Tags are installed in US passports. The tag contains the same information that is inside the passport (name, date of birth, passport number, etc.). When scanning the tag, the operator can obtain the same information contained in the passport.

RFID Tag (used in clothing to prevent shoplifting)

RFID sensor (used to provide access to vehicles)

RFID Antenna



Zigbee

- Zigbee protocol allows communication between devices requiring low power consumption and low transfer rates
- Designed for home entertainment and home automation systems, alarms, medical systems, and industrial control systems
- Provides speeds of 20 kbits/s to 250 kbits/s
- Provides a range of up to 20 meters
- Zigbee devices create a mesh network so that they can increase their range by passing the signal through a chain of devices
- Zigbee communications can be encrypted
- Zigbee was developed in 2006 and is gaining popularity

Z-Wave

- Z-wave is like Zigbee
- It is a mesh network that is used mainly in home automation
- Managed by the Z-Wave Alliance
- Z-Wave devices have a range of 24 meters
- The Z-Wave system requires a central controller, which wirelessly communicates with the other devices
- A Z-Wave controller can support up to 65,000 devices

3G/4G/5G/LTE

3G	3G (Third Generation) was a cellular network launched in 2002 3G is an analog network
4G	4G (Fourth Generation) is the current cellular network in use 4G networks support IPv6 and MIMO antennas Uses a frequency of between 700 MHz and 3 GHz A 4G antenna can cover an area of up to 3 miles
5G	5G (Fifth Generation) is the cellular network under development Specifications for the network will be complete in 2020 The network is expected to support speeds of up to 10 Gbps Will use high frequencies of up to 39 GHz 5G antennas are much smaller, but have a much shorter range (only about one city block) 5G antennas will be installed in a closer proximity to each other
LTE	LTE is Long Term Evolution It is an upgrade to 3G, and almost reaches the standards of 4G Supports speeds of up to 400 Mbits/s

	LTE is an IP-based network

2.5 Summarize the properties and purposes of services provided by networked hosts.

- *Server roles*
  - *Web server*
  - *File server*
  - *Print server*
  - *DHCP server*
  - *DNS server*
  - *Proxy server*
  - *Mail server*
  - *Authentication server*
  - *syslog*
- *Internet appliance*
  - *UTM*
  - *IDS*
  - *IPS*
  - *End-point management server*
- *Legacy/embedded systems*

Different roles of servers

- A single physical server can have multiple roles or functions
  - The word “server” can refer to a physical device or to one of the roles that a physical device fulfills
- Virtualization technology can divide a single physical server into multiple virtual servers, each of which can have a single or multiple role
- If a large capacity is required, multiple servers can be clustered together to provide a single role
- An end user is typically not concerned with the hardware setup of the servers
  - When virtualized, a server admin may not be concerned with the hardware setup either

Some server types

Server Type	Description
Web Server	Hosts websites and website data Delivers website data to end users A web server may have processing technology such as ASP or PHP A web server may interact with a database server to provide necessary data Examples include Internet Information Server and Apache
File Server	Hosts files for shared drives Can be a Network Attached Storage Device A file server will work with an authentication server to enforce permissions on the files Examples include Windows server
Print Server	A print server manages printers and print queues The printers are installed on the print server

	The print server connects users with the printers When a user prints a document, it is queued on the print server
DHCP Server	A DHCP (Dynamic Host Configuration Protocol) server dynamically assigns IP addresses to devices on the network A DHCP server keeps track of the devices that it has assigned IP addresses to A router may provide DHCP server functionality
DNS Server	A DNS (Domain Name Service) server converts domain names to IP addresses A DNS server keeps a cache of the most commonly requested websites A router may provide DNS functionality
Proxy Server	A proxy server is an intermediate server between a user and other servers. A user can make requests for websites, files, and other resources with the proxy server. The proxy server will forward the requests to other servers and provide the user with their responses. A proxy server can provide anonymous access, content filtering, and data leak protection A firewall may provide proxy server functionality
Mail Server	A mail server sends and receives e-mail on behalf of users A mail server can also store e-mails so that users can access them remotely Examples include Microsoft Exchange Server

Authentication Server	An authentication server identifies users and provides them with access to resources Examples include Microsoft Active Directory Server
syslog	Syslog is a standard for message logging A syslog server receives and stores log messages sent by other network devices

Internet Appliances

- An internet appliance could be a dedicated physical device or could be a software application that runs on a server

UTM	Unified Threat Management A UTM device provides multiple security functions (instead of having several devices each providing a single function) Features could include • Firewall • Intrusion Detection • Intrusion Prevention • Anti-Virus • Proxy • Data Leak Prevention • VPN
IDS	Intrusion Detection System An Intrusion Detection System detects attacks that are already taking place inside the network An IDS only detects attacks, it does not prevent or block traffic
IPS	Intrusion Prevention System Prevents inappropriate content and unauthorized users from entering the network An IPS can slow down the network, accidentally block legitimate traffic, or create a large amount of false alarms

	An IPS cannot monitor the content of encrypted traffic
End-point management server	An end-point management server manages "end points" or end user devices Devices could include desktops, laptops, mobile phones, VoIP phones, and printers The server can enforce security policies, install software updates and monitor user activity Examples include SCCM

Legacy/Embedded Systems

- Legacy systems are old systems that can't be replaced
- May provide a critical business function
- Embedded systems are systems that are inside other systems

2.6 Explain common network configuration concepts.

- *IP addressing*
  - *Static*
  - *Dynamic*
  - *APIPA*
  - *Link local*
- *DNS*
- *DHCP*
  - *Reservations*
- *IPv4 vs. IPv6*
- *Subnet mask*
- *Gateway*
- *VPN*
- *VLAN*
- *NAT*

IP Addresses

IP addressing - Static

- A static IP address doesn't change
- A static IP address can be public or private
- The device has the static IP programmed into its network interface (an interface can have multiple static addresses)
- Programming includes
  - Static IP address
  - Gateway IP address
  - Subnet mask
  - DNS server IP addresses (optional)
- Can create a conflict if two devices on the network have the same IP address

IP addressing – Dynamic

- When a DHCP device joints the network, it broadcasts a request for an IP address
- A dynamic IP address can be public or private
- The DHCP server receives the request and assigns an address to the device from its pool of IP addresses
- The following information is provided
  - Static IP address
  - Gateway IP address
  - Subnet mask
  - DNS server IP addresses
  - Lease time (how long the device can keep it's DHCP address before it must request a new one)

IP Addressing – APIPA / link-local

- In IPv4
  - Automatic Private IP Addressing
  - Also known as auto-IP
  - When a DHCP device joins the network, it will attempt to obtain an IP address over DHCP

- If the device doesn't receive a DHCP response, it will assign itself an IP address in the range of 169.254.0.0 to 169.254.255.255
    - The device will select an address in the range at random and query other network devices on the same segment to ensure that it has chosen a unique address
- This address is known as a link local address
- A router will not forward traffic from a device with an APIPA address; therefore, a device with a link local address won't be able to reach the internet
- The device will continue to attempt to obtain an IP address over DHCP (and will replace its link local address with an DHCP address when obtained)

- In IPv6
    - All devices are required to obtain link local addresses in addition to their DHCP addresses
    - The IPv6 address is used for Network Discovery and other protocols

DNS

- Domain Name Server or Domain Name System
- DNS translates human-friendly hostnames, to computer-friendly IP addresses
- The Domain Name System translates friendly names into IP addresses so that computers and network devices can identify and connect to the necessary network resources

- A computer resource, especially a website is hosted at a particular IP address
- Humans can remember websites and hostnames easily. It is difficult to remember IP addresses
- A website or service may change its IP address but keep its name
- The website or service will update its IP address in the Domain Name System. DNS allows users to continue to locate the site or service
- Multiple hostnames or domain names can correspond to a single IP address. For example, a server with a single IP address may host multiple websites.

DHCP

- DHCP is Dynamic Host Configuration Protocol
- Network devices require IP addresses to communicate with each other
- A DHCP network device places a DHCP request upon joining the network
- A DHCP server responds to the request by assigning a DHCP address to the network device
- A DHCP response contains the following information
    - IP address
    - Gateway IP address
    - Subnet mask
    - DNS servers (optional)
    - Lease time
- The DHCP server keeps track of the DHCP addresses that it assigns
- When selecting a DHCP address to assign, the DHCP server checks to make sure that no other devices have the same address

- We can place a DHCP reservation
    - If we want a specific device to always be assigned the same IP address over DHCP
    - We configure a DHCP reservation on the DHCP server
        - It includes the MAC address of the device and the IP address that we want
    - When the device places a DHCP request, the DHCP server checks the reservation list and assigns the correct IP address
    - IP addresses on the reservation list are never assigned to other devices, even if the devices on the list are not connected to the network

IPv4 vs IPv6

- IPv4 is Internet Protocol Version 4, IPv6 is Internet Protocol Version 6
- Despite their names, no other IP versions are in use
- IPv4
  - Provides a range of addresses in the form of xxx.xxx.xxx.xxx
  - Provides a range of addresses from 0.0.0.0 to 255.255.255.255
  - There are 4.29 billion IPv4 addresses
  - We are running out of IPv4 addresses (all IPv4 addresses have been assigned)
  - All devices and operating systems support IPv4
- IPv6
  - Provides a range of addresses in the form xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
  - Addresses are in the form from 0000 to ffff (hexadecimal)
  - There are 340,282,366,920,938,000,000,000,000,000,000,000,000 IPv6 addresses
  - Some devices and networks support IPv6, and some don't. For example, Microsoft Windows XP does not support IPv6
  - IPv6 addresses are self-configuring

Subnet Mask

- This is quite possibly the hardest network concept to learn
- A subnet mask tells us the size of the subnet
- What is a subnet?
  - A subnet is a network segment behind a gateway (router)
  - If a device wants to communicate with another device on the same segment, it sends the data directly to that device (a switch can forward the information)
  - If a device wants to communicate with another device on a different segment, it sends the data directly to the gateway (router)
  - All of the devices in your local network are in the same subnet
- IPv4 Subnets
  - A subnet mask is expressed as xxx.xxx.xxx.xxx or /xx
- How to understand the subnet masks
  - You know that a computer can think in terms of 0s and 1s right?
  - A number can be written in binary (as 8 digits of 0s and 1s)
  - A binary number is 8 bits (8 bits make up one byte)
  - For example, the number 255 can be written as 11111111. The number 254 can be written as 11111110.
  - Why is that? Look at this table.

Position	8	7	6	5	4	3	2	1
Value	128	64	32	16	8	4	2	1

  - The binary number has 8 digits. Each digit has a different value. For example, the digit on the right has a value of "1". The digit on the left (position 8) has a value of 128.
  - We add up the values in each position, where the binary value is 1.
  - For example, if we had a binary number of 10110101, what would that number be? If we write it in the table below, we can see that the values with "1" are 128 + 32 + 16 + 4 + 1 = 181

Position	8	7	6	5	4	3	2	1
Value	128	64	32	16	8	4	2	1
Binary	1	0	1	1	0	1	0	1

- A single binary number can have a value between 0 and 255. We can convert from a normal number to a binary number or vice versa.

- Going back to the subnet mask. A subnet mask is expressed as xxx.xxx.xxx.xxx or /xx
- The /xx is the number of binary bits used to express the xxx.xxx.xxx.xxx subnet mask
- For example, 255.255.255.0 can be written as 11111111.11111111.11111111.00000000 in binary form. That is 24 bits (there are 24 1's in the number).
- For example, 255.255.255.255.128 can be written as 11111111.11111111.11111111.10000000 in binary form. That is 25 bits.

- Let's back track a bit
- Each subnet has a range of IP addresses. The name of the network is the first IP address in that range.
- We want to know how big our subnet is
- Consider the following example

	Dot-Decimal Notation	Binary Form
IP address Write the IP address of the network (network name) in Binary Our network name is 192.10.2.138	192.10.2.138	11000000.00000000.00000010.10001010
Subnet mask	255.255.255.192	11111111.11111111.11111111.11000000

Write the subnet mask in Binary Our subnet mask is 255.255.255.192		There are 26 "1's in the binary mask. Therefore, the subnet is a /26 How big is this subnet (how many IPs does it contain)? 11111111.11111111.11111111.11**000000** Look at the back part of the subnet mask (the bold part that is 0s) What is the value of those 0s? We can calculate it from the binary table 32 + 16 + 8 + 4 + 2 + 1 = 63 The last IP in the subnet is called the broadcast IP, and is not useable. Therefore, we have only 62 useable IPs. We can also calculate the subnet size from the following formula, where n is the number of bits 2^n -2 In this case, n = 6 2^6 – 2 = 62
	We use the subnet mask to "mask" the binary form of the IP address	
Network prefix	Which positions match in the subnet mask and the IP address?	11000000.00000000.00000010.10000000

	In this case, positions 1, 2, 23, and 25 are "1" in both the IP and the subnet.	

The common subnets

Subnet Mask	Subnet Mask	Number of IPs per subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2
255.255.255.254	/31	2

Gateway

- The default gateway is also the router
- If a device wants to communicate with another device on the same segment, it sends the data directly to that device (a switch can forward the information)
- If a device wants to communicate with another device on a different segment, it sends the data directly to the gateway (router)

VPN

- Virtual Private Network
- Allows a user to connect to a network from another location (for example if an employee works from home)
- The VPN provider
    - Could be a windows/Unix server or could be a router/security appliance
    - This device is located inside the network
    - VPN users connect to the device remotely
    - There are several ways to authenticate users
        - Username/password
        - Active Directory
        - Certificate
    - There are several encryption protocols available
- VPN Traffic
    - The remote user receives an IP address on the local network
    - The remote device will behave exactly like it is on the local network
    - Traffic from the remote device gets packaged and travels inside a "tunnel" to the local network
    - There is an option for "split tunnel" traffic
        - Traffic destined for the corporate network (such as access to shared drives, printers, and e-mail) travels over the VPN
        - Traffic destined for the internet (such as YouTube) travels over the remote user's normal internet connection
        - Split Tunnel Traffic improves performance because it prevents internet traffic from consuming bandwidth on the VPN

VLAN

- A VLAN is a Virtual Local Area Network
- A VLAN allows us to logically separate a network into multiple networks without having to physically install additional equipment
  - For example, we can separate user traffic, VoIP traffic, and surveillance camera traffic into different VLANs
  - We can prioritize traffic from one or more VLANs
- A managed switch will tag each traffic source with its VLAN and will enforce the VLAN
  - VLAN traffic can also be tagged across a Wide Area Network
- Each VLAN typically has its own non-overlapping IP subnet
- Traffic that travels from one VLAN to another must talk to a gateway first
  - A concept called a Layer 3 Switch or a Router On A Stick can also handle traffic between VLANs, but this is outside the scope of this book

NAT

- Network Address Translation
- See the previous section on NAT

2.7 Compare and contrast Internet connection types, network types, and their features.

- *Internet connection types*
  - *Cable*
  - *DSL*
  - *Dial-up*
  - *Fiber*
  - *Satellite*
  - *ISDN*
  - *Cellular*
    - *Tethering*
    - *Mobile hotspot*
  - *Line-of-sight wireless Internet service*
- *Network types*
  - *LAN*
  - *WAN*
  - *PAN*
  - *MAN*
  - *WMN*

Internet Connection Types

Cable	Delivered over a coaxial cable Requires a cable modem Speeds up to 300 Mbps May have high latency Most urban areas have cable
DSL	Digital Subscriber Line Delivered over a phone line (can use phone and DSL internet at the same time) Requires a DSL modem Speeds up to 150 Mbps May have high latency Most urban areas have DSL, and so do many rural areas

Dial Up	Delivered over a phone line (can’t use internet and phone at the same time) Can be very slow (speeds up to 56 Kbps) May be good as a back-up to a DSL connection Doesn’t require much infrastructure; it functions anywhere a phone line is available
Fiber	Delivered over a fiber optic cable Requires a media converter to convert fiber to copper (ethernet) and a modem/router Fiber is not available in all areas, but internet providers are installing fiber in more areas Speeds up to 1 Gbps Low latency
Satellite	Satellite internet has widespread coverage, but it can be expensive and unreliable The satellite requires a “line of sight”. The satellite receiver equipment must have a clear line of sight with the sky. A satellite receiver provides a “two way” connection. The connection is high latency The connection is expensive

ISDN	Integrated Services Digital Network Old system Allows at least two simultaneous connections (data, voice, video or fax) over a single phone line Provides 128 kbits/s
Cellular	Delivered through a cellular modem Speeds of up to 100 Mbits/s Can be expensive because you must pay per GB of bandwidth used Latency is high Available anywhere you can get a cell connection. Some remote areas don't have cellular.

	Popular cellular modems include Cradlepoint modems.
Line of Sight	Also known as Point-to-Point Works with a range of up to 25 KM Requires two antennas – one to send internet, one to receive. The sender must be connected to an internet connection Good for rural areas Requires the antennas to have a line of sight (doesn't work if there are trees or walls in the way) Can be expensive if you're paying an ISP to provide the Line of Sight connection If you own the infrastructure (the sender and the receiver), such as if you're connecting two buildings, then there wouldn't be a monthly cost.

Network Types

LAN	Local Area Network This is the internal network for the home or office Devices on this network typically are assigned private IPs
WAN	Wide Area Network Allows multiple LANs to connect to each other, even if they are far apart A WAN requires low latency Devices on a WAN act as if they are all on the same LAN Requires negotiation with ISP/multiple ISPs to carry the traffic between the different LANs, and to do so at a low latency
PAN	Personal Area Network Network between devices belonging to a single user or in a specific workspace
MAN	Municipal Area Network Larger than a LAN but smaller than a WAN Can use Point-to-Point connections to connect them Typically, LANs in a single city can form a MAN
WMN	Wireless Mesh Network Multiple access points can work together to repeat a signal. APs not connected to the main network can still broadcast/receive a signal if they can connect to the main APs.

2.8 Given a scenario, use appropriate networking tool.

- *Crimper*
- *Cable stripper*
- *Multimeter*
- *Tone generator and probe*
- *Cable tester*
- *Loopback plug*
- *Punchdown tool*
- *Wi-Fi analyzer*

Network Tools

Crimper	Used to crimp an RJ-45 or RJ-11 connector (male end) onto the end of a cable Used to terminate an ethernet cable to a male end (for connecting to an AP or camera or for creating a patch cable) I personally find male ends unreliable and recommend that you terminate a cable with a female end and then insert a patch cord
Cable Stripper	Allows you to strip the outer jacket of the cable so that you can crimp or punch it down Cable strippers are available for ethernet, coaxial, or fiber cable
Multimeter	A multimeter allows you to detect voltage, current, resistance, or continuity on a cable or circuit

Tone generator and probe	Also known as a “fox and hound” Allows you to find the other end of a phone line or ethernet cable You connect the tone generator to one end of the cable Use the probe to look for the other cable When the probe rings, you will know that you’re close to the cable
Loopback Plug	Allows you to test continuity on a cable (internet connection) Takes the signal being received from the ISP and sends it back (loops it back) A Loopback plug can be copper or fiber

	 The plug connects pairs of the cable together
Punchdown Tool	Allows you to insert wires from an ethernet cable into a jack, patch panel, or phone block The tool contains a blade The most common blade shapes are 110, 66, BIX, and Krone
Wi-Fi analyser	Allows you to identify if the Wi-Fi is adequate or not (for speed, capacity, and VoIP)

	Can generate a heatmap of the Wi-Fi signal in a building Wi-Fi analyser can be a physical device or a software program installed on a computer Programs include InSSIDer, Air Magnet, and Netscout

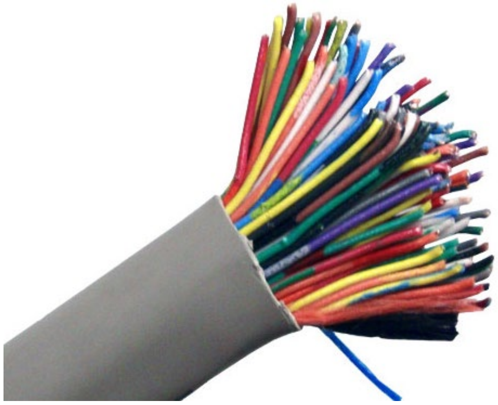
Part D: 220-1001 3.0 Hardware

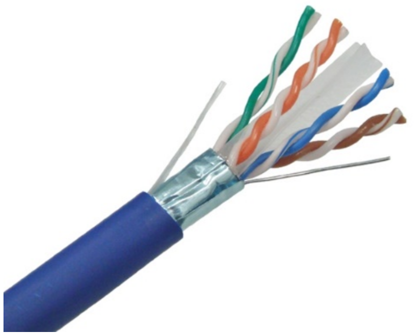
3.1 Explain basic cable types, features, and their purposes.

- *Network cables*
  - *Ethernet*
    - *Cat 5*
    - *Cat 5e*
    - *Cat 6*
    - *Plenum*
    - *Shielded twisted pair*
    - *Unshielded twisted pair*
    - *568A/B*
  - *Fiber*
  - *Coaxial*
  - *Speed and transmission limitations*
- *Video cables*
  - *VGA*
  - *HDMI*
  - *Mini-HDMI*
  - *DisplayPort*
  - *DVI*
  - *DVI-D*
  - *DVI-I*
- *Multipurpose cables*
  - *Lightning*
  - *Thunderbolt*
  - *USB*
  - *USB-C*
  - *USB 2.0*
  - *USB 3.0*
- *Peripheral cables*

    - *Serial*
- *Hard drive cables*
    - *SATA*
    - *IDE*
    - *SCSI*
- *Adapters*
    - *DVI to HDMI*
    - *USB to Ethernet*
    - *DVI to VGA*

Network Cables - Ethernet

Cat3	Old cabling system, considered obsolete Supports network speeds of 10 Mbit/s Supports analog phone systems and digital phone systems (Nortel, Panasonic, Avaya) 
Cat5	Old system for ethernet Supports speeds of up to 1000 Mbit/s Maximum length of a single cable is 100m
Cat5e	Current ethernet standard Supports speeds of up to 1000 Mbit/s Maximum length of a single cable is 100m
Cat6	Current ethernet standard Supports speeds of up to 1000 Mbit/s Maximum length of a single cable is 100m Cat6 cable is more expensive than cat5e, but has less noise and interference

	
Cat6A	New ethernet standard Supports speeds of up to 10 Gbit/s More difficult to install than cat6 because bends and kinks to the cable can reduce its capacity
Cat7	Ethernet standard that was developed and never adopted

Plenum vs Non-plenum

- A plenum space is a part of a building that is used for air circulation
- Can include the space above a dropped ceiling or inside an air return
- Cable installed in a plenum space must be rated as “plenum”
- Plenum-rated cable does not create harmful gases when it burns
- Non-plenum cable can create a fire hazard and may be prohibited by local building codes

Shielded vs Unshielded

- The cable can contain a shield made of metal foil
- The shield protects the cable from electromagnetic interference
- The entire cable can be shielded, and/or each individual pair can be shielded
- Cable is marked as UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair)

568A/568B

- There are two methods for terminating a cat5e/cat6/cat6A cable
- The methods are known as 568A and 568B
- The ethernet cables contain 4 pairs of wires (colored as blue, orange, green, brown)
- The difference between 568A and 568B is that the position of the orange and green wires is swapped
- Both 568A and 568B are acceptable termination methods
- A cable should be terminated with the same method on both sides
- A customer may require the cable to be terminated using a specific method. Most organizations prefer 568B.

Tips for installing ethernet cable

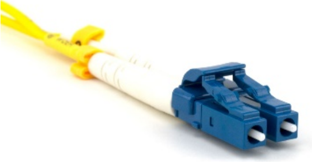
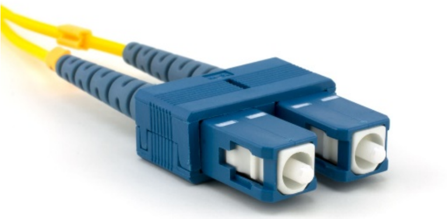
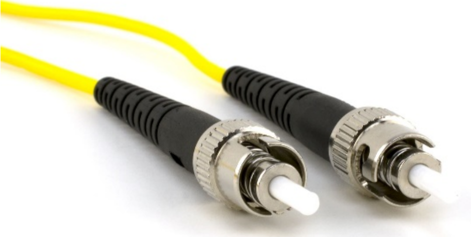
- BICSI code provides specific rules for installing cable
- Cable should be supported so that it doesn't sag
    - Can install cable inside conduits or use J-hooks
- Cable is sold in 1000' boxes
- Can buy pre-made patch cables for short distances
    - Home-made patch cables are not professional and making them is time consuming
- Cable has different ratings
    - Plenum vs non-plenum
    - Outdoor rated cable, which is gel filled
        - Resistant to cold temperatures and UV light
    - Arial cable can be installed between poles (contains a solid core to prevent the cable from sagging)

Network Cables – Fiber

Single Mode	Can be installed at distances of up to 200 km Supports speeds of between 100 Mbit/s and 100 Gbit/s depending on the length of the fiber
Multi Mode	Can be installed at distances of up to 2 km Supports speeds of between 100 Mbit/s and 100 Gbit/s depending on the length of the fiber

- Fiber is rated as single-mode or multi-mode
    - Within those ratings are sub ratings such as OM1, OM2, OM3, etc.
    - The best multi-mode rating is OM4
- A fiber optic cable consists of several layers
    - The outer layers provide protection
    - Fiber is not shielded for electromagnetic interference
    - The inner layer contains multiple fiber strands
    - A single cable contains between two and 60 strands
    - Two strands are required to make a circuit (one strand to send and one to receive)
    - A typical cable installed in a building contains 6 or 12 strands
- Fiber optic cable signal
    - The signal degrades along the length of the cable
    - The longer the cable, the weaker the signal. Think of it as a light getting dimmer as you get further away.
    - The longer the cable, the weaker the maximum speed
    - Fiber also degrades when spliced. A splice creates reflections and distortions in the light.

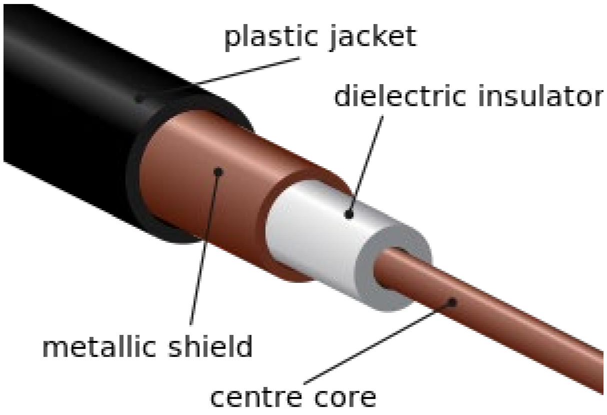
There are multiple types of fiber optic connectors, including

LC Most popular for network equipment	
SC	
ST	

It is possible to install adapters for any of these types of connectors.

Coaxial Cables

- Consists of a core wire with a braided shield



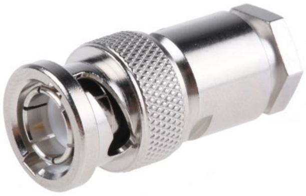
- Coaxial cable is good for
    - Coaxial cameras
    - Cable internet/television
    - Satellite dish
    - Antennas
- Coaxial cable is not used for network equipment, except for providing an analog signal to a cable modem
- A coaxial cable must be terminated to a connector. A crimping tool is used to terminate the cable.
- Siamese coaxial cable
    - Used for surveillance cameras and other devices that require both data and DC power
    - Contains both a coaxial cable and a pair of copper wires
    - Two components
        - Coaxial cable. The coaxial cable receives an analog signal from a device such as a camera.
        - DC power cable (single pair). The power cable provides DC power to a device such as a camera.

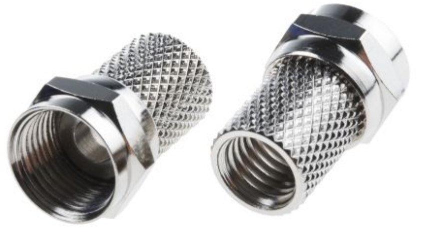
Coaxial cable types

RG-59	Used for short lengths Cheaper than RG-6
RG-6	Used for satellite and surveillance cameras Can provide a better-quality signal than RG-59

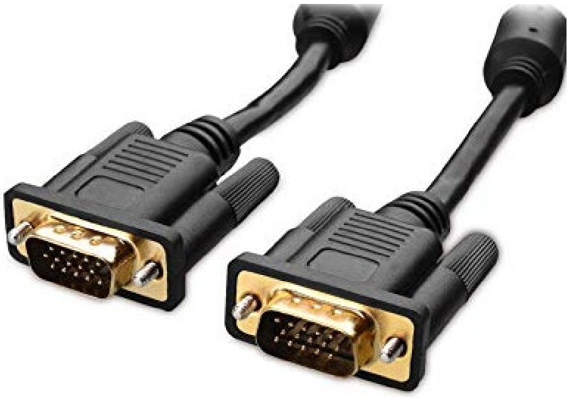
Coaxial Connectors

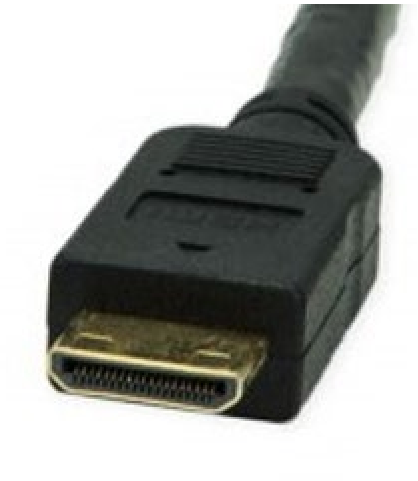
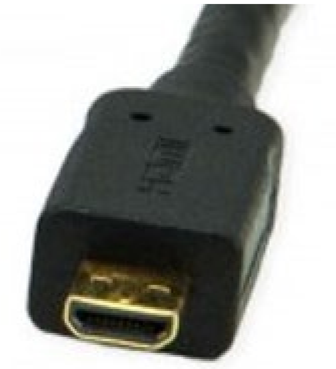
- You must use the correct sized termination (RG-59 or RG-6) for your cable
- There are different types of connectors. The most common are the BNC and the F-connector

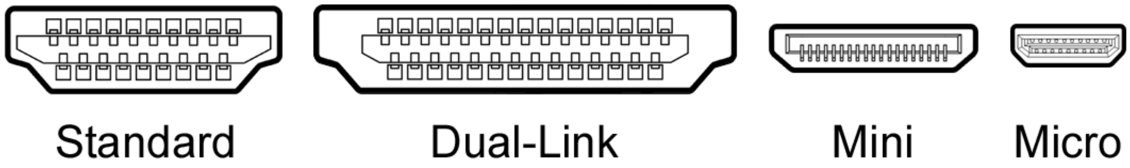
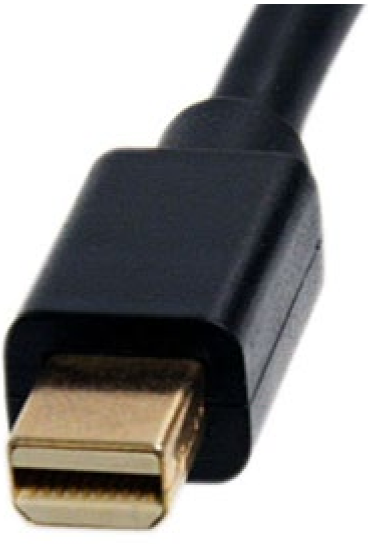
BNC Connector Used in high-end video/audio systems Twist to lock/unlock	

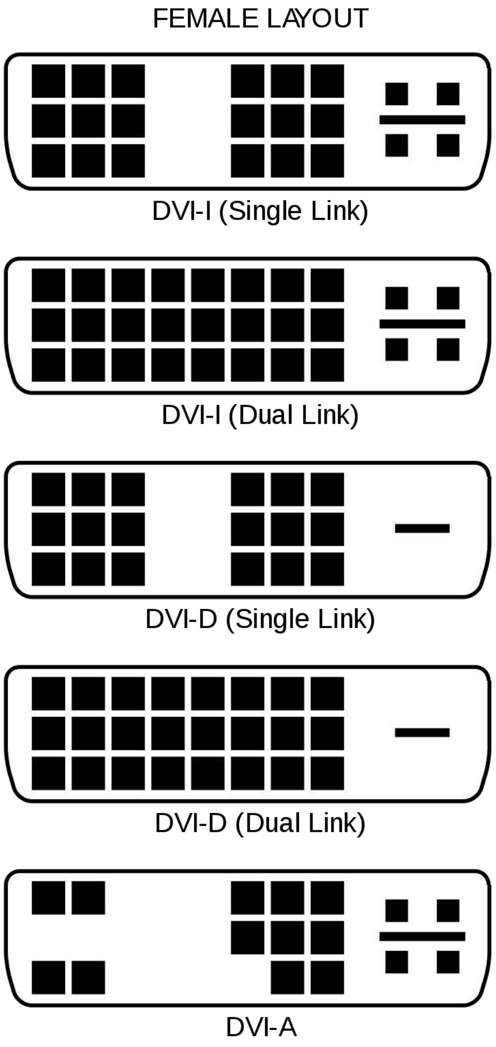
F Connector Used in residential applications Contains threads	

Video Cables

VGA Cable	Video Graphics Array Considered an analog signal Cable contains two thumbscrews to hold it in place Connector has 15 pins Most devices will have a VGA input/output Typically, the inputs/outputs are female, and the cables are male  2048×1536px is the maximum resolution Does not carry an audio signal
HDMI	High-Definition Multimedia Interface Considered a digital signal Cable held by friction Connector has 19 pins Most televisions and video devices use HDMI HDMI can carry an audio signal and an ethernet signal in addition to the vdeo Typically, the inputs/outputs are female, and the cables are male

	Can run an HDMI cable 100’ (can use an amplifier or an HDMI to ethernet converter for longer distances) Backwards compatible with DVI
Mini-HDMI	Smaller size connection for HDMI (same functionality) 
Micro-HDMI	Even smaller size 

	
DisplayPort	Considered a digital signal Cable held by a tab Connector has 20 pins Many computers and computer monitors use DisplayPort DisplayPort can carry audio Typically, the inputs/outputs are female, and the cables are male Can run a DisplayPort cable 100’ (can use an amplifier or a DisplayPort to ethernet converter for longer distances) Backwards compatible with DVI and HDMI
Mini DisplayPort	Smaller version of DisplayPort (with the same functionality) Fully compatible with Thunderbolt 

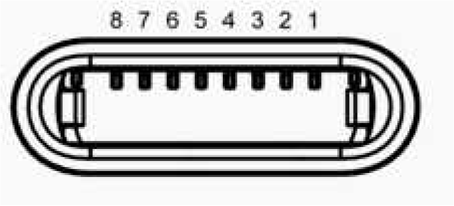
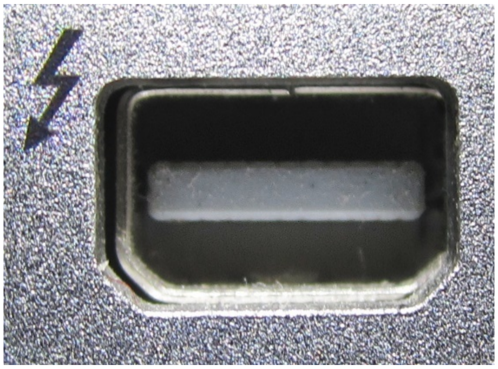
DVI	Digital Video Interface Mainly found on computer monitors; manufacturers are switching from DVI to HDMI and DisplayPort DVI can carry both an analog and a digital signal on the same cable (fully compatible with VGA) There are two types of connectors: DVI-I connector, and DVI-D connector  FEMALE LAYOUT DVI-I (Single Link) DVI-I (Dual Link) DVI-D (Single Link) DVI-D (Dual Link) DVI-A

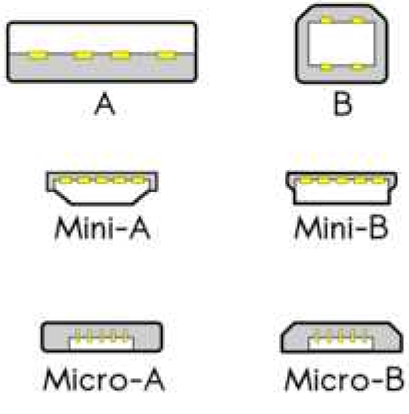
- We can convert any signal to any other signal

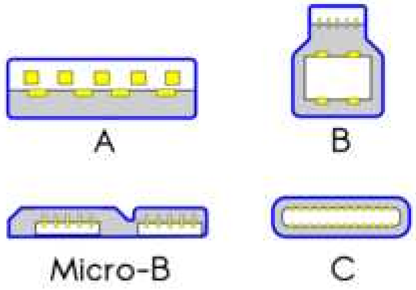
- DVI to HDMI, HDMI to Mini-HDMI, etc., any digital signal requires a simple adapter
- Convert from an analog signal to digital or from digital to analog requires an electronic converter
  - Converter may obtain power from USB port, video signal, or power outlet

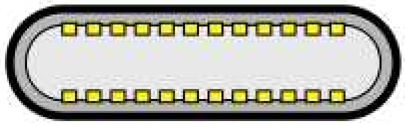
Other Cable Types

There are many cables, these are the most common

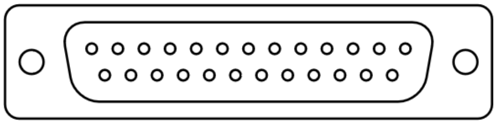
Lightning	Apple proprietary connector Provides power and data Typically to connect Apple phones and tablets 8 Pins 
Thunderbolt	Apple proprietary connector Combines PCIe, DisplayPort, and two serial signals Thunderbolt 1 and 2 use the same connector as a Mini DisplayPort  Thunderbolt 3 uses the same connection as USB C
USB	Universal Serial Bus There are three versions of USB (1.0, 2.0, and 3.0) USB devices are used to connect phones, tablets, and other peripherals

	The maximum length of a USB cable is 15 feet There are three types of connectors (Standard, Mini, and Micro) and two formats (A and B). USB 1.0 and 2.0 use the same style of connectors. USB 3.0 use a different style of connector, and also includes the Type C connector. USB ports are directional Only one side provides power and only one side receives power To prevent a user from accidentally connecting two devices that provide power, and causing electrical damage, the USB ports have different ends. USB 1.0 and 2.0 Connectors Contains four wires Two wires provide data, and two provide power Typically, a USB cable will be Type-A standard on one side and Type-B on the other side  USB 3.0 Connectors Contains eight wires

	Two wires provide data, and two provide power Four additional wires can provide data transfer in SuperSpeed mode Typically, a USB cable will be Type-A standard on one side and Type-B or Type-C on the other side, or the cable will be Type-C to Type-C. 
USB 1.0	Oldest version of USB 12Mbps maximum speed
USB 2.0	Newer version of USB 480Mbps maximum speed
USB 3.0	The latest version is USB 3.2 USB 3.0, 3.1, and 3.2 are backwards compatible with USB 2.0 and 1.0 devices USB 3.0 supports a maximum speed of 5Gbps, and contains a SuperSpeed mode that uses eight wires to transmit data (instead of the usual four)
USB-C	USB-C plug contains 24 pins

	It does not have an up or down orientation USB-C connector cables have the same plug on both sides Maximum speed of 10Gbps USB-C supports Thunderbolt 3 A USB-C port with Thunderbolt 3 can be used to connect a laptop to a docking station, charge a laptop, and output video to displays 
Parallel Cable	A parallel cable sends multiple bits at the same time. Parallel cables are used to connect to printers. Parallel cables are no longer popular, but they can be valuable when needed.
Serial Cable	A serial cable communicates via a serial protocol (sends data one bit at a time) The maximum length is 15 m The two most common serial cable connections are DE-9, which contains 9 wires

And DB-25, which contains 25 wires



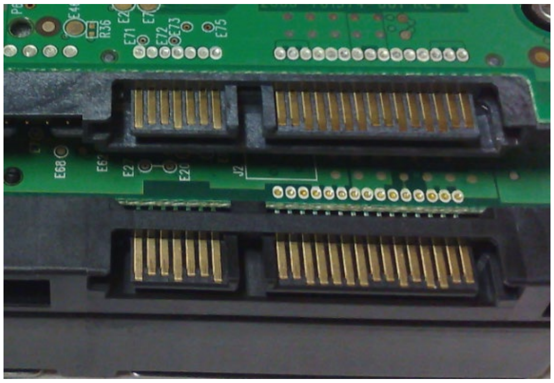
Most laptops don't have serial connections
Most desktops have serial connections

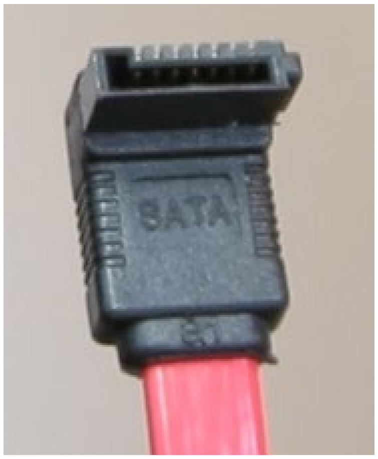
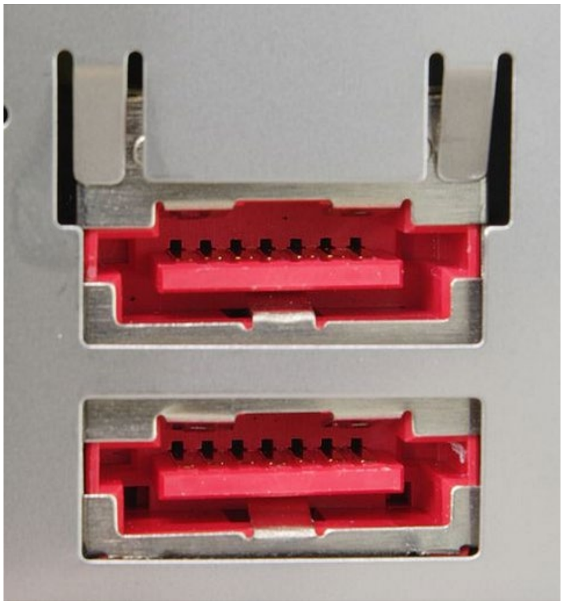
A common use of a serial cable is to connect to a piece of network or industrial equipment and configure it.

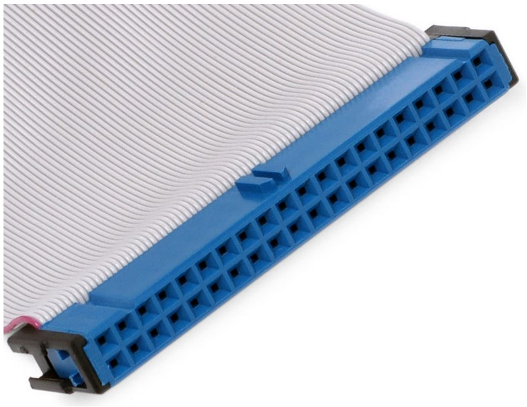
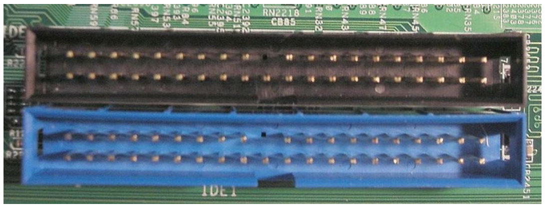
A popular cable is a DB-9 to RJ-45 cable, known as a console cable. It is used to connect to and configure network equipment such as Cisco switches and routers.

	USB to serial adapters are readily available but require a driver.

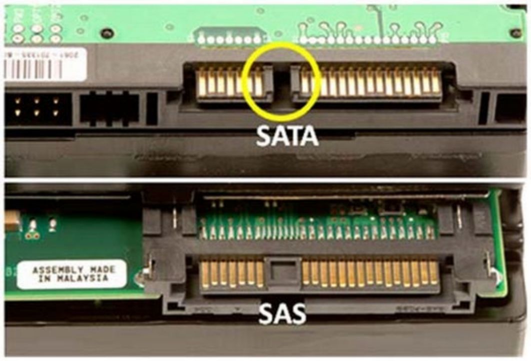
Common HDD Cables

SATA	A SATA cable is the current method of connecting Hard Disk Drives in consumer electronics The current version is 3.3 SATA is backwards compatible with older versions Supports speeds of up to 6 Gbps (burst) and 600 Mbps (average speed) A SATA data connector contains seven pins The seven-pin SATA connector on a hard disk drive is on the left. The fifteen-pin SATA power connector on a hard disk drive is on the right. Notice that a few of the pins are longer. They are used for grounding and are designed to be connected first. 

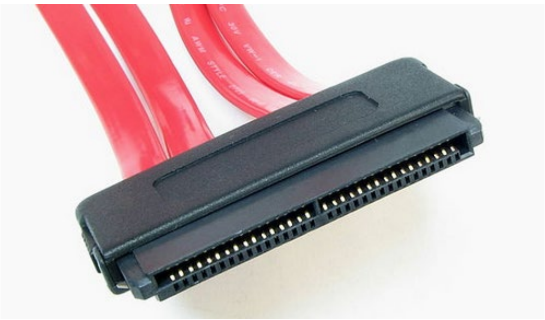
	SATA cable connector  eSATA allows connection of external storage devices. It is like USB. 
IDE	Integrated Drive Electronics (IDE) is an older method of connecting drives Also known as PATA or ULTRA ATA Uses a 40 or 80 pin ribbon cable Maximum speed of 133 Mbps

	IDE Ribbon Cable IDE Ribbon Connector  IDE Connector 
SCSI	Small Computer System Interface Available as several different connectors SCSI requires a controller Modern SCSI devices use a serial transmission; older SCSI devices use a parallel interface Speeds range between 200 Mbps and 22 Gbps
SAS	Serial Attached SCSI High speed drive interface, commonly found on enterprise server hard disk drives Also used to connect external network storage devices and controllers

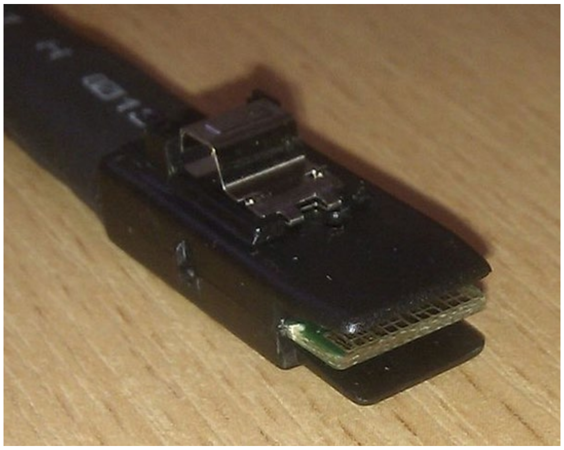
SAS connectors are like SATA connectors



Internal SAS connector



External SAS Connector



Common adapters

There are many other adapters, but these are the most important.

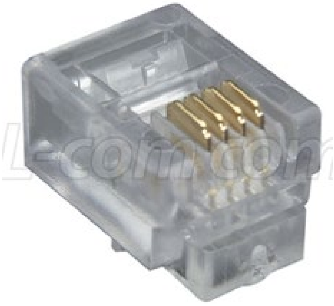
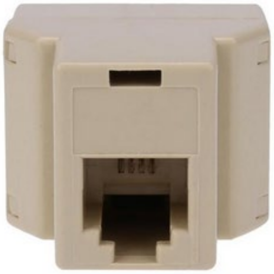
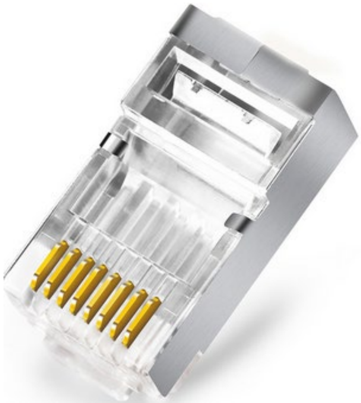
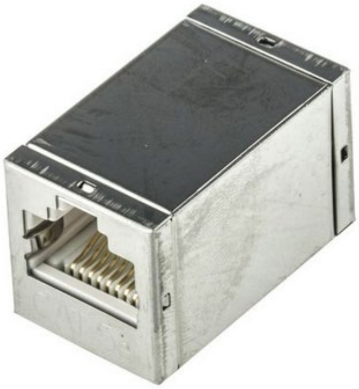
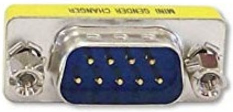
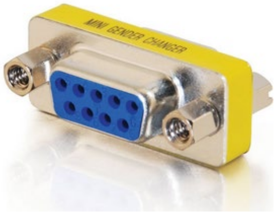
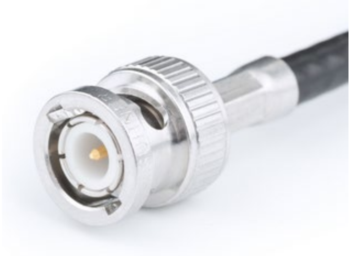
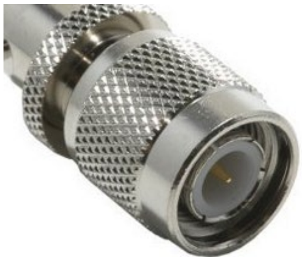
DVI to HDMI	Convert DVI (less common) to HDMI Most graphics cards have an HDMI output, but some displays have a DVI input
DVI to VGA	Convert DVI to analog VGA Will cause a loss in signal quality
USB to Ethernet	Allow you to connect an ethernet cable to a USB port. Good for laptops that don't have ethernet ports Requires a driver

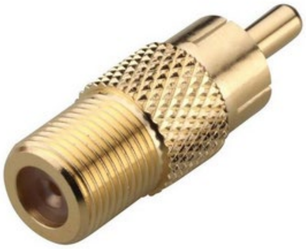
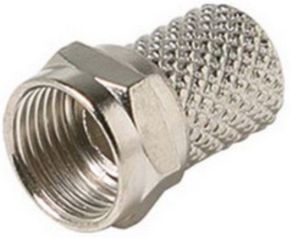
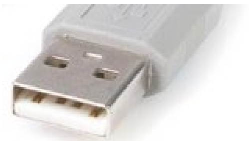
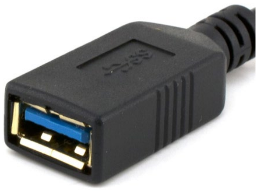
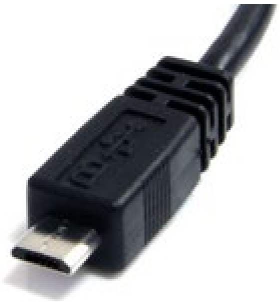
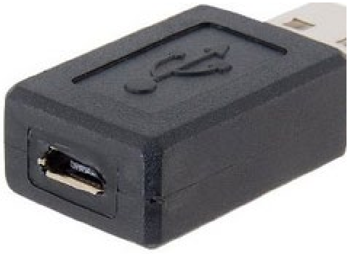
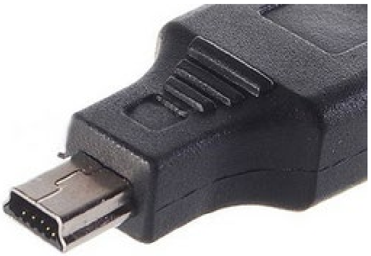
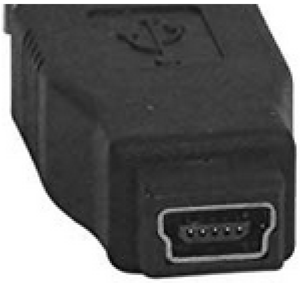
Serial to USB	Convert serial to USB Important for laptops that don’t have a serial port but need to connect to a serial device Requires a driver

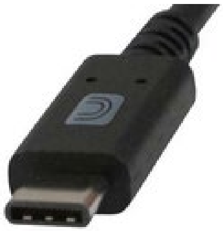
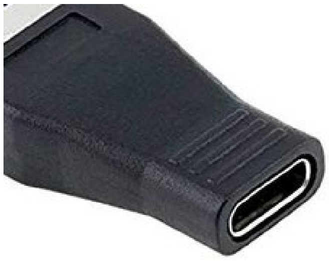
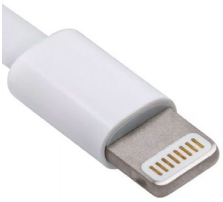
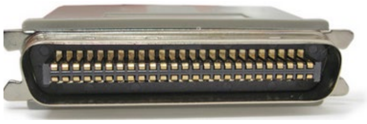
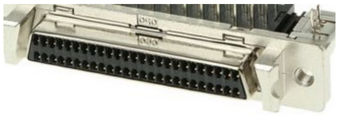
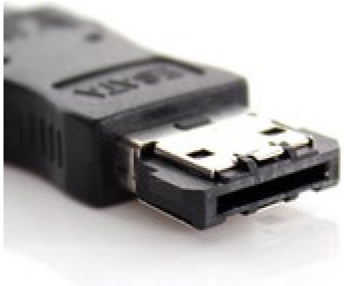
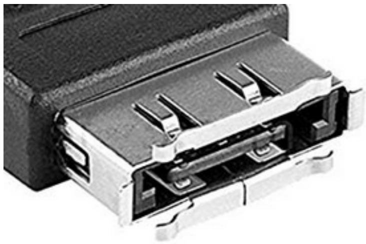
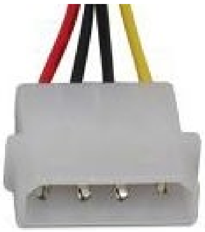
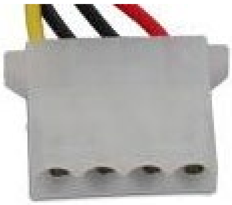
3.2 Identify common connector types.

- *RJ-11*
- *RJ-45*
- *RS-232*
- *BNC*
- *RG-59*
- *RG-6*
- *USB*
- *Micro-USB*
- *Mini-USB*
- *USB-C*
- *DB-9*
- *Lightning*
- *SCSI*
- *eSATA*
- *Molex*

Common Connectors

Name	Male	Female
RJ-11 Used for analog phone lines Contains 4 pins, but is 6 pins wide Also (RJ-12, which contains 6 pins and is 6 pins wide)		
RJ-45 Ethernet Contains 8 pins Female RJ-45 jack is available in many colors and types Can be cat5e, cat6, or cat6A		
RS-232 Serial Most common size has 9 pins		
BNC Terminates a coaxial cable The BNC connector twists on to lock to a female connector Used to terminate RG-59 and RG-6 cable		

F-connector Used to terminate RG-59 and RG-6 cable		
USB Standard connector Female connector can be part of a system board or a separate cable		
Micro USB		
Mini USB		

USB-C		
Lightning		
SCSI		
eSATA		
Molex		

3.3 Given a scenario, install RAM types.

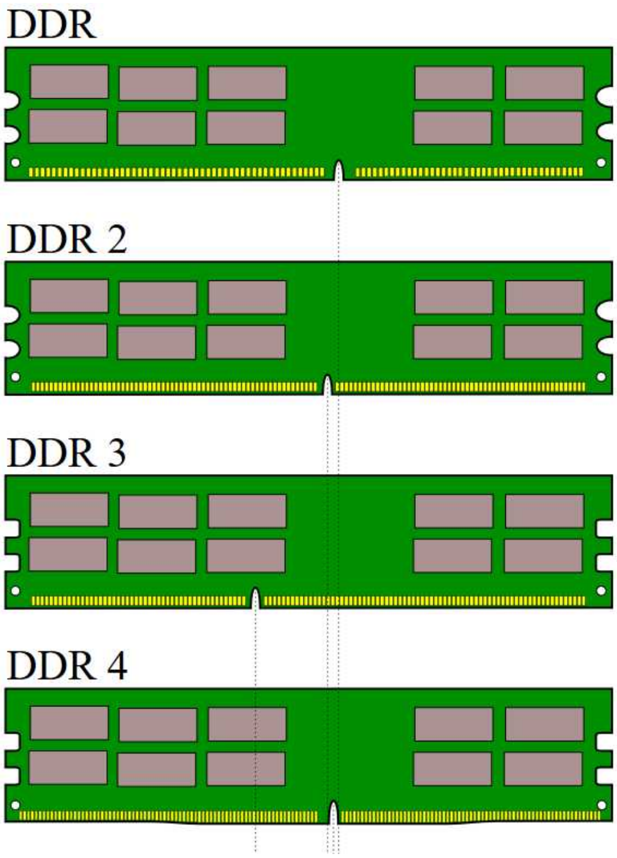
- *RAM types*
  - *SODIMM*
  - *DDR2*
  - *DDR3*
  - *DDR4*
- *Single channel*
- *Dual channel*
- *Triple channel*
- *Error correcting*
- *Parity vs. non-parity*

RAM Types

Installation of RAM was covered in a previous section. There are currently four types of RAM

DDR	Double Data Rate 2.1 GB/s transfer rate
DDR2	Double Data Rate Type 2 4.2 GB/s transfer rate
DDR3	Double Data Rate Type 3 8.5 GB/s transfer rate
DDR4	Double Data Rate Type 4 17 GB/s transfer rate

You can't mix and match RAM types. You must match the correct RAM with the correct motherboard socket. DDR RAM Types are the same width, but have notches in different locations



DIMM	Dual in-line memory module The RAM above are DIMMs They are the standard width
SODIMM	Small outline DIMM SODIMMs are used in laptops They are half the width of normal DIMMs

RAM Features - Channels

The RAM channel is a feature of the system board, not the RAM. A channel is a line of communication between a system board and the RAM. A dual-channel motherboard has twice the communication speed of a single channel. A triple-channel motherboard has three times the communication speed of a single channel.

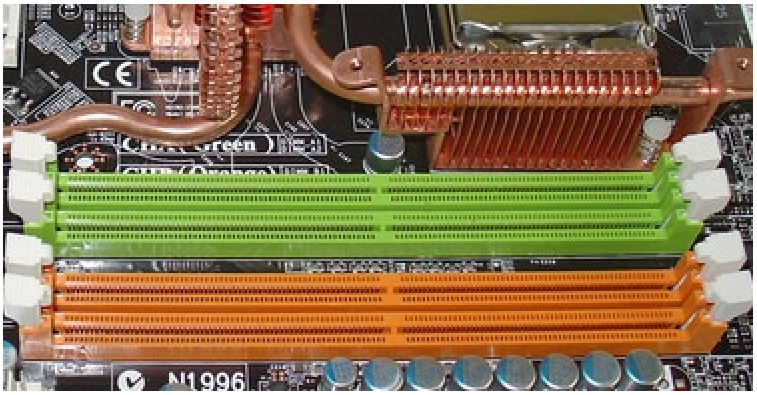
Channels are available as

- Single Channel (requires one RAM DIMM)
- Dual Channel (requires pairs of RAM DIMMs)
- Triple Channel (requires multiples of three RAM DIMMs)

If you're operating a Triple Channel system board, you will require at least three DIMMs, or a multiple of three, such as six or nine.

If you don't have the correct multiple of DIMMs, then the system board will revert to a lower channel. For example, if you install one DIMM in a Dual Channel board, the board will operate as single channel.

A system board will typically have color-coded DIMM banks. In this example, we have a dual-channel board. RAM DIMMS in the green banks belong to one channel, and DIMMs in the orange banks belong to the second channel. If you have two DIMMS, install one in a green bank and one in an orange bank.



RAM Features – Error Correcting

A RAM DIMM can be affected by electromagnetic interference, which could cause some of the data to be changed. This leads to corruption and undesired operation.

RAM with error correcting capability

- Used in specific applications such as healthcare, scientific, financial, and multi-user servers (where an error could be disastrous)
- Reduces the number of crashes
- More expensive than non-error correcting RAM

There are several ways to detect errors

- Parity Bits
- Checksums
- Cyclic Redundancy Checks
- Hash Functions

Parity features

- A bit contains eight bytes, which are 0's and 1's
- For example, a byte could be 01010101
- In a parity scheme, we want to keep the total of the bits even or odd.
- For example, if we want the total to be even, we check the first seven bits. If the first seven bits are odd, we add a 1 to the end, and now the total is even.
- For example, if the byte is 0101010, we have a total of 3, which is odd. We add a 1 to the end to come up with 01010101, which is a total of 4, which is even.
- If our data becomes corrupted, and changes to 01011101, the total is 5, which is odd. The RAM error-handling mechanism is expecting an even total. It knows that there is an error in the byte.

Checksum

- A bit contains eight bytes, which are 0's and 1's
- For example, a byte could be 01010101
- The RAM could record the total of the byte, which is 4. The total is the checksum

- If the byte changes, then the total will change. If the RAM notices that the total doesn't match, then an error will be detected.

Cyclic Redundancy Check

- More advanced mathematical formula
- We apply the formula to our data to obtain an answer
- If the data changes, and we reapply the formula, we will have a different answer
    - We will know that the data changed

Hash Function

- More advanced mathematical formula
- We apply the formula to our data to obtain an answer
- If the data changes, and we reapply the formula, we will have a different answer
    - We will know that the data changed

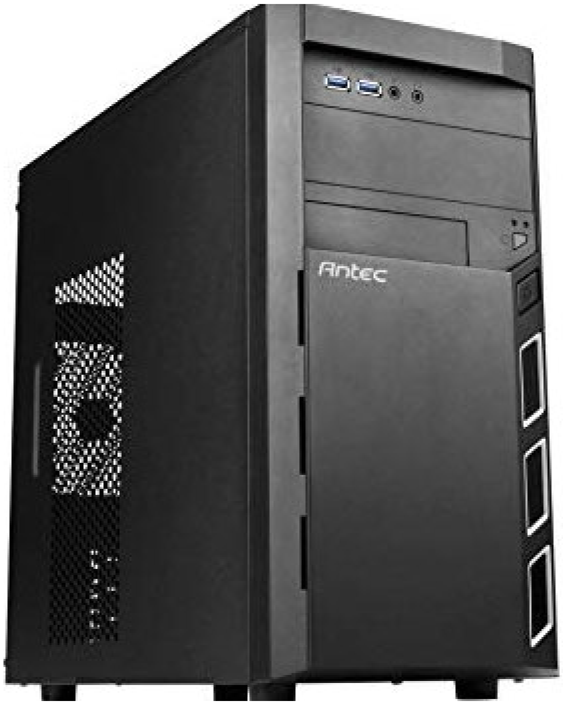
3.4 Given a scenario, select, install and configure storage devices.

- *Optical drives*
    - *CD-ROM/CD-RW*
    - *DVD-ROM/DVD-RW/DVD-RW DL*
    - *Blu-ray*
    - *BD-R*
    - *BD-RE*
- *Solid-state drives*
    - *M2 drives*
    - *NVMe*
    - *SATA 2.5*
- *Magnetic hard drives*
    - *5,400rpm*
    - *7,200rpm*
    - *10,000rpm*
    - *15,000rpm*
    - *Sizes:*
        - *2.5"*
        - *3.5"*
- *Hybrid drives*
- *Flash*
    - *SD card*
    - *CompactFlash*
    - *Micro-SD card*
    - *Mini-SD card*
    - *xD*
- *Configurations*
    - *RAID 0, 1, 5, 10*
    - *Hot swappable*

Optical Drives

How to install an optical drive in a desktop PC

- Choose an available drive bay (typically 3.5")



- Open the side of the case

- Insert the drive into the bay. Secure with screws if necessary.
- Connect SATA cable from system board to drive
- Connect power cable from PSU to drive
- Close the case
- Power on the computer and install the driver (it may install automatically)

An optical disc is read by a laser.

Choose a drive that is compatible with the media you want to record on and/or read.

CD-ROM/CD-R/CR-RW 	CD-ROM Compact Disk-Read Only Memory Can't modify the contents Typically stamped from a factory CD-R Compact Disk-Writable Can write to the disk once, and then data is permanent CD-RW Compact Disk-Rewritable Can write to the disk multiple times You must erase the disk each time you change the data (you can't add data one file at a time) A drive that can modify CD-Rs and CD-RWs is called a "CD Burner" Capacity is 700MB
DVD-ROM/DVD-RW/DVD-RW DL	DVD-ROM

	Digital Versatile Disk-Read Only Memory Can't modify contents Typically stamped from a factory DVD-RW Digital Versatile Disk-Rewritable Can write to the disk multiple times You must erase the disk each time you change the data (you can't add data one file at a time) Capacity is 4.7GB DVD-RW DL Digital Versatile Disk-Rewritable Dual Layer Contains two layers Capacity is 8.5 GB A drive that can modify DVD-RWs is called a "DVD Burner"
Blu-Ray/BD-R/BD-RE 	Blu-Ray Capacity is 25GB per layer (with up to four layers, for a total of 100GB) BD-R Blu-ray Disc-Recordable Can write to the disk once, and then data is permanent BD-RE Blu-ray Disc-Rerecordable Can write to the disk multiple times You must erase the disk each time you change the data (you can't add data one file at a time)

Light Scribe	Allows you to etch an image into the front of the disc You must have • A disc drive with the light scribe feature • A disc with light scribe • Necessary software LightScribe images are a single color. The LightScribe technology has been discontinued. An example of a LightScribe disc THE BEATLES LET IT BE 1970 1. Two of Us 3:33 2. Dig a Pony 3:51 3. Across the Universe 3:42 4. I Me Mine 2:23 5. Dig It 0:47 6. Let It Be 3:59 7. Maggie Mae 0:36 8. I've Got a Feeling 3:34 9. One After 909 2:50 10. The Long and Winding Road 3:35 11. For You Blue 2:28 12. Get Back 3:07

Hard Disk Drive

How to install a hard disk drive in a PC

- Open the side of the case

- Choose an available internal bay
  - Some cases have 3.5″ and 2.5″ bays
  - If you're installing a 2.5″ drive, but only have 3.5″ bays, you must install the drive in a 2.5″ to 3.5″ adapter
- Insert the drive into the bay. Secure with screws if necessary.
- Connect SATA cable from system board to drive
- Connect power cable from PSU to drive
- Close the case
- Power on the computer and install the driver (it may install automatically)

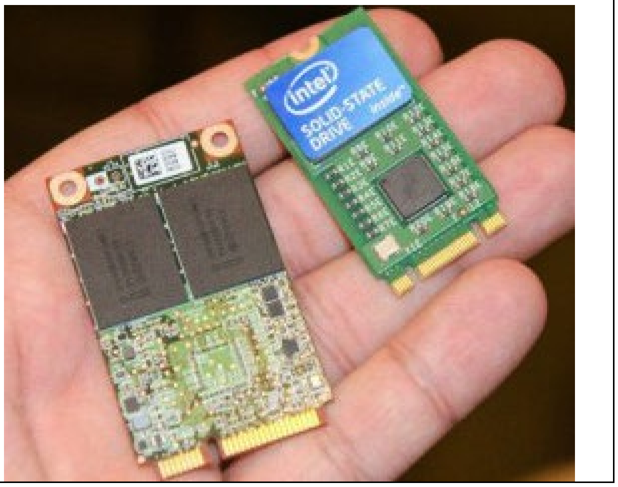
There are three types of hard disk drives

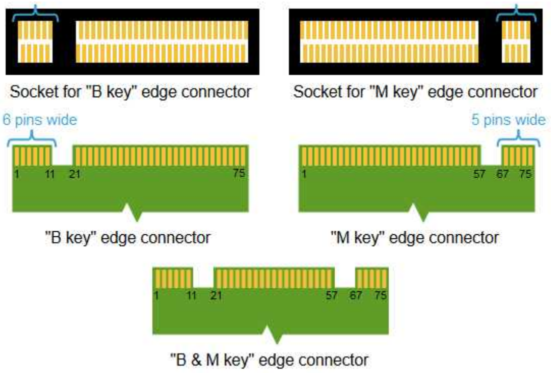
Magnetic Drive	Contains a spinning magnetic platter Can be noisy and heavy Available in 2.5″ and 3.5″ sizes Low cost (around $100)

	Slow speeds Available in sizes of up to 6TB
Solid State Drives	Contain no moving parts, only flash memory Produce little noise or heat Available in 2.5″ sizes and some other sizes (requires an adapter to install in a 3.5″ drive bay) Expensive (around $500) Maximum capacity is 6TB
Hybrid Drive	Magnetic drive with a small solid-state chip Solid-state chip records most commonly accessed data Same size as magnetic drives Low cost, but with improved performance

Solid State Drives

- Adapters to connect a 2.5″ SATA drive to another drive connector are available (for example SATA to M2)

M2 drives	Typically found in laptops Rectangular shape Available in different sizes 

	Connectors  Socket for "B key" edge connector Socket for "M key" edge connector 6 pins wide 5 pins wide 1 11 21 75 1 57 67 75 "B key" edge connector "M key" edge connector 1 11 21 57 67 75 "B & M key" edge connector
NVMe	Solid State Drive that can connect to a PCI Express port Approximately four times faster than a SATA SSD Connects to the PCI Express port, which reduces overhead when accessing data Available in two sizes - PCI Express - U.2

SATA 2.5	Most Common SSD Size Available in a 2.5″ size

Magnetic Hard Drives – Speeds

- For a drive to read data, it must rotate to the location of the data. The faster the drive, the faster it can read data.
- Slower moving drives produce less noise
- Drives will slow down when not in use in order to save power
- Drives contain shock resistance to protect against damage

Common speeds

5,400rpm	Laptop HDDs and some Desktop HDDs
7,200rpm	High-end Desktop HDDs
10,000rpm	Enterprise Server HDDs
15,000rpm	Enterprise Server HDDs

Magnetic Hard Drives - Sizes

2.5″

- SATA laptops will only fit 2.5″ drives
- Can install a 2.5″ drive in a desktop 3.5″ drive bay, but an adapter is required

3.5″

- Larger and heavier than a 3.5″ drive

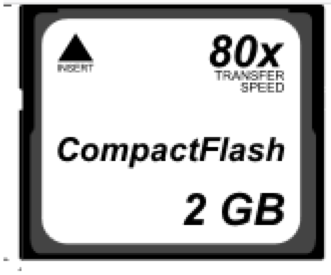
Tips for selecting an HDD

- Consider the application
    - Is the hard drive being used for gaming, video editing, or another high-performance application? You should consider an HDD with a high rotational speed or a Solid-State Drive.
    - Is the hard drive being used for an enterprise application? Consider a SAS drive.
- Consider the budget
    - Magnetic drives cost approximately $100, while solid state drives cost between $500 and $1000. Enterprise SAS drives can cost over $1000.
- Consider the capacity
    - How much storage space do you require? Buy a drive with adequate space.
- Consider the computer
    - Does the computer BIOS support the type of drive that you want to install? NVMe drive technology is not supported by older BIOSs.
    - Does the computer have space to install the drive? If it's a desktop, does it have an available 3.5″ or 2.5″ drive bay? If it's a laptop it might only have space for one or two drives.
    - Does the computer have the correct connector? For example, does it have a PCIe slot for an NVMe drive?

Memory

- Memory cards are typically used for cameras and phones
- A memory card can be read by an internal or external card reader
- A memory card will typically have an external switch to convert it from “read only” to “read/write”
- Adapters are available so that you can insert a micro/mini-SD card into a device with an SD Card reader

There are several types of cards

CompactFlash	Old Format, with a capacity of up to 512GB 
SD Card	Secure Digital Card Secure Digital ▼LOCK 2GB

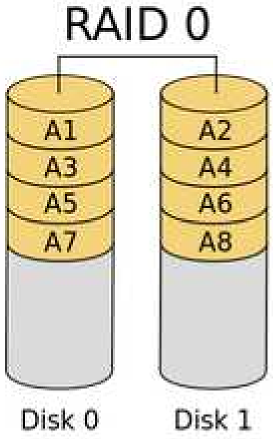
Micro-SD card	Replaced the SD Card Smaller size
Mini-SD card	Replaced the Micro-SD Card Smaller size Maximum capacity of 2TB Transfer speed between 12.5MB/s and 985 MB/s
xD Card	xD Card Currently, no devices use the xD card Maximum capacity of 2GB

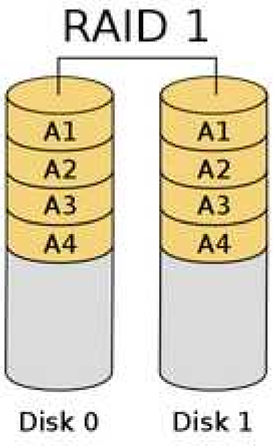
When selecting a card, consider

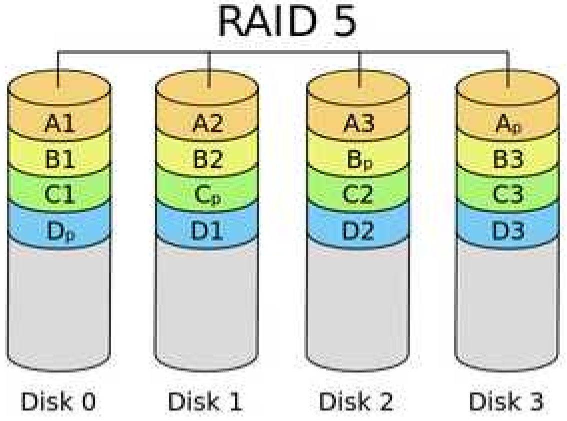
- Form factor. A device (camera, phone, etc.) will only have a connector for one type of card. You will typically be limited by the type of connector.
- Capacity. Select a card with adequate capacity.
- Speed. Cards have different recording speeds. A device such as a video camera will require a card with a fast recording speed.

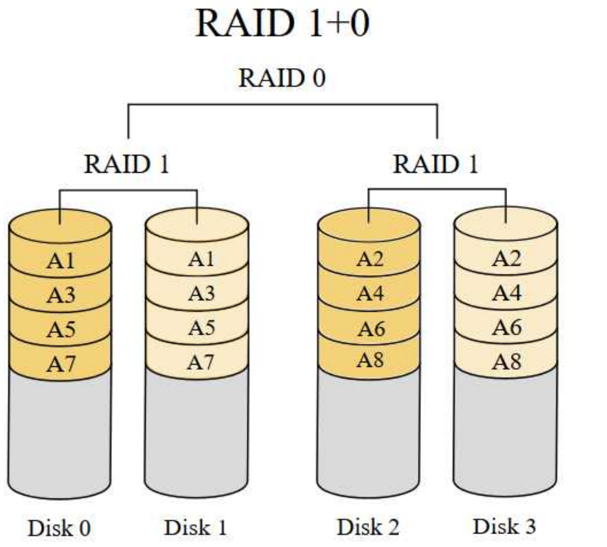
RAID

- RAID is a Redundant Array of Independent Disks
- Requires two or more drives to make an array
- RAID is fault-tolerant (in most cases)
  - The data is split over multiple disks in the array
  - If one disk in the array fails, then the data is not lost
  - Disks are typically hot swappable (we can remove a disk from the computer while it is powered on and insert a new disk). The computer will automatically rebuild data on the new disk.
- Requires a RAID controller to manage the drives
- Drives without a controller are called JBOD = Just a Bunch of Disks (no RAID)

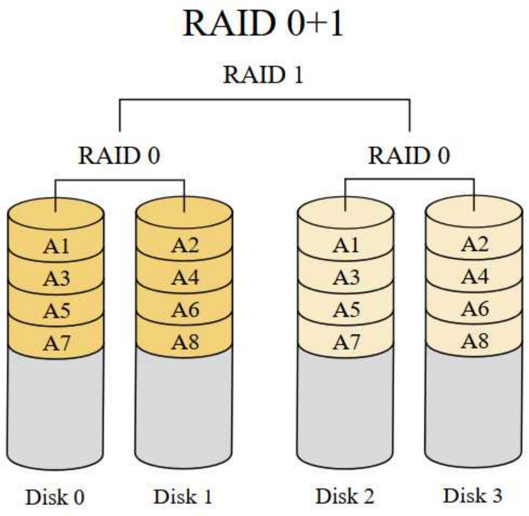
RAID 0	Data is split across two or more disks Each disk contains half of the data If one disk fails, all the data is lost RAID 0 is faster than a single disk because we can access data from two disks at the same time  RAID 0 A1 A3 A5 A7 A2 A4 A6 A8 Disk 0 Disk 1
RAID 1	Data is replicated across two disks Each disk contains all the data If one disk fails, no data is lost When reading data, RAID 1 is faster than a single disk because we can access data from two disks at the same time.

	When writing data, RAID 1 is the same speed as a single disk.  RAID 1 A1 A2 A3 A4 A1 A2 A3 A4 Disk 0 Disk 1
RAID 5	RAID 5 is faster and has redundancy Parity is distributed across multiple drives It requires at least three disks • We split the data across three (or more disks) • In this example, we split the data "A" across Disk 0, 1, and 2. • We calculate the parity bit Ap (the sum of the data bits A1, A2, and A3 • If a disk fails, we can rebuild the disk by recalculating the data from the parity bit (or by recalculating the parity bit) • Notice that parity is distributed across multiple drives • If we were to store all the parity bits on a single drive, that drive would become overloaded. That is why we distribute the parity across multiple disks.

	 RAID 5 A1 B1 C1 D_p A2 B2 C_p D1 A3 B_p C2 D2 A_p B3 C3 D3 Disk 0 Disk 1 Disk 2 Disk 3
RAID 10	RAID 10 is a nested RAID level It combines RAID 0 and RAID 1 We split the data across two drives, and then we make a copy of each of those drives This gives us faster speed (because we can read data from four drives at the same time) and redundancy (because we have two copies of the data) RAID 10 is the best choice for storing data where we have lots of read and write activities. We can write twice as fast because we only write half the data to each set of drives. We can read four times as fast because we can read from four drives at the same time.

<table>
<tr>
<td></td>
<td>


</td>
</tr>
<tr>
<td>RAID 01</td>
<td>
RAID 01 is a nested RAID level
It combines RAID 0 and RAID 1
We copy the data across two or more drives, and then we split each drive onto two drives
This gives us faster speed (because we can read data from four drives at the same time) and redundancy (because we have two copies of the data)



</td>
</tr>
</table>

Other types of RAID	Other types of RAID include RAID 2 RAID 3 RAID 4 RAID 6 RAID 50 RAID 60 RAID 100 But these are less common

3.5 Given a scenario, install and configure motherboards, CPUs, and add-on cards.

- *Motherboard form factor*
  - *ATX*
  - *mATX*
  - *ITX*
  - *mITX*
- *Motherboard connectors types*
  - *PCI*
  - *PCIe*
  - *Riser card*
  - *Socket types*
  - *SATA*
  - *IDE*
  - *Front panel connector*
  - *Internal USB connector*
- *BIOS/UEFI settings*
  - *Boot options*
  - *Firmware updates*
  - *Security settings*
  - *Interface configurations*
  - *Security*
    - *Passwords*
    - *Drive encryption*
      - *TPM*
      - *LoJack*
      - *Secure boot*
- *CMOS battery*
- *CPU features*
  - *Single-core*
  - *Multicore*
  - *Virtual technology*
  - *Hyperthreading*

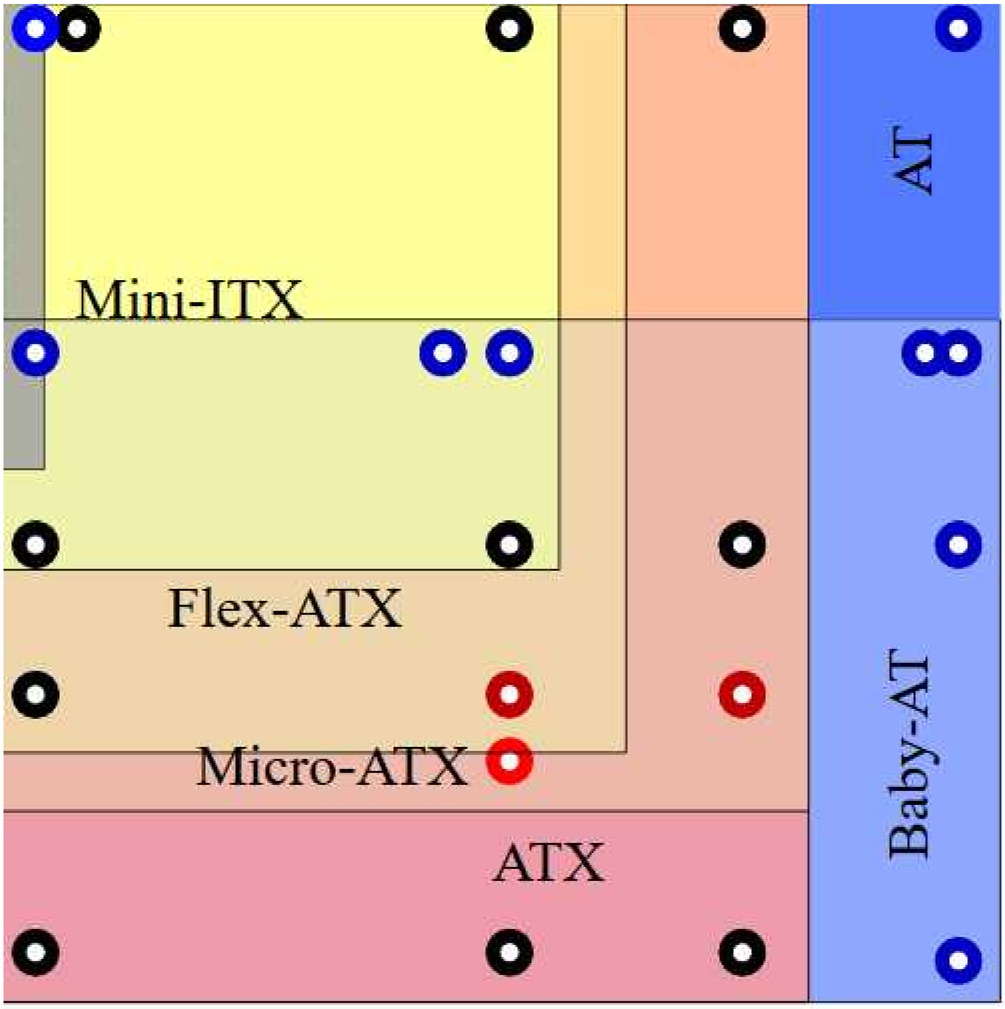
    - *Speeds*
    - *Overclocking*
    - *Integrated GPU*
- *Compatibility*
    - *AMD*
    - *Intel*
- *Cooling mechanism*
    - *Fans*
    - *Heat sink*
    - *Liquid*
    - *Thermal paste*
- *Expansion cards*
    - *Video cards*
        - *Onboard*
        - *Add-on card*
    - *Sound cards*
    - *Network interface card*
    - *USB expansion card*
    - *eSATA card*

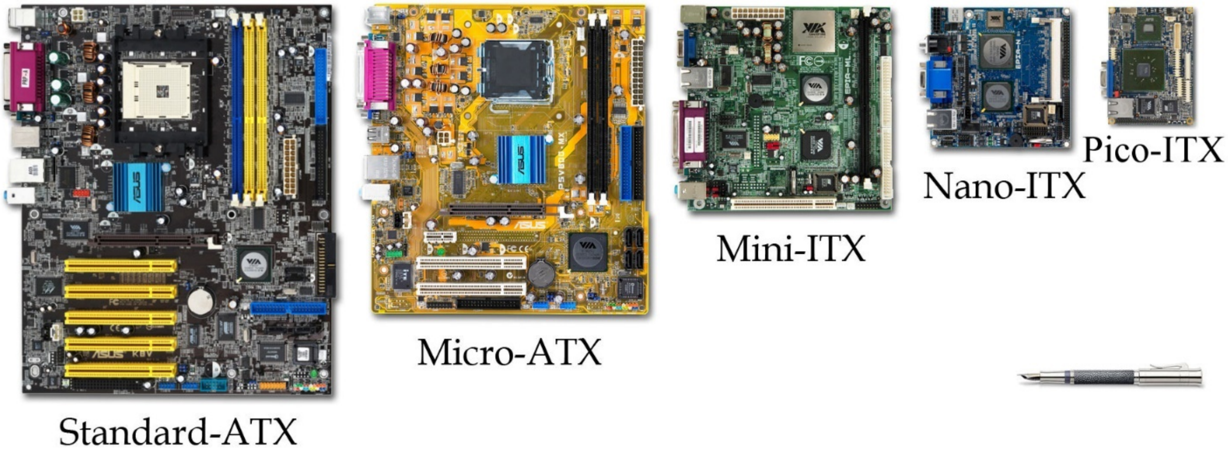
Motherboard Form Factor

The form factor includes

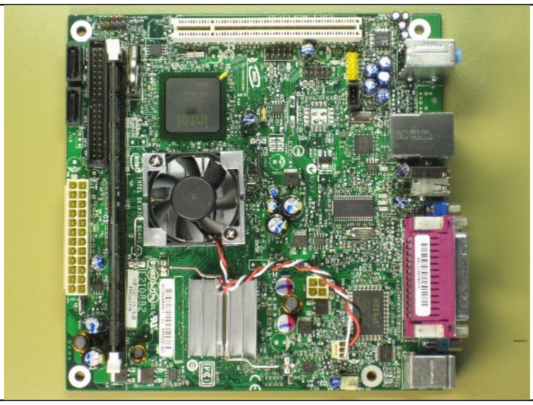
- Motherboard dimensions
- Number of slots
- Location of screw holes
- Type of power connector

Motherboard sizes and screw holes





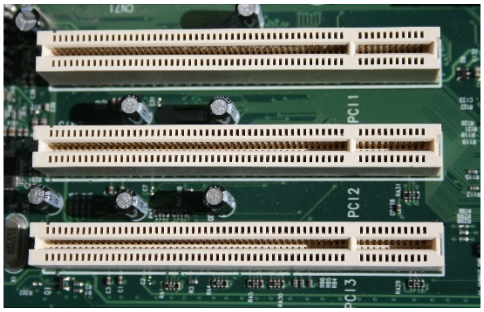
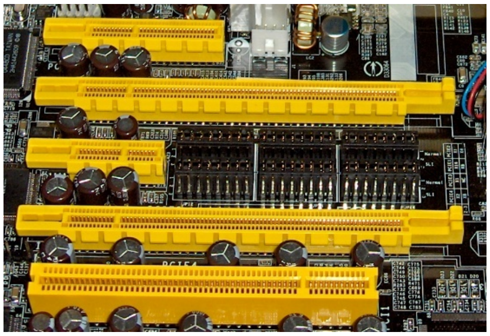
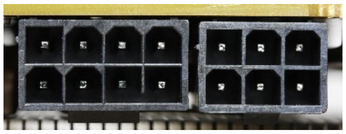
ATX	Most common size Uses a 20-pin or 24-pin power connector Can supply 3.3V, 5V, and 12V power to connected devices Up to seven PCI or PCIe slots
mATX (Micro-ATX)	Backwards compatible with an ATX motherboard Can be mounted to the same cases as an ATX board (screw holes line up)
mITX (mini-ITX)	Some boards contain an on-board CPU Can be mounted to the same cases as an ATX board (screw holes line up)

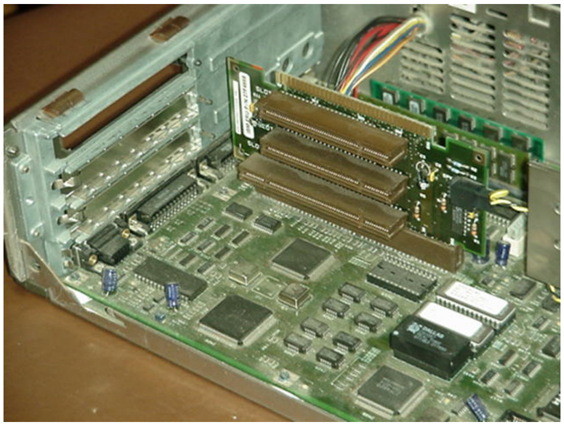
	

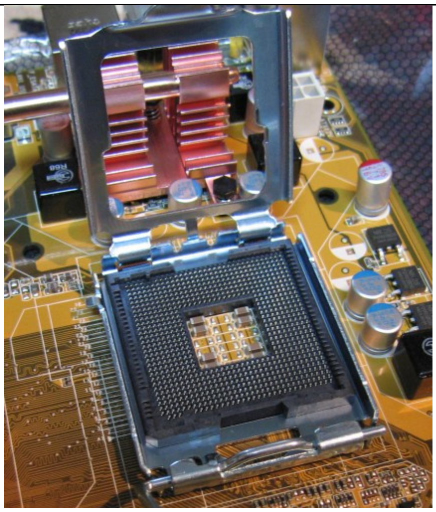
How to install a motherboard

- Place motherboard in case and line up with screw holes
- Insert screws and tighten
- Connect appropriate cables (power, peripherals)
- Install other components such as the RAM and processor

Motherboard Connector Type

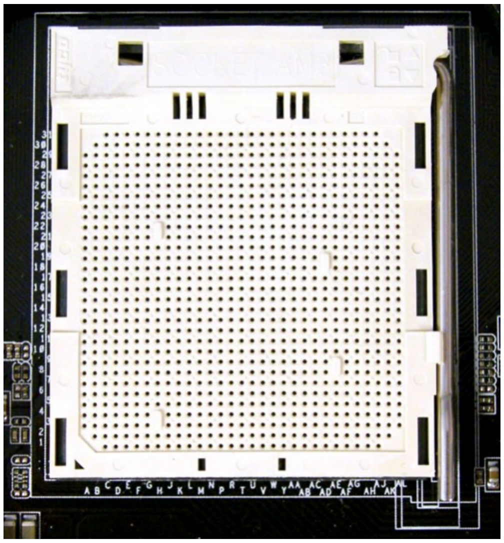
PCI	Peripheral Component Interconnect Allows us to connect a PCI card (such as a graphics card) Card slot is only available in one size 
PCIe	Peripheral Component Interconnect Express Allows us to connect a PCIe card (such as a graphics card) A PCIe slot is faster than a PCI slot and available in more sizes  A PCIe card may obtain power from the system board or may have a separate power connector  PCIe slots are backwards compatible with PCI cards

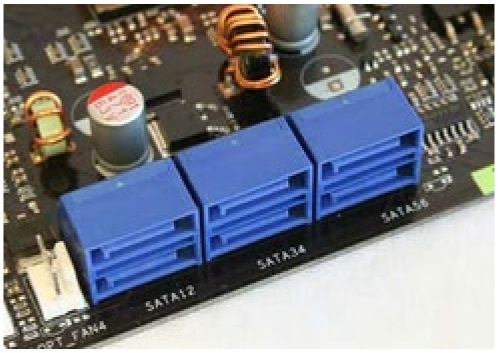
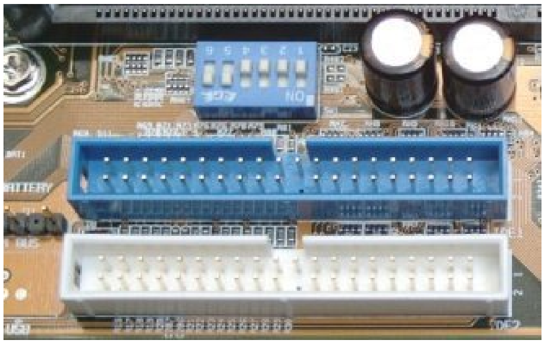
Riser Card	A Riser Card allows us to connect additional cards by providing additional slots It is inserted into the system board Allows us to install cards horizontally Used mainly in rack-mount servers, which don’t have enough space to mount cards vertically 
Socket Types	A socket is a slot for a processor There are two main socket types LGA (Land Grid Array) • Used by Intel • The socket contains pins • There are multiple types of LGA sockets such as LGA 1156, and LGA 1155 • Each socket type has a different number of pins and a different shape • You must match the processor socket type with the motherboard socket type. If the sockets are different, the processor won’t fit.

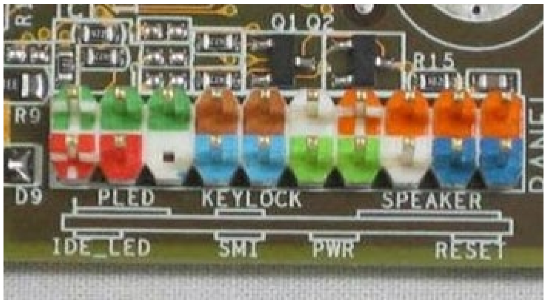
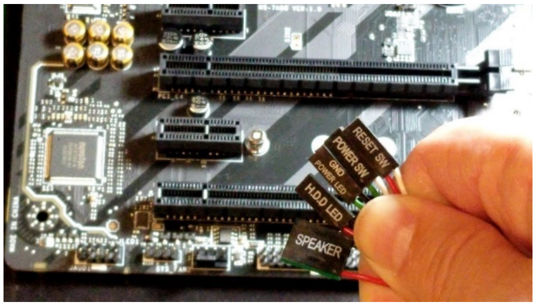


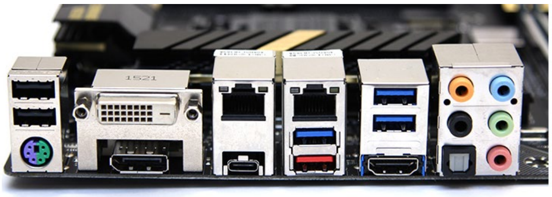
PGA (Processor Grid Array)

- Used by AMD
- Pins are on the processor
- There are multiple types of PGA sockets such as AM2+ and AM3
- Each socket type has a different number of pins and a different shape
- You must match the processor socket type with the motherboard socket type. If the sockets are incompatible, the processor won't fit.

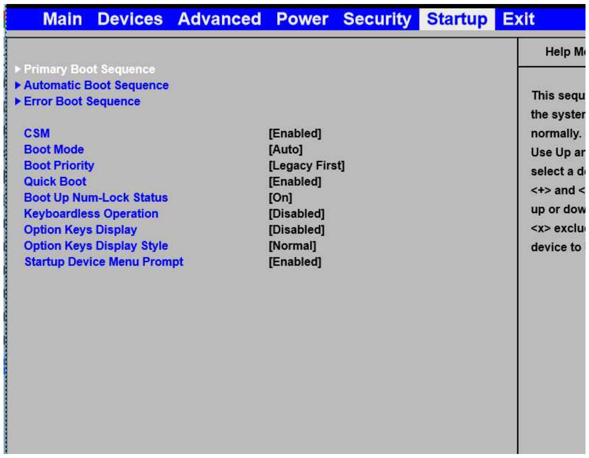


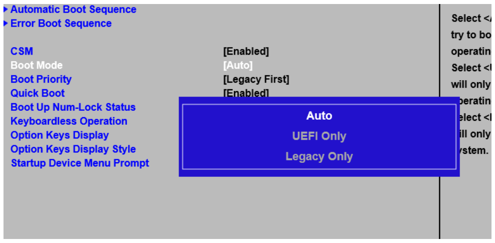
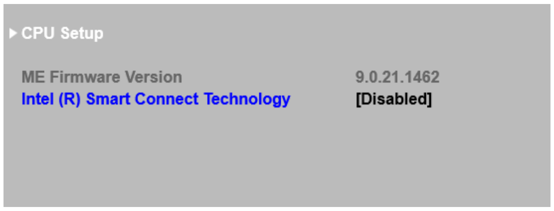
SATA	A motherboard will have multiple SATA connectors Each SATA connector can connect to a drive (HDD or Optical Drive) SATA connectors can be horizontal or vertical 
IDE	IDE connectors are used to connect to HDDs and Optical Drives Older motherboards will have IDE connectors 
Front Panel Connector	The PC case will have several items on the front panel, including • Power button • Reset button • Power light • Hard Drive activity light • Speaker

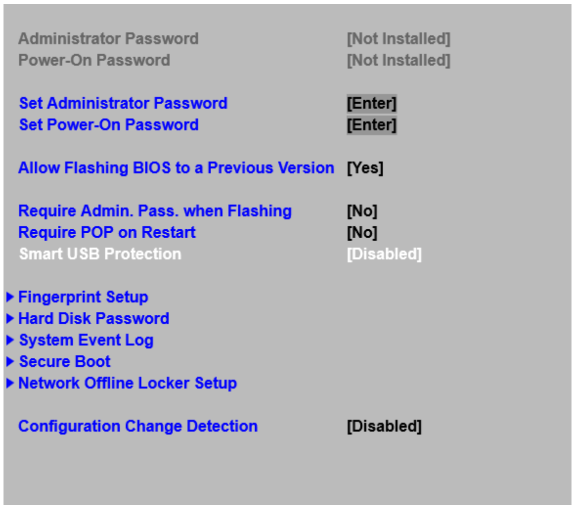
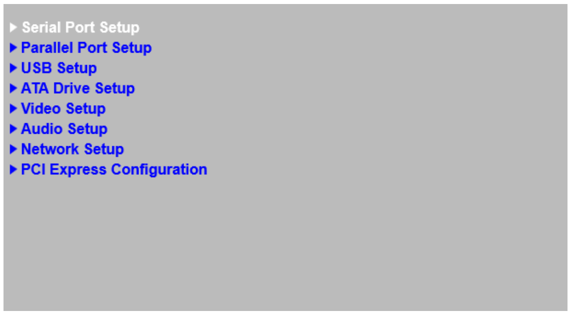
	   The front panel is connected to the motherboard via a cable The connectors on the motherboard may be color coded. Consult the motherboard manual to see how to connect them  Q1 Q2 R15 R9 D9 PLED KEYLOCK SPEAKER PANEL IDE_LED SMI PWR RESET The connectors are typically labelled  RESET SW POWER SW GND POWER LED H.D.D LED SPEAKER
Internal USB Connector	The front panel may contain some USB ports A cable connects the front USB ports to the motherboard USB connector

External Connectors	A motherboard will contain external connectors, including • USB • PS/2 for keyboard/mouse • Ethernet • Speaker/Microphone • Video port (one or more of HDMI, DVI, DisplayPort, VGA) 

BIOS Features

Boot Options	Also known as “start up” Allows you to choose the order of the boot devices The computer will attempt to boot from the first available boot device. If no bootable operating system is found, it will try the next item on the list. Choices include • Hard disk drives • Optical drive • Network • USB (some BIOSs don’t support USB booting)  Main Devices Advanced Power Security Startup Exit Help M ▸ Primary Boot Sequence ▸ Automatic Boot Sequence ▸ Error Boot Sequence This sequ the syster normally. Use Up ar select a d <+> and < up or dow <x> exclu device to CSM [Enabled] Boot Mode [Auto] Boot Priority [Legacy First] Quick Boot [Enabled] Boot Up Num-Lock Status [On] Keyboardless Operation [Disabled] Option Keys Display [Disabled] Option Keys Display Style [Normal] Startup Device Menu Prompt [Enabled] Can choose a “boot mode” • Legacy (run by traditional firmware on Read Only Memory). If you upgrade the computer, you must upgrade the drivers in the Read Only Memory, or a boot error might occur. • UEFI (provides advanced options such as additional operating systems). New Microsoft operating systems don’t

	support Legacy any more. UEFI allows drivers to be incorporated into the system and updated. UEFI is faster • Auto (allows both Legacy and UEFI; automatically detects the correct one to use)  ▸ Automatic Boot Sequence ▸ Error Boot Sequence CSM [Enabled] Boot Mode [Auto] Boot Priority [Legacy First] Quick Boot [Enabled] Boot Up Num-Lock Status Keyboardless Operation Option Keys Display Option Keys Display Style Startup Device Menu Prompt Auto UEFI Only Legacy Only Select < try to bo operatin Select < will only peratin elect < ill only ystem.
Firmware Updates	Allows us to update the BIOS Check the firmware version in the BIOS. Check with the manufacturer to see if an update is available A firmware update can be made by downloading the new firmware and running the update utility  ▸ CPU Setup ME Firmware Version 9.0.21.1462 Intel (R) Smart Connect Technology [Disabled]
Security Settings	Several settings are available • BIOS password (requires a password to change BIOS settings) • Power-On Password (requires a password to power on the computer, before the Operating System is loaded) • Smart USB Protection (prevents copying or use of USB devices) • Secure Boot (prevent new or unauthorized operating systems from

	being loaded, such as on USB drives). Secure boot remembers the digital signature of the boot operating system. It blocks operating systems with different signatures from loading.  Administrator Password [Not Installed] Power-On Password [Not Installed] Set Administrator Password [Enter] Set Power-On Password [Enter] Allow Flashing BIOS to a Previous Version [Yes] Require Admin. Pass. when Flashing [No] Require POP on Restart [No] Smart USB Protection [Disabled] ▸ Fingerprint Setup ▸ Hard Disk Password ▸ System Event Log ▸ Secure Boot ▸ Network Offline Locker Setup Configuration Change Detection [Disabled]
Interface Configuration	Allows us to enable/disable computer interfaces, including • Audio • Video • USB • Network • PCI cards • Serial/Parallel ports  ▸ Serial Port Setup ▸ Parallel Port Setup ▸ USB Setup ▸ ATA Drive Setup ▸ Video Setup ▸ Audio Setup ▸ Network Setup ▸ PCI Express Configuration
TPM	Trusted Platform Module Secure chip that stores encryption keys

	Allows a user to encrypt and decrypt a hard disk drive, and prevents brute-force password guessing Ensures that the computer boot process is not hijacked by unauthorized applications
LoJack	Theft recovery system Allows a user to remotely lock, erase, or locate a stolen laptop LoJack software is installed in the BIOS, not the HDD (it’s installed on the HDD on Apple computers). The LoJack software remains on the BIOS even if the firmware is changed

CMOS Battery

- Allows BIOS to store settings and keep an accurate real-time clock, even when the computer is powered off
- Lifespan of approximately three years
- If the computer fails to keep an accurate time, the battery is probably dead and should be changed

CPU Features

Single Core	A processor chip with a single processor, is considered to have a "single core". It can run one task/thread at a time
Multi Core	A processor chip with multiple processors Allows the processor to execute multiple tasks/threads at the same time Commonly, processors will have a "dual core" or two processing units The advantage of having a multi-core processor, as opposed to multiple single-core processors, is that the signals travel faster between the cores The operating system and software must be written to handle multi-core processors in order to take advantage of their functionality
Virtualization	Virtualization allows a single processor to act as multiple processors Typically, must be enabled in the BIOS Virtualization is required to run a virtual machine or a hypervisor Virtualization allows a processor to isolate tasks received from the different virtual machines
Hyperthreading	For each physical core, allows the processor to create two virtual cores The operating system will send instructions addressed to each virtual core Allows an operating system to send two instructions to each core

	Performance improvement is application dependant
CPU Speeds	How many instructions per second a processor can handle Also known as the ‘clock rate’ The clock rate is not an accurate measurement of speed unless you are comparing two processors of the same model Other factors affect processing speed, including the number of cores, hyperthreading technology, the type of application in use, and the architecture of the processor
Overclocking	Overclocking is the process of forcing a processor to run at a faster clock rate than was originally intended The default clock rate is set by the manufacturer considering the amount of heat generated and the amount of power consumed Overclocking causes a processor to use more power and generate more heat When overclocking, consider • Providing adequate cooling (a processor that is overclocked may overheat, causing permanent damage) • Providing adequate power (the system board may not be able to provide enough power) • System stability (a processor that is overclocked may cause errors)

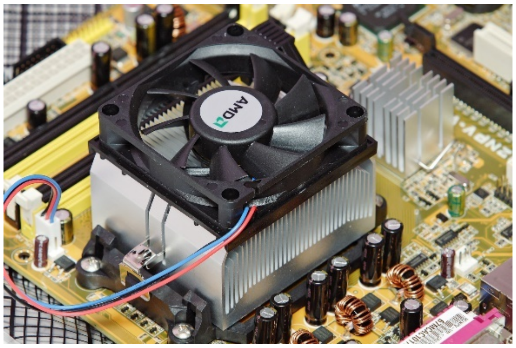
Integrated GPU	An Integrated Graphics Processing Unit allows the processor to handle graphics processing, instead of using a separate GPU System RAM is used for graphics memory

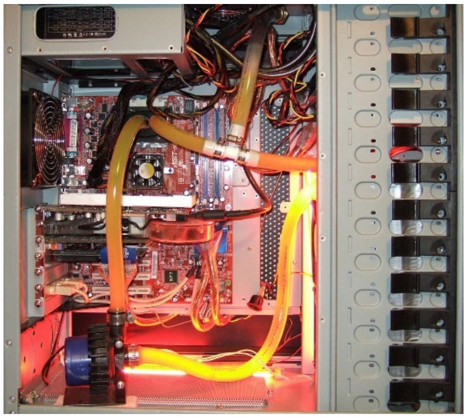
Processor Types

AMD	AMD and Intel both make good processors They have most of the market share There are differences in the processors, but products tend to change over time
Intel	Intel produces processors for desktops, laptops, and other devices Main Intel product line • i3 processor: dual-core, 4MB cache • i5 processor: quad-core, doesn’t supports hyperthreading, 6MB cache • i7 processor: quad-core. supports hyperthreading, 8MB cache
ARM	ARM processors are used in consumer electronics such as phones, tablets, multimedia players Processors are smaller and use less power

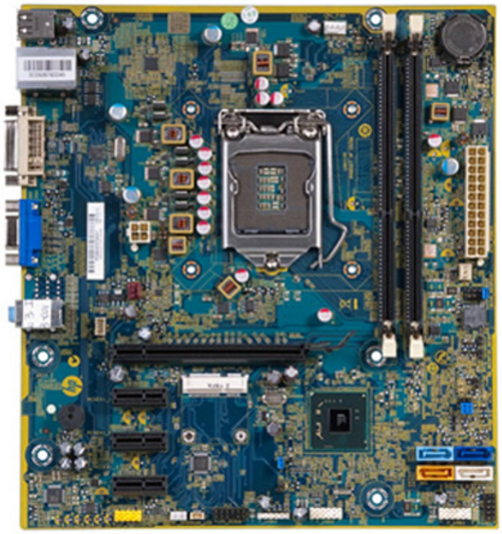
Computer Cooling

Fans	A computer fan is usually, but not always necessary It depends on the design of the case Typical computer cases will come with fans pre-installed A fan draws cool air from outside the case and blows it inside. As the air warms up, it is ejected outside the case. Proper cooling is important. Heat can damage computer components. arctic cooling www.arctic-cooling.com arctic fan Pro TC A CPU will normally have a fan mounted on top of it. A processor is typically sold with a fan and heatsink. A graphics card will also typically have a fan installed on it.
Heat Sink	A heat sink sits on top of the processor It absorbs heat from the processor It has fins, which increase its surface area and allow cooling

	 A fan may sit on top of the heatsink 
Thermal Paste	Between the heatsink and the processor is a layer of thermal paste Thermal paste allows more efficient transfer of heat from the processor to the heatsink
Liquid Cooling	Liquid cooling involves pumping a liquid through the computer A pump forces the liquid through a heat exchanger, which is in contact with the processor and other components Liquid passing through the heat exchanger absorbs heat The liquid then passes through a radiator, which is external to the computer

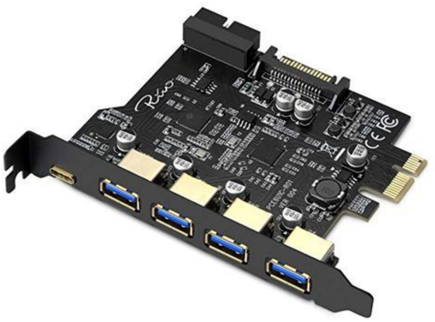
	The liquid cools off in the radiator, and then is returned to the computer  Note that the liquid never actually touches the computer components Liquid cooling is more efficient than air cooling, and is necessary for overclocking

Expansion Card

Video Card - Onboard	An onboard video card is a chip that is integrated into the motherboard or part of the existing processor Also known as an integrated graphics chip Most motherboards have integrated graphics chips The graphics chip on this motherboard is located on the lower right corner It is not possible to upgrade an onboard video card 
Video Card - Expansion	An expansion video card is a separate card The graphics card will have separate video ports as outputs The type and quantity of ports depends on the model of graphics card It is possible to use both an integrated and an expansion video card at the same time • Can force specific monitors to use the integrated graphics and others to use

	the expansion graphics, if you change the video setting in the BIOS The expansion card plugs into the motherboard (PCIe port or AGP port) An additional driver may be required An expansion video card may have separate • Processors • Fans • Memory • Video Ports
Sound Card	Most motherboards are equipped with integrated sound cards. A sound card provides audio input and output. It is possible to add a separate sound card

	A sound card may provide enhanced audio quality as compared to the integrated sound TAD CD_IN AUX_IN I2S_IN CD_SPDIF MODEL: CT4670 Sound BLASTER live! NEITRON Important to consider - How many audio channels a sound card produces (each audio channel corresponds to a source). If we're mixing music from multiple sources, then each source could be a different channel. - Intel High Definition Audio is an integrated audio chip. It is a standard feature of many motherboards and provides 15 channels.
NIC	Network Interface Card The network interface provides an ethernet connection. A motherboard will typically have one integrated network interface, which can operate at 100 or 1000 Mbps. It is possible to add additional network interfaces through expansion cards. Additional interfaces can be copper or fiber, and can operate at 100

	Mbps, 1000 Mbps, 10 Gbps, or even 40 Gbps. These faster speeds are not practical for most applications.
USB Expansion Card	USB Expansion Card A motherboard will typically have several integrated USB interfaces. They may be USB 2.0, 3.0, or a combination of the two. A motherboard will also typically have a connector for the USB ports at the front of the case. It is possible to add additional USB ports with an expansion card. 
eSATA Card	A motherboard may have an integrated eSATA interface.

	The eSATA interface provides connectivity to external storage devices. It is possible to add additional eSATA interfaces through an eSATA card.

3.6 Explain the purposes and uses of various peripheral types.

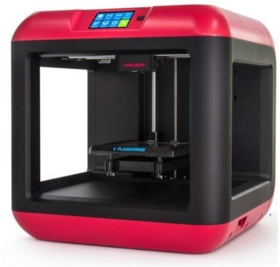
- *Printer*
- *ADF/flatbed scanner*
- *Barcode scanner/QR scanner*
- *Monitors*
- *VR headset*
- *Optical*
- *DVD drive*
- *Mouse*
- *Keyboard*
- *Touchpad*
- *Signature pad*
- *Game controllers*
- *Camera/webcam*
- *Microphone*
- *Speakers*
- *Headset*
- *Projector*
    - *Lumens/brightness*
- *External storage drives*
- *KVM*
- *Magnetic reader/chip reader*
- *NFC/tap pay device*
- *Smart card reader*

Printer

Purpose	Converts an electronic document into a paper document
Features	There are many types of printers • Inkjet Printer (applies drops of ink to the page). • Laser Printer (can be black & white or color; applies toner to a drum; the toner is applied to the paper and fused) • Solid Ink Printer (melts blocks of solid ink; the melted ink is sprayed onto the paper) • Thermal Printer (applies heat to a thermosensitive paper, which changes color; common for receipt printers and label printers) • Impact printer (contains a ribbon; a bank of hammers strike the ribbon to produce an ink impact on the page) • 3D Printer ('prints' 3D objects using a plastic polymer or another chemical, which cures and hardens) Printing media • Typical printers accept paper of 8.5" x 11" dimensions. • Larger printers can accept paper of 11" x 17" dimensions. • Plotter-type printers can accept paper rolls, which can be up to 5' wide • Printers can also print on DVDs, t-shirts, and transparent sheets

	A printer may be an “all-in-one” • Includes a scanner, photocopier, and fax machine A printer may have the ability to collate, staple, and hole-punch documents.
Size	Printers range in size from small portable printers to large printing press printers that can occupy an entire room
Cost	Printer costs • $100 to $500 for basic laser printers • $1000 to $5000 for enterprise laser printers • $20,000 to $200,000 for high capacity printers • $1,000 to $1,000,000 for 3D printers
Connectivity	A printer will include one or more of the following interfaces • USB • Ethernet • Wi-Fi • Bluetooth • Parallel (old) • Some printers have connectors for memory cards and USB drives (they can read and print documents off memory cards and USB drives)

	A printer may have the ability to connect via more than one interface at a time.
Examples	A Basic Laser Printer An All-In-One

	A Large Printing Press Type Printer A 3D Printer  A Thermal Printer

	An Impact Printer

ADF/Flatbed Scanner

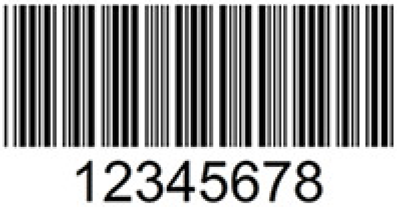
Purpose	Converts a paper document into an electronic document
Features	A Flatbed scanner requires you to place the document face down. It will scan one page at a time. • Good for scanning books, pages that are stapled together, and other documents that can't be separated An Automatic Document Feeder allows you to insert multiple sheets. It automatically feeds the sheets through the scanner. • Good for scanning loose sheets with little effort Can automatically save the document as an image or PDF. Some scanners can e-mail scanned documents. A scanner may be part of a printer/all-in-one. Scanners have different input sizes, including • 8.5" x 11" size • 11" x 17" size • large format scanners for scanning blueprints
Size	Range in size from portable scanners to large format scanners.

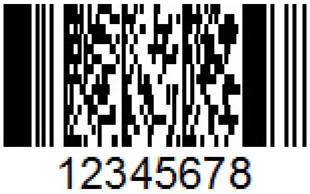
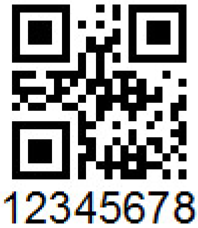
Cost	Price ranges from $100 for a portable scanner to $10,000 for a large format scanner.
Connectivity	A scanner will include one or more of the following interfaces • USB • Ethernet • Wi-Fi • Bluetooth • Parallel (old) • Some scanners have connectors for memory cards and USB drives (they can save documents to memory cards and USB drives) A scanner may have the ability to connect via more than one interface at a time.
Examples	All in One

	Flatbed Scanner Scanner with Automatic Document Feeder Large Format Scanner

	Portable Scanner

Barcode Scanner/QR Scanner

Purpose	Scans barcodes or QR codes
Features	A barcode scanner can be handheld or fixed to a machine A mobile device can be equipped with a barcode scanner There are several different barcode styles that can be scanned A barcode scanner receives power • via USB, or • includes a battery, and can be recharged by placing it into a docking station Android-based "smartphone style" barcode scanners are becoming popular. They can run different applications and can retrieve and display data corresponding to the barcodes that they scan. Typical Barcode Style (contains only numeric information) 

	Advanced Barcode Style (can contain additional data)  QR Code (Can contain a substantial amount of data) 
Size	Small in size
Cost	Cost between $100 and $1000
Connectivity	A barcode reader will connect with one of the following interfaces • Wi-Fi • Bluetooth • USB

Examples	Wireless Barcode Scanner Barcode Scanner with Display Android-Based Smartphone-Style Barcode Scanner

Monitor

Purpose	Displays video
Features	Monitors range in size, quality, and features Monitor technology • LCD monitors are most common (flat screen, but contains a backlight) • LED monitors are becoming more popular (flat screen, without a backlight; LED monitors can display colors better) • Older monitors are CRT (poor video resolution) Size • 15" to 17" monitors are less popular • 19" to 25" monitors are more popular • Larger sizes (up to 80") are available. It is possible to connect a television to a PC video output. • Smaller sizes are available for industrial equipment and appliances (e.g. control panels, refrigerators, etc.) Resolution • 1080p • 2K • 4K • 8K A monitor will have adjustments for the color, contrast, and image location.

	Additional features • A monitor may contain USB ports, for user convenience. The monitor has an ”output” USB cable, which connects to the PC. • Some monitors have touchscreen capabilities. A touchscreen monitor will connect to the PC via USB. • Curved monitors. Curved monitors are popular with gamers. • Output. A monitor may have a video output, so that it can send video to another monitor. Several monitors can work together to display one large image or video.
Size	Monitors range in size from 15” to 80”
Cost	Cost depends on size and quality Monitors cost between $100 and $10,000
Connectivity	A monitor will have one or more inputs • HDMI (most popular) • DisplayPort (also popular) • DVI (less popular) • VGA (popular) Most monitors will have a VGA port and an HDMI or DisplayPort port A monitor will connect via USB if it contains USB ports. A monitor will connect via USB (or rarely by serial) it has touchscreen capabilities

Examples	Monitor Curved Monitor CRT Monitor

	Industrial Monitor

VR Headset

Purpose	Provides a virtual reality experience
Features	Contains cameras and sensors that capture the user's movement and where his or her eyes are looking
Size	Size of a football helmet
Cost	Cost between $500 and $5000
Connectivity	Connect via HDMI, Wi-Fi, Bluetooth, and/or USB A device may require multiple connections.
Examples	

Optical/DVD Drive

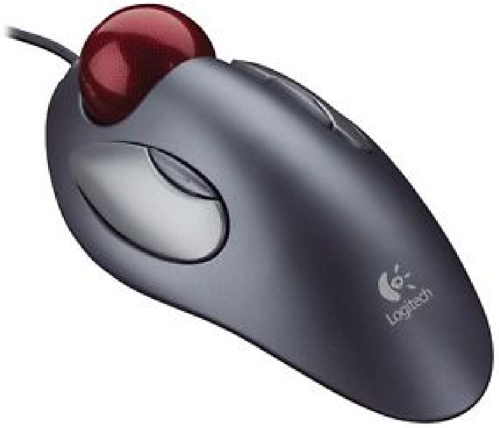
Purpose	Allow you to read data from a CD, DVD, or Blu-Ray Disc Allow you to record data to a CD-R, DVD-R, etc.
Features	A drive may be a 3.5" wide drive that fits into a computer tower or may be external (connects via USB). Optical media is becoming less popular. Increasingly, laptops are being manufactured without optical drives. Drives range in read/write speed Some drives offer LightScribe (which allows you to etch an image into a rewritable CD/DVD). This feature has been discontinued by its manufacturer.
Size	Typically, 3.5" wide
Cost	Cost around $100
Connectivity	Connects via SATA (internal drive) or USB (external drive)

Examples	Internal Drive External Drive

Mouse

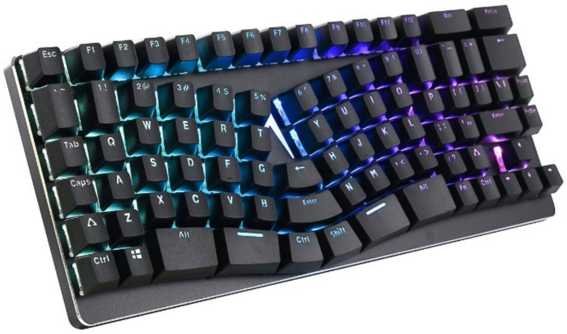
Purpose	Allow you to interact with the computer by pointing and clicking
Features	Typical mouse will have • Left button • Right button • Scroll wheel (can scroll up and down; may also be able to scroll left and right, or click with the scroll wheel) Some mice have additional buttons, which can be programmed to perform specific tasks. Some mice have ergonomic features, which can reduce hand strain. Features include • Ergonomic shape • Rubber coating At the bottom of the mouse is an optical sensor, which detects the direction and speed of the mouse. Older mice use rubber balls, which roll. A mouse may be sold with a keyboard.
Size	About 5” long
Cost	Cost between $10 and $100
Connectivity	Three primary ways to connect a mouse • USB

	- Bluetooth - Wireless dongle (a dongle connects to the computer via USB, and the mouse connects to the dongle). If you lose the dongle, you must purchase a new mouse.
Examples	Old Roller Mouse New Basic Mouse

	New Advanced Mouse Roller-Type Mouse (the mouse does not move; instead the user rotates the red ball to move the cursor) 

Keyboard

Purpose	Allow you to interact with the computer by typing
Features	Typical keyboard will have • Several keys (letters A to Z, numbers, and special characters) • A number pad containing the numbers • Several function keys that can perform special functions • Windows keyboards have a key with the Windows logo, which launches the start menu • Keyboards are available in multiple languages besides English • A keyboard may contain a backlight that lights up the keys in a dark room. Some keyboards have additional buttons, which can be programmed to perform specific tasks. Some keyboards have ergonomic features, which can reduce hand strain. Features include • Ergonomic shape • Rubber coating At the bottom of the mouse is an optical sensor, which detects the direction and speed of the mouse. Older mice use rubber balls, which roll. A mouse may be sold with a keyboard.
Size	About 12" wide

Cost	Cost between $10 and $100
Connectivity	Three primary ways to connect a keyboard • USB • Bluetooth • Wireless dongle (a dongle connects to the computer via USB, and the keyboard connects to the dongle). If you lose the dongle, you must purchase a new keyboard. If you purchase a keyboard and mouse as a set, they will come with one dongle.
Examples	Basic Keyboard Ergonomic Keyboard 

Touchpad

Purpose	Similar to a mouse; allows a user to interact with the screen by pointing and clicking.
Features	Touch sensitive pad Contains two or three buttons (left and right click). May have the ability to scroll, click, or zoom in/out by clicking on the pad or using multiple fingers. Advanced drawing pads contain multiple levels of pressure sensitivity Can interact with the pad via a stylus
Size	About 5" square
Cost	Cost between $10 and $100
Connectivity	Can connect via • USB • Bluetooth • ZIF connector (for laptops)

Examples	Drawing Pad Larger Drawing Pad Laptop Touch Pad

Signature Pad

Purpose	Allows a user to capture a signature Commonly used in banks and on point of sale systems
Features	Contains a stylus for allowing a user to sign. May also accept feedback from a finger. The signature pad may include an LCD screen that can display the signature. Signature pads can be integrated into smartphones, tablets, and credit card machines.
Size	About the size of a smartphone.
Cost	Cost between $10 and $100
Connectivity	Connect to PC via - USB - Serial cable
Examples	Signature Pad with Screen

	Signature Pad with no Screen

Game Controller

Purpose	Input to play games
Features	Contains several buttons with different shapes and functions. Buttons can be programmed and may have different functions with different games. May contain “force feedback”, which allows the controller to vibrate in response to on-screen events. Controllers may be shaped ergonomically to reduce hand strain.
Size	Size of a smartphone or larger
Cost	Between $50 and $1000
Connectivity	Connects via • USB • USB (with a wireless dongle) • Bluetooth • Proprietary Connector

Examples	Standard Game Controller Controller for a Flight Simulator Steering Wheel Controller for Automotive Games

Camera/Webcam

Purpose	Allow you to input video for live video conferencing. Allow you to record video for later use.
Features	Cameras are available in several resolutions, including 1080p and 4k. A camera may also capture video. Advanced cameras for video conferencing can detect motion and automatically pan/tilt/zoom towards the person who is speaking. These cameras are ideal for large conference rooms. It's possible (although difficult) to connect a DSLR camera or camcorder to a computer via a video capture card and HDMI port.
Size	Small size
Cost	Cost between $100 for a basic web cam and $2000 for a conference room camera
Connectivity	Connect via USB

Examples	Web Cam Conference Room Camera

Microphone

Purpose	Allow you to capture audio
Features	Most laptops have integrated microphones, which have poor quality. USB microphones can capture audio at a higher quality A microphone can be integrated into a set of earphones or headphones Some microphones can • Adjust the gain (the volume of the audio that is captured) • Filter noise such as crackles, pops, and hisses • Adjust the range of audio capture (from directly in front of the microphone to the entire room)
Size	Small size
Cost	Cost between $10 and $1000
Connectivity	Connect via • Microphone jack (headphone jack) • USB • Bluetooth

Examples	Microphone with Headset High Quality Microphone

Speakers

Purpose	Play audio
Features	Computer speakers can be stereo (two speakers) or can offer a surround sound experience such as Dolby 5.1 Surround Sound Computer speakers may include a subwoofer (plays low sounds) Speakers may have a volume control adjustment Audio quality depends on the type of speakers Larger speakers may require an external power source
Size	Can be portable or large
Cost	Cost between $10 and $1000
Connectivity	Connect via • Speaker jack (headphone jack) • USB • Bluetooth

Examples	Basic Computer Speakers (connect to audio jack for audio, and USB for power) Computer Speakers with Subwoofer

Headset

Purpose	Can hear audio privately and can record audio or broadcast live audio
Features	Audio and microphone quality vary between headset models A headset may or may not include a microphone May contain noise cancelling features to prevent you from hearing external sounds
Size	Small size
Cost	Between $10 and $1000
Connectivity	Connect via - Headphone jack - USB - Bluetooth
Examples	Headset with Microphone

	Headset without Microphone

Projector

Purpose	Displays video on a wall or screen
Features	A projector functions like a monitor and can have different resolutions, inputs, and features A projector can display video on a wall, floor, or screen, but it is better to display video on a dedicated screen. Projector screens are designed to provide optimal display quality. A projector may use LED, LCD, or DLP technology. A projector is rated based on the number of lumens that it can output. Projectors with larger amounts of lumens are good for larger rooms and/or rooms with high amounts of ambient light • A projector with 1500 lumens is good for a small room • A projector with 4000 lumens is good for a conference room • A projector with 30,000 lumens is good for an auditorium or for projecting onto the side of an office building Resolution • 1080p • 2K • 4K • 8K

	A projector will have one or more inputs • HDMI (most popular) • DisplayPort (also popular) • DVI (less popular) • VGA (popular) Most projectors will have a VGA port and an HDMI or DisplayPort port A projector will have adjustments for the color, contrast, and image location. A projector will have additional adjustments for "keystone", image position, and focus. Advanced projectors can "auto-focus" the image.
Size	Projectors can be portable (small) or ceiling-mounted (large and heavy)
Cost	Range in cost from $500 to $50,000 for advanced theater projectors
Connectivity	Connects via • HDMI, DVI, VGA, etc. for video signal input • Bluetooth • USB for control and possibly for video input (a portable projector may only have one USB input for power, video, and control) • Ethernet for network connectivity • Serial cable for external control

Examples	Portable Projector Standard Sized Projector Ceiling-Mount Projector

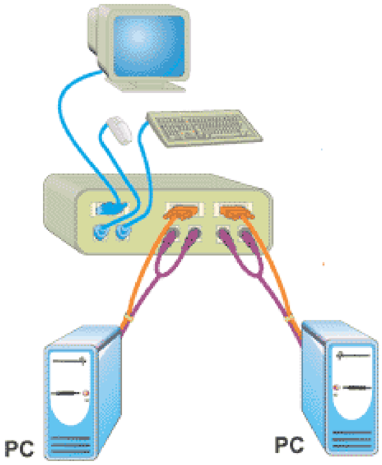
External Storage Drive

Purpose	Stores data externally. Good for back ups and for storing data when there is no space available.
Features	External Storage Devices include • Portable hard drive • USB thumb drive • Memory cards Capacity can range from 1GB to 4TB. Memory cards and thumb drives contain solid state memory. Larger portable hard drives contain magnetic drives. Thumb drives are available in a wide variety of shapes and colors. Can be customized for promotional activities.
Size	Portable hard drives are 3.5”, thumb drives are smaller
Cost	Cost between $5 for a thumb drive, and $200 for a portable hard drive
Connectivity	Drives connect via USB External cards connect via a card slot in a computer or phone

Examples	Thumb Drive SD Card Portable Hard Drive

KVM

Purpose	Keyboard-Video-Mouse. Allows you to share a keyboard, video display, and mouse with multiple computers.
Features	The KVM Switch contains three output ports • one for a keyboard (USB or PS/2) • one for a mouse (USB or PS/2) • one for a monitor (HDMI, VGA, or another connector) The KVM Switch has two or more input ports. Each input port allows you to connect a computer via USB and via video (typically VGA). You can switch inputs by pressing a button on the KVM switch. Good for a rack of servers, where there is only enough space for a single monitor. A KVM can also be connected to the internet, allowing a user to remotely connect to a computer via the internet, even when it is booting up.

	
Size	Can be small, can be rack-mounted, depending on the number of inputs
Cost	Cost between $100 and $1000
Connectivity	Connect via USB and video input
Examples	KVM Outputs

	Large KVM

Magnetic Reader/Chip Reader

Purpose	Allows you read/write data stored on a magnetic card or on a credit card.
Features	Can be standalone or part of a credit card/debit card machine, which would allow you to process transactions. A wide range of credit card machines are available. Some are touch screen. Typically used with point of sale systems.
Size	Small size
Cost	Cost between $100 and $1000
Connectivity	Connect to computer via USB, serial, or Bluetooth. May connect to the internet via ethernet or Wi-Fi, or may connect to the internet through the computer.

Examples	Magnetic Card Reader Chip Card Reader (contains magnetic card reader as well) Handheld Reader

NFC/Tap Pay Device

Purpose	Allows you to read/write data from a cell phone or credit card via Near Field Communication.
Features	May be integrated into a credit card reader
Size	Handheld
Cost	Cost between $100 and $500
Connectivity	Connect to computer via USB, serial, or Bluetooth. May connect to the internet via ethernet or Wi-Fi, or may connect to the internet through the computer.
Examples	Chip Card Reader (contains magnetic card reader as well) Handheld Reader

Smart Card Reader

Purpose	Allows you to read/write data stored on a smart card. Allows you to access restricted data on a computer requiring two-factor authentication.
Features	There are many standards for smart cards. It is important to locate a reader that works with the type cards you are utilizing
Size	Small
Cost	Cost about $100
Connectivity	Connects via USB or serial
Examples	

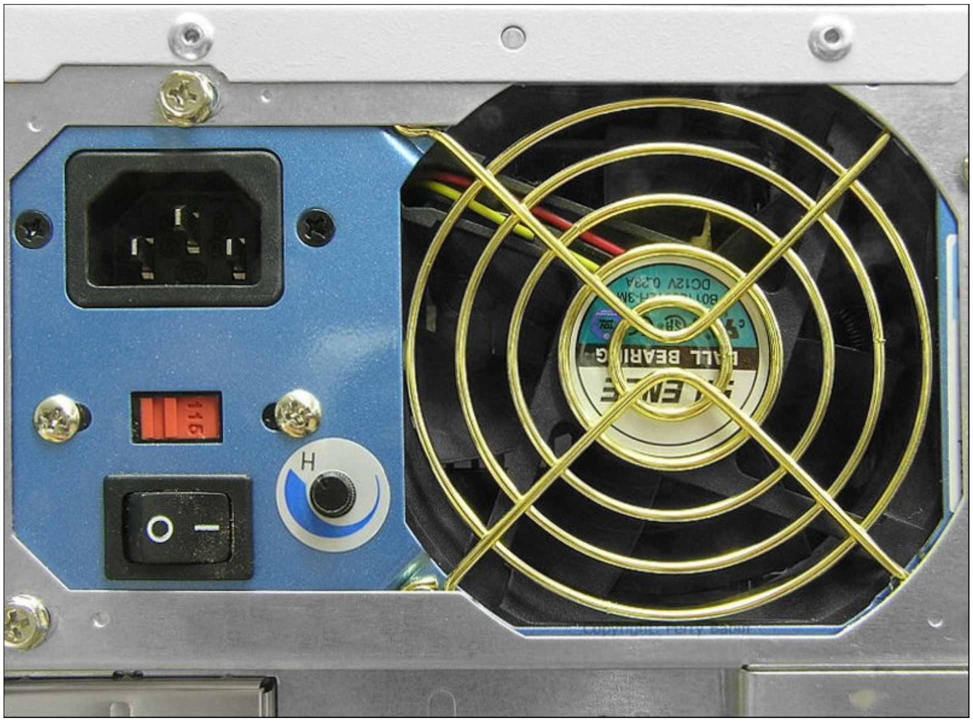
3.7 Summarize power supply types and features.

- *Input 115V vs. 220V*
- *Output 5.5V vs. 12V*
- *24-pin motherboard adapter*
- *Wattage rating*
- *Number of devices/types of devices to be powered*

Power supply

115V vs 220V

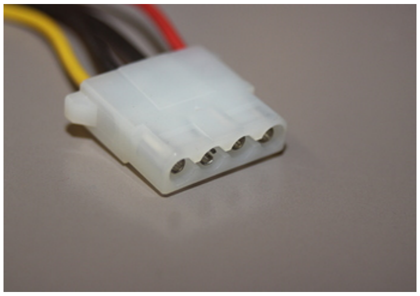
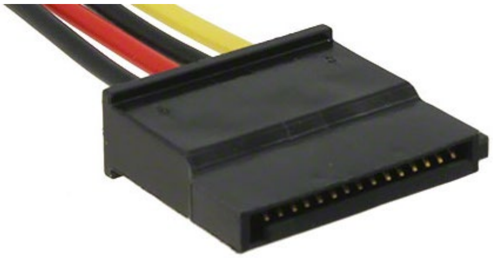
- Canada, United States. Mexico, and many South American countries use 120V electricity at 60 Hz
- European and Asian countries use 220V, 230V, or 240V electricity at 50 Hz
- Electricity supplied by a wall outlet is AC (Alternating Current). That means that the electricity changes direction 50 (50 Hz) times per second or 60 (60 Hz) times per second.
- A computer requires electricity in DC (Direct Current) at +3.3 V, +5 V, and +12 V. That means that the power supply must change the electricity and its voltage.
- At the back of the power supply is an input voltage selector (the red switch)

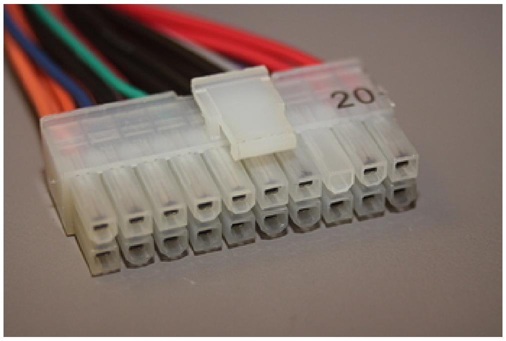
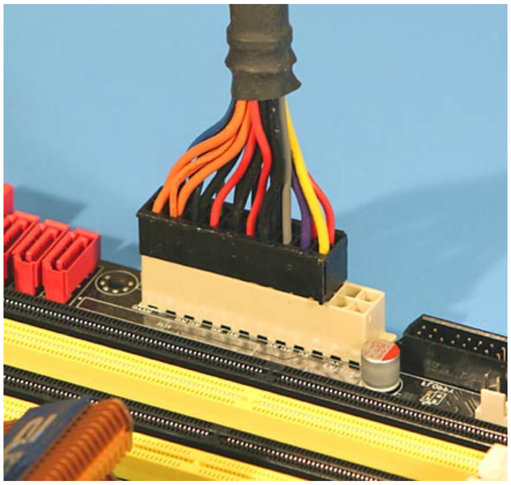
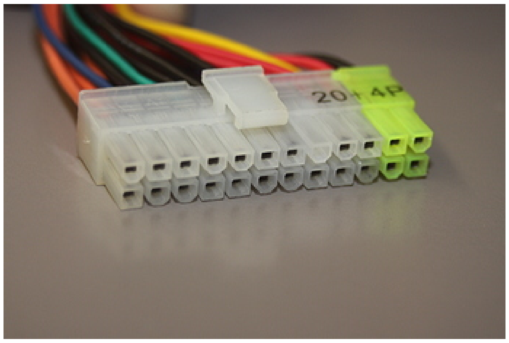


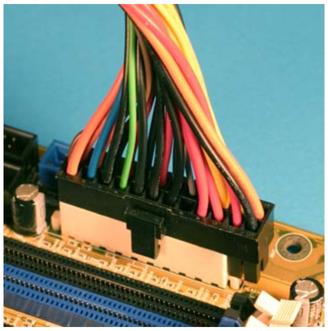
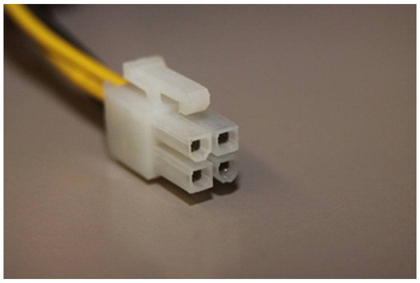
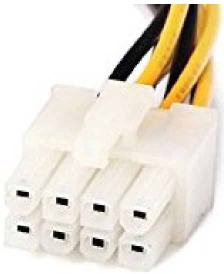
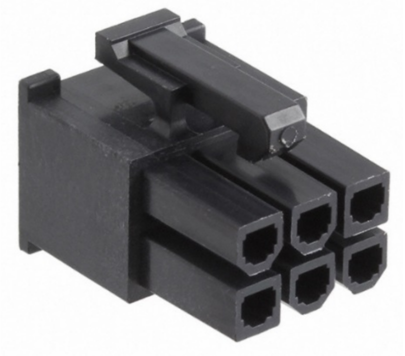
- A power supply has a Wattage rating (the number of Watts it can produce)
    - The wattage required is typically around 300W for a basic computer, and up to 1000W for a gaming computer
- Calculate the power consumption of each computer component to determine the total power requirement (in Watts). Select a power supply that is 40% more than the total power requirements.

Output of +3.3 V, +5 V, and +12 V

- A power supply has multiple power outputs
- Each output is known as a rail
- Older processors use 5V power, newer processors use 12V power
- There are numerous connection types
- Connect each rail to the appropriate computer component

4-Pin Peripheral Connector Also known as a "Molex" connector, which is the brand name A power supply will have several Connects older HDDs	
SATA Connector Provides 12V power to a SATA drive A power supply will have several, daisy chained together	

20-Pin Connector Connects Power Supply to Motherboard Provides +3.3V, +5V, and +12V	 It's possible to connect a 20-Pin cable into a 24-Pin connector 
24-Pin connector Connects Power Supply to Motherboard Identical to the 20-Pin connector, with 4 additional pins added to provide more current. The additional 4 pins can be removed, which allows the device to connect to a 20-pin motherboard instead.	 It's possible to connect a 24-Pin cable into a 20-Pin connector

	
4-Pin Connector Provides power to CPU This is different from the 4-Pin connector in the 24-pin connector	
8-Pin Connector Powers high-end graphics cards	
6-Pin PCIe Connector Powers PCIe cards	

3.8 Given a scenario, select and configure appropriate components for a custom PC configuration to meet customer specifications or needs.

- *Graphic/CAD/CAM design workstation*
  - *Multicore processor*
  - *High-end video*
  - *Maximum RAM*
- *Audio/video editing workstation*
  - *Specialized audio and video card*
  - *Large, fast hard drive*
  - *Dual monitors*
- *Virtualization workstation*
  - *Maximum RAM and CPU cores*
- *Gaming PC*
  - *Multicore processor*
  - *High-end video/specialized GPU*
  - *High-definition sound card*
  - *High-end cooling*
- *Standard thick client*
  - *Desktop applications*
  - *Meets recommended requirements for selected OS*
- *Thin client*
  - *Basic applications*
  - *Meets minimum requirements for selected OS*
  - *Network connectivity*
- *Network attached storage device*
  - *Media streaming*
  - *File sharing*
  - *Gigabit NIC*
  - *RAID array*

Graphic/CAD/CAM Design Workstation

Purpose	Design of 3D models or Computer Aided Drafting / Modeling
Case	Standard ATX Case
Processor	Multi-Core Processor
RAM	16GB or 32GB, DDR4 dual-channel
Storage	Solid State Drive, adequate capacity (may store data on network, check with user)
Graphics	Separate graphics card with adequate memory (4GB), output for multiple monitors
Sound	Optional
Display	Multiple monitors
Cooling	Normal cooling
Software	Special software for engineering and/or drafting
Network	Integrated NIC

Audio/Video Editing

Purpose	Audio and video editing workstation
Case	Standard ATX Case
Processor	Multi-core processor
RAM	16GB or 32GB, DDR4 dual-channel
Storage	Solid State Drive, large capacity to store raw video May require multiple drives to store video (additional drives can be magnetic to reduce costs)
Graphics	Separate graphics card with adequate memory (4GB), output for multiple monitors
Sound	16-Channel sound card with speakers
Display	Multiple high-resolution displays
Cooling	Normal cooling
Software	Special software for audio/video editing
Network	Integrated NIC

Virtualization Workstation

Purpose	Acts as a server that runs multiple virtual machines. Will handle applications for multiple users. Typically, will connect to computer via RDP or other remote access protocol.
Case	Ideal to use a rack-mount case
Processor	Multi-core processor, or multiple processors if demand is high enough
RAM	32GB or 64GB of RAM Determine amount of RAM based on number of users
Storage	Solid State Drive, medium capacity 1TB may be okay, may use SAS drives May use RAID setup or Network Attached Storage
Graphics	Integrated graphics is acceptable, since computer won't be connected to a monitor
Sound	Sound not required
Display	Display not required, or use a basic monitor or KVM
Cooling	Standard cooling
Software	Hypervisor software Server operating system

	Other software as required by users
Network	NIC with multiple interfaces, 1Gbps

Gaming PC

Purpose	Requires high-end components for optimal performance
Case	Standard case. May provide case with LEDs or other fancy components
Processor	Multi-core
RAM	16GB or 32GB, DDR4 dual-channel
Storage	Solid State Drive, large capacity 1TB may be adequate
Graphics	Separate graphics card with adequate memory (4GB) and output for multiple monitors
Sound	High quality sound card with 16-channels High quality surround sound speakers
Display	Multiple monitors with high resolution & refresh rate
Cooling	Liquid cooling if computer is overclocked
Software	None
Other Components	Mechanical keyboard Game controller
Network	Integrated NIC

Standard Thick Client

Purpose	Standard computer used for basic office applications and e-mail.
Case	Standard ATX Case
Processor	Multi-core processor
RAM	8GB or 12GB of RAM
Storage	Magnetic hard drive
Graphics	Integrated graphics card
Sound	Integrated sound card
Display	Basic monitor or two monitors
Cooling	Standard cooling
Software	Typical office software
Network	Integrated NIC

Thin Client

Purpose	Connects to virtualization server. Doesn't require much processing power. Processing will take place on the server.
Case	Standard ATX case or mini case.
Processor	Single-core processor
RAM	4GB RAM
Storage	Magnetic Drive, 250GB
Graphics	Integrated graphics
Sound	Integrated sound
Display	Basic display or two displays
Cooling	Basic cooling
Software	Typical office software
Network	Integrated NIC

Network Attached Storage Device

Purpose	Stores data for users, network drives, and servers. Could act as a DVR for a surveillance system. Doesn't require much processing power.
Case	Rack-mounted case or Standard ATX Case
Processor	Basic processor
RAM	12GB RAM
Storage	Combination of solid-state and magnetic drives to reduce cost. Use solid-state drives for data that is frequently accessed, and magnetic drive for data that is archived. Use SAS connector if needed. Provide as much capacity as possible Provide RAID controller for redundancy
Graphics	Integrated graphics
Sound	Integrated sound
Display	No display required
Cooling	Standard cooling
Software	No software required
Network	NIC with multiple interfaces May require NIC with Fiber Channel or NIC with 10Gbps connections

3.9 Given a scenario, install and configure common devices.

- *Desktop*
    - *Thin client*
    - *Thick client*
    - *Account setup/settings*
- *Laptop/common mobile devices*
    - *Touchpad configuration*
    - *Touchscreen configuration*
    - *Application installations/configurations*
    - *Synchronization settings*
    - *Account setup/settings*
    - *Wireless settings*

Thin Client

- Connect power, network, peripherals
- Install required software
- Configure settings to connect thin client to virtualization server; possibly a Remote Desktop Connection
- Configure necessary settings on virtualization server

Thick Client

- Connect power, network, peripherals
- Add security tether and asset tag
- Give computer a name based on user preference or corporate policy
- Join Active Directory domain, if applicable
- Set up user account
  - Set up local account on computer
  - Or set up active directory account and have user log in to computer
- Configure user preferences
  - Mouse, keyboard, monitor
  - Desktop
- Install required software
  - Includes antivirus, office productivity, and other software
  - Can push software to computer through server if computer is on a corporate network
- Configure network settings
- Check for software updates
- Install drivers for necessary peripherals
- Encrypt device

Account Setup/Settings

- Is the account a local account or an Active Directory account?
    - Local account is configured on computer
        - On a new computer, you will be prompted to create an account
        - On a computer already in use, go to user profiles and create a new account
        - Will the account require admin access? At least one local account must have admin access.
        - Choose a username and temporary password. The user should be required to change the password.
    - Active Directory account is configured on server
        - Log in to Active Directory
        - Create an account in the correct user group
        - Add necessary policies
        - Generate the temporary password. The user should be required to change the password the first time he/she logs in.
        - In a corporate environment, create accounts for other services (e-mail, HR, etc.). This may be performed manually or automatically depending on the system setup.

Laptop/Mobile Device Settings

Touchpad	Each model of touchpad may have different settings, including • Sensitivity • Function of using multiple fingers at a time (for example using two fingers at a time allows you to zoom in/out)
Touchscreen	Touchscreen may be enabled or disabled depending on the user preference The touchscreen settings can include • Visual feedback when touching the screen
Application Installation	There are thousands of applications and millions of possible settings
Synchronization	Laptop/desktop can sync with cloud and/or phone May require you to install an application, create an account/subscription with cloud service, and then log in on the desktop
Wireless Settings	Connect to correct SSID Enter correct password, username/password, or certificate If the network is hidden, enter SSID
Encryption	Set up encryption Common encryption is BitLocker Choose a password if required

3.10 Given a scenario, configure SOHO multifunction devices/printers and settings.

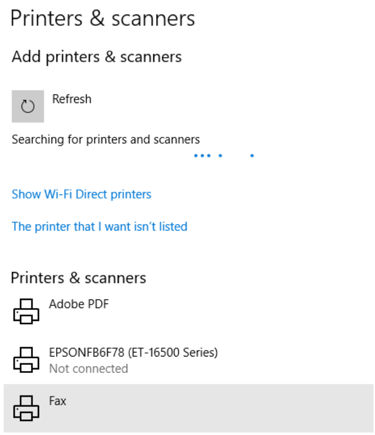
- *Use appropriate drivers for a given operating system*
  - *Configuration settings*
    - *Duplex*
    - *Collate*
    - *Orientation*
    - *Quality*
- *Device sharing*
  - *Wired*
    - *USB*
    - *Serial*
    - *Ethernet*
  - *Wireless*
    - *Bluetooth*
    - *802.11(a, b, g, n, ac)*
    - *Infrastructure vs. ad hoc*
  - *Integrated print server (hardware)*
  - *Cloud printing/remote printing*
- *Public/shared devices*
  - *Sharing local/networked device via operating system settings*
    - *TCP/Bonjour/AirPrint*
  - *Data privacy*
    - *User authentication on the device*
    - *Hard drive caching*

How to install a printer in Windows - USB

- Best practice based on many years of experience
- Plug the printer into the computer
- Go to the manufacturer's website and download the latest software application compatible with your operating system
- Run the installation
- The software will automatically detect and install the printer

How to install a printer in Windows – Network/Corporate Environment

- Set a static IP address on the printer and connect it to the network. Why a static IP? If the printer is on DHCP and the address changes, users will have trouble connecting.
- Go to Devices & Printers or Printers & Scanners



Printers & scanners

Add printers & scanners

Refresh

Searching for printers and scanners

Show Wi-Fi Direct printers

The printer that I want isn't listed

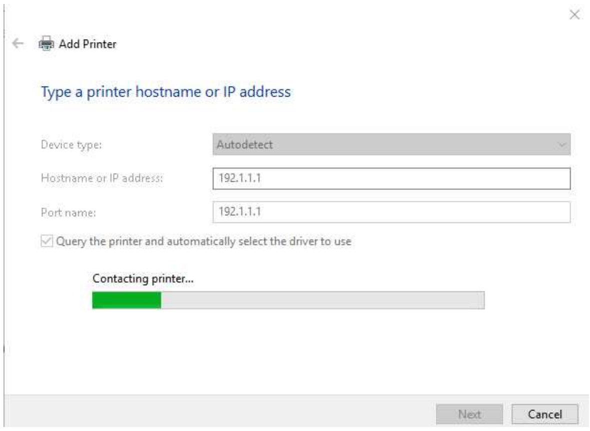
Printers & scanners

Adobe PDF

EPSONFB6F78 (ET-16500 Series)
Not connected

Fax

- Choose to "Add a new Printer"
  - Windows will automatically search for new printers (USB and network)
  - Choose "The printer wasn't listed"
  - Enter the IP address of the printer



Add Printer

Type a printer hostname or IP address

Device type: Autodetect

Hostname or IP address: 192.1.1.1

Port name: 192.1.1.1

☑ Query the printer and automatically select the driver to use

Contacting printer...

- Windows will connect to the printer and automatically select a driver
- In rare cases, Windows won't be able to locate the correct driver
  - Download the correct driver from the manufacturer's website
  - Choose "Have Disk" and select the driver that you downloaded
- Windows will install the driver

- Choose a meaningful name for the printer

How to install a printer in Windows – Network/Corporate Environment (Shared Printer)

- Browse to the hostname of the computer that shares the printer
- Double-click on the printer that you want to share
- Windows will automatically install the printer

Common Printer Settings

Duplex	Printing on both sides of a sheet of paper Saves paper Printer must have a component called a "duplexer" in order to do this A printer without a duplexer might allow you to choose "duplex" from the printer options. It will • print all the odd numbered pages • ask you to flip the sheets over and reinsert them into the printer • print the even numbered pages
Collate	When you print multiple copies of a document, the printer will print all the copies of each page at a time. For example, if you print five copies of a ten-page document, the printer will print five copies of the first page, then five copies of the second page, etc. until the end. With collating, it will print one copy of the document at a time.
Orientation	Portrait or Landscape This is determined in Windows or in the software that created the document
Quality	Can print a document in high quality or low quality Lower quality is faster, uses less toner/ink

Device Sharing

Applies to other devices besides printers

Wired – USB	Printer connects to one PC (main PC) via USB cable Can share with other devices on network, if main PC is powered on
Wired – Serial	Printer connects to one PC via Serial cable Can share with other devices on network, if main PC is powered on
Wired – Ethernet	Printer connects to network Any device on network can connect to the printer and print if it has permission
Wireless – Bluetooth	Any device in range and with Bluetooth capability can connect directly to the printer and print
Wireless – 802.11	Printer connects to network wirelessly Any device on network can connect to the printer and print if it has permission
Infrastructure vs ad hoc	An infrastructure Wi-Fi connection is a connection between the printer and the Wi-Fi network. Other devices connect to the same Wi-Fi network and can access the printer. An ad hoc Wi-Fi network connection is a Wi-Fi connection between the printer and the computer. During connection, the printer and the computer won't be connected to other

	devices. The ad hoc connection is temporary and only for the purpose of printing.
Integrated Printer Server	A print server accepts print jobs and queues them. An integrated print server is one that is part of the printer. Why do we need a print server? • A printer may receive print jobs faster than it can print them • A printer may receive print jobs but be low on necessary supplies (ink, toner, paper, staples, etc.) The printer won't be able to print until supplies are restocked. • For security reasons, a user may want to print a document to a shared printer, but not actually have it print until he or she is next to the printer. The server keeps the document secure until the user is physically present to receive it.
Cloud Printing/Remote Printing	Google Cloud Print is an example The Google Cloud Print app is installed on a computer with a USB or network connection to the printer. Other users (including remote users) connect to the Google Cloud Print app. The app transfers the document to the computer that is connected to the printer. The computer automatically prints the document. Google cloud print allows you to print documents remotely

TCP/Bonjour/AirPrint	Bonjour is a service that allows Apple resources to find each other on the network. Resources include iTunes, and printers. AirPrint allows an Apple device to wirelessly connect to an AirPrint-enabled printer or to a non-AirPrint-enabled printer that is connected to a Windows or Mac OS computer.

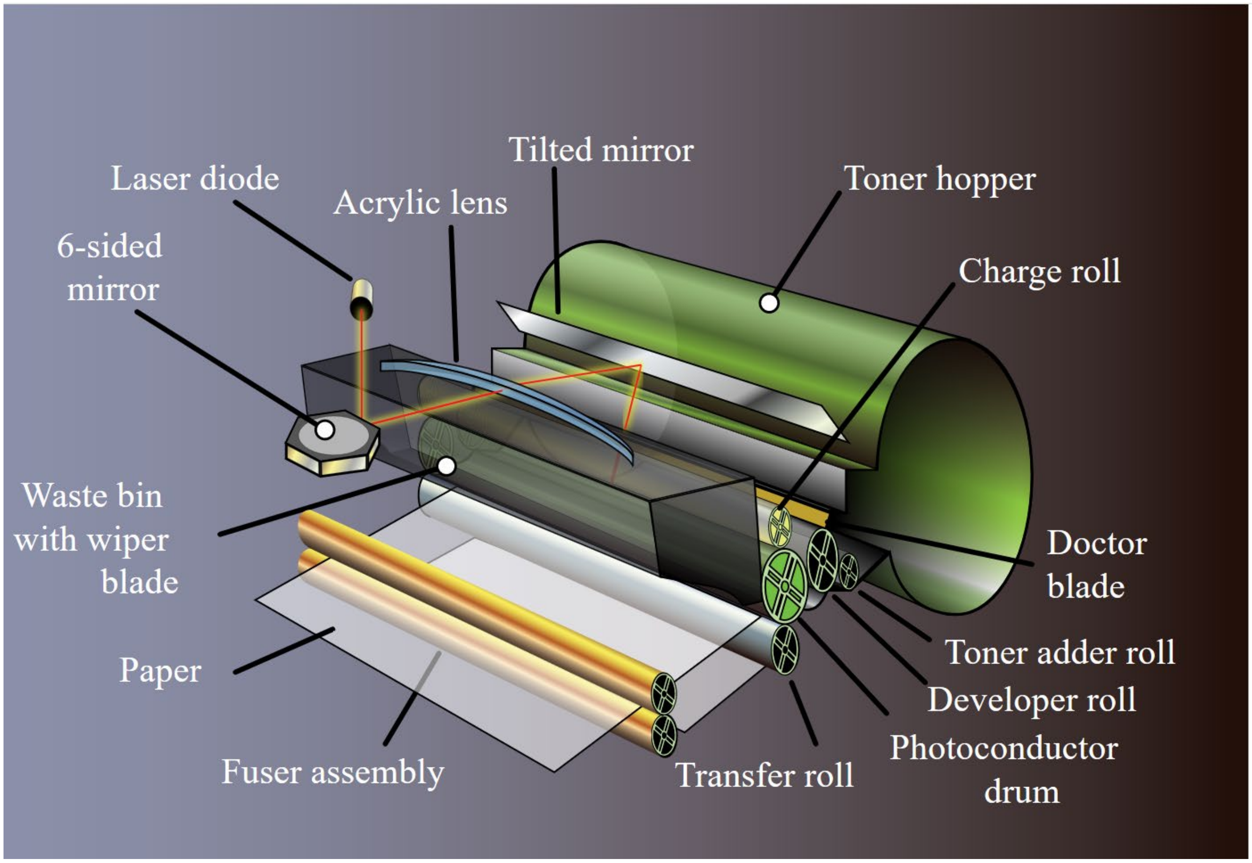
Printer Security

- Best practice for securing a printer
  - Make sure that you install firmware updates when they become available
  - Protect the printer configuration page from unauthorized access
  - Lock printer configuration settings from unauthorized users (change the default password)
  - Disable remote printing
  - Encrypt the printer hard disk. The hard disk will contain copies of printed documents. If the printer is stolen, and the drive is encrypted, nobody will be able to access the contents.
  - Connect to the printer via https instead of http. Use a print driver that supports encryption.
  - Replace old printers that use outdated technology.
- Use private printing
  - Private printing sends the job to the printer, but doesn't automatically print it
  - The printer will "release" (print) the job only when the user arrives at the printer and logs in. Authentication can be
    - Username/password (can authenticate via LDAP or Active Directory)
    - PIN
    - Access card/proximity card
- For highly sensitive printers
  - Connect the printer only via USB and don't share it

3.11 Given a scenario, install and maintain various print technologies.

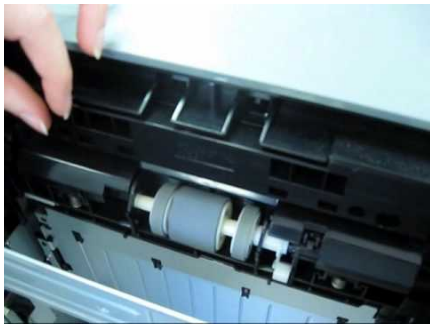
- *Laser*
  - *Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separate pads, duplexing assembly*
  - *Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning*
  - *Maintenance: Replace toner, apply maintenance kit, calibrate, clean*
- *Inkjet*
  - *Ink cartridge, print head, roller, feeder, duplexing assembly, carriage, and belt*
  - *Calibrate*
  - *Maintenance: Clean heads, replace cartridges, calibrate, clear jams*
- *Thermal*
  - *Feed assembly, heating element*
  - *Special thermal paper*
  - *Maintenance: Replace paper, clean heating element, remove debris*
- *Impact*
  - *Print head, ribbon, tractor feed*
  - *Impact paper*
  - *Maintenance: Replace ribbon, replace print head, replace paper*
- *Virtual*
  - *Print to file*
  - *Print to PDF*
  - *Print to XPS*
  - *Print to image*
- *3D printers*
  - *Plastic filament*

Laser Printer



Laser printer components/process

High Voltage Power Supply	Generates a high voltage which applies a negative charge to the imaging drum Maintenance: not required
Imaging Drum/Photoconductor Drum	A laser strikes the drum and neutralizes areas where toner should stick Toner sticks to the drum in the areas that were neutralized by the laser Maintenance: replace every 200,000 pages

Developer Roll	The developer roll is coated in toner, which is received from the toner cartridge. The developer roll applies toner to the imaging drum. The toner doctor blade applies toner to the developer roll. Maintenance: replace every 200,000 pages
Paper Tray	Holds Paper Maintenance: not required
Pickup Roller 	While the drum is being charged, paper is pulled up into the printer The pickup roller sits on top of the paper tray and picks up paper that is in the tray Maintenance: replace every 200,000 pages
Separation Pad	Sits at the front of the paper tray Separates the paper so that only one sheet of paper can exit at a time Maintenance: replace every 200,000 pages
Toner Cartridge	Holds toner Maintenance: replace when empty

Transfer Roller	Positions the paper against the imaging drum, forcing the toner sticks to the paper At this point in the process, it is easy for the toner to fall off the paper Maintenance: replace every 200,000 pages
Fuser Assembly	The toner-covered paper travels to the fuser The fuser uses high heat to bind the toner to the paper Maintenance: replace every 200,000 pages; belts in the toner wear out
Cleaning Blade	Cleans excess toner off the imaging drum, which is deposited into a waste toner container (not all printers have a waste toner container) Maintenance: not required
Duplexing Assembly	Flips sheets of paper over so that the printer can print on both sides.

A color laser printer works the same as a black and white laser printer. The difference is that there are four toner cartridges (black, yellow, cyan, and magenta). There is a separate system for each color. One color is applied to a page at a time. Therefore, the laser print process is repeated four times in a color laser printer. Each of the four systems must align perfectly, or colors on the printed page won't line up.

Maintenance procedure

- Replace the toner cartridge when empty
- Empty or replace the waste toner bottle (if the printer is equipped with one)

- Clean the inside of the printer when dirty (use a dry cloth)
- Print a configuration page. The page will list the most recent errors.
    - Look up the errors in the maintenance manual to determine what other actions to take.
- Print a cleaning page. The cleaning page will clean the inside of the printer.
- Replace the
    - Fuser
    - Separation Pad
    - Pick Up Roller
    - Transfer Roller
    - Imaging drum, if necessary
    - Developer unit, if necessary
    - Other components as determined by the manufacturer
- Typically, the fuser, separation pad, pick up rollers, and transfer roller are sold together as part of a maintenance kit. They all tend to wear out at the same time. The printer will keep track of the number of pages printed, and when it reaches a certain level, it will register a "maintenance" error. Maintenance is typically required after 200,000 pages, but this varies between printer makes and models.
- Check the maintenance manual for instructions on how to replace each component.
    - It is difficult to change parts in older printers. Many steps are required, and many components must be removed.
    - It is easy to replace parts in newer printers. Many parts are held in by plastic tabs; no tools are required.

Common Issues

Paper Jam	The wrong paper is used The correct paper is used but the printer rollers are worn out (or the fuser is worn out) and need to be replaced
Print is faded	Not enough toner is reaching the page Could be an issue with

	- High voltage power supply - Transfer roller
Dirty Print	Clean the printer
Repeating defects on print	Damage on one of the rollers Measure the distance between the defects Compare the distance to the circumference of the rollers to determine which roller is damaged

Inkjet Printer

Ink Cartridge	Holds ink A printer may have one or more ink cartridges
Print Head	Holds the print cartridges The print head transfers ink from the cartridge to the paper Print heads wear out and become clogged with ink They must be cleaned when plugged and replaced when worn out
Roller	Ejects paper from the printer
Feeder	Feeds paper into the printer
Duplexing Assembly	Flips the paper over so that the printer can print on the other side Rare on inkjet printers
Belt	The belt moves the print head from side to side so that it can cover the entire sheet

Inkjet Maintenance

- It is necessary to calibrate the printer. Calibration forces the print head to line up with the edge of the paper correctly.
- Clean the print head regularly
- Replace the print head when it is worn
- Replace the ink cartridges when they are empty

Thermal Printer

Sensor	Detects the position of the paper/media
Feed Assembly	Feeds the paper into the heating element
Heating Element	The heating element heats the paper, creating images and text

Thermal Printer Maintenance

- A thermal printer will print on special thermal paper or thermal labels
- The printer can automatically detect the end of the label (where one label starts and another label ends)
    - It might require automatic or manual calibration
- Clean the heating element regularly

Impact Printer

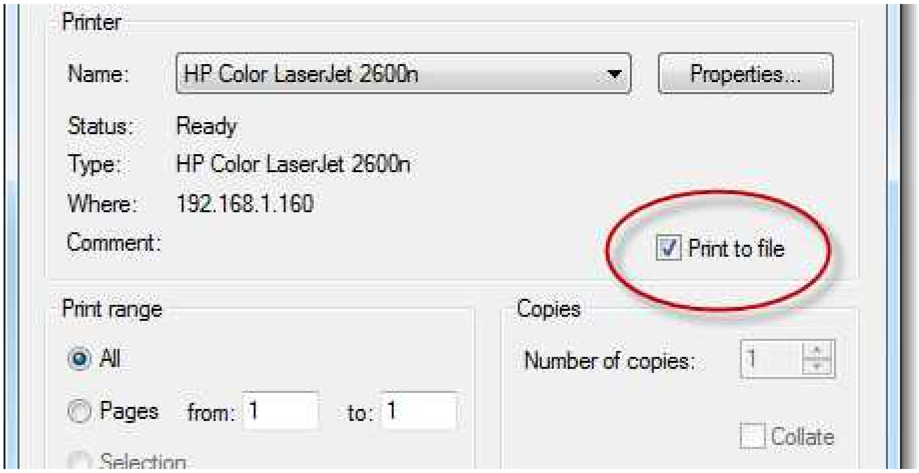
Print Head	Contains a bank of hammers The hammers strike the ribbon against the paper to create an image The paper is pulled through the printer line-by-line
Ribbon	Ribbon passes between the paper and the print head

Impact Printer Maintenance

- Replace the ribbon
- Clean the print head
- Replace the print head (consult the manual)

Virtual Printing

- When you print from a program, you are converting the document into a format that the printer can read.
- Instead of printing to a printer, you can print virtually
  - The most common file print is "PDF". Adobe Acrobat is a program that generates PDFs. When Acrobat is installed, it creates a PDF printer driver. You select "PDF" from the printer options. Data for the document to be printed goes to Adobe Acrobat, which generates a PDF document.
  - Printing to an XPS file. An XPS file is like a PDF. It is written in a language called XML Paper Specification.
  - Printing to an image. Printing to an image converts a document to an image. Text inside an image file can't be edited.
  - Printing to a file. Choose this option to print the document to a file. The instructions that are normally sent to the printer are saved in a file instead. You can reuse those instructions later to reprint the document without having to go through the original program. This is useful when the program takes a long time to generate the print.



Printer

Name: HP Color LaserJet 2600n

Status: Ready

Type: HP Color LaserJet 2600n

Where: 192.168.1.160

Comment:

☑ Print to file

Print range

● All

○ Pages from: 1 to: 1

○ Selection

Copies

Number of copies: 1

□ Collate

3D Printing

- A 3D printer will build a 3D object one layer at a time
- It will deposit a layer of plastic and continue to build on top of it until all the layers are complete
- There are several methods of printing in 3D and a wide variety of raw materials available, each with its own properties

Part E 220-1001 4.0 Virtualization and Cloud Computing

4.1 Compare and contrast cloud computing concepts.

- *Common cloud models*
  - *IaaS*
  - *SaaS*
  - *PaaS*
  - *Public vs. private vs. hybrid vs. community*
- *Shared resources*
  - *Internal vs. external*
- *Rapid elasticity*
- *On-demand*
- *Resource pooling*
- *Measured service*
- *Metered*
- *Off-site email applications*
- *Cloud file storage services*
  - *Synchronization apps*
- *Virtual application streaming/cloud-based applications*
  - *Applications for cell phones/tablets*
  - *Applications for laptops/desktops*
- *Virtual desktop*
  - *Virtual NIC*

Cloud Models Include

IaaS	Infrastructure as a Service Rent physical infrastructure on a monthly or hourly basis No upfront costs or hardware maintenance costs No cost for internet, power, heating, cooling, etc. Customer will see each system hardware component and is responsible for configuring them. Examples include Amazon Web Services and Microsoft Azure
SaaS	Software as a Service Software is licensed on a per hour or per month basis. The software is centrally hosted. The customer does not manage software, hardware, or licenses. Examples include Salesforce
PaaS	Platform as a Service Service between IaaS and SaaS A "platform" is licensed per hour or per month. Customer does not manage hardware directly but can run any application they want.

	Advantage is ability to run applications without having to build the underlying infrastructure.
Public Cloud	A public cloud is available to the general public. The resources inside a public cloud are shared amongst all customers, which improves efficiency and reduces cost. Multiple customers may run on the same physical server without realizing it (cloud software is supposed to prevent data leaks between customers)
Private Cloud	A private cloud is built by one organization for its internal use. A large organization can use a private cloud to share resources amongst different departments.
Hybrid Cloud	A mix of a private cloud and a public cloud. A company may decide that some applications are too sensitive to host with a public cloud, or that some applications will not run properly when they are off site, but would like to take advantage of the public cloud. Applications that can run on the public cloud are placed there, and remaining applications are placed on a private cloud. The private cloud and public cloud are connected via a WAN or VPN.

Community Cloud	Like a private cloud except that infrastructure is shared by several organizations. Several organizations pool their computing resources.

Cloud Benefits

There are five essential characteristics of a cloud computing service

- On-demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Shared Resources	Allow multiple users to share computer resources, including • File storage • Databases • Processing • Network connectivity
Rapid Elasticity	Ability to instantly add or remove capacity. A resource can scale on demand. Scaling can happen automatically (via a script that detects an overload) or manually
On-Demand	A user can obtain cloud services "on demand" from a control panel
Resource Pooling	Resources are shared across multiple customers. When a resource is released by one customer, it can be provided to another
Measured Services	The cloud provider can measure the amount of services used by a customer. A user is billed for resources he or she consumes.

Metered	A cloud provider can meter or limit the amount of resources a user can use. Important because a user could request too many resources at once, which could impact other customers.

Off-Site E-mail Applications

There are three main cloud e-mail services

G Suite	Provided by Google Billed on a per-user per-month license Includes the following services • E-mail (Gmail) • File Sharing (Google Drive) • Calendar (Google Calendar) • Hangouts (Chat and Collaboration) E-mail can be accessed via a web app or via an e-mail client, such as Outlook
Exchange	Provided by Microsoft Billed on a per-user per-month license E-mail can be accessed via a web app or via an e-mail client, such as Outlook
Office 365	Provided by Microsoft Billed on a per-user per-month license Includes all the features of Exchange plus each user can install Office 365 on up to five devices Includes • Office 365 includes Excel, Word, Outlook, PowerPoint, Access, and Skype • Skype allows users to communicate via messaging, voice, and video • Store files in the cloud with OneDrive • SharePoint allows a company to create internal websites Additional features • eDiscovery

	• Integration with active directory • Data Leak Prevention • Message encryption

Cloud Storage

There are five main cloud storage services

Google Drive	Provided by Google Free for personal use Pay for business use on a per-user per month basis (integrates with Google Apps) Files are available through a web interface Can share files and folders with internal and external users
One Drive	Provided by Microsoft Free for personal use Pay for business use on a per-user per month basis (integrated with Office 365) Files are available through a web interface, and also through a downloadable app Allows you to sync files between your computer and the cloud Can share files and folders with internal and external users
SharePoint	Provided by Microsoft Pay per-user per-month Available with an Office 365 business license Allows you to create internal corporate websites, accessible through a web interface Can share files and folders with internal and external users
Amazon WorkDocs	Provided by Amazon Web Services Pay per-user per-month

	Files are available through a web interface, and also through a downloadable app Allows you to sync files between your computer and the cloud Can share files and folders with internal and external users
Dropbox / Box	Cloud apps that provide file sharing Free for personal use Pay for business use Can share files and folders with internal and external users

Virtual Application Streaming/Cloud-Based Applications/Virtual Desktops

Citrix	Creates a system called "application virtualization" Allows a user to run an app regardless of the type of computer system he is using How? • The app runs on a Citrix server • The user runs a "plug in" on his computer that connects to the server • The server streams the application through the plugin to the user over the internet Advantages • Application will operate on any type of computer • Application data is stored centrally on Citrix server and can be backed up Disadvantages • Requires internet to function • Licensing costs associated with Citrix
Amazon WorkSpaces	Cloud Desktop Service User "desktops", files, applications, and computing resources are stored in the Amazon cloud A user can install the client on their Windows, iOS, Apple, or Android device and connect to their desktop The desktop is in the cloud, so a user can connect to it from multiple locations, and begin working where they left off It is easily backed up

	Integrates with Active Directory and other authentication protocols WorkSpaces allows a customer to scale a desktop to hundreds or thousands of users instantly Customer is billed for each WorkSpace in use on an hourly basis; customer is only billed for WorkSpaces when they are actually in use
Remote Desktop Services	A central server stores user desktops, applications, and settings Server can be hosted in the cloud or on location, but must stay operating A user can connect to the server via a Remote Desktop Protocol from any Windows device Requires a per-user license (CAL) to access the server
Virtual NIC/SDN	Software Defined Networking Allows multiple virtual machines to communicate with each other as if they are separate physical machines on a network The networking elements are handled by a computer server instead of by dedicated network equipment (switches and routers)

4.2 Given a scenario, set up and configure client-side virtualization.

- *Purpose of virtual machines*
- *Resource requirements*
- *Emulator requirements*
- *Security requirements*
- *Network requirements*
- *Hypervisor*

Why do we need virtual machines?

There are several benefits

- Run multiple operating systems on the same physical server at the same time. For example, we can run Windows and Unix on the same physical server at the same time.
- Run multiple virtual servers on the same physical server at the same time. We install a program called a hypervisor. The hypervisor is the base operating system. We use the hypervisor to create virtual servers. We install an operating system on each virtual server. The hypervisor allows the virtual servers share the same physical resources. The virtual servers can't talk to each other, except through a software defined network.
- Reduce resource consumption. Consider an example where our organization requires a file server, an e-mail server, and a web server. If we purchase a separate physical server for each function, we would require three servers, even if each service does not utilize its server to its maximum capacity. We could do the following instead:
    - Obtain one physical server
    - Create three virtual servers on the physical server
    - Install a file server function on one virtual server, an e-mail server on the second, and a web server on the third
    - The server would operate at a higher capacity, and would therefore be more efficient
- Desktop virtualization. Desktop virtualization allows users to connect to the machine via a remote desktop protocol. It reduces the total amount of computing resources because a single server can host many user desktops at the same time. It also centralizes the location of user data, allowing easy back ups.

How much resources are required?

When you set up a hypervisor, you must select the necessary amount of resources for each virtual machine, including RAM, processing speed, and hard drive space.

The virtual resources allocated to a virtual machine can be different from the actual physical resources on the underlying hardware. The hypervisor tricks the virtual machine into believing that the resources are there. The total amount of resources allocated to all the virtual machines on a physical server can be greater than the total amount of resources that exist on the physical server.

Not every server needs all its resources all the time. But every server needs some resources. If too many virtual servers are created, performance could suffer.

Emulator vs Hypervisor?

A hypervisor works with the CPU's virtualization technology. It is a bare metal approach in that it runs directly on the server as the base operating systems. All virtual machine operating systems run on top of the hypervisor.

An emulator is a software program that mimics the specific hardware properties. It does not rely on the CPU. It runs as a guest inside a host operating system. The emulator tricks the guest operating system into thinking that the computer has a specific combination of compatible hardware.

Security?

Hypervisor software is robust and secure, but there are always bugs and software flaws that could be discovered later. The biggest concern is that data could leak from one virtual server to another (either through the RAM, processor, or hard disk drive).

It is important to

- Apply software updates when they become available
- Keep the server physically secure
- Secure the management interface for the hypervisor
- Disable unnecessary services
- Avoid running sensitive applications on shared servers

Network Requirements?

Each virtual machine will have one or more virtual network interfaces, each with a virtual MAC address. The network interfaces will be established through software defined network. The hardware ethernet port(s) on the server will connect to the network and must be shared by the virtual servers. It is possible to create a virtual (software-defined) network that connects the virtual machines and route traffic to the physical network. The hardware ethernet port(s) therefore act as a switch, where the virtual servers are considered connected devices.

Part F 220-1001 5.0 Hardware and Network Troubleshooting

5.1 Given a scenario, use the best practice methodology to resolve problems.

- *Always consider corporate policies, procedures, and impacts before implementing changes*

1. *Identify the problem*
    a. *Question the user and identify user changes to computer and perform backups before making changes*
    b. *Inquire regarding environmental or infrastructure changes*
    c. *Review system and application logs*
2. *Establish a theory of probable cause (question the obvious)*
    a. *If necessary, conduct external or internal research based on symptoms*
3. *Test the theory to determine cause*
    a. *Once the theory is confirmed, determine the next steps to resolve problem*
    b. *If theory is not confirmed re-establish new theory or escalate*
4. *Establish a plan of action to resolve the problem and implement the solution*
5. *Verify full system functionality and, if applicable, implement preventive measures*
6. *Document findings, actions, and outcomes*

Problem Solving Process

We should always follow the policy of the customer or the employer before doing anything. Always follow policy unless it is illegal or immoral.

If you don’t agree with the policy, you have the option to bring it up with management. You should remember that policies are created by people with experience. You must respect their decisions and their judgement.

Step 1: Ask what is the problem?

Ask the user if they made any changes. Users will forget. Users will lie. Users will assume that some changes they made didn't cause the problem and neglect to mention them. Remember that most users are not computer experts.

Check if there have been environmental/infrastructure changes.

- For example, a site wide network upgrade, or a roll out of a software update that has created undesired effects. In larger organizations, networks, storage, servers, and other infrastructure may be managed by separate teams, who don't necessarily communicate with each other when they should.
- Check the system logs, event viewer, etc. on the user's computers

Step 2: Come up with a theory for what caused the issue and perform some research if necessary

Many good sources of information include

- Online sites such as Stack Overflow, Spiceworks, Experts Exchange
- Other professionals
- Manufacturers

Step 3: Test the theory

- Determine if the theory is the cause of the problem
- Determine the steps required to solve the problem
- If the theory is not the correct cause of the problem, find a new theory

Step 4: Take Action

- Execute the plan to resolve the problem
- Step 4 and Step 5 can be combined

Step 5: Verify Functionality

- Confirm that the system is operational
- Confirm that the measures you took to correct the problem did not create additional problems
- Preventative measures
    - Educate the user about the cause of the problem
    - Educate other users and teams so that they understand the cause of the problem and the solutions. This will help them take corrective action in the future.
    - Make corrective actions/settings permanent
    - Add restrictions or warning signs to the systems

Step 6: Document Findings

- Important to document the findings so that others can learn
- Good to share knowledge with co-workers and with the community
- If you discover a security flaw, you should share it to prevent others from being harmed

5.2 Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power

- *Common symptoms*
  - *Unexpected shutdowns*
  - *System lockups*
  - *POST code beeps*
  - *Blank screen on bootup*
  - *BIOS time and setting resets*
  - *Attempts to boot to incorrect device*
  - *Continuous reboots*
  - *No power*
  - *Overheating*
  - *Loud noise*
  - *Intermittent device failure*
  - *Fans spin – no power to other devices*
  - *Indicator lights*
  - *Smoke*
  - *Burning smell*
  - *Proprietary crash screens (BSOD/pin wheel)*
  - *Distended capacitors*
  - *Log entries and error messages*

Problems, Causes, & Solutions

Problem	Possible Causes	Possible Solutions
Unexpected Shutdown	Computer Overheating	Check to make sure that the fans are operating and are not obstructed. Clean the computer and replace the fans if necessary. Check to make sure that there is enough ventilation for the computer. Move the computer to a location with better ventilation. Check to make sure that there is adequate thermal paste between the processor and the heat sink. Check to make sure that the processor is not overclocked. Install a liquid cooling system or additional fans.
	Hardware Error	Check the error log to determine if a piece of hardware is failing. Replace the failing hardware.
	Software Error	Boot the computer to BIOS and leave it there. If it does not shut down, then the issue may be software related.

		Review the error log for errors or perform a clean install of the operating system.
System Lockup (Hang)	Hardware error	The hardware is damaged or mismatched. Check to make sure that the hardware is compatible and that updated drivers have been installed. Check the error log for details.
	Issue with application	The application that you are running may have a bug. Check for updates to the application. Check with other users to see if they are experiencing the same issue. Check online or with the manufacturer to see if there are solutions to the error.
	System is slow	Too many applications are open at the same time. It is possible that the computer is slow, and only appears to be hanging. Check the quantity of computer resources being utilized. Wait a few minutes to see if the computer improves.

		Look at the hard drive activity light. If it is flashing, then the computer is operating.
POST Code Beep	Hardware failure	POST = Power On Self Test When the computer powers on, it will check all the hardware for errors. If it detects an error, it will produce a series of beeps. The number of beeps corresponds to the type of error. Check with the manufacturer to see what error corresponds to the beep sequence and correct it.
Blank Screen on Bootup	Hardware failure (graphics)	If the computer has onboard graphics and dedicated graphics, move the display cable to a different graphics port or to a different graphics card. Reseat the graphics card in the motherboard or replace the graphics card.
	Display issue	Check to make sure that the display is functioning. Try the display with a functioning video source.

		Check to see if the display is on the correct input. Check that the display is connected correctly.
	Software issue	If the display is blank even during the BIOS POST, then the issue is likely with the display or the graphics card/motherboard If the display is blank after the BIOS loads, it is likely an issue with the operating system. Attempt to boot into safe mode, disable unnecessary devices, and reinstall the graphics drivers.
BIOS time/Setting Reset	CMOS Battery	The CMOS battery is dead. It is not storing data when the computer is powered off. Replace the CMOS battery.
	Defective BIOS	The BIOS firmware is corrupted. Update the BIOS firmware. The BIOS is defective. Replace the system board.
Boot to Incorrect Device	Boot Order Not Set	Set the boot order correctly. Check to see if the boot options allow for legacy or UEFI

		boot mode. Adjust the options appropriately.
	No boot device found	The device that you are trying to boot to does not contain a recognizable operating system. Repair or reformat the boot device. Check if the BIOS boot mode is set correctly (legacy or UEFI). Change it to the correct setting.
Continuous Reboots	Software Issue	A software issue is causing the system to reboot. If an important service stops working, it can force the system to reboot. Change service setting to not reboot upon termination, then correct the issue causing the service to fail. Check the error log to see if another issue is causing the reboot and correct the issue. Reinstall operating system.
No Power	No power from outlet	Check the power outlet to make sure that it is providing adequate power.

		Check that the power cord is plugged in securely. Check the power switch on the PSU to ensure that it is in the on position.
	Failing PSU	Check the power supply to make sure that it has not failed. Replace the power supply if necessary.
	Motherboard	Check that the power supply is securely connected to the motherboard. The motherboard may be defective and needs to be replaced. Check that the power buttons on the case are not broken. Check that the cable between the power button and the motherboard is secure.
Overheating	Not enough cooling	Check to make sure that the fans are operating and are not obstructed. Clean the computer and replace the fans if necessary.

		Check to make sure that there is enough ventilation for the computer. Move the computer to a location with adequate ventilation. Check to make sure that there is adequate thermal paste between the processor and the heat sink.
Loud Noise	Damage to fan or obstructions in the fan	Replace the fan or clean the fan
	Fan is operating at maximum capacity	Computer is overheating, causing the fan to operate at full speed. Correct the overheating issue. Temperature sensor is providing inaccurate temperature information. Adjust or replace the temperature sensor.
Intermittent Device Failure	Device is failing	Replace the device. If the device is a hard disk drive, back up the data immediately.
Fans Spin, no power	Damage to System board	Check the system board to ensure that it is receiving an adequate power supply. Replace the system board.

	Damage to PSU	Replace the PSU
Indicator Lights		Check with the manufacturer to see what the indicator lights mean and take appropriate action.
Smoke	Short circuit	Turn off the computer to avoid further damage Check the source of the smoke. Look for burn marks. A short circuit in the system board could cause system components to burn. Check that all cables and connections are secure. Replace burned components. Do not operate a computer that is producing smoke.
Burning Smell	Short circuit	Turn off the computer to avoid further damage Check the source of the smoke. Look for burn marks. A short circuit in the system board could cause system components to burn. Check that all cables and connections are secure. Do not operate a computer that is producing a burning smell.

BSOD/Pin Wheel	Hardware failure	Can ignore unless it becomes a recurring problem Check error log to see if it is caused by a hardware issue. Replace the hardware.
Distended Capacitators	SXS Rubycon CE 105°C 400v 150 SXS Rubycon CE 105°C	A bad capacitator will have a bulge at the top and/or will leak electrolyte. Replace the capacitator or replace the system board that it is on.
Log Entries/Error Messages	Numerous causes	Read the log to determine the error message and take corrective action.

5.3 Given a scenario, troubleshoot hard drives and RAID arrays.

- *Common symptoms*
    - *Read/write failure*
    - *Slow performance*
    - *Loud clicking noise*
    - *Failure to boot*
    - *Drive not recognized*
    - *OS not found*
    - *RAID not found*
    - *RAID stops working*
    - *Proprietary crash screens (BSOD/pin wheel)*
    - *S.M.A.R.T. errors*

Hard Drive Issues

When diagnosing a hard drive issue

- Determine whether you have a magnetic drive or a solid-state drive. They function differently.
- Back up your data. Most hard drive issues are physical in nature and can't be corrected. The easiest solution is to replace the drive. As the condition of the drive deteriorates, data recovery becomes less and less likely.

Read/Write Failure	Can be caused by a software bug, especially if multiple users/hard disk drives are affected. Can be caused by damage to the hard disk drive.
Slow Performance	Disk is fragmented. Run disk defragmenter. Disk is functioning well, but computer is slow. Computer may require more memory or a faster processor. Replace the SATA cable.
Loud Clicking Noise	Mechanical problem with the hard disk drive
Failure to Boot	Check the boot order in the BIOS, and make sure that the HDD is set to boot Make sure that the HDD is connected correctly Run check disk utility to correct any data errors Operating system is corrupted. Reinstall the operating system

Drive Not Recognized	A drive with the wrong file system is connected (for example HFS+ drive connected to a Windows computer) Check to see that the SATA cable is connected securely Check to see that the power cable is connected properly, and that the PSU is outputting adequate power Check that the drive is enabled in the BIOS Check that you have installed the correct drivers for the HDD
OS Not Found	Check that you are booting in the correct mode (legacy or UFEI). Check if there are errors with the operating system. Insert a bootable operating system DVD/USB and attempt to correct errors
BSOD/Pin Wheel	Check the cause of the error and act as appropriate
SMART Error	SMART = Self-Monitoring, Analysis, and Reporting Technology SMART monitors the drive for errors and predicts hardware failures. SMART warns you prior to the failure of the HDD

	When seeing a SMART warning, back up data and replace the HDD

RAID Issues

RAID Not Found	The BIOS might be ignoring the RAID controller. Check the BIOS to see if RAID is enabled, or if the computer is set to boot from AHCI. If the problem is with the RAID itself • Too many RAID disks have failed, rendering the entire array defective • The RAID volume itself was deleted • The RAID controller is defective Log in to the RAID controller (normally it's possible to access the RAID controller through an option such as CTRL+J, which is accessible when the computer is booting). If you can't reach the RAID controller, it may have failed. • Try reseating the RAID controller. Replace the controller if appears to be failing. • If it's an integrated controller, the system board may have to be replaced. Log in to the controller to see if the virtual disks are present. If the virtual disk configuration is lost, but the physical disks are still functional, you can try to have the controller "detect" the original configuration. Check inside the controller to see if the disks are functional. The disks may not be seated correctly.
RAID Stops Working	One or more disks have failed

	Typically, an enterprise disk will show an error light on the front (a red or amber light) indicating that it has failed. If you're using RAID 5, or another redundant RAID version, the failure of a single disk won't cause data loss. But you must replace the disk. The failure of an additional disk could result in complete data loss.

5.4 Given a scenario, troubleshoot video, projector, and display issues.

- *Common symptoms*
  - *VGA mode*
  - *No image on screen*
  - *Overheat shutdown*
  - *Dead pixels*
  - *Artifacts*
  - *Incorrect color patterns*
  - *Dim image*
  - *Flickering image*
  - *Distorted image*
  - *Distorted geometry*
  - *Burn-in*
  - *Oversized images and icons*

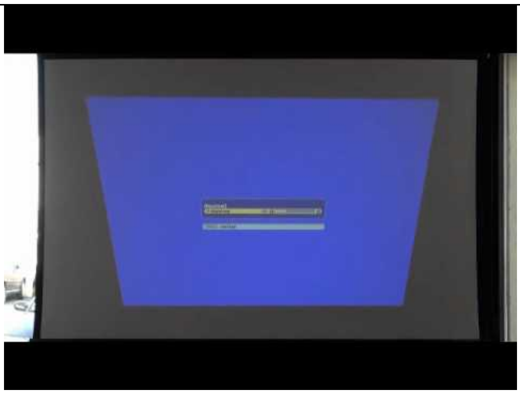
Troubleshoot Display/Projector

VGA Mode	Check that the video cable is connected to the projector correctly. Check that the projector/display is set to the correct input. Check that the video cable is connected to the video source correctly. Check that the video source is powered on, and that it is set to output to an external display. Replace the cable if necessary. Some video cables only work in one direction. Make sure that the cable is connected in the correct direction.
No Image	Check that the video cable is connected to the projector correctly. Check that the projector/display is set to the correct input. Check that the video cable is connected to the video source correctly. Check that the video source is powered on, and that it is set to output to an external display.

	Some cables only work in one direction. Make sure that the cable is connected in the correct direction.
Overheat Shutdown	Projector is overheating. Check that the fans and air vents on the projector/display are not obstructed and clean them if necessary. Move the projector/display to an area with adequate ventilation. If the fans are not functioning, they must be replaced.
Dead Pixel	The display is damaged and should be replaced. The projector is damaged and should be replaced. The light processing chip (DLP) may be replaced.
Artifact	Determine if the artifact is caused by the display or by the video source. Replace the display and video cable first. If the artifact remains, then the issue is with the video source. • Reboot the video source • Adjust the settings on the video source • Replace the graphics card/system board

	If the artifact disappears, then the issue is with the display. • Perform a factory reset on the display • Replace the display.
Incorrect Color Pattern	Determine if the pattern is caused by the display or by the video source. Replace the display and video cable first. If the color pattern remains, then the issue is with the video source. • Reboot the video source • Adjust the settings on the video source • Replace the graphics card/system board If the color pattern disappears, then the issue is with the display. • Perform a factory reset on the display • Replace the display.
Dim Image	Increase the brightness of the display. If you're unable to increase the brightness, the backlight may have burned out and should be replaced.
Flickering Image	Determine if the issue is caused by the display or by the video source. Replace the display and video cable first. If the flickering remains, then the issue is with the video source. • Reboot the video source

	• Adjust the settings on the video source • Replace the graphics card/system board If the flickering disappears, then the issue is with the display. • Perform a factory reset on the display • Check the refresh rate on the display • Replace the display.
Distorted Image	Determine if the distorted image is caused by the display or by the video source. Replace the display and video cable first. If the distorted image remains, then the issue is with the video source. • Reboot the video source • Adjust the settings on the video source • Replace the graphics card/system board If the distorted image disappears, then the issue is with the display. • Perform a factory reset on the display • Check the refresh rate on the display • Replace the display.
Distorted Geometry	Typically found on projectors, when the projector is not 100% parallel to the screen. Adjust the projector “keystone”.

	
Burn-In	A burn-in occurs when a fixed image is displayed on the screen for a long period of time. The burn-in will disappear after some time. Try displaying different moving images on the screen. There are apps that can clear the burn-in. If the damage is permanent, then the screen must be replaced.
Oversized Images/Icons	Adjust screen resolution on the video source. Adjust the zoom on the video source and on the display/projector.

5.5 Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.

- *Common symptoms*
    - *No display*
    - *Dim display*
    - *Flickering display*
    - *Sticking keys*
    - *Intermittent wireless*
    - *Battery not charging*
    - *Ghost cursor/pointer drift*
    - *No power*
    - *Num lock indicator lights*
    - *No wireless connectivity*
    - *No Bluetooth connectivity*
    - *Cannot display to external monitor*
    - *Touchscreen non-responsive*
    - *Apps not loading*
    - *Slow performance*
    - *Unable to decrypt email*
    - *Extremely short battery life*
    - *Overheating*
    - *Frozen system*
    - *No sound from speakers*
    - *GPS not functioning*
    - *Swollen battery*
- *Disassembling processes for proper reassembly*
    - *Document and label cable and screw locations*
    - *Organize parts*
    - *Refer to manufacturer resources*
    - *Use appropriate hand tools*

Common Mobile Device Issues

No Display	The battery is dead. Charge the phone. The screen is broken. Replace the screen. The screen connector is loose. Check/reseat the connector between the screen and the system board.
Dim Display	The backlight is damaged (if equipped with a backlight). Replace the screen and/or backlight. The screen dims automatically in response to low-light conditions. Clean and/or replace the light sensor.
Flickering Display	Display is defective. Replace the display. The screen connector is loose. Check the connector between the screen and the system board.
Sticking Keys	The keys are broken. Replace the keyboard. The keys have debris. Clean the keyboard.
Intermittent Wireless	The wireless antenna is damaged. Replace the antenna and/or system board. The phone is in an area with poor wireless signals. Move to an area with better wireless signals.

Battery Not Charging	The battery is defective. Replace the battery. The charging port is defective. Replace the charging port. The cable or power adapter is defective. Replace the cable or power adapter. You're using a power adapter that provides less wattage than what the battery requires. Swap with an adequate power adapter.
Ghost Cursor/Pointer Drift	The touch screen is cracked. Replace the touch screen. The touchpad is damaged. Replace the touch pad.
No Power	The battery is dead. Charge the battery. If the battery won't charge, replace the battery. The phone is defective. Replace the phone or the system board.
Num Lock Indicator Light	Num lock key is stuck. Hold down the num key. Reboot the phone. Clean the keyboard with an alcohol swab and/or compressed air.
No Wi-Fi	The wireless antenna is damaged. Replace the antenna and/or system board.

	The phone is in an area with poor wireless signals. Move to an area with better wireless signals. The phone is set to airplane mode or Wi-Fi is disabled. Enable Wi-Fi from settings.
No Bluetooth	The wireless antenna is damaged. Replace the antenna and/or system board. The phone is too far from the Bluetooth device that you're trying to connect to. Move the phone closer to the Bluetooth device. The Bluetooth device that you're trying to connect to is defective. Replace the device. The phone is set to airplane mode or Bluetooth is disabled. Enable Bluetooth from settings.
Can't display to external monitor	The monitor is not set to the correct input. Set the monitor to the correct input. The connection cable is defective. Replace the cable. The output on the phone is not set correctly. Adjust the settings.
Touchscreen not responsive	The touchscreen is damaged or needs to be calibrated. Calibrate or replace the touchscreen.

Apps Not Loading	The version of the app that you’re using has a bug. Check if other users have the same issue. Uninstall and reinstall the app. The app is not compatible with your phone and/or operating system. Obtain a phone that is compatible with your app, or obtain an app version that is compatible with your phone. The device’s operating is corrupted. Reformat the device.
Slow Performance	The phone is overloaded. Reboot the phone. Uninstall or disable unnecessary applications. Obtain to a more powerful phone.
Unable to decrypt email	The user’s password has changed or his account has been disabled. Check to make sure that the user can log in to his e-mail via another method. Remove the e-mail account and add it back to the phone.
Short Battery Life	The battery is defective and should be replaced. The phone is overloaded, causing it to drain the battery quickly. Reduce the number of open applications.
Overheating	The phone is overloaded. Uninstall unnecessary applications.

	The phone is being kept in an environment where it is prone to overheating. Move to a better environment.
Frozen	The phone is overloaded. Reboot the phone. Uninstall or disable unnecessary applications. Obtain to a more powerful phone.
No sound	The volume is disabled. Unmute the phone. The speakers are damaged. Replace the speakers. The phone is set to output sound to another audio device such as Bluetooth speakers. Switch to the correct audio device.
No GPS	The GPS antenna is damaged. Replace the GPS antenna or the system board. The GPS is not available in the area where the phone is located.
Swollen battery	The battery is defective. Replace the battery.

Disassemble Procedures for a Mobile Device

- If this is the first phone that you have repaired, you'll probably mess it up.
- Ask yourself if the component is held in by screws or by adhesive. Increasingly, phone components are held in with adhesive, which is much more difficult to remove.
    - Consider calling in an expert. In any large city, there are at least 100 cell phone repair shops full of experts who know how to fix phones.
    - If you choose to do it yourself, and it is a sensitive application, consider practising on some donor phones before working on the customer's device.
- Watch a video of the assembly and disassembly procedure.
- Make sure that you have all of the correct components and tools.
- Use a mat or a piece of paper with a grid to mark each screw as you remove it. That way, you'll know exactly where each screw came from.

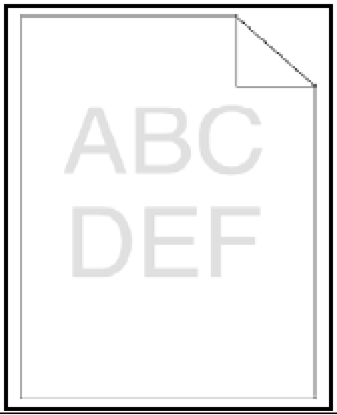
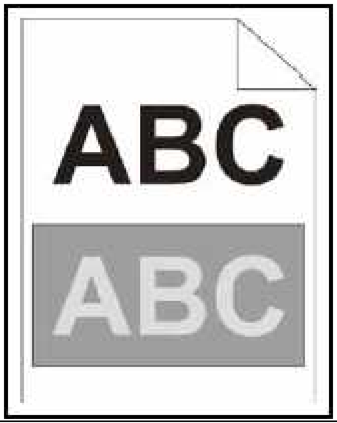
5.6 Given a scenario, troubleshoot printers.

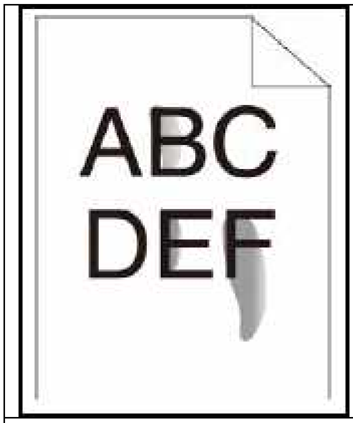
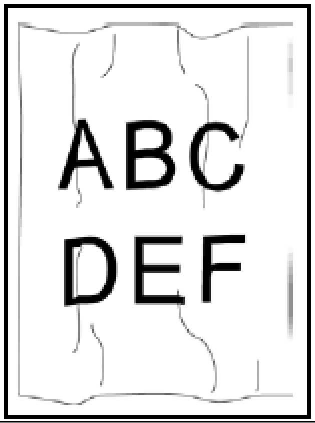
- *Common symptoms*
  - *Streaks*
  - *Faded prints*
  - *Ghost images*
  - *Toner not fused to the paper*
  - *Creased paper*
  - *Paper not feeding*
  - *Paper jam*
  - *No connectivity*
  - *Garbled characters on paper*
  - *Vertical lines on page*
  - *Backed-up print queue*
  - *Low memory errors*
  - *Access denied*
  - *Printer will not print*
  - *Color prints in wrong print color*
  - *Unable to install printer*
  - *Error codes*
  - *Printing blank pages*
  - *No image on printer display*

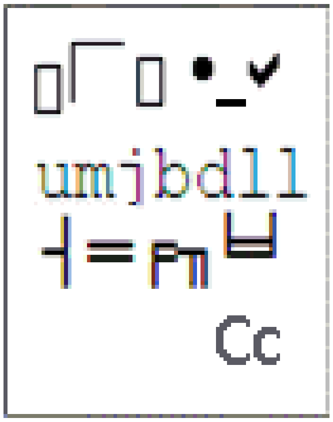
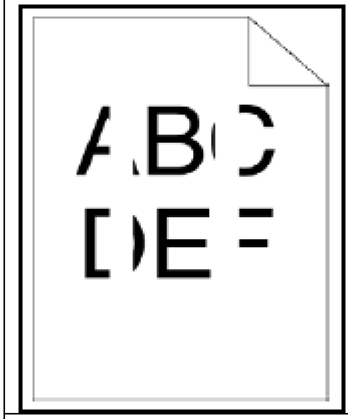
Common Printer Issues

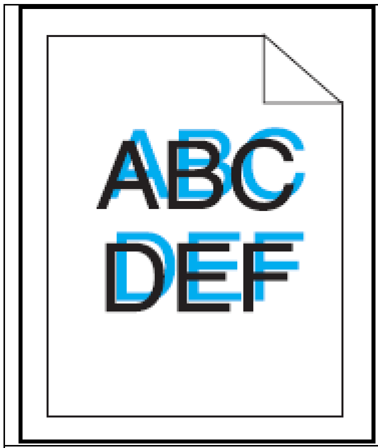
Think about how paper travels through the printer, from the paper tray to the output basket. Then think about the locations in the printer where the print quality could be affected.

Check the manufacturer's maintenance manual for the printer.

Streaks	The print head is dirty or blocked. Clean the printer. Run a cleaning page through the printer.
Faded Prints  	The printer is low on toner. Change the toner cartridge. The printer's High Voltage Power Supply is damaged. Change the power supply. The printer is set to print on "economical" mode. Change the mode.
Ghost Images  	The previous print job is stuck to the imaging drum. The imaging drum has reached the end of its life and should be replaced. The previous print job is stuck to the fuser. The fuser should be replaced.
Toner not Fusing	The fuser is damaged or not hot enough. Adjust the fuser settings or replace the fuser. Check that the fuser is connected correctly.

	If the toner is not fusing, prints appear normal, but the toner can be easily rubbed off.
Creased Paper 	There is a paper jam in the printer or damage to one of the rollers. Replace the rollers.
Paper Not Feeding	The wrong paper is inserted. Insert the correct type of paper. Adjust the paper tray to accommodate the paper size. The pick-up rollers are worn. Replace the rollers.
Paper Jam	Debris in the printer. Clean the printer. The rollers or fuser are worn. Replace the rollers or fuser.

No Connectivity	The printer is not connected to the USB or internet. Check the connection and/or replace the paper. Check the DHCP, Static IP, or Wi-Fi settings.
Garbled Characters  	Determine if the issue is caused by the printer or by the computer. Try printing a configuration page from the menu. If the configuration is good, then the issue is likely with the computer. Update the drivers on the computer. If the configuration is bad, then the issue is likely with the printer. Check if the printer is connected to a good quality power supply and replace the toner cartridge.
Vertical Lines  	Toner is not being deposited on the page. Replace the toner cartridge, imaging drum and developer unit.
Color Registration Out of Alignment	This occurs with printers that have multiple colors. The different colored toner imaging drums/toner cartridges are not aligned. Align and calibrate them.

	
Backed-up Print Queue	The print queue is full of documents, but not enough resources are available. Check that the correct size and type of paper is loaded. Too many users are printing at the same time. Consider installing additional printers.
Low Memory	The printer is low on memory. There are too many documents being printed. Add more memory or consider installing additional printers. Install a print server or additional memory to queue all of the jobs.
Access Denied	The user doesn't have permission to print. This may be controlled by the printer or by the print server. Provide the user with permission.
Won't Print	Uninstall and reinstall the printer. Confirm that the correct driver is installed and that you can connect to the printer.
Color Prints in Wrong Print Color	The wrong colored toner or ink cartridges are installed. This is normally not an issue because

	printers with multiple colors have unique shapes for each cartridge.
Unable to Install Printer	The printer is not accessible. Check that the printer is connected to the correct network. The driver is not compatible with the operating system. Check that the correct driver is installed.
Error Codes	There are hundreds of error codes. Look up the error code in the maintenance manual to determine the affected component. Follow the manual's procedure for troubleshooting and/or replacing the part.
Blank Pages	The toner or ink is low. Replace the toner or ink. The developer unit is damaged. Replace the developer unit.
No Image on Printer Display	The printer is powered off. Replace the printer. The display is damaged or disconnected. Replace or reconnect the display.

5.7 Given a scenario, troubleshoot common wired and wireless network problems.

- *Common symptoms*
    - *Limited connectivity*
    - *Unavailable resources*
    - *Internet*
    - *Local resources*
        - *Shares*
        - *Printers*
        - *Email*
    - *No connectivity*
    - *APIPA/link local address*
    - *Intermittent connectivity*
    - *IP conflict*
    - *Slow transfer speeds*
    - *Low RF signal*
    - *SSID not found*

Troubleshooting Wi-Fi/Network

- There are 7 layers in the OSI Network model
- When troubleshooting a network issue, you should begin troubleshooting at Layer 1 and work your way up to Layer 7, until you have resolved the issue.

Layer 1 Physical Layer	This layer deals with physical connections. Are the devices physically connected to each other? Test the ethernet to make sure that the continuity is good on all pairs. Check that all the devices are powered on correctly. Check that the network interface cards are functioning.
Layer 2 Data Link Layer	This layer deals with Ethernet and Point to Point Protocols between two devices A cable with good continuity may still have interference from electrical or other sources. Check that the interfaces are connected at the correct speed (10, 100, 1000, etc.) and the correct duplex (full duplex or half duplex). Both devices should have the same speed and duplex settings. Remember that a network interface's speed and duplex could be set manually or automatically. Check that the device is connected in the correct VLAN.
Layer 3 Network Layer	This layer contains the IPv4 and IPv6 Protocols

	Check that all the devices have the correct IP addresses, gateway addresses, and DNS servers Check other routing protocols to make sure that they are connected correctly Check that the device has received an address over DHCP Check that nothing is being blocked by a firewall
Layer 4 Transport Layer	This layer delivers data from the network card to the application Check that the applications are configured correctly, and with the correct port number Check that nothing is being blocked by firewalls or antivirus programs
Layer 5 Session Layer	The session layer involves authentication Check that the applications are configured correctly and that the correct credentials (URLs, usernames, passwords, certificates, etc.) have been entered into the applications
Layer 6 Presentation Layer	Sometimes the presentation layer and application layers are combined The presentation layer is responsible for formatting received information and sending it to the application layer

	Check that the application is configured correctly
Layer 7 Application Layer	The application layer is the user interface that displays received information to the user Check that the application is configured correctly

Limited Connectivity	The device is not able to reach the internet. If the device is set to DHCP, this issue is typically associated with an APIPA/link local address. If the device is not able to reach a DHCP server, check that the DHCP server is configured. If the device is set to static, ensure that the static IP address is in the correct subnet and has the correct gateway. Check that the DNS servers are correct and reachable. Check that no firewall is blocking the connection. Check that the network is connected to the internet. Confirm that the modem or WAN connection is operating correctly.
Unavailable Resources	The resources may be powered off or disconnected from the network. Check that the resources are available and that their network connection is configured correctly. Check if the other resources are functioning correctly, and that no security appliances are blocking the connection.
No Connectivity	The device is not connected to the network. Check that the cable is connected, the network switch is powered on, and that the network interface is connected.

APIPA/Link Local Address	The device is not able to reach a DHCP server. Check that the DHCP server is functioning and connected to the network.
Intermittent Connectivity	The network switch is failing, or the cable connection is damaged. Replace the cable or network switch. Check that the Wi-Fi signal is adequate and not being blocked by obstructions.
IP Conflict	Multiple devices on the same network have the same IP address. This typically occurs when the addresses are statically assigned (since a DHCP server will automatically check for conflicts) Change the devices to DHCP (if available) or change one of the static IPs.
Slow Transfer Speeds	Find out where the bottleneck is in the network topology. Is it the computer, the local network, or the internet? If only one resource (server, website, etc.) is slow, then the issue is with the resource and/or the route that traffic is taking to the resource. If other sites are slow, the internet connection might be slow. Check the connection directly from the internet modem. If the modem provides fast speeds, another portion of the network might be slow. Check

	the switch and router to see if the connection is slow. If the network is fast, the computer may be the issue. Check if the computer is providing slow speeds, or programs running in the background are affecting it.
Low RF Signal	The Wi-Fi signal is poor. The Wi-Fi signal can be reduced by walls, concrete, and steel. The Wi-Fi access point may be too far away, or may not have adequate antennas. Move to an area with better signals or install additional access points.
SSID Not Found	The SSID is not correct, or the SSID is not broadcasting. Check the configuration on the Access Points.

Part G 220-1002 1.0 Operating Systems

1.1 Compare and contrast common operating system types and their purposes.

- *32-bit vs. 64-bit*
    - *RAM limitations*
    - *Software compatibility*
- *Workstation operating systems*
    - *Microsoft Windows*
    - *Apple Macintosh OS*
    - *Linux*
- *Cell phone/tablet operating systems*
    - *Microsoft Windows*
    - *Android*
    - *iOS*
    - *Chrome OS*
- *Vendor-specific limitations*
    - *End-of-life*
    - *Update limitations*
- *Compatibility concerns between operating systems*

Operating System Types – 32-bit vs 64-bit

- What do we mean when we say 32-bit or 64-bit?
- Each portion of RAM has an address. A processor performing calculations stores data in the RAM. It must be able to locate the data by specifying its address. A 32-bit processor can support up to a maximum of 2^{32} bits of RAM, which is 4GB. A 64-bit processor can support up to 2^{64} bits of RAM, which is 18 EB
- You can run a 32-bit operating system on most 64-bit processors, but won't be able to take full advantage of the processor's features
- A 64-bit operating system can only run on a 64-bit processor
- If you install a 32-bit operating system on a 64-bit processor, you'll only be able to use 4GB of RAM, even if your computer has more RAM installed
- Some programs require 64-bit operating systems. A program might be written to run on a 64-bit operating system

Workstation Operating System – Windows vs Apple vs Linux

- Windows
  - Manufactured by Microsoft
  - Closed source (the source code is not available)
  - Most computers run Microsoft Windows, especially business computers
  - Latest version is Windows 10
  - Stores files in NTFS file system (hierarchical file system)
  - Stores settings in the Windows registry
  - Most programs are written to run on Windows
  - Frequent security updates are released by Microsoft (almost weekly), and are mandatory
- Apple
  - Manufactured by Apple
  - Closed source
  - Based on Linux operating system
  - Typically bundled with Apple hardware (iMac, MacBook Pro, etc.)
  - Current version is macOS 10.14
  - Stores files in HFS file system (hierarchical file system)
  - Stores settings in various plist files
  - Fewer programs run on macOS
  - Security updates are not frequent
- Linux
  - Open source
  - Many versions of Linux are available from different manufacturers and community groups
  - Both files and folders (directories) are considered files. File metadata is stored in inodes. Each inode corresponds to a different file.
  - Each application stores its own settings in its own files
  - Few programs run on Linux
- Emulator

- It’s possible to install an emulator that allows you to run Windows programs on a Mac or Mac programs on Windows

Cellular Operating System

- Microsoft Windows
    - Current version is Windows 10 mobile
    - Released by Microsoft
    - Not popular
    - Microsoft plans to discontinue it
- Android
    - Developed by Google
    - Open source
    - Based on Linux
    - Google is responsible for creating updates to Android, and releasing them (updates are released in an open source format)
    - Device manufacturers will customize the Android operating system released by Google to suit their own devices
    - Android is used by many phone manufacturers, including LG, Samsung, HTC, and Huawei
    - Can download Apps from the Google Play Store or the Amazon store
    - Can download Apps from other sources such as the internet, but these might present a security risk
    - Typically bundled with Google Apps such as Chrome
    - Easy to “root” (gain admin access) in order to run other unauthorized applications or to modify the software
    - Data is backed up to a Google account
- iOS
    - Developed by Apple
    - Closed source
    - Based on Linux
    - Only runs on Apple devices
    - Can download Apps from the iTunes store (only apps authorized by Apple are available in the store). Apps are not available anywhere else.
    - Data is optionally backed up to iCloud (Apple service)

    - Difficult or impossible to “root” or “jailbreak” (gain admin access) in order to run other unauthorized applications, especially on newer versions of the iPhone
- Chrome OS
    - Developed by Google
    - Based on Linux
    - Available pre-installed on hardware manufactured by Google partners
    - Runs on phones, tablets, and laptops
    - Designed as a thin client operating system, with primary support for web apps
    - Primary user interface is the Google Chrome web browser
    - Can run most Android apps (downloadable through the Google play web store)

Operating System Vendor-Specific Limitations

- End of Life
  - Technically, an operating system will function forever (if the hardware doesn't change). That doesn't mean that the operating system will be relevant forever, because technology changes.
  - An operating system will typically announce the "end of life" at least a year in advance
  - End of life means that manufacturer will stop creating updates, especially security updates after a certain point
  - For enterprise customers, the manufacturer will also stop providing technical support
  - Newer apps won't run on older versions of operating systems; therefore, users will be forced to upgrade
- Update Limitations
  - A new operating system update may not operate on the current hardware set. A user may need to purchase more advanced hardware
  - A vendor can charge customers to upgrade to a newer version of the operating system. The cost of the upgrade may be less than the cost of the full version.

1.2 Compare and contrast features of Microsoft Windows versions.

- *Windows 7*
- *Windows 8*
- *Windows 8.1*
- *Windows 10*
- *Corporate vs. personal needs*
    - *Domain access*
    - *BitLocker*
    - *Media center*
    - *Branchcache*
    - *EFS*
- *Desktop styles/user interface*

Windows 7

- Released in 2009
- Most enterprise users operate Windows 7 (forced to upgrade to Windows 7 after Windows XP end of life was announced), and are in the process of upgrading to Windows 10
- Can downgrade from Windows 8 or Windows 10 to Windows 7
- Support ended on January 15, 2015, and extended support ends January 14, 2020
- New features
    - Windows PowerShell
    - Touch and handwriting recognition
    - Ability to pin applications to the task bar
    - Each user has "Libraries" such as Documents, Music, Pictures, and Video
    - BitLocker drive encryption
- Editions
    - Starter: basic edition supporting 2GB of RAM
    - Home Basic: basic edition sold in emerging markets
    - Home Premium: sold to home users
    - Professional: supports Remote Desktop, 192GB of RAM, EFS, and software restriction policies
    - Enterprise: intended for Enterprise users and sold through volume licensing
    - Ultimate: same features as Enterprise but available through individual licensing
- Hardware
    - Available in 32-Bit or 64-Bit
    - Supports two physical processors

Windows 8

- Released in 2012
- Intended for use on tablets and touch devices. Microsoft assumed that most computers would be touch by time Windows 8 was released, but touch features did not become popular on laptops and desktops.
- Currently supported by Microsoft
- New features
  - UEFI integration
  - Support for USB 3.0
  - Recovery with Refresh and Reset functions
  - Ability to log in with a PIN, picture password, or Windows Live account
  - Ability to purchase Apps from the Windows Store
- Editions
  - Windows 8 Basic version: contains basic features; can purchase a "Pro Pack" to upgrade to Windows 8 Pro
  - Windows 8 Pro: contains BitLocker, Hyper-V, ability to join a domain
  - Windows 8 Enterprise: similar to Pro, but sold through volume licensing
- Only available as an upgrade, not available as a full version
  - Full version sold only to PC manufacturers for installation on new computers

Windows 8.1

- Released in 2013
- Available as a free upgrade to Windows 8
- Available as a full license
- New features
    - Enhanced user interface based on complaints from users of Windows 8

Windows 10

- Released in 2015
- New features
    - Support for universal apps (an app that runs on PCs, tablets, smartphones, Xbox, and Internet of Things devices)
    - Microsoft Edge web browser
    - DirectX 12
    - Cortana digital assistant
    - Ability to search the internet through the start menu
    - Updates are mandatory
- Editions
    - Home: intended for home users
    - Pro: supports advanced features such as Remote Desktop, domains, group policy, active directory
    - Education: like Enterprise edition but for educational institutions
    - Enterprise: like Pro, but sold in volume licensing deals only
- Windows Insider Programs
    - Allows select individuals to receive advanced copies of Windows 10 Operating System and updates for testing
- When Windows 10 was first released, Microsoft offered a free upgrade to any Windows 7 or 8.1 user

Windows Corporate Features

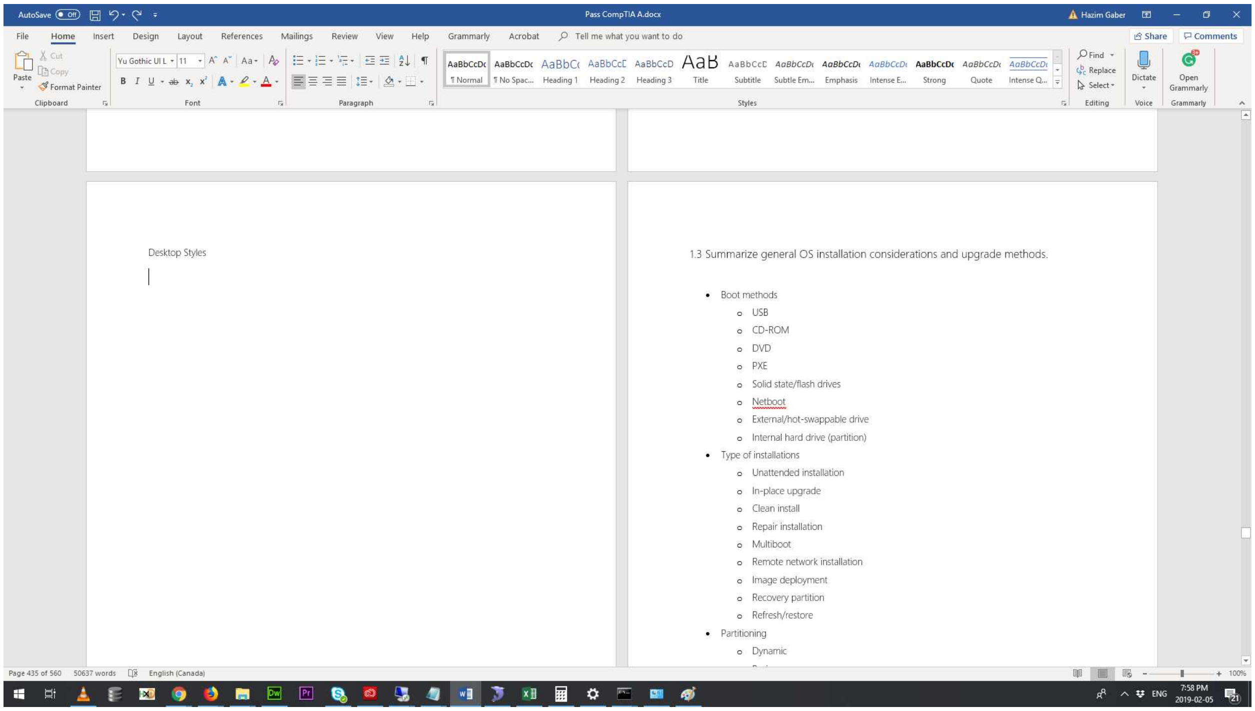
Domains	User accounts, computers and security policies are registered with a central server, known as an "Active Directory" server These users and computers become part of a "domain" A computer must be "joined" to the domain. When joined, it checks the Active Directory server for the correct policies to apply to itself. When a user logs in to a computer that is on the domain, the computer authenticates the user with the Active Directory server. The computer checks the server for policies to apply to the user account that has logged in.
BitLocker	Provides full-disk encryption. If the computer contains a TPM, the encryption key is stored inside the TPM. When BitLocker is enabled, the computer can load to Windows, but none of the additional files are decrypted until the user successfully logs in. Operating system data is stored in a separate partition. Can store the encryption key in Active Directory. If the computer does not contain a TPM, the computer will not load to Windows. A user must enter a password when the computer

	boots. An encryption key could also be stored on a USB. Possible to decrypt contents through a “cold boot” attack.
Media Center	Allowed users to record video and play media. Discontinued in 2009. Supported media files, DVDs, TV tuner cards and photos.
Branchcache	Bandwidth optimization feature Reduces WAN traffic by caching data on local servers When a client downloads data from a remote server, it first checks if a current version of the data is available on the local server. If the data is available locally, it will download the data locally. If the data is available on the remote server, it will download from the remote, and save a copy to the local server for use by other users.
EFS	Encrypting File System Without encryption, a hacker with physical access to the computer can remove the hard disk drive and access all file contents (even without knowing any username or passwords)

	EFS encrypts all files EFS decrypts files in the background so that applications don’t notice

Desktop Styles

A typical Windows user interface

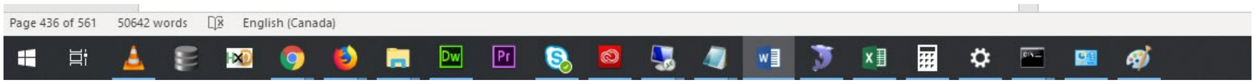


Desktop Styles

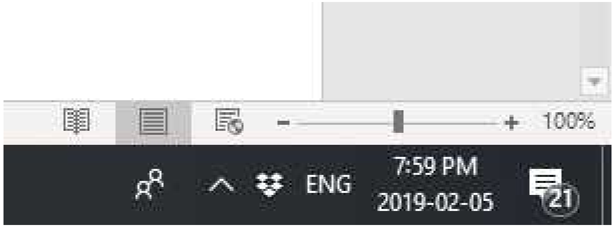
1.3 Summarize general OS installation considerations and upgrade methods.

- Boot methods
  - USB
  - CD-ROM
  - DVD
  - PXE
  - Solid state/flash drives
  - Netboot
  - External/hot-swappable drive
  - Internal hard drive (partition)
- Type of installations
  - Unattended installation
  - In-place upgrade
  - Clean install
  - Repair installation
  - Multiboot
  - Remote network installation
  - Image deployment
  - Recovery partition
  - Refresh/restore
- Partitioning
  - Dynamic

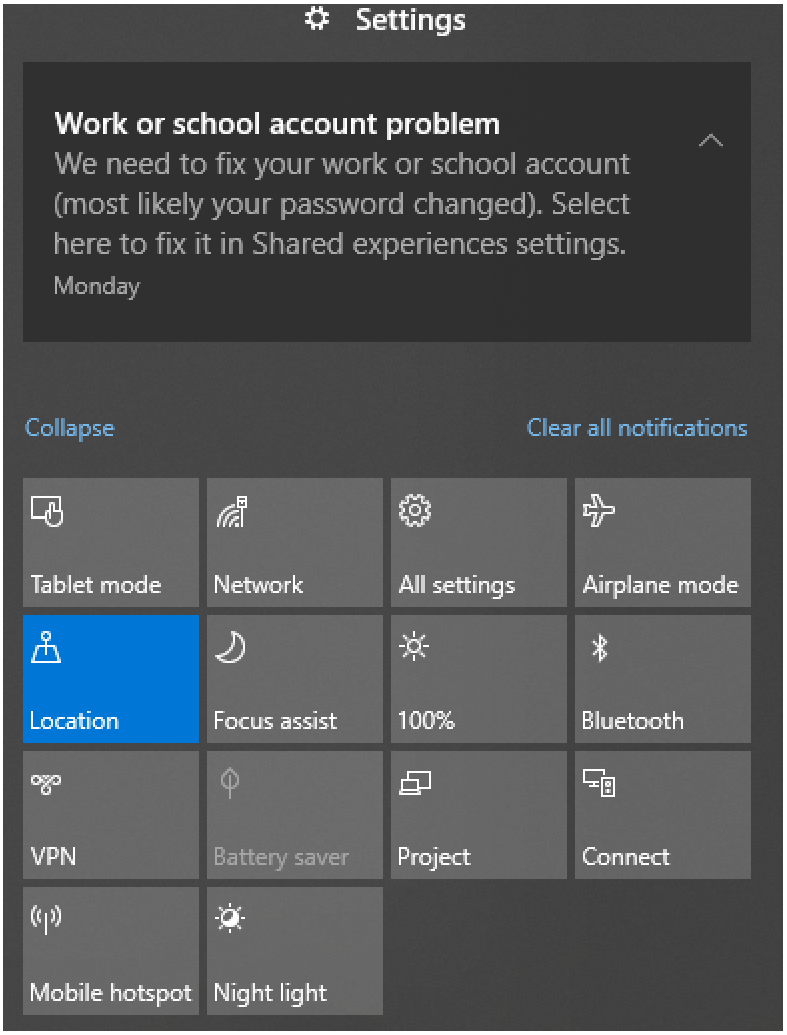
The bottom of the screen contains the task bar, which contains icons for each running application



In the right corner of the task bar is the clock. Icons for background applications appear there.



The notifications page shows different notifications, and provide access to frequent settings

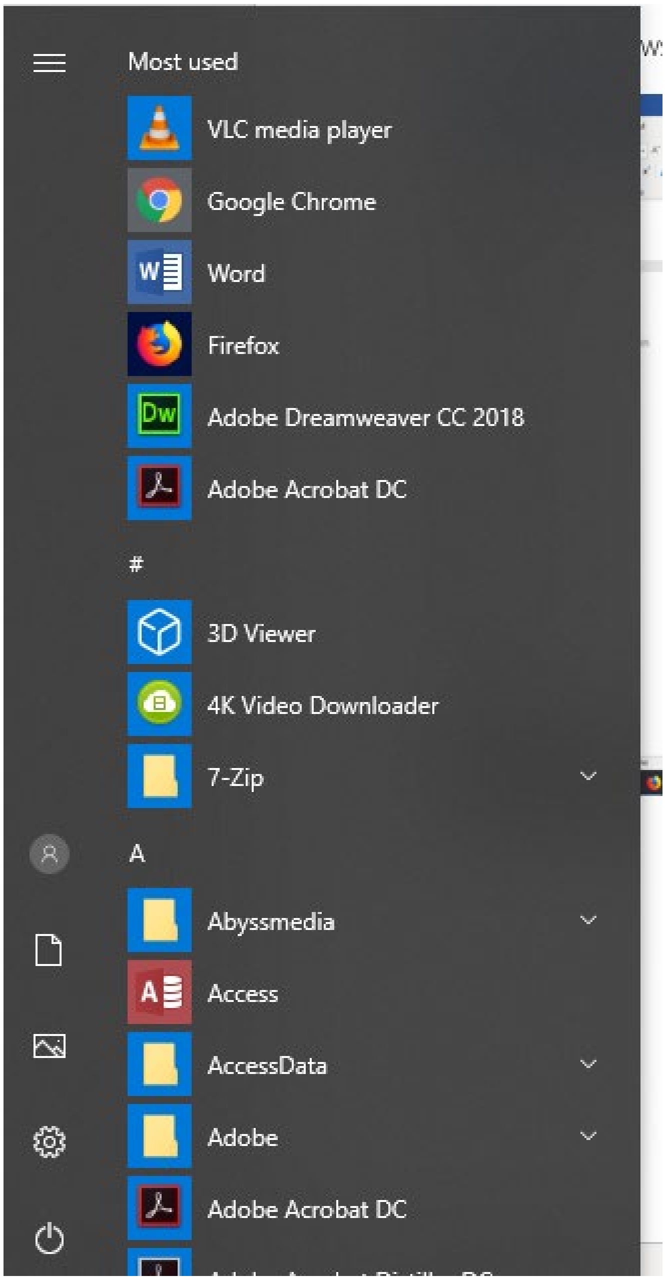


Work or school account problem

We need to fix your work or school account (most likely your password changed). Select here to fix it in Shared experiences settings.

Monday

The start menu provides access to applications



Most used
VLC media player
Google Chrome
Word
Firefox
Adobe Dreamweaver CC 2018
Adobe Acrobat DC
#
3D Viewer
4K Video Downloader
7-Zip
A
Abyssmedia
Access
AccessData
Adobe
Adobe Acrobat DC

1.3 Summarize general OS installation considerations and upgrade methods.

- *Boot methods*
  - *USB*
  - *CD-ROM*
  - *DVD*
  - *PXE*
  - *Solid state/flash drives*
  - *Netboot*
  - *External/hot-swappable drive*
  - *Internal hard drive (partition)*
- *Type of installations*
  - *Unattended installation*
  - *In-place upgrade*
  - *Clean install*
  - *Repair installation*
  - *Multiboot*
  - *Remote network installation*
  - *Image deployment*
  - *Recovery partition*
  - *Refresh/restore*
- *Partitioning*
  - *Dynamic*
  - *Basic*
  - *Primary*
  - *Extended*
  - *Logical*
  - *GPT*
- *File system types/formatting*
  - *ExFAT*
  - *FAT32*

  - *NTFS*
  - *CDFS*
  - *NFS*
  - *ext3, ext4*
  - *HFS*
  - *Swap partition*
  - *Quick format vs. full format*
- *Load alternate third-party drivers when necessary*
- *Workgroup vs. Domain setup*
- *Time/date/region/language settings*
- *Driver installation, software, and Windows updates*
- *Factory recovery partition*
- *Properly formatted boot drive with the correct partitions/format*
- *Prerequisites/hardware compatibility*
- *Application compatibility*
- *OS compatibility/upgrade path*

Boot Methods

USB / Solid/State/Flash Drive	Insert bootable USB drive into PC USB drive must be formatted to be "bootable" BIOS must support ability to boot from USB
CD-ROM	Boot from bootable CD-ROM
DVD	Boot from bootable DVD
PXE	Boot from Preboot Execution Environment The computer will query a server for the operating system and configuration settings The computer will download and install necessary installation files over the network Works over DHCP • The device being booted sends a special DHCP request requesting PXE information • The PXE server will reply with the correct parameters
NetBoot	Apple technology Allows a Mac to boot from the network
External/Hot-Swappable Drive	Can boot from eSATA drive or other external drive
Internal HDD Partition	Most common way of booting Can divide an HDD into multiple partitions

	Can boot from each partition separately (each partition may contain a separate operating system)

Type of Installation

Unattended Installation	Also known as a silent installation The operating system installer is pre-programmed with all the required settings Once, executed, it installs without user intervention
In-Place Upgrade	The operating system is "upgraded" to a newer version Operating system files are replaced Applications and user files remain It's usually possible to revert to the old installation
Clean Install	The entire disk is erased and the operating system is installed All user files and programs are deleted
Repair Installation	The existing operating system is repaired The operating system detects files that are damaged or missing and repairs or replaces them The operating system version remains the same All user files and programs remain
Multiboot	Ability to have multiple operating systems on the same drive Can boot from more than one operating system
Remote Network Installation	The operating system installer downloads over the network Once downloaded, an unattended installation is performed

	Typical for enterprise environments
Image Deployment	A company may create a custom Windows image, which is a version of the operating system with specific settings unique to the company. It might include specific security policies, settings, and applications. The enterprise can distribute this image across multiple computers automatically.
Recovery Partition	The recovery partition contains a new version of windows. It is contained on a separate partition of the hard disk drive. If the user wishes to restore to a clean image of the operating system, he can access the partition.
Refresh/Restore	Refresh and restore are recovery options available on Windows 8 and later. Refresh repairs all missing and damaged system files. It does not erase user data or applications. Restore performs a clean install of Windows

Partition

A physical disk can be divided into one ore more logical disks. Each logical disk is known as a partition and can be assigned a drive letter.

Dynamic	A dynamic disk allows you to create a volume that spans multiple physical disks (such as RAID 5) Data about the dynamic disks is stored inside a dynamic disk volume. The volume is replicated across all physical disks.
Basic	A basic disk can contain multiple partitions, but each partition must be comprised of contiguous, unallocated space
Primary	A primary partition is a partition where an operating system's boot files are located There can be a maximum of four primary partitions on a physical disk The MBR or Master Boot Record identifies the first sector of the hard disk (where the operating system's boot files are located). The MBR allows the computer to boot. MBR is limited to drives of 2TB or smaller A hard disk drive is divided into sectors Newer drives use sectors of 4KB in size, and this size is not compatible with MBR

Extended	The extended partition contains all the remaining free space It can be subdivided into multiple segments There can be a maximum of one extended partition per physical disk
Logical	A logical partition is a virtual section of the physical hard disk that acts as an independent drive.
GPT	GUID Partition Table Lists the location and type of each partition on the hard disk Newer than MBR

File Systems

The file system is a scheme for storing data on a hard disk drive. To the hard disk, the files are just zeros and ones. There must be a directory so that the hard disk can locate each file.

Every file system contains a "table" or database. The table contains a list of all the files contained on the partition, a description of their attributes, and their physical location on the drive.

exFAT	Extended File Allocation Table Designed by Microsoft for USB drives Good for embedded systems because it has low power requirements Must pay Microsoft a license fee to use exFAT in your product
FAT32	File Allocation Table (previous versions were FAT16 and FAT12) Used by USB drives Previously used by Windows computers Maximum size of 4GB per file
NTFS	New Technology File System Current system in use on most Windows computers Optimized for hard disks with 4KB sectors Key features • Journaling (tracks changes to file metadata) • Volume Shadow Copy (retains previous versions of files) • Transactions (groups multiple changes to files in a single transaction;

	guarantees that all changes happen to a file at the same time) • Encrypting File System (can encrypt and decrypt files automatically)
CDFS	Compact Disk Filing Format Data structure for CDs
NFS	Network File System Developed by Sun Used by UNIX and macOS Allows users to access files over the network
ext3, ext4	Extended File System Version 3 and Extended File System Version 4 Used by Linux
HFS	Hierarchical File System Developed by Apple New version is HFS+ (or HFS Extended) Probably the worst file-system ever (according to Linux users), because it doesn't support checksums (which leads to data corruption)
Swap Partition	When your computer is low on RAM (you have more applications open than available RAM), Windows will store the remaining data in a file called the swap file. The swap file is stored on the hard disk.

	The area that Windows stores it is called the swap file or the swap partition You can change the location and size of the swap file
Quick Format vs Full Format	Formatting is the process of setting up a new file system on a partition. When you format a disk, all the data is erased. A hard drive is divided into sectors. Typically, the size of a sector is 4KB. A 1TB hard disk could have 250,000 sectors. Some sectors might get damaged and can't reliability store data. They should be excluded from the system. A Quick Format erases all the data and sets up the file allocation tables and data structures. A Full Format erases all the data and sets up the file allocation tables and data structures. A Full Format also scans the hard disk for bad sectors.

Other OS Install Considerations

- Load alternate third-party drivers when necessary
  - During installation of an operating system, Windows will attempt to detect the hardware (mouse, keyboard, graphics card, NIC, etc.) and install the drivers.
  - This doesn’t really apply to Mac’s because the hardware and software are part of the same package
  - Windows won’t have drivers for some newer SSDs (must copy these drivers to the installation media prior to installing Windows)
  - Your company may use specific drivers for their hardware (basic print driver for example) or proprietary drivers for specific items
- Workgroup vs. Domain setup
  - Does the office use a workgroup or a domain?
  - If the office uses a domain, you must join the computer to the domain.
  - You must use an account that has permission to join the computer to the domain (typically an admin account)
- Time/date/region/language settings
  - Set the correct date, time, region, and language
  - The date and time can be updated automatically
- Driver installation, software, and Windows updates
  - Windows will automatically check for updates after installation
  - Some software programs will also check for updates
- Factory recovery partition
  - The factory partition contains recovery files for the operating system, which you can revert back to
- Properly formatted boot drive with the correct partitions/format
  - If you’re installing Windows from a USB key, the key should be bootable (contains a boot record)
- Prerequisites/hardware compatibility
  - Make sure that your computer has adequate and compatible hardware for the operating system that you’re installing
- Application compatibility

    - Must check to make sure that applications will function with the operating system that you are installing
- OS compatibility/upgrade path

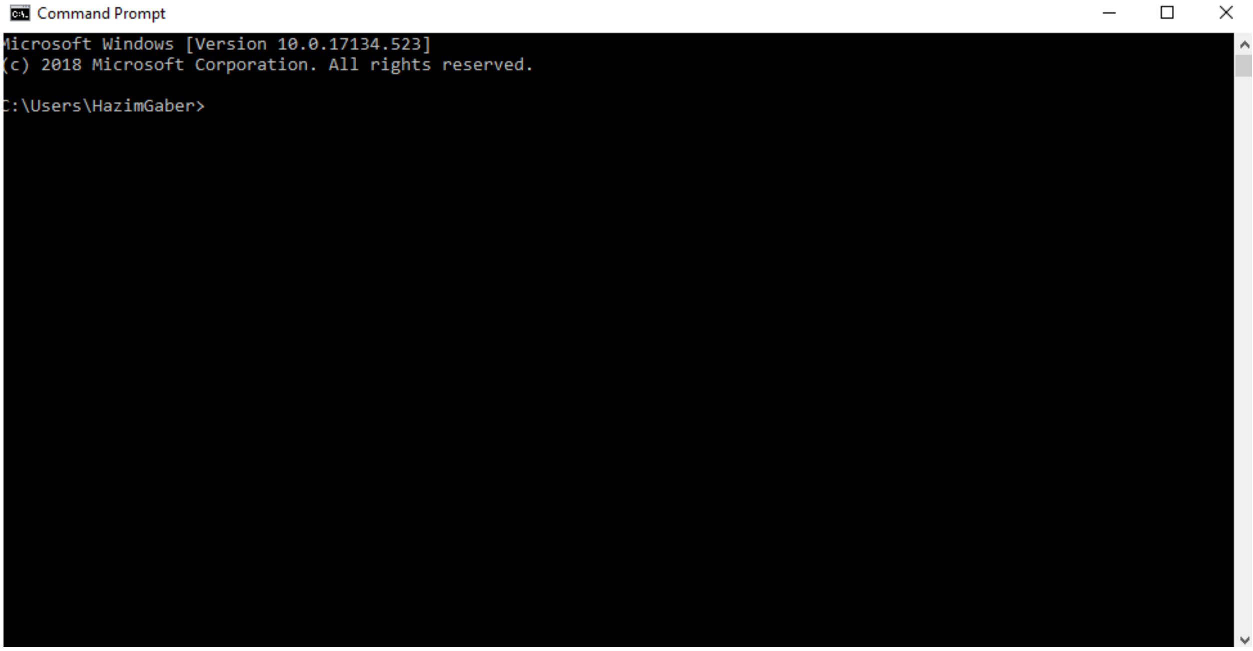
1.4 Given a scenario, use appropriate Microsoft command line tools.

- *Navigation*
  - *dir*
  - *cd*
  - *..*
- *ipconfig*
- *ping*
- *tracert*
- *netstat*
- *nslookup*
- *shutdown*
- *dism*
- *sfc*
- *chkdsk*
- *diskpart*
- *taskkill*
- *gpupdate*
- *gpresult*
- *format*
- *copy*
- *xcopy*
- *robocopy*
- *net use*
- *net user*
- *[command name] /?*
- *Commands available with standard privileges vs. administrative privileges*

Command Line Tools

How to run a command in Windows?

Go to start menu and launch the command prompt (type cmd)



```
icrosoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

:\Users\HazimGaber>
```

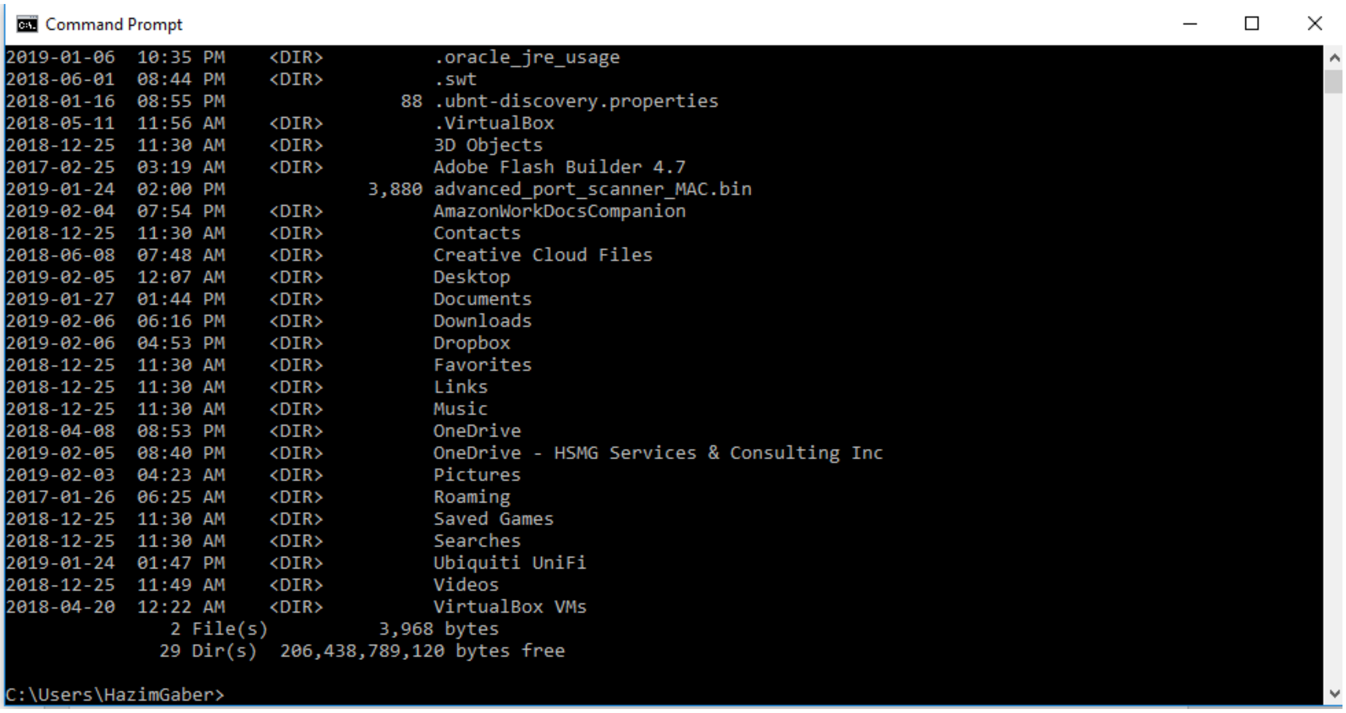
The command prompt's default location is the current user's directory

You can type a command and press Enter

Each command may have one or more options that provide additional features dir

Lists the contents of a directory

- Date modified
- File size
- File name
- Whether the item is a file or a directory (indicated by <DIR>)
- Type *dir /A* to list all files, including hidden files



```
2019-01-06  10:35 PM    <DIR>          .oracle_jre_usage
2018-06-01  08:44 PM    <DIR>          .swt
2018-01-16  08:55 PM                88 .ubnt-discovery.properties
2018-05-11  11:56 AM    <DIR>          .VirtualBox
2018-12-25  11:30 AM    <DIR>          3D Objects
2017-02-25  03:19 AM    <DIR>          Adobe Flash Builder 4.7
2019-01-24  02:00 PM             3,880 advanced_port_scanner_MAC.bin
2019-02-04  07:54 PM    <DIR>          AmazonWorkDocsCompanion
2018-12-25  11:30 AM    <DIR>          Contacts
2018-06-08  07:48 AM    <DIR>          Creative Cloud Files
2019-02-05  12:07 AM    <DIR>          Desktop
2019-01-27  01:44 PM    <DIR>          Documents
2019-02-06  06:16 PM    <DIR>          Downloads
2019-02-06  04:53 PM    <DIR>          Dropbox
2018-12-25  11:30 AM    <DIR>          Favorites
2018-12-25  11:30 AM    <DIR>          Links
2018-12-25  11:30 AM    <DIR>          Music
2018-04-08  08:53 PM    <DIR>          OneDrive
2019-02-05  08:40 PM    <DIR>          OneDrive - HSMG Services & Consulting Inc
2019-02-03  04:23 AM    <DIR>          Pictures
2017-01-26  06:25 AM    <DIR>          Roaming
2018-12-25  11:30 AM    <DIR>          Saved Games
2018-12-25  11:30 AM    <DIR>          Searches
2019-01-24  01:47 PM    <DIR>          Ubiquiti UniFi
2018-12-25  11:49 AM    <DIR>          Videos
2018-04-20  12:22 AM    <DIR>          VirtualBox VMs
               2 File(s)          3,968 bytes
              29 Dir(s)  206,438,789,120 bytes free

C:\Users\HazimGaber>
```

cd

Changes Directory

Type *cd* ***directory name***

Where *directory name* is the directory you want to go to

The directory you need to access must be inside the directory you're already in

..

To go “up one level” in the directory, type *cd ..*

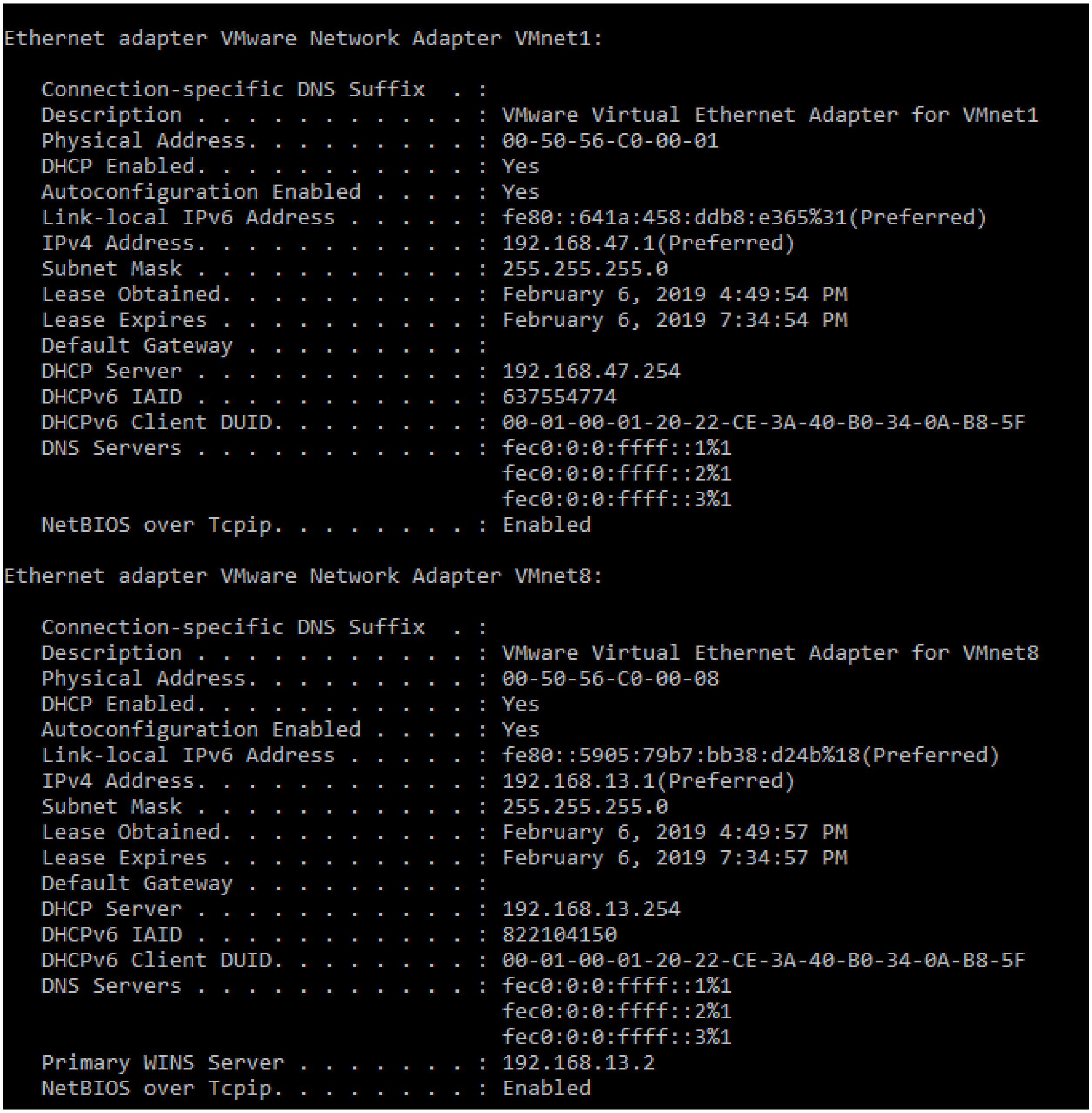
For example if you’re in C: \Main\Second, and you want to go to C: \Main, type *cd ..*

ipconfig

Displays the IP configuration of the computer

ipconfig /a lists all the network adapters, including

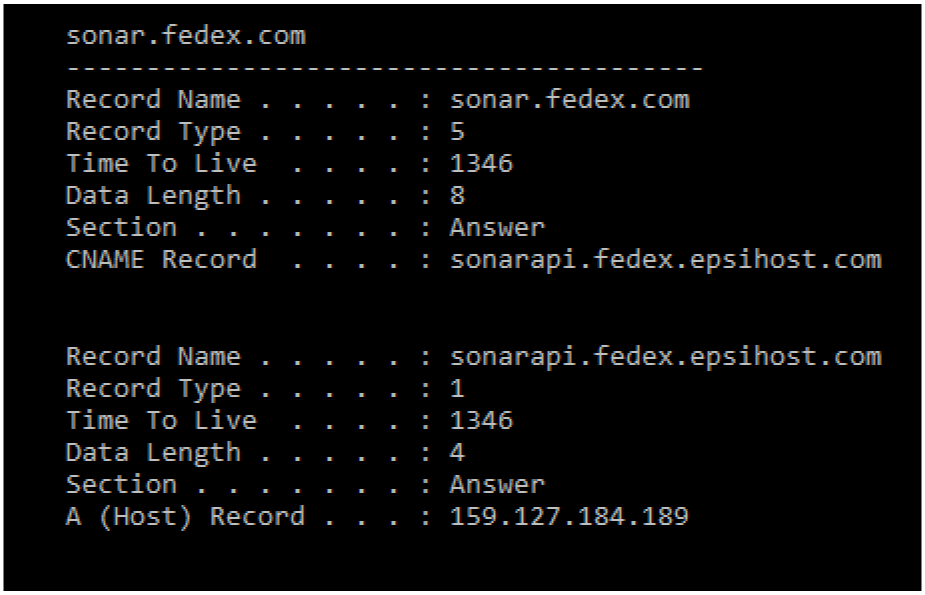
- Network adapter name
- MAC address (physical address)
- IP address, gateway, subnet mask, DHCP server, and DNS servers (if available)



```
Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::641a:458:ddb8:e365%31(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.47.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : February 6, 2019 4:49:54 PM
   Lease Expires . . . . . . . . . . : February 6, 2019 7:34:54 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.47.254
   DHCPv6 IAID . . . . . . . . . . . : 637554774
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-22-CE-3A-40-B0-34-0A-B8-5F
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5905:79b7:bb38:d24b%18(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.13.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : February 6, 2019 4:49:57 PM
   Lease Expires . . . . . . . . . . : February 6, 2019 7:34:57 PM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.13.254
   DHCPv6 IAID . . . . . . . . . . . : 822104150
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-22-CE-3A-40-B0-34-0A-B8-5F
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   Primary WINS Server . . . . . . . : 192.168.13.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Some other commands

- *ipconfig /renew*: renews the IP address (if over DHCP). Attempts to obtain a new IP address from the DHCP server.
- *ipconfig /release*: releases the IP address (if over DHCP). Gives the IP address back to the DHCP server.
- *ipconfig /flushdns*:: erases the DNS
- *ipconfig /displaydns*: lists the DNS entries that are currently logged by the computer

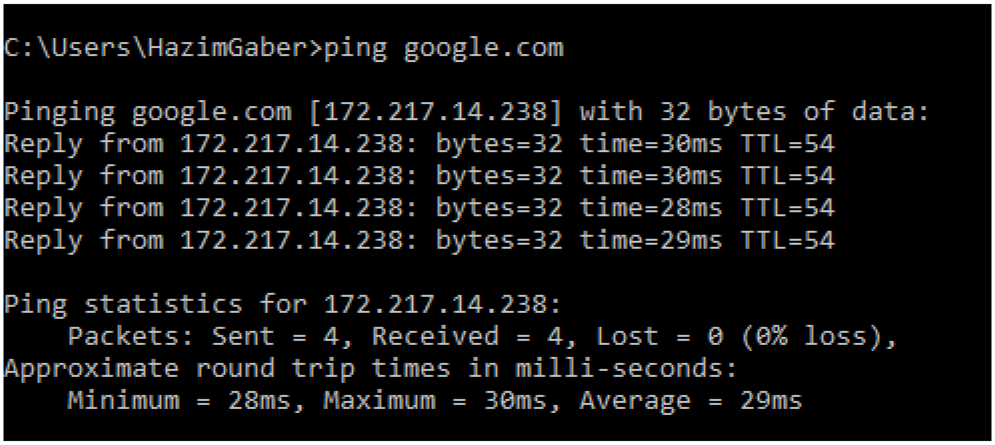


```
    sonar.fedex.com
    ----------------------------------------
    Record Name . . . . . : sonar.fedex.com
    Record Type . . . . . : 5
    Time To Live  . . . . : 1346
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    CNAME Record  . . . . : sonarapi.fedex.epsihost.com


    Record Name . . . . . : sonarapi.fedex.epsihost.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1346
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 159.127.184.189
```

ping

Allows you to ping another computer (by hostname or IP address)

- The command is *ping* ***hostname or IP address***
- For example, ***ping 8.8.8.8*** or ***ping google.com*** will attempt to ping 8.8.8.8 or ping google.com
- The computer will try four pings
- If you enter a hostname, the computer will try to translate it into an IP address via DNS first, and then ping it



```
C:\Users\HazimGaber>ping google.com

Pinging google.com [172.217.14.238] with 32 bytes of data:
Reply from 172.217.14.238: bytes=32 time=30ms TTL=54
Reply from 172.217.14.238: bytes=32 time=30ms TTL=54
Reply from 172.217.14.238: bytes=32 time=28ms TTL=54
Reply from 172.217.14.238: bytes=32 time=29ms TTL=54

Ping statistics for 172.217.14.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 30ms, Average = 29ms
```

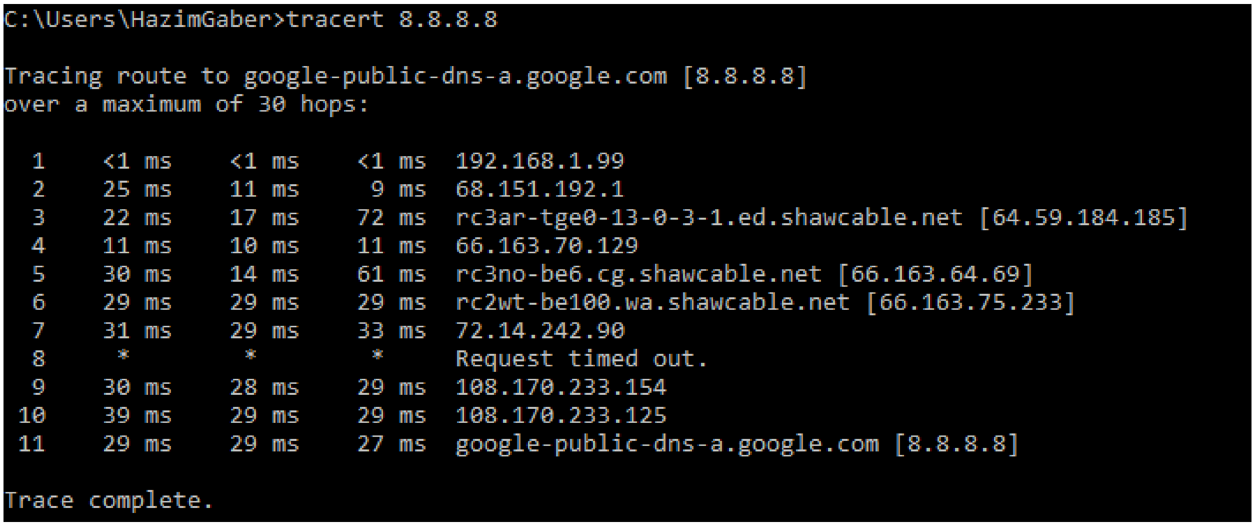
Some options

- *ping -n ####*: can specify the times to send the ping

tracert

Traces the route from your computer to another computer (by hostname or IP address)

The command is *tracert* ***hostname or IP address***

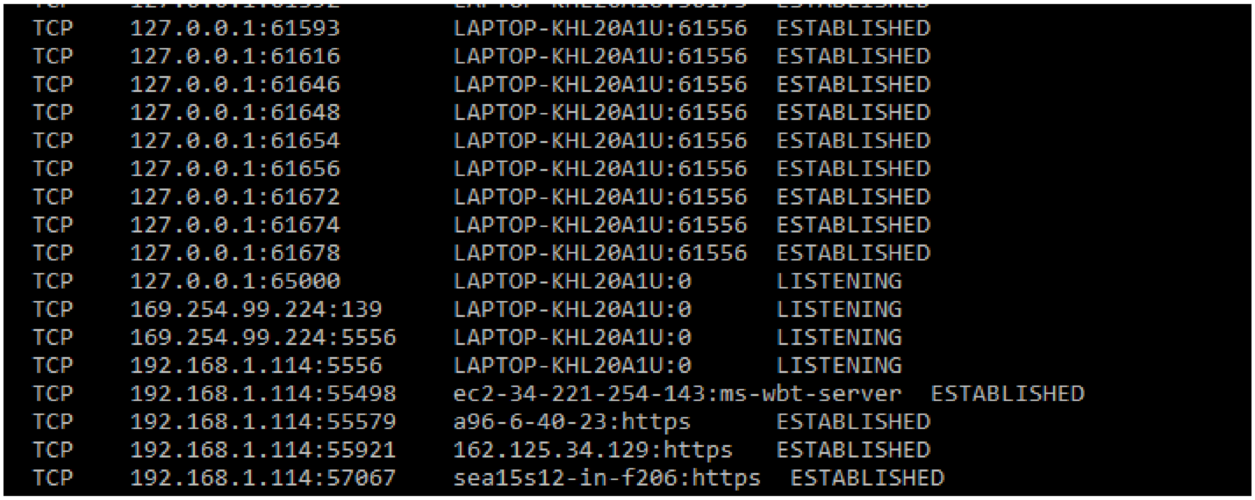


```
C:\Users\HazimGaber>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.99
  2    25 ms    11 ms     9 ms  68.151.192.1
  3    22 ms    17 ms    72 ms  rc3ar-tge0-13-0-3-1.ed.shawcable.net [64.59.184.185]
  4    11 ms    10 ms    11 ms  66.163.70.129
  5    30 ms    14 ms    61 ms  rc3no-be6.cg.shawcable.net [66.163.64.69]
  6    29 ms    29 ms    29 ms  rc2wt-be100.wa.shawcable.net [66.163.75.233]
  7    31 ms    29 ms    33 ms  72.14.242.90
  8     *        *        *     Request timed out.
  9    30 ms    28 ms    29 ms  108.170.233.154
 10    39 ms    29 ms    29 ms  108.170.233.125
 11    29 ms    29 ms    27 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

netstat

Lists all the active connections between your computer and other computers

The command is *netstat*



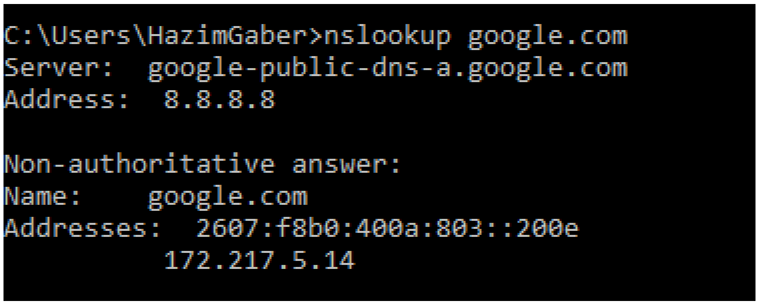
```
  TCP    127.0.0.1:61593        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61616        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61646        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61648        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61654        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61656        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61672        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61674        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:61678        LAPTOP-KHL20A1U:61556  ESTABLISHED
  TCP    127.0.0.1:65000        LAPTOP-KHL20A1U:0      LISTENING
  TCP    169.254.99.224:139     LAPTOP-KHL20A1U:0      LISTENING
  TCP    169.254.99.224:5556    LAPTOP-KHL20A1U:0      LISTENING
  TCP    192.168.1.114:5556     LAPTOP-KHL20A1U:0      LISTENING
  TCP    192.168.1.114:55498    ec2-34-221-254-143:ms-wbt-server  ESTABLISHED
  TCP    192.168.1.114:55579    a96-6-40-23:https      ESTABLISHED
  TCP    192.168.1.114:55921    162.125.34.129:https   ESTABLISHED
  TCP    192.168.1.114:57067    sea15s12-in-f206:https  ESTABLISHED
```

nslookup

Tells us the name server corresponding to a domain name

The command is *nslookup* ***domain name***

For example, if we want to look up where google.com is hosted, we type *nslookup google.com*



```
C:\Users\HazimGaber>nslookup google.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:400a:803::200e
          172.217.5.14
```

shutdown

Shuts down the computer

The command is *shutdown*

dism

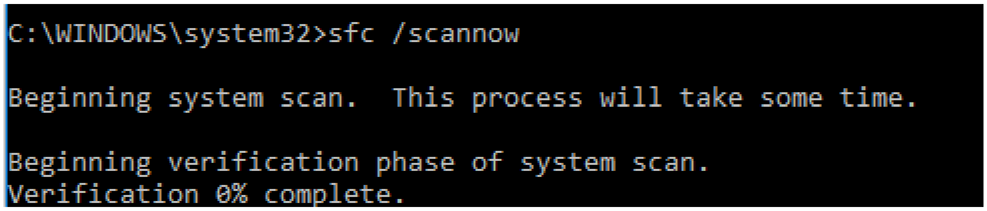
Deployment Image Servicing and Management

- Allows you to repair the Windows installation, if it is corrupted
- DISM will download the correct files from a good source
    - You must have a new copy of the Windows ISO to give to the DISM
    - The DISM uses the Windows ISO to repair the existing Windows installation
- DISM requires admin privileges
- *DISM /Online /Cleanup-Image /RestoreHealth*
    - Checks for errors and repairs them
- *DISM /Online /Cleanup-Image /CheckHealth*
    - Checks for errors, but doesn't repair them

sfc

System File Checker

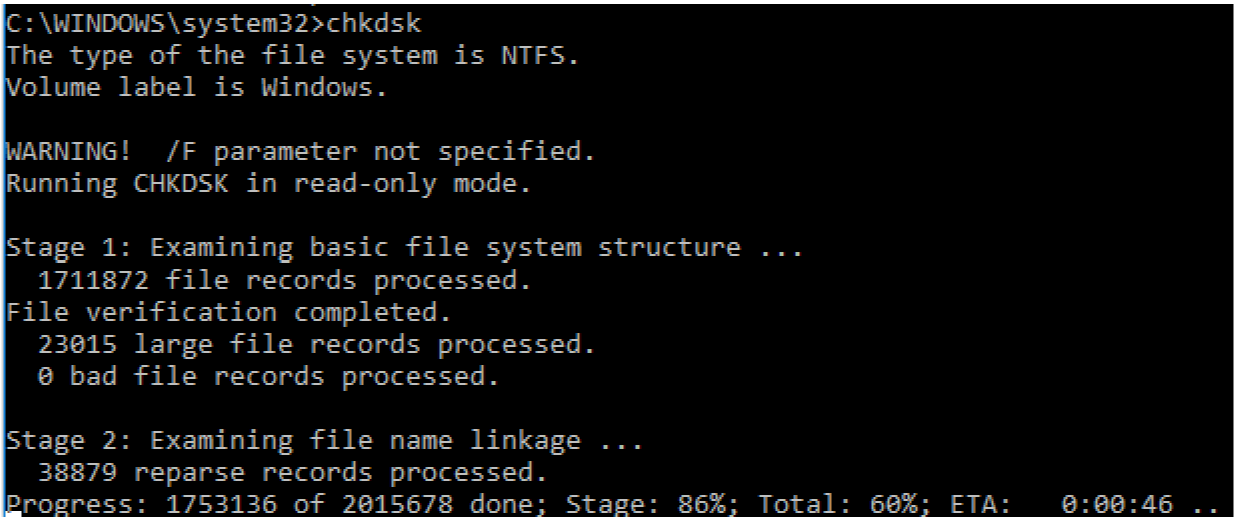
- Requires admin privileges
- *sfc /scannow*
    - Checks for corrupted system files, and repairs them
- sfc /verifyonly
    - Checks for corrupted system files, but does not repair them



```
C:\WINDOWS\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 0% complete.
```

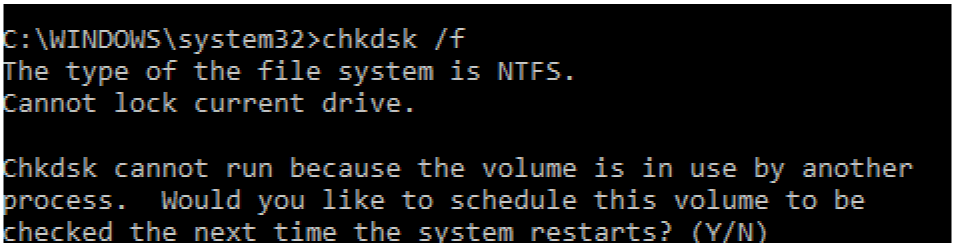
chkdsk

- Checks the hard disk for errors
- Requires admin privileges
- *chkdsk* will only check for errors



```
C:\WINDOWS\system32>chkdsk
The type of the file system is NTFS.
Volume label is Windows.

WARNING!  /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
  1711872 file records processed.
File verification completed.
  23015 large file records processed.
  0 bad file records processed.

Stage 2: Examining file name linkage ...
  38879 reparse records processed.
Progress: 1753136 of 2015678 done; Stage: 86%; Total: 60%; ETA:   0:00:46 ..
```

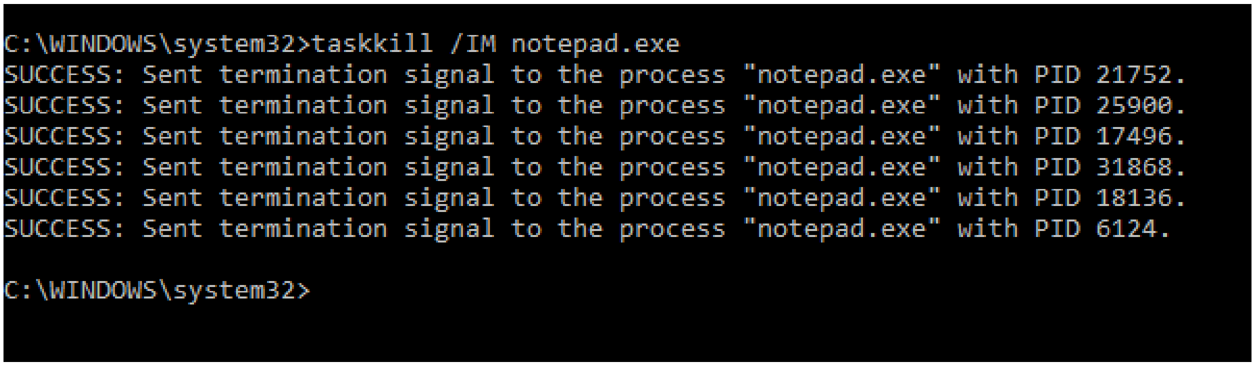
- *chkdsk /f* will check for errors and repair them
- If the drive is in use, then Check Disk won't repair the errors. It will prompt you to run the Check Disk the next time the computer restarts



```
C:\WINDOWS\system32>chkdsk /f
The type of the file system is NTFS.
Cannot lock current drive.

Chkdsk cannot run because the volume is in use by another
process.  Would you like to schedule this volume to be
checked the next time the system restarts? (Y/N)
```

taskkill

- Ends a task
- *taskkill /IM* ***task name***
    - You can end a task with the task name
    - For example, if you want to end notepad.exe, type *taskkill /IM notepad.exe*
    - If there are multiple tasks with the same name, they will all be closed



```
C:\WINDOWS\system32>taskkill /IM notepad.exe
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 21752.
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 25900.
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 17496.
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 31868.
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 18136.
SUCCESS: Sent termination signal to the process "notepad.exe" with PID 6124.

C:\WINDOWS\system32>
```

- *taskkill /PID* ***process ID number***
    - You can end a task with the task process ID
    - For example, if you want to end notepad.exe, and the process ID number is 43, *type taskkill /PID 43*

gpupdate

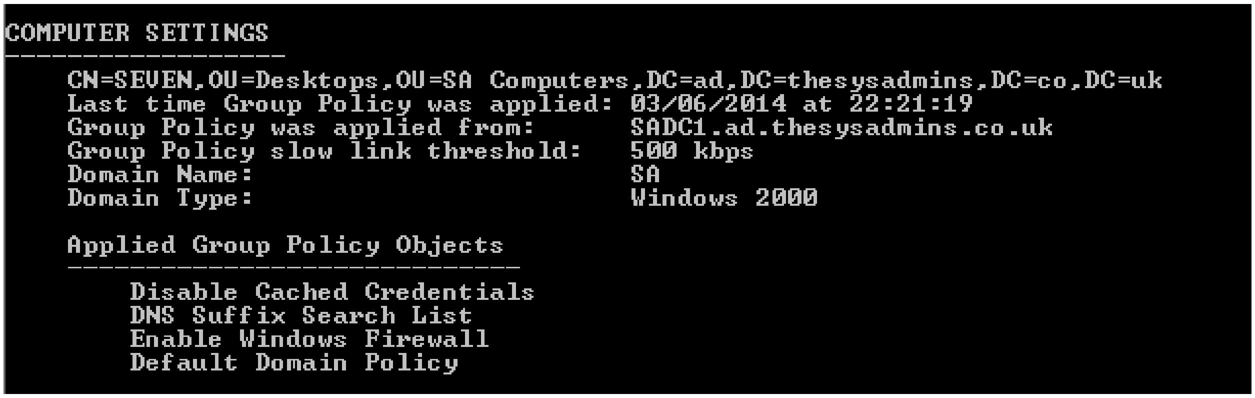
Performs a Group Policy Update

- Applies only to computers connected to a domain
- Downloads the group policy from the active directory server and applies it to the computer
- Type *gpupdate*

gpresult

Determines how a Group Policy applies to a computer or a user

- gpresult: shows how the group policy applies
- gpresult /r /scope:user: shows how the group policy applies to a specific user
- gpresult /r /scope:computer: shows how the group policy applies to a specific computer (and not the user)
- Shows us the last time that the group policy was applied, and from what server



```
COMPUTER SETTINGS
------------------
    CN=SEVEN,OU=Desktops,OU=SA Computers,DC=ad,DC=thesysadmins,DC=co,DC=uk
    Last time Group Policy was applied: 03/06/2014 at 22:21:19
    Group Policy was applied from:      SADC1.ad.thesysadmins.co.uk
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        SA
    Domain Type:                        Windows 2000

    Applied Group Policy Objects
    -----------------------------
        Disable Cached Credentials
        DNS Suffix Search List
        Enable Windows Firewall
        Default Domain Policy
```

format

Formats a drive

- The command is *format* ***drive letter*** */fs:****file-system***
- Where drive letter is the drive letter of the drive you want to format
- File-system is the type of file system you want to implement (NTFS, FAT32, etc.)

copy

Allows you to copy a file

- The command is *copy* ***source file destination directory***
- Source file is the file we want to copy
- Destination directory is the location we want to copy it to
- It is assumed that the source file is located in the current directory
- For example, if we want to copy C: \folder\file1.txt to C: \folder2\, and we are in the C: \folder directory, we would type *copy file1.txt C:\folder2*

xcopy

Allows you to copy a file or directory

- The command is *copy* ***source file or directory destination directory***
- Source file is the file we want to copy
- Destination directory is the location we want to copy it to
- It is assumed that the source file is in the current directory
- For example, if we want to copy C: \folder\file1.txt to C: \folder2\, and we are in the C: \folder directory, we would type *copy file1.txt C:\folder2*

robocopy

Robocopy is the Robust File Copy application

- Allow for faster copying of files
- Command is *Robocopy* ***Source Destination***
- Source is the source directory
- Destination is the destination directory
- For example, if we want to copy files from Directory_A to Directory_B, we type C:\Directory_A C:\Directory_B
- Robocopy can also mirror a directory (it will delete files in the destination directory that were not present in the source directory)

net use

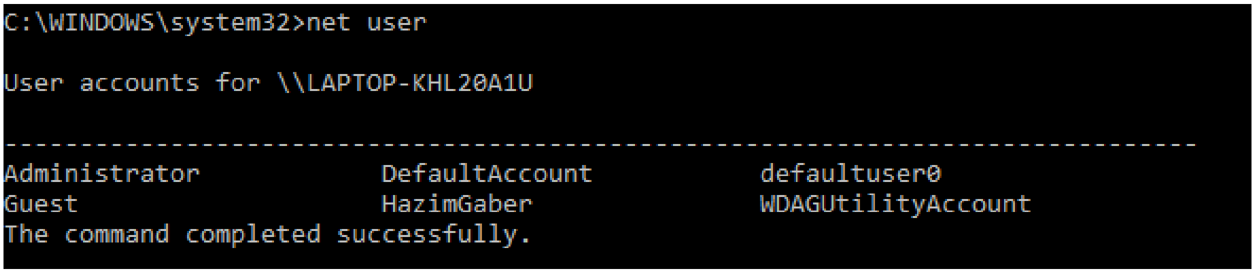
Connects to shared resources (maps a shared resource as a drive)

- Command is *net use* ***drive letter resource name***
- Drive letter is the letter we want to map the resource to
- Resource is the resource location
- For example, if we wanted to map \\server\my media to the E drive, we would type *net use e: "\\server\my media"*
- We can also delete a resource by typing *net use* ***resource name*** */delete*
- For example, if we want to delete the p drive, we type *resource p: /delete*
- If we type *net use*, we can see all of the network resources currently connected

net user

Add, remove, or change users on the computer

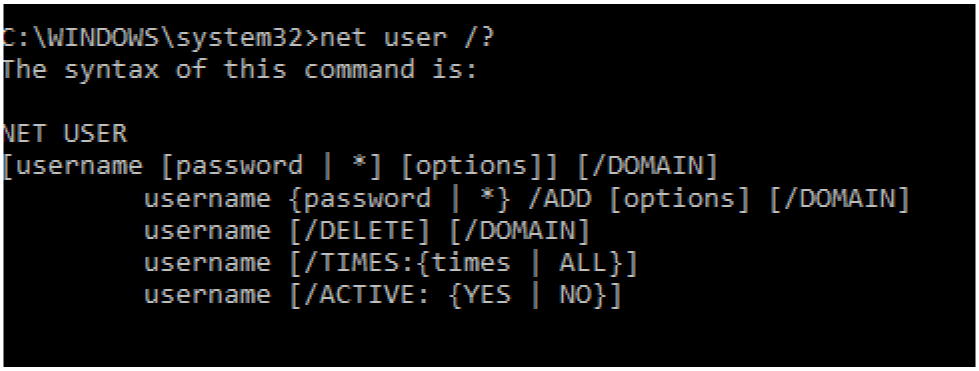
- Requires admin privileges
- Command is *net user*
  - Shows a list of all the user accounts
- *net user* ***username password***
  - Changes the password of an account, where username is the user name, and password is the password
- *net user* ***username password*** */add*
  - Adds a new account, where username is the user name, and password is the password
- *net user* ***username*** */delete*
  - Removes a user account, where username is the user name



```
C:\WINDOWS\system32>net user

User accounts for \\LAPTOP-KHL20A1U

-------------------------------------------------------------------------------
Administrator            DefaultAccount           defaultuser0
Guest                    HazimGaber               WDAGUtilityAccount
The command completed successfully.
```

[command name] /?

Provides help on the command, including all possible options



```
C:\WINDOWS\system32>net user /?
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]
```

Some commands will also display the help when you type an option incorrectly.

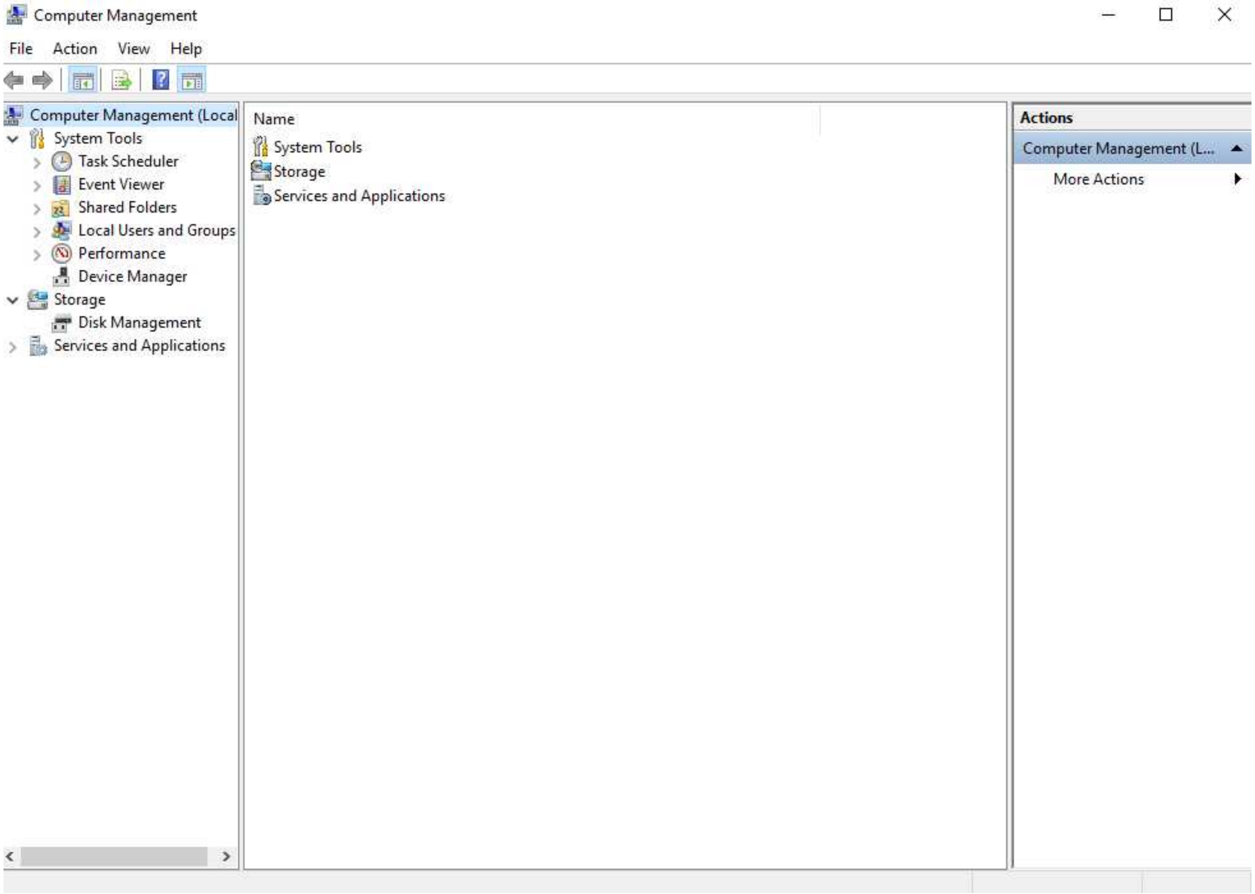
1.5 Given a scenario, use Microsoft operating system features and tools.

- Administrative
    - Computer Management
    - Device Manager
    - Local Users and Groups
    - Local Security Policy
    - Performance Monitor
    - Services
    - System Configuration
    - Task Scheduler
    - Component Services
    - Data Sources
    - Print Management
    - Windows Memory Diagnostics
    - Windows Firewall
    - Advanced Security
    - Event Viewer
    - User Account Management
- MSConfig
    - General
    - Boot
    - Services
    - Startup
    - Tools
- Task Manager
    - Applications
    - Processes
    - Performance
    - Networking
    - Users

- Disk Management
    - Drive status
    - Mounting
    - Initializing
    - Extending partitions
    - Splitting partitions
    - Shrink partitions
    - Assigning/changing drive letters
    - Adding drives
    - Adding arrays
    - Storage spaces
- System utilities
    - Regedit
    - Command
    - Services.msc
    - MMC
    - MSTSC
    - Notepad
    - Explorer
    - Msinfo32
    - DxDiag
    - Disk Defragmenter
    - System Restore
    - Windows Update

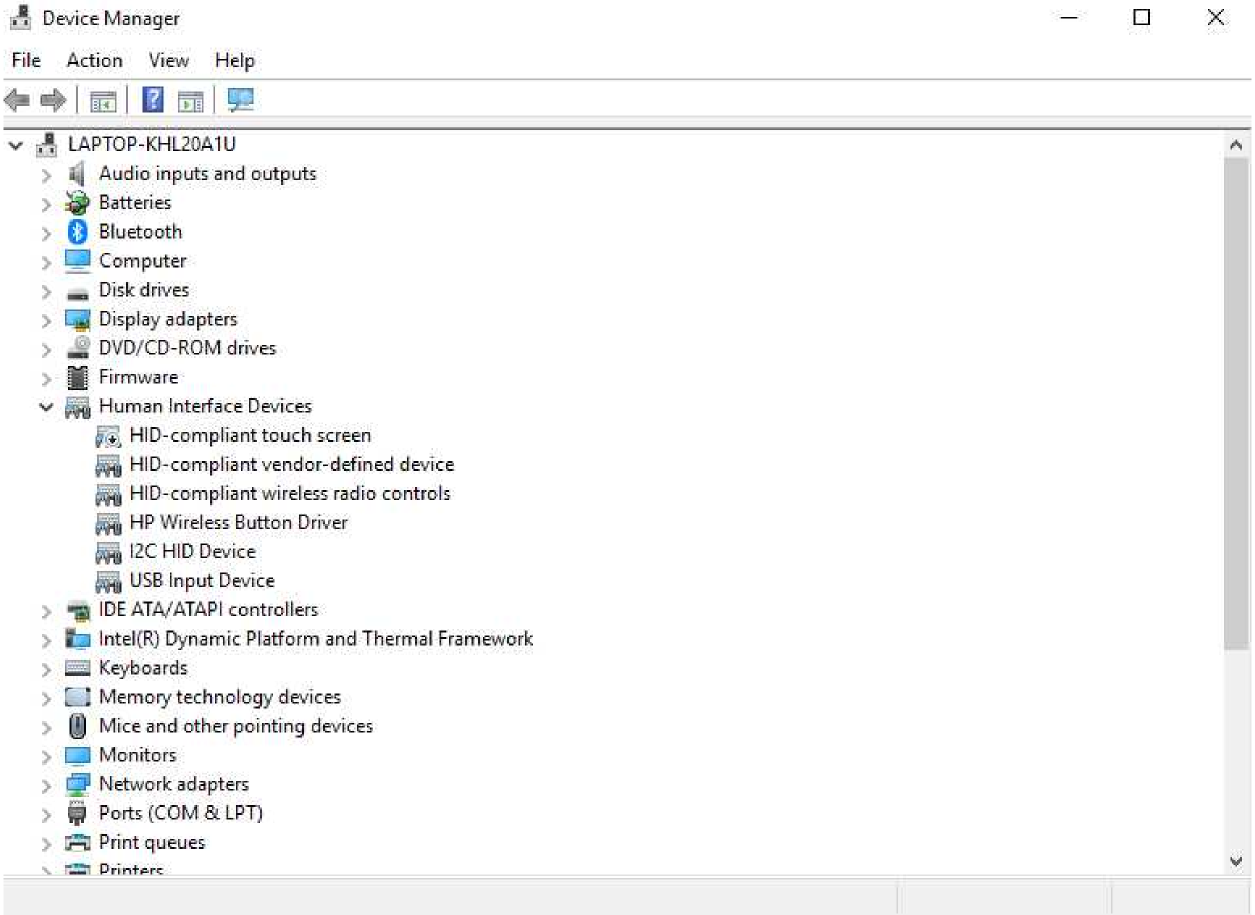
Administrative Tools - Computer Management

- Allows us to access the Task Scheduler, Event Viewer, Disk Management, and other resources (explained further on)



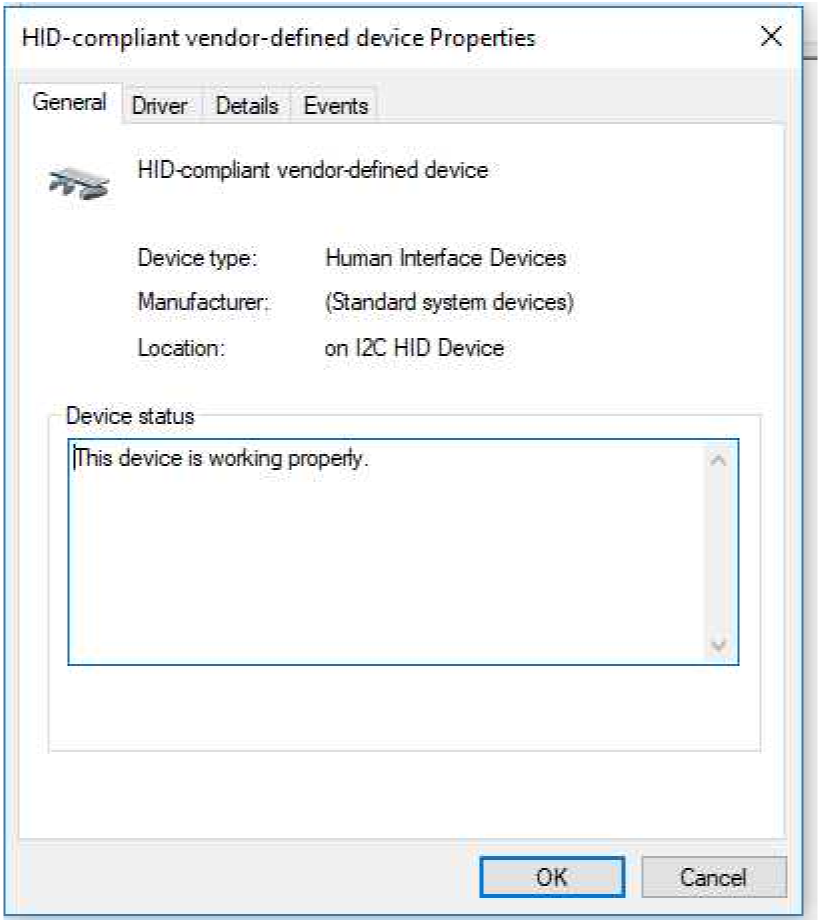
Administrative Tools – Device Manager

- Shows us a list of devices connected to the computer (internal and external)
- Devices are categorized by type
- We can use Device Manager to view, disable, enable, or configure devices



- LAPTOP-KHL20A1U
  - Audio inputs and outputs
  - Batteries
  - Bluetooth
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Firmware
  - Human Interface Devices
    - HID-compliant touch screen
    - HID-compliant vendor-defined device
    - HID-compliant wireless radio controls
    - HP Wireless Button Driver
    - I2C HID Device
    - USB Input Device
  - IDE ATA/ATAPI controllers
  - Intel(R) Dynamic Platform and Thermal Framework
  - Keyboards
  - Memory technology devices
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Ports (COM & LPT)
  - Print queues
  - Printers

- Click on a device to see its status, drivers, and settings



HID-compliant vendor-defined device

Device type: Human Interface Devices

Manufacturer: (Standard system devices)

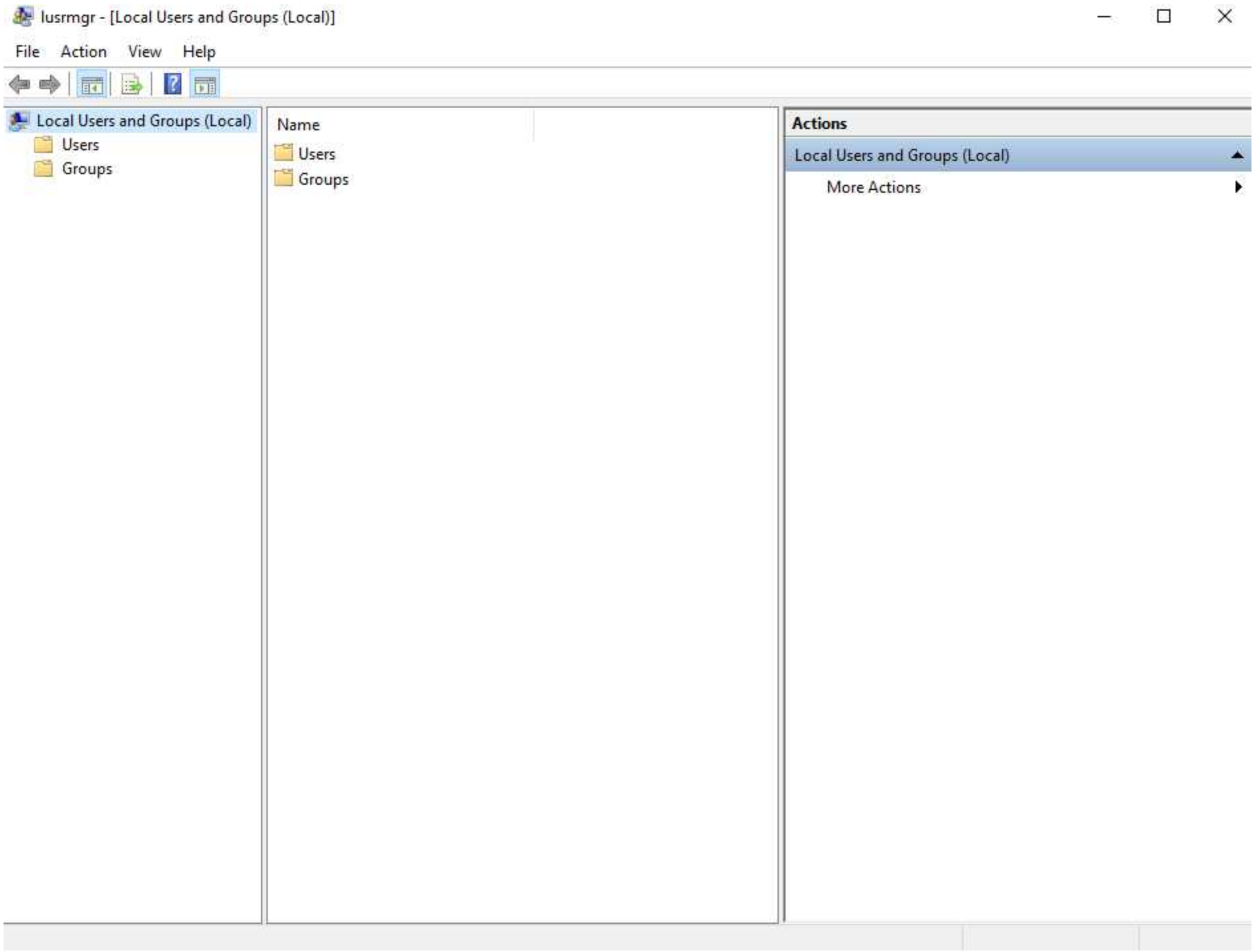
Location: on I2C HID Device

Device status

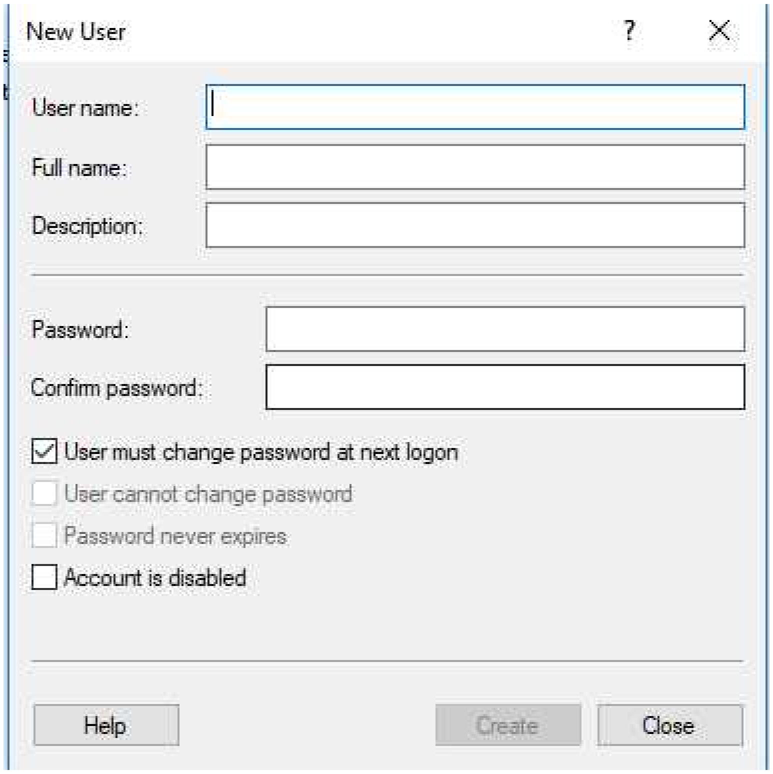
This device is working properly.

Administrative Tools - Local Users and Groups

- Shows us local users and groups
- We can use Local Users and Groups to view, create, delete, or disable user accounts


lusrmgr - [Local Users and Groups (Local)]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Users
Groups
Actions
Local Users and Groups (Local)
More Actions

- Only available in Windows Pro versions
- We can create a user or a user group
    - A group is a set of users with specific privileges
    - We can add a user to one or more groups



New User

User name:

Full name:

Description:

Password:

Confirm password:

☑ User must change password at next logon

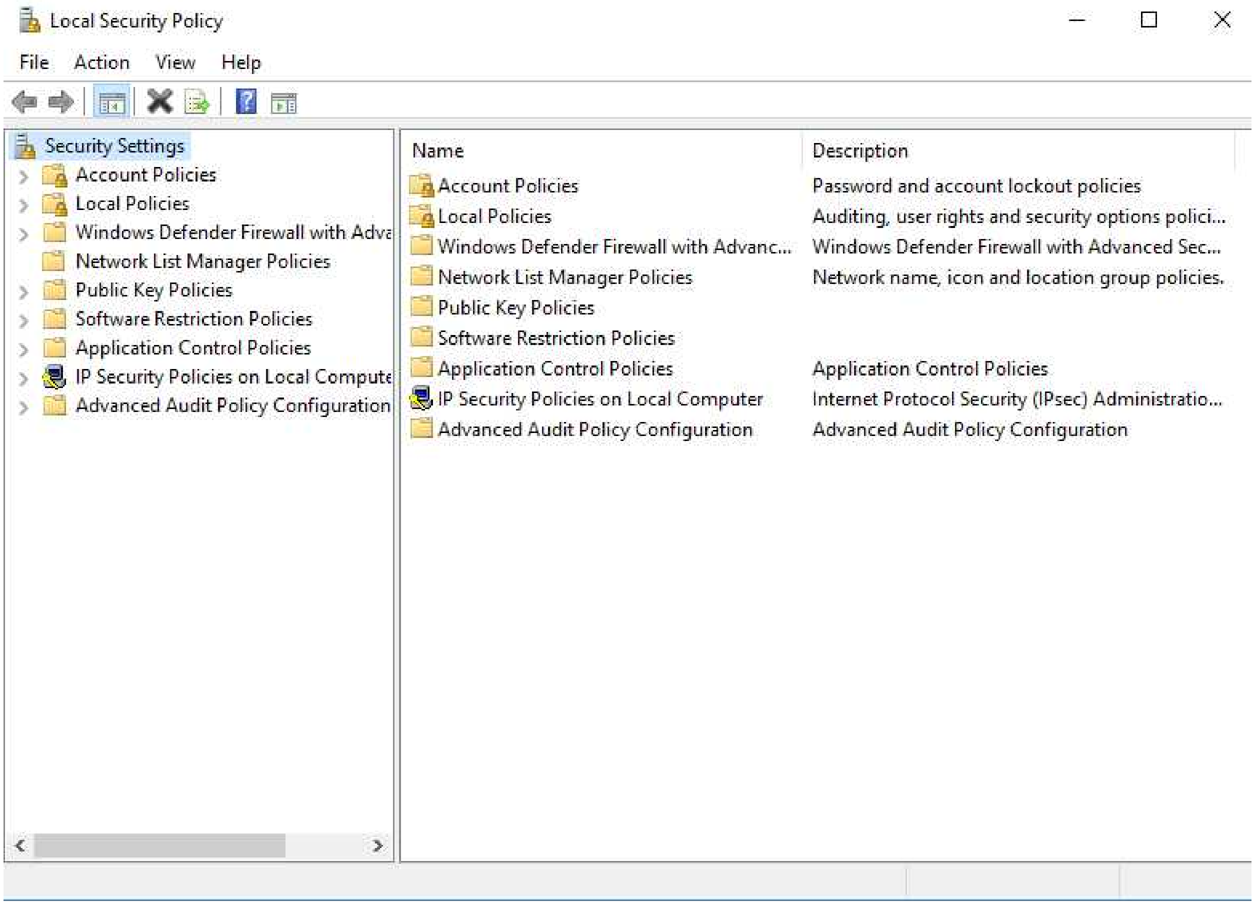
□ User cannot change password

□ Password never expires

□ Account is disabled

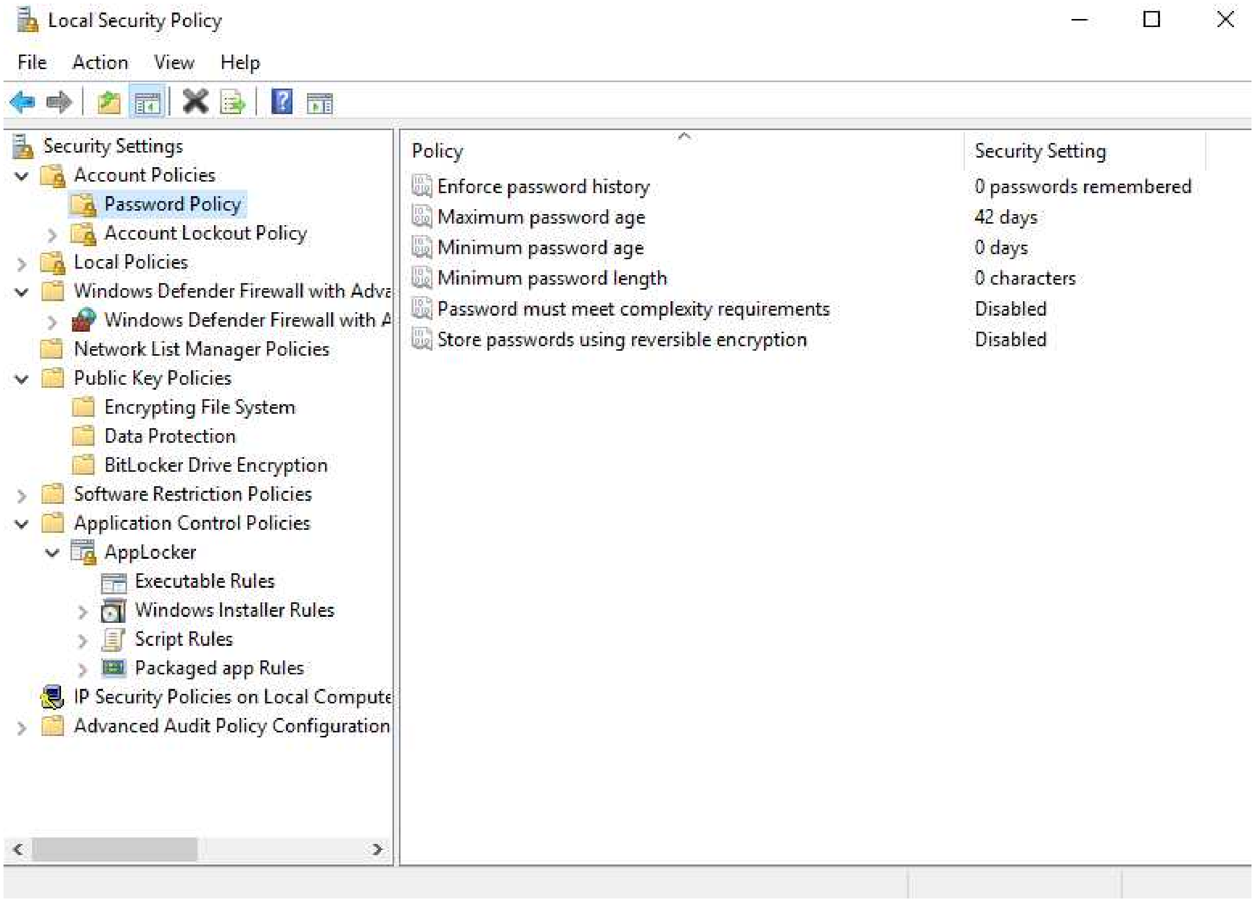
Administrative Tools – Local Security Policy

- Allows us to set security policies on the computer
- Policies are categorized by type
- We can use Local Security Policy to create or modify security policies


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

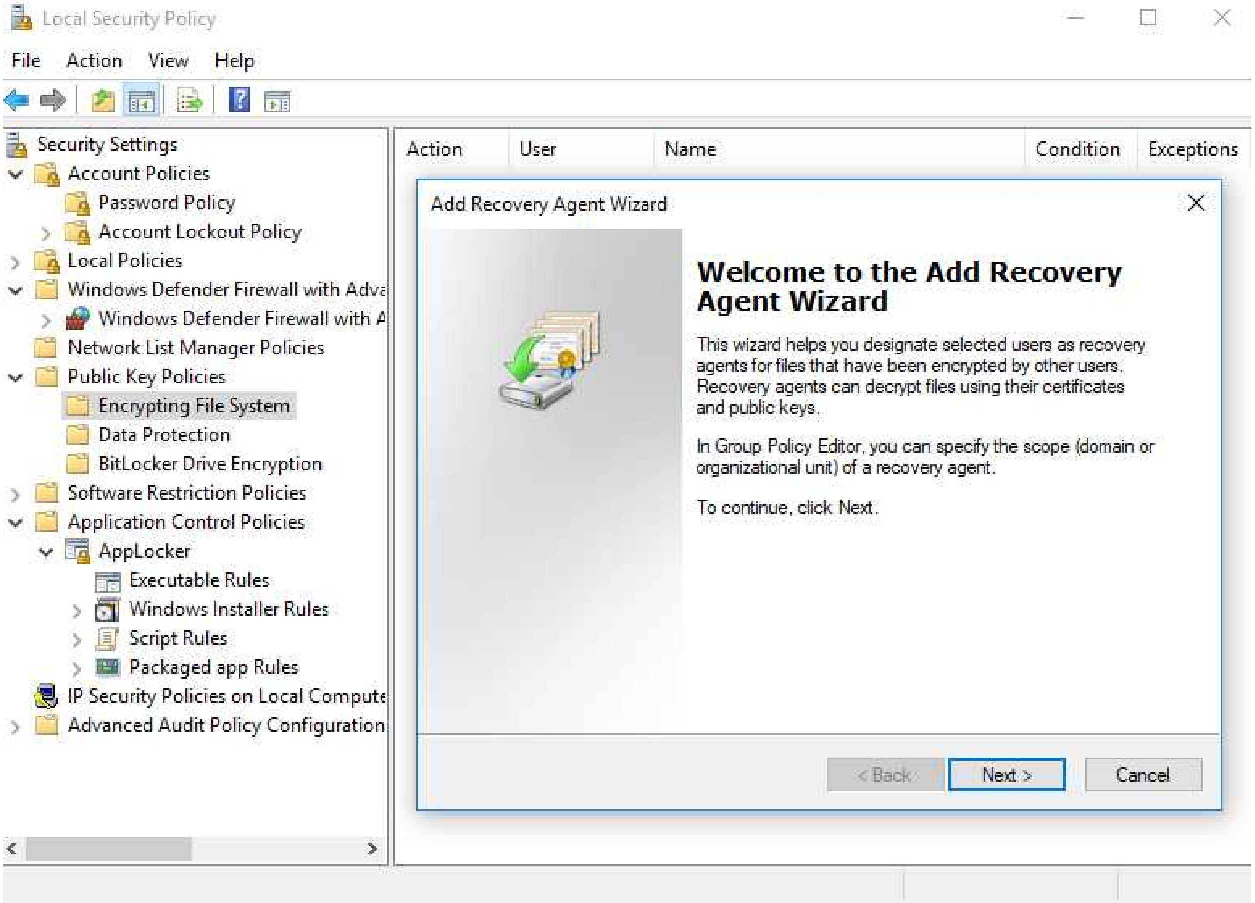
Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

- Some policies are predefined and can be edited (for example, password policy)



Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

- Other policies can be created through a wizard



Welcome to the Add Recovery Agent Wizard

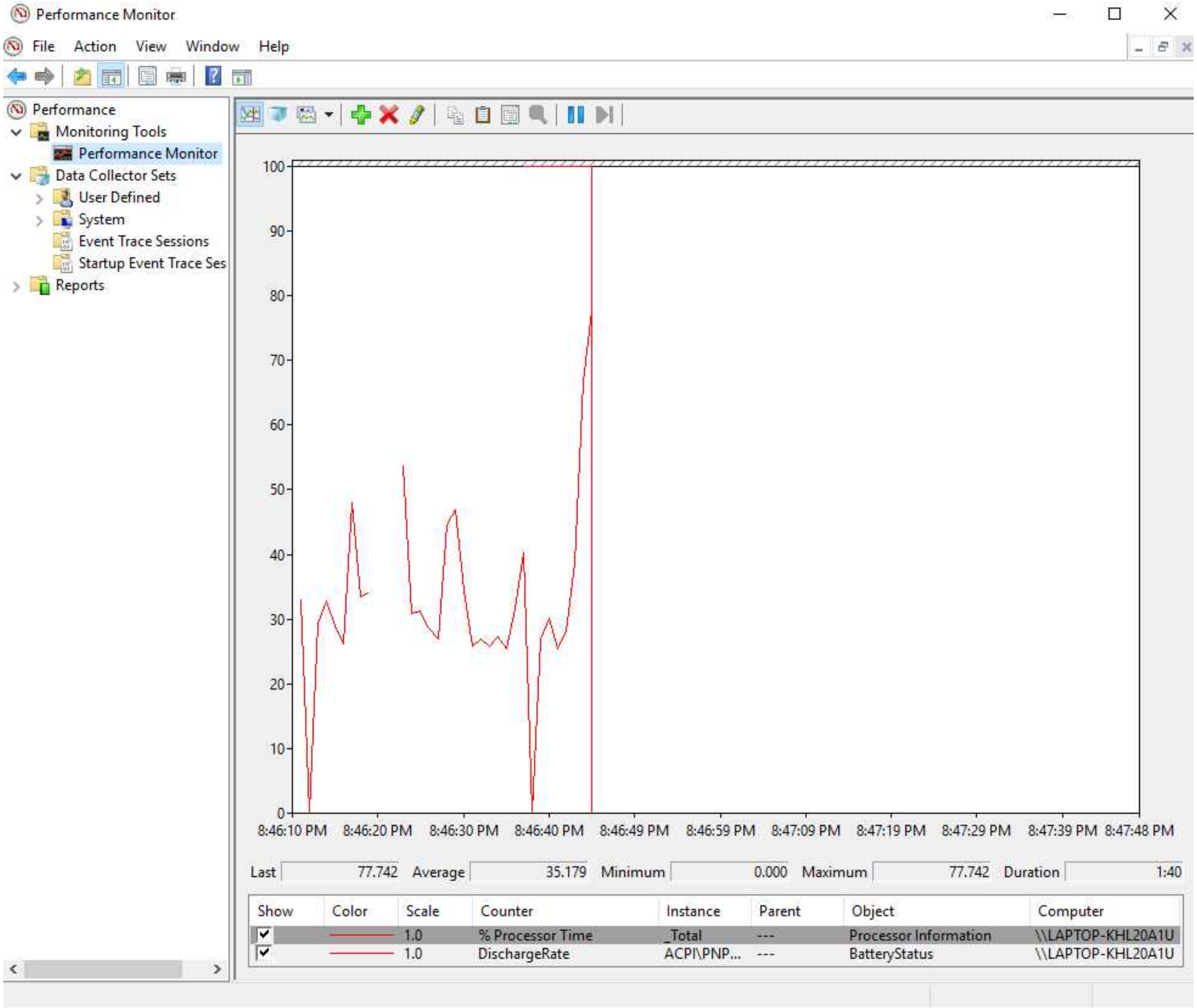
This wizard helps you designate selected users as recovery agents for files that have been encrypted by other users. Recovery agents can decrypt files using their certificates and public keys.

In Group Policy Editor, you can specify the scope (domain or organizational unit) of a recovery agent.

To continue, click Next.

Administrative Tools - Performance Monitor

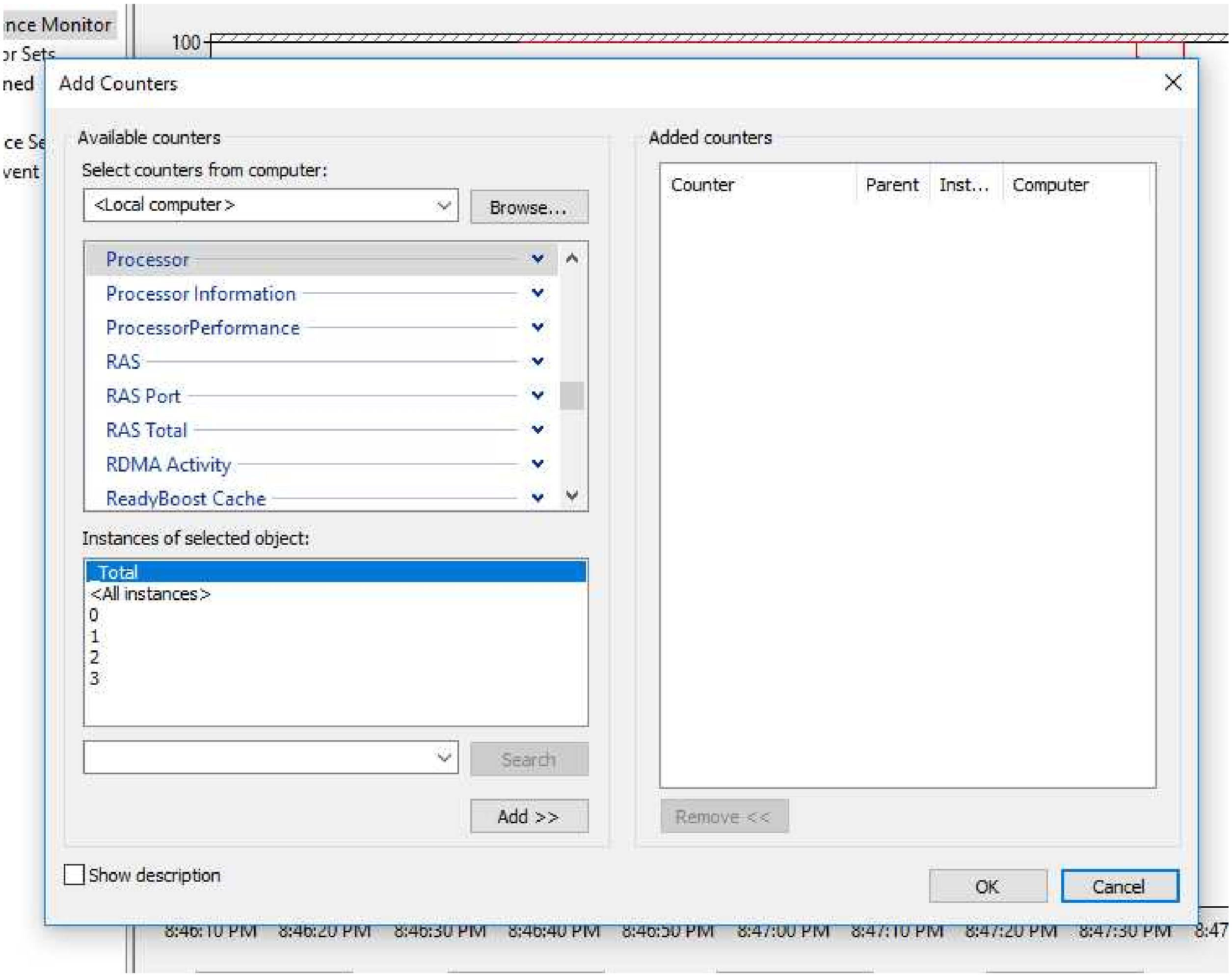
- Allows us to monitor different system resources
- We can use the performance monitor to measure system resources, which could identify sources of error or poor performance



Last 77.742 Average 35.179 Minimum 0.000 Maximum 77.742 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	—	1.0	% Processor Time	_Total	---	Processor Information	\\LAPTOP-KHL20A1U
☑	—	1.0	DischargeRate	ACPI\PNP...	---	BatteryStatus	\\LAPTOP-KHL20A1U

- We can add additional items to track



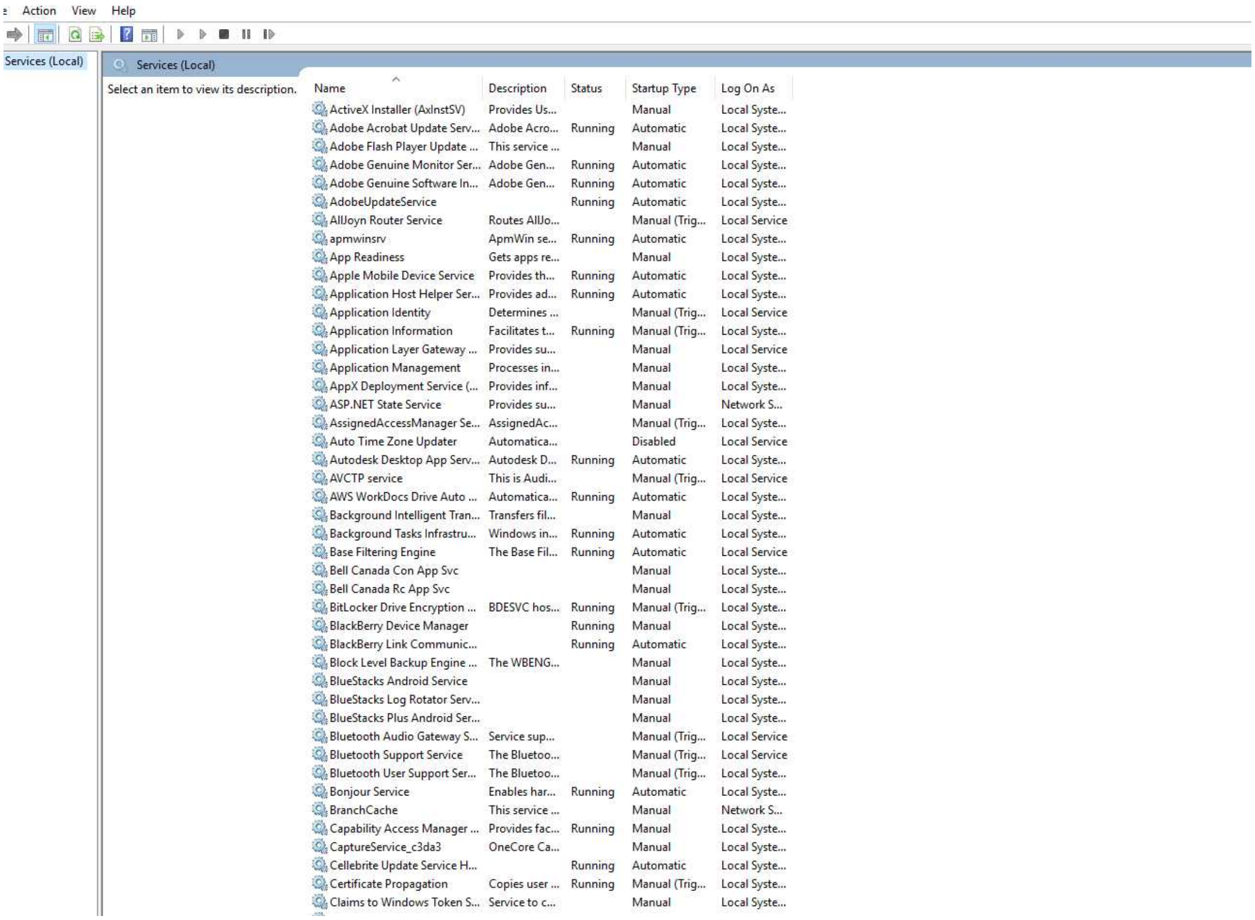
Add Counters

Select counters from computer: <Local computer>

Instances of selected object: _Total

Administrative Tools – Services

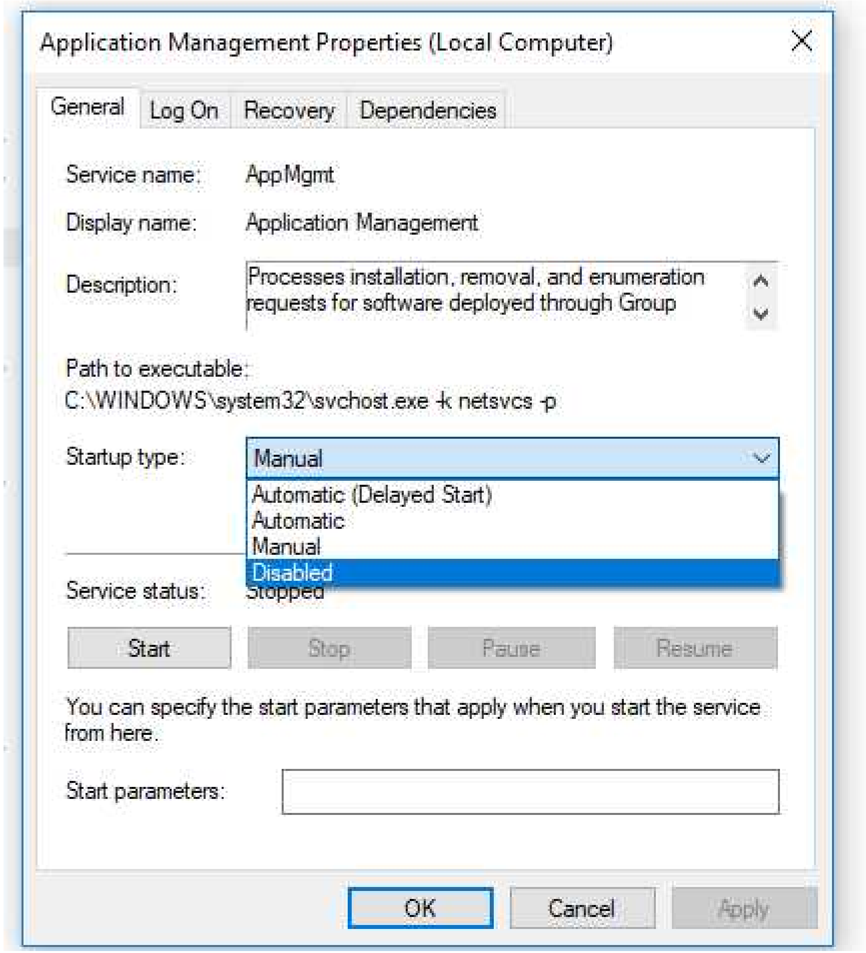
- Shows us all the installed services
    - A service is a program that runs in the background
- We can use Services to view, start, stop, restart, or disable services
- Services can cause errors or impact performance



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
Adobe Flash Player Update ...	This service ...		Manual	Local Syste...
Adobe Genuine Monitor Ser...	Adobe Gen...	Running	Automatic	Local Syste...
Adobe Genuine Software In...	Adobe Gen...	Running	Automatic	Local Syste...
AdobeUpdateService		Running	Automatic	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
apmwinsrv	ApmWin se...	Running	Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Apple Mobile Device Service	Provides th...	Running	Automatic	Local Syste...
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...		Manual	Local Syste...
ASP.NET State Service	Provides su...		Manual	Network S...
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
Autodesk Desktop App Serv...	Autodesk D...	Running	Automatic	Local Syste...
AVCTP service	This is Audi...		Manual (Trig...	Local Service
AWS WorkDocs Drive Auto ...	Automatica...	Running	Automatic	Local Syste...
Background Intelligent Tran...	Transfers fil...		Manual	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Bell Canada Con App Svc			Manual	Local Syste...
Bell Canada Rc App Svc			Manual	Local Syste...
BitLocker Drive Encryption ...	BDESVC hos...	Running	Manual (Trig...	Local Syste...
BlackBerry Device Manager		Running	Manual	Local Syste...
BlackBerry Link Communic...		Running	Automatic	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
BlueStacks Android Service			Manual	Local Syste...
BlueStacks Log Rotator Serv...			Manual	Local Syste...
BlueStacks Plus Android Ser...			Manual	Local Syste...
Bluetooth Audio Gateway S...	Service sup...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...		Manual (Trig...	Local Syste...
Bonjour Service	Enables har...	Running	Automatic	Local Syste...
BranchCache	This service ...		Manual	Network S...
Capability Access Manager ...	Provides fac...	Running	Manual	Local Syste...
CaptureService_c3da3	OneCore Ca...		Manual	Local Syste...
Cellebrite Update Service H...		Running	Automatic	Local Syste...
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Local Syste...
Claims to Windows Token S...	Service to c...		Manual	Local Syste...

- A service can run manually (user must manually run it, or application must trigger it) or automatically. A service can also be disabled
- A service may have dependencies
    - A dependency is a service required for another service to operate



Application Management Properties (Local Computer)

Service name: AppMgmt

Display name: Application Management

Description: Processes installation, removal, and enumeration requests for software deployed through Group

Path to executable:
C:\WINDOWS\system32\svchost.exe -k netsvcs -p

Startup type: Manual

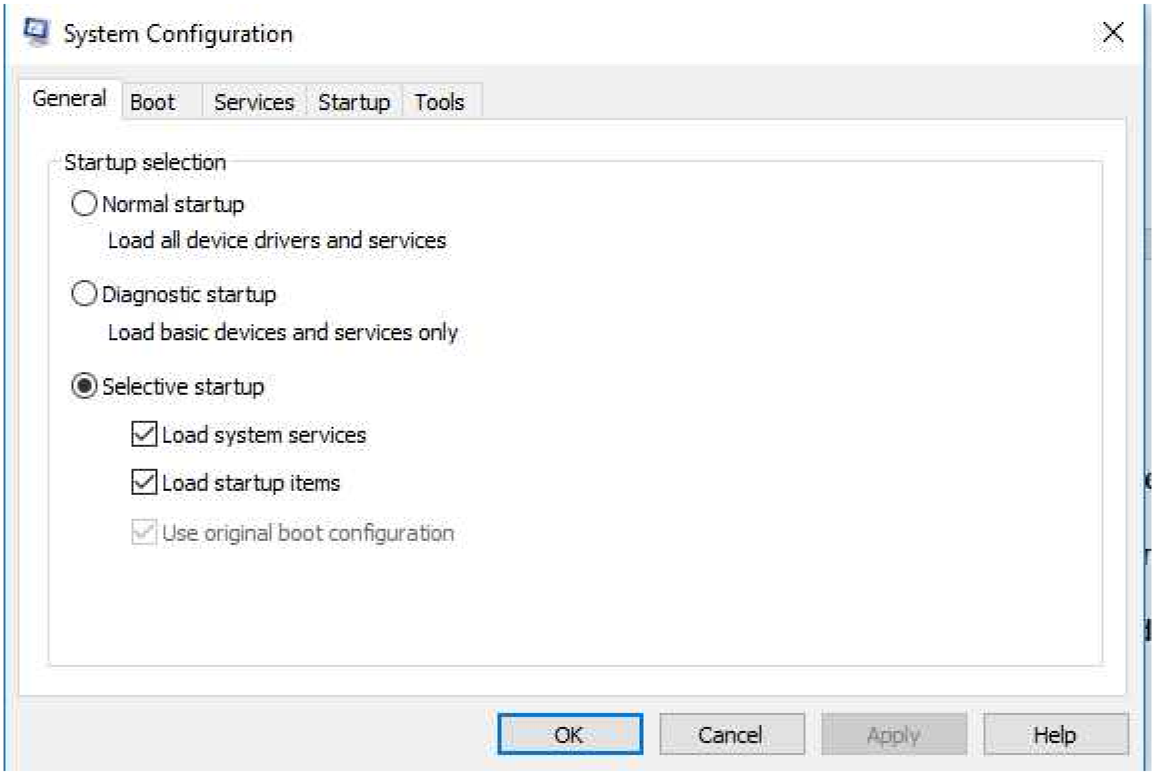
Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Administrative Tools – System Configuration

- Also known as msconfig
- Shows us the start up menu, start up selection, and provides some tools
- Will be discussed in more detail
- We can use services to modify the services that start up when the computer does



Startup selection

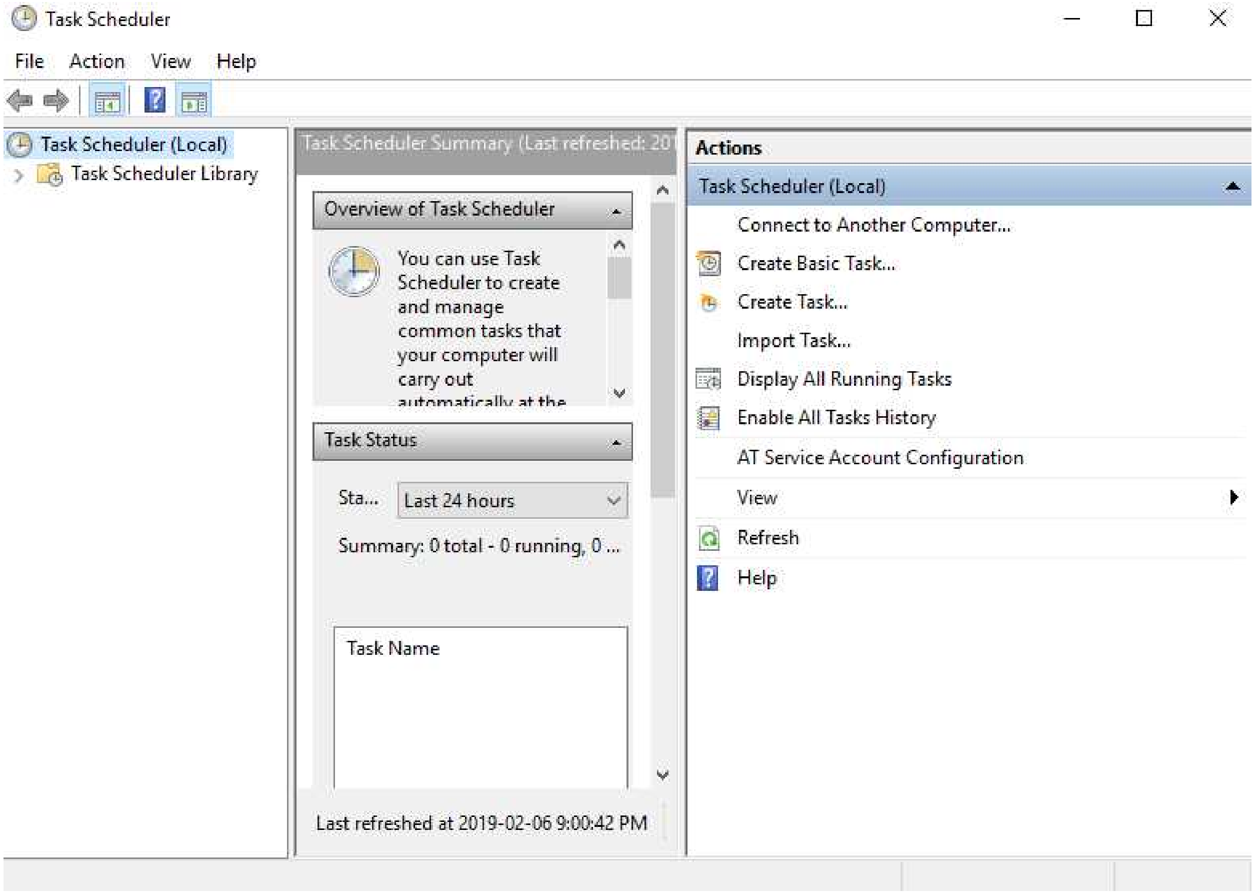
○ Normal startup
Load all device drivers and services

○ Diagnostic startup
Load basic devices and services only

● Selective startup
☑ Load system services
☑ Load startup items
☑ Use original boot configuration

Administrative Tools – Task Scheduler

- Allows us to create, delete, or modify automated tasks
- For example, we might create a task to automatically run an antivirus program each day

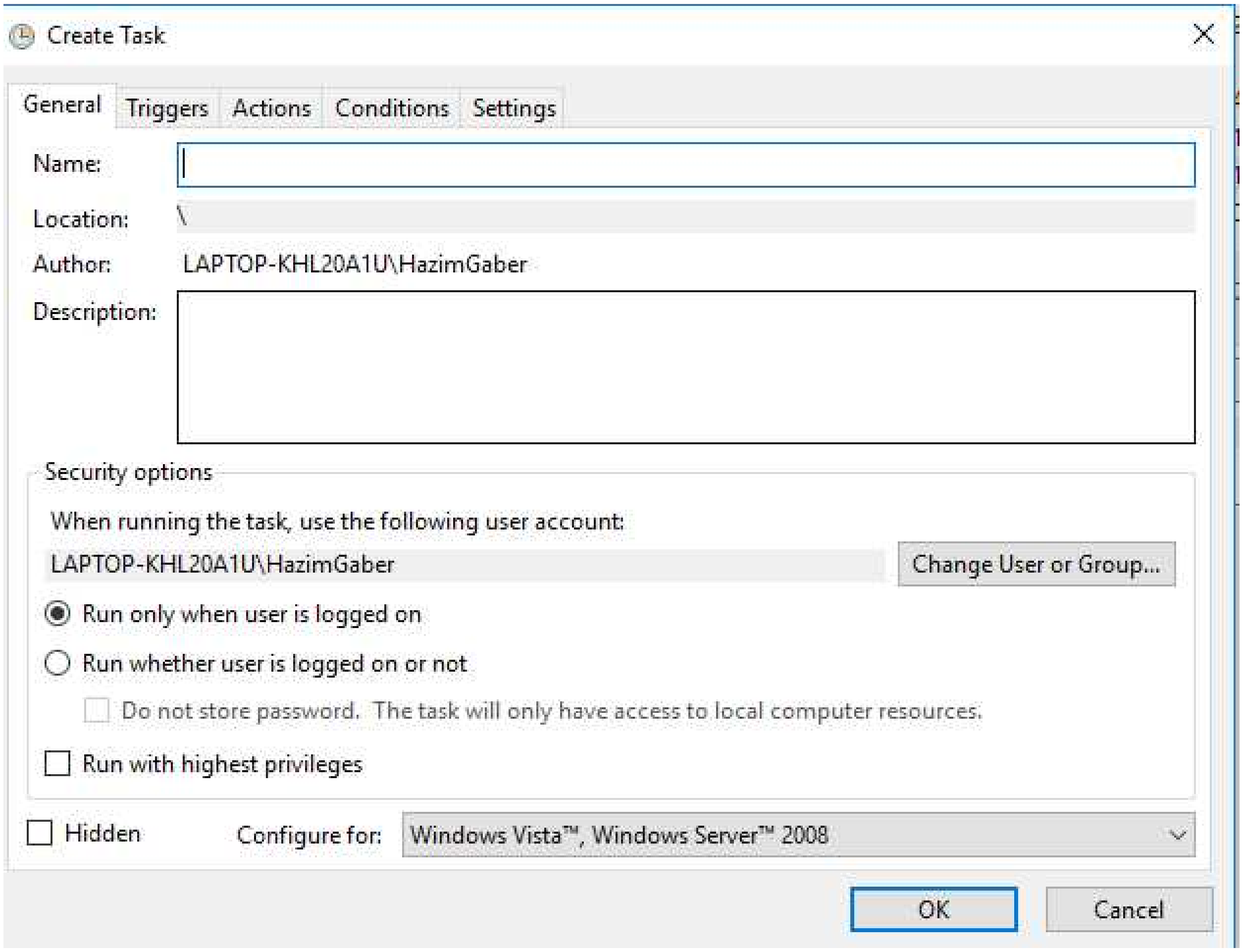


You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the

Summary: 0 total - 0 running, 0 ...

Last refreshed at 2019-02-06 9:00:42 PM

- A task must have a name and may have a description



Name:

Location: \

Author: LAPTOP-KHL20A1U\HazimGaber

Description:

Security options

When running the task, use the following user account:

LAPTOP-KHL20A1U\HazimGaber

● Run only when user is logged on

○ Run whether user is logged on or not

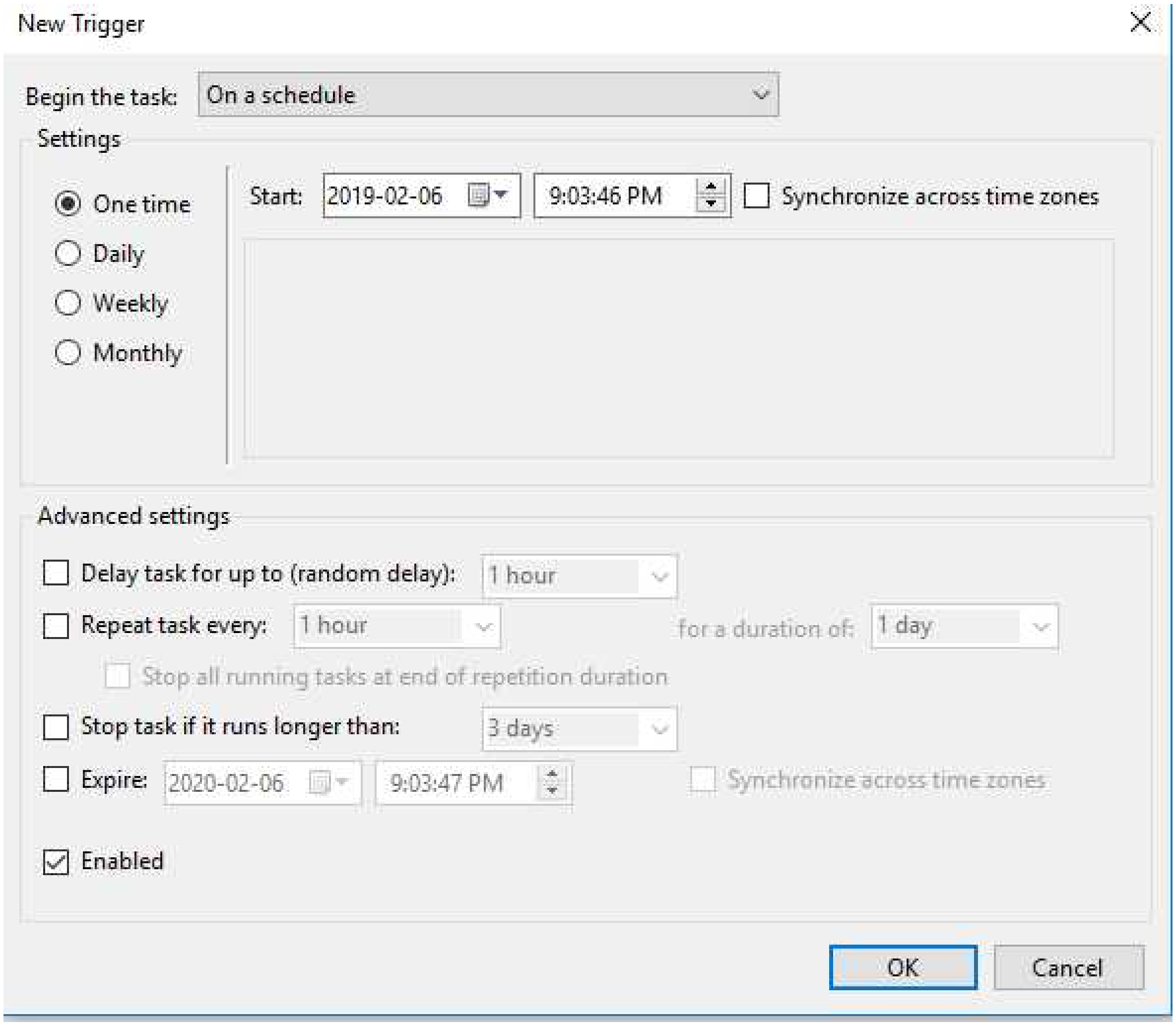
□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

- A task will have one or more triggers
  - A trigger is a scenario or event that causes the task to execute
  - A trigger could be a time (the task may run daily, hourly, weekly, on week days, etc.)



New Trigger

Begin the task: On a schedule

Settings

● One time
○ Daily
○ Weekly
○ Monthly

Start: 2019-02-06 9:03:46 PM □ Synchronize across time zones

Advanced settings

□ Delay task for up to (random delay): 1 hour

□ Repeat task every: 1 hour for a duration of: 1 day

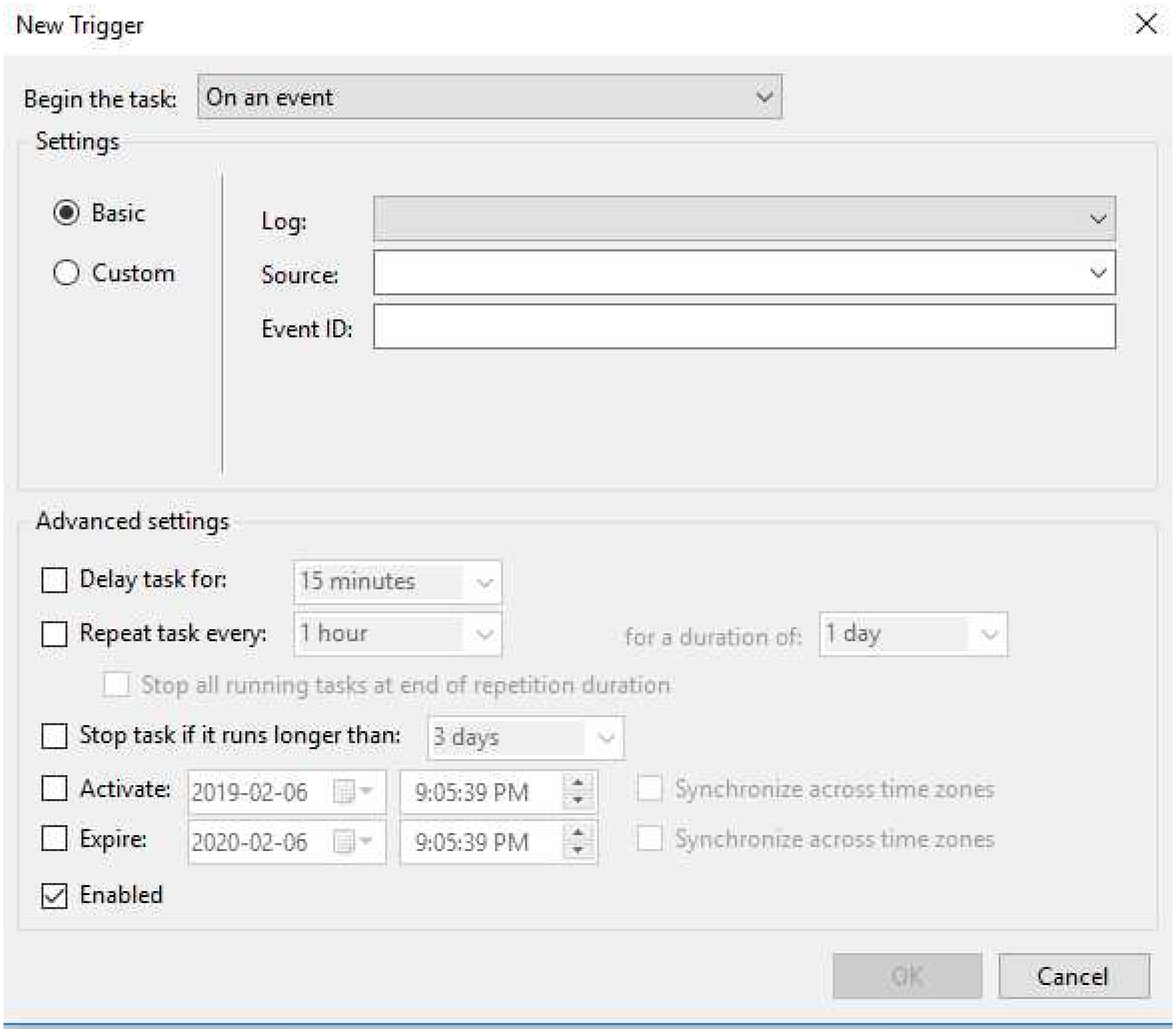
□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 2020-02-06 9:03:47 PM □ Synchronize across time zones

☑ Enabled

- A trigger could be an event (for example, system start up, network connection, program crash)



New Trigger

Begin the task: On an event

Settings

● Basic

○ Custom

Log:

Source:

Event ID:

Advanced settings

□ Delay task for: 15 minutes

□ Repeat task every: 1 hour for a duration of: 1 day

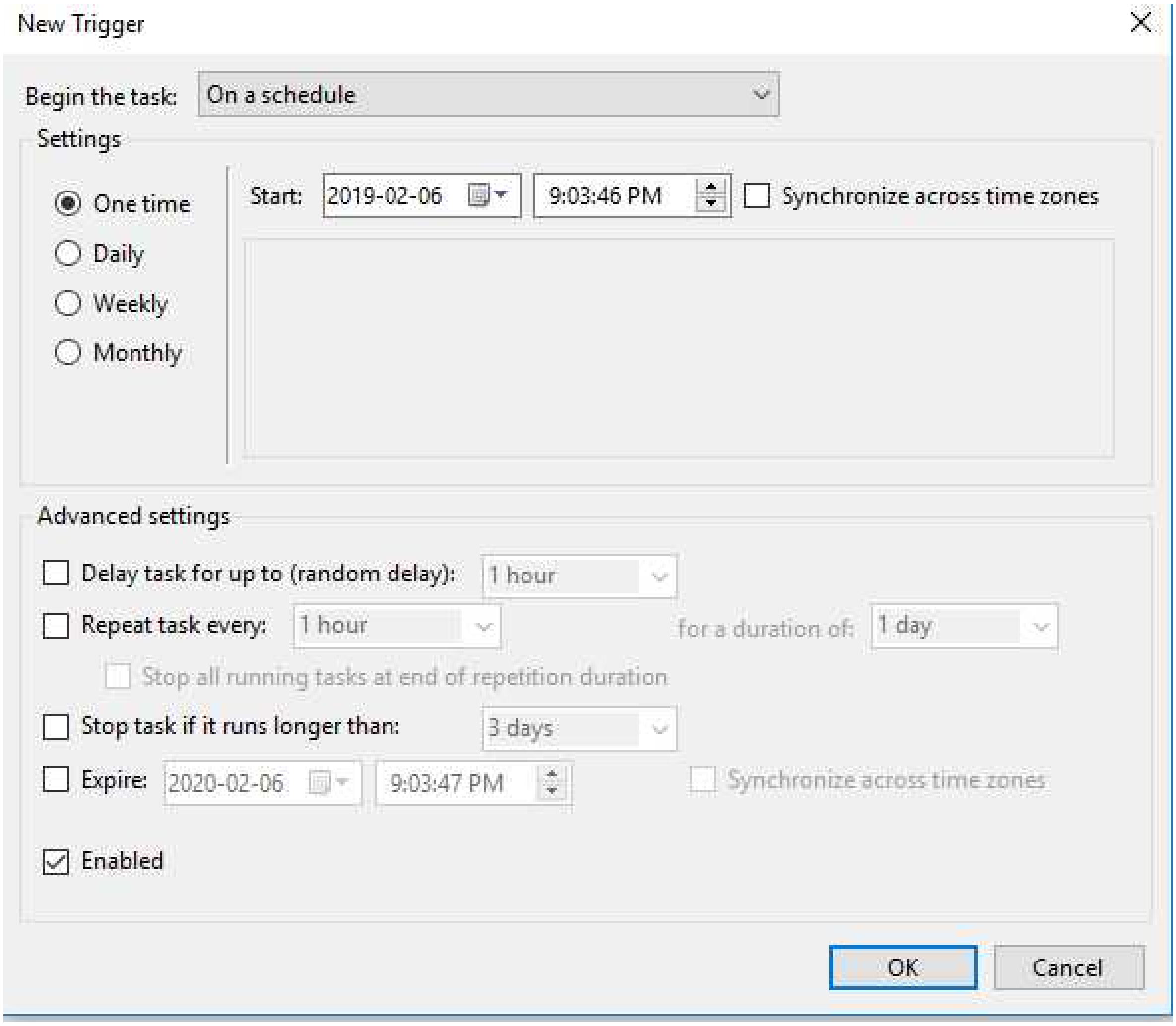
□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Activate: 2019-02-06 9:05:39 PM □ Synchronize across time zones

□ Expire: 2020-02-06 9:05:39 PM □ Synchronize across time zones

☑ Enabled



New Trigger

Begin the task: On a schedule

Settings

● One time
○ Daily
○ Weekly
○ Monthly

Start: 2019-02-06 9:03:46 PM □ Synchronize across time zones

Advanced settings

□ Delay task for up to (random delay): 1 hour

□ Repeat task every: 1 hour for a duration of: 1 day

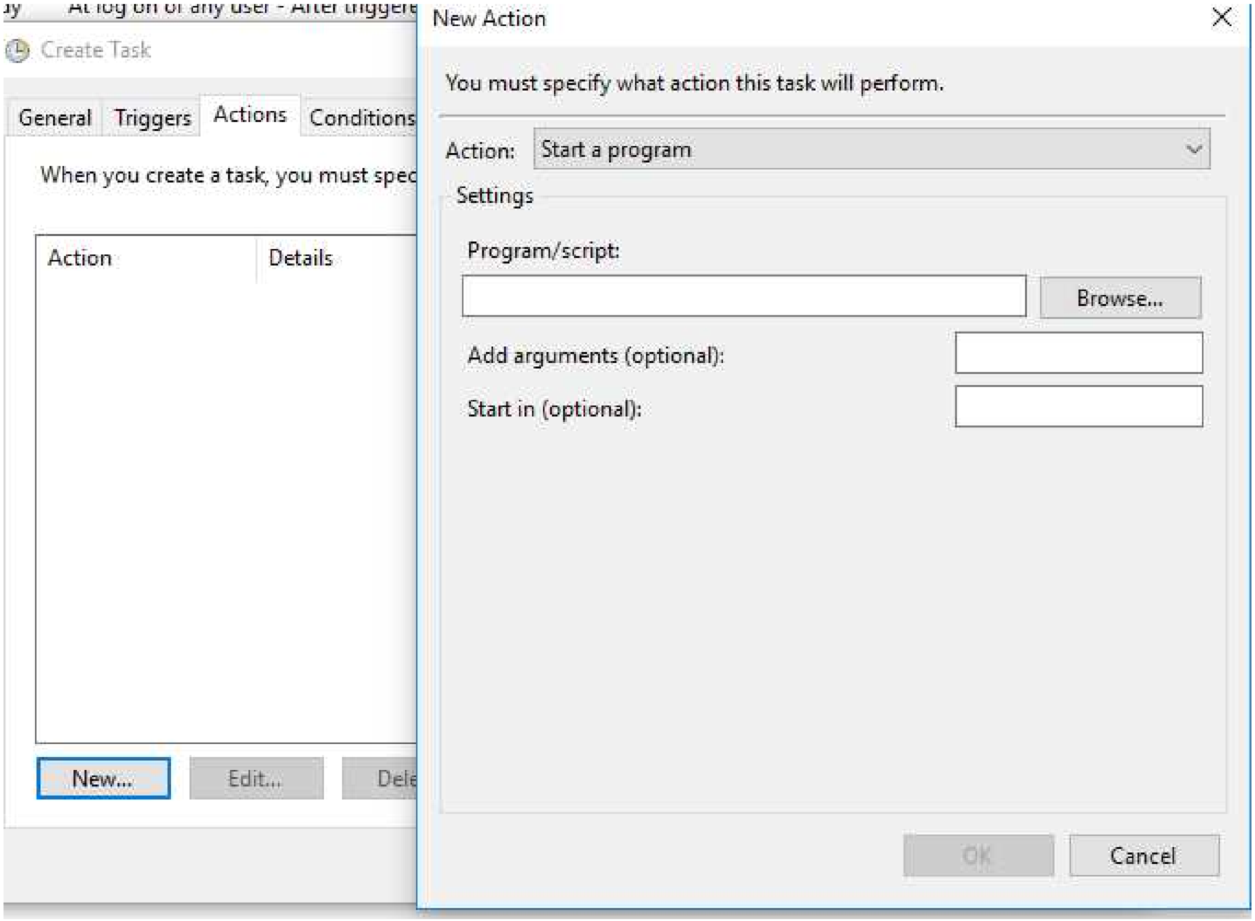
□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 2020-02-06 9:03:47 PM □ Synchronize across time zones

☑ Enabled

- A task will have one or more actions
  - An action is something that the task must do (run a program, establish a connection, execute a script, etc.)

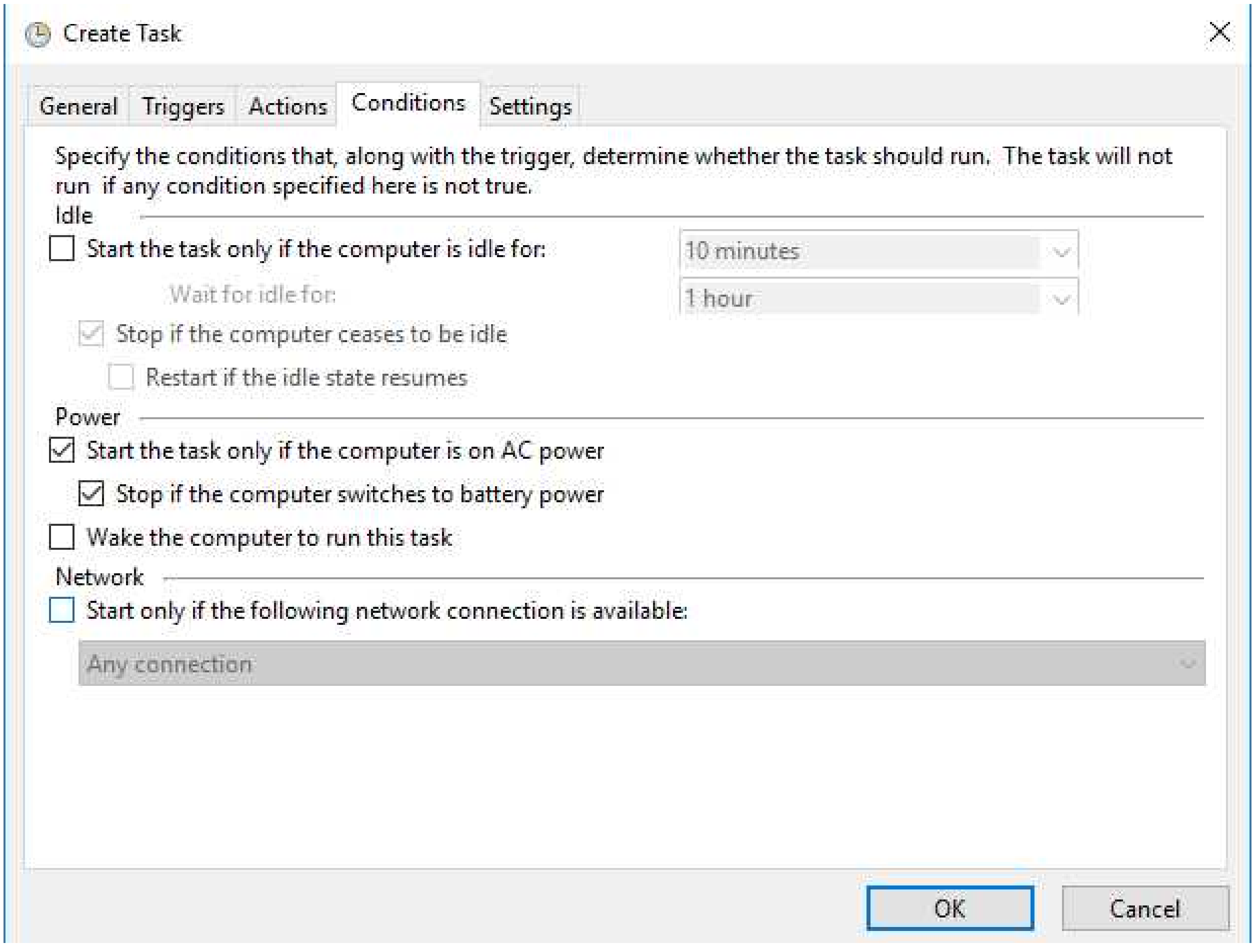


When you create a task, you must spec

You must specify what action this task will perform.

Action: Start a program

- We can also set conditions for the task



Create Task

General | Triggers | Actions | Conditions | Settings

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 10 minutes

Wait for idle for: 1 hour

☑ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

☑ Start the task only if the computer is on AC power

☑ Stop if the computer switches to battery power

□ Wake the computer to run this task

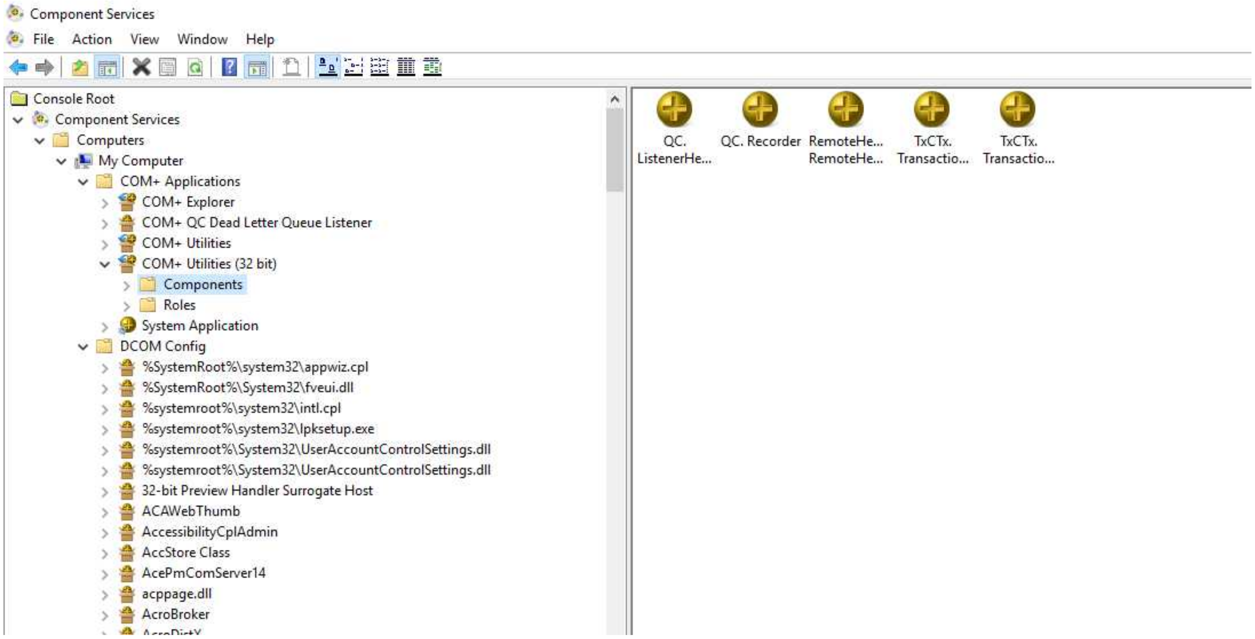
Network

□ Start only if the following network connection is available:

Any connection

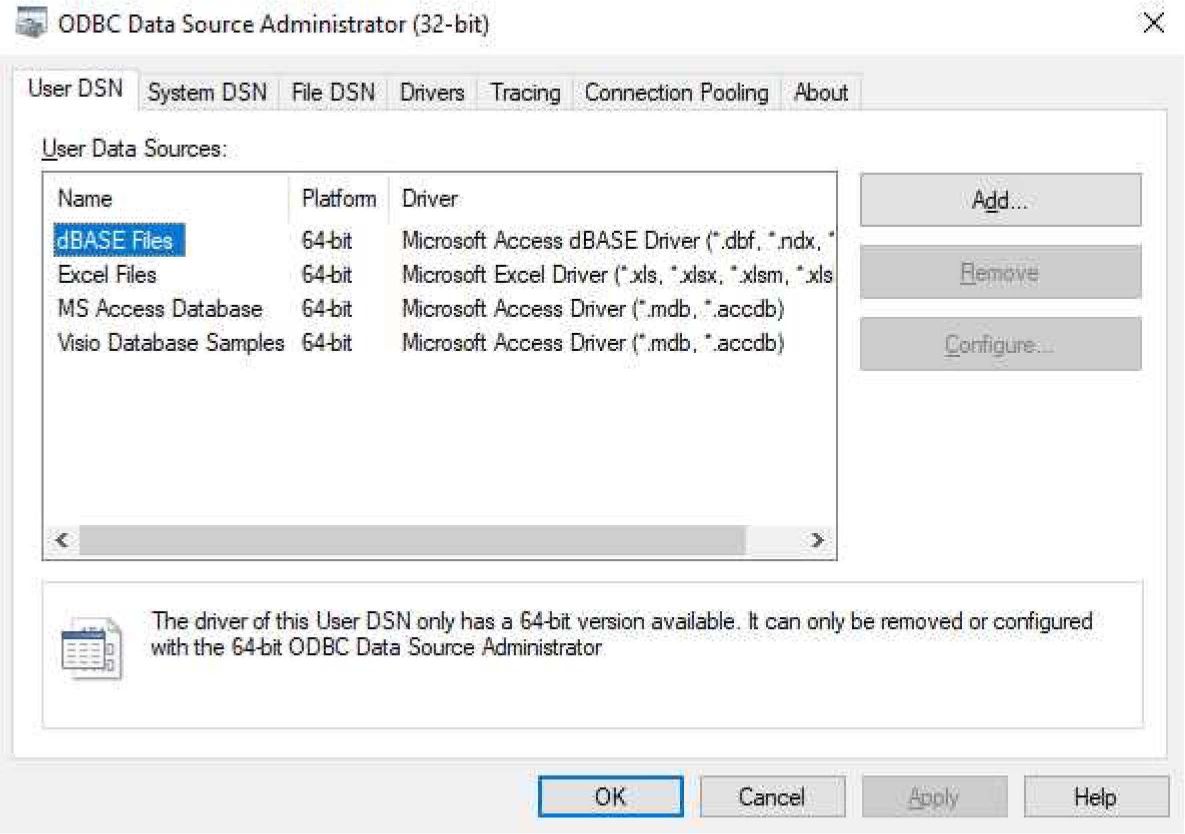
Administrative Tools – Component Services

- Manages COM+ and DCOM components
- COM+ and DCOM are Windows plug ins that allow developers to create applications that run smoothly and scale better



Administrative Tools – Data Sources

- Data Sources lists the databases that the computer can connect to

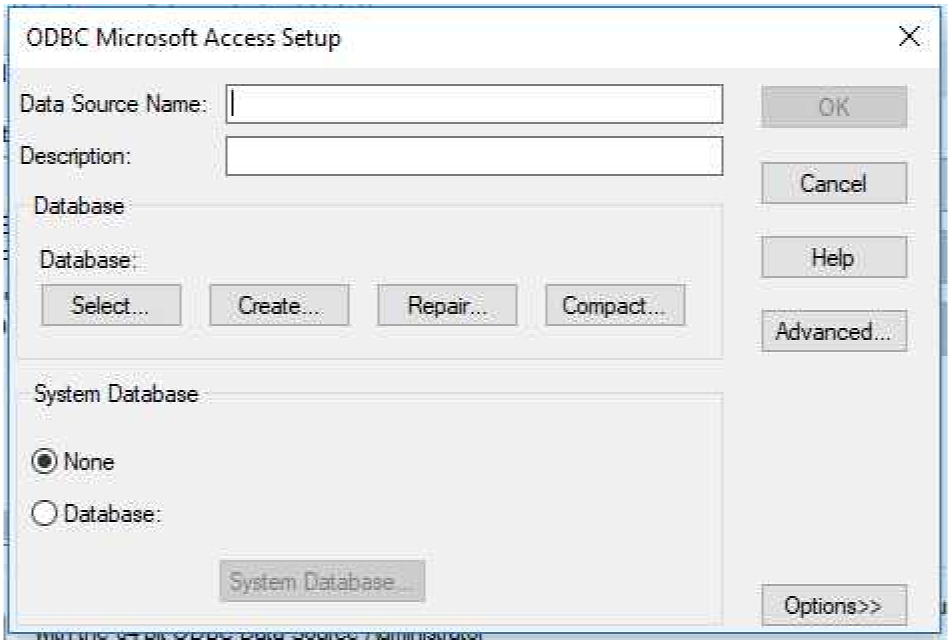


User Data Sources:

Name	Platform	Driver
dBASE Files	64-bit	Microsoft Access dBASE Driver (*.dbf, *.ndx, *
Excel Files	64-bit	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.xls
MS Access Database	64-bit	Microsoft Access Driver (*.mdb, *.accdb)
Visio Database Samples	64-bit	Microsoft Access Driver (*.mdb, *.accdb)

The driver of this User DSN only has a 64-bit version available. It can only be removed or configured with the 64-bit ODBC Data Source Administrator

- We can add a new database to the system by specifying the database type, name, and location
  - Once a database is added to the data source, other applications can connect to the database by simply mentioning its name

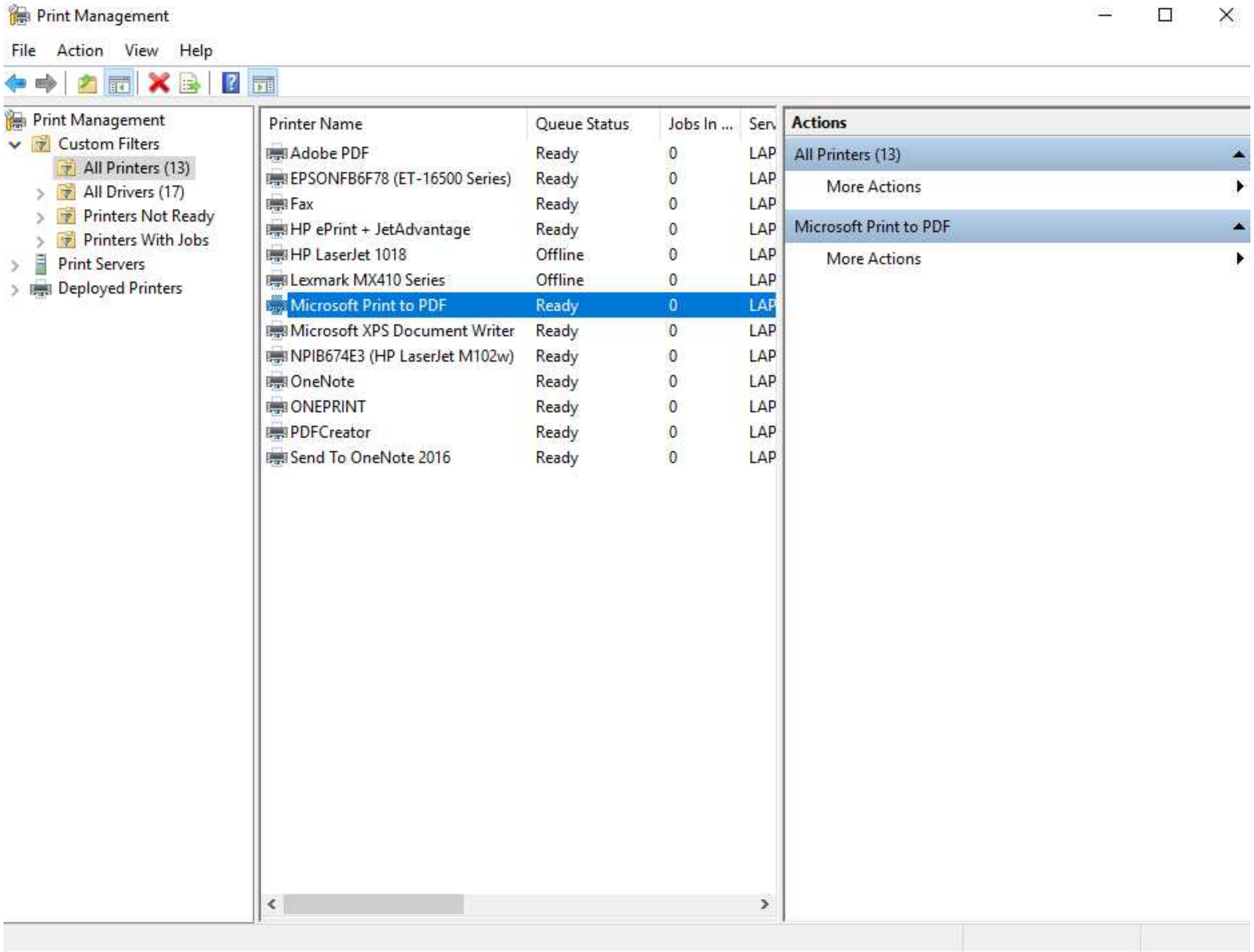


● None

○ Database:

Administrative Tools – Print Management

- Allows us to view and delete printers installed on the computer



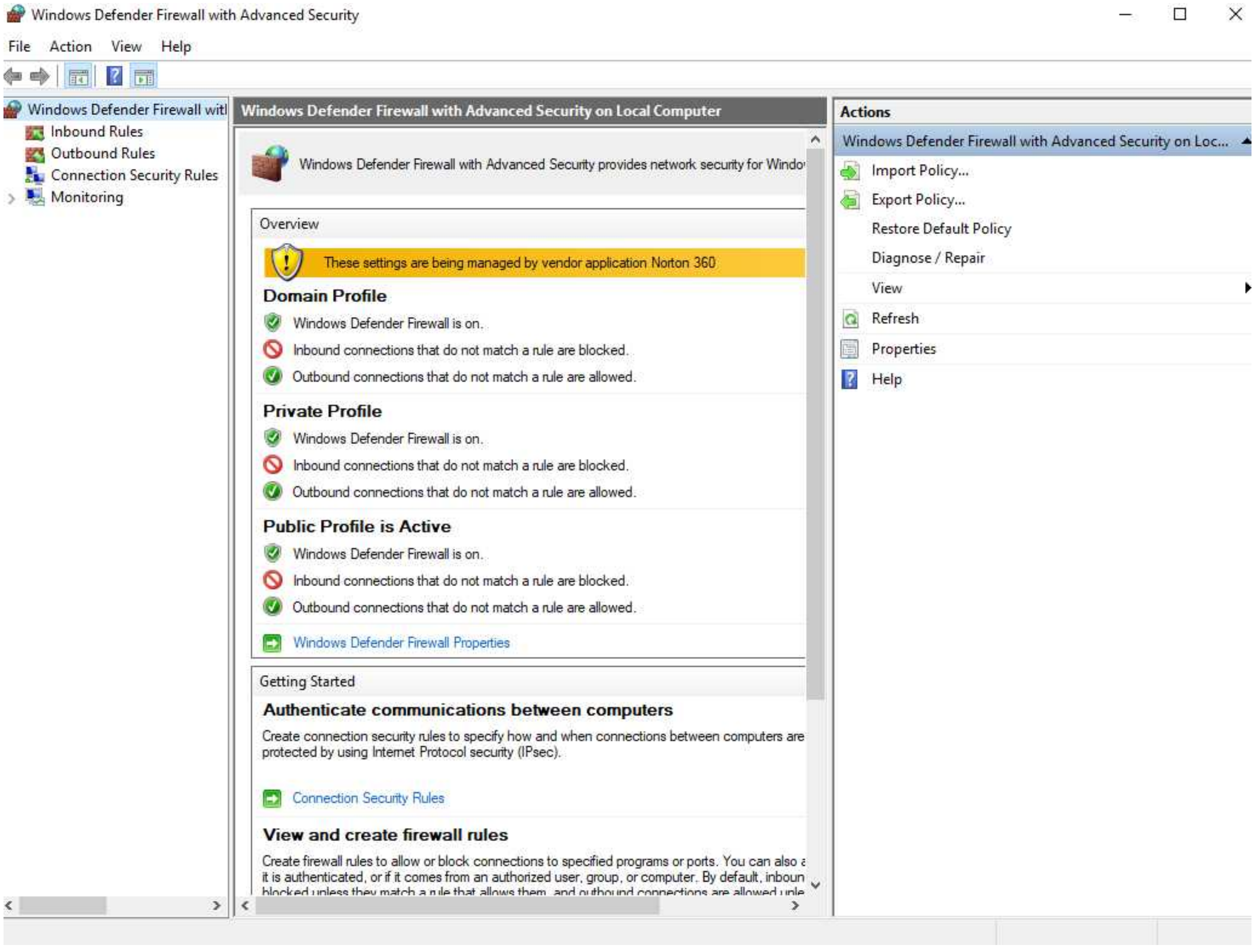
Printer Name	Queue Status	Jobs In ...	Serv
Adobe PDF	Ready	0	LAP
EPSONFB6F78 (ET-16500 Series)	Ready	0	LAP
Fax	Ready	0	LAP
HP ePrint + JetAdvantage	Ready	0	LAP
HP LaserJet 1018	Offline	0	LAP
Lexmark MX410 Series	Offline	0	LAP
Microsoft Print to PDF	Ready	0	LAP
Microsoft XPS Document Writer	Ready	0	LAP
NPIB674E3 (HP LaserJet M102w)	Ready	0	LAP
OneNote	Ready	0	LAP
ONEPRINT	Ready	0	LAP
PDFCreator	Ready	0	LAP
Send To OneNote 2016	Ready	0	LAP

Administrative Tools – Windows Memory Diagnostics

- Diagnoses errors with the memory (RAM)
- The diagnostics runs when the computer restarts

Administrative Tools – Windows Firewall

- Allows us to set rules that permit or deny traffic on our computer
- The Firewall may be disabled and managed by an antivirus application (such as Norton Antivirus)
- We can create an Inbound Rule
    - Affects traffic that is entering
- We can create an Outbound Rule
    - Affects traffic that is leaving
- A rule can be set to block traffic (a blacklist) or allow traffic (whitelist)
    - For example, in a highly secured environment, we can block all traffic, and then only allow (whitelist) specific sources


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Windows Defender Firewall with Advanced Security on Loc...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windo

Overview

These settings are being managed by vendor application Norton 360

Domain Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are protected by using Internet Protocol security (IPsec).

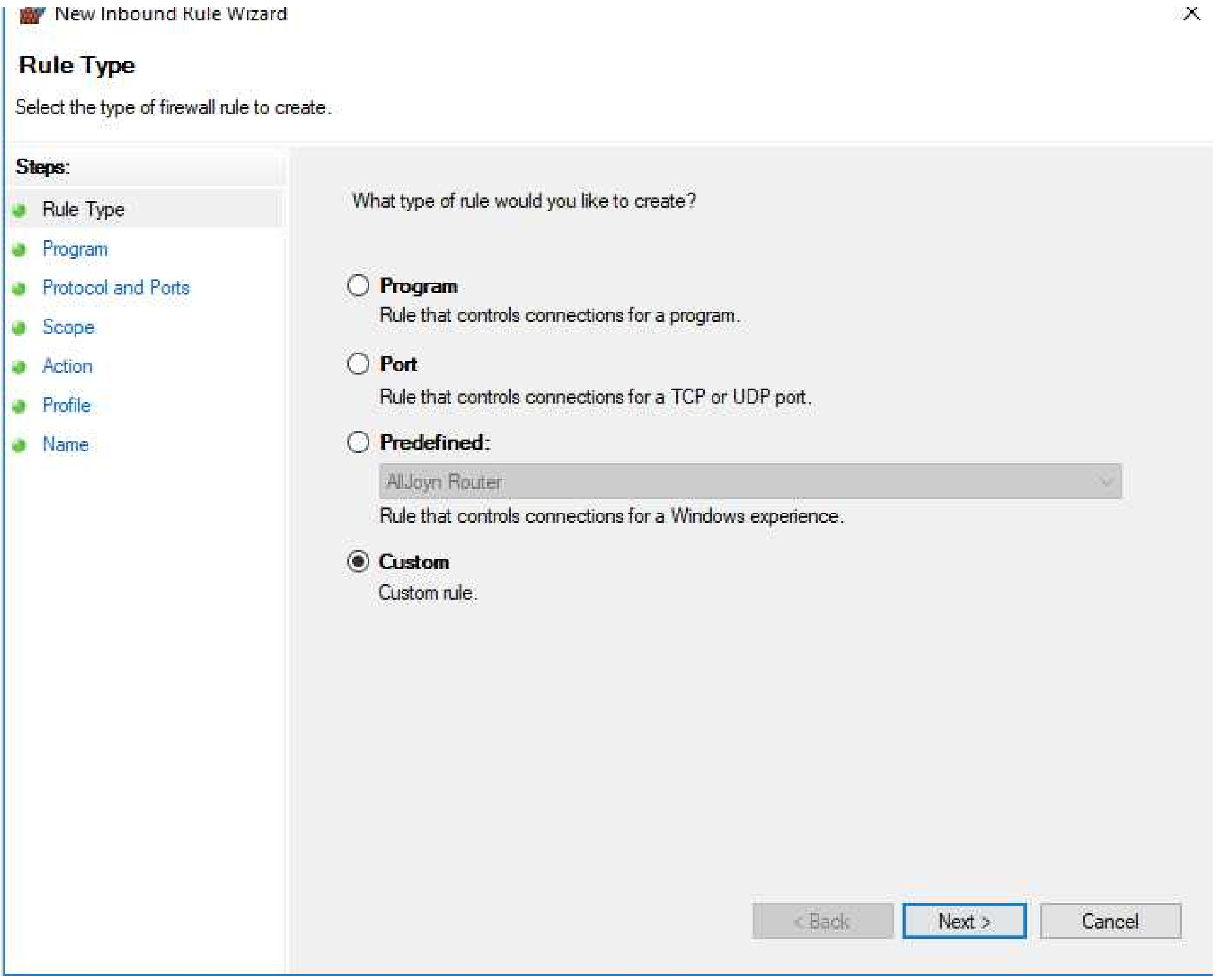
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also a
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inboun
blocked unless they match a rule that allows them, and outbound connections are allowed unle

- We can use a wizard to create rules
- We can block/allow traffic from a specific program, port, IP address, or a combination

- When you install a program, it might add rules to the firewall, so that it can operate properly



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

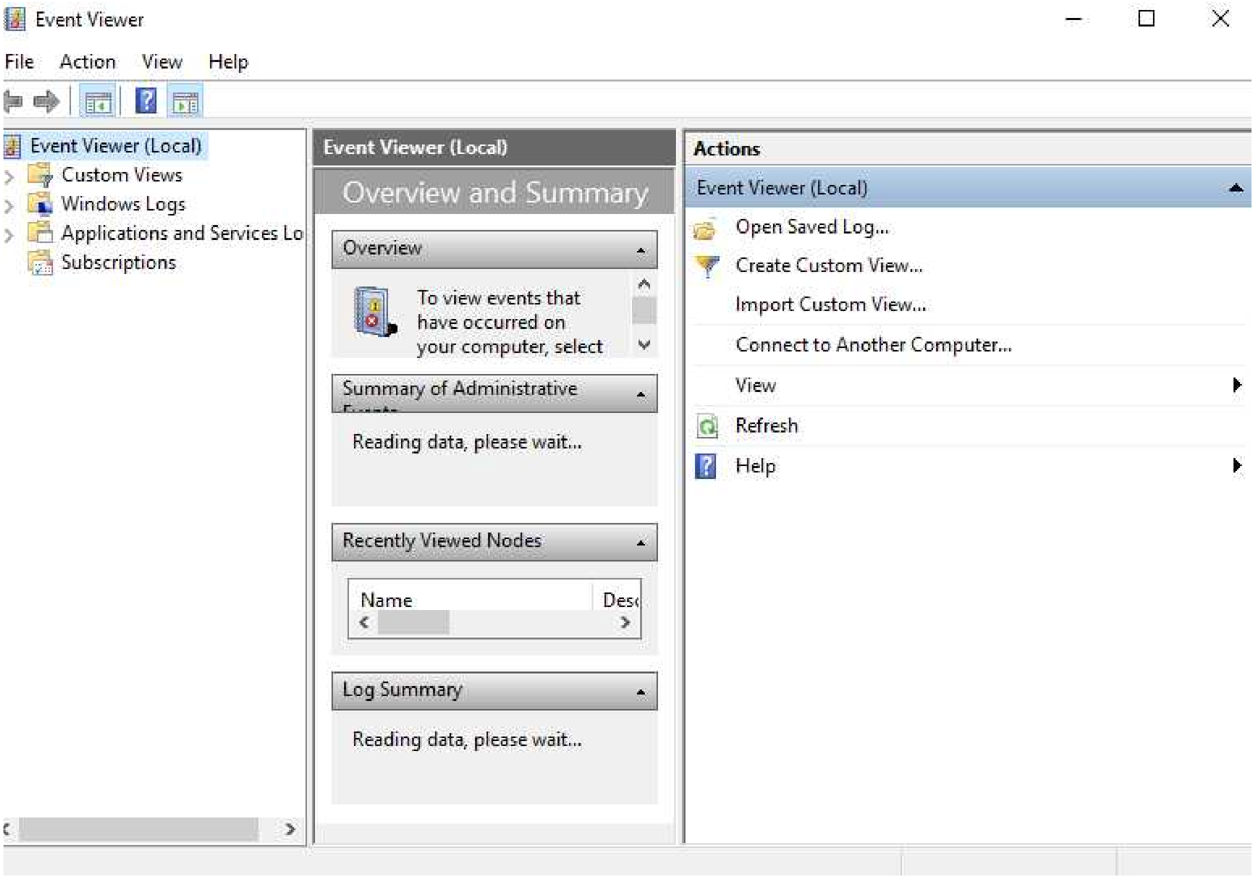
○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

Administrative Tools – Event Viewer

- The event viewer shows us a list of events (automatically logged by Windows)
- We can use the event viewer to identify the source of errors

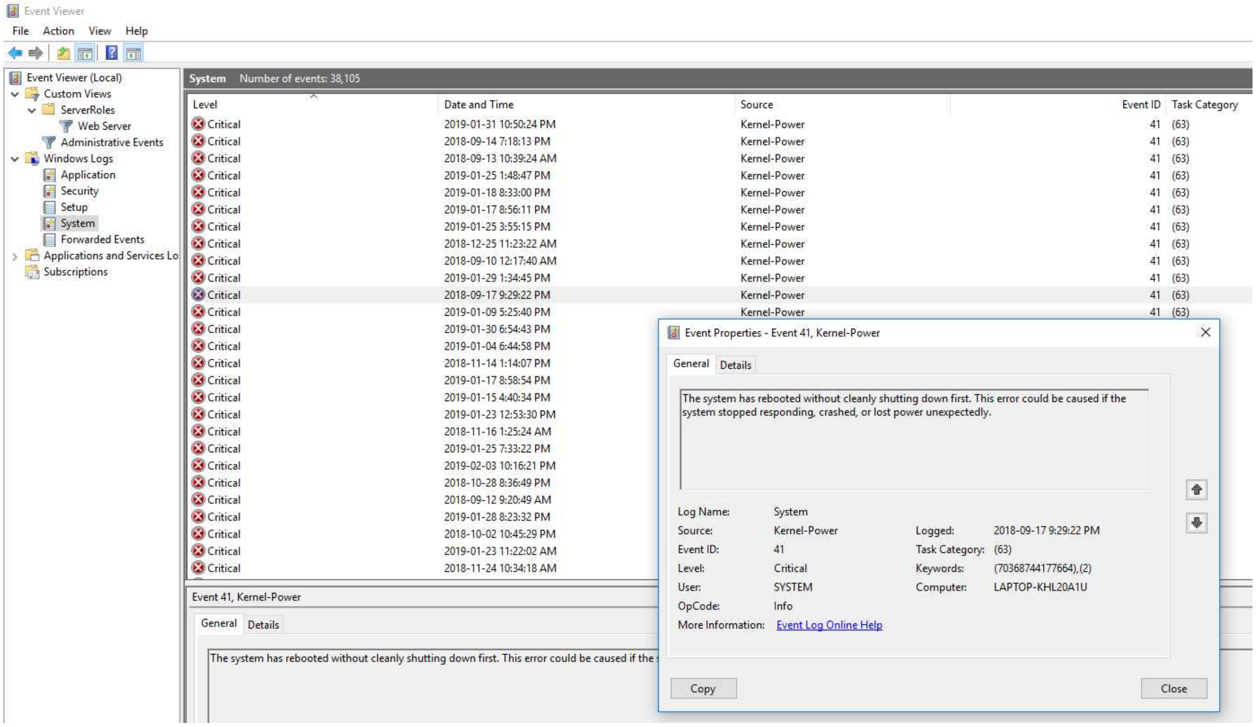


To view events that have occurred on your computer, select

Reading data, please wait...

Reading data, please wait...

- Events are generated by the System, by Security issues, and by Applications
- An event can be a piece of information, a warning, an error, or a critical error
- We can filter by the type of error, the source, or the date/time that it occurred



System Number of events: 38,105

Level	Date and Time	Source	Event ID	Task Category
Critical	2019-01-31 10:50:24 PM	Kernel-Power	41	(63)
Critical	2018-09-14 7:18:13 PM	Kernel-Power	41	(63)
Critical	2018-09-13 10:39:24 AM	Kernel-Power	41	(63)
Critical	2019-01-25 1:48:47 PM	Kernel-Power	41	(63)
Critical	2019-01-18 8:33:00 PM	Kernel-Power	41	(63)
Critical	2019-01-17 8:56:11 PM	Kernel-Power	41	(63)
Critical	2019-01-25 3:55:15 PM	Kernel-Power	41	(63)
Critical	2018-12-25 11:23:22 AM	Kernel-Power	41	(63)
Critical	2018-09-10 12:17:40 AM	Kernel-Power	41	(63)
Critical	2019-01-29 1:34:45 PM	Kernel-Power	41	(63)
Critical	2018-09-17 9:29:22 PM	Kernel-Power	41	(63)
Critical	2019-01-09 5:25:40 PM	Kernel-Power	41	(63)
Critical	2019-01-30 6:54:43 PM			
Critical	2019-01-04 6:44:58 PM			
Critical	2018-11-14 1:14:07 PM			
Critical	2019-01-17 8:58:54 PM			
Critical	2019-01-15 4:40:34 PM			
Critical	2019-01-23 12:53:30 PM			
Critical	2018-11-16 1:25:24 AM			
Critical	2019-01-25 7:33:22 PM			
Critical	2019-02-03 10:16:21 PM			
Critical	2018-10-28 8:36:49 PM			
Critical	2018-09-12 9:20:49 AM			
Critical	2019-01-28 8:23:32 PM			
Critical	2018-10-02 10:45:29 PM			
Critical	2019-01-23 11:22:02 AM			
Critical	2018-11-24 10:34:18 AM			

Event 41, Kernel-Power

The system has rebooted without cleanly shutting down first. This error could be caused if the

Event Properties - Event 41, Kernel-Power

The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.

Log Name:	System		
Source:	Kernel-Power	Logged:	2018-09-17 9:29:22 PM
Event ID:	41	Task Category:	(63)
Level:	Critical	Keywords:	(70368744177664),(2)
User:	SYSTEM	Computer:	LAPTOP-KHL20A1U
OpCode:	Info		
More Information:	Event Log Online Help		

msconfig – General, Boot, Services, Startup, Tools

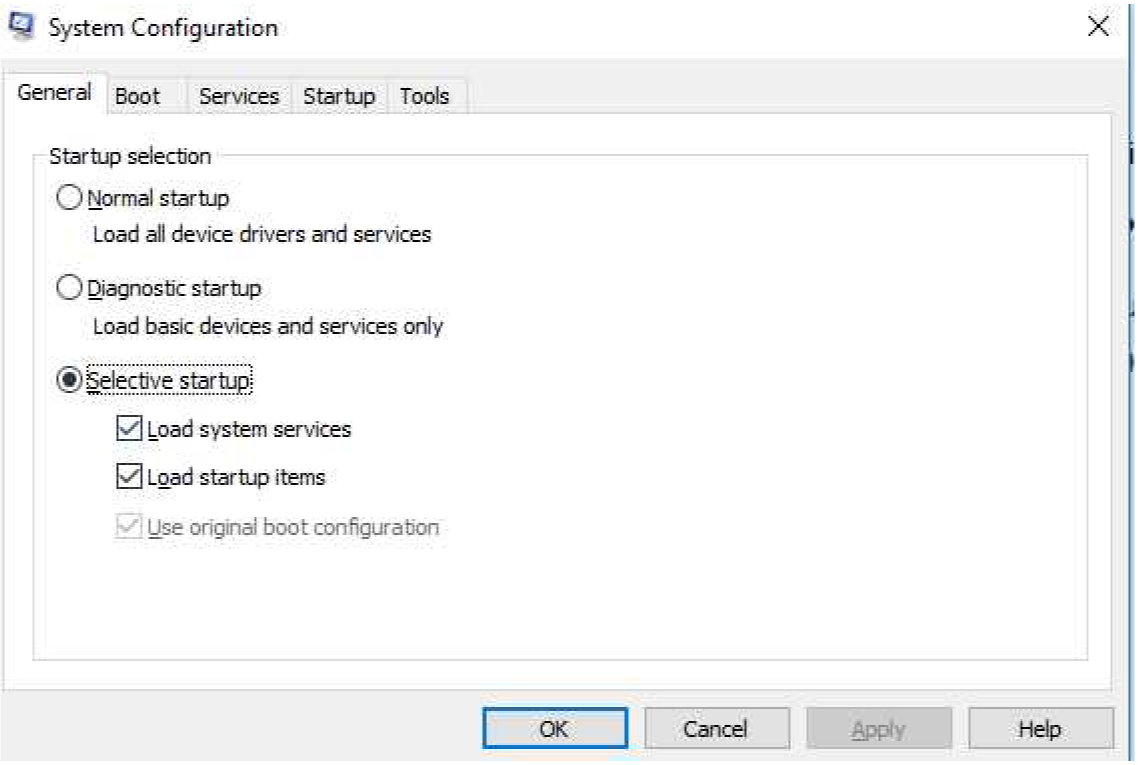
When Windows boots, it loads

- Drivers for all the installed hardware components
- The programs that are listed in the Startup list
- All the services that are set to run automatically

Drivers, programs, and services can cause errors.

In msconfig, the general tab has three options

- Normal startup: loads all start-up items (drivers, programs, and services)
- Diagostic start-up: loads only basic start-up items and services (we can use this to disable many drivers and start-up items, and then enable them one by one to see which one is the cause of the error)
- Selective startup: can choose whether to load system services and/or start-up items



Startup selection

○ Normal startup
Load all device drivers and services

○ Diagnostic startup
Load basic devices and services only

● Selective startup

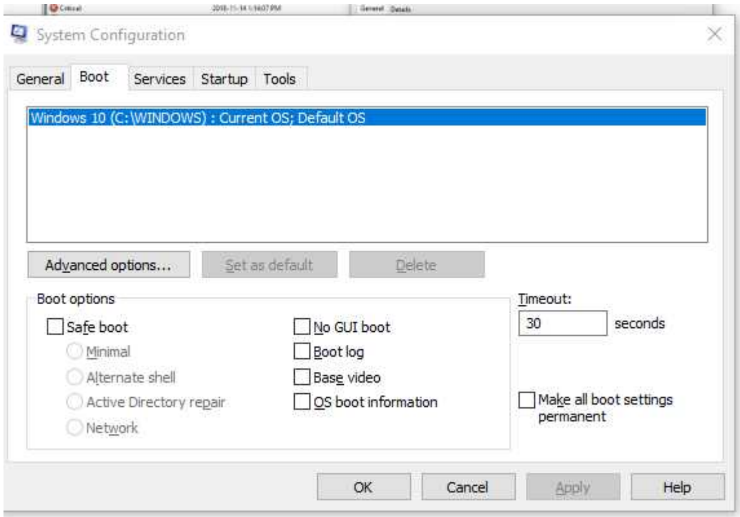
☑ Load system services

☑ Load startup items

☑ Use original boot configuration

The boot tab allows us to choose advanced boot settings

- Boot in Safe Mode (minimal features), an Alternate Shell (boot to a command prompt), or from the Network
- We can also choose to limit the number of processors or amount of memory in use



Windows 10 (C:\WINDOWS) : Current OS; Default OS

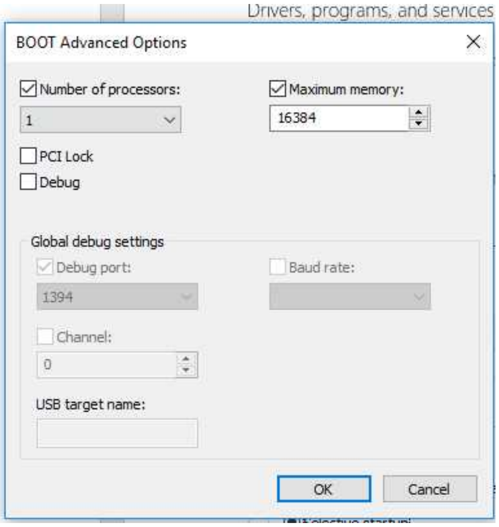
Boot options

□ Safe boot
○ Minimal
○ Alternate shell
○ Active Directory repair
○ Network

□ No GUI boot
□ Boot log
□ Base video
□ OS boot information

Timeout: 30 seconds

□ Make all boot settings permanent



☑ Number of processors: 1

☑ Maximum memory: 16384

□ PCI Lock
□ Debug

Global debug settings

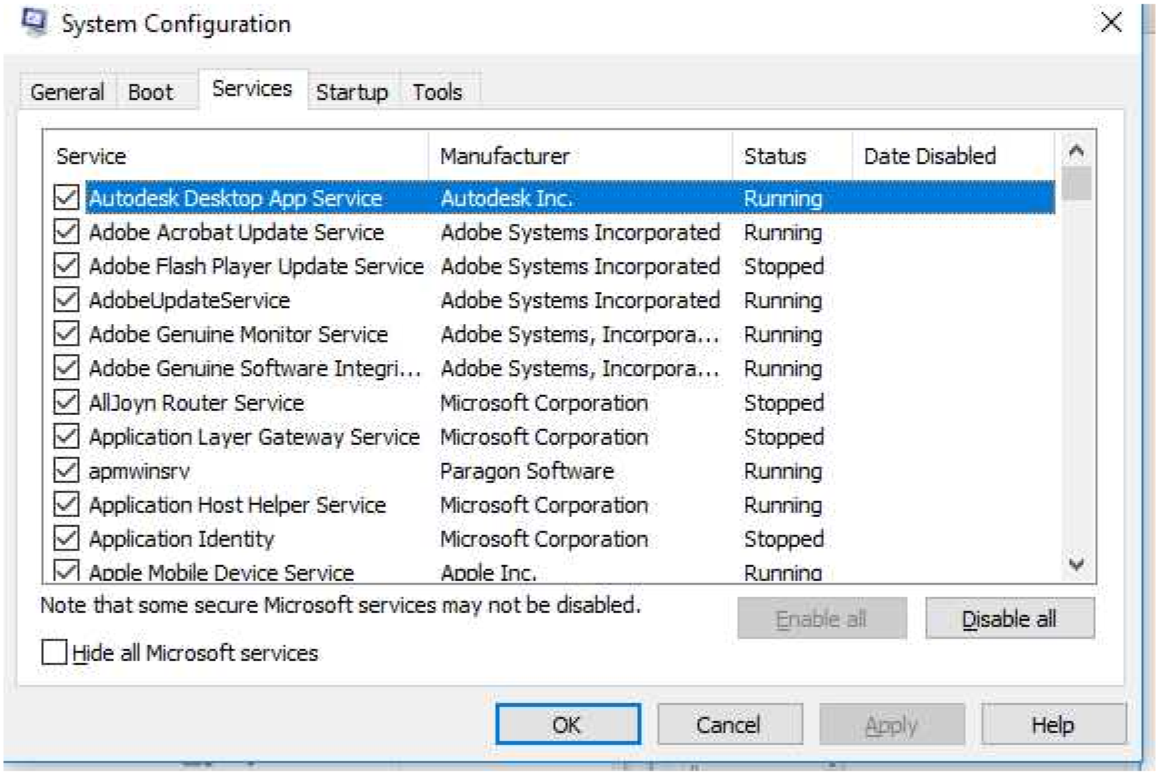
☑ Debug port: 1394

□ Baud rate:

□ Channel: 0

USB target name:

The services tab allows us to enable or disable services



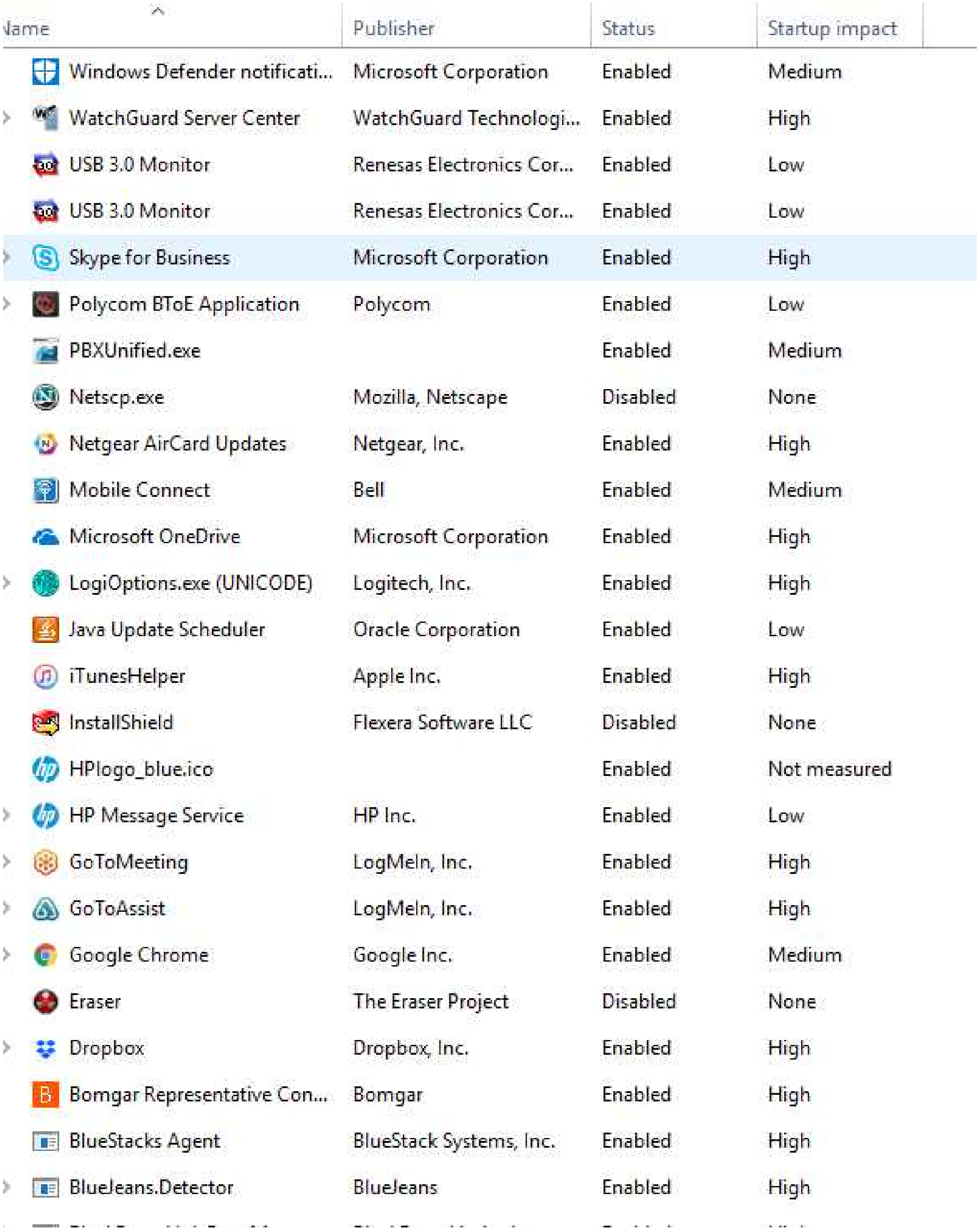
Service	Manufacturer	Status	Date Disabled
☑ Autodesk Desktop App Service	Autodesk Inc.	Running	
☑ Adobe Acrobat Update Service	Adobe Systems Incorporated	Running	
☑ Adobe Flash Player Update Service	Adobe Systems Incorporated	Stopped	
☑ AdobeUpdateService	Adobe Systems Incorporated	Running	
☑ Adobe Genuine Monitor Service	Adobe Systems, Incorpora...	Running	
☑ Adobe Genuine Software Integri...	Adobe Systems, Incorpora...	Running	
☑ AllJoyn Router Service	Microsoft Corporation	Stopped	
☑ Application Layer Gateway Service	Microsoft Corporation	Stopped	
☑ apmwinsrv	Paragon Software	Running	
☑ Application Host Helper Service	Microsoft Corporation	Running	
☑ Application Identity	Microsoft Corporation	Stopped	
☑ Apple Mobile Device Service	Apple Inc.	Running	

Note that some secure Microsoft services may not be disabled.

□ Hide all Microsoft services

The startup tab lists all the applications that start up when the computer starts

- In newer versions of Windows, the startup tab is in the Task Manager
- The startup tab also lists the impact each item has on the computer's performance (may not be completely accurate)
- You can enable or disable each item

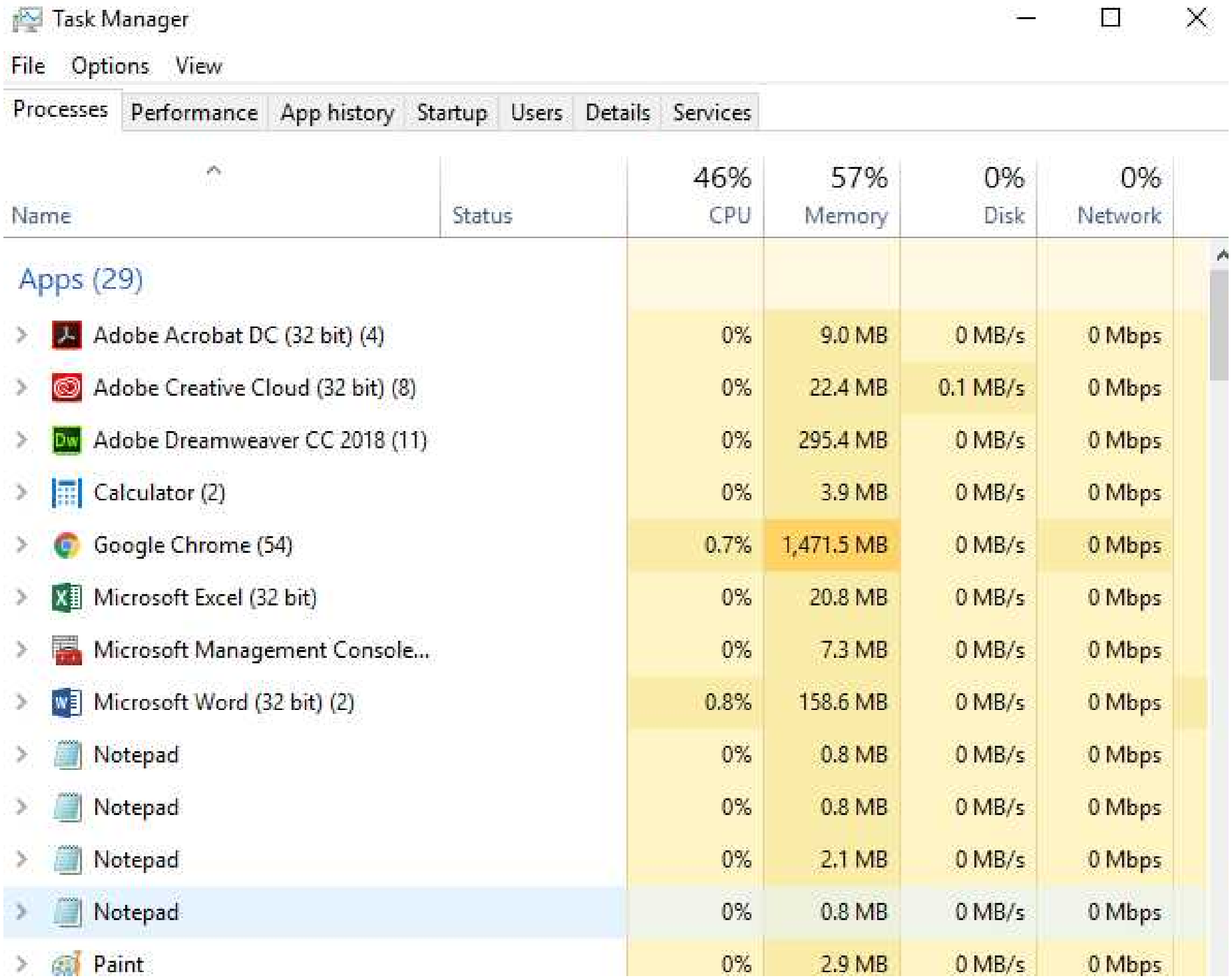


Name	Publisher	Status	Startup impact
Windows Defender notificati...	Microsoft Corporation	Enabled	Medium
WatchGuard Server Center	WatchGuard Technologi...	Enabled	High
USB 3.0 Monitor	Renesas Electronics Cor...	Enabled	Low
USB 3.0 Monitor	Renesas Electronics Cor...	Enabled	Low
Skype for Business	Microsoft Corporation	Enabled	High
Polycom BToE Application	Polycom	Enabled	Low
PBXUnified.exe		Enabled	Medium
Netscp.exe	Mozilla, Netscape	Disabled	None
Netgear AirCard Updates	Netgear, Inc.	Enabled	High
Mobile Connect	Bell	Enabled	Medium
Microsoft OneDrive	Microsoft Corporation	Enabled	High
LogiOptions.exe (UNICODE)	Logitech, Inc.	Enabled	High
Java Update Scheduler	Oracle Corporation	Enabled	Low
iTunesHelper	Apple Inc.	Enabled	High
InstallShield	Flexera Software LLC	Disabled	None
HPlogo_blue.ico		Enabled	Not measured
HP Message Service	HP Inc.	Enabled	Low
GoToMeeting	LogMeIn, Inc.	Enabled	High
GoToAssist	LogMeIn, Inc.	Enabled	High
Google Chrome	Google Inc.	Enabled	Medium
Eraser	The Eraser Project	Disabled	None
Dropbox	Dropbox, Inc.	Enabled	High
Bomgar Representative Con...	Bomgar	Enabled	High
BlueStacks Agent	BlueStack Systems, Inc.	Enabled	High
BlueJeans.Detector	BlueJeans	Enabled	High

Task Manager – Applications, Processes, Performance, Networking, Users

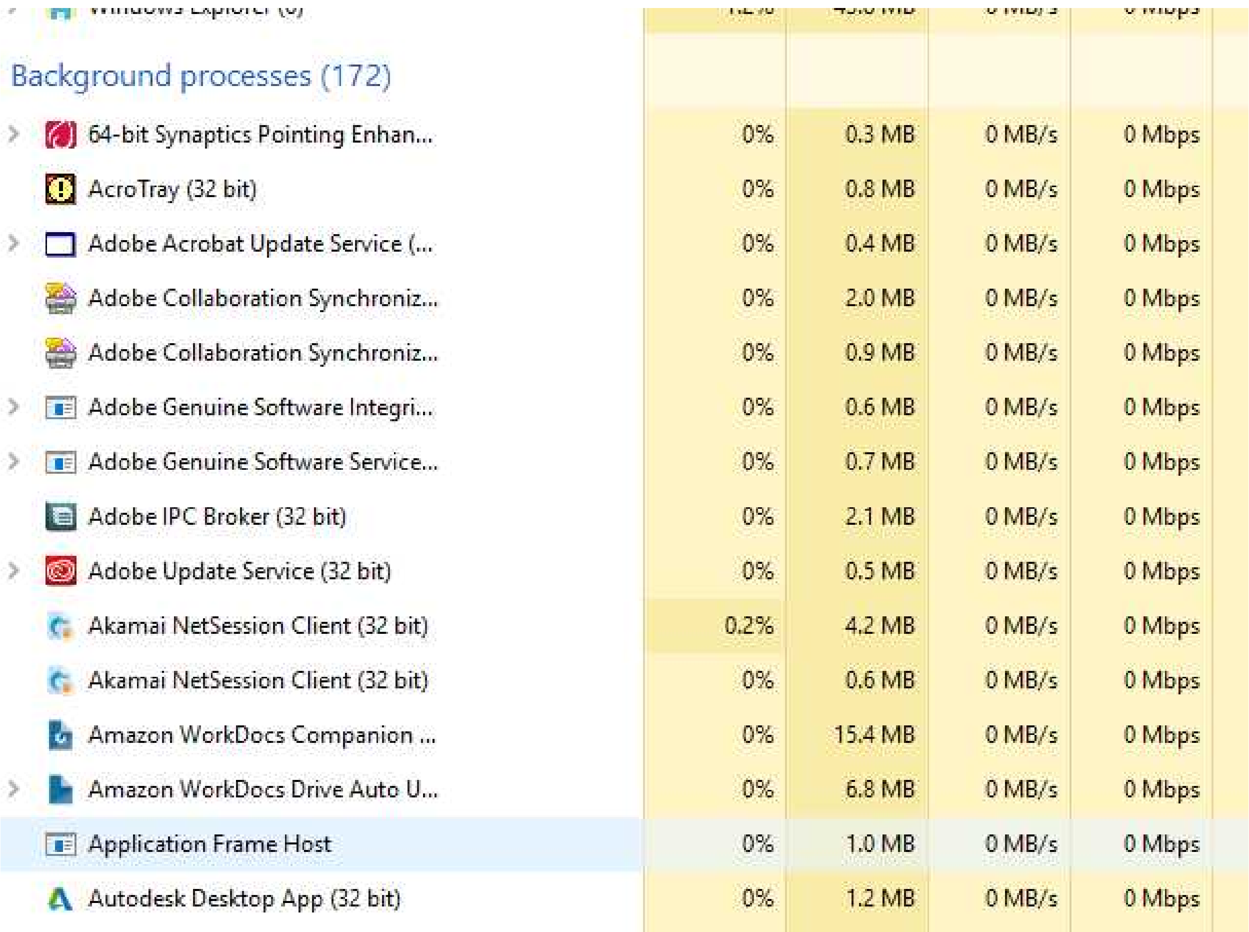
The Task Manager Applications (now known as Processes) tab

- Lists each running application
- For each application, it lists the current CPU, Memory, Disk, and Network usage
- Lists the total CPU, Memory, Disk, and Network usage
- Can show us if a specific application is hogging resources
- We can use the Task Manager to end an application



Name	Status	46% CPU	57% Memory	0% Disk	0% Network
Apps (29)					
Adobe Acrobat DC (32 bit) (4)		0%	9.0 MB	0 MB/s	0 Mbps
Adobe Creative Cloud (32 bit) (8)		0%	22.4 MB	0.1 MB/s	0 Mbps
Adobe Dreamweaver CC 2018 (11)		0%	295.4 MB	0 MB/s	0 Mbps
Calculator (2)		0%	3.9 MB	0 MB/s	0 Mbps
Google Chrome (54)		0.7%	1,471.5 MB	0 MB/s	0 Mbps
Microsoft Excel (32 bit)		0%	20.8 MB	0 MB/s	0 Mbps
Microsoft Management Console...		0%	7.3 MB	0 MB/s	0 Mbps
Microsoft Word (32 bit) (2)		0.8%	158.6 MB	0 MB/s	0 Mbps
Notepad		0%	0.8 MB	0 MB/s	0 Mbps
Notepad		0%	0.8 MB	0 MB/s	0 Mbps
Notepad		0%	2.1 MB	0 MB/s	0 Mbps
Notepad		0%	0.8 MB	0 MB/s	0 Mbps
Paint		0%	2.9 MB	0 MB/s	0 Mbps

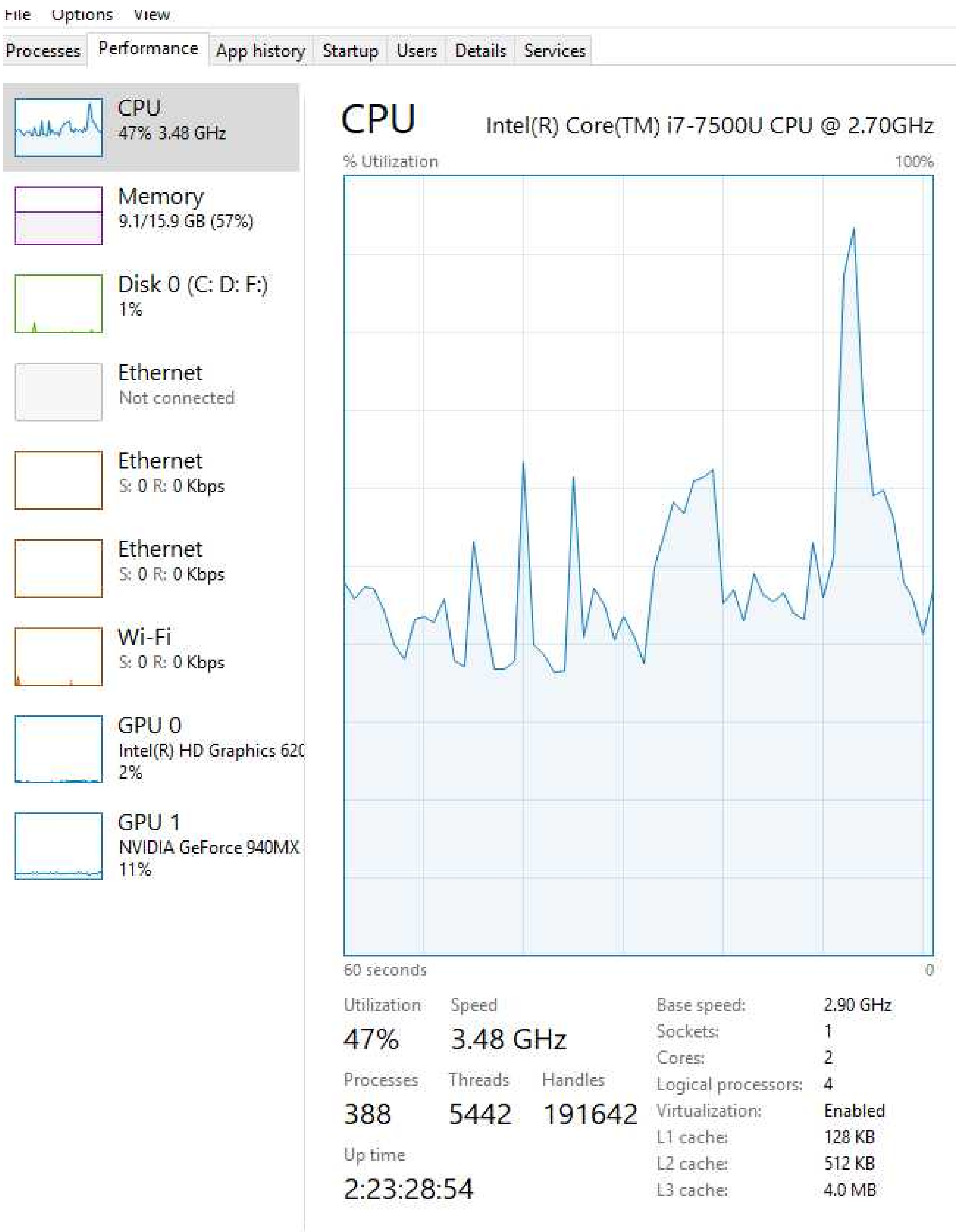
- In newer versions of Windows, the Processes tab lists Applications and Background Processes



Windows Explorer (6)				
Background processes (172)				
64-bit Synaptics Pointing Enhan...	0%	0.3 MB	0 MB/s	0 Mbps
AcroTray (32 bit)	0%	0.8 MB	0 MB/s	0 Mbps
Adobe Acrobat Update Service (...	0%	0.4 MB	0 MB/s	0 Mbps
Adobe Collaboration Synchroniz...	0%	2.0 MB	0 MB/s	0 Mbps
Adobe Collaboration Synchroniz...	0%	0.9 MB	0 MB/s	0 Mbps
Adobe Genuine Software Integri...	0%	0.6 MB	0 MB/s	0 Mbps
Adobe Genuine Software Service...	0%	0.7 MB	0 MB/s	0 Mbps
Adobe IPC Broker (32 bit)	0%	2.1 MB	0 MB/s	0 Mbps
Adobe Update Service (32 bit)	0%	0.5 MB	0 MB/s	0 Mbps
Akamai NetSession Client (32 bit)	0.2%	4.2 MB	0 MB/s	0 Mbps
Akamai NetSession Client (32 bit)	0%	0.6 MB	0 MB/s	0 Mbps
Amazon WorkDocs Companion ...	0%	15.4 MB	0 MB/s	0 Mbps
Amazon WorkDocs Drive Auto U...	0%	6.8 MB	0 MB/s	0 Mbps
Application Frame Host	0%	1.0 MB	0 MB/s	0 Mbps
Autodesk Desktop App (32 bit)	0%	1.2 MB	0 MB/s	0 Mbps

The Performance tab

- Shows us the performance of the computer in a graphical interface



CPU 47% 3.48 GHz

Memory 9.1/15.9 GB (57%)

Disk 0 (C: D: F:) 1%

Ethernet Not connected

Ethernet S: 0 R: 0 Kbps

Ethernet S: 0 R: 0 Kbps

Wi-Fi S: 0 R: 0 Kbps

GPU 0 Intel(R) HD Graphics 62(2%

GPU 1 NVIDIA GeForce 940MX 11%

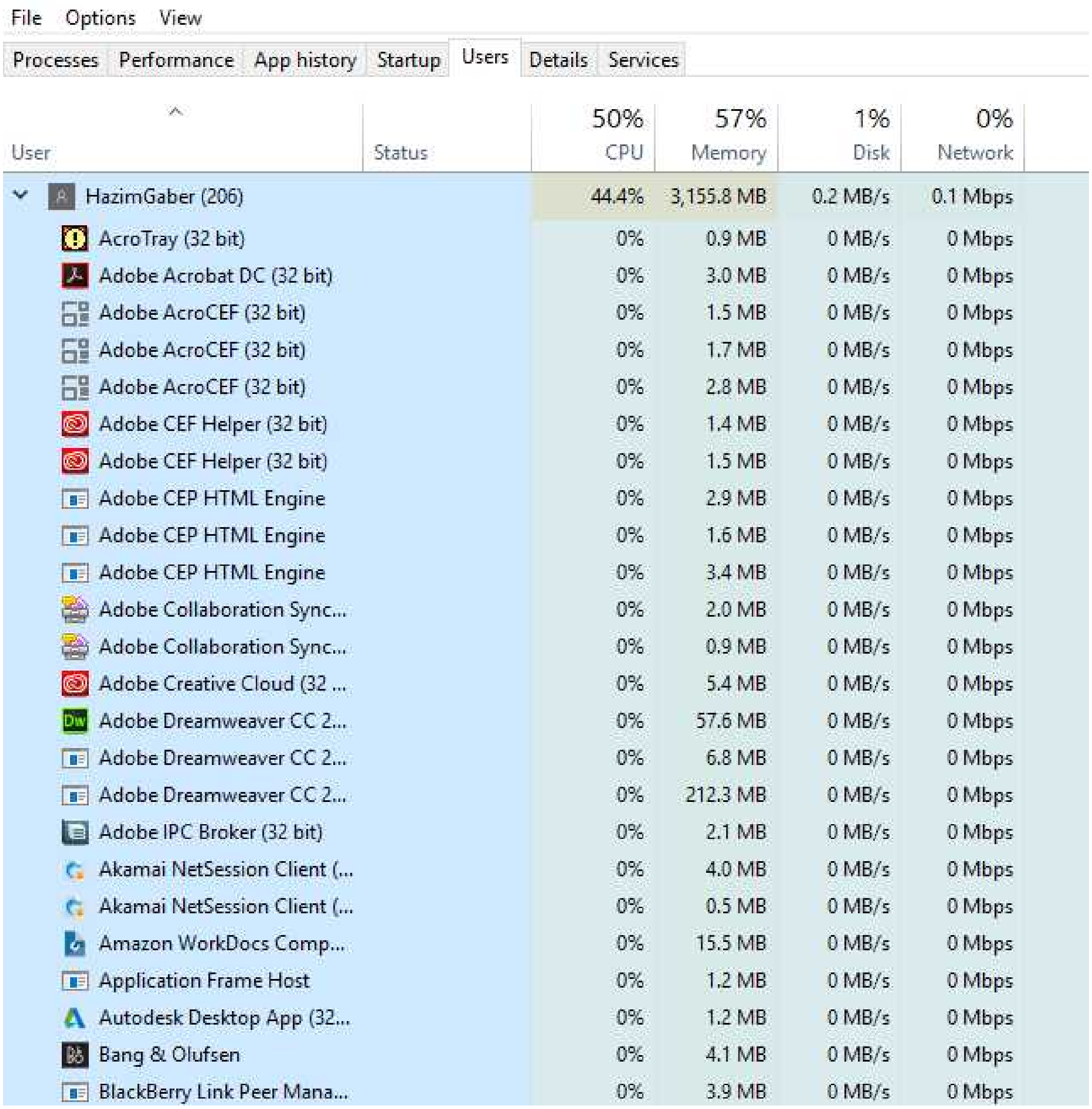
CPU Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz

Utilization 47%
Speed 3.48 GHz
Processes 388
Threads 5442
Handles 191642
Up time 2:23:28:54

Base speed:	2.90 GHz
Sockets:	1
Cores:	2
Logical processors:	4
Virtualization:	Enabled
L1 cache:	128 KB
L2 cache:	512 KB
L3 cache:	4.0 MB

The Users tab

- Shows a list of users who are logged in
- For each user, it shows the applications that the user is running, and the resources that each of the applications is using

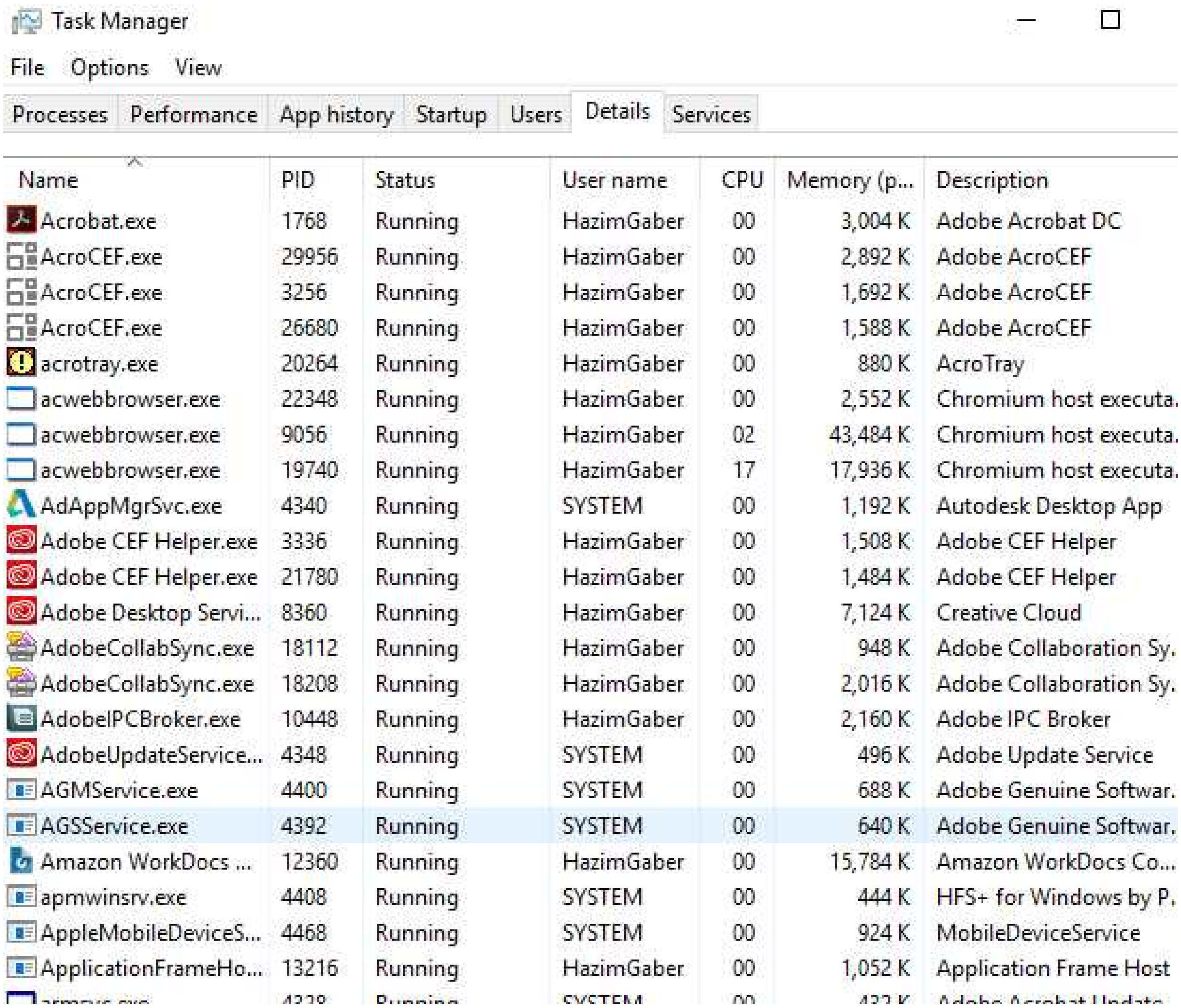


User	Status	50% CPU	57% Memory	1% Disk	0% Network
HazimGaber (206)		44.4%	3,155.8 MB	0.2 MB/s	0.1 Mbps
AcroTray (32 bit)		0%	0.9 MB	0 MB/s	0 Mbps
Adobe Acrobat DC (32 bit)		0%	3.0 MB	0 MB/s	0 Mbps
Adobe AcroCEF (32 bit)		0%	1.5 MB	0 MB/s	0 Mbps
Adobe AcroCEF (32 bit)		0%	1.7 MB	0 MB/s	0 Mbps
Adobe AcroCEF (32 bit)		0%	2.8 MB	0 MB/s	0 Mbps
Adobe CEF Helper (32 bit)		0%	1.4 MB	0 MB/s	0 Mbps
Adobe CEF Helper (32 bit)		0%	1.5 MB	0 MB/s	0 Mbps
Adobe CEP HTML Engine		0%	2.9 MB	0 MB/s	0 Mbps
Adobe CEP HTML Engine		0%	1.6 MB	0 MB/s	0 Mbps
Adobe CEP HTML Engine		0%	3.4 MB	0 MB/s	0 Mbps
Adobe Collaboration Sync...		0%	2.0 MB	0 MB/s	0 Mbps
Adobe Collaboration Sync...		0%	0.9 MB	0 MB/s	0 Mbps
Adobe Creative Cloud (32 ...		0%	5.4 MB	0 MB/s	0 Mbps
Adobe Dreamweaver CC 2...		0%	57.6 MB	0 MB/s	0 Mbps
Adobe Dreamweaver CC 2...		0%	6.8 MB	0 MB/s	0 Mbps
Adobe Dreamweaver CC 2...		0%	212.3 MB	0 MB/s	0 Mbps
Adobe IPC Broker (32 bit)		0%	2.1 MB	0 MB/s	0 Mbps
Akamai NetSession Client (...		0%	4.0 MB	0 MB/s	0 Mbps
Akamai NetSession Client (...		0%	0.5 MB	0 MB/s	0 Mbps
Amazon WorkDocs Comp...		0%	15.5 MB	0 MB/s	0 Mbps
Application Frame Host		0%	1.2 MB	0 MB/s	0 Mbps
Autodesk Desktop App (32...		0%	1.2 MB	0 MB/s	0 Mbps
Bang & Olufsen		0%	4.1 MB	0 MB/s	0 Mbps
BlackBerry Link Peer Mana...		0%	3.9 MB	0 MB/s	0 Mbps

The Details tab (also known as the processes tab on older versions of Windows)

- Shows a list of running processes

- For each process, it shows the Process ID, the status, the user who is running the process, and the CPU/memory utilization
- A process could be an application or a service
- We can end a process or view the location of the file that contains the process

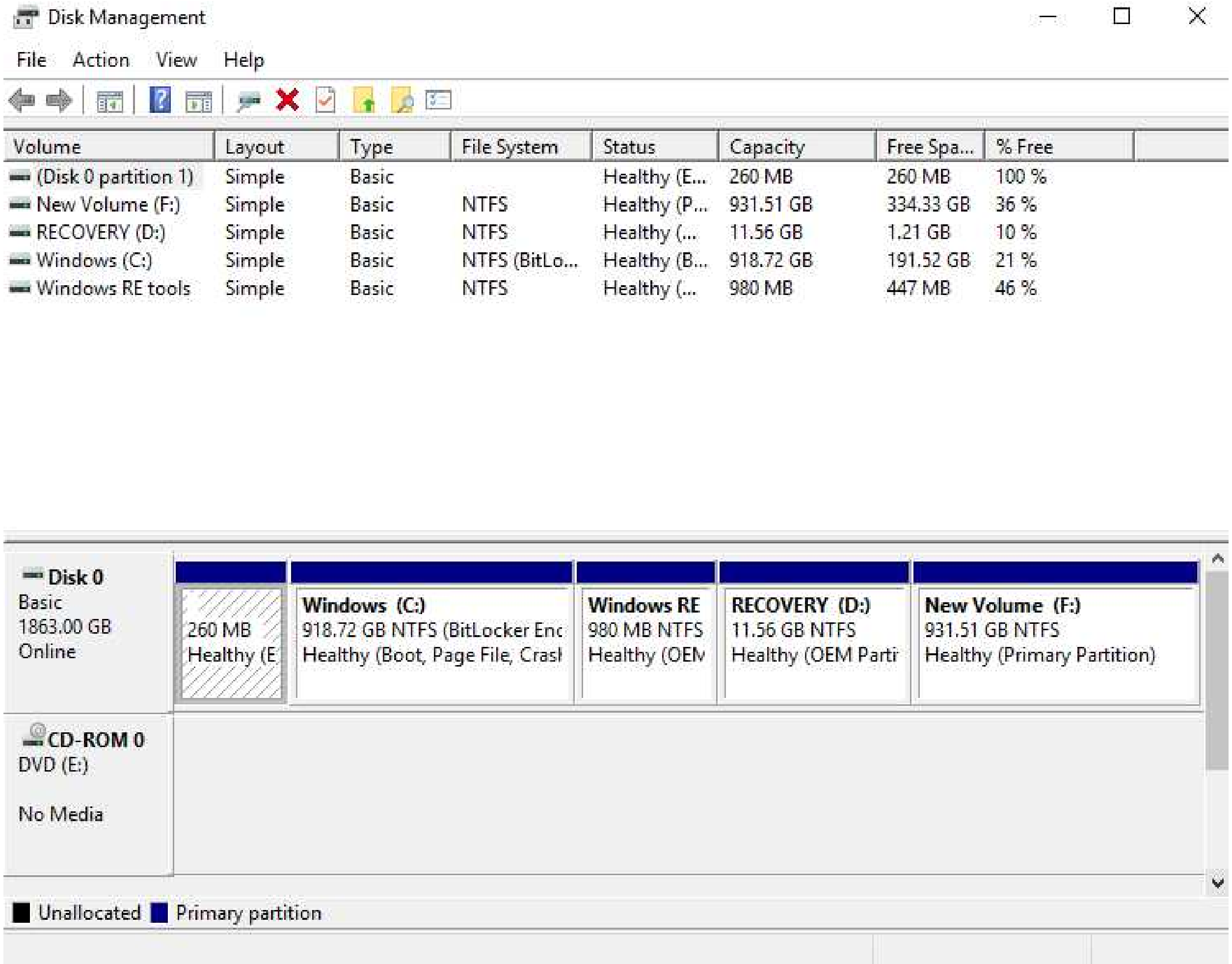


Name	PID	Status	User name	CPU	Memory (p...	Description
Acrobat.exe	1768	Running	HazimGaber	00	3,004 K	Adobe Acrobat DC
AcroCEF.exe	29956	Running	HazimGaber	00	2,892 K	Adobe AcroCEF
AcroCEF.exe	3256	Running	HazimGaber	00	1,692 K	Adobe AcroCEF
AcroCEF.exe	26680	Running	HazimGaber	00	1,588 K	Adobe AcroCEF
acrotray.exe	20264	Running	HazimGaber	00	880 K	AcroTray
acwebbrowser.exe	22348	Running	HazimGaber	00	2,552 K	Chromium host executa.
acwebbrowser.exe	9056	Running	HazimGaber	02	43,484 K	Chromium host executa.
acwebbrowser.exe	19740	Running	HazimGaber	17	17,936 K	Chromium host executa.
AdAppMgrSvc.exe	4340	Running	SYSTEM	00	1,192 K	Autodesk Desktop App
Adobe CEF Helper.exe	3336	Running	HazimGaber	00	1,508 K	Adobe CEF Helper
Adobe CEF Helper.exe	21780	Running	HazimGaber	00	1,484 K	Adobe CEF Helper
Adobe Desktop Servi...	8360	Running	HazimGaber	00	7,124 K	Creative Cloud
AdobeCollabSync.exe	18112	Running	HazimGaber	00	948 K	Adobe Collaboration Sy.
AdobeCollabSync.exe	18208	Running	HazimGaber	00	2,016 K	Adobe Collaboration Sy.
AdobeIPCBroker.exe	10448	Running	HazimGaber	00	2,160 K	Adobe IPC Broker
AdobeUpdateService...	4348	Running	SYSTEM	00	496 K	Adobe Update Service
AGMService.exe	4400	Running	SYSTEM	00	688 K	Adobe Genuine Softwar.
AGSService.exe	4392	Running	SYSTEM	00	640 K	Adobe Genuine Softwar.
Amazon WorkDocs ...	12360	Running	HazimGaber	00	15,784 K	Amazon WorkDocs Co...
apmwinsrv.exe	4408	Running	SYSTEM	00	444 K	HFS+ for Windows by P.
AppleMobileDeviceS...	4468	Running	SYSTEM	00	924 K	MobileDeviceService
ApplicationFrameHo...	13216	Running	HazimGaber	00	1,052 K	Application Frame Host
armsvc.exe	4328	Running	SYSTEM	00	432 K	Adobe Acrobat Update

Disk Management – Drive Status, Mounting, Initializing, Extending Partitions, Splitting Partitions, Shrink Partitions, Assign/Change Drive Letters, Add Drives, Add Arrays

Shows us a list of physical disks, and how they are partitioned

- At the top, we can see a list of every partition, the type of partition (Basic or Dynamic), the File System, the Status, the Capacity, and the amount of Free Space
- At the bottom, it shows us each disk, its capacity, and a layout of the partitions (remember that partitions must be contiguous on a basic drive)

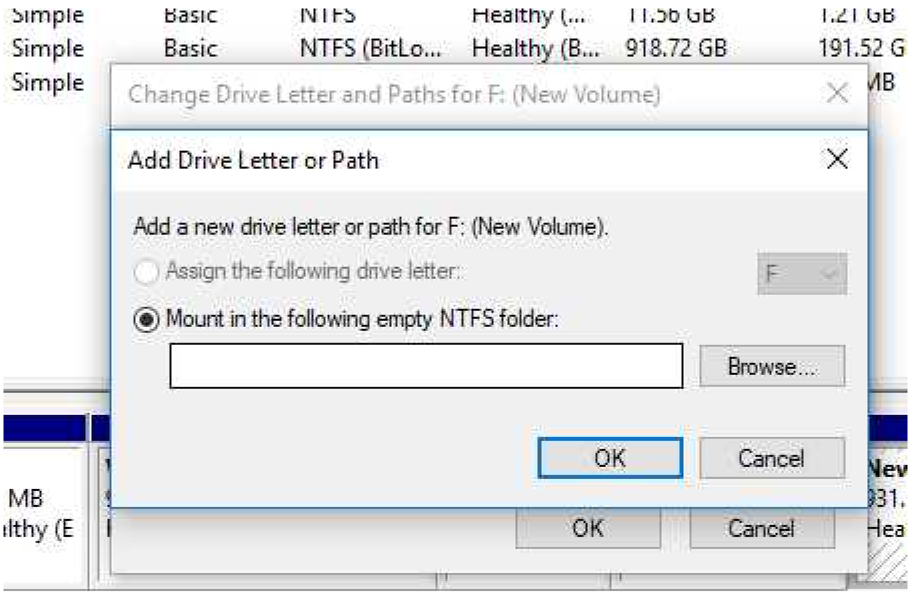


Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	260 MB	260 MB	100 %
New Volume (F:)	Simple	Basic	NTFS	Healthy (P...	931.51 GB	334.33 GB	36 %
RECOVERY (D:)	Simple	Basic	NTFS	Healthy (...	11.56 GB	1.21 GB	10 %
Windows (C:)	Simple	Basic	NTFS (BitLo...	Healthy (B...	918.72 GB	191.52 GB	21 %
Windows RE tools	Simple	Basic	NTFS	Healthy (...	980 MB	447 MB	46 %

Disk 0 Basic 1863.00 GB Online	260 MB Healthy (E	**Windows (C:)** 918.72 GB NTFS (BitLocker Enc Healthy (Boot, Page File, Crasl	**Windows RE** 980 MB NTFS Healthy (OEM	**RECOVERY (D:)** 11.56 GB NTFS Healthy (OEM Parti	**New Volume (F:)** 931.51 GB NTFS Healthy (Primary Partition)
CD-ROM 0 DVD (E:) No Media					

■ Unallocated ■ Primary partition

- We can add a drive letter to a partition



Change Drive Letter and Paths for F: (New Volume)

Add Drive Letter or Path

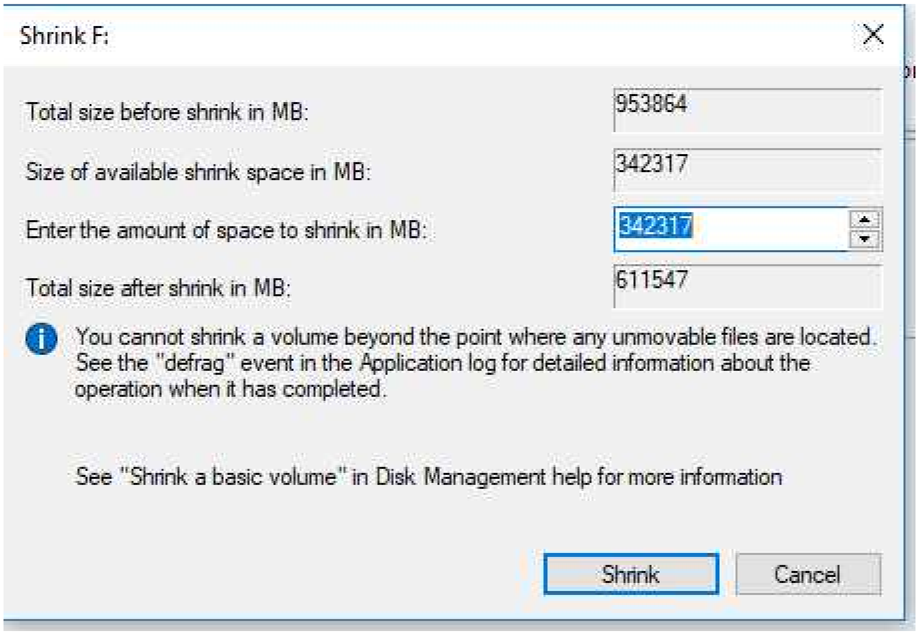
Add a new drive letter or path for F: (New Volume).

○ Assign the following drive letter: F

● Mount in the following empty NTFS folder:

Browse...
OK
Cancel
OK
Cancel
Simple Basic NTFS Healthy (... 11.56 GB 1.21 GB
Simple Basic NTFS (BitLo... Healthy (B... 918.72 GB 191.52 G
Simple

- We can shrink a volume by up to the maximum amount of free space available. For example, if the volume is 1000MB, with 250MB of free space, then we can shrink it by up to 250MB.



Shrink F:

Total size before shrink in MB: 953864

Size of available shrink space in MB: 342317

Enter the amount of space to shrink in MB: 342317

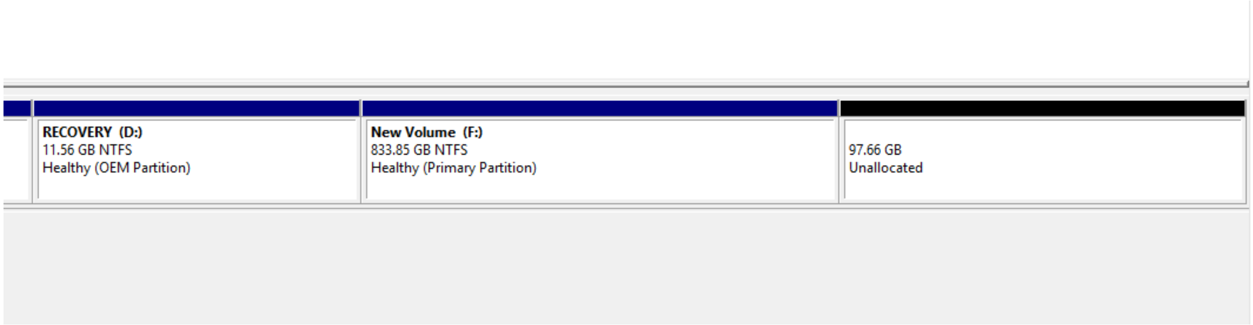
Total size after shrink in MB: 611547

You cannot shrink a volume beyond the point where any unmovable files are located. See the "defrag" event in the Application log for detailed information about the operation when it has completed.

See "Shrink a basic volume" in Disk Management help for more information

- We can increase the size of a partition.
  - There must be free space available on the drive
  - The free space must be to the right of the partition

- For example, in the photo, we can increase the Volume F by 97.66GB (since we have 97.66 GB to the right of Volume F).
- We can't increase Volume D, or add the 97.66GB to volume D, because there is no free space to the right of Volume D
- We can also turn the 97.66GB into one or more new volumes

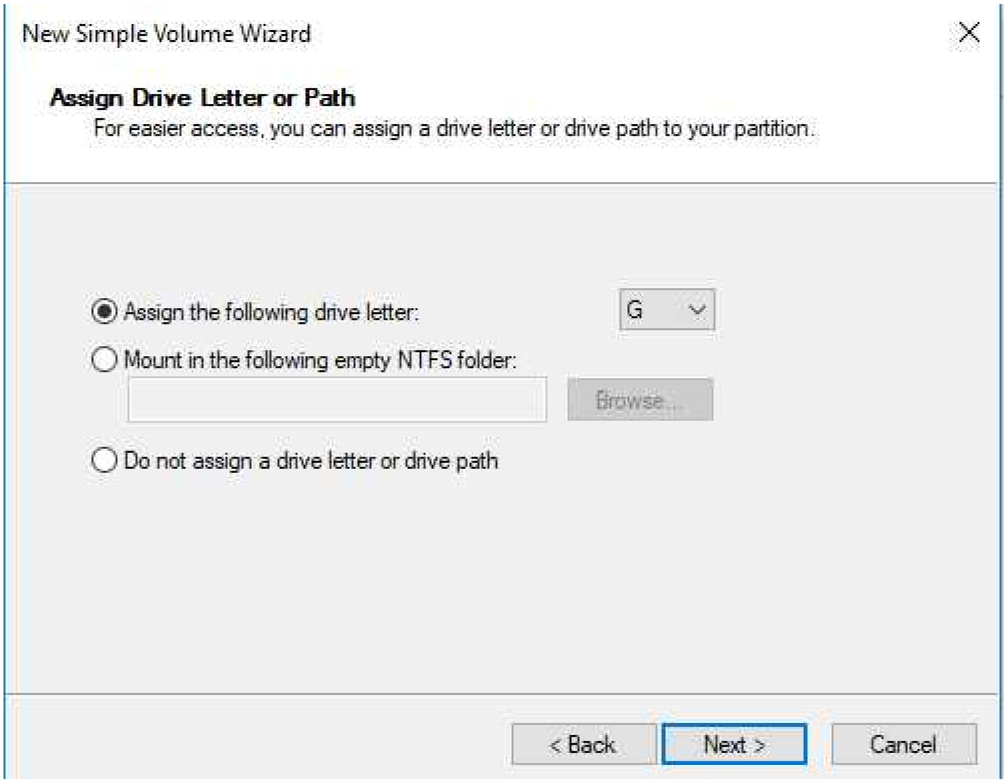


RECOVERY (D:)
11.56 GB NTFS
Healthy (OEM Partition)

New Volume (F:)
833.85 GB NTFS
Healthy (Primary Partition)

97.66 GB
Unallocated

- We can create a new volume from some unallocated free space



New Simple Volume Wizard

Assign Drive Letter or Path

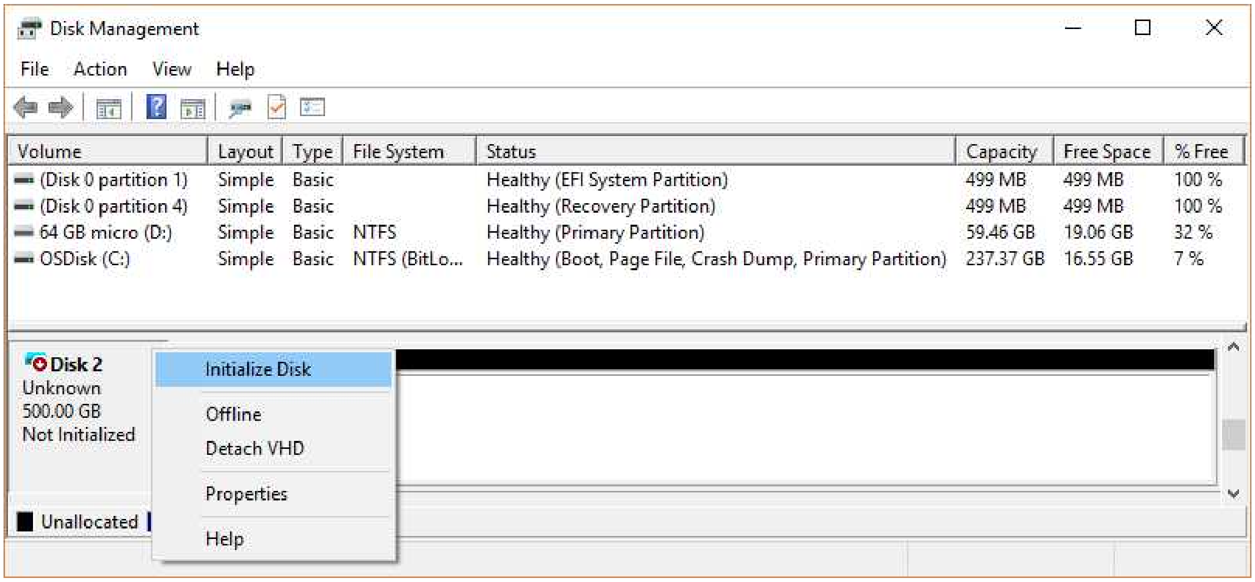
For easier access, you can assign a drive letter or drive path to your partition.

● Assign the following drive letter: G

○ Mount in the following empty NTFS folder:

○ Do not assign a drive letter or drive path

- If we install a new physical disk, it will appear in Disk Management



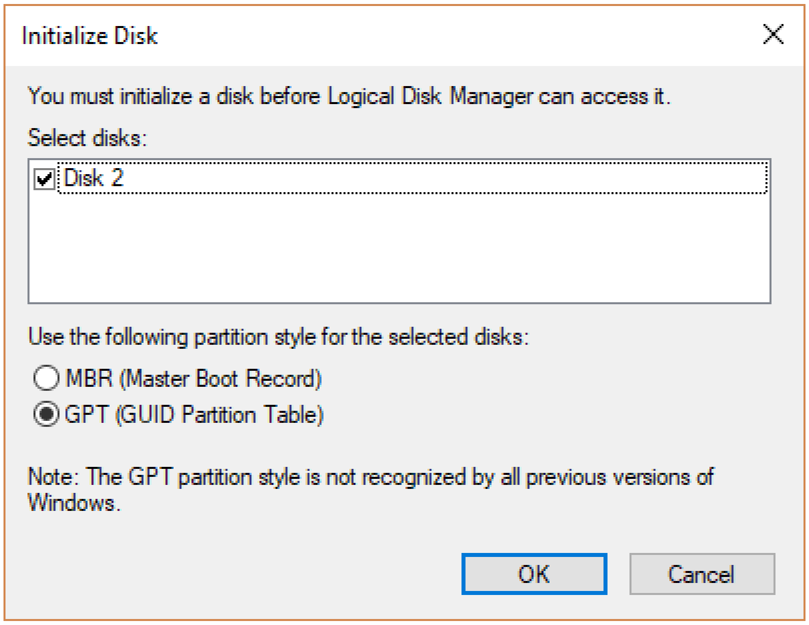
Disk Management

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (EFI System Partition)	499 MB	499 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (Recovery Partition)	499 MB	499 MB	100 %
64 GB micro (D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	59.46 GB	19.06 GB	32 %
OSDisk (C:)	Simple	Basic	NTFS (BitLo...	Healthy (Boot, Page File, Crash Dump, Primary Partition)	237.37 GB	16.55 GB	7 %

Disk 2
Unknown
500.00 GB
Not Initialized

■ Unallocated

- Choose to initialize the disk either as a GPT or MBR



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 2

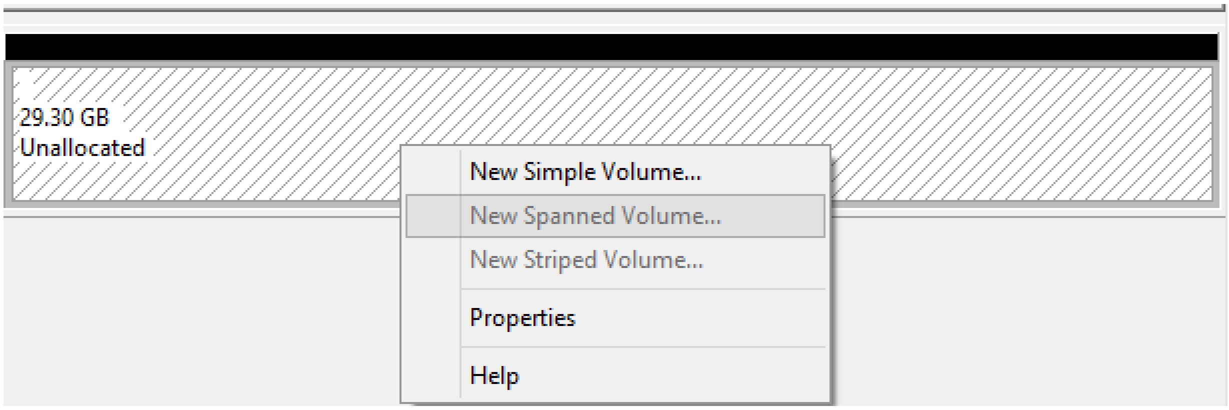
Use the following partition style for the selected disks:

○ MBR (Master Boot Record)

● GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

- To create a RAID array
  - Choose a New Spanned Volume
  - Then choose the type of RAID

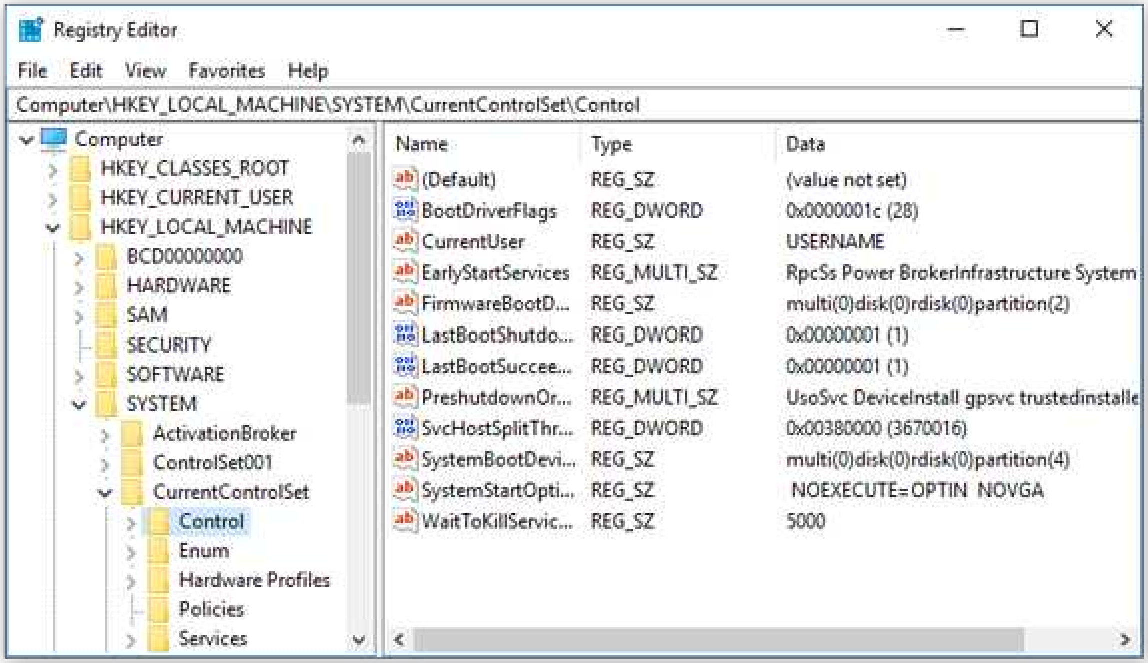


Disk Management isn't always the best tool

- Consider using a commercial tool for more advanced operations

System Utilities – Regedit

- Windows Registry Editor
- Need admin privileges to operate
- Contains system, user, and application settings & preferences



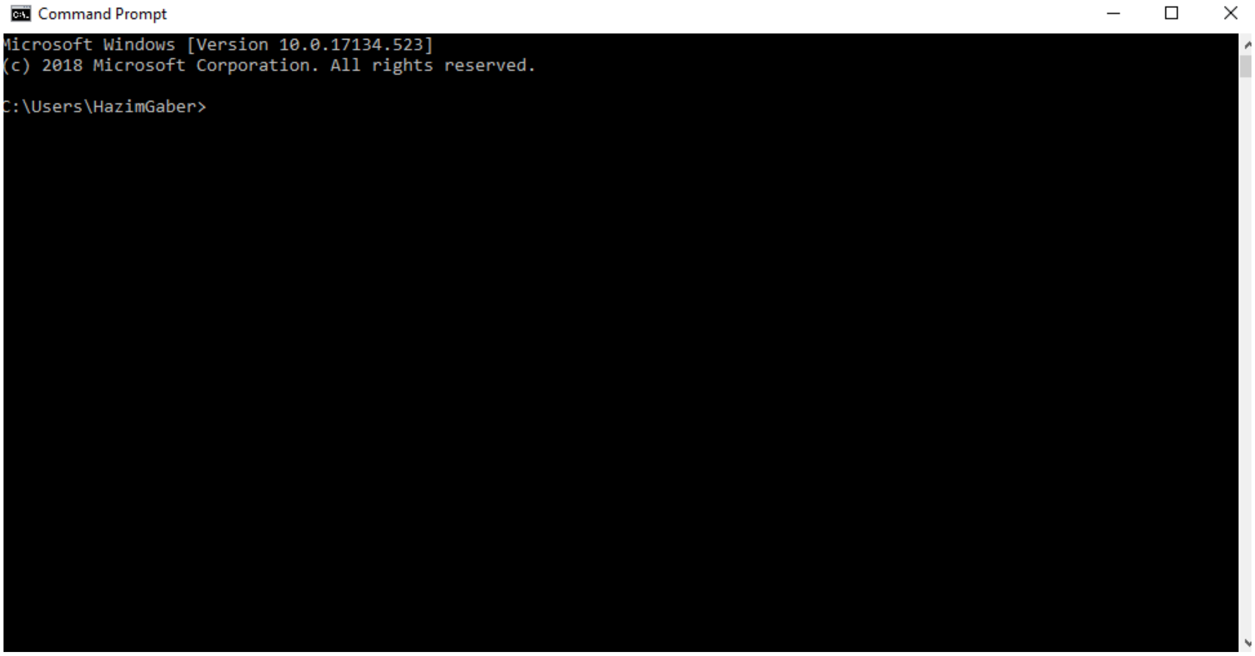
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

Name	Type	Data
(Default)	REG_SZ	(value not set)
BootDriverFlags	REG_DWORD	0x0000001c (28)
CurrentUser	REG_SZ	USERNAME
EarlyStartServices	REG_MULTI_SZ	RpcSs Power BrokerInfrastructure System
FirmwareBootD...	REG_SZ	multi(0)disk(0)rdisk(0)partition(2)
LastBootShutdo...	REG_DWORD	0x00000001 (1)
LastBootSuccee...	REG_DWORD	0x00000001 (1)
PreshutdownOr...	REG_MULTI_SZ	UsoSvc DeviceInstall gpsvc trustedinstalle
SvcHostSplitThr...	REG_DWORD	0x00380000 (3670016)
SystemBootDevi...	REG_SZ	multi(0)disk(0)rdisk(0)partition(4)
SystemStartOpti...	REG_SZ	NOEXECUTE=OPTIN NOVGA
WaitToKillServic...	REG_SZ	5000

- The registry is hierarchical (contains keys, which are like folders)
- Keys store values; each value contains a different setting
- There are five main keys
  - HKEY_LOCAL_MACHINE: contains computer settings
  - HKEY_CURRENT_CONFIG: contains information generated at boot time (this information is regenerated each time the compute reboots)
  - HKEY_CLASSES_ROOT: contains information about applications
  - HKEY_USERS: contains settings for all users
  - HKEY_CURRENT_USER: contains settings for the user who is logged in
- It's possible to store a registry value inside a registry file
- Double-clicking on the file adds it to the registry

System Utilities – Command

- The command prompt allows you to type in commands



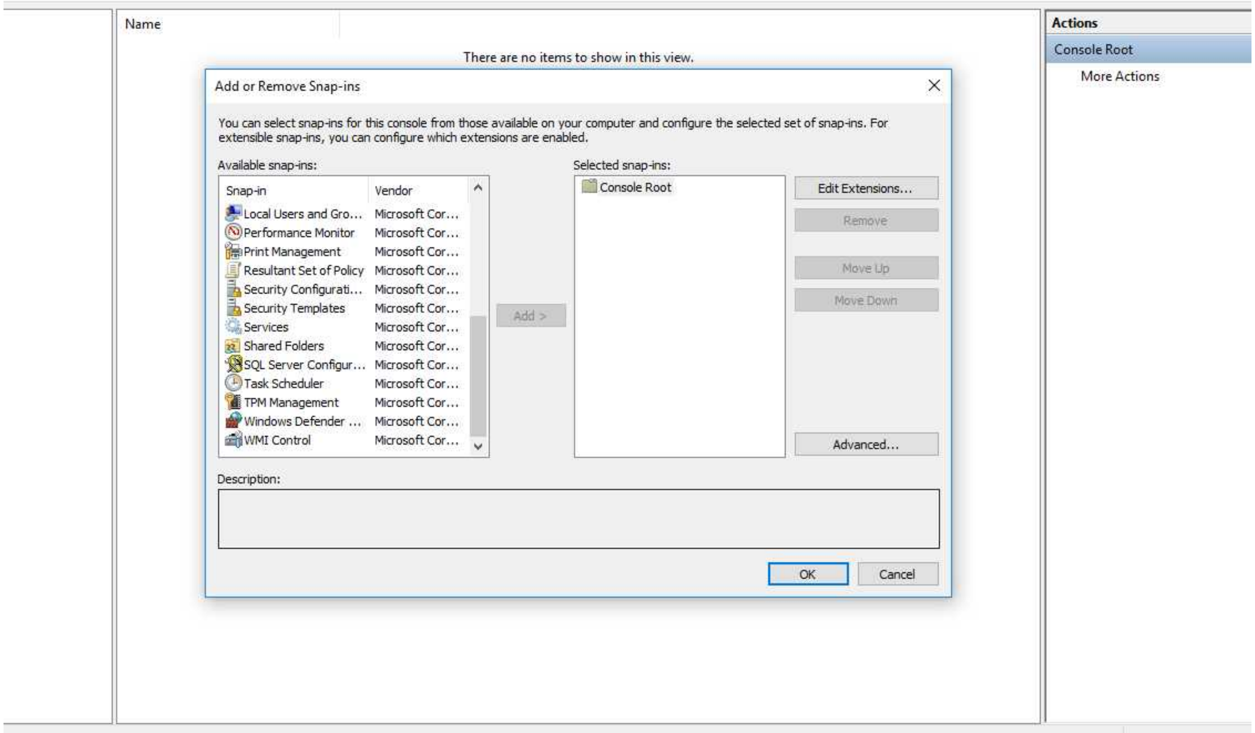
```
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\HazimGaber>
```

System Utilities – Services.msc

- Services shows a list of services (as mentioned earlier)

System Utilities – MMC

- Microsoft Management Console
- A framework for managing multiple sets of Windows settings (such as Device Manager, Disk Management, etc.)
- You can add "snap ins" to the Console; a snap in is a module that controls a specific function



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

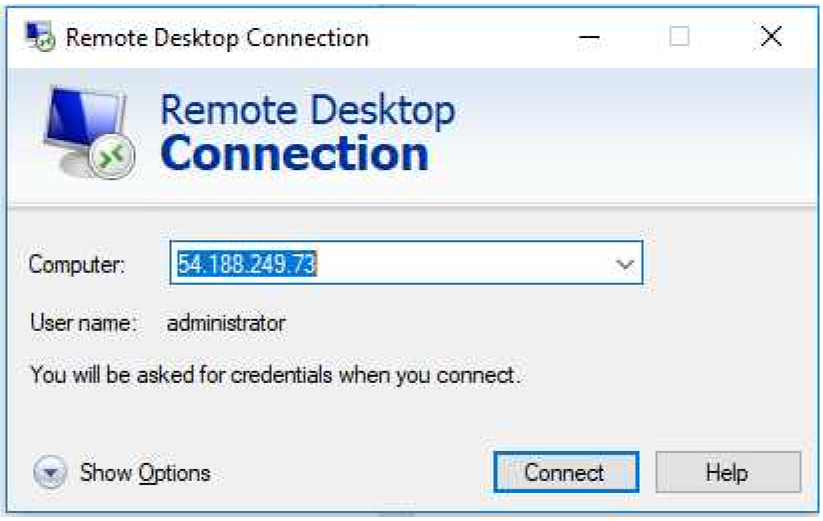
Snap-in	Vendor
Local Users and Gro...	Microsoft Cor...
Performance Monitor	Microsoft Cor...
Print Management	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...
Shared Folders	Microsoft Cor...
SQL Server Configur...	Microsoft Cor...
Task Scheduler	Microsoft Cor...
TPM Management	Microsoft Cor...
Windows Defender ...	Microsoft Cor...
WMI Control	Microsoft Cor...

Selected snap-ins:

Console Root

System Utilities – MSTSC

- Also known as Remote Desktop Connection
- Allows you to create a connection to a remote computer



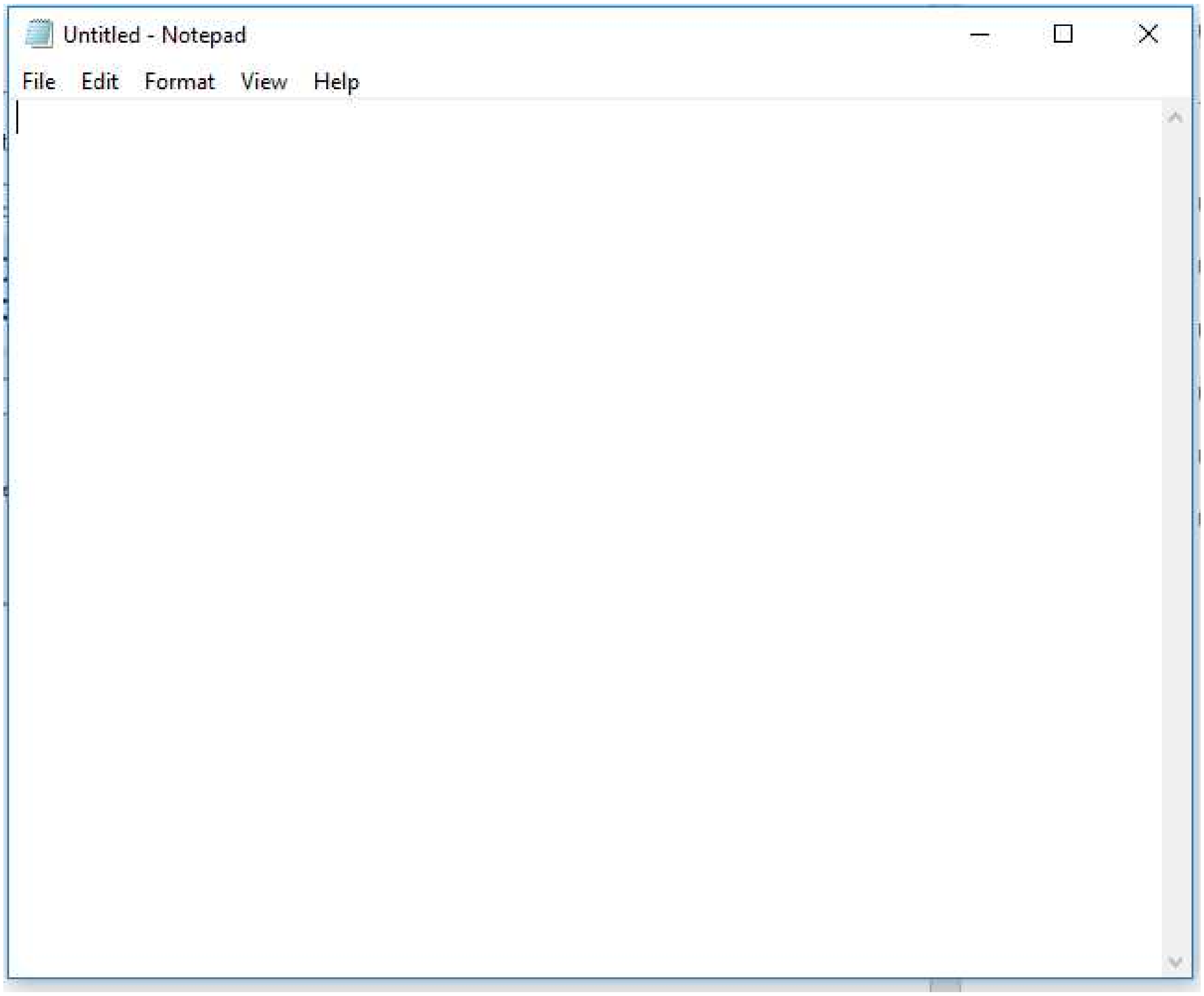
Computer: 54.188.249.73

User name: administrator

You will be asked for credentials when you connect.

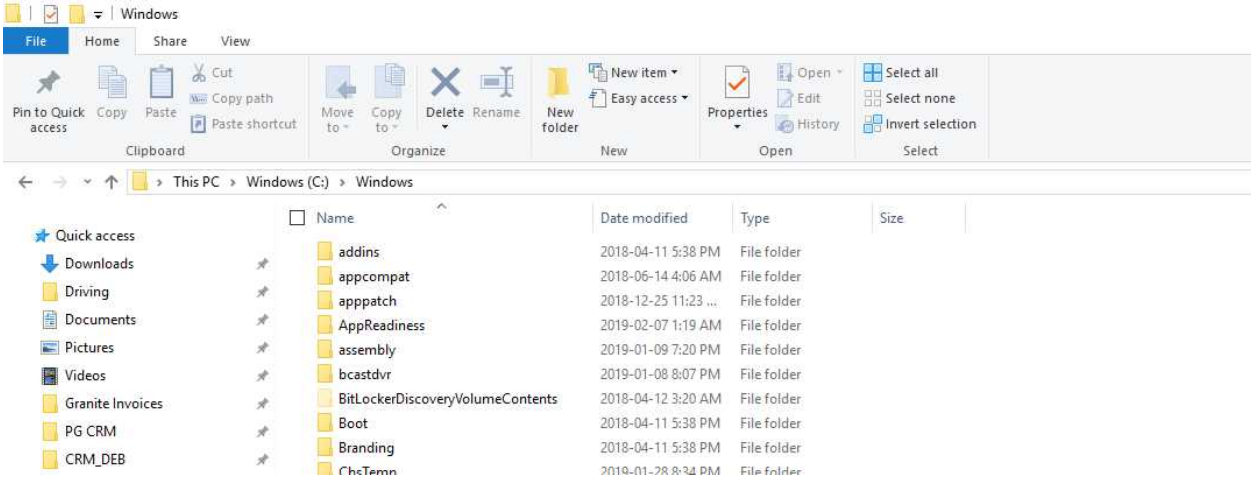
System Utilities – Notepad

- Allows you to create and edit text documents
- Does not provide fonts or formatting



System Utilities – Explorer

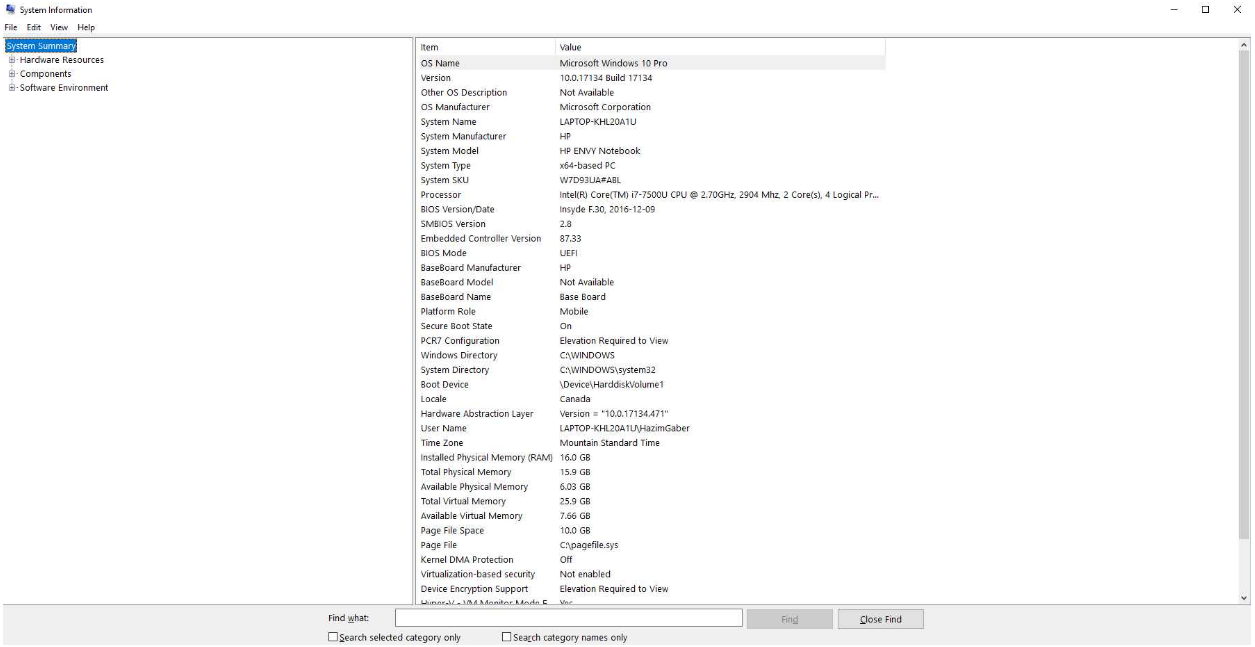
- Allows you to navigate between folders
- Also known as "This PC"
- In the top left, you can pin folders that you access most frequently
- In the right, you can navigate between different folders
- At the top, there are buttons to rename, delete, move, or copy selected files (although you can right click on a file/folder to do the same thing)
- There is also an address bar that shows you where in the folder hierarchy you are; you can type in a different address to go to another folder



Name	Date modified	Type	Size
addins	2018-04-11 5:38 PM	File folder	
appcompat	2018-06-14 4:06 AM	File folder	
apppatch	2018-12-25 11:23 ...	File folder	
AppReadiness	2019-02-07 1:19 AM	File folder	
assembly	2019-01-09 7:20 PM	File folder	
bcastdvr	2019-01-08 8:07 PM	File folder	
BitLockerDiscoveryVolumeContents	2018-04-12 3:20 AM	File folder	
Boot	2018-04-11 5:38 PM	File folder	
Branding	2018-04-11 5:38 PM	File folder	
ChsTemp	2019-01-28 8:34 PM	File folder	

System Utilities – msinfo32

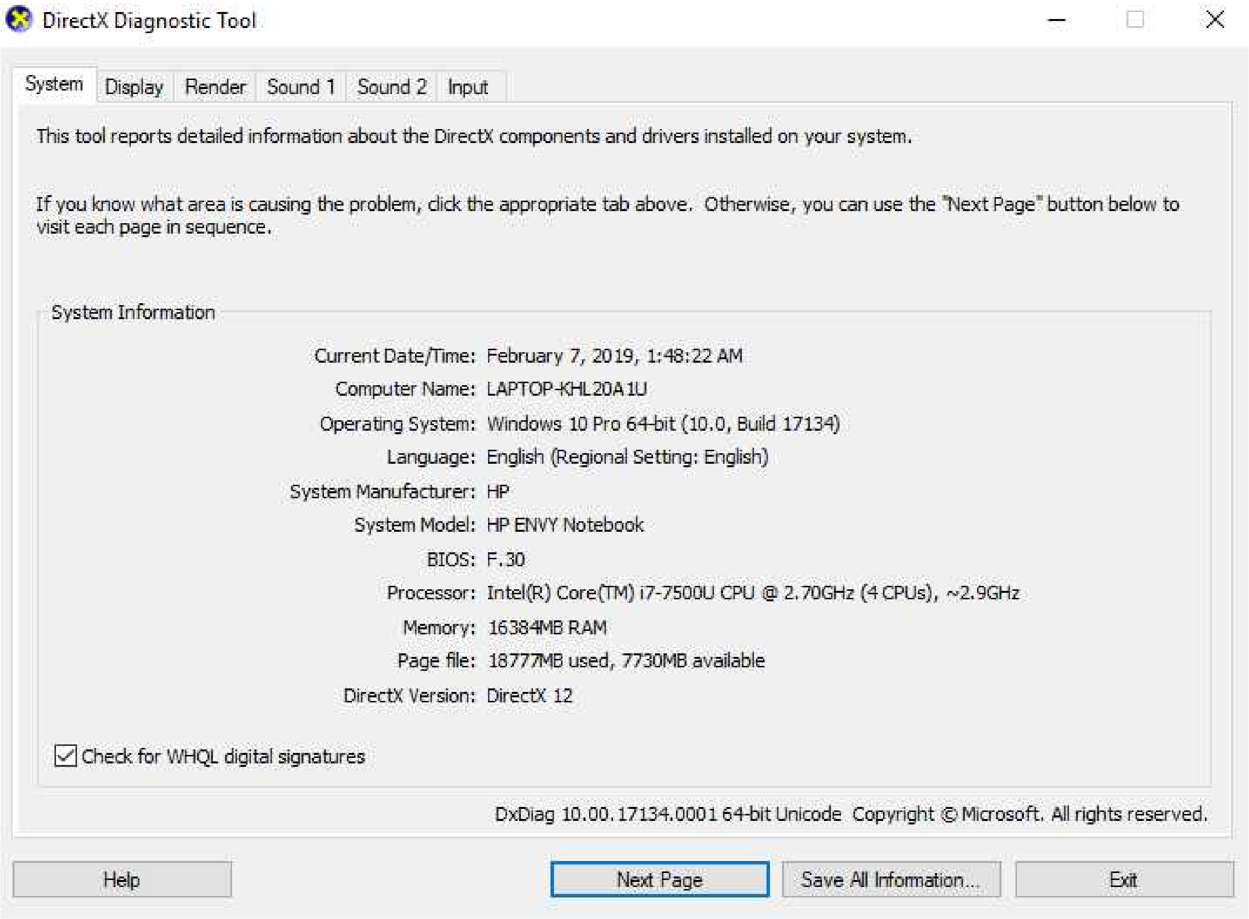
- Provides information about the computer
- Includes the operating system version, the processor type, and the amount of RAM
- Also lists the hardware installed and the details about the software environment



Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.17134 Build 17134
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	LAPTOP-KHL20A1U
System Manufacturer	HP
System Model	HP ENVY Notebook
System Type	x64-based PC
System SKU	W7D93UA#ABL
Processor	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 2904 Mhz, 2 Core(s), 4 Logical Pr...
BIOS Version/Date	Insyde F.30, 2016-12-09
SMBIOS Version	2.8
Embedded Controller Version	87.33
BIOS Mode	UEFI
BaseBoard Manufacturer	HP
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Mobile
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	Canada
Hardware Abstraction Layer	Version = "10.0.17134.471"
User Name	LAPTOP-KHL20A1U\HazimGaber
Time Zone	Mountain Standard Time
Installed Physical Memory (RAM)	16.0 GB
Total Physical Memory	15.9 GB
Available Physical Memory	6.03 GB
Total Virtual Memory	25.9 GB
Available Virtual Memory	7.66 GB
Page File Space	10.0 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Not enabled
Device Encryption Support	Elevation Required to View
Hyper-V - VM Monitor Mode E	Yes

System Utilities – DxDiag

- Runs DirectX diagnostics
- Runs diagnostics for sound and video drivers
- DirectX is a set of Microsoft APIs (Application Programming Interfaces) that allow software developers to write programs that interact better with common video and sound hardware
- When there are errors with the display or the audio, running the DxDiag tool can help locate errors



This tool reports detailed information about the DirectX components and drivers installed on your system.

If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.

System Information

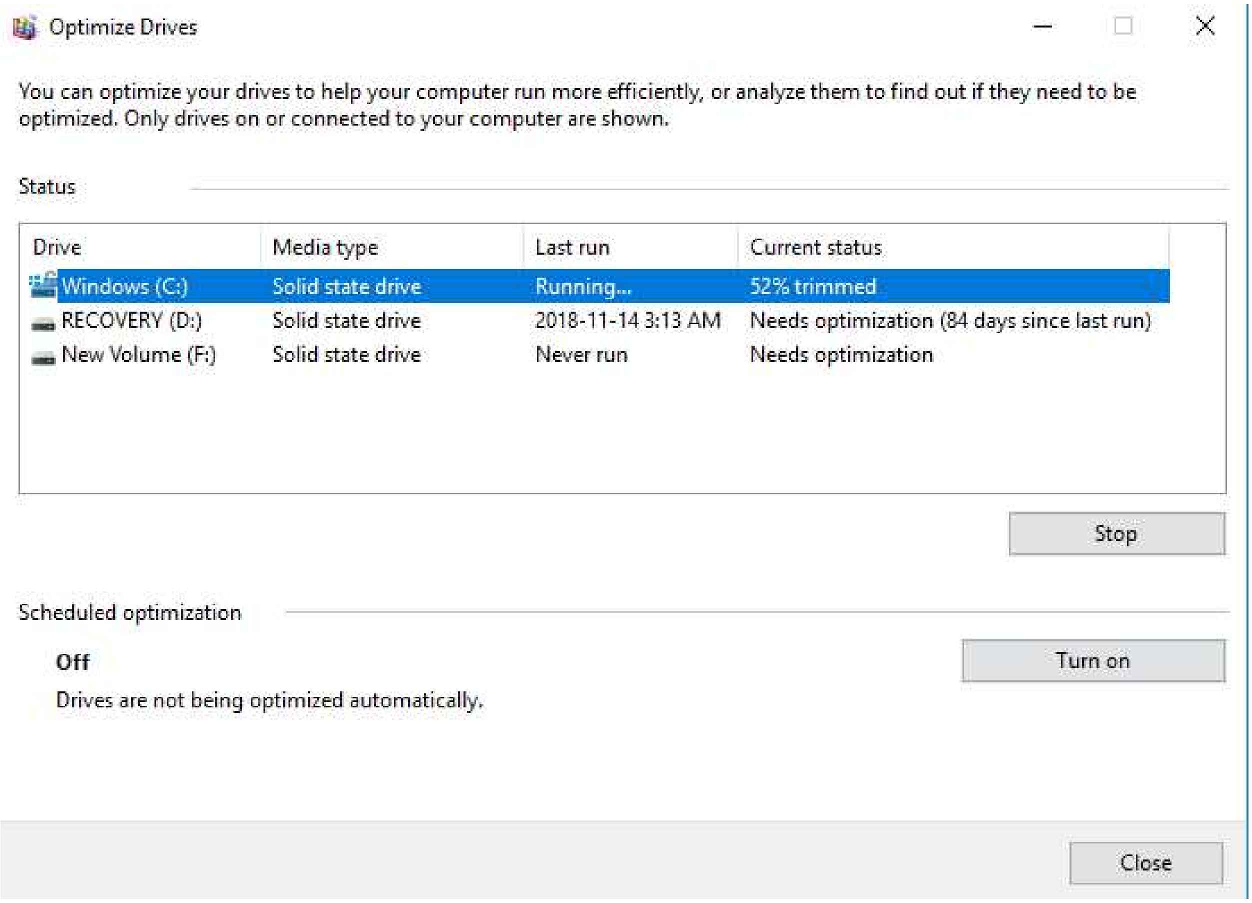
Current Date/Time: February 7, 2019, 1:48:22 AM
Computer Name: LAPTOP-KHL20A1U
Operating System: Windows 10 Pro 64-bit (10.0, Build 17134)
Language: English (Regional Setting: English)
System Manufacturer: HP
System Model: HP ENVY Notebook
BIOS: F.30
Processor: Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz (4 CPUs), ~2.9GHz
Memory: 16384MB RAM
Page file: 18777MB used, 7730MB available
DirectX Version: DirectX 12

☑ Check for WHQL digital signatures

DxDiag 10.00.17134.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.

System Utilities – Disk Defragmenter

- Allows you to defragment your disk
    - A disk becomes fragmented when files are stored in multiple pieces in different parts of the drive (instead of being stored contiguously)
- The defragmentation process can be run when the computer isn't busy



You can optimize your drives to help your computer run more efficiently, or analyze them to find out if they need to be optimized. Only drives on or connected to your computer are shown.

Status

Drive	Media type	Last run	Current status
Windows (C:)	Solid state drive	Running...	52% trimmed
RECOVERY (D:)	Solid state drive	2018-11-14 3:13 AM	Needs optimization (84 days since last run)
New Volume (F:)	Solid state drive	Never run	Needs optimization

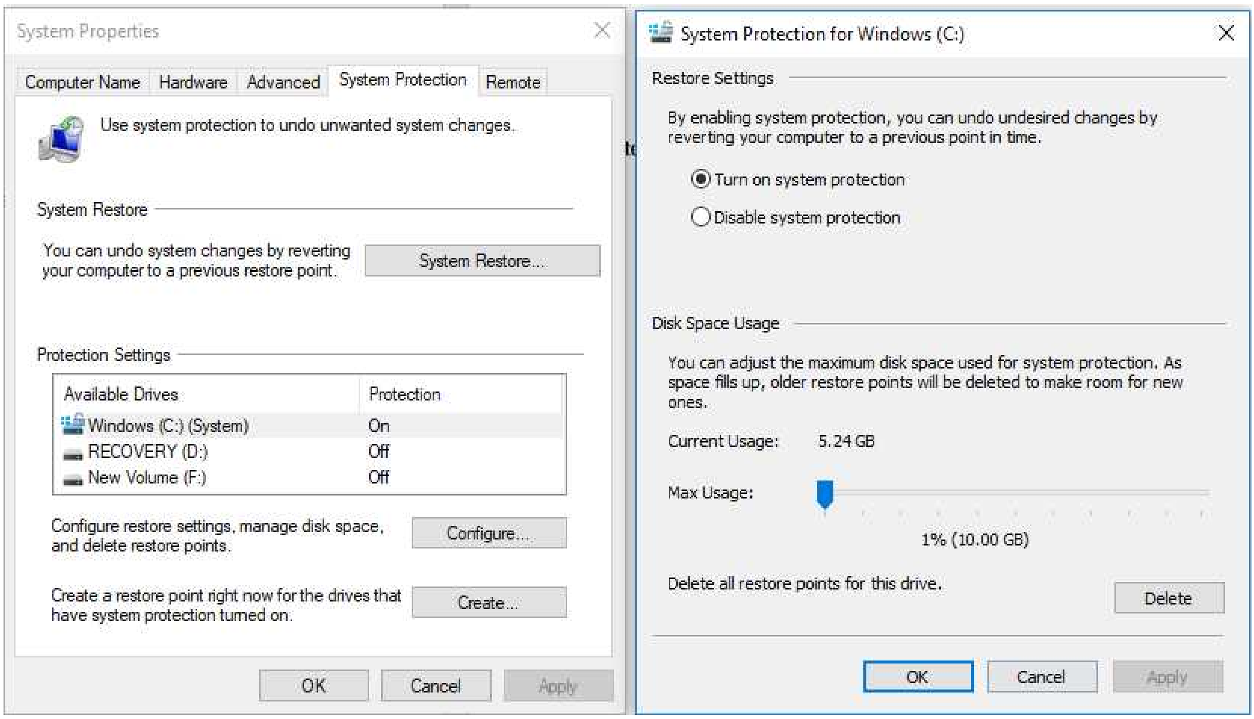
Scheduled optimization

Off

Drives are not being optimized automatically.

System Utilities – System Restore

- Allows you to restore your computer to a previous time and state
    - You can restore your computer only to a “restore point”
    - Windows automatically creates “restore points” when major system changes occur (updates and installation of software programs)
    - You can also manually create a restore point
- Restores system files and drivers
- Does not affect documents
- You must have System Restore enabled for it to function



Use system protection to undo unwanted system changes.

System Restore

You can undo system changes by reverting your computer to a previous restore point.

Protection Settings

Available Drives	Protection
Windows (C:) (System)	On
RECOVERY (D:)	Off
New Volume (F:)	Off

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

Restore Settings

By enabling system protection, you can undo undesired changes by reverting your computer to a previous point in time.

● Turn on system protection

○ Disable system protection

Disk Space Usage

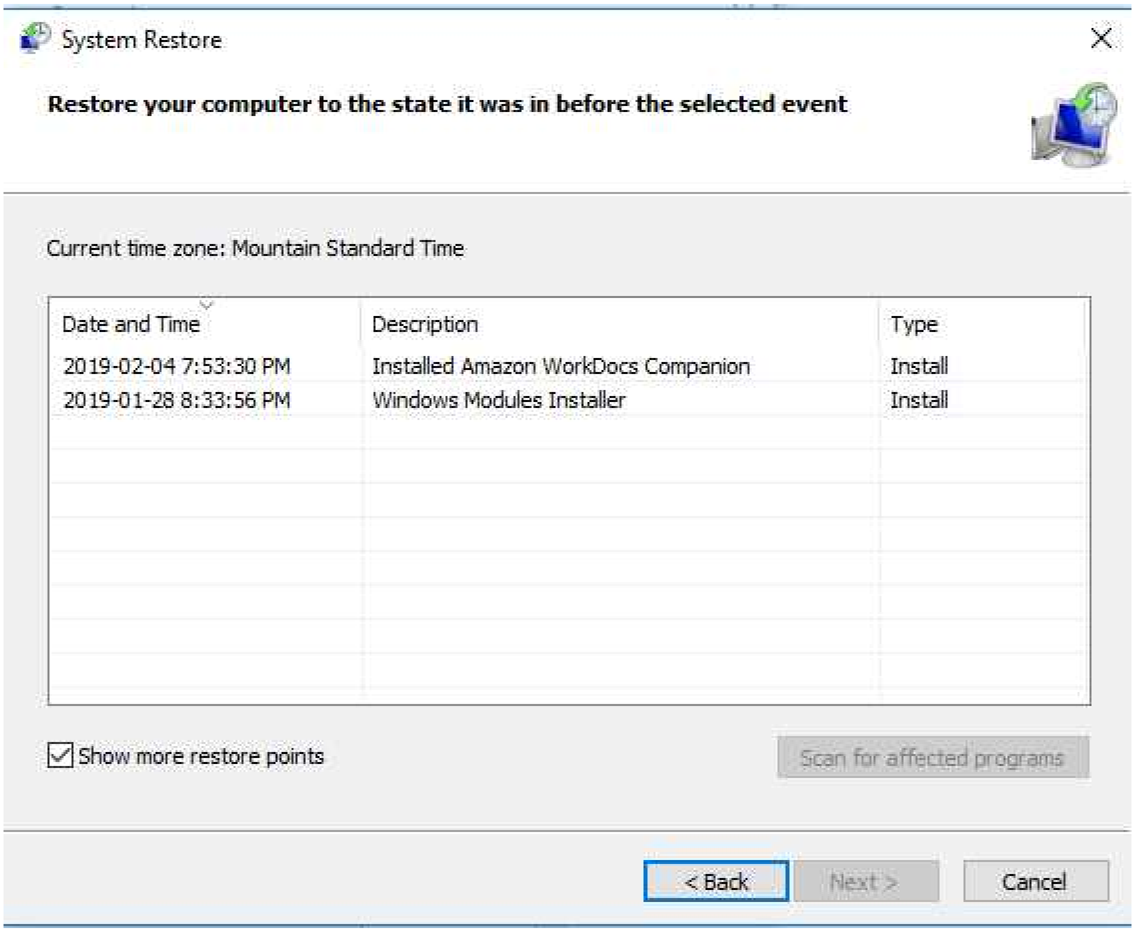
You can adjust the maximum disk space used for system protection. As space fills up, older restore points will be deleted to make room for new ones.

Current Usage: 5.24 GB

Max Usage: 1% (10.00 GB)

Delete all restore points for this drive.

- When restoring, Windows will show you a list of available restore points



Restore your computer to the state it was in before the selected event

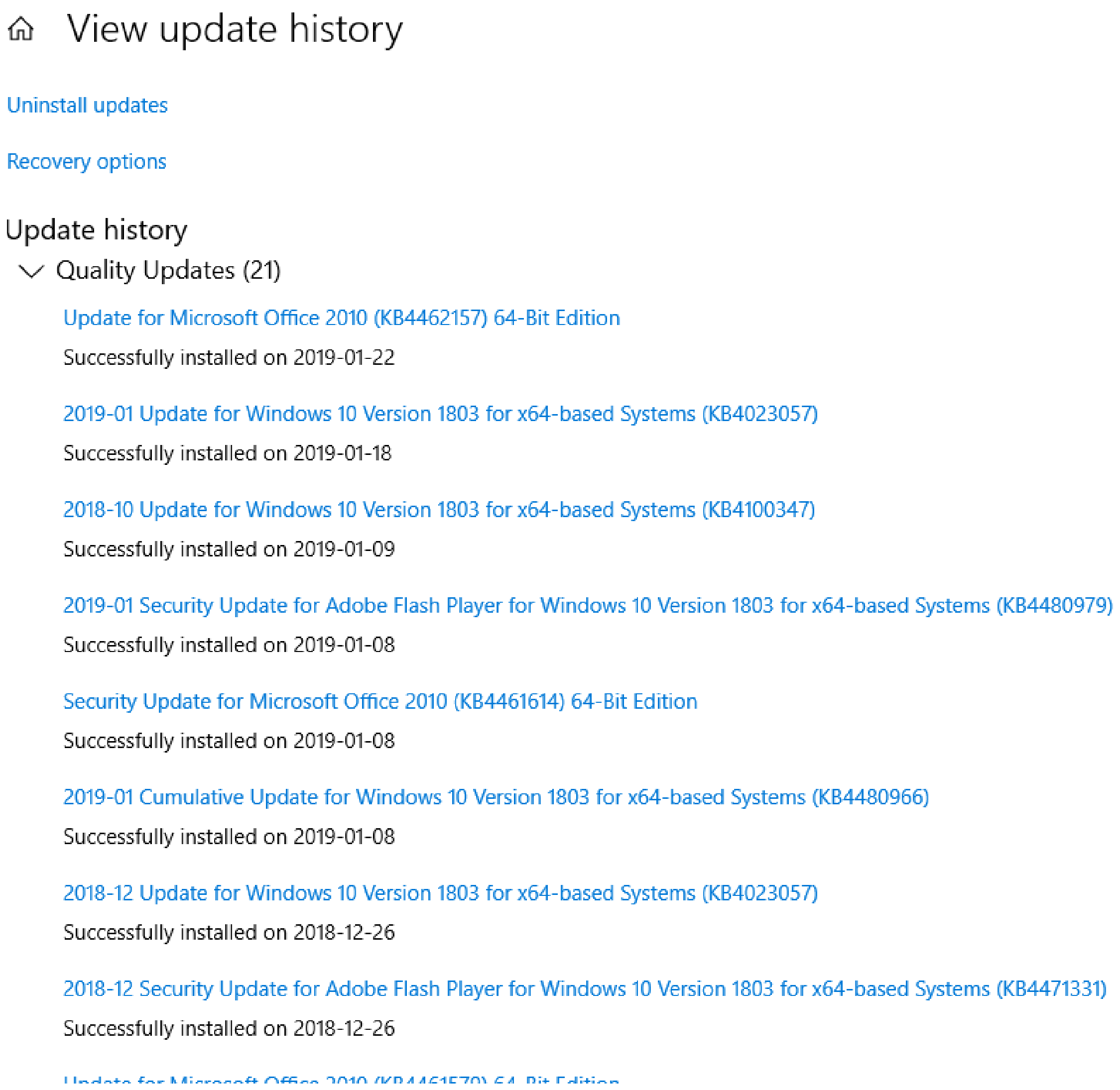
Current time zone: Mountain Standard Time

Date and Time	Description	Type
2019-02-04 7:53:30 PM	Installed Amazon WorkDocs Companion	Install
2019-01-28 8:33:56 PM	Windows Modules Installer	Install

☑ Show more restore points

System Utilities – Windows Update

- With Windows 10, updates are mandatory
- Windows Update automatically checks with Microsoft servers for available updates
  - Updates are downloaded in the background
  - Updates are installed automatically
  - You can choose a time to install the update (when your computer isn't busy)
- You can view a list of updates previously installed



View update history

Uninstall updates

Recovery options

Update history

Quality Updates (21)

Update for Microsoft Office 2010 (KB4462157) 64-Bit Edition
Successfully installed on 2019-01-22

2019-01 Update for Windows 10 Version 1803 for x64-based Systems (KB4023057)
Successfully installed on 2019-01-18

2018-10 Update for Windows 10 Version 1803 for x64-based Systems (KB4100347)
Successfully installed on 2019-01-09

2019-01 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4480979)
Successfully installed on 2019-01-08

Security Update for Microsoft Office 2010 (KB4461614) 64-Bit Edition
Successfully installed on 2019-01-08

2019-01 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4480966)
Successfully installed on 2019-01-08

2018-12 Update for Windows 10 Version 1803 for x64-based Systems (KB4023057)
Successfully installed on 2018-12-26

2018-12 Security Update for Adobe Flash Player for Windows 10 Version 1803 for x64-based Systems (KB4471331)
Successfully installed on 2018-12-26

Update for Microsoft Office 2010 (KB4461570) 64-Bit Edition

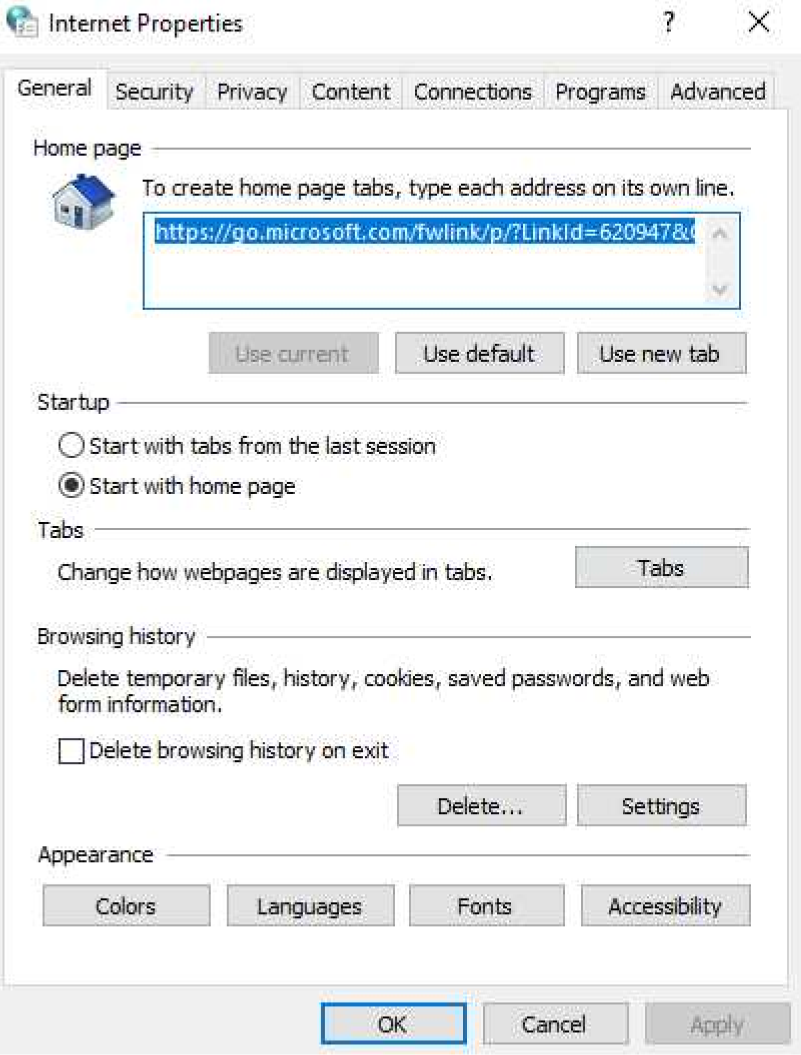
1.6 Given a scenario, use Microsoft Windows Control Panel utilities.

- *Internet Options*
    - *Connections*
    - *Security*
    - *General*
    - *Privacy*
    - *Programs*
    - *Advanced*
- *Display/Display Settings*
    - *Resolution*
    - *Color depth*
    - *Refresh rate*
- *User Accounts*
- *Folder Options*
    - *View hidden files*
    - *Hide extensions*
    - *General options*
    - *View options*
- *System*
    - *Performance (virtual memory)*
    - *Remote settings*
    - *System protection*
- *Windows Firewall*
- *Power Options*
    - *Hibernate*
    - *Power plans*
    - *Sleep/suspend*
    - *Standby*
- *Credential Manager*
- *Programs and features*

- *HomeGroup*
- *Devices and Printers*
- *Sound*
- *Troubleshooting*
- *Network and Sharing Center*
- *Device Manager*
- *BitLocker*
- *Sync Center*

Control Panel – Internet Options

- Internet Options can be accessed from the Control Panel or from Internet Explorer
- Internet settings don't apply to other web browsers (Google Chrome, Firefox, etc.)
- The General tab allows you to
    - Set a homepage (the page that is displayed when you first open Internet Explorer)
    - Allows you to modify the appearance of the browser



To create home page tabs, type each address on its own line.

https://go.microsoft.com/fwlink/p/?LinkId=620947&

○ Start with tabs from the last session

● Start with home page

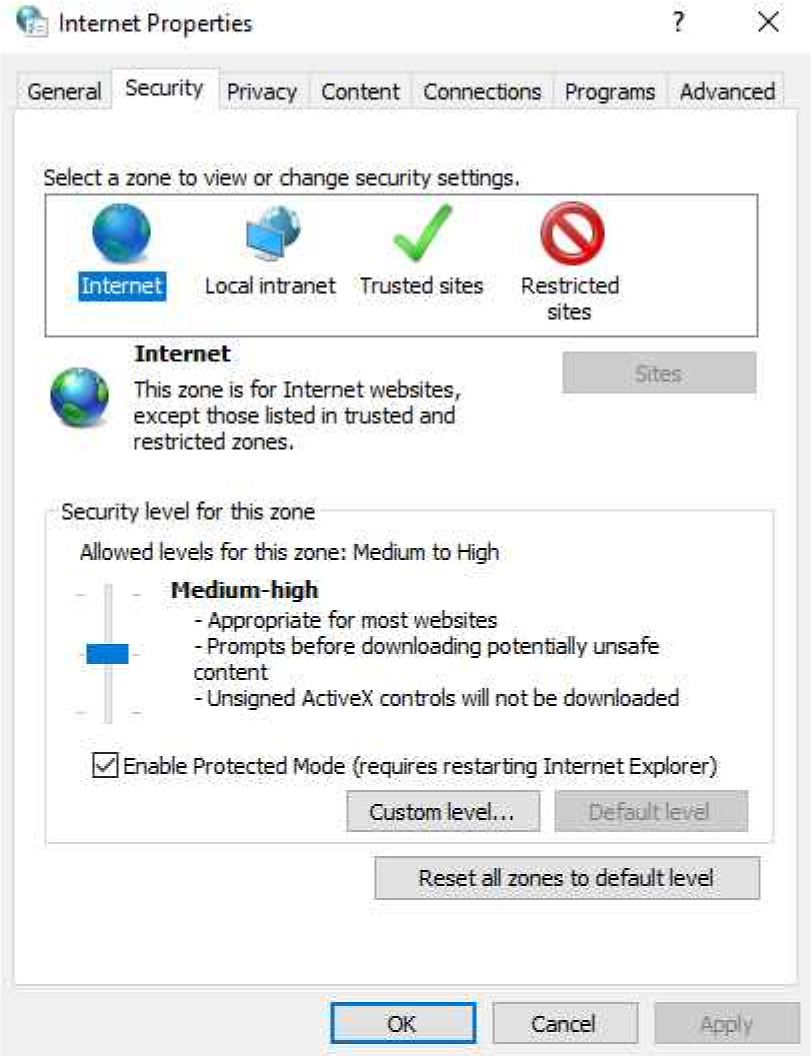
Change how webpages are displayed in tabs.

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

- The Security tab allows you to set the security level for a website
- Websites have four categories
    - Internet: normal websites; Internet websites are normally not trusted
    - Local Intranet: websites on the corporate network; Local Intranet websites are normally trusted

  - Trusted sites: sites that are considered trusted. A user can add websites to the Trusted Sites list
  - Restricted sites: sites that are not trusted. A user can add websites to the Restricted sites list



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

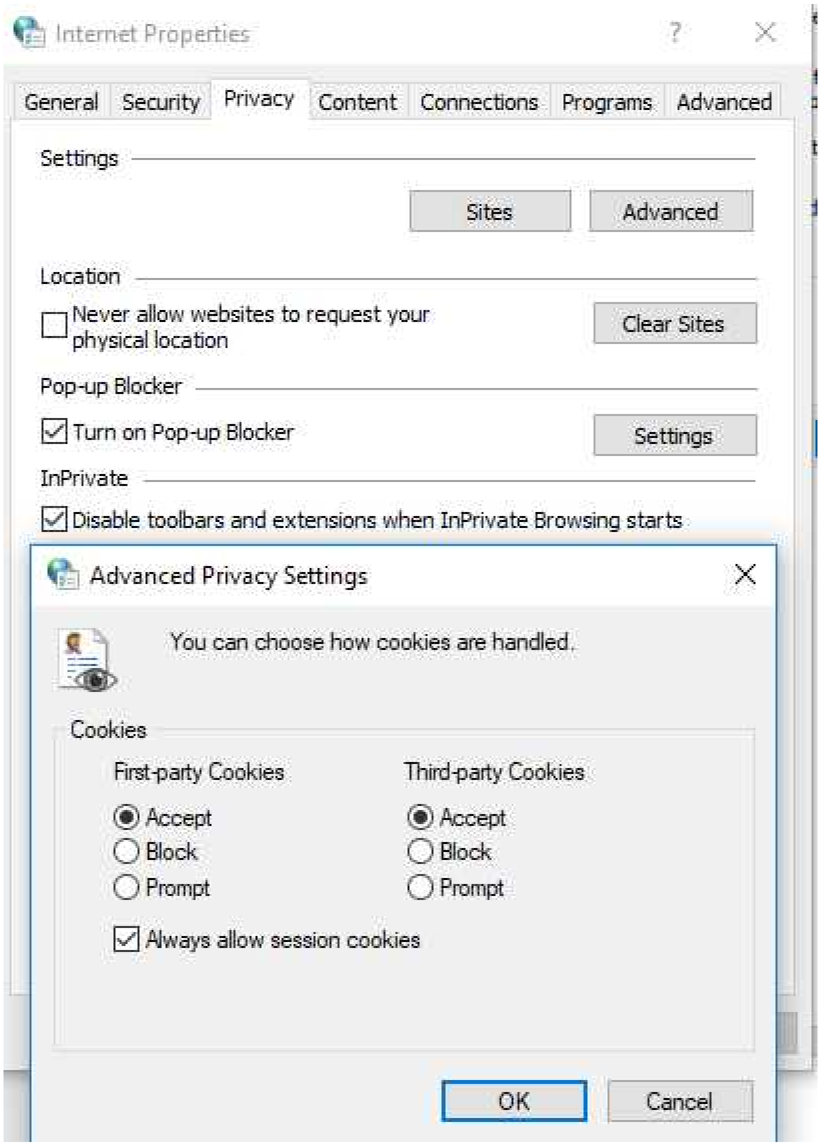
Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

- The Privacy tab allows you to set which websites can save cookies



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Sites | Advanced

Location

□ Never allow websites to request your physical location

Clear Sites

Pop-up Blocker

☑ Turn on Pop-up Blocker

Settings

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

Advanced Privacy Settings

You can choose how cookies are handled.

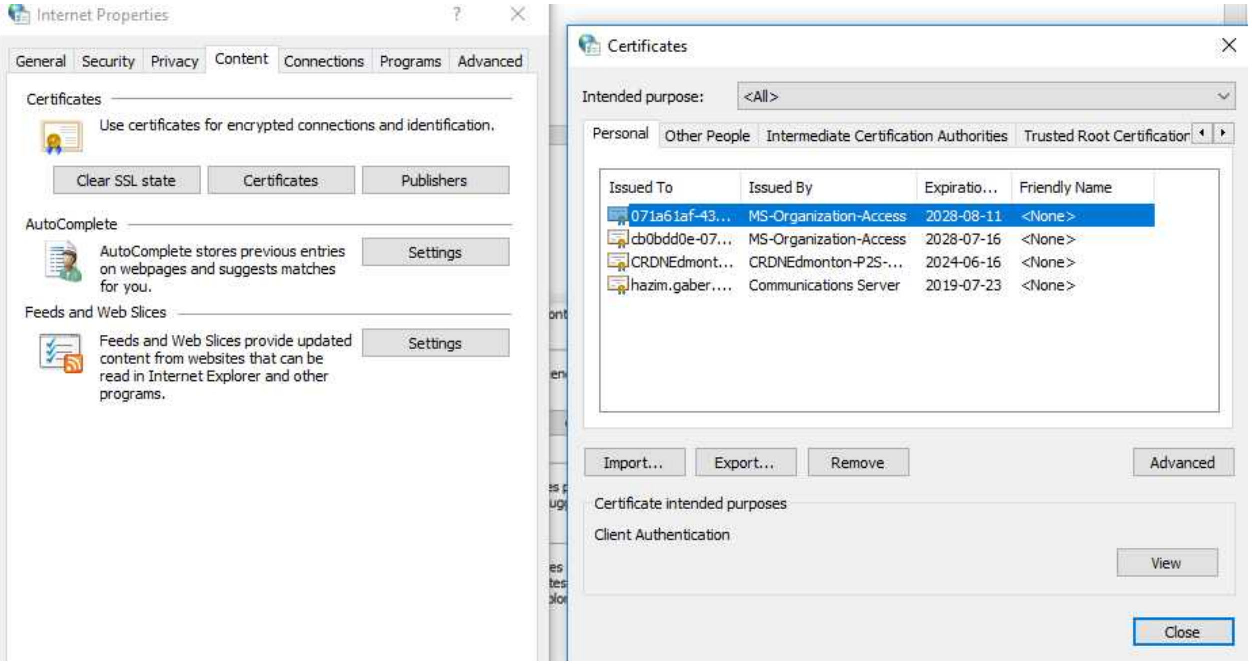
Cookies

First-party Cookies	Third-party Cookies
● Accept	● Accept
○ Block	○ Block
○ Prompt	○ Prompt

☑ Always allow session cookies

OK | Cancel

- The Content tab lists all the certificates installed on the computer



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Certificates

Use certificates for encrypted connections and identification.

AutoComplete

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

Certificates

Intended purpose: <All>

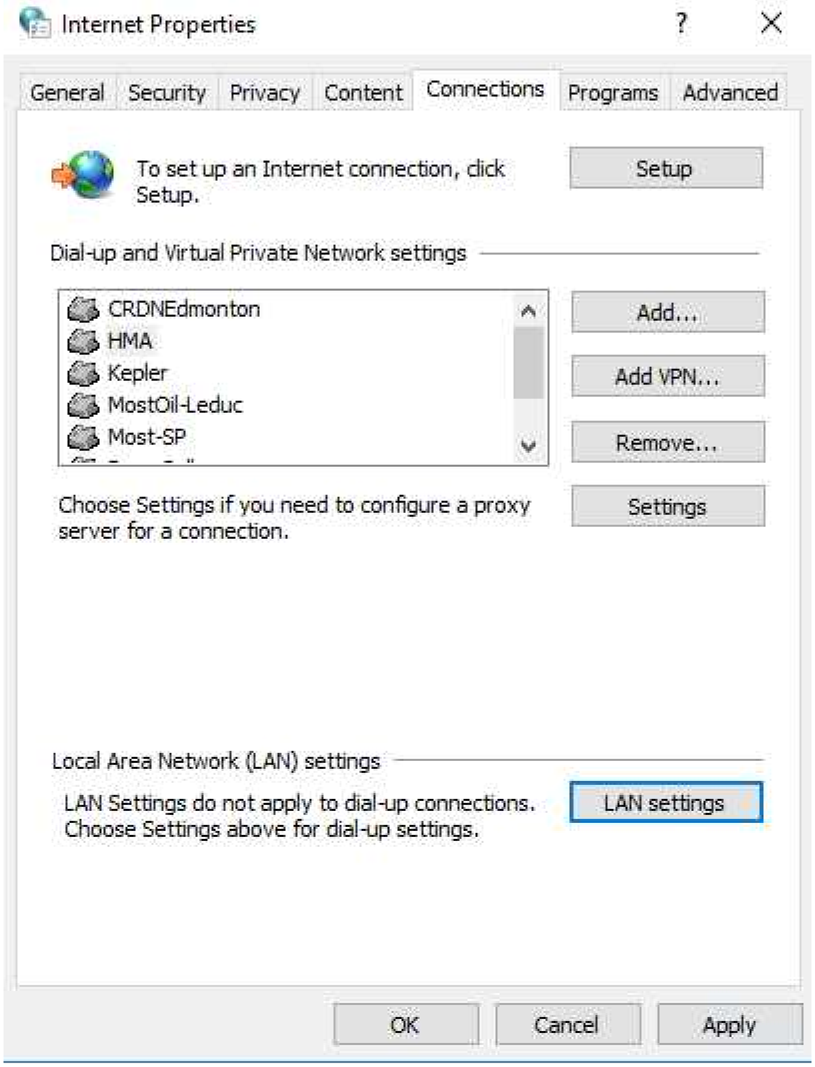
Personal | Other People | Intermediate Certification Authorities | Trusted Root Certificatior

Issued To	Issued By	Expiratio...	Friendly Name
071a61af-43...	MS-Organization-Access	2028-08-11	<None>
cb0bdd0e-07...	MS-Organization-Access	2028-07-16	<None>
CRDNEdmont...	CRDNEdmonton-P2S-...	2024-06-16	<None>
hazim.gaber....	Communications Server	2019-07-23	<None>

Certificate intended purposes

Client Authentication

- The Content tab allows you to add and remove VPN connections



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

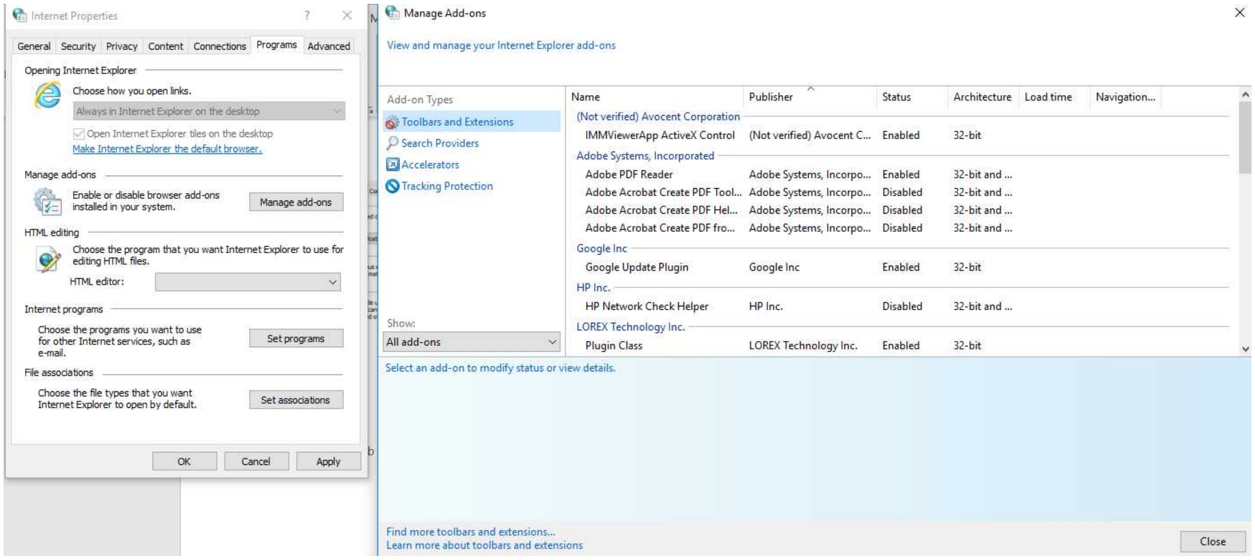
CRDNEdmonton
HMA
Kepler
MostOil-Leduc
Most-SP

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

- The Programs tab lists the installed add-ons and plug-ins
- It also allows you to set default programs for browsing the internet



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Opening Internet Explorer

Choose how you open links.

Always in Internet Explorer on the desktop

☑ Open Internet Explorer tiles on the desktop

Make Internet Explorer the default browser.

Manage add-ons

Enable or disable browser add-ons installed in your system. [Manage add-ons]

HTML editing

Choose the program that you want Internet Explorer to use for editing HTML files.

HTML editor:

Internet programs

Choose the programs you want to use for other Internet services, such as e-mail. [Set programs]

File associations

Choose the file types that you want Internet Explorer to open by default. [Set associations]

[OK] [Cancel] [Apply]

Manage Add-ons

View and manage your Internet Explorer add-ons

Add-on Types

- Toolbars and Extensions
- Search Providers
- Accelerators
- Tracking Protection

Show:

All add-ons

Name	Publisher	Status	Architecture	Load time	Navigation...
(Not verified) Avocent Corporation					
IMMViewerApp ActiveX Control	(Not verified) Avocent C...	Enabled	32-bit		
Adobe Systems, Incorporated					
Adobe PDF Reader	Adobe Systems, Incorpo...	Enabled	32-bit and ...		
Adobe Acrobat Create PDF Tool...	Adobe Systems, Incorpo...	Disabled	32-bit and ...		
Adobe Acrobat Create PDF Hel...	Adobe Systems, Incorpo...	Disabled	32-bit and ...		
Adobe Acrobat Create PDF fro...	Adobe Systems, Incorpo...	Disabled	32-bit and ...		
Google Inc					
Google Update Plugin	Google Inc	Enabled	32-bit		
HP Inc.					
HP Network Check Helper	HP Inc.	Disabled	32-bit and ...		
LOREX Technology Inc.					
Plugin Class	LOREX Technology Inc.	Enabled	32-bit		

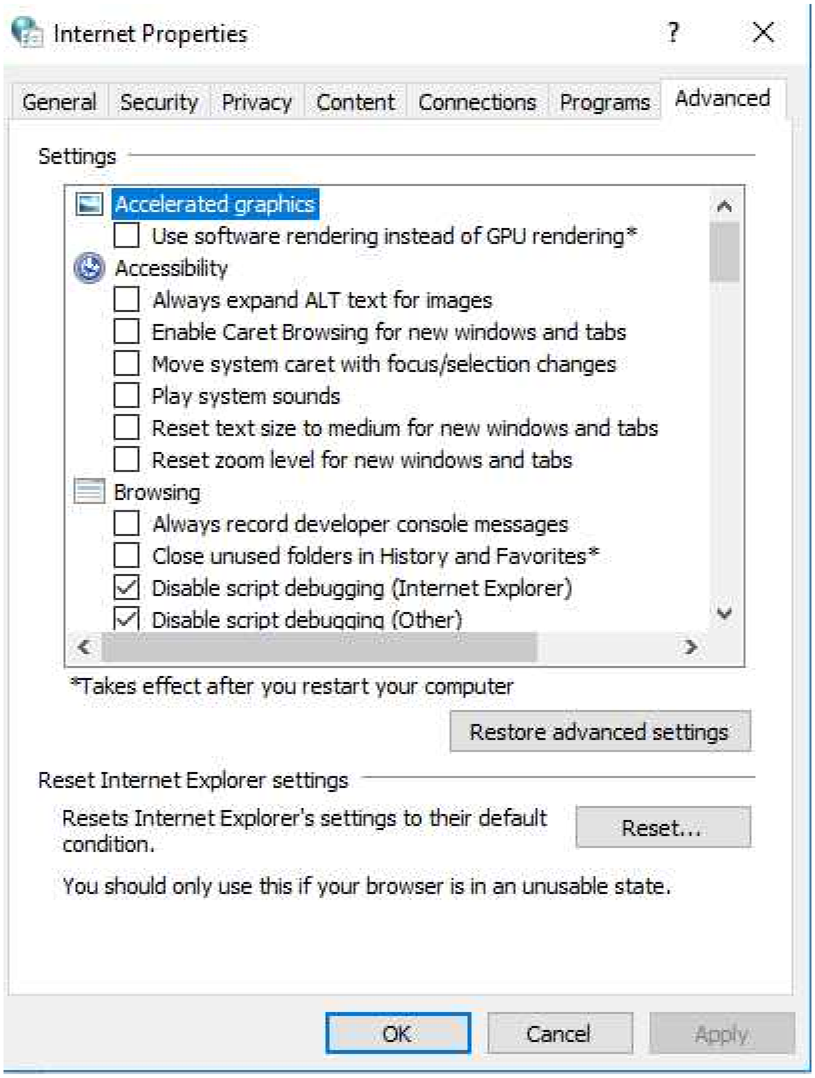
Select an add-on to modify status or view details.

Find more toolbars and extensions...

Learn more about toolbars and extensions

[Close]

- The Advanced tab allows to you to select advanced options such as Accessibility, script debugging, HTTP settings, and security settings



Settings

Accelerated graphics

□ Use software rendering instead of GPU rendering*

Accessibility

□ Always expand ALT text for images

□ Enable Caret Browsing for new windows and tabs

□ Move system caret with focus/selection changes

□ Play system sounds

□ Reset text size to medium for new windows and tabs

□ Reset zoom level for new windows and tabs

Browsing

□ Always record developer console messages

□ Close unused folders in History and Favorites*

☑ Disable script debugging (Internet Explorer)

☑ Disable script debugging (Other)

*Takes effect after you restart your computer

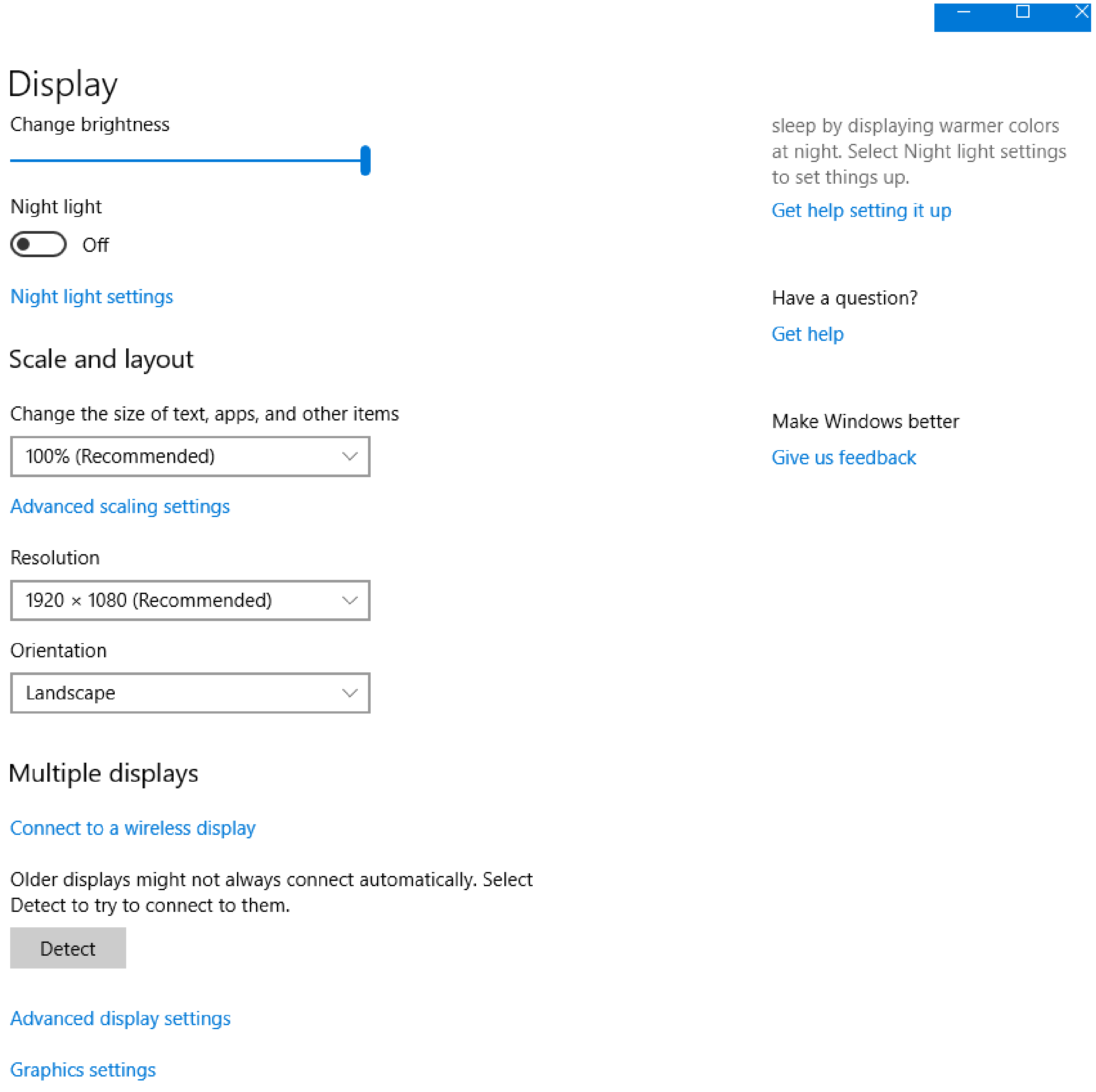
Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Control Panel – Display

- Display settings allows you to
    - Set the brightness (on a laptop screen)
    - Set the scale (zoom)
    - Set the screen resolution
        - Windows will show you the recommended screen resolution
        - The available screen resolutions depend upon the type of graphics card and monitor that are installed
    - Set the order of the displays (when there are multiple displays)



Display

Change brightness

Night light

Off

Night light settings

Scale and layout

Change the size of text, apps, and other items

100% (Recommended)

Advanced scaling settings

Resolution

1920 × 1080 (Recommended)

Orientation

Landscape

Multiple displays

Connect to a wireless display

Older displays might not always connect automatically. Select Detect to try to connect to them.

Detect

Advanced display settings

Graphics settings

sleep by displaying warmer colors at night. Select Night light settings to set things up.

Get help setting it up

Have a question?

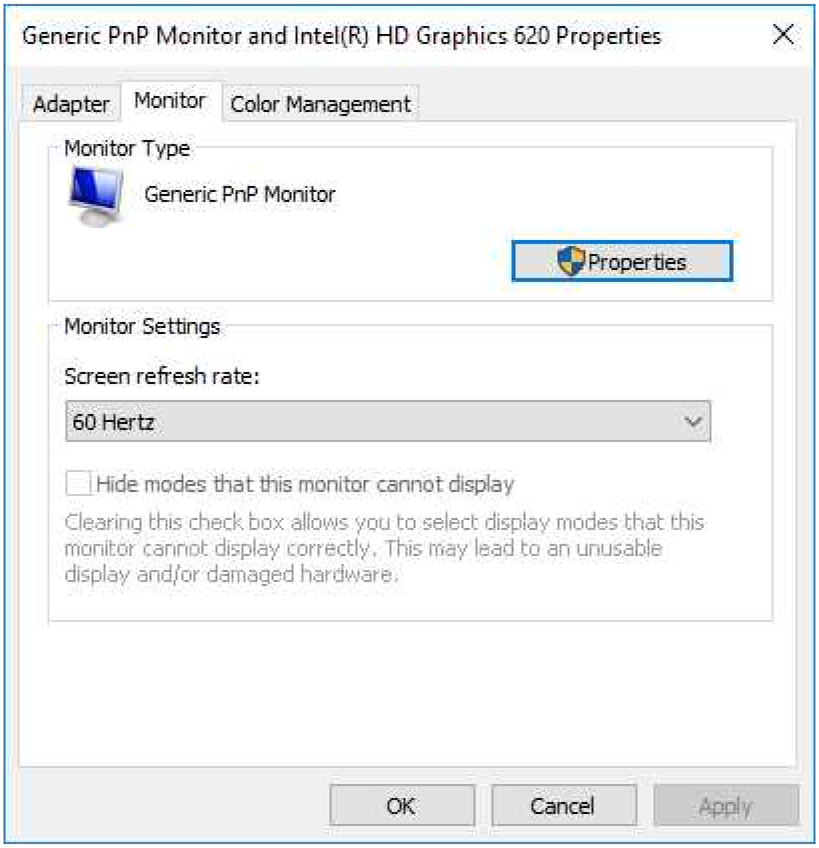
Get help

Make Windows better

Give us feedback

In advanced display settings, you can set the Refresh Rate

- The refresh rate is the speed at which the screen updates (like frames per second)
- 60 Hz is the most common setting
- High-end graphics cards and monitors may offer higher refresh rates



Generic PnP Monitor

Screen refresh rate: 60 Hertz

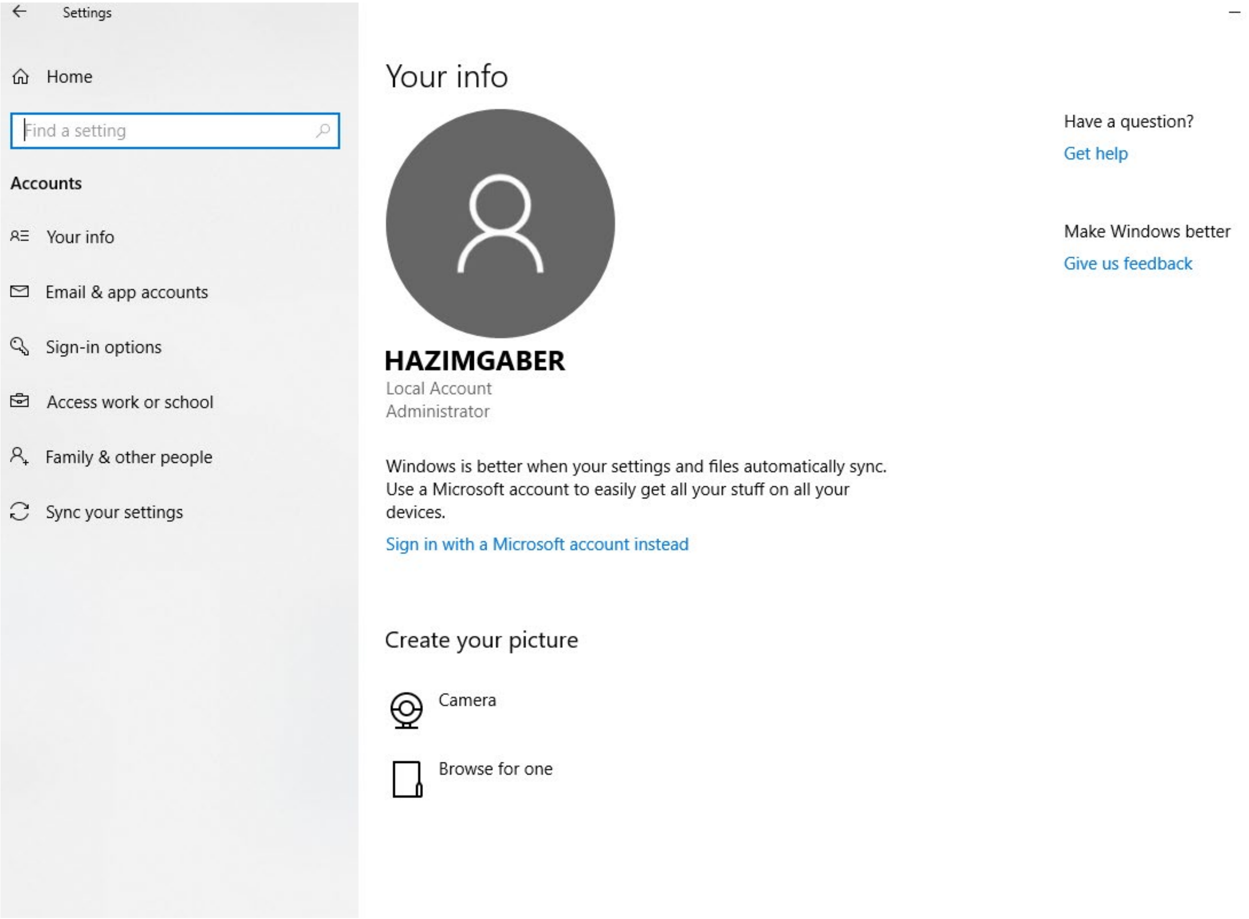
□ Hide modes that this monitor cannot display

Clearing this check box allows you to select display modes that this monitor cannot display correctly. This may lead to an unusable display and/or damaged hardware.

Control Panel – User Accounts

Accounts allows you to set a photo and login type on your own account

- You can choose to log in with a password, a pin, a photo, or with no password
- You can choose to log in with a Microsoft Account
  - If you log in with a Microsoft Account, your password is stored by Microsoft.
  - The computer authenticates your log in with Microsoft (over the internet)
  - The computer will record the last correct password you entered. If your computer is offline and you try to log in, the computer will check your password against the last correct password saved on the computer
- You can change your account from an Administrator to a Standard user
  - There must be at least one admin account on a computer
  - Only an admin has privileges to change account types, add new accounts, or disable accounts
- If your computer is connected to the domain, you won't be able to use the User Accounts feature



Your info

HAZIMGABER
Local Account
Administrator

Windows is better when your settings and files automatically sync. Use a Microsoft account to easily get all your stuff on all your devices.

Sign in with a Microsoft account instead

Create your picture

Camera

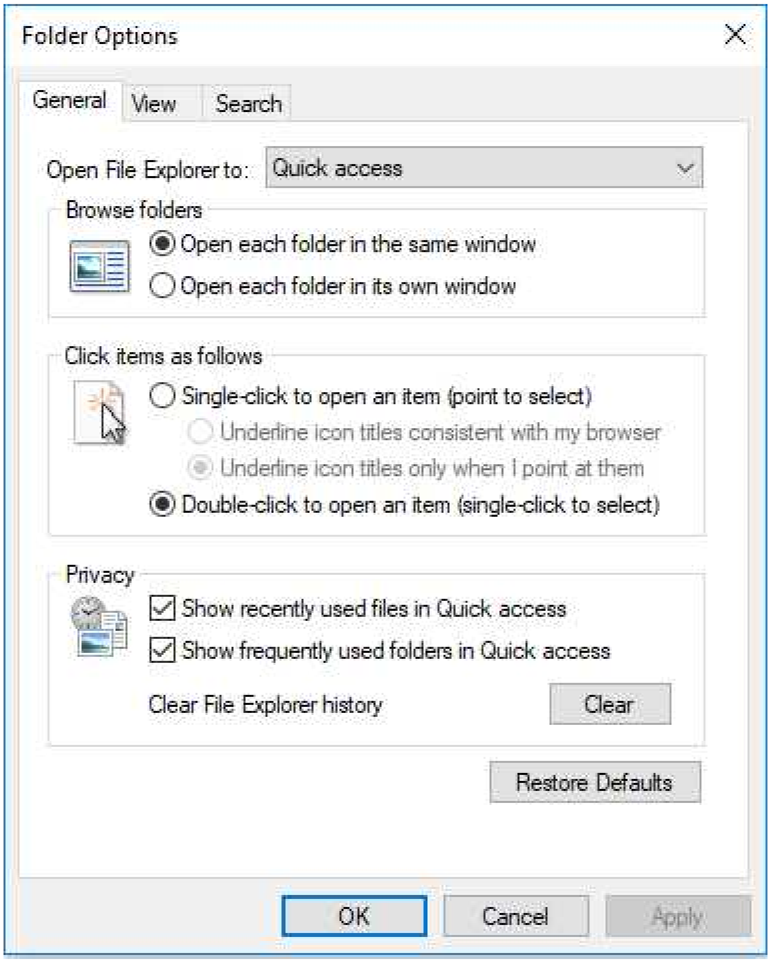
Browse for one

Control Panel – Folder Options

Folder options allows you to control how files and folders are displayed

On the General Tab

- Choose whether to open new folders in the same window or in new windows
- Choose whether an item opens with a single-click or a double-click
- Ability to delete your history (File Explorer remembers the folders you recently visited)



Folder Options

General | View | Search

Open File Explorer to: Quick access

Browse folders

● Open each folder in the same window

○ Open each folder in its own window

Click items as follows

○ Single-click to open an item (point to select)

○ Underline icon titles consistent with my browser

● Underline icon titles only when I point at them

● Double-click to open an item (single-click to select)

Privacy

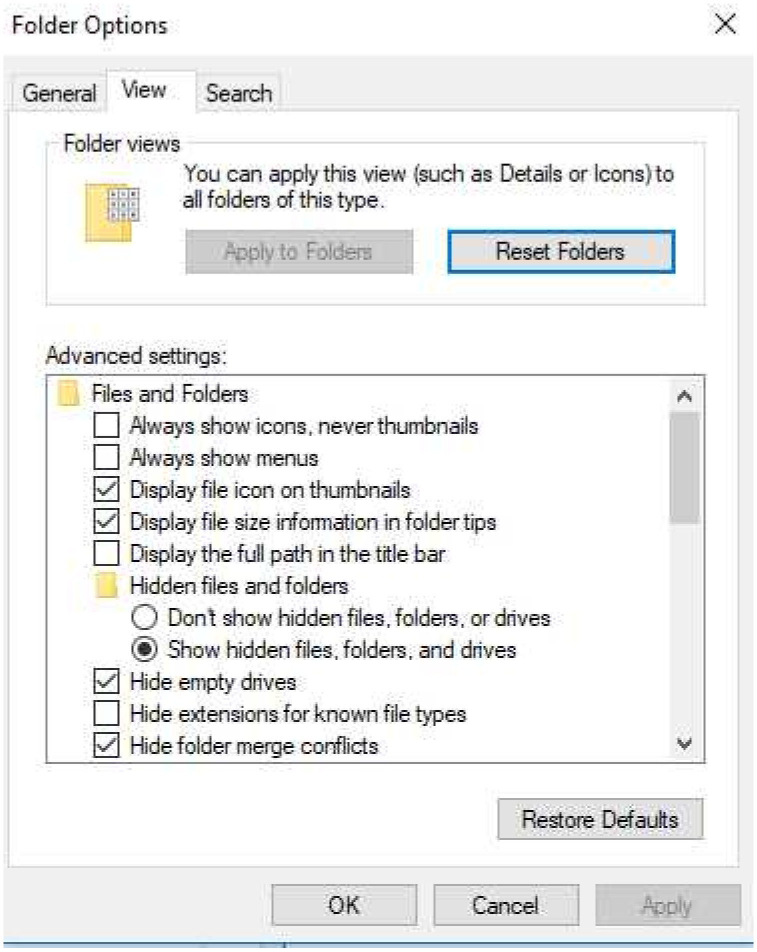
☑ Show recently used files in Quick access

☑ Show frequently used folders in Quick access

Clear File Explorer history

On the Advanced Tab

- Can choose to show or hide hidden files and/or protected operating system files
- Can choose to show or hide other items such as the status bar, drive letters, file sizes, etc.



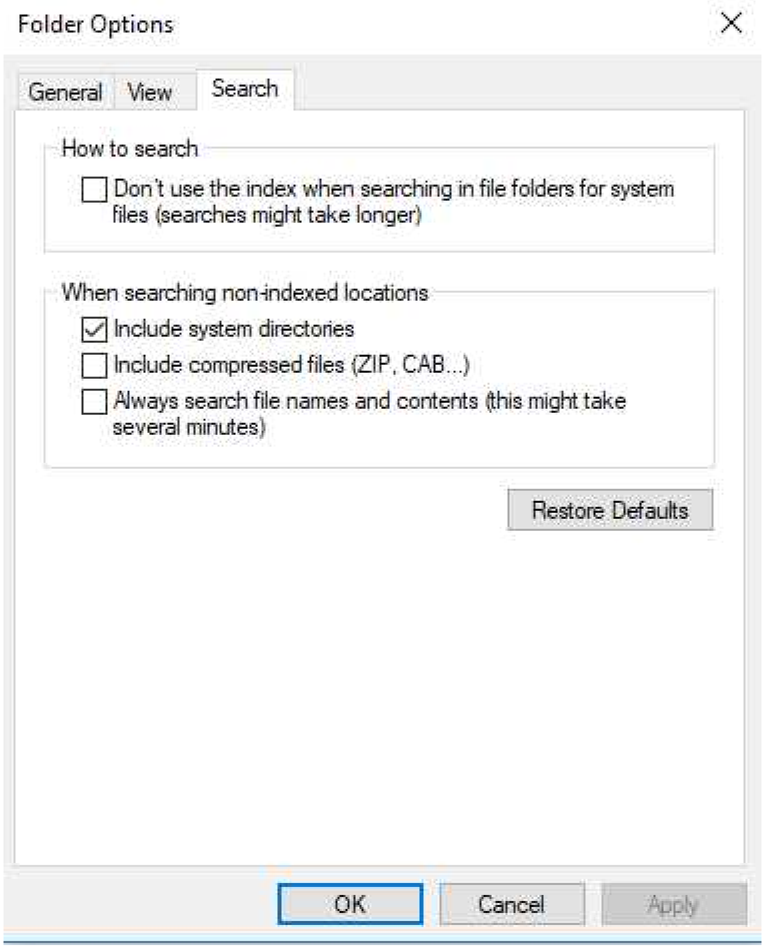
You can apply this view (such as Details or Icons) to all folders of this type.

Advanced settings:

Files and Folders
- □ Always show icons, never thumbnails
- □ Always show menus
- ☑ Display file icon on thumbnails
- ☑ Display file size information in folder tips
- □ Display the full path in the title bar
- Hidden files and folders
  - ○ Don't show hidden files, folders, or drives
  - ● Show hidden files, folders, and drives
- ☑ Hide empty drives
- □ Hide extensions for known file types
- ☑ Hide folder merge conflicts

On the Search Tab

- Choose whether to use the search index (Windows creates an index of file names). Using the index makes the search faster, but less accurate, especially for slower computers.
- Choose whether to search directories that aren't indexed



How to search

□ Don't use the index when searching in file folders for system files (searches might take longer)

When searching non-indexed locations

☑ Include system directories

□ Include compressed files (ZIP, CAB...)

□ Always search file names and contents (this might take several minutes)

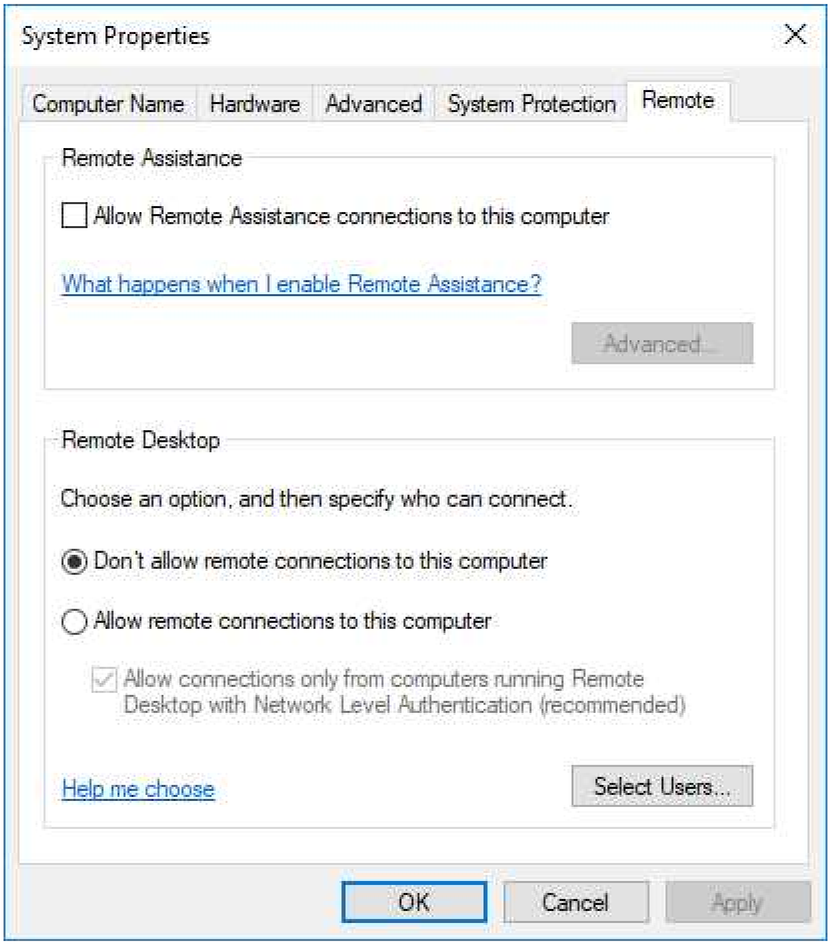
Control Panel – System (Performance, Remote, Protection)

In Windows 10, Performance is a separate utility

- In older versions of windows, Performance is part of System Properties

Remote allows remote access to the computer (via Remote Desktop)

- If you disable it, others may still be able to connect via third-party applications



System Properties

Remote Assistance

□ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

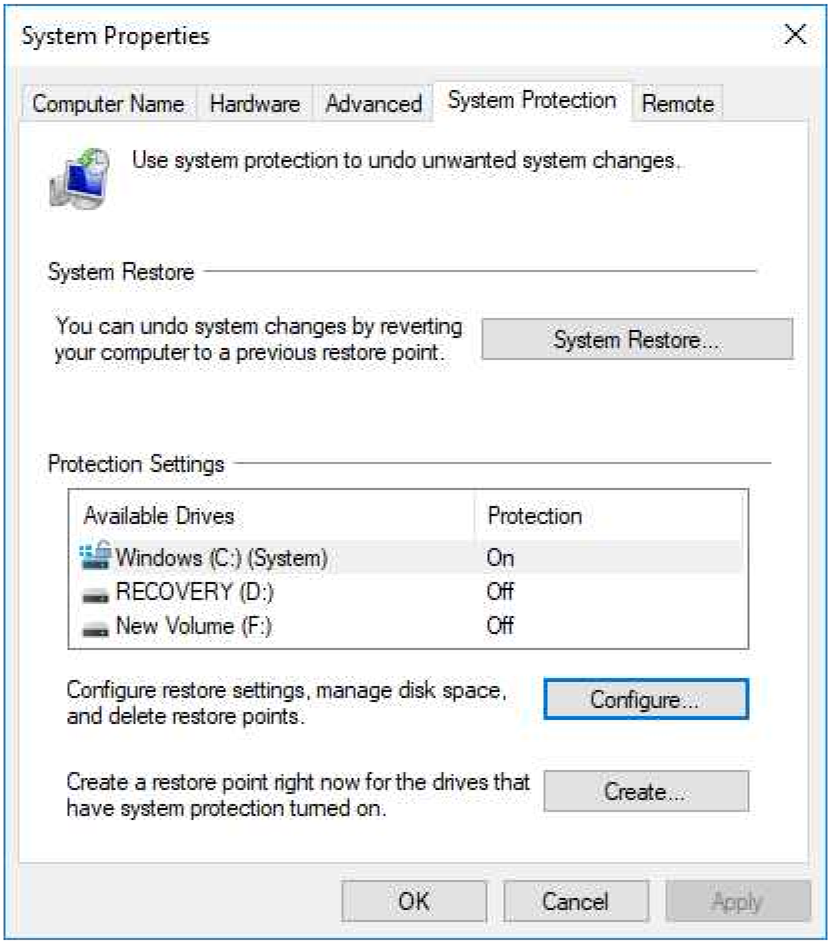
● Don't allow remote connections to this computer

○ Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Protection allows you to enable/disable System Restore (already mentioned)



Use system protection to undo unwanted system changes.

You can undo system changes by reverting your computer to a previous restore point.

Available Drives	Protection
Windows (C:) (System)	On
RECOVERY (D:)	Off
New Volume (F:)	Off

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

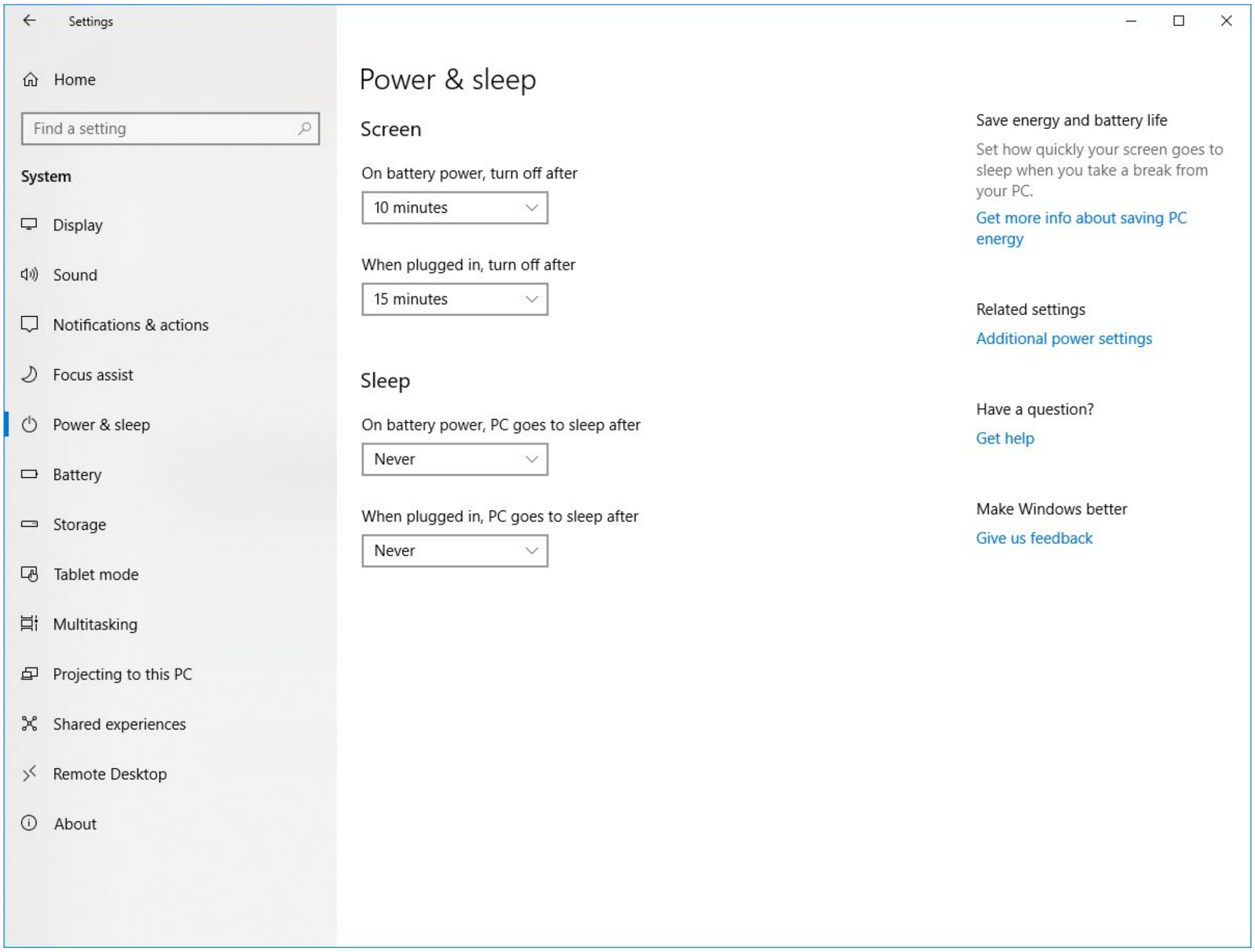
Control Panel – Windows Firewall

See the previous section for details about Windows Firewall

Control Panel – Power Options

Allows you to choose how many minutes of inactivity are required until the computer goes to sleep / turns off the screen

- Options are between one minute and never
- Different settings for when the computer is on battery power and when it is plugged in



Power & sleep

Screen

On battery power, turn off after: 10 minutes

When plugged in, turn off after: 15 minutes

Sleep

On battery power, PC goes to sleep after: Never

When plugged in, PC goes to sleep after: Never

Save energy and battery life

Set how quickly your screen goes to sleep when you take a break from your PC.

Get more info about saving PC energy

Related settings

Additional power settings

Have a question?

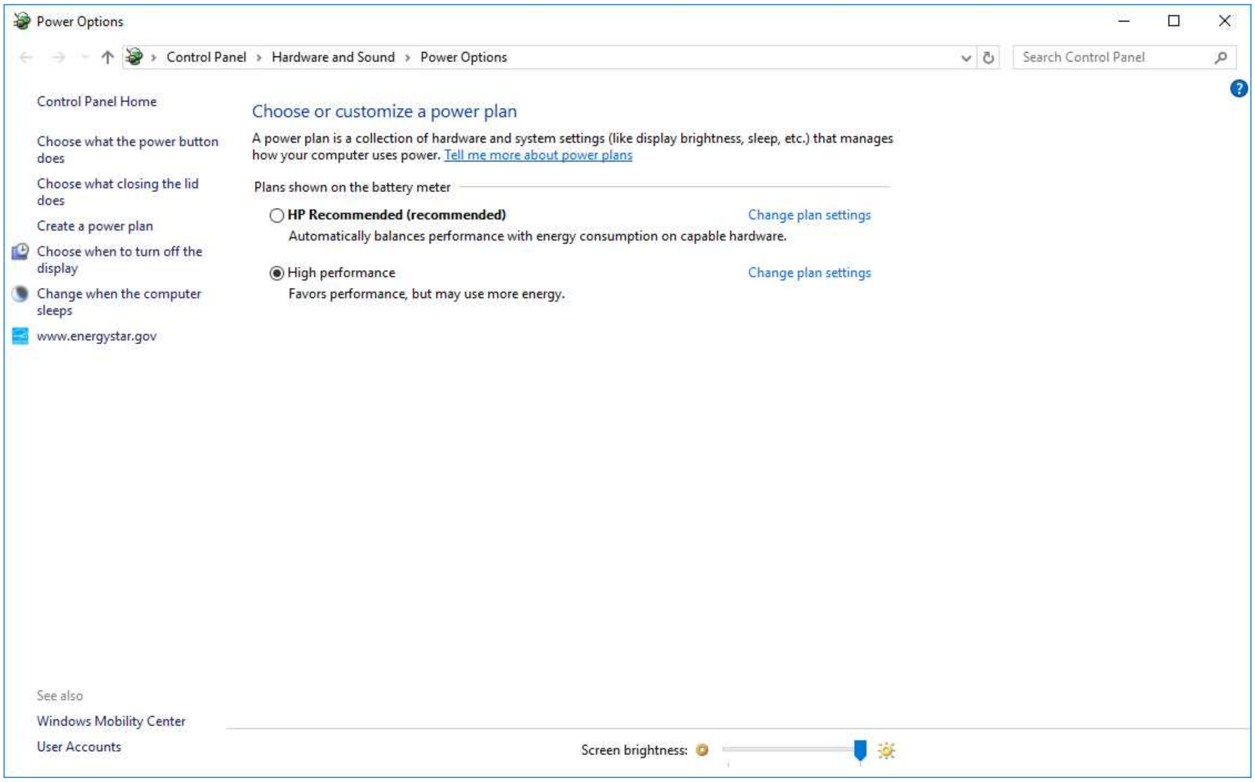
Get help

Make Windows better

Give us feedback

Advanced Power Options

- Choose what the power button does
    - Can Sleep, Hibernate, Shut Down, Turn off the Display, or Do Nothing
    - Different choices for when the computer is on battery and when it is plugged into a wall outlet
- Choose what closing the lid does (on a laptop)
    - Can Sleep, Hibernate, Shut Down, or Do Nothing
    - Different choices for when the computer is on battery and when it is plugged into a wall outlet
- Other settings
    - Turn on fast startup (allows you to turn the computer on in a few seconds by saving some data to the hard disk)
    - Choose whether Sleep, Hibernate, and Lock options are available
        - Sleep is a “low power” mode. The computer is still running and will slowly drain the battery if not connected to a wall outlet.
        - Hibernate forces the computer to shut down (but the contents of the RAM are saved to disk). When the computer starts back up, the contents of the RAM are reloaded back to memory and the computer resumes as before.
- Choose or customize a power plan


Power Options
Control Panel > Hardware and Sound > Power Options
Search Control Panel
Control Panel Home
Choose what the power button does
Choose what closing the lid does
Create a power plan
Choose when to turn off the display
Change when the computer sleeps
www.energystar.gov
See also
Windows Mobility Center
User Accounts

Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

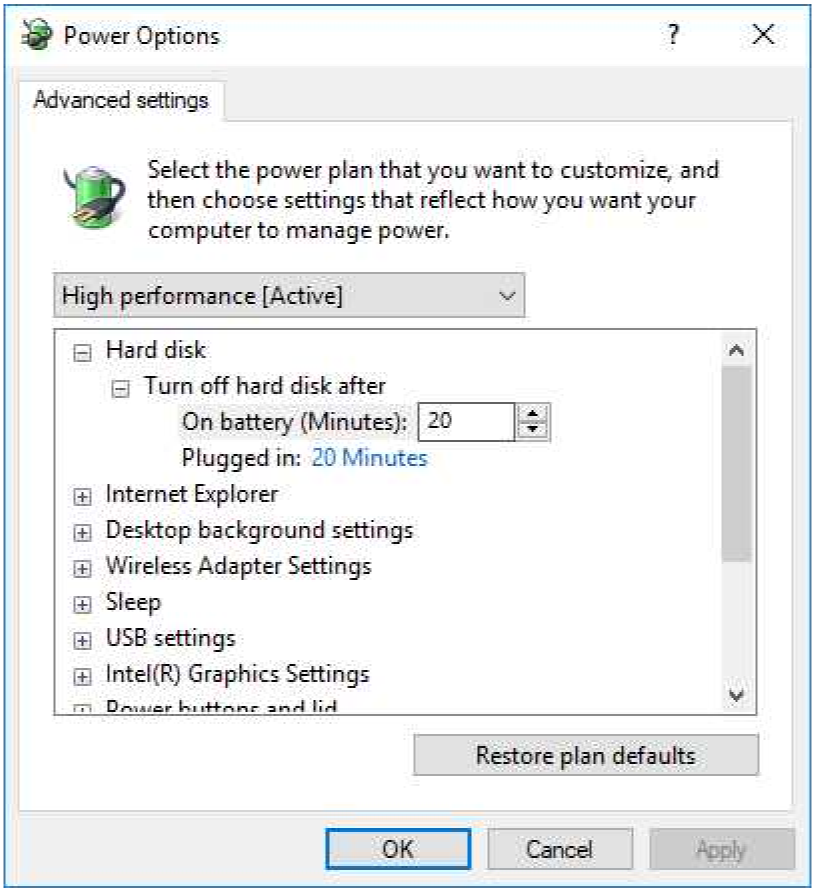
Plans shown on the battery meter

○ **HP Recommended (recommended)** Change plan settings
Automatically balances performance with energy consumption on capable hardware.

● High performance Change plan settings
Favors performance, but may use more energy.

Screen brightness:

- You can customize additional settings for the computer hardware and limit how much power they consume when the computer is plugged in vs when it is on battery



Power Options

Advanced settings

Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.

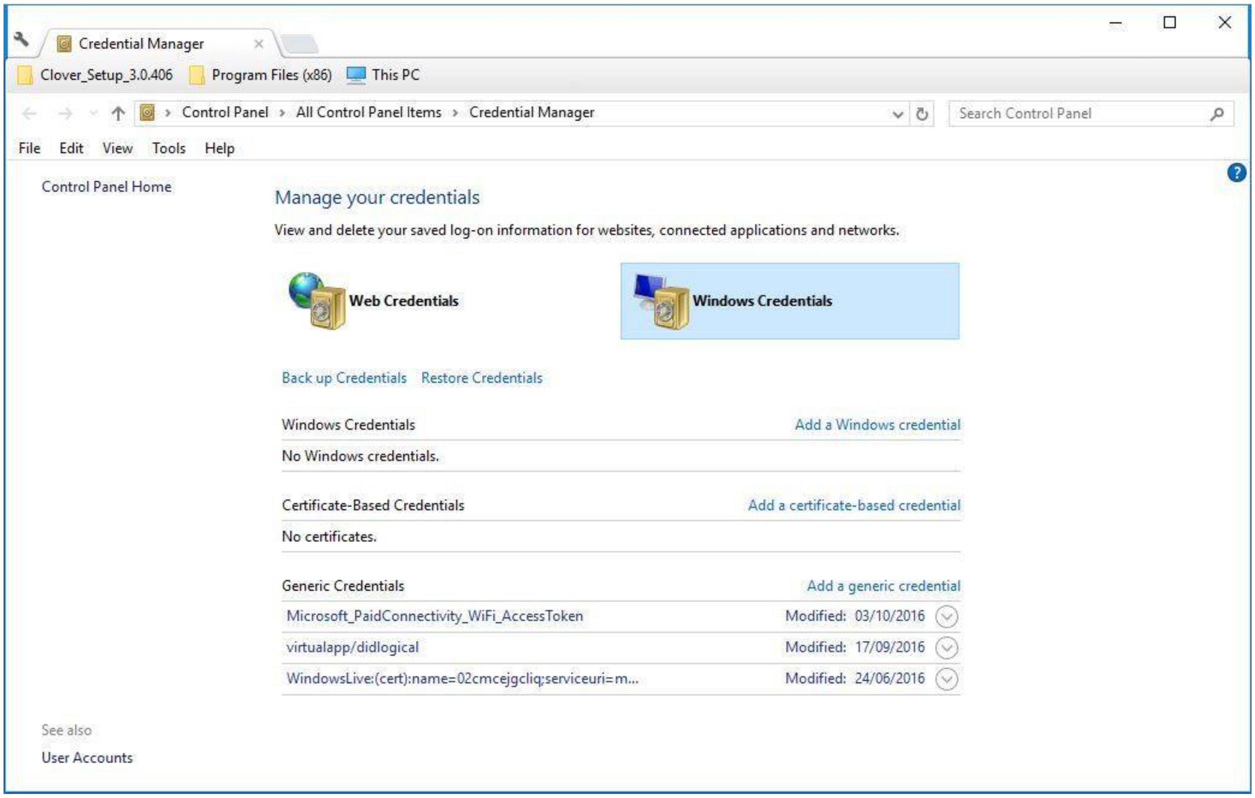
High performance [Active]

- ⊟ Hard disk
  - ⊟ Turn off hard disk after
    - On battery (Minutes): 20
    - Plugged in: 20 Minutes
- ⊞ Internet Explorer
- ⊞ Desktop background settings
- ⊞ Wireless Adapter Settings
- ⊞ Sleep
- ⊞ USB settings
- ⊞ Intel(R) Graphics Settings
- ⊞ Power buttons and lid

Control Panel – Credential Manager

Displays a list of stored credentials

- Windows will save usernames/passwords and certificates in the credential manager
- If you're having trouble logging into a resource, try deleting the credential and recreating it



Manage your credentials

View and delete your saved log-on information for websites, connected applications and networks.

Windows Credentials

No Windows credentials.

Certificate-Based Credentials

No certificates.

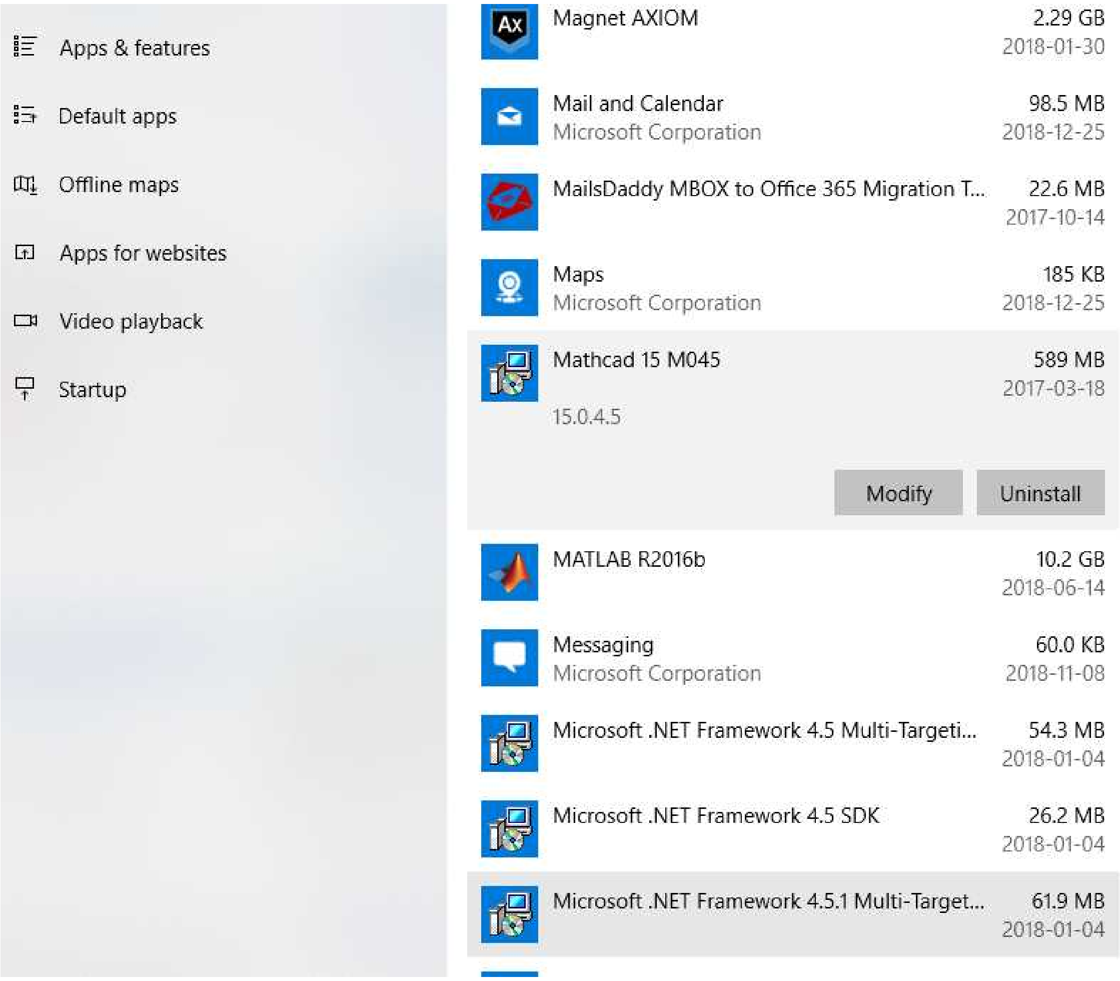
Generic Credentials

Microsoft_PaidConnectivity_WiFi_AccessToken	Modified: 03/10/2016
virtualapp/didlogical	Modified: 17/09/2016
WindowsLive:(cert):name=02cmcejgcliq;serviceuri=m...	Modified: 24/06/2016

Control Panel – Programs and Features

View a list of installed programs and details such as

- Program name
- Program manufacturer
- Size of the program
- Date installed
- Option to uninstall the program (will either uninstall in the background, or launch the uninstall wizard). You can only uninstall one program at a time.
- Option to modify or repair the program's installation (only available on some programs)



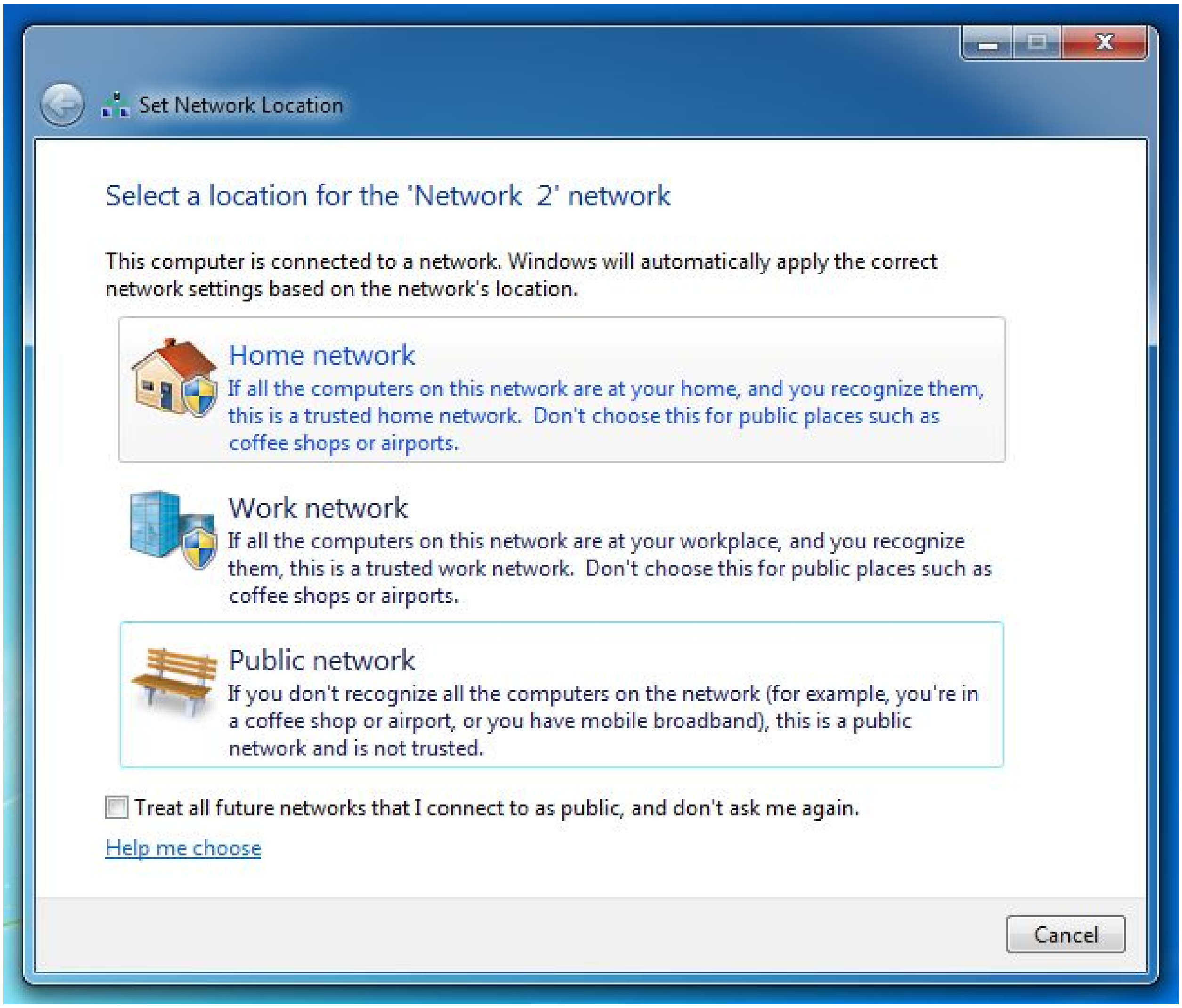
Magnet AXIOM	2.29 GB 2018-01-30
Mail and Calendar Microsoft Corporation	98.5 MB 2018-12-25
MailsDaddy MBOX to Office 365 Migration T...	22.6 MB 2017-10-14
Maps Microsoft Corporation	185 KB 2018-12-25
Mathcad 15 M045 15.0.4.5	589 MB 2017-03-18
MATLAB R2016b	10.2 GB 2018-06-14
Messaging Microsoft Corporation	60.0 KB 2018-11-08
Microsoft .NET Framework 4.5 Multi-Targeti...	54.3 MB 2018-01-04
Microsoft .NET Framework 4.5 SDK	26.2 MB 2018-01-04
Microsoft .NET Framework 4.5.1 Multi-Target...	61.9 MB 2018-01-04

Under Optional Features

- It is possible to add or delete windows features

Control Panel – Homegroup

- A Homegroup allows multiple computers on a LAN to share data with each other
- Homegroups have been discontinued in Windows 10 due to having too many issues
  - Replaced by the Workgroup
  - The default workgroup name is "WORKGROUP"
- Can share files, folders, and printers
- All computers must be set to be part of the same homegroup in order for them to communicate
- You must set the network as a "home" network, and enable sharing



Select a location for the 'Network 2' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

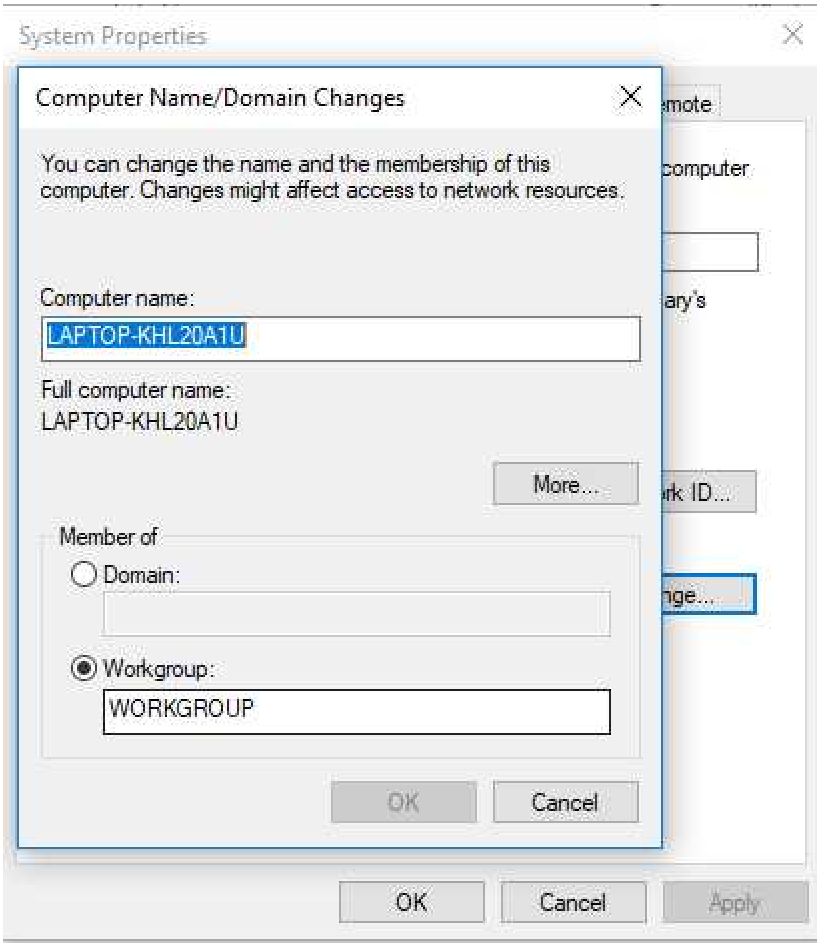
Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

☐ Treat all future networks that I connect to as public, and don't ask me again.

- Set the homegroup from System Properties



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: LAPTOP-KHL20A1U

Full computer name:
LAPTOP-KHL20A1U

Member of

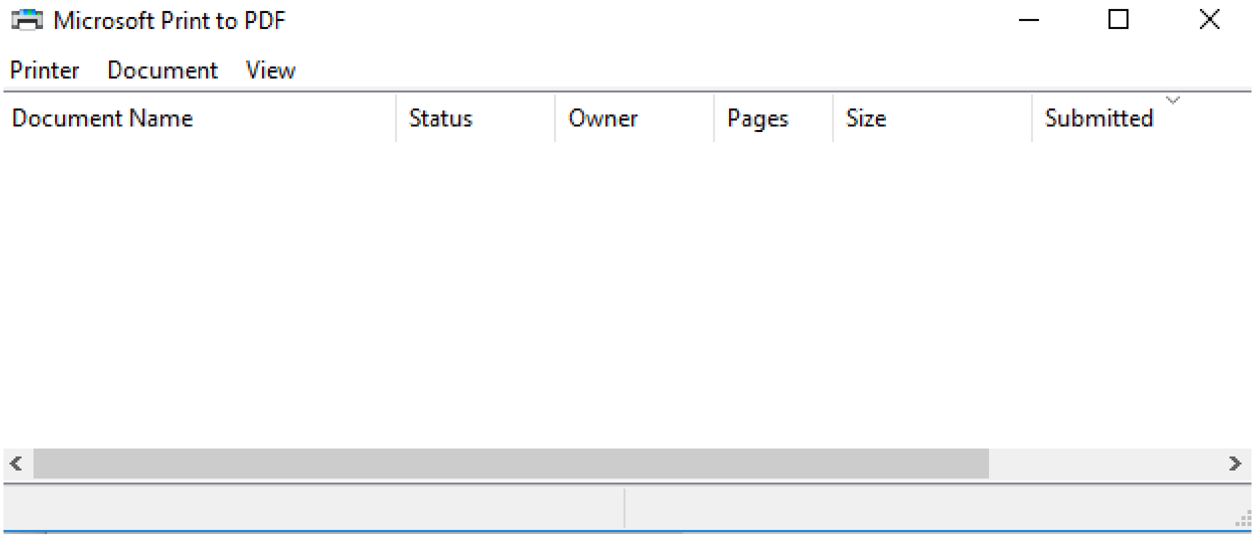
○ Domain:

● Workgroup: WORKGROUP

Control Panel – Devices and Printers

Shows a list of installed printers and scanners

- Name of device
- Status of printer (Online, Offline, Disconnected)
- Can Open Print Queue (shows documents that the printer will print, and their status)



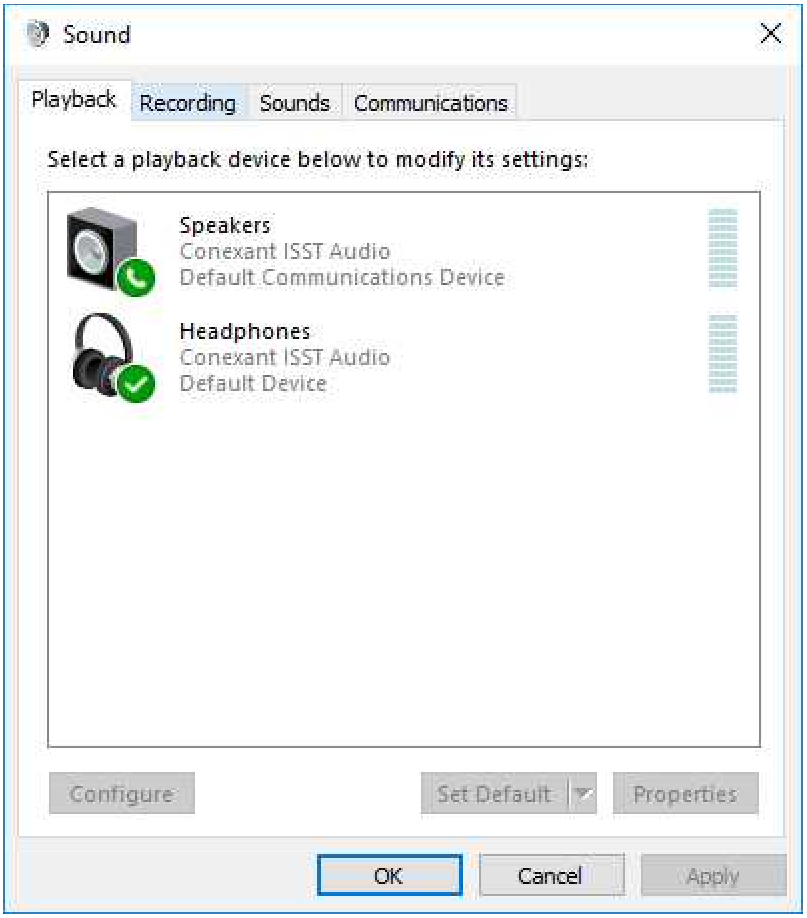
- Can choose to Manage printer (edit printer settings)
- Can choose to Remove printer

Can add a printer using a wizard (see previous section on printers)

Control Panel – Sound

Playback Tab

- Shows a list of playback devices (speakers and headphones)
- Can choose to set one device as default



Sound

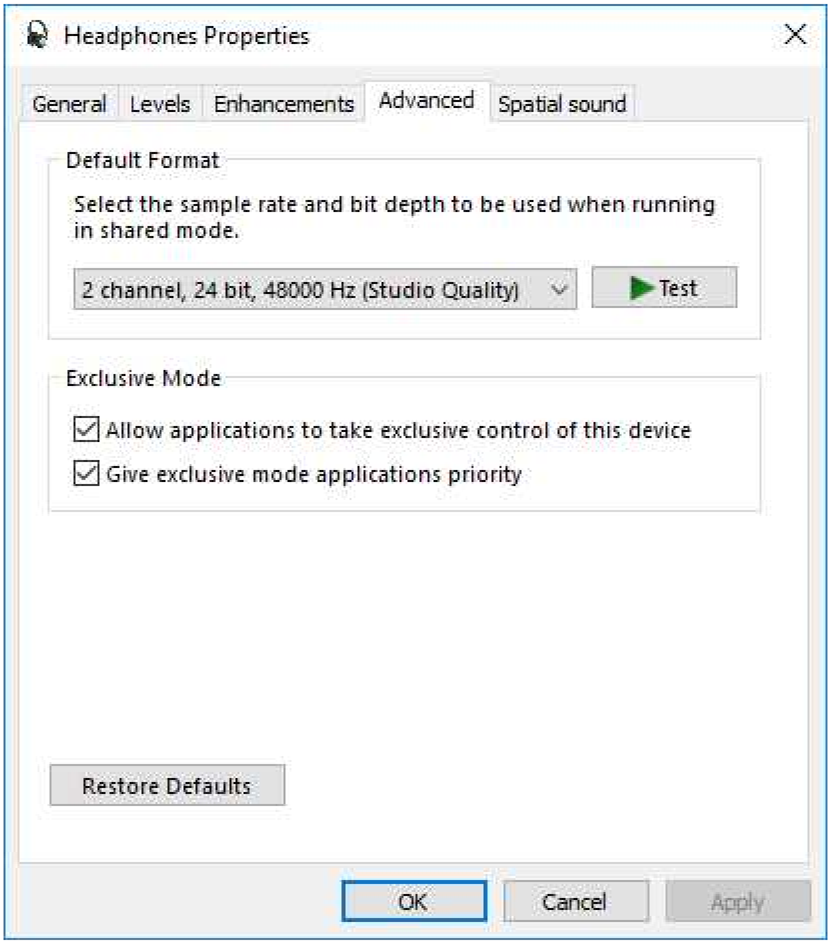
Playback | Recording | Sounds | Communications

Select a playback device below to modify its settings:

Speakers
Conexant ISST Audio
Default Communications Device

Headphones
Conexant ISST Audio
Default Device

- Can double-click on a device to show its properties
    - Enable/disable device
    - Edit name
    - Edit volume
    - Edit audio quality
- Different types of devices have different properties


Headphones Properties

Default Format

Select the sample rate and bit depth to be used when running in shared mode.

2 channel, 24 bit, 48000 Hz (Studio Quality)

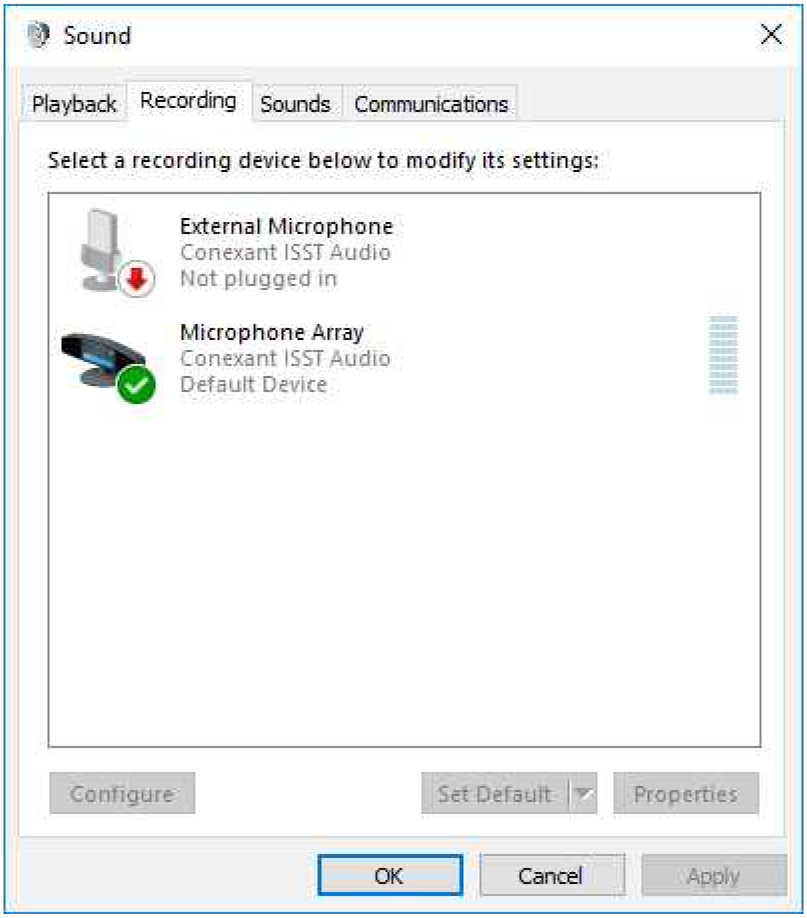
Exclusive Mode

☑ Allow applications to take exclusive control of this device

☑ Give exclusive mode applications priority

Recording Tab

- Shows a list of recording devices (microphones)
- Can double-click on a device to show its properties
  - Enable/disable device
  - Edit name
  - Edit volume
  - Edit audio quality
- Different types of devices have different properties



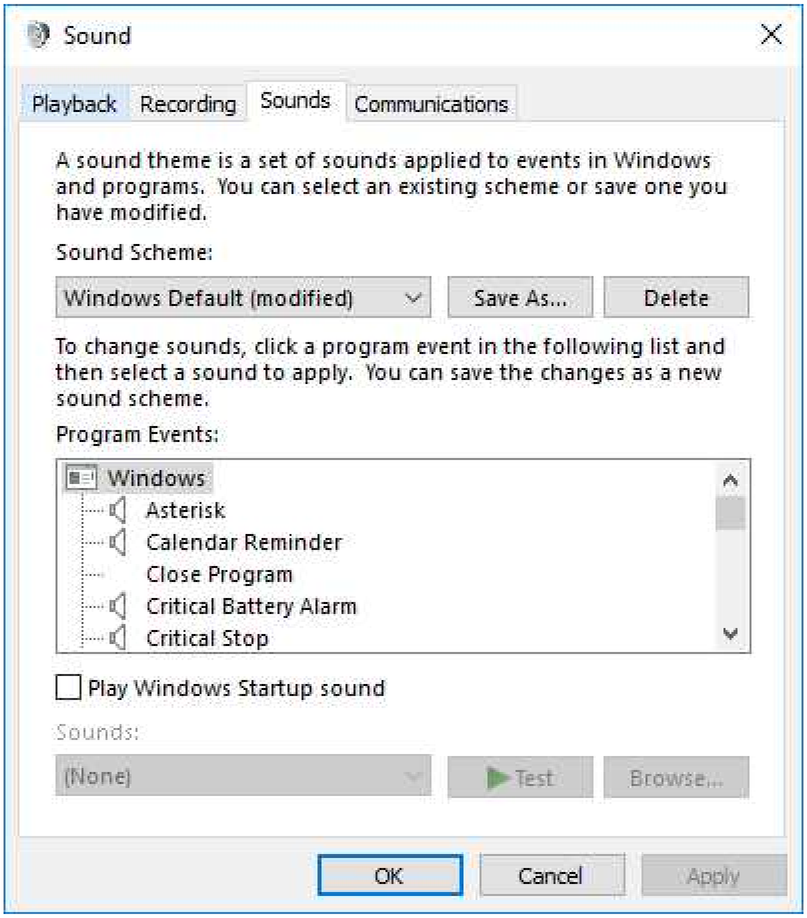
Select a recording device below to modify its settings:

External Microphone
Conexant ISST Audio
Not plugged in

Microphone Array
Conexant ISST Audio
Default Device

Sounds Tab

- Allows you to modify the default Windows sounds for events (Critical Alert, Windows Login, etc.)
- Can choose a sound from a Windows library or record your own sound



A sound theme is a set of sounds applied to events in Windows and programs. You can select an existing scheme or save one you have modified.

Sound Scheme: Windows Default (modified)

To change sounds, click a program event in the following list and then select a sound to apply. You can save the changes as a new sound scheme.

Program Events:

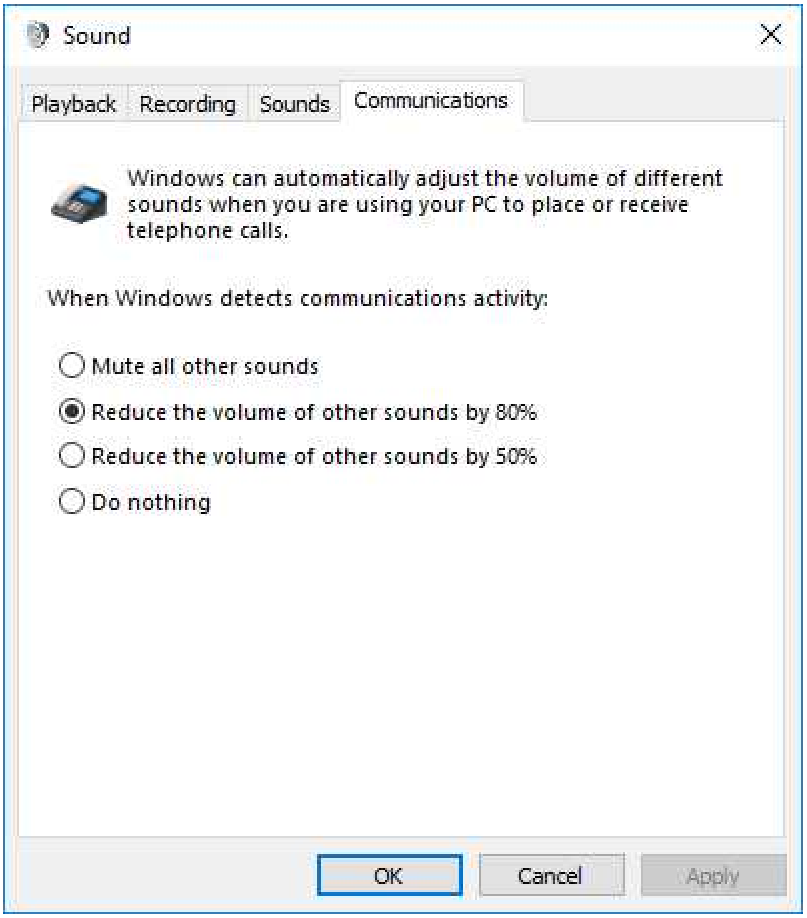
- Windows
  - Asterisk
  - Calendar Reminder
  - Close Program
  - Critical Battery Alarm
  - Critical Stop

□ Play Windows Startup sound

Sounds: (None)

Communications Tab

- Allows Windows to reduce the volume of other sounds when it detects you making/receiving a phone call (for example, on Skype)
- Options are
  - Mute sounds
  - Reduce volume by 80%
  - Reduce volume by 50%
  - Do nothing



Windows can automatically adjust the volume of different sounds when you are using your PC to place or receive telephone calls.

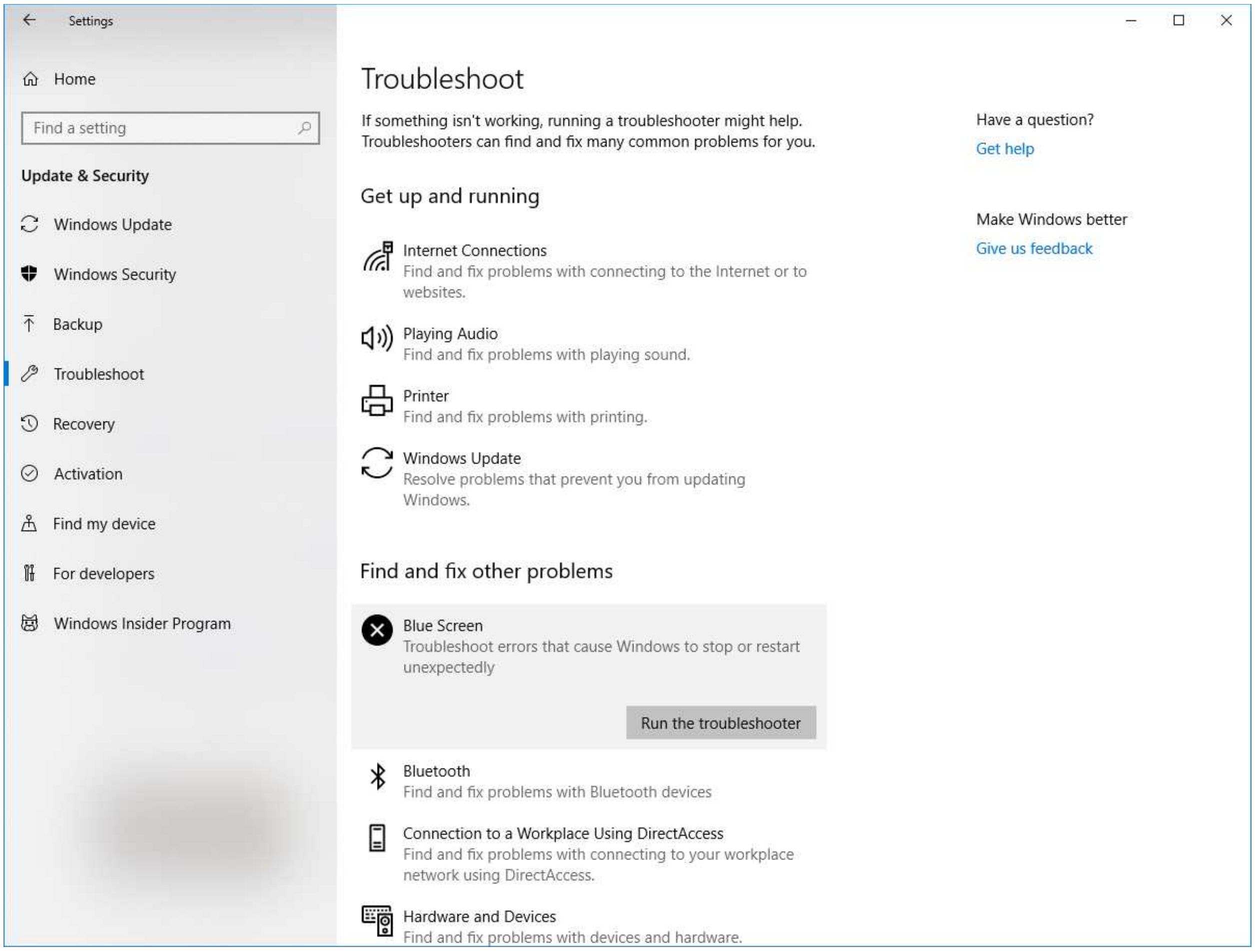
When Windows detects communications activity:

○ Mute all other sounds
● Reduce the volume of other sounds by 80%
○ Reduce the volume of other sounds by 50%
○ Do nothing

Control Panel – Troubleshooting

Windows includes a set of trouble-shooters for different scenarios

- Internet
- Audio
- Printer
- Windows Update
- Hardware
- Speech
- Program Compatibility
- Power



Troubleshoot

If something isn't working, running a troubleshooter might help. Troubleshooters can find and fix many common problems for you.

Get up and running

Internet Connections
Find and fix problems with connecting to the Internet or to websites.

Playing Audio
Find and fix problems with playing sound.

Printer
Find and fix problems with printing.

Windows Update
Resolve problems that prevent you from updating Windows.

Find and fix other problems

Blue Screen
Troubleshoot errors that cause Windows to stop or restart unexpectedly

Bluetooth
Find and fix problems with Bluetooth devices

Connection to a Workplace Using DirectAccess
Find and fix problems with connecting to your workplace network using DirectAccess.

Hardware and Devices
Find and fix problems with devices and hardware.

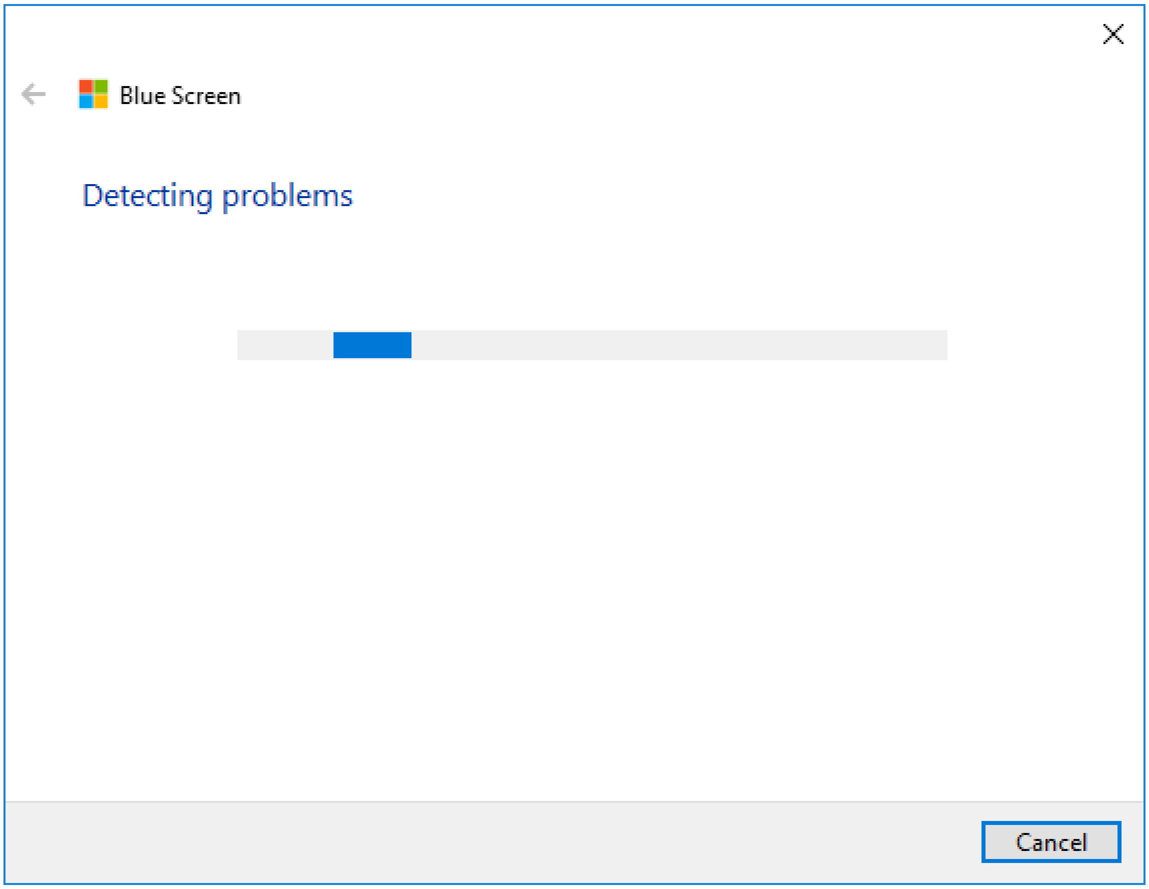
Have a question?

Make Windows better

How to use the trouble-shooter

- Select the type of trouble-shooter that most closely matches your issue

- The wizard will ask you a series of questions
- The wizard will detect problems
- It will offer you a set of solutions
  - It will show you the most likely solution first (and ask if you want to apply it)
  - You can use the trouble-shooter to apply the solution
  - After applying the solution, the trouble-shooter will ask you if the issue was resolved
  - If it wasn't resolved, the trouble-shooter will offer another solution
  - This will continue until the issue is resolved or the trouble-shooter has run out of solutions
- The trouble-shooter is only good for basic issues
- For example, if you're having trouble connecting to the internet, and it's because your Network Interface is disabled, the trouble-shooter will suggest that you enable your Network Interface. It won't be able to detect more complicated routing or internet traffic issues.



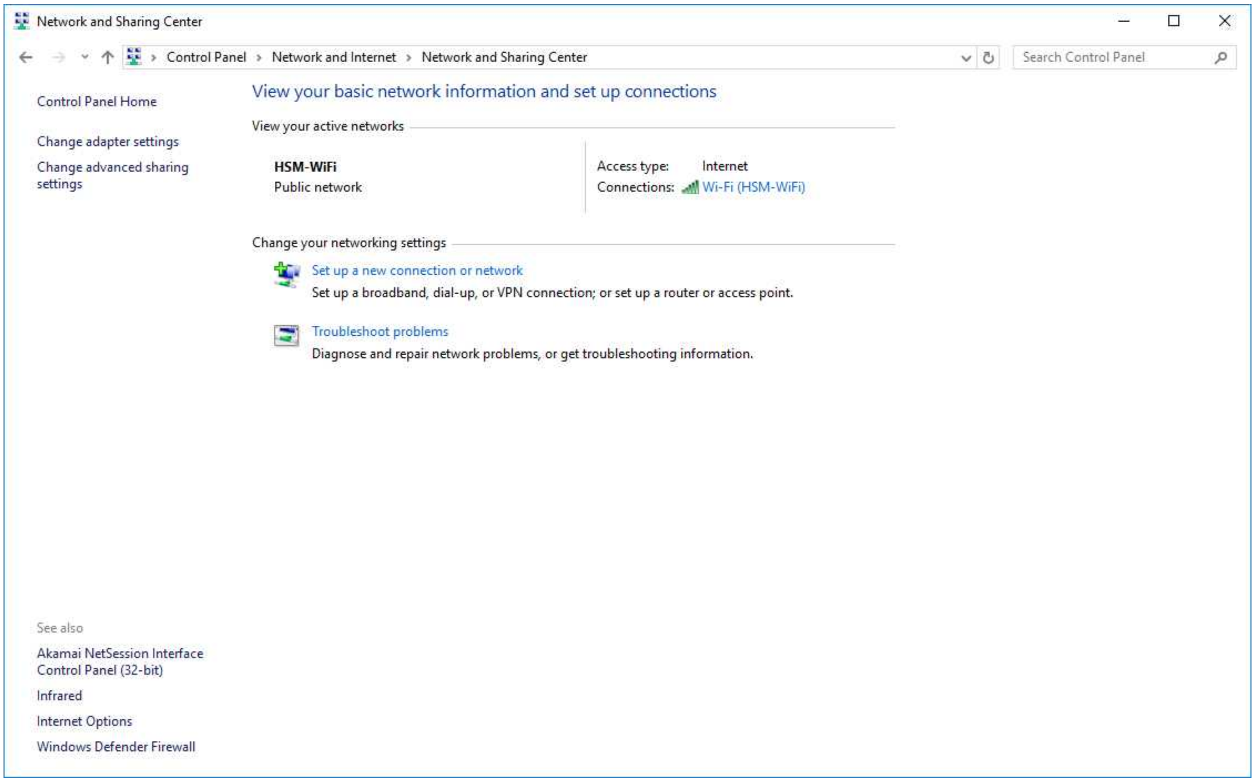
Blue Screen

Detecting problems

Control Panel – Network and Sharing Center

Shows the network or networks that the computer is currently connected to

- Can set up a new network (such as a VPN or PPPoE connection)
- Can access the internet properties of the network adapter
- Can access the Sharing Settings


Network and Sharing Center
Control Panel > Network and Internet > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Akamai NetSession Interface Control Panel (32-bit)
Infrared
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

HSM-WiFi
Public network

Access type: Internet
Connections: Wi-Fi (HSM-WiFi)

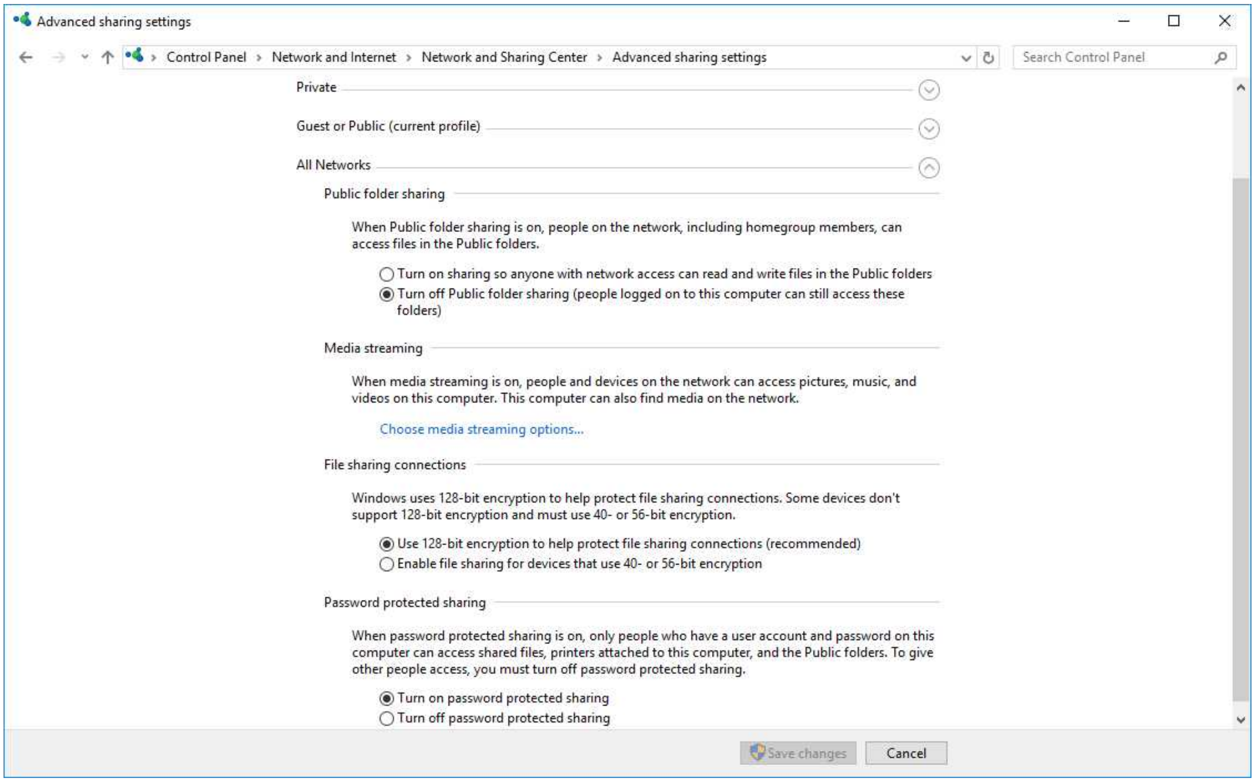
Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Sharing Settings

- Different sharing settings can be set for Private, Guest (Public) or All Networks
- Public Folder Sharing: allows the computer to share folders with others on the network (others can only access folders that are set to public)
- File Sharing Connections: choose whether to require 128-bit encryption in file sharing (more secure), or whether to allow 40 or 56-bit encryption (less secure, but allows access to more devices)
- Password Protected Sharing: choose whether to require others to use a username/password to access shared files. Note that the username/password must be set on the computer providing the shared files.



Advanced sharing settings

Control Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings
Search Control Panel

Private

Guest or Public (current profile)

All Networks

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

○ Turn on sharing so anyone with network access can read and write files in the Public folders

● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Choose media streaming options...

File sharing connections

Windows uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.

● Use 128-bit encryption to help protect file sharing connections (recommended)

○ Enable file sharing for devices that use 40- or 56-bit encryption

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

● Turn on password protected sharing

○ Turn off password protected sharing

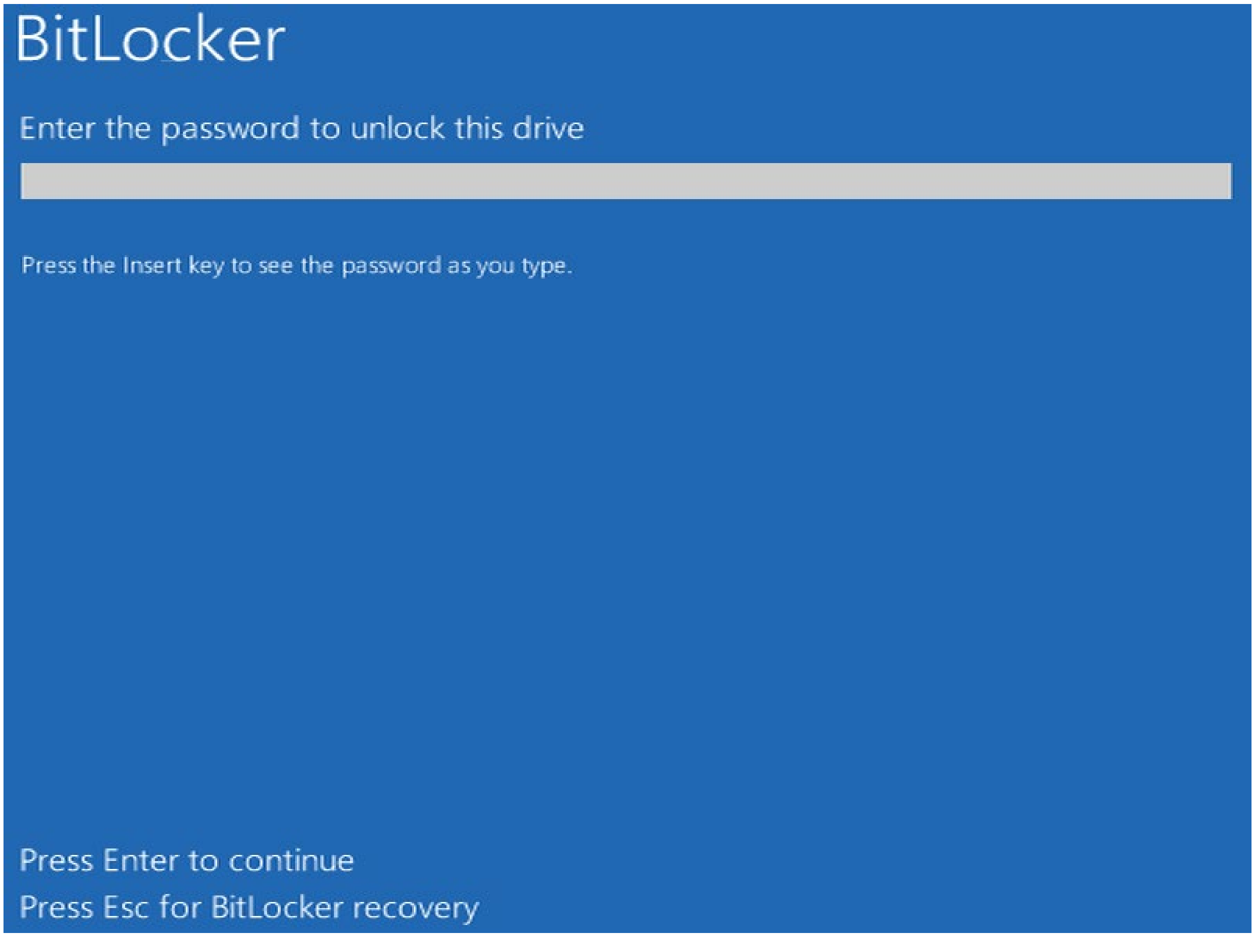
Control Panel – Device Manager

See previous section on Device Manager

Control Panel – BitLocker

How BitLocker works

- Encrypts the entire hard disk drive volume with an encryption key (a very long password)
    - The key is stored to the hard disk drive and encrypted with your login password
- When you first activate BitLocker, the key is randomly generated
    - You have the option to print the key, save it to OneDrive, or save it to USB
    - If you forget your password, you must use the key to unlock your drive
- There are two modes
    - User Authentication Mode
        - The key is encrypted with your password and stored on the hard drive
        - When you first activate BitLocker, the key is randomly generated
        - To unlock the computer, you must enter your password
        - BitLocker uses your password to decrypt the key
        - BitLocker uses the key to decrypt files on the drive
        - If you forget your password, you will be prompted to enter the key



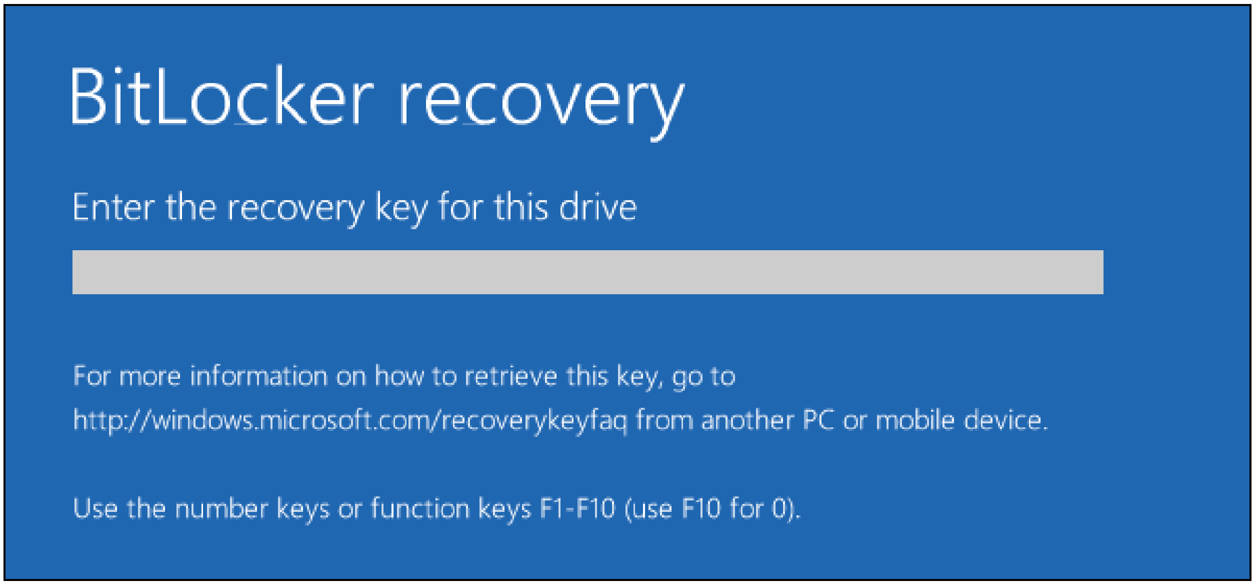
BitLocker

Enter the password to unlock this drive

Press the Insert key to see the password as you type.

Press Enter to continue

Press Esc for BitLocker recovery



BitLocker recovery

Enter the recovery key for this drive

For more information on how to retrieve this key, go to http://windows.microsoft.com/recoverykeyfaq from another PC or mobile device.

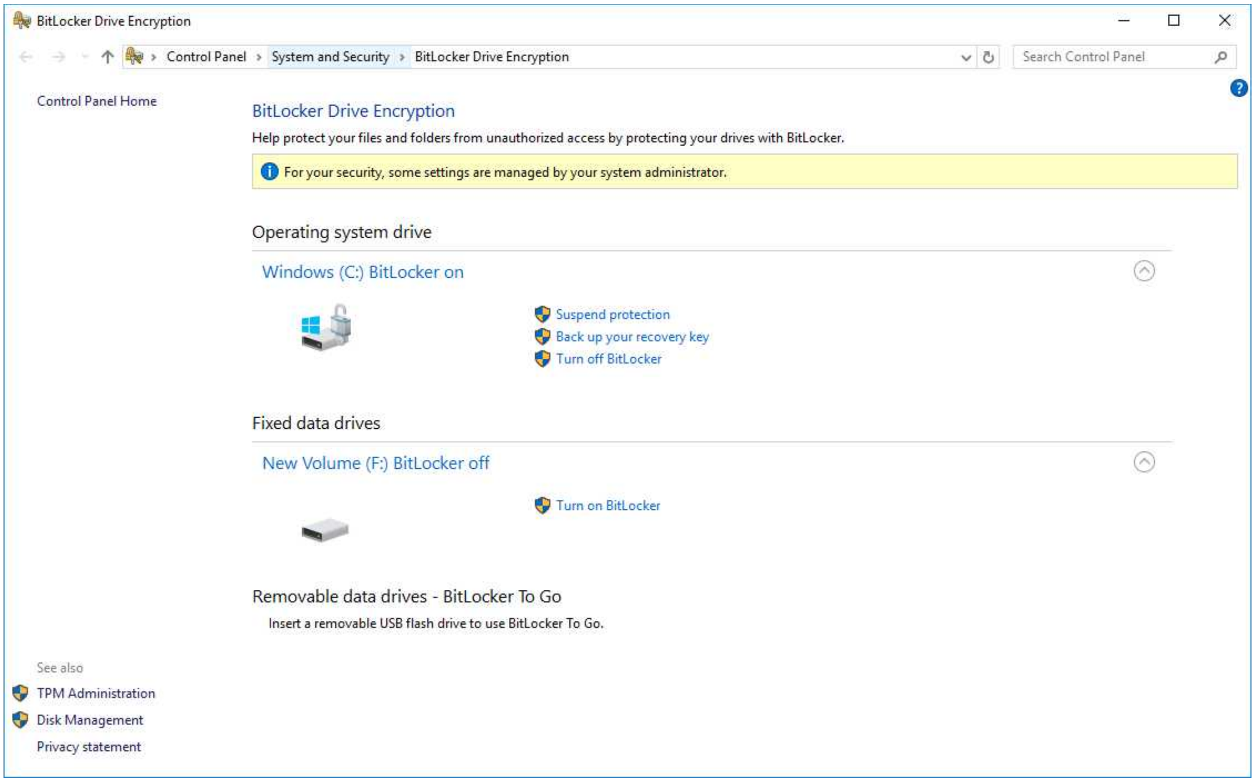
Use the number keys or function keys F1-F10 (use F10 for 0).

- Transparent Mode
  - The key is stored in the Trusted Platform Module (TPM)

        - May also be stored in Active Directory (for Windows Domain users)
    - You are not prompted for a key or a password when the computer boots
    - The most basic parts of Windows are not encrypted
    - When you boot your computer, Windows appears to load like normal (it loads the unencrypted files)
    - The TPM verifies that the Windows files have not been modified, and knows that it can trust the Windows files
    - You log in with your Windows password
    - Windows authorizes the TPM to release the key, and decrypt the remaining files on the drive

From the BitLocker menu

- You can see a list of available drives and whether BitLocker is enabled on each of them
- Turn BitLocker on or off
- Suspend BitLocker
- Back up the recovery key


BitLocker Drive Encryption
Control Panel > System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

Windows (C:) BitLocker on

Suspend protection
Back up your recovery key
Turn off BitLocker

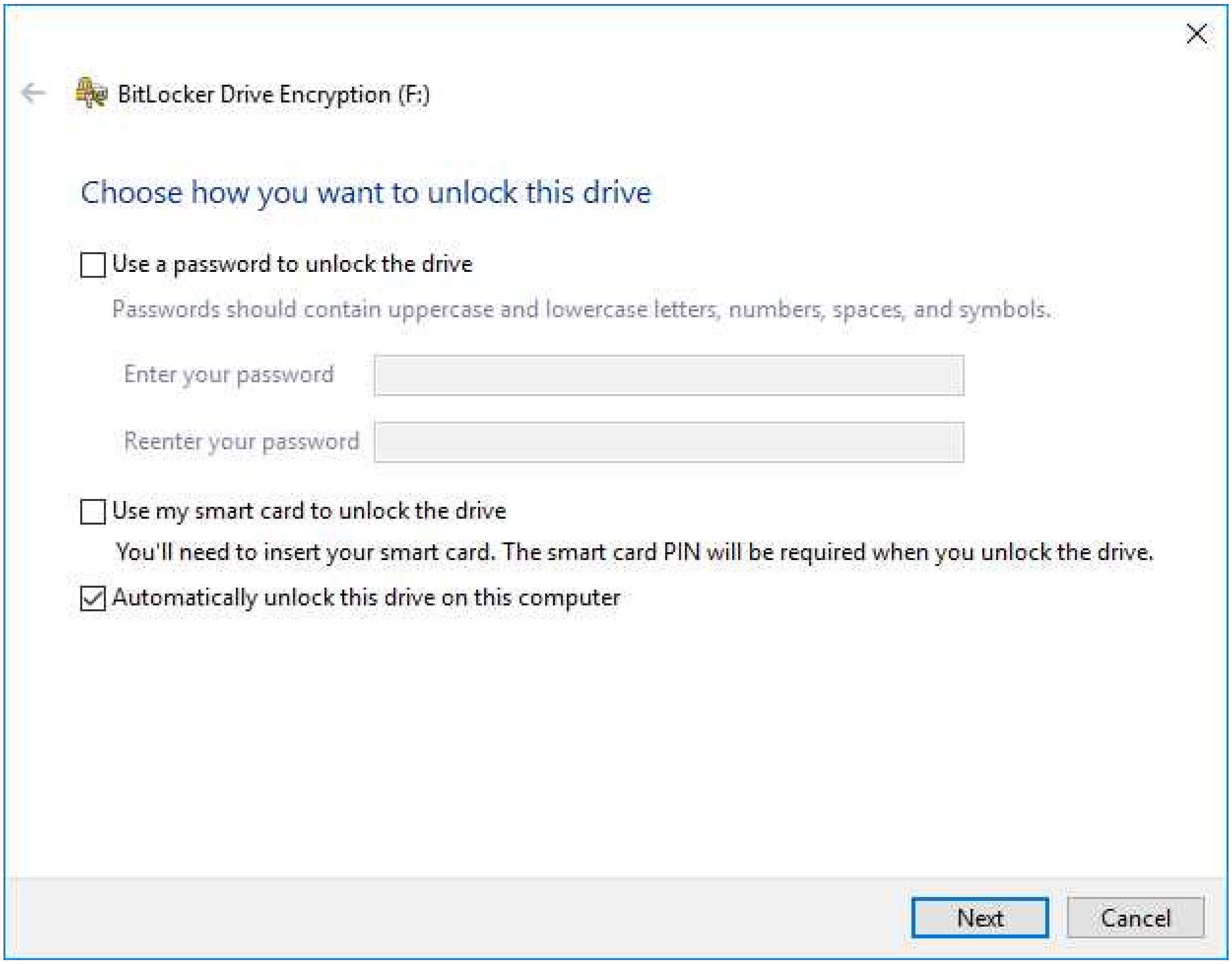
Fixed data drives

New Volume (F:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

- You can choose to allow Windows to automatically unlock the drive (through the TPM) or force it to require an additional password



BitLocker Drive Encryption (F:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

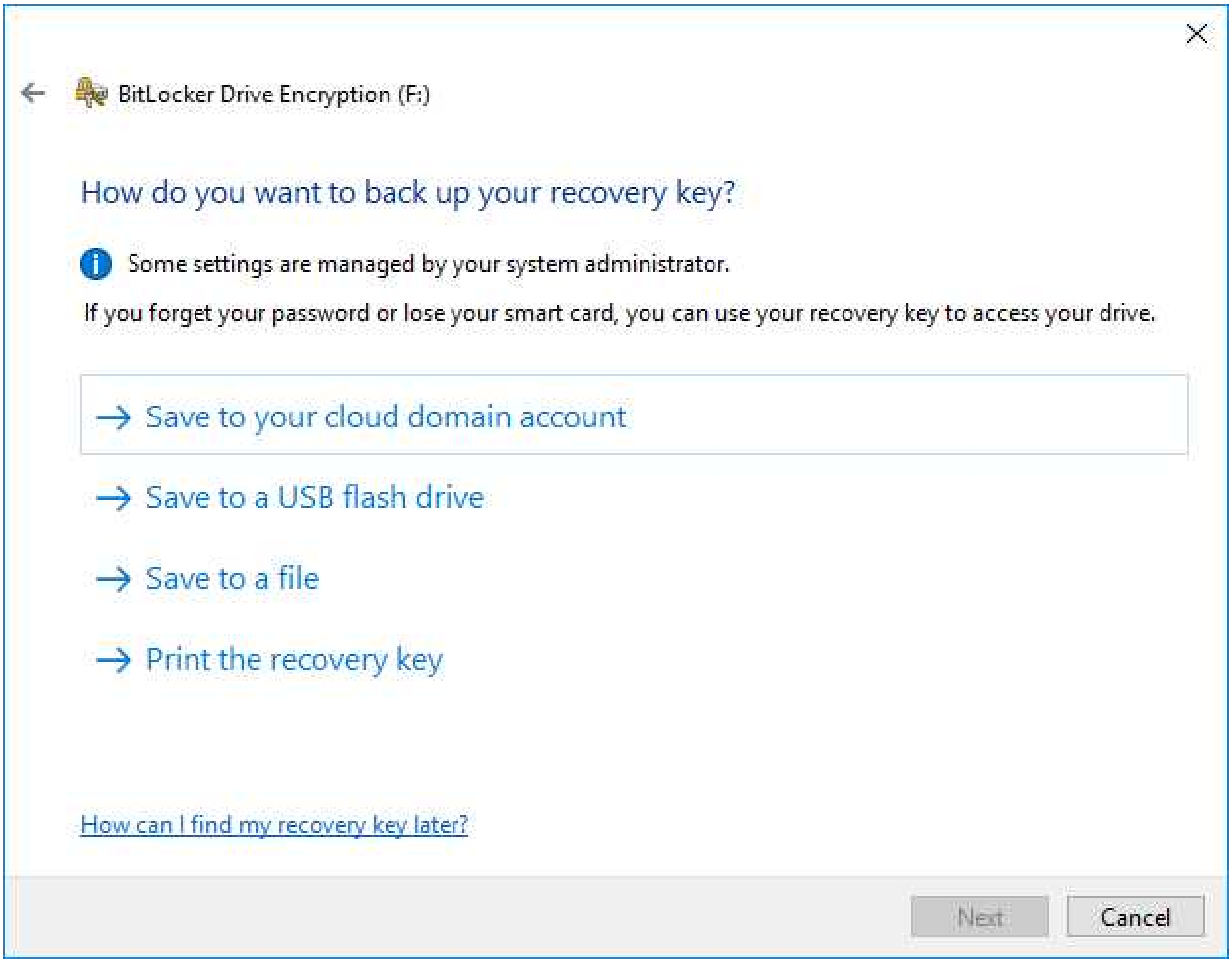
Reenter your password

□ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

☑ Automatically unlock this drive on this computer

- Choose where to save the recovery key
  - Cloud account
  - USB flash drive
  - Save to a file
  - Print the key



BitLocker Drive Encryption (F:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your cloud domain account

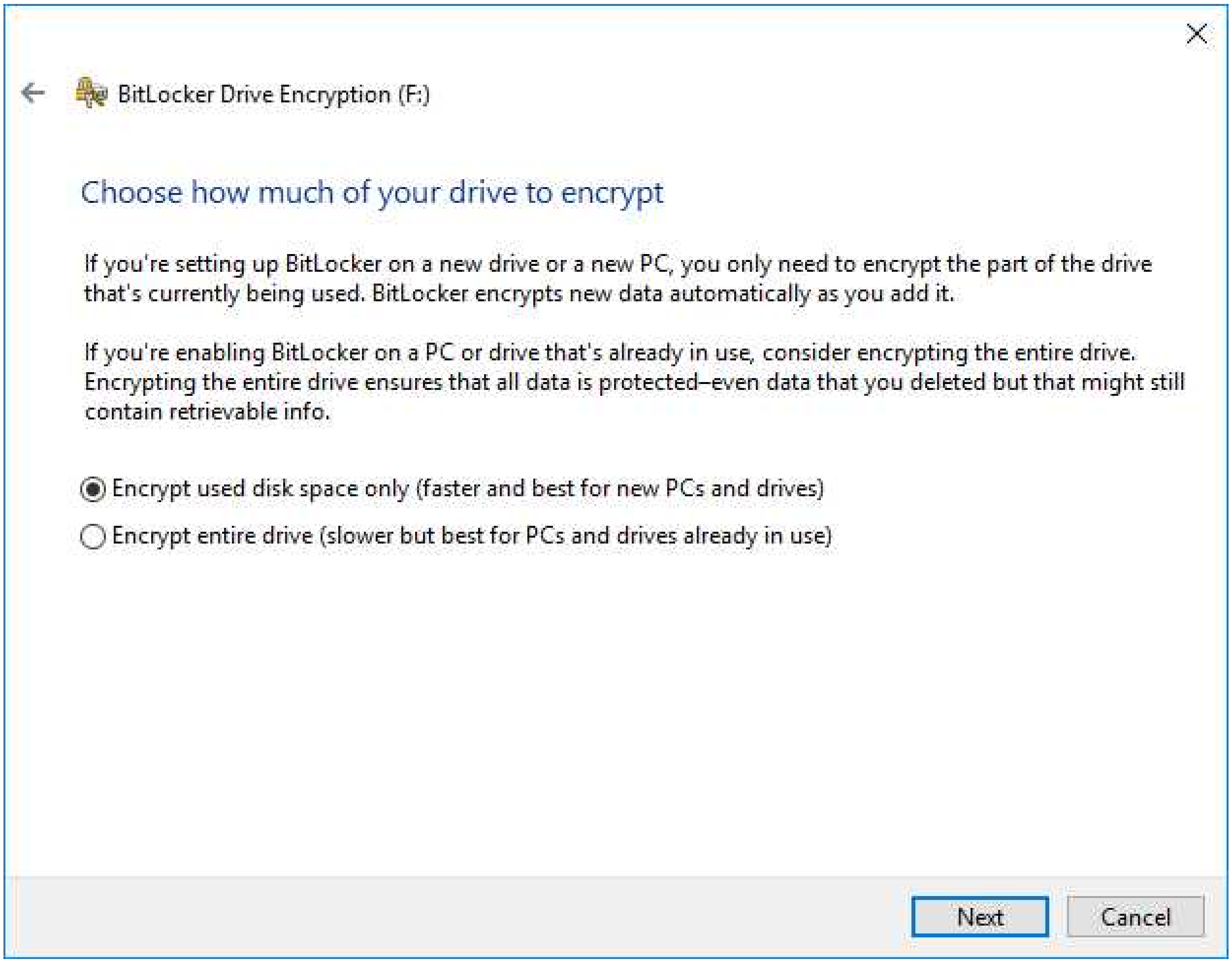
→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

How can I find my recovery key later?

- Can choose to encrypt used disk space (faster) or all disk space (more secure because it encrypts deleted data)



BitLocker Drive Encryption (F:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

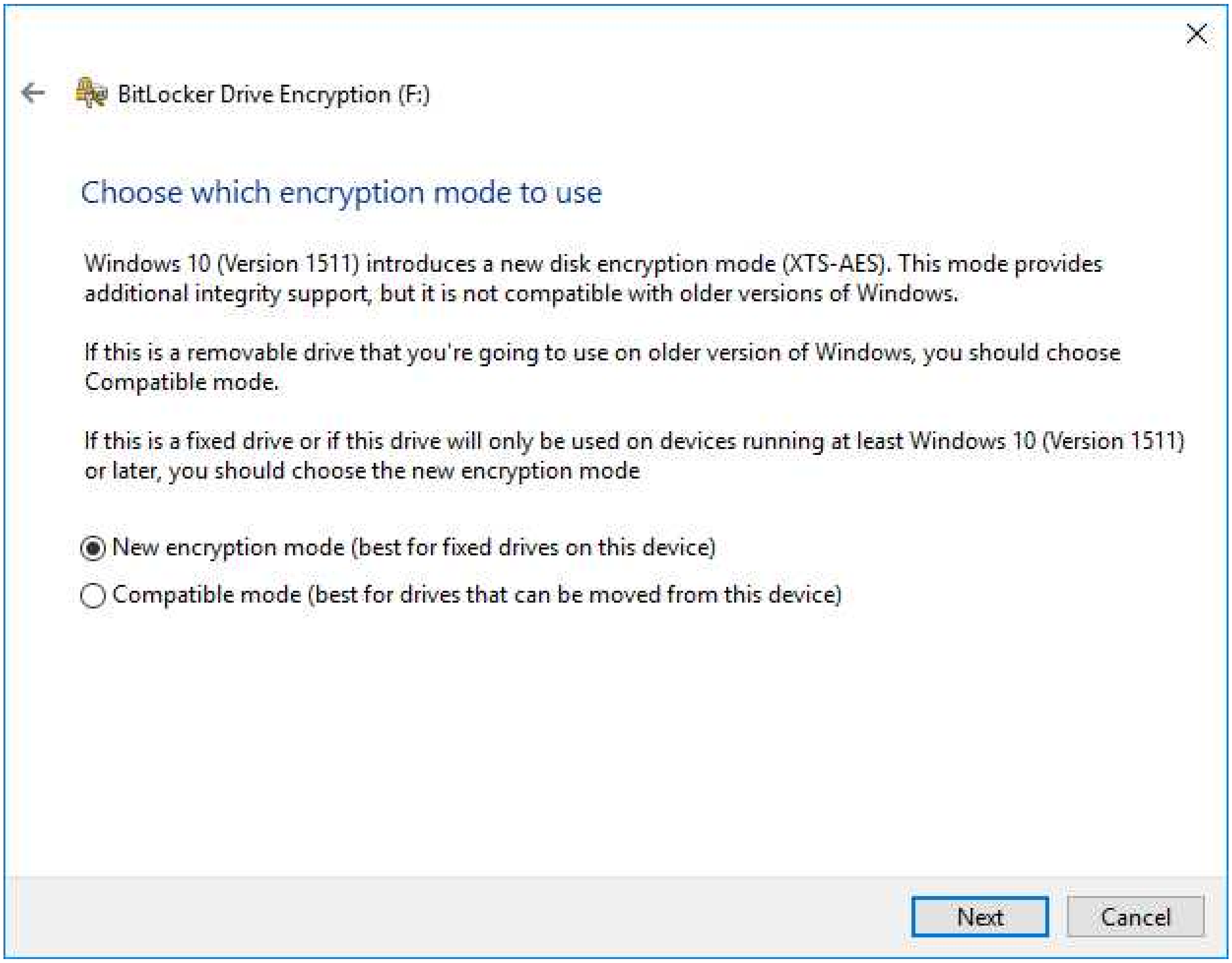
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

● Encrypt used disk space only (faster and best for new PCs and drives)

○ Encrypt entire drive (slower but best for PCs and drives already in use)

Choose the type of encryption mode

- New encryption mode
  - More stable; reduces the risk of losing your data
  - Only compatible with Windows 10; if you're encrypting a USB drive, don't choose this option because previous versions of Windows won't be able to decrypt it
- Compatible mode
  - Less stable
  - Compatible with older versions of Windows



BitLocker Drive Encryption (F:)

Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

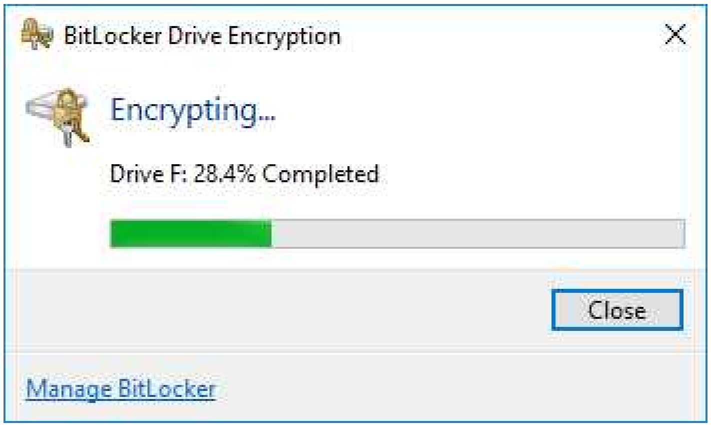
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

● New encryption mode (best for fixed drives on this device)

○ Compatible mode (best for drives that can be moved from this device)

- Windows will encrypt the drive



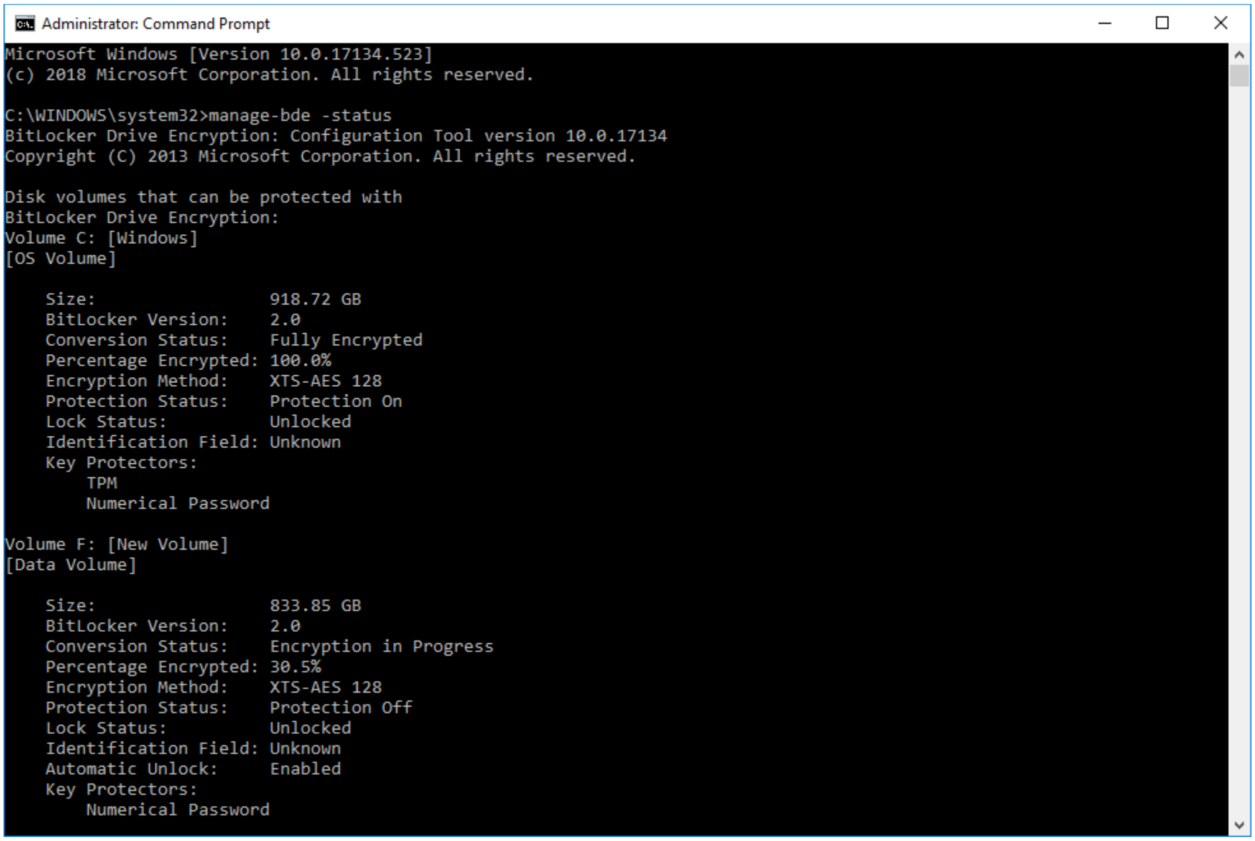
BitLocker Drive Encryption

Encrypting...

Drive F: 28.4% Completed

You can also access the BitLocker status from the command prompt

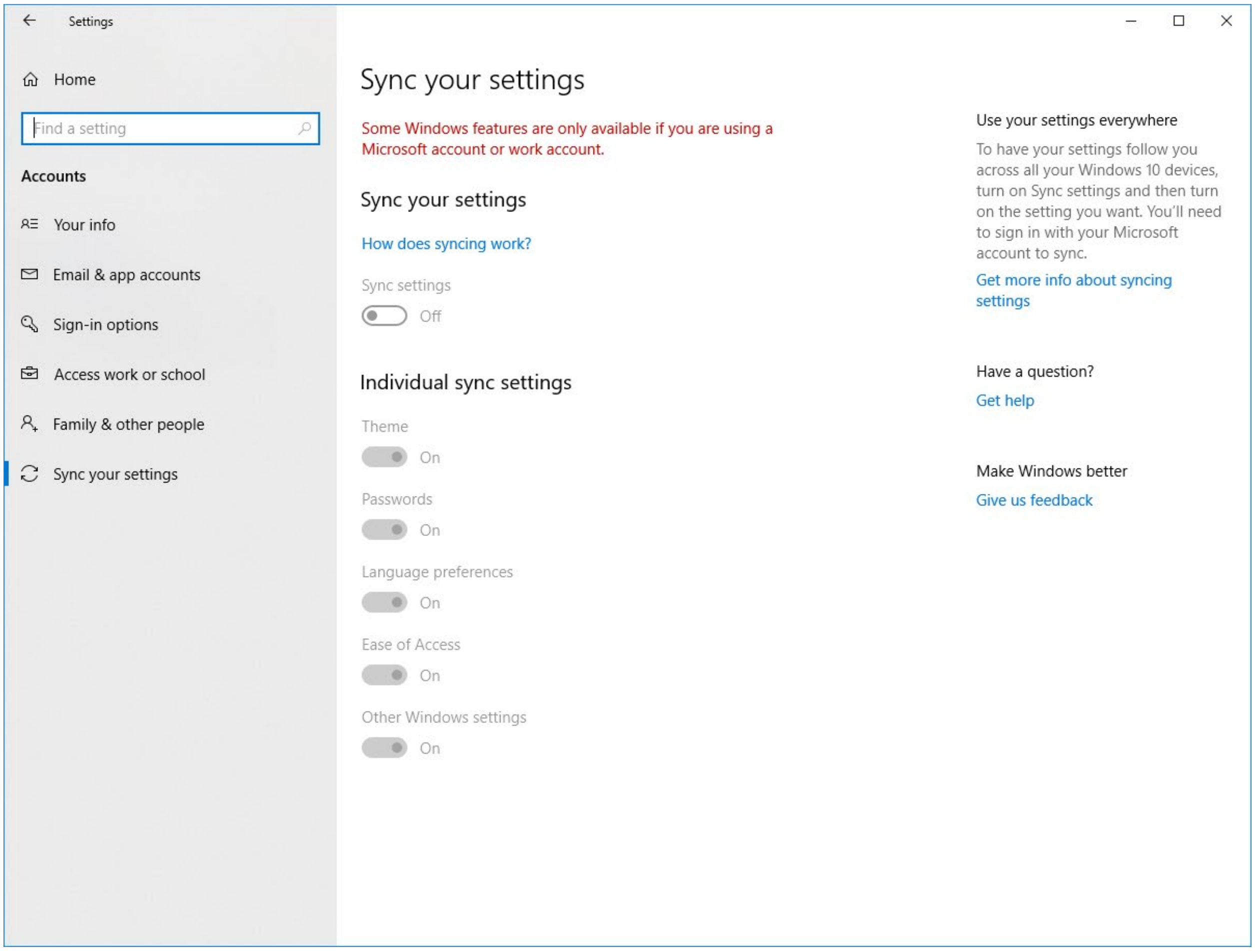
- Type *manage-bde status*



```
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.17134
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [Windows]
[OS Volume]

    Size:                 918.72 GB
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        TPM
        Numerical Password

Volume F: [New Volume]
[Data Volume]

    Size:                 833.85 GB
    BitLocker Version:    2.0
    Conversion Status:    Encryption in Progress
    Percentage Encrypted: 30.5%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: Unknown
    Automatic Unlock:     Enabled
    Key Protectors:
        Numerical Password
```

Control Panel – Sync Center

- Allows you to sync your Windows settings across multiple devices
- You must be logged in to each device with the same Microsoft account (or Active Directory account)



Sync your settings

Some Windows features are only available if you are using a Microsoft account or work account.

Sync your settings

How does syncing work?

Sync settings: Off

Individual sync settings

Theme: On

Passwords: On

Language preferences: On

Ease of Access: On

Other Windows settings: On

Use your settings everywhere

To have your settings follow you across all your Windows 10 devices, turn on Sync settings and then turn on the setting you want. You'll need to sign in with your Microsoft account to sync.

Get more info about syncing settings

Have a question?

Get help

Make Windows better

Give us feedback

1.7 Summarize application installation and configuration concepts.

- *System requirements*
    - *Drive space*
    - *RAM*
- *OS requirements*
    - *Compatibility*
- *Methods of installation and deployment*
    - *Local (CD/USB)*
    - *Network-based*
- *Local user permissions*
    - *Folder/file access for installation*
- *Security considerations*
    - *Impact to device*
    - *Impact to network*

Installation Consideration

- Ensure that your computer has adequate hardware
    - Drive space to install the program
    - RAM
    - Processor speed
    - Other necessary hardware (graphics card, etc.)
- Ensure that you have the correct OS Requirements
    - Correct operating system (Windows, macOS, Linux, etc.)
    - Correct operating system version (Windows 7, Windows 10, etc.)
    - Correct operating system type (32-bit, 64-bit)
- Installation methods
    - Most common method was CD/DVD
        - Insert the CD/DVD and run the setup file
    - Other method is through USB
    - Most programs are available for download from the internet
        - Download the program and install it
    - Install the program over the network
        - Common in enterprise environments
        - Program is "pushed" to the user's computer from a software server and installs in the background
- Local User Permissions
    - You must have permission to install the program (admin permissions)
    - You must also have permission to write to the folders that the program files will be copied to
- Security Considerations
    - Consider if the program is digitally signed and from a reputed publisher
    - A program can have access to sensitive data on the computer, especially if it runs with admin privileges
        - Unlike Android and iOS apps, Windows apps don't run in a sandbox (they have access to everything)
    - A program can send data over the network or leak data

- Consider installing a Data Leak Prevention device

1.8 Given a scenario, configure Microsoft Windows networking on a client/desktop.

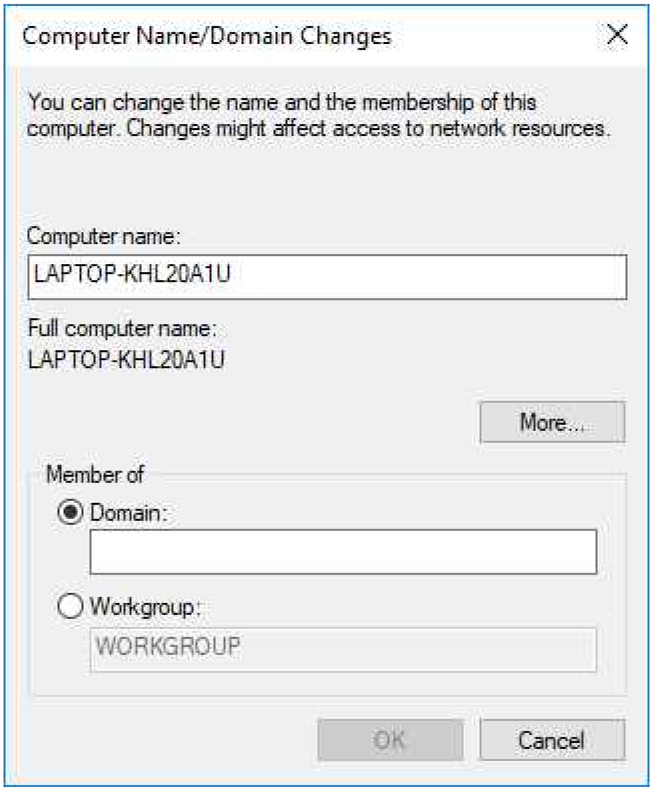
- *HomeGroup vs. Workgroup*
- *Domain setup*
- *Network shares/administrative shares/mapping drives*
- *Printer sharing vs. network printer mapping*
- *Establish networking connections*
  - *VPN*
  - *Dial-ups*
  - *Wireless*
  - *Wired*
  - *WWAN (Cellular)*
- *Proxy settings*
- *Remote Desktop Connection*
- *Remote Assistance*
- *Home vs. Work vs. Public network settings*
- *Firewall settings*
  - *Exceptions*
  - *Configuration*
  - *Enabling/disabling Windows Firewall*
- *Configuring an alternative IP address in Windows*
  - *IP addressing*
  - *Subnet mask*
  - *DNS*
  - *Gateway*
- *Network card properties*
  - *Half duplex/full duplex/auto*
  - *Speed*
  - *Wake-on-LAN*
  - *QoS*
  - *BIOS (on-board NIC)*

HomeGroup vs WorkGroup

- A WorkGroup and a HomeGroup allow users to share files and printers over the network
- WorkGroup
  - WorkGroup is a hybrid of a Domain system
  - All computers must be on the same network to be part of the same WorkGroup
  - A WorkGroup is not protected by a password
    - To log on to a WorkGroup computer, a user must have an account on that computer
- HomeGroup
  - All computers must be on the same network to be part of the same HomeGroup
  - The HomeGroup is protected by a password, but a user only needs to enter the password once to access the HomeGroup

Domain Setup

- Make sure that you can reach the domain controller via the network
- Go to System Properties
- Enter the domain
- The computer will prompt you for a username/password that has permission to join the domain (typically an admin account)
- The computer will join the domain (a reboot is required for the change to take effect)


Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
LAPTOP-KHL20A1U

Full computer name:
LAPTOP-KHL20A1U

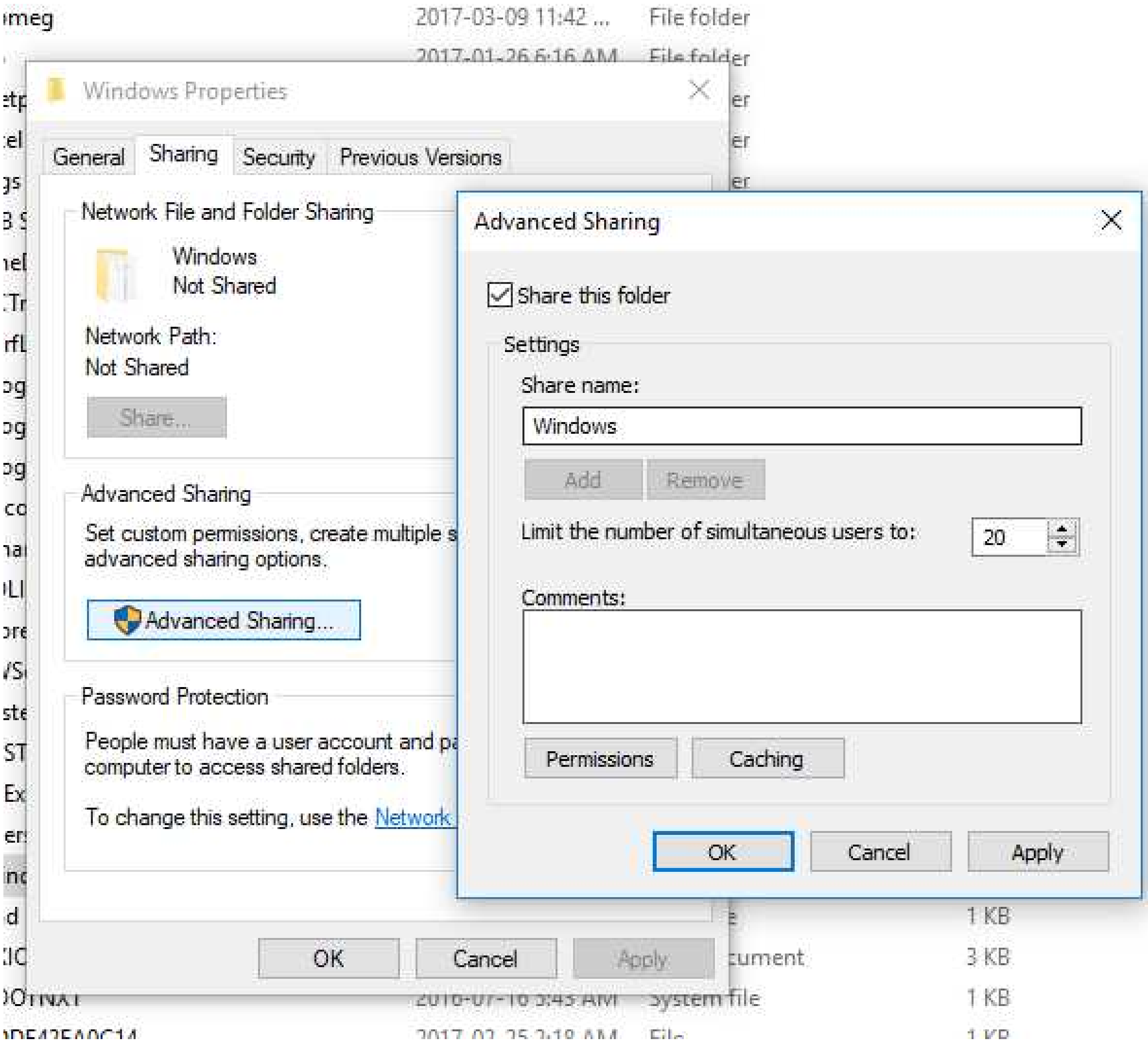
Member of

● Domain:

○ Workgroup:
WORKGROUP

Network shares/administrative shares/mapping drives

- Can share a folder with other users on the network
- Go to folder properties and choose Share
- Enter a Share name



Windows
Not Shared

Network Path:
Not Shared

Set custom permissions, create multiple s
advanced sharing options.

People must have a user account and pa
computer to access shared folders.

To change this setting, use the Network

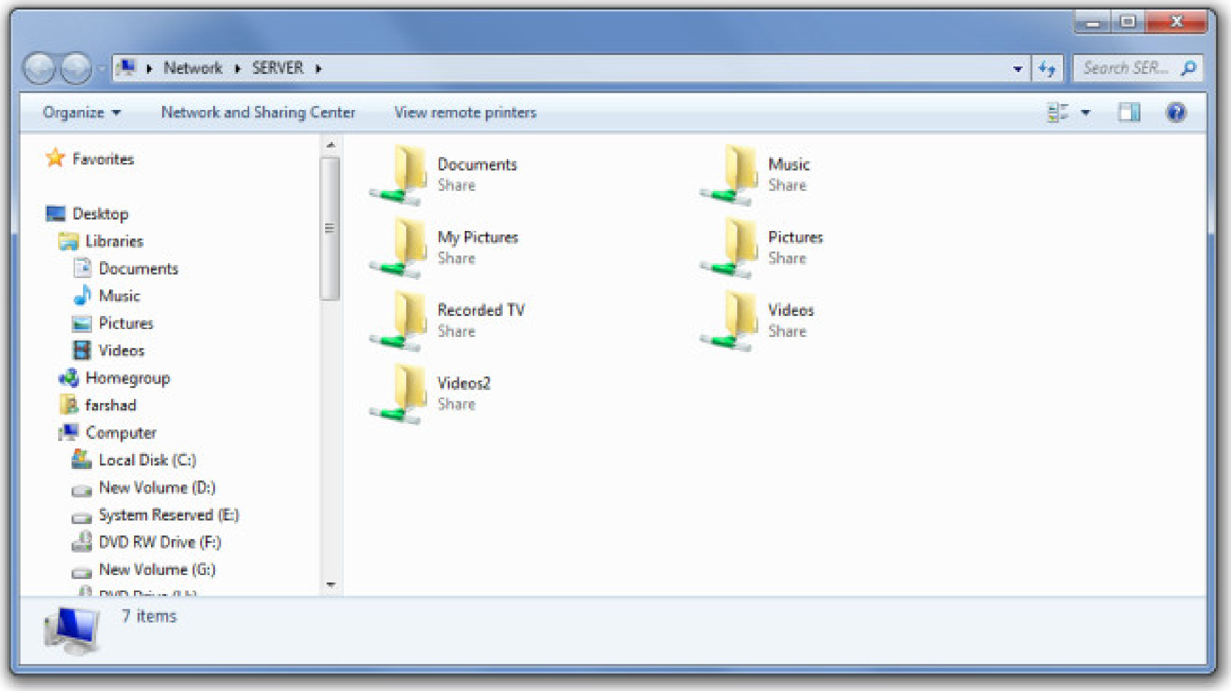
Advanced Sharing

☑ Share this folder

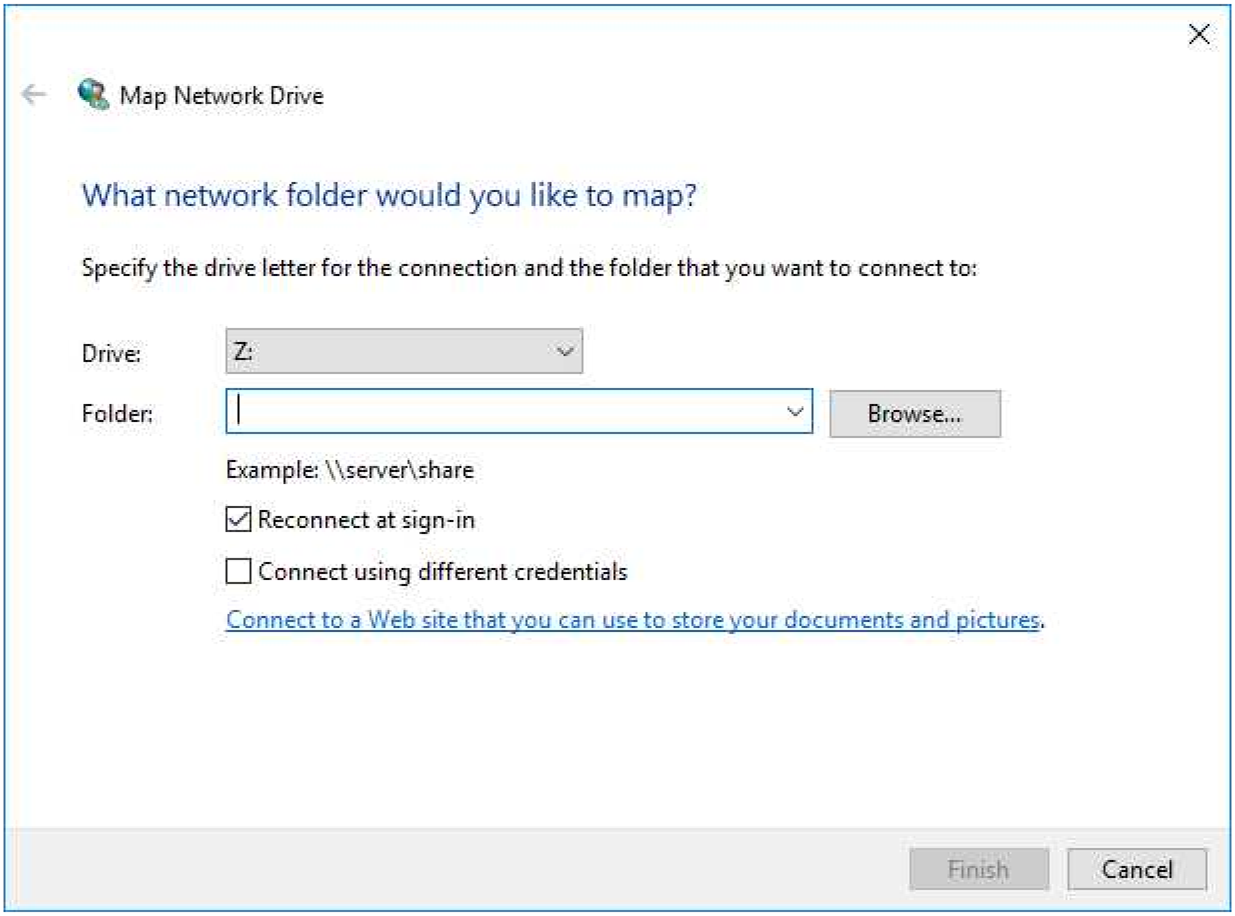
Share name: Windows

Limit the number of simultaneous users to: 20

- Other users can access the folder by navigating to Network, choosing the hostname of the computer that is sharing the folder, and then viewing the folder



- A network folder can be mapped as a drive
    - Choose Map Network Drive from This PC
    - Choose a drive letter
    - Enter the network location (hostname or IP address)
    - You may be required to enter a username or password



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

Folder:

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

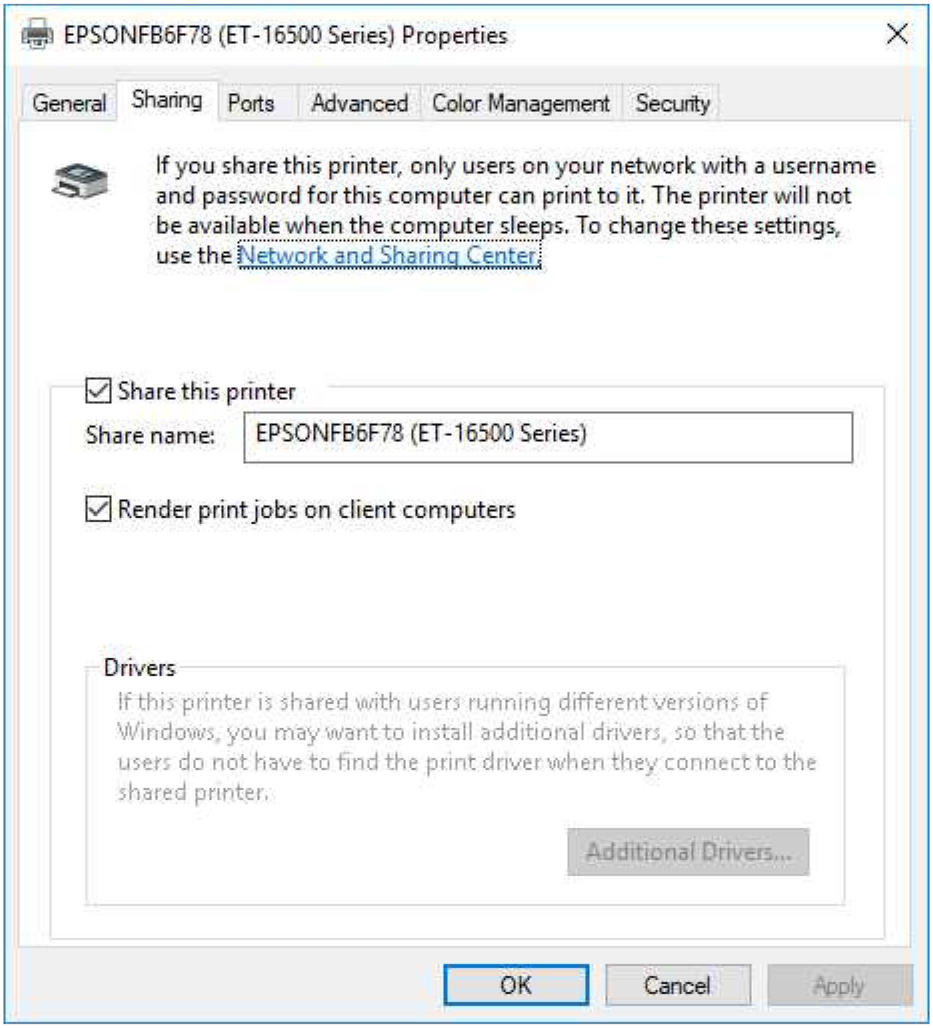
Printer sharing vs. network printer mapping

There are two ways to access a printer

- Printer Sharing: the printer is installed on one computer and other users connect to the printer through that computer
- Printer Mapping: the printer is set on the network. Each user connects to the printer directly.

You can share a printer the same way you can share a folder

- Go to Printer Properties
- Choose the Sharing tab
- Choose to share the printer and enter a name



If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

Share name: EPSONFB6F78 (ET-16500 Series)

☑ Render print jobs on client computers

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

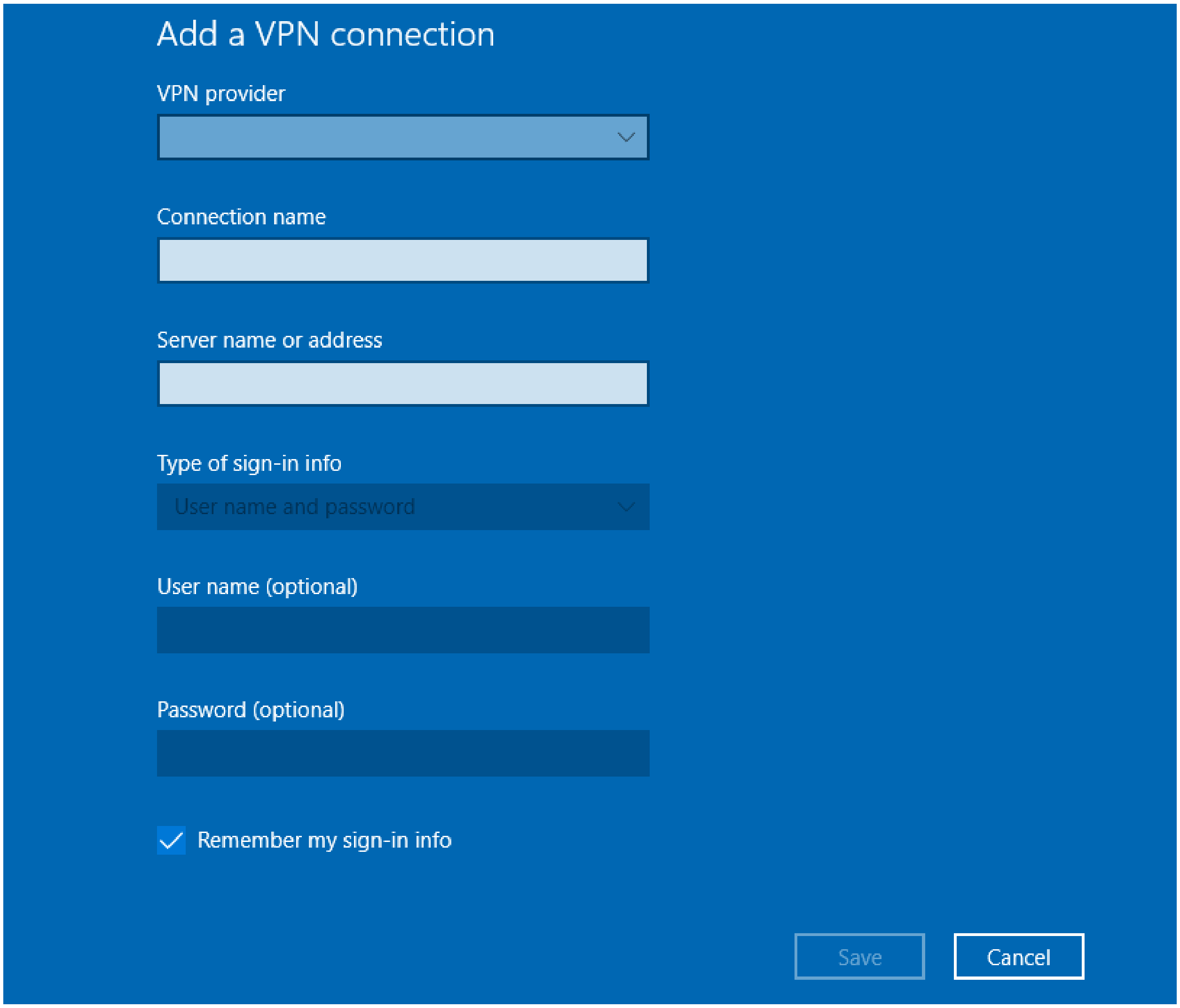
- Other users can access the printer by navigating to Network, choosing the hostname of the computer that is sharing the printer, and then viewing the printer
- Any document being printed passes through the computer that is sharing the printer

You can map a printer over the network

- This is detailed in a previous section

Establish networking connections (VPN, Dial-ups, Wireless, Wired, WWAN – Cellular)

- VPN
    - Can install a VPN client application (such as Cisco VPN) or set up the VPN manually
    - The VPN client application can configure advanced settings
    - Choose to add a VPN



Add a VPN connection

VPN provider

Connection name

Server name or address

Type of sign-in info

User name and password

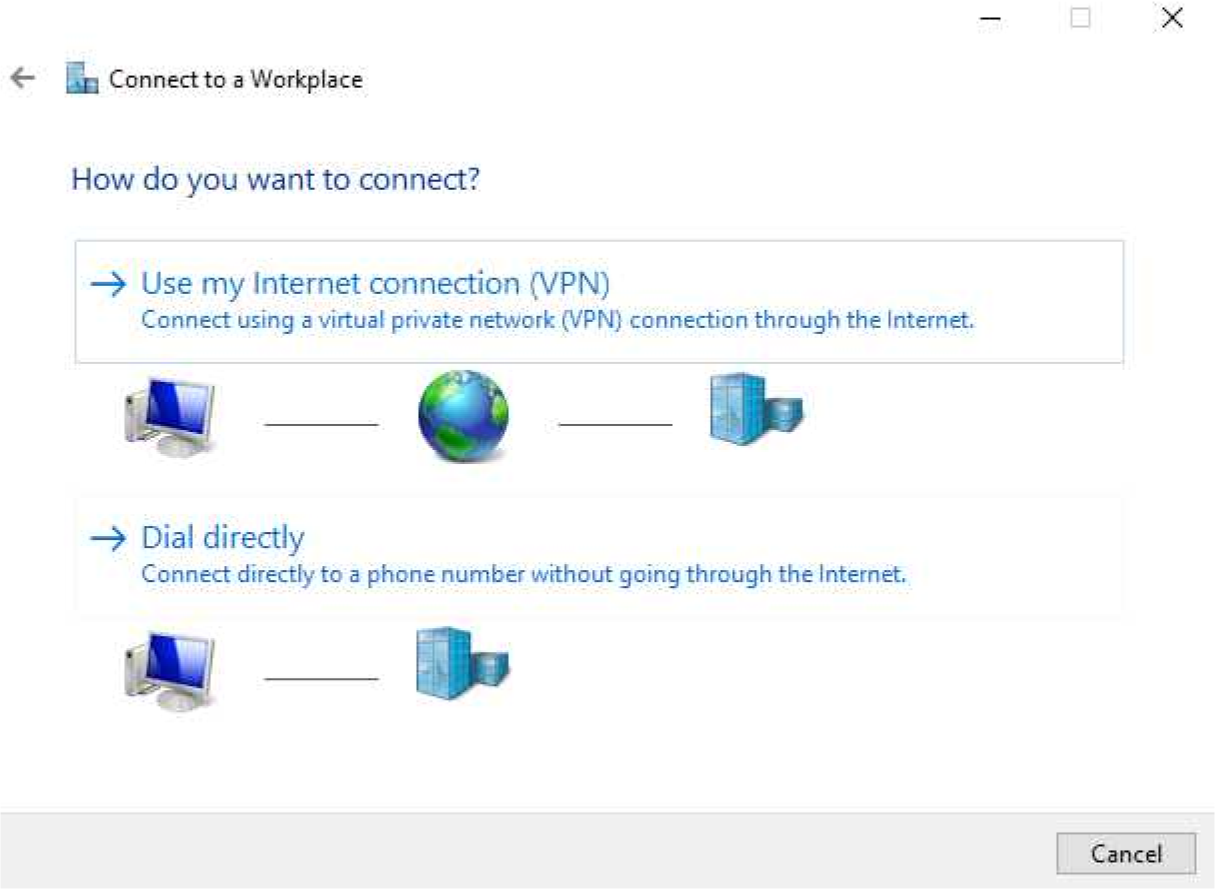
User name (optional)

Password (optional)

☑ Remember my sign-in info

-
    - Enter the information
        - VPN Connection Name
        - VPN address
        - Username/Password (optional)
            - It is possible to connect via a certificate

- Dial-Up
    - Choose to configure a Dial-Up connection
    - Your computer must be connected to a dial-up modem
    - Enter the dial-up phone number, username and password

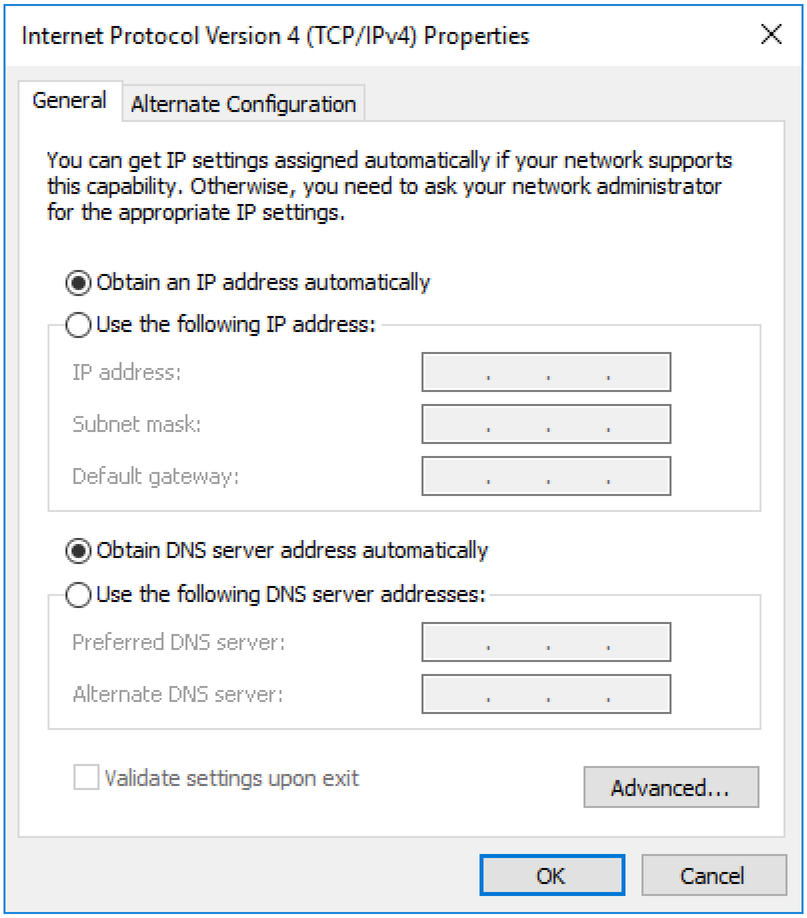


How do you want to connect?

→ Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly
Connect directly to a phone number without going through the Internet.

- Wireless
    - Select a wireless SSID from one that is available
    - Enter the password or username/password
- Wired
    - Connect the cable to the ethernet port on the computer
    - The computer should automatically connect to the wired network
    - You may need to configure a static IP if the network isn't DHCP
        - Select the Ethernet adapter
        - Choose IPv4 or IPv6 properties
        - Enter the IP address, gateway, subnet mask, and DNS server addresses



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

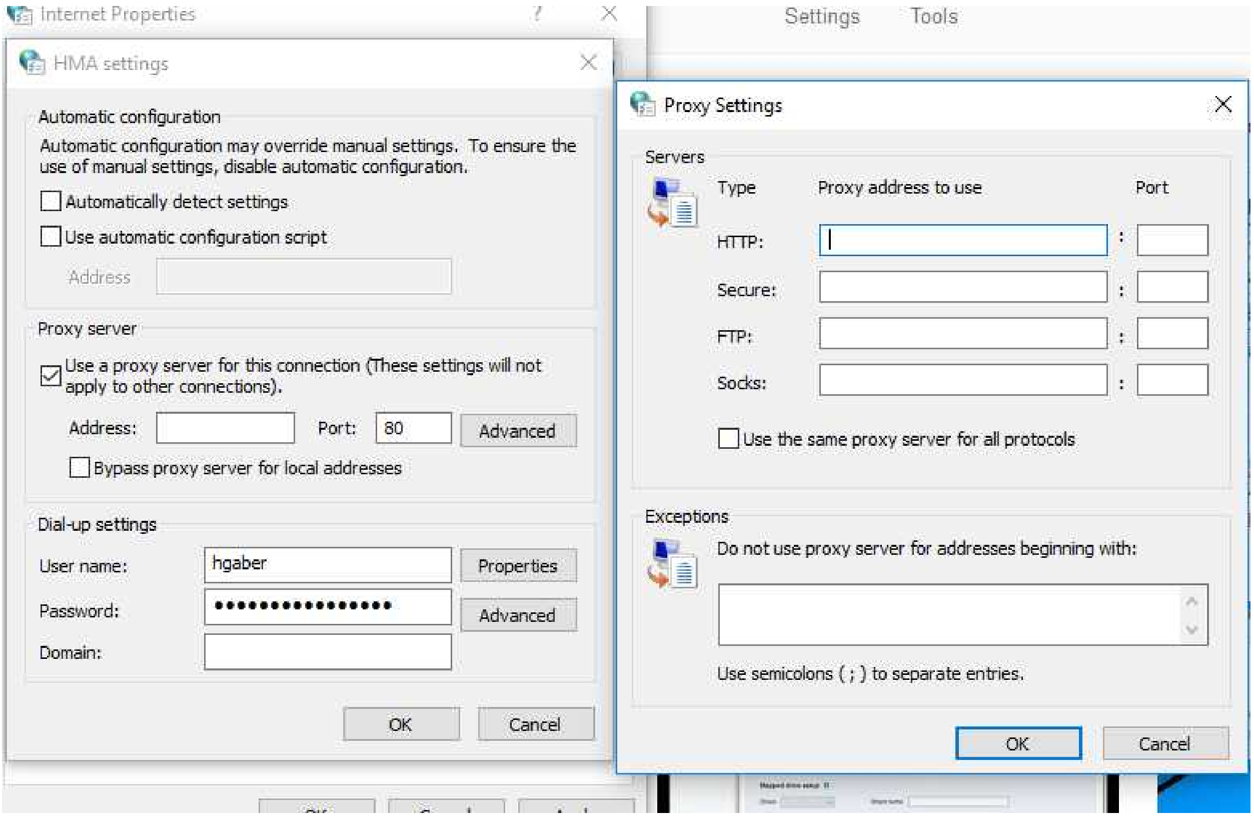
Alternate DNS server: . . .

□ Validate settings upon exit

- WWAN – Cellular
  - Your computer must be equipped with a cellular modem and SIM card
  - The modem will typically obtain all settings from the network automatically
  - If not, you must configure the APN settings
    - You can obtain these settings from the ISP

Proxy Settings

- A proxy server sits between your computer and the internet
- You can access the proxy server from the Internet Properties
    - Enter the proxy address and port for each server



HMA settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

☑ Use a proxy server for this connection (These settings will not apply to other connections).

Address: Port: 80 Advanced

□ Bypass proxy server for local addresses

Dial-up settings

User name: hgaber Properties

Password: ●●●●●●●●●●●●●●●● Advanced

Domain:

OK Cancel

Proxy Settings

Servers

Type	Proxy address to use		Port
HTTP:		:	
Secure:		:	
FTP:		:	
Socks:		:	

□ Use the same proxy server for all protocols

Exceptions

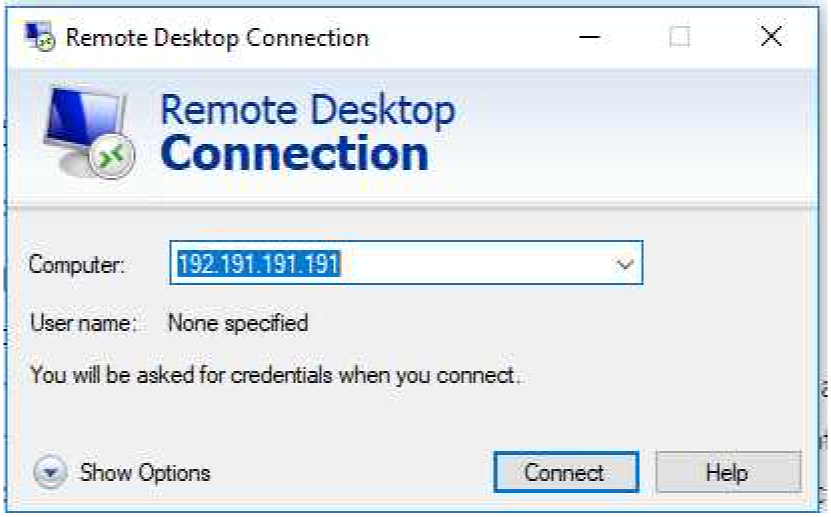
Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

OK Cancel

Remote Desktop Connection

- Uses Remote Desktop Protocol
- Developed by Microsoft.
- Allows you to connect to a Windows machine
  - Install xrdp on a UNIX machine to connect to it via RDP
- The machine that you connect to must have RDP enabled (requires Windows Professional)
- You can share
  - Hard Drives
  - Printers
  - Audio
  - Clipboard (can copy to/from host/remote computer)
- You launch RDP and enter the IP address / hostname

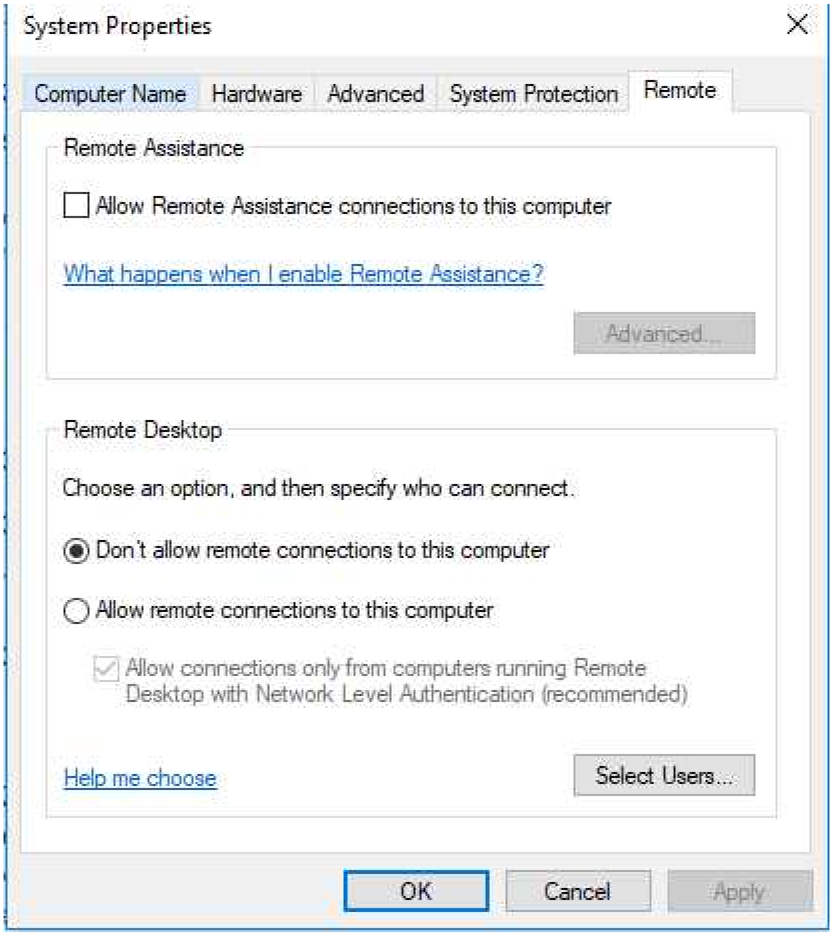


Computer: 192.191.191.191

User name: None specified

You will be asked for credentials when you connect.

- You are required to enter your username and password (on the remote computer) to connect
  - The username and password must be configured on the remote computer
  - Or the username and password must be configured on an Active Directory server of which the remote computer is a part of
- RDP uses TCP port 3389
- The computer that you're connecting to must permit remote connections
  - To enable RDP, go to System Properties
  - You can choose to permit only specific users to connect



System Properties

Remote Assistance

□ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

● Don't allow remote connections to this computer

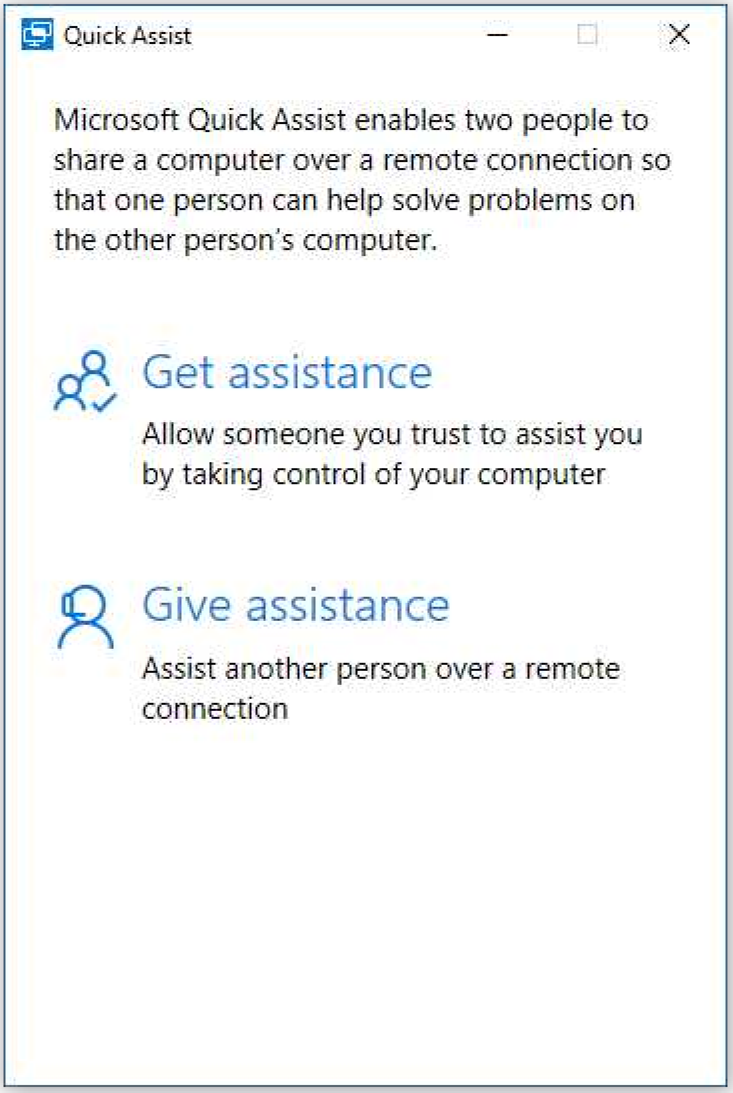
○ Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Remote Assistance

- Allows others to connect to your computer to assist you
- They must use the Quick Assist application
- Your computer must have the "remote assistance" option enabled
- There are some better third-party tools for providing remote assistance (discussed later)



Microsoft Quick Assist enables two people to share a computer over a remote connection so that one person can help solve problems on the other person's computer.

Get assistance

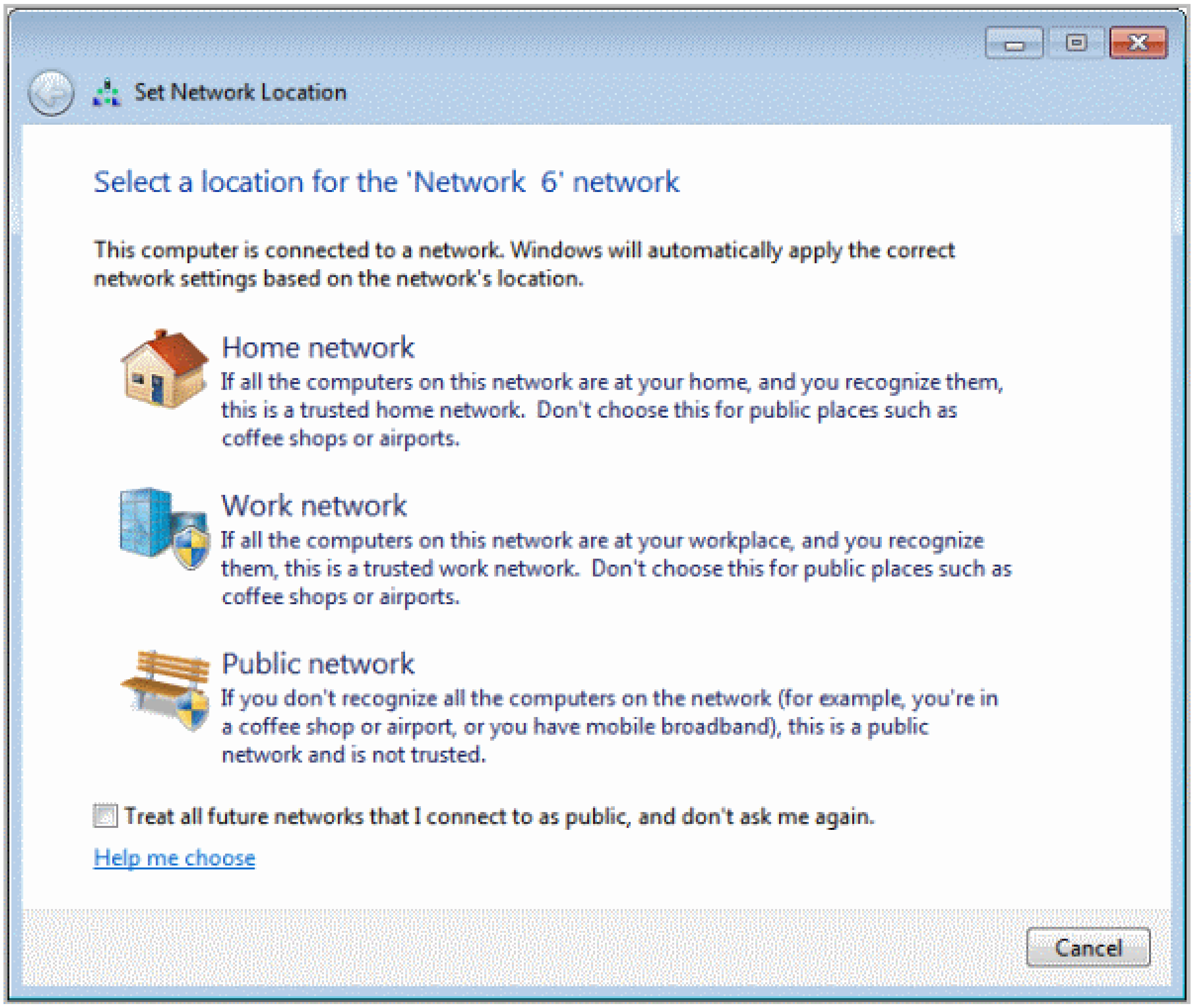
Allow someone you trust to assist you by taking control of your computer

Give assistance

Assist another person over a remote connection

Home vs Work vs Public Network Settings

- When connecting to a network for the first time, you're asked to choose what kind of network it is
  - Home and Work networks are trusted (can share files and printers)
    - Home and Work networks have the same settings, but Work networks won't allow you to join a HomeGroup
  - Public Networks are not trusted (don't share files or printers)



Select a location for the 'Network 6' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

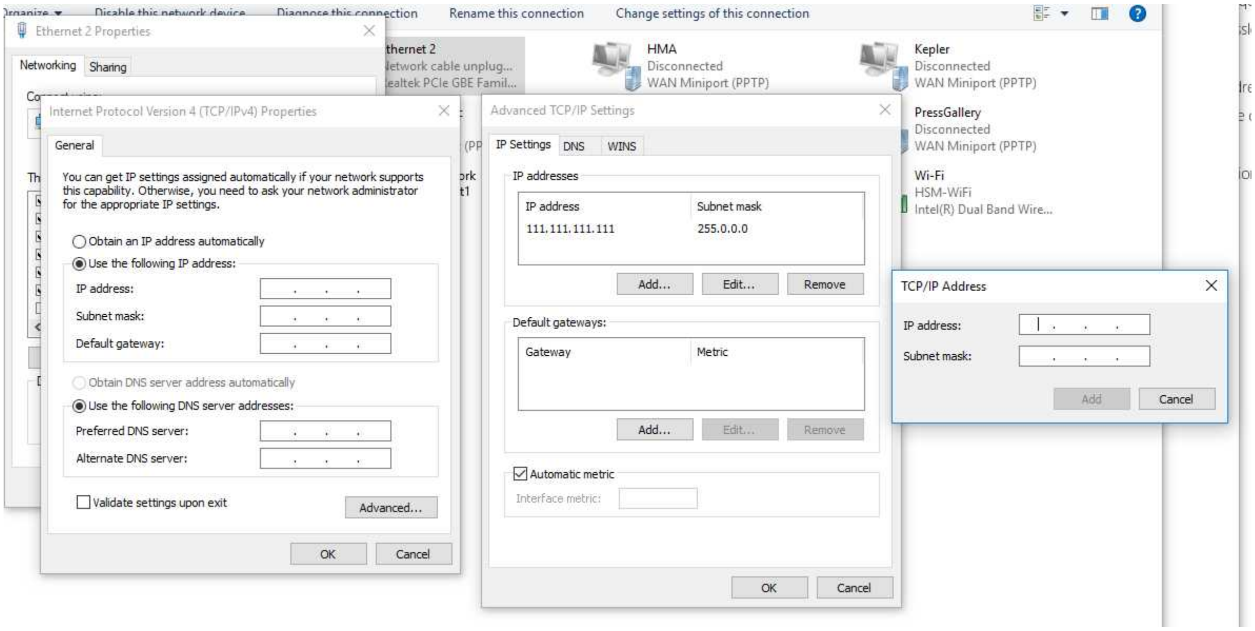
□ Treat all future networks that I connect to as public, and don't ask me again.

Firewall Settings (Exceptions, Configuration, Enable/Disable)

- Mentioned earlier
- There are two ways to configure a firewall
  - Block all traffic and then set rules to allow specific items (whitelisting)
    - More secure, but can cause issues if legitimate traffic is blocked
  - Allow all traffic and then set rules to block specific items (blacklisting)
    - Less secure, but more convenient
- Firewall comes preconfigured with a set of rules
  - When you install an application, it will add/modify rules as necessary so that it can function
  - Can create rules with the wizard
    - Allow/block traffic coming from or heading to a specific IP address, port, or application
- The Windows Firewall can be disabled
  - Not recommended
  - Can be disabled if you use a third-party app to manage security (such as Norton Antivirus)

Configuring an Alternative IP address in Windows (IP address, subnet mask, DNS, Gateway)

- There are two scenarios
  - Your computer is accessible on more than one IP address at the same time (for example, a computer server is connected to multiple networks)
    - Choose Advanced from the IPv4 Properties window
    - In the Advanced window (IP Settings tab), you can add multiple IP addresses, subnet masks and gateways
    - In the Advanced window (DNS tab), you can add multiple DNS servers



Ethernet 2 Properties

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced TCP/IP Settings

IP Settings | DNS | WINS

IP addresses

IP address	Subnet mask
111.111.111.111	255.0.0.0

Default gateways:

Gateway	Metric

☑ Automatic metric
Interface metric:

TCP/IP Address
IP address: . . .
Subnet mask: . . .

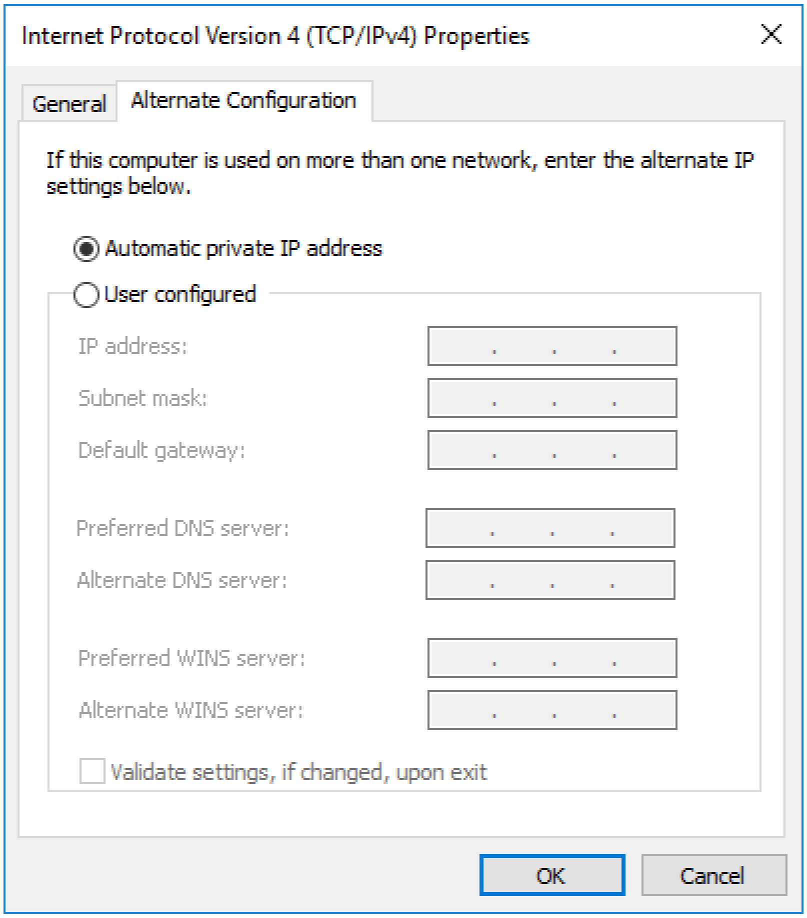
HMA
Disconnected
WAN Miniport (PPTP)

Kepler
Disconnected
WAN Miniport (PPTP)

PressGallery
Disconnected
WAN Miniport (PPTP)

Wi-Fi
HSM-WiFi
Intel(R) Dual Band Wire...

  - Your computer is used in two separate locations, and both require static IPs (for example at an office and at home, and it is too much of a hassle to change the static IP each time you go to work or go home)
    - It's possible to configure a second (or multiple) IP addresses on a computer
    - Traffic won't route to the second IP address unless the computer is in the correct subnet
    - Access IPv4 settings and choose Alternate Configuration



If this computer is used on more than one network, enter the alternate IP settings below.

● Automatic private IP address

○ User configured

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

Preferred DNS server: . . .

Alternate DNS server: . . .

Preferred WINS server: . . .

Alternate WINS server: . . .

□ Validate settings, if changed, upon exit

Network Card Properties (Duplex, Speed, Wake-on-LAN, QoS, BIOS (on-board NIC))

- Depending on the type of network card, some of the following settings can be modified
    - Can access the settings from the NIC Properties (in Device Manager)
- Duplex
    - There are three options: Auto, Half-Duplex, and Full-Duplex
    - Half-Duplex is used for 10/100Mbps traffic (uses 4 of the 8 wires in an ethernet cable)
    - Full-Duplex is used for 1000Mbps traffic (uses all 8 wires in an ethernet cable), although it can be used for 10/100Mbps traffic
    - Auto allows the two devices (your network card, and the switch/router/other network device you're connected to) to automatically agree on a duplex setting
- Speed
    - There are three options (at least): Auto, 100Mbps, 1000Mbps
    - There may be other (faster options) such as 10Gbps, depending on the size of the card
    - Older cards may offer the 10Mbps option as well
    - Auto allows the two devices (your network card, and the switch/router/other network device you're connected to) to automatically agree on a speed
- Wake-on-LAN
    - Allows a computer that is asleep (but connected to ethernet) to automatically wake up if it receives a "magic packet"
    - A Magic Packet is the value "FF FF FF FF FF FF" followed by sixteen repetitions of the computer's MAC address
- QoS
    - Quality of Service
    - Allows the network card to prioritize different types of traffic
- BIOS
    - The NIC might be integrated into the motherboard
    - Can enable or disable an integrated NIC from the BIOS

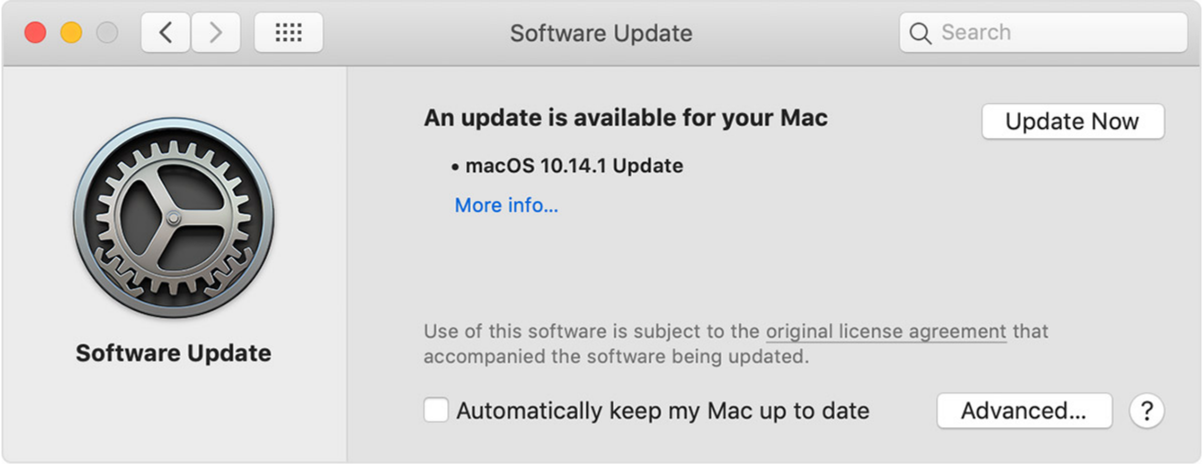
1.9 Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems.

- *Best practices*
  - *Scheduled backups*
  - *Scheduled disk maintenance*
  - *System updates/App Store*
  - *Patch management*
  - *Driver/firmware updates*
  - *Antivirus/Anti-malware updates*
- *Tools*
  - *Backup/Time Machine*
  - *Restore/Snapshot*
  - *Image recovery*
  - *Disk maintenance utilities*
  - *Shell/Terminal*
  - *Screen sharing*
  - *Force Quit*
- *Features*
  - *Multiple desktops/Mission Control*
  - *Key Chain*
  - *Spot Light*
  - *iCloud*
  - *Gestures*
  - *Finder*
  - *Remote Disc*
  - *Dock*
  - *Boot Camp*
- *Basic Linux commands*
  - *ls*
  - *grep*

- *cd*
- *shutdown*
- *pwd vs. passwd*
- *mv*
- *cp*
- *rm*
- *chmod*
- *chown*
- *iwconfig/ifconfig*
- *ps*
- *su/sudo*
- *apt-get*
- *vi*
- *dd*
- *kill*

Best Practices for a Mac

- Scheduled backups
    - Use a program such as Carbonite or schedule a task through Automator (Mac Task Scheduling app)
    - Regular backups are important in case of damage to the computer
- Scheduled disk maintenance
    - Run disk utility to scan the disk for errors and repair them
    - Can repair bad sectors, corrupted files, and fragmented files
- System Updates/App Store
    - You can check for updates from System Preferences (Software Update)
    - If an update is available, you can choose the Update Now button to download and install it
    - You can also set the Update tool to automatically download and install updates
    - An update to macOS will automatically update apps like Mail and iTunes



An update is available for your Mac

- **macOS 10.14.1 Update**

Use of this software is subject to the original license agreement that accompanied the software being updated.

□ Automatically keep my Mac up to date

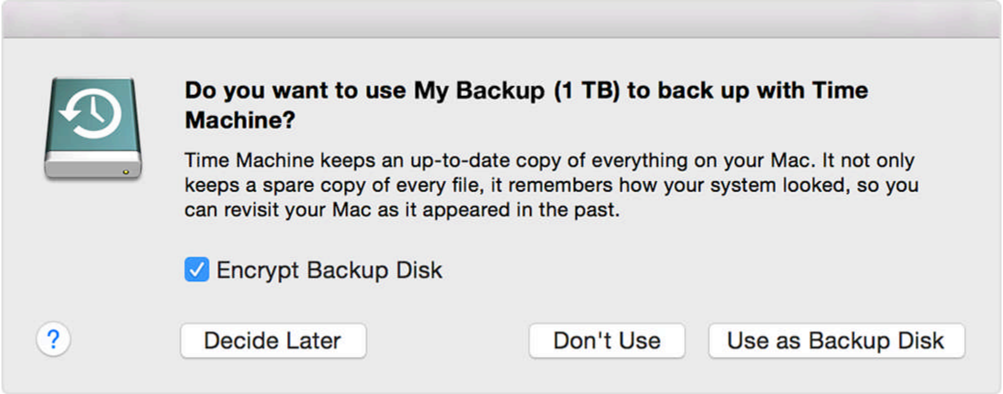
- Patch Management
    - Security updates come through the normal Apple procedure
    - You can also use a third-party tool to manage updates for multiple machines at a time
- Driver/Firmware Updates
    - Driver updates typically download & install automatically from the Software Update tool

    - If the driver update doesn’t download automatically, then download it from the manufacturer’s website
- Antivirus/Anti-malware
    - Download and install an antivirus program
    - The antivirus program should automatically check for and download updates

Mac Tools - Backup/Time Machine

Time Machine allows you to back up your Mac

- Connect an external drive (USB or Network Attached Storage)
- Choose to back up to the drive via Time Machine (the Mac will automatically prompt you when you connect the drive)

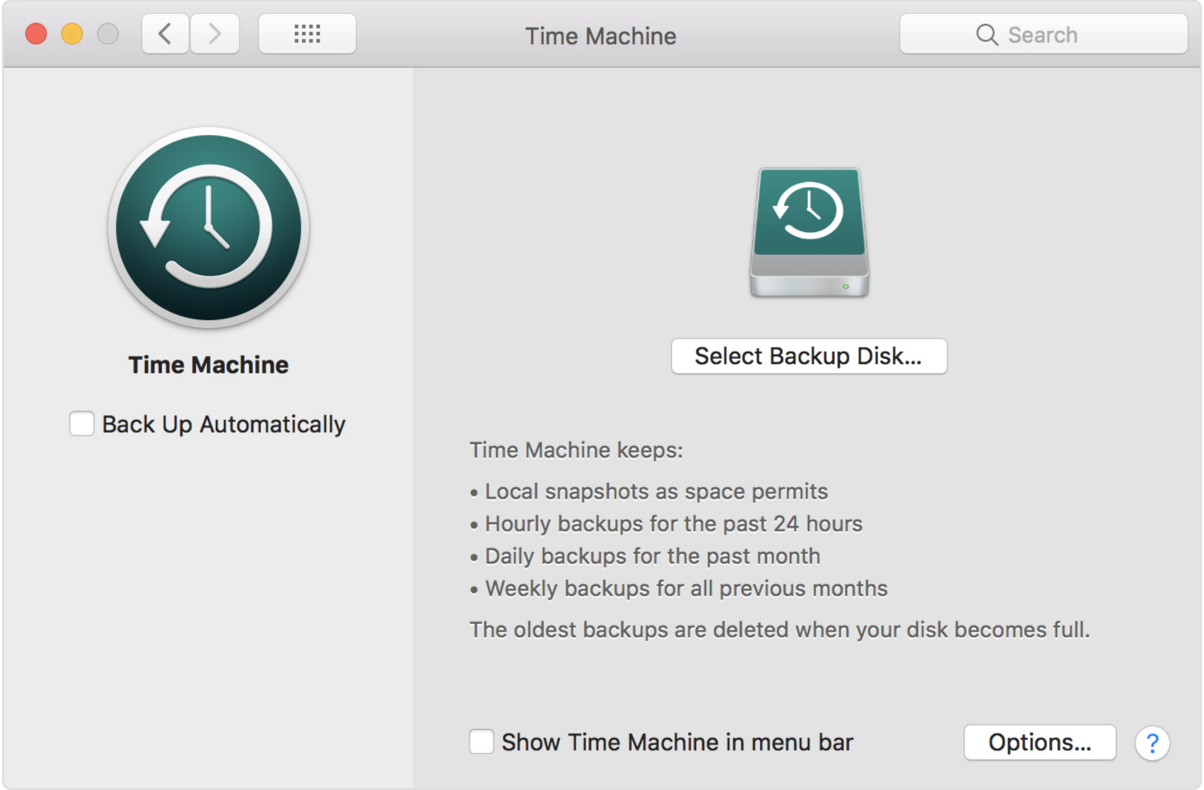


Do you want to use My Backup (1 TB) to back up with Time Machine?

Time Machine keeps an up-to-date copy of everything on your Mac. It not only keeps a spare copy of every file, it remembers how your system looked, so you can revisit your Mac as it appeared in the past.

☑ Encrypt Backup Disk

- You may also choose to back up to an external drive from Time Machine



□ Back Up Automatically

Time Machine keeps:

- Local snapshots as space permits
- Hourly backups for the past 24 hours
- Daily backups for the past month
- Weekly backups for all previous months

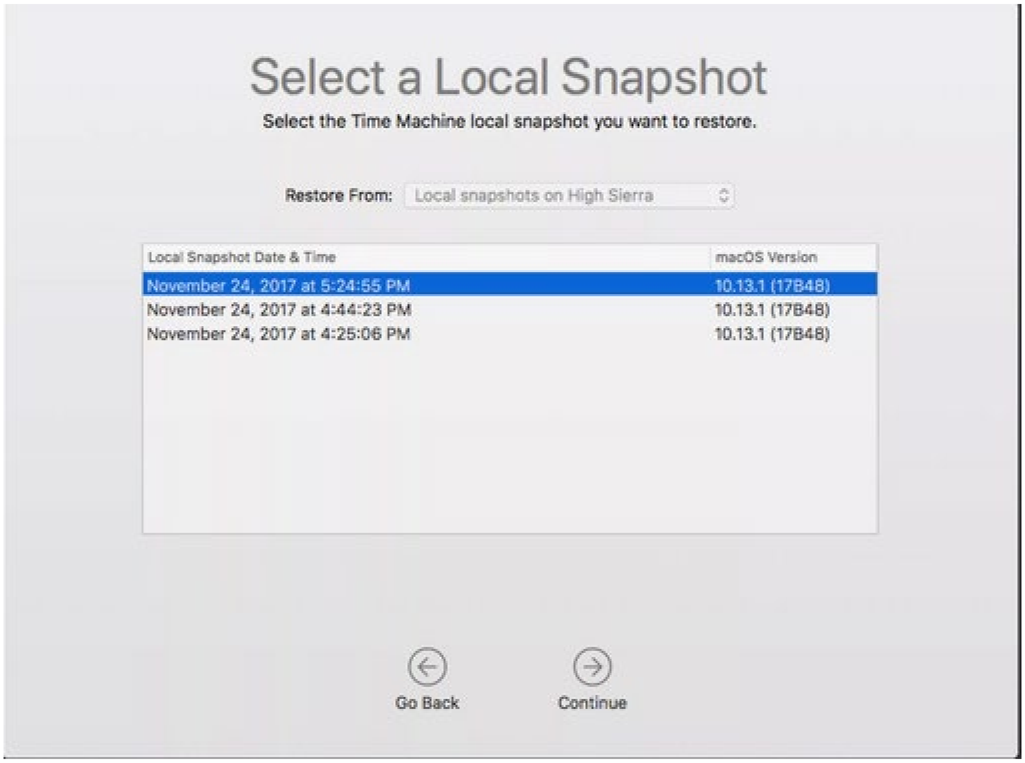
The oldest backups are deleted when your disk becomes full.

□ Show Time Machine in menu bar

Mac Tools – Restore/Snapshot

Snapshots allow you to restore your Mac to previous points in time

- Similar to Windows System Restore
- You can roll back to a previous point in time
- Combine Snapshot with Time Machine
- Snapshots are automatic, and created when system updates are installed
- It's possible to create a manual snapshot
- You can restore to a snapshot by
    - Rebooting your Mac
    - Choose the Recovery option
    - Choose to Restore from Time Machine
    - Choose a snapshot from the list



Select a Local Snapshot

Select the Time Machine local snapshot you want to restore.

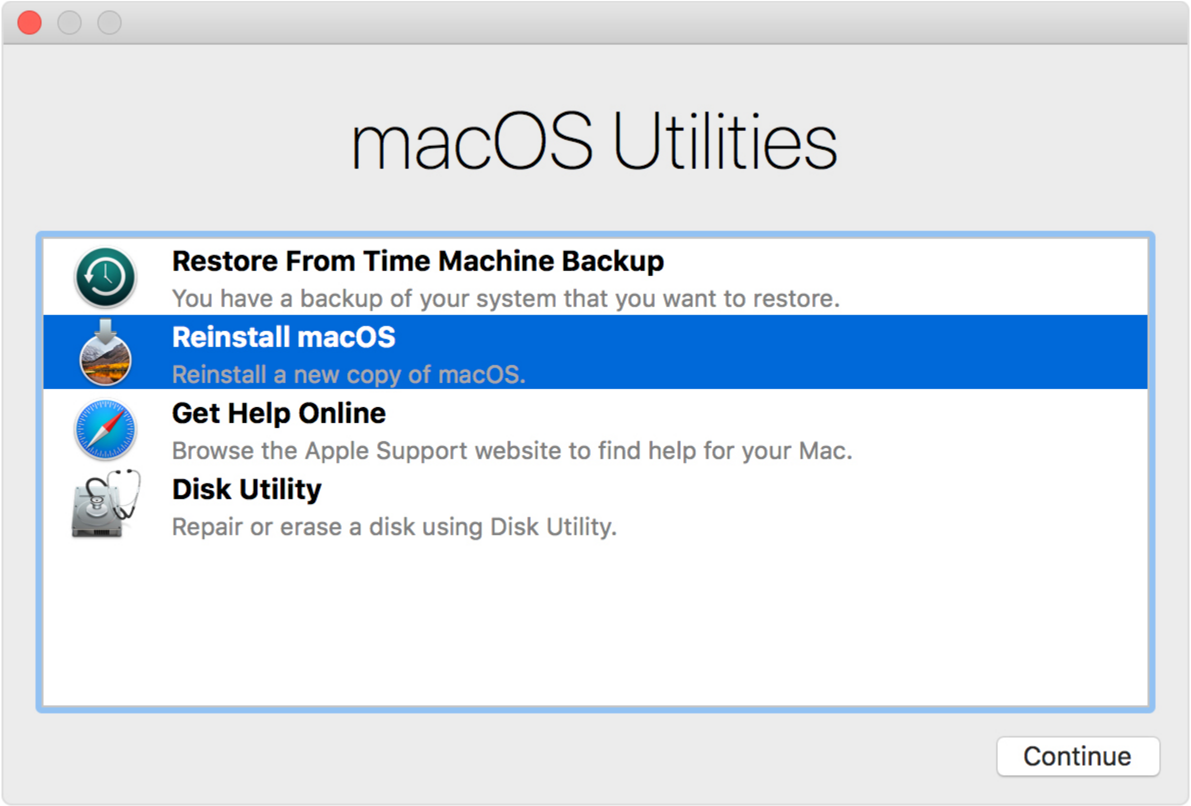
Restore From: Local snapshots on High Sierra

Local Snapshot Date & Time	macOS Version
November 24, 2017 at 5:24:55 PM	10.13.1 (17B48)
November 24, 2017 at 4:44:23 PM	10.13.1 (17B48)
November 24, 2017 at 4:25:06 PM	10.13.1 (17B48)

Mac Tools – Image Recovery

To access Mac Utilities

- During boot, hold down the Command + R keys
- The Utilities window will come up



macOS Utilities

Restore From Time Machine Backup
You have a backup of your system that you want to restore.

Reinstall macOS
Reinstall a new copy of macOS.

Get Help Online
Browse the Apple Support website to find help for your Mac.

Disk Utility
Repair or erase a disk using Disk Utility.

- Choose
  - Restore from Time Machine Backup (restore from a back up, if you have one)
  - Reinstall macOS (reinstalls the operating system)
  - Disk Utility (repairs or erases a disk)
- Newer computers can try to connect to an Apple server and download recovery files over the internet
- If neither the Utilities nor the Internet recovery will function
  - Download a macOS Installer from the Apple website
  - Create installation media
    - Connect a flash drive to another Mac
    - Run Terminal

    - Type the command *sudo /Applications/Install/ macOS/ Mojave.app/Contents/Resources/createinstallmedia --volume /Volumes/MyVolume* (for Mojave)
        - Replace Mojave with the name of the operating system that you downloaded
    - The command will create a bootable installer on the USB
- Boot from the USB

Mac Tools – Disk Maintenance Utilities

To access Disk Maintenance

- Reboot the Mac
- During booting, hold down the Command + R keys
- Choose Disk Utility
    - Select the disk you want to repair
    - Choose “First Aid”
    - The Disk Utility will scan the drive and repair any errors

Mac Tools – Shell/Terminal

- Similar to Command Prompt on Windows
- Runs on a UNIX shell
- Run Terminal from Finder
- Details about commands are explained later

Mac Tools – Screen Sharing

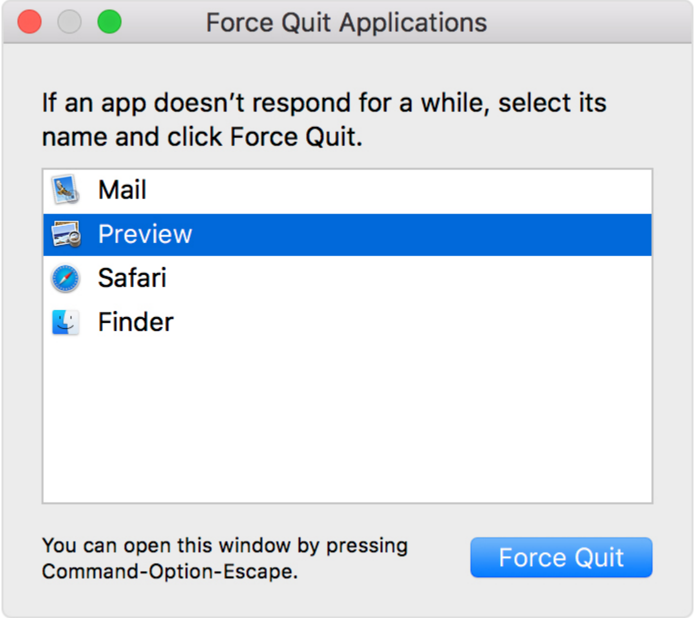
Can share your Mac screen with another Mac

- Similar to Remote Desktop on Windows
- Enable Screen Sharing by choosing System Preferences from the Apple menu
    - Choose Screen Sharing
    - Add users who are authorized to access the screen
    - Sign in to iCloud if necessary
- Connect to the Mac
    - Check Finder Preferences
    - Choose the remote Mac from the list
    - You must be signed in to the same iCloud account on both Macs
- You must have a router that supports UPnP at the remote Mac

Mac Tools – Force Quit

Fore Quit allows you to exit a program that is stuck

- Hold down Option + Command + Escape
- The Force Quit window will pop up



Force Quit Applications

If an app doesn't respond for a while, select its name and click Force Quit.

Mail
Preview
Safari
Finder

You can open this window by pressing Command-Option-Escape.

- Select the app you want to close from the list, and choose Force Quit

Mac Features - Multiple Desktops/Mission Control

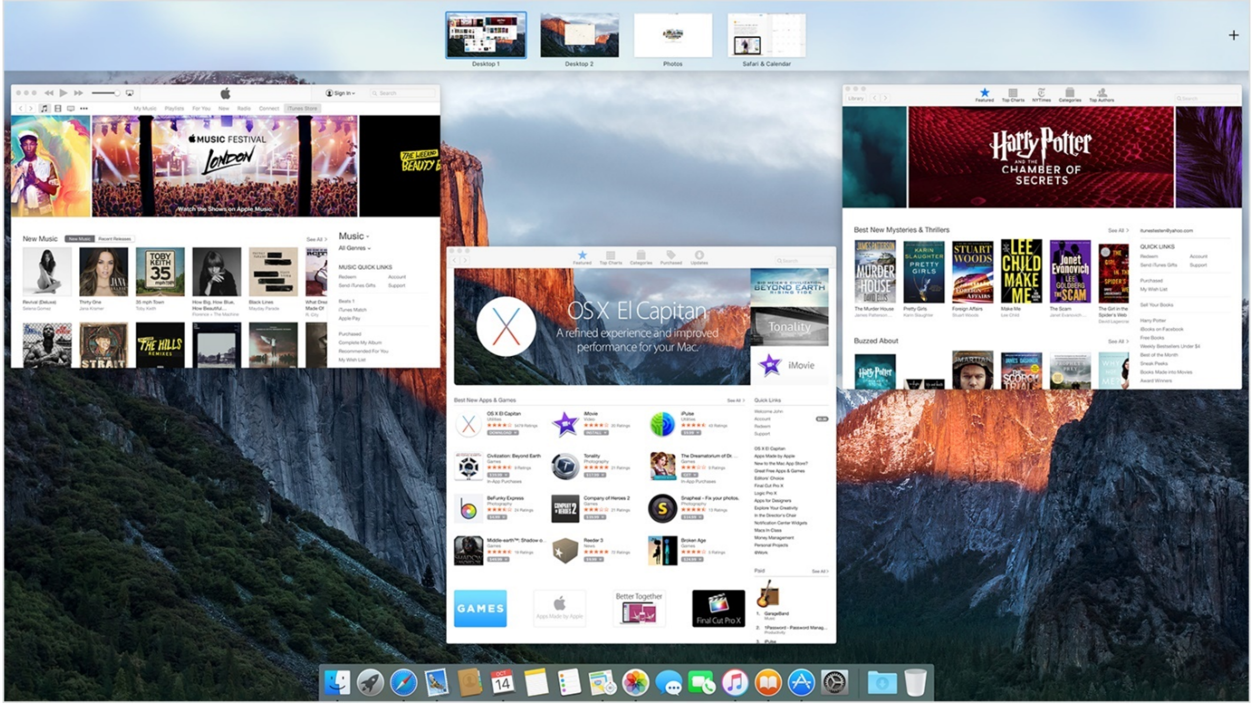
Mission Control allows you to view all open windows at the same time

Multiple ways to cccess Mission Control

- Swipe up with three or four fingers on your Multi-Touch trackpad or Magic Trackpad.
- Double-tap the surface of your Magic Mouse with two fingers.
- Click Mission Control in the Dock or Launchpad.
- Press the Mission Control key on your Apple keyboard or press Control–Up Arrow.
- In OS X El Capitan, drag a window to the top of the screen.

It's possible to have multiple desktops (known as spaces)

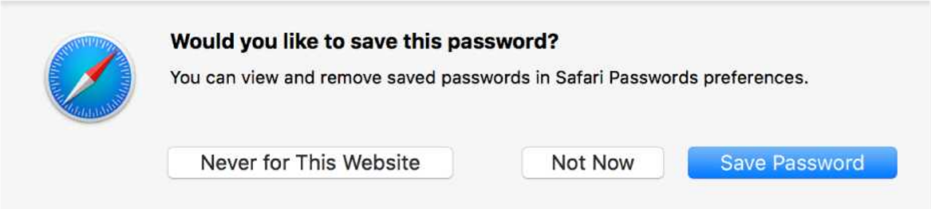
- Each desktop can have multiple windows and programs
- For example, you might have one desktop for work, one for school, and one for entertainment
- The different desktops are shown at the top of the screen (you can switch between desktops)
- You can add additional desktops
- You can move a window from one desktop to another by dragging it
- It's possible to close a desktop


Desktop 1
Desktop 2
Photos
Safari & Calendar
+
MUSIC FESTIVAL
LONDON
OS X El Capitan
A refined experience and improved performance for your Mac.
Harry Potter and the Chamber of Secrets
GAMES

Mac Features – Key Chain

The Key Chain keeps track of usernames and passwords

- You can choose to save usernames and passwords in the keychain
- When you first enter a username/password into a website or app, Mac will prompt you to store it



Would you like to save this password?

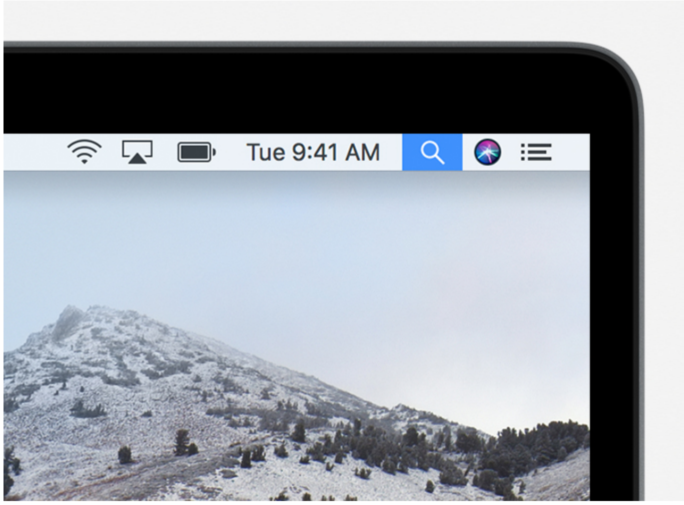
You can view and remove saved passwords in Safari Passwords preferences.

- Websites and apps can automatically store tokens and certificates in the keychain

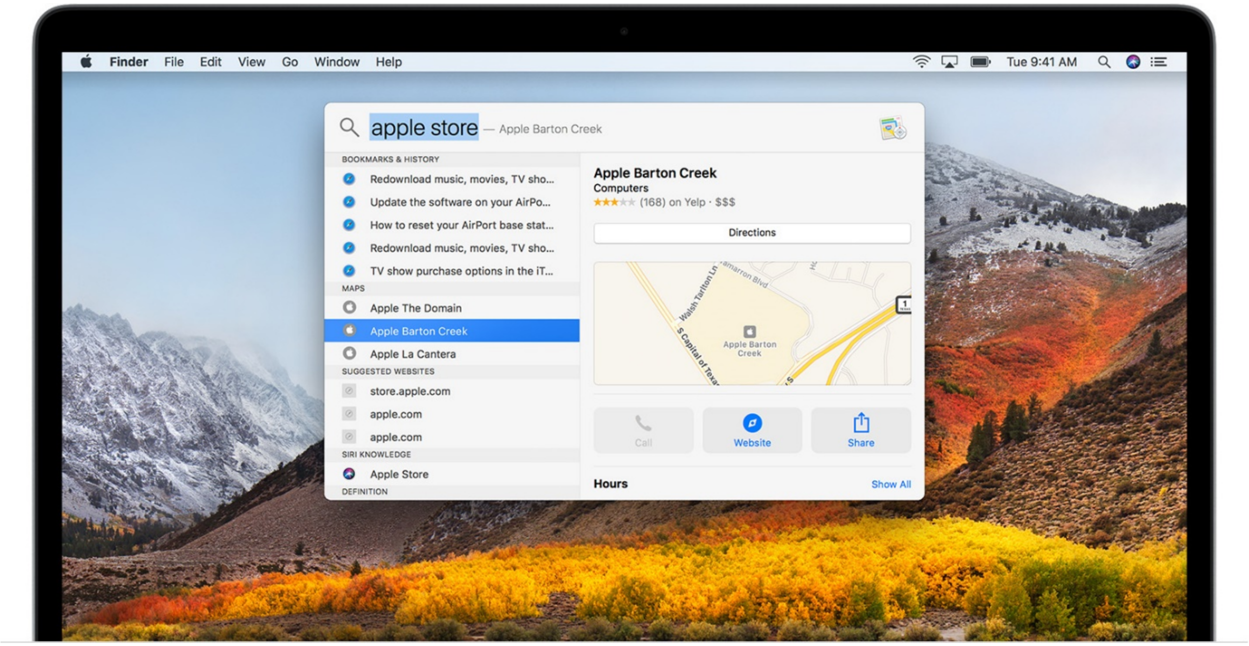
Mac Features – Spot Light

Spot Light allows you to find items on your Mac

- Choose the spoltlight icon from the top right bar



- You can search for items on the computer and/or items on the internet, including
    - Weather forecast
    - Definitions
    - Calculations
    - Measurement conversions
    - Movie showtimes


Finder File Edit View Go Window Help
Tue 9:41 AM
apple store — Apple Barton Creek
BOOKMARKS & HISTORY
Redownload music, movies, TV sho...
Update the software on your AirPo...
How to reset your AirPort base stat...
Redownload music, movies, TV sho...
TV show purchase options in the iT...
MAPS
Apple The Domain
Apple Barton Creek
Apple La Cantera
SUGGESTED WEBSITES
store.apple.com
apple.com
apple.com
SIRI KNOWLEDGE
Apple Store
DEFINITION
Apple Barton Creek
Computers
★★★☆☆ (168) on Yelp · $$$
Directions
Apple Barton Creek
Call
Website
Share
Hours
Show All

Mac Features – iCloud

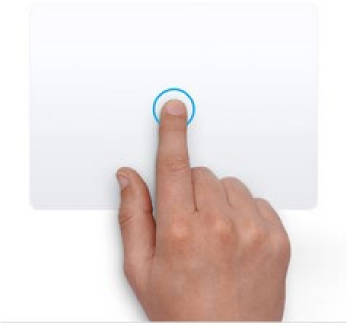
iCloud backs up your data to an iCloud account

- iCloud is installed on every Apple device
- iCloud syncs data between all devices signed in with the same Apple ID
- Apple charges for storage costs beyond the first5 GB

Mac Features – Gestures

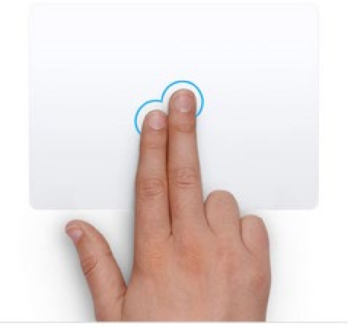
Gestures allow you to access different features

- Gestures work on the Magic Trackpad or on a normal mouse (limited functionality on a mouse)
- On the Magic Trackpad



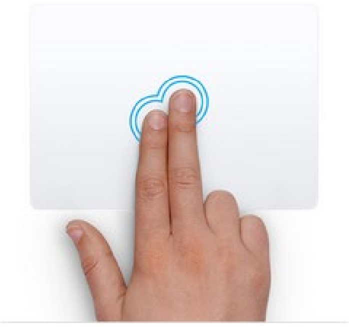
Tap to click

Tap with one finger to click.



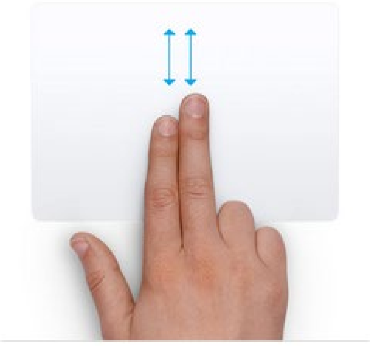
Secondary click (right-click)

Click or tap with two fingers.



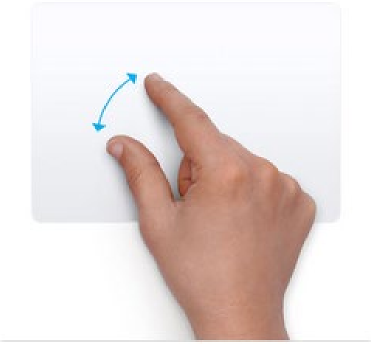
Smart zoom

Double-tap with two fingers to zoom in and back out of a webpage or PDF.



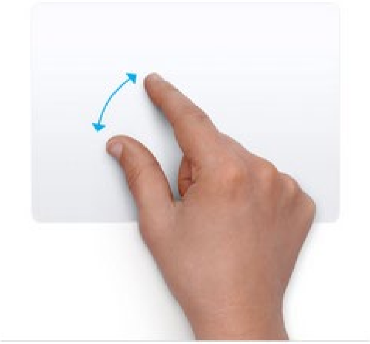
Scroll

Slide two fingers up or down to scroll.[1]



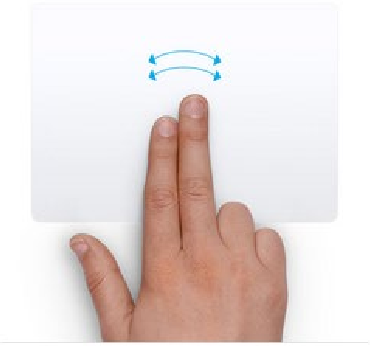
Zoom in or out

Pinch with two fingers to zoom in or out.

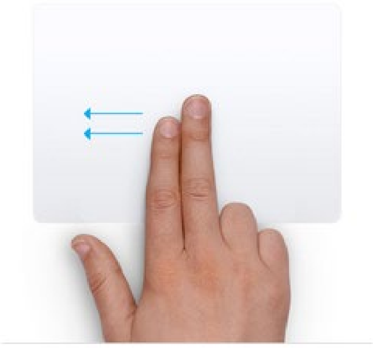


Rotate

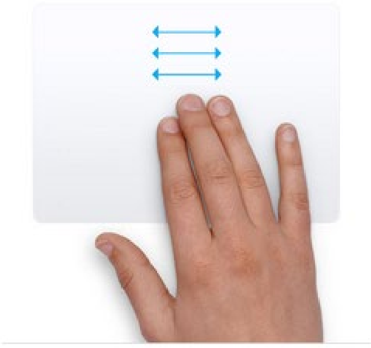
Move two fingers around each other to rotate a photo or other item.



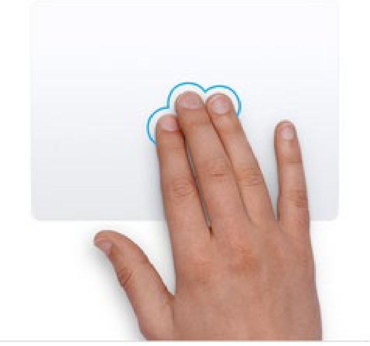
Swipe between pages
Swipe left or right with two fingers to show the previous or next page.



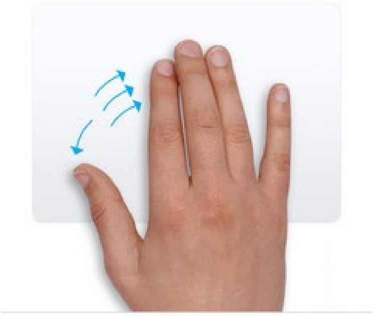
Open Notification Center
Swipe left from the right edge with two fingers to show Notification Center.



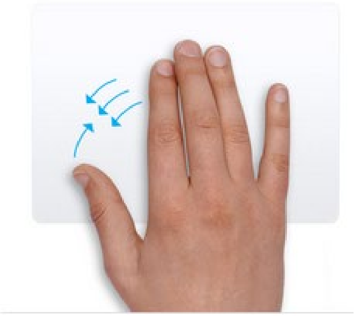
Three finger drag
Use three fingers to drag items on your screen, then click or tap to drop.



Look up and data detectors
Tap with three fingers to look up a word or take actions with dates, addresses, phone numbers, and other data.



Show desktop
Spread your thumb and three fingers apart to show your desktop.

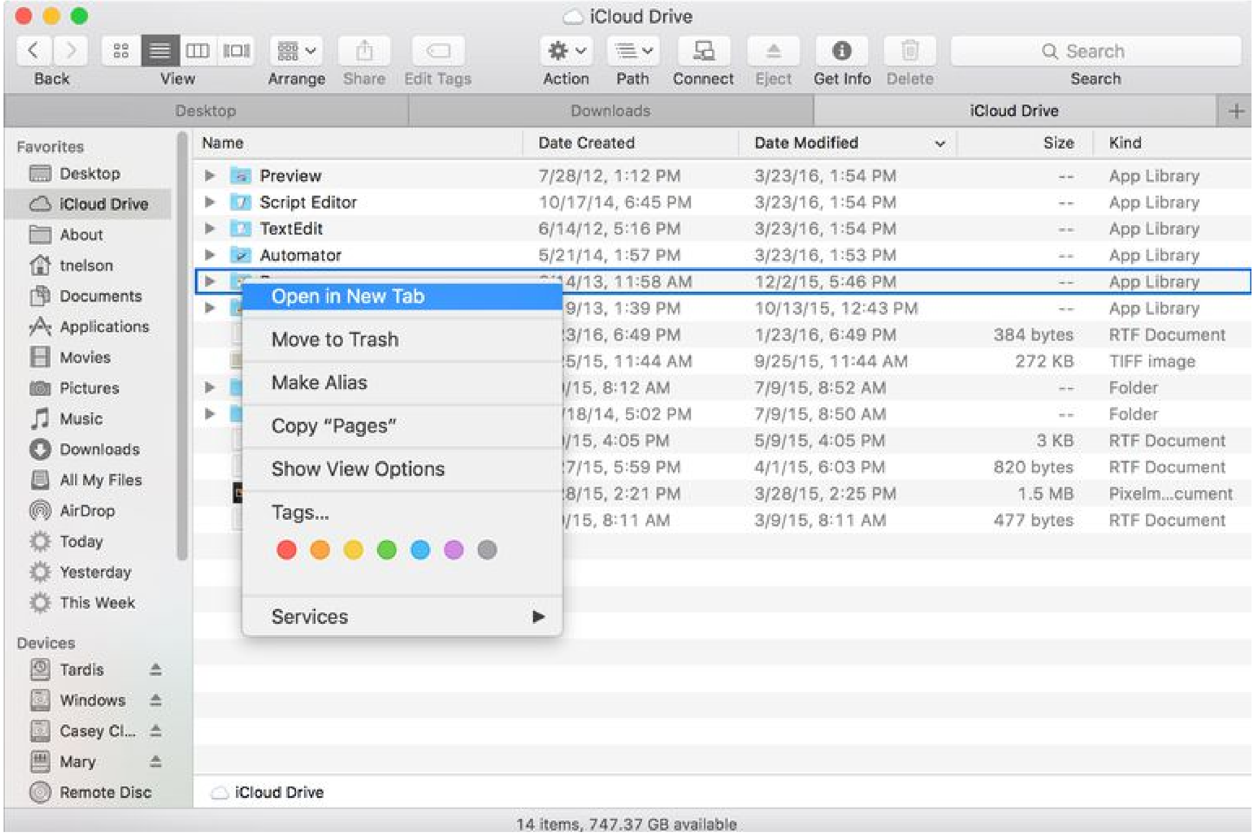


Launchpad
Pinch your thumb and three fingers together to display Launchpad.

Mac Features – Finder

The finder is the file manager

- Similar to Windows Explorer
- Allows you to launch apps, view files and view disks
- Can show a preview of a file



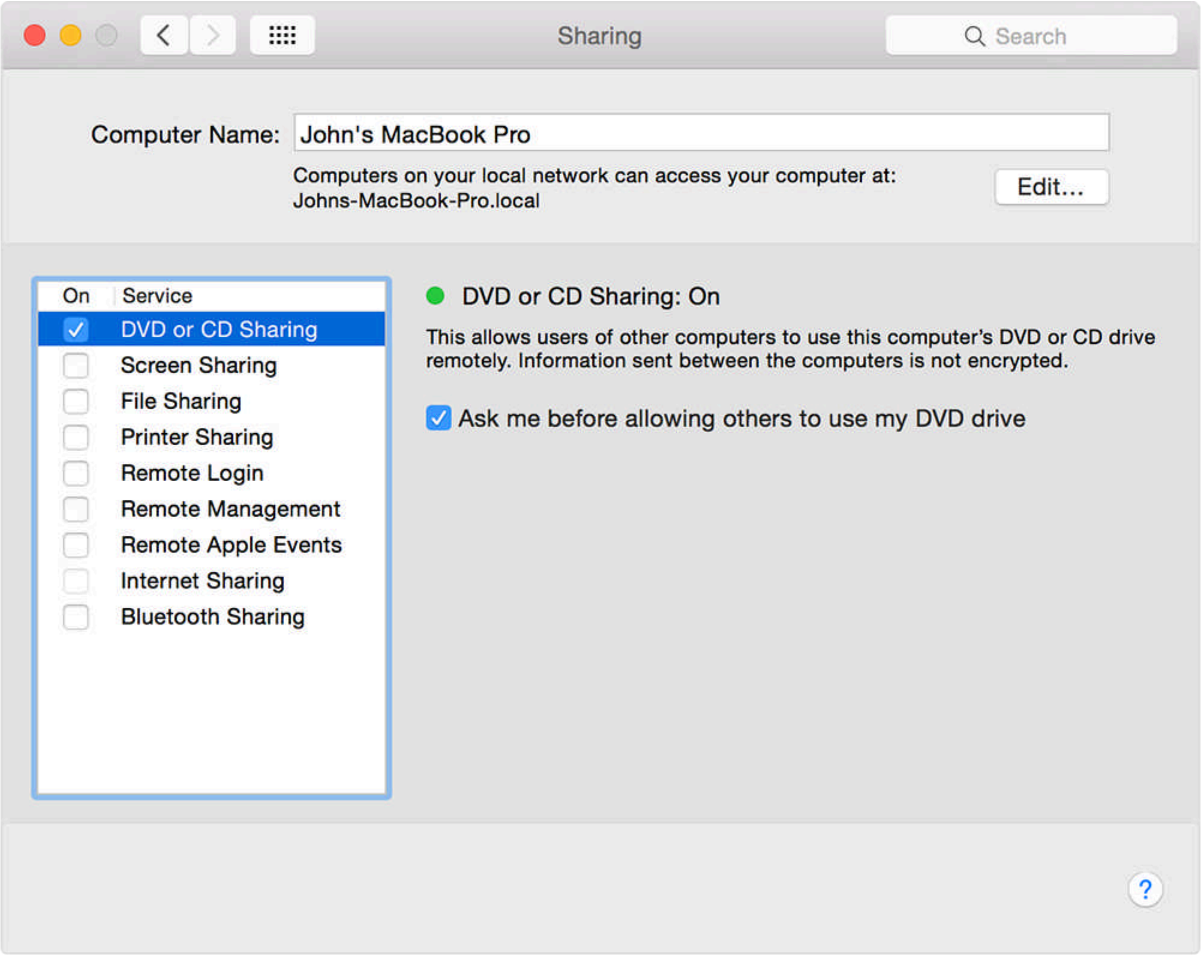
Name	Date Created	Date Modified	Size	Kind
Preview	7/28/12, 1:12 PM	3/23/16, 1:54 PM	--	App Library
Script Editor	10/17/14, 6:45 PM	3/23/16, 1:54 PM	--	App Library
TextEdit	6/14/12, 5:16 PM	3/23/16, 1:54 PM	--	App Library
Automator	5/21/14, 1:57 PM	3/23/16, 1:53 PM	--	App Library
	4/13, 11:58 AM	12/2/15, 5:46 PM	--	App Library
	9/13, 1:39 PM	10/13/15, 12:43 PM	--	App Library
	3/16, 6:49 PM	1/23/16, 6:49 PM	384 bytes	RTF Document
	5/15, 11:44 AM	9/25/15, 11:44 AM	272 KB	TIFF image
	/15, 8:12 AM	7/9/15, 8:52 AM	--	Folder
	18/14, 5:02 PM	7/9/15, 8:50 AM	--	Folder
	/15, 4:05 PM	5/9/15, 4:05 PM	3 KB	RTF Document
	7/15, 5:59 PM	4/1/15, 6:03 PM	820 bytes	RTF Document
	8/15, 2:21 PM	3/28/15, 2:25 PM	1.5 MB	Pixelm...cument
	/15, 8:11 AM	3/9/15, 8:11 AM	477 bytes	RTF Document

14 items, 747.37 GB available

Mac Features – Remote Disc

Allows you to share a CD-ROM/DVD drive with another Mac (or Windows Computer). You can view files stored on a CD-ROM/DVD that is inserted into the optical drive of another Mac (or Windows computer)

- Useful if your Mac doesn't have an optical drive
- Doesn't work for CDs/DVDs that contain movies or other copy-protected data
- Set up sharing on the computer that has the drive
    - Choose DVD or CD Sharing from the Sharing menu (on a Mac)



Computer Name: John's MacBook Pro

Computers on your local network can access your computer at:
Johns-MacBook-Pro.local

On	Service
☑	DVD or CD Sharing
□	Screen Sharing
□	File Sharing
□	Printer Sharing
□	Remote Login
□	Remote Management
□	Remote Apple Events
□	Internet Sharing
□	Bluetooth Sharing

● DVD or CD Sharing: On

This allows users of other computers to use this computer's DVD or CD drive remotely. Information sent between the computers is not encrypted.

☑ Ask me before allowing others to use my DVD drive

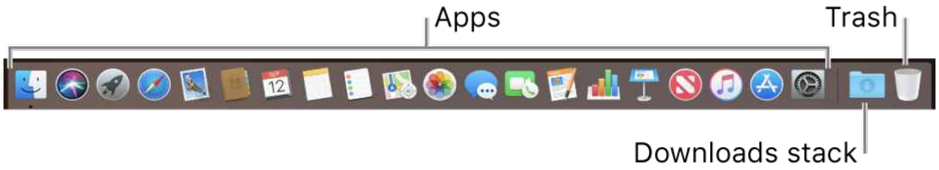
    - Install the DVD Sharing Update (on a Windows machine)
        - Choose DVD Sharing from the Hardware menu in the Control Panel
- Access the CD-ROM/DVD
    - No further steps are required

- Insert the CD-ROM/DVD into the optical drive
- It will automatically be available on any other Mac connected to the same network

Mac Features – Dock

The dock shows common files and programs

- Shows the last three recently opened apps
- Click on an app icon to open it
- Drag a file over an app icon to open the file with the app (for example drag a Word document over the Word icon to open that file in Word)
- You can add an app to the dock by dragging it there
- You can remove an app from the dock by dragging it off the dock
- You can rearrange the order of the apps on the dock by dragging them



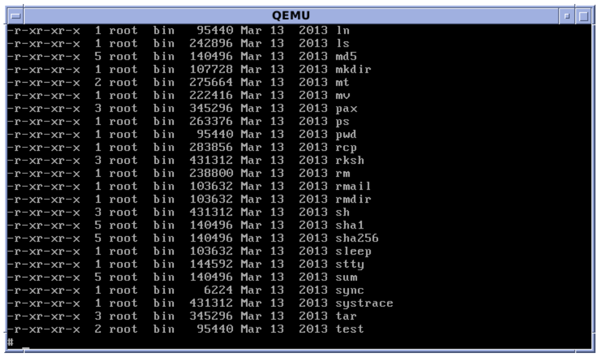
Mac Features – Boot Camp

- Allows you to install Windows on your Mac
- Recommended to have 128GB of free disk space
- To install Windows
    - Download Windows as a disk image (ISO)
    - Open Boot Camp Assistant
    - Create and format a partition for Windows
    - Install Windows
- To switch between Windows and Mac, you must reboot the computer
- A better, third-party program that allows you to run Windows is called Parallels
    - Allows you to run Windows and macOS at the same time
    - Allows you to run specific Windows programs on the macOS without having to run the full version of Windows (which could occupy significant system resources)
    - Allows you to access Windows files on OS X and vice versa
    - Windows 10 runs slower on Parallels than on Boot Camp

Basic Linux commands

macOS is based on Linux

- Includes a terminal (similar to a command prompt)
- The terminal runs a UNIX shell, which accepts Linux commands (other operating system shells are available however)
- As with Windows commands, each command could have several options
- Some commands include

ls	Lists all the files in a directory (similar to dir in Windows) 

```
-r-xr-xr-x  1 root  bin   95440 Mar 13  2013 ln
-r-xr-xr-x  1 root  bin  242896 Mar 13  2013 ls
-r-xr-xr-x  5 root  bin  140496 Mar 13  2013 md5
-r-xr-xr-x  1 root  bin  107728 Mar 13  2013 mkdir
-r-xr-xr-x  2 root  bin  275664 Mar 13  2013 mt
-r-xr-xr-x  1 root  bin  222416 Mar 13  2013 mv
-r-xr-xr-x  3 root  bin  345296 Mar 13  2013 pax
-r-xr-xr-x  1 root  bin  263376 Mar 13  2013 ps
-r-xr-xr-x  1 root  bin   95440 Mar 13  2013 pwd
-r-xr-xr-x  1 root  bin  283856 Mar 13  2013 rcp
-r-xr-xr-x  3 root  bin  431312 Mar 13  2013 rksh
-r-xr-xr-x  1 root  bin  238800 Mar 13  2013 rm
-r-xr-xr-x  1 root  bin  103632 Mar 13  2013 rmail
-r-xr-xr-x  1 root  bin  103632 Mar 13  2013 rmdir
-r-xr-xr-x  3 root  bin  431312 Mar 13  2013 sh
-r-xr-xr-x  5 root  bin  140496 Mar 13  2013 sha1
-r-xr-xr-x  5 root  bin  140496 Mar 13  2013 sha256
-r-xr-xr-x  1 root  bin  103632 Mar 13  2013 sleep
-r-xr-xr-x  1 root  bin  144592 Mar 13  2013 stty
-r-xr-xr-x  5 root  bin  140496 Mar 13  2013 sum
-r-xr-xr-x  1 root  bin    6224 Mar 13  2013 sync
-r-xr-xr-x  1 root  bin  431312 Mar 13  2013 systrace
-r-xr-xr-x  3 root  bin  345296 Mar 13  2013 tar
-r-xr-xr-x  2 root  bin   95440 Mar 13  2013 test
# _
```

grep	Search for text (as a regular expression) Can search inside files
cd	Change directory to a different directory (same as cd in Windows) Type *cd directory name* or *cd..* to move up one level
shutdown	Shuts down the computer
pwd vs passwd	pwd prints the name of the working directory passwd allows the user to change his password
mv	Moves or renames a file or directory

	Type *mv* ***oldfilename newfilename*** to rename a file from *oldfilename* to *newfilename* Type *mv* ***oldfilename newlocation*** to move a file from its current location to *newlocation*
cp	Makes a copy of a file Type *cp* ***filename newfilename*** to make a copy of filename called *newfilename* (in the same directory) Type *cp* ***filename newlocation*** to make a copy of filename in *newlocation* directory
rm	Deletes a file or directory Type *rm* ***directoryname*** to delete a directory
chmod	Changes file permissions In UNIX, a file has three sets of permissions • Read: view the file • Write: change the file • Execute: run the file The permissions are represented by a three-digit code The owner of a file, or the administrator can change permissions Type *chmod* ***permissioncode filename*** to change a file's permssions
chown	Changes the owner of a file or directory

	Type *chown* ***newowner filename*** where *newowner* is the name of the new owner and *filename* is the filename
iwconfig/ifconfig	iwconfig allows you to configure wireless interfaces ifconfig allows you to configure ethernet interfaces
ps	Lists all the running processes (similar to Windows task manager) Lists the process name and ID
su/sudo	su allows you to run a command as another user Requires the password of the other user Type *su* ***username*** sudo allows you to run a command with the security privileges of another user You don't need the other user's password, but your account must have permission to execute the command If you type *sudo* ***username*** command, you can run the command as username If you type *sudo* ***command***, with no username, sudo will run as the superuser
apt-get	Allows you to download packages (applications) Type *apt-get* ***applicationname***
vi	Runs the vi text editor

dd	Can duplicate data across multiple devices (similar to robocopy on Windows) Can also wipe a disk
kill	Ends a process Type *kill* ***processid***

Part H 220-1002 2.0 Security

2.1 Summarize the importance of physical security measures.

- *Mantrap*
- *Badge reader*
- *Smart card*
- *Security guard*
- *Door lock*
- *Biometric locks*
- *Hardware tokens*
- *Cable locks*
- *Server locks*
- *USB locks*
- *Privacy screen*
- *Key fobs*
- *Entry control roster*

Physical Security

Physical security is important

Physical security keeps the wrong people out of data centers, office buildings, server rooms, and other secure locations.

Mantrap 	A set of double doors. Combined with biometrics or access cards Designed to prevent multiple people from entering with one swipe of a card A user enters through the outer door. The door locks behind him. Once the door locks, the user is "trapped" between the two doors. Inside, the user must swipe an access card, and/or enter biometrics. The inner door then unlocks and the user is allowed to proceed.
Badge Reader 	A user must wave a proximity card or swipe a magnetic card to gain access to a room. A badge reader can also be integrated onto a printer to allow secure printing Access badges are better than keys because they can be revoked if lost or stolen. They can contain the photograph of the user. They can also be used to record and monitor when a user accesses a room or building.

Smart Card acs ACOS5-64 FIPS Certified PKI FIPS 140-2 Cryptographic Smart Card	Contains a cryptographic chip, which may contain biometric data The smart card allows access to a computer and/or a physical resource
Security Guard 	Provides physical access Security guard can stop people he doesn't recognize (for example a person trying to use a stolen key or stolen access card) Security guards cost money and can be distracted Security guard can provide temporary access to people who forgot or lost their keys, and are subject to social engineering
Door Locks 	Door locks provide physical security to doors Door locks can be picked If a user loses the keys, all keys and door locks using that key must be replaced

Biometric Lock 	Typically integrated with a badge reader Provides access in response to positive identification with retina, fingerprint, palm print, or other unique identifier
Hardware Token 	Provides a one-time password that changes every 30 seconds or every 60 seconds Token is synchronized with a server Token can be integrated into an app
Cable Lock 	Allows an electronic to be physically secured to a desk or piece of furniture Many electronics have ports for cable locks Can be easily cut

USB Lock 	Allows you to lock USB ports Either lock a USB port so that nothing can be inserted or lock a USB port so that nothing can be removed Prevents unauthorized copying of data
Privacy Screen 	A privacy screen prevents people from viewing the screen if they are looking at it from a different angle
Key Fob 	Similar to an access card, but does not contain a photograph Allows a user to access a room or resource by scanning the fob

Entry Control Roster 	A list of people who are permitted access Managed by a security guard who checks people against the list

2.2 Explain logical security concepts.

- *Active Directory*
  - *Login script*
  - *Domain*
  - *Group Policy/Updates*
  - *Organizational Units*
  - *Home Folder*
  - *Folder redirection*
- *Software tokens*
- *MDM policies*
- *Port security*
- *MAC address filtering*
- *Certificates*
- *Antivirus/Anti-malware*
- *Firewalls*
- *User authentication/strong passwords*
- *Multifactor authentication*
- *Directory permissions*
- *VPN*
- *DLP*
- *Access control lists*
- *Smart card*
- *Email filtering*
- *Trusted/untrusted software sources*
- *Principle of least privilege*

Active Directory	Login Script – a login script is a script that automatically runs when a user logs in (it could perform tasks such as mapping network drives, setting a default printer, or running specific programs) Domain – a domain authenticates users and ensures that they have permission to log in Group Policy/Updates – group policy controls what a user can and can't do. For example, group policy can block access to specific programs, force a computer to connect to a specific Wi-Fi network, or prohibit users from installing applications Organizational Units – computers and users can be assigned to organizational units. Each organizational unit may have multiple organizations. For example, an organization may have Accounting, Engineering, Management, and HR, each of which has different permissions and settings. Home Folder – a home folder contains the user's personal files (Documents, Desktop, Music, Photos, and Videos). Some policies prevent users from saving files anywhere except in the home folder. A user can only access files in his own home folder. Folder Redirection – allows you to redirect the "local path" of a folder to a network location.

	This allows/forces users to save files to a network location instead of the local computer.
Software Token	A software token is used in multi-factor authentication A software token is an app that generates a password (typically a six-digit code). A new code is regenerated every 30 or 60 seconds. The software token syncs with the login server When a user logs in, they must enter their username, password, and the token. The token prevents unauthorized users from logging in, even if they have the username and password, because they won't be able to guess the current token code.
MDM Policy	Mobile Device Management Software that is installed on mobile devices (phones and tablets). It allows an administrator to mange mobile devices (features include the ability to erase a lost or stolen device, preventing users from installing applications or changing settings)
Port Security/MAC Address Filtering	On a managed network switch, it is possible to turn off ports that are not in use. It is also possible to limit traffic to specific MAC addresses on a port-by-port basis.

	For example, if a device with MAC address 00:11:22:33:44 is connected to port 6 on a switch, the switch port security can be configured to allow traffic from only that device. If a device with a different MAC address is connected, the switch can allow the traffic, block the traffic, or completely disable the port. If the switch port is connected to another switch, it will see traffic from multiple MAC addresses (multiple devices will be connected to the second switch). A switch port can be configured to allow traffic from a limited number of unique MAC addresses. For example, a switch port can be set to allow traffic from six unique MAC addresses. If the switch receives traffic from seven unique MAC addresses on a particular port, it will turn off the port.
Certificates	A certificate is used to verify the identity of a user. A certificate should be issued by a Certificate Authority (a company that is trusted to issue certificates). A Certificate Authority signs the certificate with its own certificate, proving its validity. Most computers are configured to trust Certificate Authorities by default. A computer or a user will present a certificate when connecting to another computer. The

	computer receiving the certificate will validate its authenticity.
Antivirus/Anti-Malware	Antivirus programs block viruses, malware, spyware, adware, phishing scams, inappropriate websites, and other harmful content Antivirus programs automatically track user activities such as downloaded files, USB drive insertions, and e-mails received. Antivirus programs automatically scan these activities for viruses. An antivirus program keeps track of known viruses through definitions (a definition is a file size or characteristic that identifies a particular virus). An antivirus program also detects viruses through heuristics (a heuristic is a pattern or behavior that makes it likely that a file is a virus). An antivirus program may fail to detect a virus if the virus doesn't match a definition or heuristic.
Firewall	A firewall restricts network traffic based on specific rules Rules can include whether the traffic is inbound or outbound, the source/destination, the port number, and/or the application

User Authentication/Strong Passwords	Users are encouraged to choose strong passwords An administrator can set different password rules, including • Number of characters • Presence of special characters, capitals, and/or numbers • Not including name, common words, or other information in the password • Forcing a user to change their password regularly
Multi-Factor Authentication	Requires a user to authenticate with more than just their username/password Can include a software token, a smart card, and/or a biometric (retinal scan, fingerprint, face, voice, etc.)
Directory Permissions	Directory permissions prevent users from accessing folders that they don't have permission to view Typically applied to network shared folders The server hosting the network folder is on a domain An administrator or the folder owner can add/remove permissions to specific users or groups of users

VPN	A Virtual Private Network allows users to connect to the corporate network over the internet A VPN creates a tunnel back to the corporate network and routes the traffic there
DLP	Data Leak Prevention Prevents data leaks Typically installed as a network appliance or software application Scans outgoing traffic for sensitive data (can be predefined specific data or patterns) Blocks traffic that appears to be sensitive. Can quarantine suspicious traffic for review by an administrator (who can choose to allow or block the traffic) If the DLP is installed on end user computers, it may be configured to prevent users from copying files onto USB keys or printing sensitive documents
Access Control List	Can be applied to files and to network equipment A file Access Control List lists the users who are permitted to access the file (including their level of permission). A user might have read-only

	access (can view the file but not edit) or write access (can read and edit the file)
Smart Card	A smart card is a credit card-sized card which contains a microchip A user inserts the smart card into a card reader in order to authenticate himself with the server A smart card prevents an unauthorized user from logging in, even if he has the username and password
E-mail Filtering	E-mail filtering can block • SPAM • Viruses • Phishing e-mails • Attachments The e-mail filter can be installed on each user's computer or on the e-mail server Cloud e-mail services such as Microsoft Office 365 and Google Apps have e-mail filters enabled by default
Trusted/Untrusted Software Sources	Most enterprise software applications are digitally signed by their manufacturer. When installing a software program, Windows will verify the validity of the digital signature. It's possible to set Windows to install programs only if they are digitally signed.

	Many software programs created by small publishers are not digitally signed
Principle of Least Privilege	Provide users with only the minimum privilege/access they require to perform their jobs A user who has access to many resources may be tempted to explore or make changes. A user who is disgruntled may log in and damage or delete files. A user may have his login/password stolen. An unauthorized user could use the login/password to steal data or cause damage.

2.3 Compare and contrast wireless security protocols and authentication methods.

- *Protocols and encryption*
  - *WEP*
  - *WPA*
  - *WPA2*
  - *TKIP*
  - *AES*
- *Authentication*
  - *Single-factor*
  - *Multifactor*
  - *RADIUS*
  - *TACACS*

Protocols and Encryption

- When connecting to Wi-Fi, you must use a protocol and an algorithm
- The protocol is the way that the computer and access point exchange data
    - Includes WEP, WPA, WPA2
- The algorithm is the equation that the computer and access point use to encrypt/decrypt traffic
    - Includes TKIP and AES
- You must a combination of the protocol and the algorithm, for example WEP with TKIP or WPA2 with AES

WEP	Wired Equivalent Privacy WEP keys protect wireless networks When connecting, the user is prompted to enter the WEP key Considered weak and shouldn't be used Can be cracked in less than one minute
WPA	Wi-Fi Protected Access When WEP was cracked, the Wi-Fi Alliance quickly developed WPA to protect Wi-Fi networks until a better solution could be implemented
WPA2	Wi-Fi Protected Access 2 Current Wi-Fi encryption protocol When connecting, the user is prompted to enter the WPA key The computer and the access point use the WPA key to generate a new key The new key is used to encrypt traffic between the computer and access point Being replaced by WPA3

TKIP	Temporal Key Integrity Protocol Developed in 2004 as a temporary replacement to WEP Considered weak and easily broken Current standards say that it should not be used, but many Wi-Fi devices still use it
AES	Advanced Encryption Standard Current encryption standard in use

Authentication

Single-Factor	Requires a user to enter a password and/or a username/password
Multi-Factor	Requires a user to enter "something else" in addition to the username/password, which could include • Software token • Biometric • Smart Card
RADIUS	Remote Authentication Dial-In User Service (RADIUS) A RADIUS server provides authentication, authorization, and accounting to remote users Authentication: verifies the identity of the remote user Authorization: determines whether the remote user is permitted to connect Accounting: keeps track of when the user connected to the network A user can use one username/password to connect to multiple resources
TACACS	Terminal Access Controller Access Control System

	Forwards a user’s username/password to an authentication server to determine if access should be permitted/denied

2.4 Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

- *Malware*
  - *Ransomware*
  - *Trojan*
  - *Keylogger*
  - *Rootkit*
  - *Virus*
  - *Botnet*
  - *Worm*
  - *Spyware*
- *Tools and methods*
  - *Antivirus*
  - *Anti-malware*
  - *Recovery console*
  - *Backup/restore*
  - *End user education*
  - *Software firewalls*
  - *SecureDNS*

Malware Types – Ransomware

Ransomware is a type of virus that encrypts the user's sensitive files.

- Ransomware enters through e-mail attachments
- Typically, ransomware encrypts documents and photos
  - The computer continues to function, but the documents and photos become inaccessible
- A user will be prompted with a message that the files are encrypted
- The user is instructed to pay a "ransom" to the hacker
- The ransom is paid in bitcoins (which are untraceable)
- Upon payment, the user receives a tool to decrypt the files
- Removal
  - Some versions of ransomware use weak encryption that can be broken without paying the ransom
  - Some versions of ransomware are released by hackers who have no intention of providing a method for decrypting the files
  - Paying the ransom has a 0% to 100% chance of success
- Users may be targeted specifically; hospitals, educational institutions, and large businesses are often required to pay a larger ransom than other users

Malware Types – Trojan

- A trojan is a type of malware that creates a “backdoor” for a hacker to enter
- The trojan doesn’t create any damage, but allows the hacker to steal files or spy on information
- Trojans enter through security flaws in Windows

Malware Types – Keylogger

- A keylogger records the keystrokes entered by a user
- A keylogger may also take screenshots of the user's computer
- A keylogger might be installed by a private investigator, police department (in connection with an investigation), a jealous lover, or an employer
- A keylogger is usually installed through a security flaw
- The hacker uses the key's logged to
  - Spy on the user
  - Capture usernames/passwords for bank accounts and other online accounts
  - Blackmail the user
  - Further an investigation
  - Detect unauthorized activity
- A keylogger might be legal if installed on a work or public computer and if the user has consented to it, or if permitted by court order

Malware Types – Rootkit

- A rootkit allows another program or user to obtain privileged/elevated/admin access to a computer
- A rootkit allows the other program (known as the payload) to remain undetected
- A rootkit replaces code in the operating system files, which allows it to bypass system security, or pretends to be a legitimate system process
- Rootkit detection
    - A rootkit can hide its presence while running, which makes it difficult to detect
    - It is possible to detect a rootkit by booting to a clean version of Windows from a DVD/USB, and then checking critical operating system files for changes
    - Generate cryptographic signatures of critical operating system files during installation and compare them to see if there are changes
- Rootkits can enter
    - Through security flaws
    - As trojans
    - Disguised as legitimate applications
- Rootkits can have legitimate purposes
    - An antivirus program can run as a rootkit to prevent viruses from damaging it
    - Bypass copyright protection/DRM

Malware Types – Virus

A virus is a program that attaches itself to other legitimate files; a virus can't operate by itself

- When the legitimate file runs, the virus executes with it
- Viruses spread through e-mail, USB keys, and security flaws in Windows
- A virus may attach itself to a Microsoft Office document
- The type of damage that a virus causes can vary (a virus may cause substantial damage or just be annoying)
  - A virus may remain dormant (not cause any damage) for a period of time, before being triggered (causing substantial damage)
- A virus might spread to other computers
  - Attaching itself to e-mails
  - Copying itself to USB drives inserted in the computer
  - Copying itself to other computers on the network
- Advanced viruses can encrypt themselves or change their code each time they are copied (if the virus changes its code, it can't be detected by an antivirus program that is looking for specific code patterns)
- A virus could infect the BIOS or other computer firmware, which can't be erased even if the hard drive is erased or replaced

Malware Types – Botnet

A botnet is a group of computers that are under control by another user

- Also known as zombie computers
- A hacker will infect a computer with a virus that allows him to take remote control over it
- When the hacker has infected many computers, he is now in control of a botnet
- Computers in the botnet won't know that they're infected, and usually won't experience any issues
- The owner of the botnet will rent the botnet to a person who wants to do something illegal
- Recently, botnet software has been used to infect IoT devices including cameras and appliances
- Botnets are typically used to launch denial of service attacks
  - Each computer in the botnet is ordered to send traffic to a website or server
  - The website's servers become overloaded with traffic and crashe
  - Since the traffic originates from many thousands of different computers, it appears to be legitimate and can't be blocked
- Other uses of botnets
  - Bitcoin mining (computers in the botnet are used to mine bitcoins)
  - Click fraud (computers in the botnet are used to automatically click on advertisements; the botnet is run by a person who profits from the clicks)
  - E-mail SPAM (the botnet is used to send unwanted e-mails)

Malware Types – Worm

- A worm is like a virus
    - It is unauthorized and enters a computer through a security flaw
    - It attempts to spread to other computers, especially though a network
    - It may cause harm or just be annoying
- A worm runs by itself (it does not infect other files)

Malware Types – Spyware

- Spyware tracks user activity
- Enters through security flaws in Windows or Internet Explorer
- Can contain a keylogger or other tools to capture files, screenshots, video from the webcam, and audio from the microphone
- Spyware can be installed by the government, employers, or malicious people
- Spyware can infect mobile devices such as phone and tablets

Tools and Methods – Antivirus

An antivirus program detects and removes viruses

- Can be a program that is installed permanently and runs in the background, or can be a "one-time use" program that is designed to detect and remove one specific virus
- Antivirus programs detect viruses by monitoring user behavior and file downloads
- Most antivirus programs are sold on a yearly subscription (must renew the subscription to continue protection)
- Antivirus program can include other features such as
    - Web filter
    - SPAM filter
    - Firewall
    - Data backup
- Detection methods
    - Virus definition
        - Antivirus program has a list of virus definitions (keywords, file sizes, and file signatures)
        - The program compares files against the list
        - If it detects a match, it knows that it has found a specific virus
        - Viruses without definitions can't be detected this way
    - Heuristics
        - Antivirus program has a list of rules that indicate the presence of a virus
        - If a program or file's behavior matches one of the rules, then program considers it to be a virus
        - Can lead to false positives (detecting a legitimate program as a virus)
        - Some viruses can adapt to avoid behaviors that could get them detected
    - Cloud detection
        - Antivirus programs send suspicious files back to a cloud service for further analysis
        - If the analysis determines that the file is a virus, a definition is created
        - Antivirus programs will download the updated definitions

        - Cloud detection allows many computers to work together

- There is a delay between the release of a virus and its detection
    - Viruses are becoming more advanced
    - When a new virus is created, it's impossible to detect
    - It appears to behave as a legitimate program
    - Antivirus programs don't have updated heuristics or definitions to detect the virus
    - After a few hours or days, the antivirus manufacturer begins receiving reports about the virus and creates updated definitions
    - Antivirus programs download the updated definitions and begin detecting the virus

Tools and Methods – Anti-Malware

Anti-malware programs are like anti-virus programs, but able to detect additional types of malware (such as trojans, keyloggers, and spyware)

- Most antivirus programs are actually anti-malware programs

Tools and Methods – Recovery Console

Remove malware by reverting to a previous point in time

- It’s possible to remove malware by using System Restore to go back to a time when the malware was not installed
- Not guaranteed to work because the virus may infect the recovery partition, or infect documents and/or files that are not part of the restore image

Tools and Methods – Backup/Restore

- It’s important to keep regular back ups in case of fires, floods, etc.
- There is no guarantee that an antivirus program will remove a virus
- Remove malware by erasing the computer and restoring from back up
    - Erase the computer
    - Reinstall Windows/other operating system
    - Reinstall programs and reapply settings
    - Copy documents back to the computer from the back up
        - Make sure that the back up doesn’t contain the virus

Tools and Methods – End User Education

The best way to prevent malware is to educate end users, especially for viruses that can’t be detected

- Don’t open suspicious e-mail attachments
- Don’t visit websites that are inappropriate or untrusted
- Don’t insert USB devices unless you trust their source
- Don’t install programs from untrusted publishers
- Don’t leave your computer unlocked
- Back up your data regularly
- Download updates regularly

Tools and Methods – Software Firewall

- A firewall can block unauthorized traffic from entering the network
- A firewall won't block
  - An e-mail attachment containing a virus
  - A security flaw in an operating system
  - Malicious content that is encrypted
- A firewall might detect/block
  - A hacker trying to connect to a computer via an unsecure protocol, on a specific port
  - A piece of spyware connecting to an external server

Tools and Methods – SecureDNS

- Remember that DNS converts a hostname (easy for humans to remember) to an IP address (easy for computers to locate)
- A hacker can hijack the DNS and provide the wrong information to computers making DNS requests
- Users can be redirected to servers set up to distribute malware (instead of legitimate websites)
- For example
  - If google.com is located at 8.8.8.8
  - A legitimate DNS will tell users that google.com is located at 8.8.8.8, which is where computers will visit
  - The hacker will set up a server with the IP address of 9.9.9.9
  - On the server is a fake website that might capture logins or other information (the hacker will set it up to look like google.com)
  - The hijacked DNS will tell computers that google.com is located at 9.9.9.9
  - People will visit the fake google.com and enter their login/password, which will be captured by the hacker
- This can be avoided
  - Enforce https security on website traffic (check the website to make sure that it is https and uses an extended validation certificate to ensure that it is legitimate)
  - Look up DNS records from authoritative servers (servers that hold the original DNS records, not copies)
  - Connect to DNS via a secure connection

2.5 Compare and contrast social engineering, threats, and vulnerabilities.

- *Social engineering*
  - *Phishing*
  - *Spear phishing*
  - *Impersonation*
  - *Shoulder surfing*
  - *Tailgating*
  - *Dumpster diving*
- *DDoS*
- *DoS*
- *Zero-day*
- *Man-in-the-middle*
- *Brute force*
- *Dictionary*
- *Rainbow table*
- *Spoofing*
- *Non-compliant systems*
- *Zombie*

Social Engineering

Phishing	Phishing is a malicious attempt to obtain your login credentials A hacker will set up a website that appears to look legitimate (could be for an online service such as e-mail or a bank) The hacker will send a link to the website, via e-mail, to thousands or millions of people, who will attempt to log in The e-mail might contain a threat (for example that the account will be locked out if the user doesn't respond) The hacker will capture the credentials and later use them to break into the users' online accounts A phishing website is usually easy to detect, if you're an expert. It will have • The wrong domain name • Lack of an extended validation certificate • Possible spelling mistakes Phishing attempts sent to thousands of people are usually detected. Once somebody reports the phishing attempt, authorities will shut down the website. But it can be difficult to identify and warn users who accessed the site.

Spear Phishing	Spear Phishing is the same as phishing, except that it targets a specific company or person. The hacker will research the company, its users, and its policies, to devise an e-mail or scenario that tricks a person into handing over their credentials. Spear Phishing can use • A person pretending to be from the IT, HR, or accounting department • A website disguised as a legitimate company website Spear Phishing can be detected by instituting strong controls and educating users. Users should know not to give their usernames/passwords to others, regardless of who they are.
Impersonation	Impersonating is the act of pretending to be somebody else. A hacker could attempt to obtain access to an account by calling the service provider (e-mail provider, bank, credit card company, or other resource) and pretending that he lost his password The service provider will ask the hacker some security questions, and if the hacker guesses correctly, he will be provided access. Impersonation can be prevented by setting up

	• Difficult security questions • Two-factor authentication • Alerts (sent via SMS and e-mail) when somebody logs in to your online account or attempts to changes your password
Shoulder Surfing	A hacker will look over your shoulder when you are accessing sensitive data, and observe you typing in your username/password A hacker doesn't have to be physically present (it's possible to shoulder surf by viewing surveillance camera footage, and due to security vulnerabilities, many security cameras are accessible over the internet) Difficult to detect shoulder surfing Prevent shoulder surfing • Install a privacy screen over your laptop • Don't access sensitive resources in public places
Tailgating	If a door is protected by an access card reader or a lock, each person who enters must swipe their card or unlock the door. A hacker who does not have a key or a keycard will attempt to enter by following somebody else in.

	Can be prevented by requiring every person who enters to swipe their card and/or by installing man trap doors. Institute a policy to ensure that each person swipes their card when they enter.
Dumpster Diving	A hacker will dig through a garbage can to find sensitive documents and files. A hacker can find sensitive data on USB drives, DVDs, and hard drives that are not properly disposed of. Can be prevented by shredding sensitive documents

DOS – Denial of Service

Flood a host with requests

- For example, if we wanted to bring down ebay.com, we would set up a server and send as much traffic as possible to ebay.com (open millions of ebay.com browser tabs for example)
- This requires a lot of computing power and bandwidth (can be very expensive)
- It's easy for eBay to stop us; they would just block our IP address
- A smaller website might not be able to react fast enough to stop our attack

DDOS – Distributed Denial of Service

Improved version of DOS

- We flood ebay.com with traffic from thousands or hundreds of thousands of different computers
- eBay can’t keep up with the traffic and shuts down
- Legitimate visitors can’t access the site
- eBay can’t block us because the traffic comes from thousands of different sources; they’re unable to distinguish between legitimate and malicious traffic
- We use a botnet to create the DDOS attack
    - Infect thousands of computers
    - Take control of the computers
    - Use the computers to send traffic to eBay

Zero-day

- A zero-day vulnerability is a security hole in a software program that isn't known to the general public
- The manufacturer doesn't know about it, therefore, no patch is available
- Some hackers might know about it, and might be using it to their advantage
- As soon as it's discovered or disclosed to the public, it becomes a zero-day vulnerability
- Manufacturers will work to make a patch as soon as they are aware of the issue

Man-In-The-Middle

- In secure internet communications, we use public key cryptography
- How does it work?
  - Let’s say Alice and Bob are two computers
  - If Alice wants to receive messages from Bob, she would create a public key and a private key
  - The private key is created first and used to generate the public key
  - She publishes the public key and keeps the private key a secret (to herself)
  - The public key can be used to encrypt messages and the private key can be used to decrypt messages
  - Bob looks up the Alice’s public key, writes a message and encrypts it with Alice’s public key
  - Bob sends the encrypted message to Alice
  - Alice uses the private key to decrypt the message
- The Man-In-The Middle
  - Public keys are sometimes stored in a directory known as a key server (such as Apple iMessage)
  - If Eve wants to eavesdrop on Bob and Alice, she can create her own public and private keys
  - She sits in the middle of Bob and Alice (on the key server)
  - If she has control over the key server, she would give Bob her own public key (and pretend that it was Alice’s public key)
  - Bob would encrypt the message using Eve’s public key
  - Eve intercepts the message and decrypts it using her private key, reads the message, encrypts the message with Alice’s public key, and sends it to Alice
  - Alice decrypts the message with her private key
  - Neither Bob nor Alice find out that Eve is in the middle

Brute Force

- Brute Force is a method of guessing a user’s password
- We try one password at a time until we get in
- We try every possible combination of letters, numbers, and special characters, even in combinations that make no sense
  - Another possibility is to guess common passwords first
- Brute force is not practical when the passwords are long or complicated
  - It could take years to guess the correct password, even with a powerful computer
- A program might lock you out after several incorrect password attempts

Dictionary Attack

- Dictionary Attack is a method of guessing a user’s password
- We create a list of common passwords and try those
- This is more effective than brute force, but could still take a long time
- A good software program will have a limit to the number of passwords we can try

Rainbow Table

- It is a good security practice to not store user passwords in plain text
- Instead, we hash the passwords
  - When the account is created, the password is converted into a hash through a one-way mathematical function, which is stored in a database
  - It's not possible to convert the hash back to the password
  - When a user attempts to log in
    - The program hashes the password he entered
    - The program compares the hash it just created with the one on the database to determine if the password is correct
  - If the password database is compromised, the passwords themselves are not leaked
- To break a hashed password, we can create a "rainbow table"
  - We create a dictionary of passwords and hash each one
  - We now have a table of hashes and corresponding passwords
  - If we steal a table full of hashed passwords, we can compare the hashes against the rainbow table and figure out what the passwords were
  - Attacks through rainbow tables can be prevented by adding a "salt" to the password before hashing it
    - A salt is a set of random characters
    - It prevents the rainbow table from guessing the password (a hacker would have to generate a rainbow table for each password and salt combination, which would take a long time)

Spoofing

- A hacker can impersonate another device or user
- Several things can be spoofed
    - An IP address
        - The hacker sets his computer to have the same IP address as a legitimate computer
        - This creates an IP conflict and could force the legitimate computer off the network
        - Only works if the hacker's computer is on the same subnet
    - MAC address
        - On some network card's it's possible to change the MAC address
        - A hacker can change the MAC address and access Wi-Fi networks and other resources that use MAC address authentication
    - E-mail address
        - A hacker can change the e-mail header to make his e-mails appear to be coming from legitimate senders
        - If a user replies to the e-mail, the reply will go to the legitimate account holder, but the hacker can insert links to phishing websites or malicious content
        - It's possible to detect spoofed e-mail addresses by comparing the server from where the e-mail originated

Zombie

- A zombie is a computer that was taken over by a botnet

2.6 Compare and contrast the differences of basic Microsoft Windows OS security settings.

- *User and groups*
  - *Administrator*
  - *Power user*
  - *Guest*
  - *Standard user*
- *NTFS vs. share permissions*
  - *Allow vs. deny*
  - *Moving vs. copying folders and files*
  - *File attributes*
- *Shared files and folders*
  - *Administrative shares vs. local shares*
  - *Permission propagation*
  - *Inheritance*
- *System files and folders*
- *User authentication*
  - *Single sign-on*
- *Run as administrator vs. standard user*
- *BitLocker*
- *BitLocker To Go*
- *EFS*

User and Groups

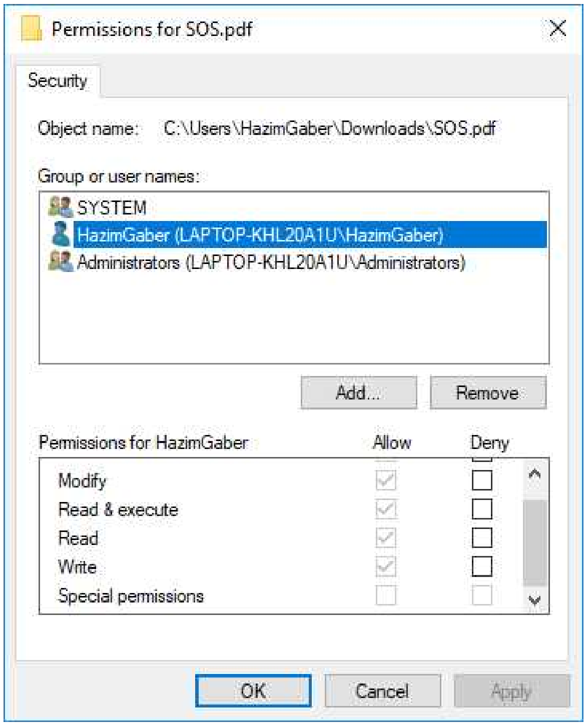
A user account can be assigned to a group.

- The user account inherits the privileges assigned to the group
- It is possible to create multiple account groups

Administrator	Also known as a Superuser There can be multiple admin accounts, and there can be a hierarchy of admin accounts On a local Windows computer, there must be at least one admin account Ad admin account • Can create other accounts • Install programs • Change settings • View files (documents, desktop, etc.) belonging to all users A program must ask for permission when it attempts to run with admin privileges
Power User	A Power User is more powerful than a Standard User, but less than and admin Power User accounts should be granted to more experienced users only Power User accounts were present in Windows XP and then removed

Standard user	A Standard User can log in, run programs, edit files, and perform general tasks A Standard User can't • Create other user accounts • Install programs • Change advanced system settings • View files (desktop, documents, etc.) that belong to other users If the account is an Active Directory account, more granular permissions are available (can restrict the account from modifying specific settings)
Guest	Not assigned to a specific person Disabled by default Allows anybody to access the computer without a password A Guest account can't • Store data • Create other user accounts • Install programs • Change advanced system settings • View files (desktop, documents, etc.) that belong to other users

NTFS Permissions

Allow vs Deny	A folder or file will inherit permissions from the folder that it is in For example C:\folder1\folder2 will inherit permissions from C:\folder1 A sub-folder will stop inheriting permissions if different permissions are set on it In the folder security tab, you can set “allow” permissions and “deny” permissions for the ability to modify, read, read & execute, or write A deny permission will override an allow permission.  Permissions for SOS.pdf Security Add... Remove OK Cancel Apply Object name: C:\Users\HazimGaber\Downloads\SOS.pdf Group or user names: SYSTEM HazimGaber (LAPTOP-KHL20A1U\HazimGaber) Administrators (LAPTOP-KHL20A1U\Administrators) Permissions for HazimGaber — Allow — Deny Modify ☑ ☐ Read & execute ☑ ☐ Read ☑ ☐ Write ☑ ☐ Special permissions ☐ ☐ Why do we need both allow and deny?

	It's possible to give permission to a user or to a group of users. We can then go back and override the permissions. For example, we don't want the Accountants group to have access to "Folder1". We would add Accountants and check the Deny boxes. But Bob is an Accountant and we want to provide him with access. We would add Bob and check the Allow boxes (the Allow overrides). For example, we want the Engineers group to have access to "Folder1". We would add Engineers and check the Allow boxes. But John is an Engineer and we don't want to provide him with access. We would add John and check the Deny boxes (the Deny overrides).
Moving vs Copying files and folders	When you move a protected file or folder, it retains the current permissions. When you copy a protected file or folder, it inherits the permissions from the folder that you copied it into.
File Attributes	The standard NTFS file attributes are • File name • Security descriptor (who owns the file and who can access it) • Object ID (unique file ID) • Data (other unique file attributes)

	- Standard Information (date and time stamp)

Shared Files & Folders

An administrative share is a hidden network share that allows an administrator to remotely access all disk volumes on network computers

How to access an administrative share?

- Navigate to the computer via its network hostname
- Access the volume with the drive letter followed by an $
- For example, if we want to access the C drive on a computer called somecomputer, we would type \\somecomputer\C$
- We can also access printers connected to the computer

An administrative share can be disabled but not deleted

A local share is a network share set up by the local computer

- The local user must manually set up the shared file or folder
- The local user must manually enable network sharing
- Local shares can be disabled or deleted

Like NTFS permissions, when a share is set up, permissions can be granted

The permissions are

- Read
  - Can view the file
  - This is the default permission
- Change
  - Can read and change the file
- Full Control
  - Can also change permissions
  - Administrators have full control

If a file has share permissions, and NTFS permissions, the most restrictive set of permissions applies

User Authentication / SSO

There are several ways for a user to authenticate

- Local user account (username/password are stored on the local computer; local computer checks if credentials are valid)
- Active Directory (username/password are stored on server; server checks if credentials are valid)
- Third Party Authentication (username/password are stored on third party/cloud service; service checks if credentials are valid)

Single Sign On (SSO)

- Convenient tool for allowing user to enter username/password only once, and access many resources
- In a large organization, a user may require access to multiple applications and resources, each of which requires a username/password
  - For example
    - Computer login
    - Printers
    - Shared Folders
    - Web apps
    - HR software
    - Scheduling software
    - E-mail
    - SharePoint
  - It's easier to have all the different resources authenticate with one central authentication server
  - This allows the organization to create one account for the user instead of multiple accounts
- The user will become frustrated if he must enter his username/password for each application
- Single Sign On
  - When the user logs in to the computer, SSO authenticates the user with all the different applications through a token

- The user only needs to log in once
- Works with LDAP (Lightweight Directory Access Protocol)

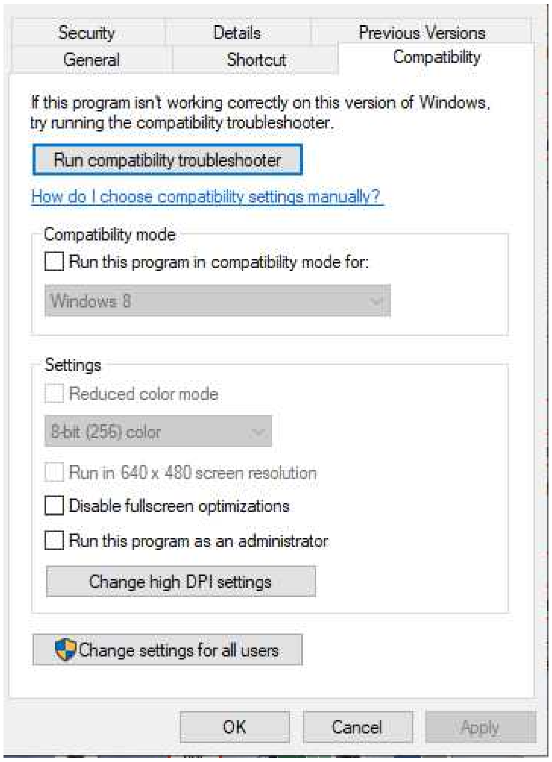
Run as Administrator vs Standard User

On older versions of Windows (such as Windows XP), when you run an application, it will run at the level of the user

- If the user is an admin, the app will run with admin privileges
- If the user is a standard user, the app will run with standard privileges

Allowing all applications to run with admin privileges is a bad idea

- Some applications require admin privileges to run
- They might need to save files to protected directories and/or modify settings
- On newer versions of Windows, UAC (User Access Control) will prompt the user if the app requires admin privileges
- It's possible to run an app with admin privileges once, or by default by checking the box (in properties -: Run this program as an administrator)


Security
Details
Previous Versions
General
Shortcut
Compatibility

If this program isn't working correctly on this version of Windows, try running the compatibility troubleshooter.

Run compatibility troubleshooter
How do I choose compatibility settings manually?

Compatibility mode

□ Run this program in compatibility mode for:

Windows 8

Settings

□ Reduced color mode

8-bit (256) color

□ Run in 640 x 480 screen resolution

□ Disable fullscreen optimizations

□ Run this program as an administrator

Change high DPI settings
Change settings for all users
OK
Cancel
Apply

BitLocker

BitLocker is an encryption protocol built into Windows Pro

Provides full-disk encryption.

If the computer contains a TPM, the encryption key is stored inside the TPM. The computer can load to Windows, but none of the additional files are decrypted until the user successfully logs in. Operating system data is stored in a separate partition.

Can store the encryption key in Active Directory.

If the computer does not contain a TPM, the computer will not load to Windows. A user must enter password when the computer boots. An encryption key could also be stored on a USB.

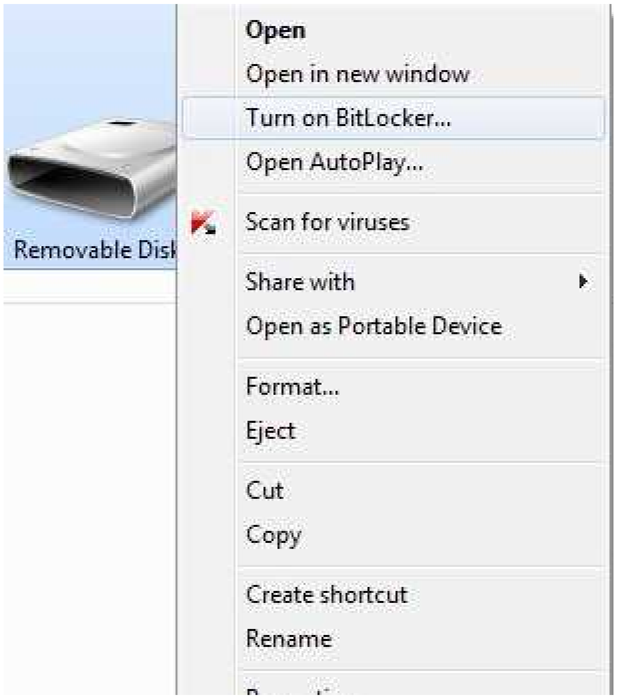
Possible to decrypt contents through a “cold boot” attack.

See the previous section on BitLocker for more details.

BitLocker To Go

BitLocker To Go allows you to encrypt removable drives, including USB drives and SD cards, which could use NTFS, FAT16, FAT32, or exFAT file systems.

When you insert un unencrypted removable drive into a Windows computer, you can select the “Turn on BitLocker” option and follow the steps to activate BitLocker



When you insert an encrypted removable drive into a Windows computer, Windows will automatically require you to enter the password in order to unlock it.

EFS

EFS is the Encrypting File System

Why do we need to encrypt the file system?

Normally, Windows provides / denies access to files based on user permissions and an access control list. If we take the hard disk out of the computer and plug it into an external reader, we can bypass Windows and read the files directly regardless of the permissions. This would be bad if the computer was stolen, because the thief could remove the hard drive and see all the files.

Therefore, we should encrypt each file. Doing so manually would be tedious, in fact, impossible, because Windows creates many temporary files, and a hard drive could contain over a million files.

In an Encrypting File System

- The system marks each folder for encryption in the metadata (encryption is inherited to files and subfolders)
- Each file is encrypted with a different key
- A private key is created and used to generate a public key
- All the file keys are encrypted with the public key
- The private key can only decrypt files and the public key can only encrypt files
- The private key is stored on the drive, but is encrypted with the user's password
- Encryption and decryption are handled transparently by the file system. That is, when Windows requests a file from the file system, the file system automatically decrypts and delivers it. When Windows stores a file, the file system automatically encrypts it.

Security Problems with EFS

- When you send a file over the network or move it to a portable drive, the file will remain decrypted
- In Windows 2000, the local admin account can decrypt all files by default. In future versions of Windows, this is not possible
- Windows XP and further versions of Windows store the private key on a password reset disk and in Active Directory (if the computer is connected to a domain)

- If the user forgets/resets his password, then the private key is lost forever (it is encrypted with the user’s password)
- If the user’s password is compromised, then all the files are compromised

2.7 Given a scenario, implement security best practices to secure a workstation.

- *Password best practices*
    - *Setting strong passwords*
    - *Password expiration*
    - *Screensaver required password*
    - *BIOS/UEFI passwords*
    - *Requiring passwords*
- *Account management*
    - *Restricting user permissions*
    - *Logon time restrictions*
    - *Disabling guest account*
    - *Failed attempts lockout*
    - *Timeout/screen lock*
    - *Change default admin user account/password*
    - *Basic Active Directory functions*
        - *Account creation*
        - *Account deletion*
        - *Password reset/unlock account*
        - *Disable account*
    - *Disable autorun*
    - *Data encryption*
    - *Patch/update management*

Password Best Practices

- Choose a strong password that includes
  - Numbers
  - Capital & lowercase letters
  - Special characters
- Choose a strong password that does not include
  - Your name, address, or other personal information
  - Common words such as “password” or “1234”
  - Previously used passwords
  - Passwords used in other locations/organizations
- Set passwords to expire after a specific time (30 days or 90 days)
  - The user will be required to change his password when it expires
- Set the computer to automatically lock the screen after a period of inactivity (such as 10 minutes)
  - Screensavers aren’t common
- BIOS/UEFI
  - Set a strong password for the BIOS
  - It is important to protect the BIOS because it contains settings for secure boot, boot sources, and the TPM
  - Unlike Windows passwords, the BIOS password can’t be managed centrally through Active Directory, although some BIOSs will lock the user out after several failed attempts
- Passwords should be required to access any computer resource

Account Management

- Restrict user permissions to only those that they specifically require
  - It may be easier to manager users in groups based on their roles in the organization
- Restrict logon times
  - A user can be restricted from logging in to a computer during certain times (for example evenings and weekends)
  - A cashier who has a specific shift can be restricted from logging in at another time for example
  - This is not always practical for employees who are workaholics, such as engineers and lawyers
- Disable guest account
  - Disable the guest account
  - The guest account allows users to log in without a username or password
- Failed attempts lockout
  - Lock the account after three failed attempts (automatically)
  - If the user enters an incorrect password after several attempts, the account is automatically locked
  - The administrator will unlock the account
- Screen lock
  - Lock the screen after a specific period of inactivity
  - If the user leaves the computer, it will automatically lock
- Change default admin account
  - Change the default admin account username and password so that it can't be guessed
  - The local admin account can be used to unlock the computer in circumstances where it loses connectivity to the domain controller; disabling the account even when the computer is on a domain may not be a good idea
  - Restrict what the default admin account can do
  - Change the default admin account for other devices such as modems, printers, and surveillance cameras
- Disable Autorun

    - Autorun allows Windows to automatically play/execute content from a USB drive, CD-ROM, or DVD as soon as you insert it
    - The content could be malicious if you don't know the source of the drive, CD-ROM or DVD
    - Disable autorun to prevent Windows from automatically executing the content
- Encryption
    - It's possible to make data encryption mandatory (for example require BitLocker to be enabled)
- Patch/Update Management
    - It's possible to require computers under management to automatically install Windows updates, and security updates for other applications

Basic Active Directory Functions

- Active Directory allows you to manage accounts centrally
- Active Directory can be connected to other services
- A large organization with many users and resources may use a script to generate accounts. A user may have an Active Directory account, an e-mail account, and other services, all of which can use the same login. The different services authenticate the user through the Active Directory server.
- Basic functions
    - Create a user account
        - Create the user account and add the user to one or more groups
        - Groups help you manage users by assigning different permissions to each group
    - Delete a user account
        - The account no longer exists, and the data is gone (or goes to a recycle bin)
    - Disable a user account
        - Locks the account so that the user can't log in
        - The user data remains in the account
    - Reset a user's password and/or unlock the account
        - Accounts can become locked automatically (for example if the user attempts to log in too many times incorrectly)
- Microsoft offers Azure Active Directory
    - Azure Active Directory is in the cloud and can be accessed through a web-based interface

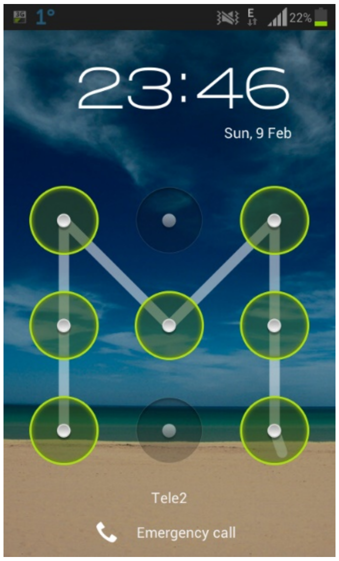
2.8 Given a scenario, implement methods for securing mobile devices.

- *Screen locks*
  - *Fingerprint lock*
  - *Face lock*
  - *Swipe lock*
  - *Passcode lock*
- *Remote wipes*
- *Locator applications*
- *Remote backup applications*
- *Failed login attempts restrictions*
- *Antivirus/Anti-malware*
- *Patching/OS updates*
- *Biometric authentication*
- *Full device encryption*
- *Multifactor authentication*
- *Authenticator applications*
- *Trusted sources vs. untrusted sources*
- *Firewalls*
- *Policies and procedures*
  - *BYOD vs. corporate-owned*
  - *Profile security requirements*

Mobile Device Screen Lock

There are several ways to secure a phone

- Fingerprint
  - A fingerprint scanner built into the phone is not as sophisticated as a fingerprint scanner used by an enterprise (for example at a military base)
  - Phone fingerprint scanners create a mathematical approximation (a summary) of the fingerprint. Many different fingerprints can generate the same approximation. Therefore, there is a 1 in 50,000 chance that the fingerprint can be broken.
  - Fingerprints (on phones) are less accurate than passwords.
  - That's why a phone might require a password instead of a fingerprint when rebooting or during other scenarios, or might require a password if the wrong fingerprint has been entered too many times
  - Some phones don't have fingerprint scanners
- Face Lock
  - Uses facial recognition
  - Face Lock is a new technology and its accuracy hasn't been established
  - It has been shown that it can be tricked
  - Allows you to unlock the phone just by looking at it
- Swipe Lock
  - Phone displays a grid of dots and you must connect the dots to unlock the phone
  - Effectively as accurate as a passcode, but may be easier to remember because the dots might form a meaningful shape



- Passcode Lock
    - Requires you to enter a passcode
    - Passcode can be 4-digits, 6-digits, or a longer alphanumeric password

Other Policies

Remote Wipe

- Allows an administrator to erase the content of the device remotely
- The phone must be connected to the internet for the remote wipe to work

Locator Applications

- Displays the location/GPS coordinates of the phone
- Can be integrated into a different App such as Google Apps or Norton Security
- If the phone is lost/stolen, you can use the locator app to find the last location of the phone
- Requires the phone to be connected to the internet and have location sharing enabled

Remote Backup Applications

- Backs up the content of the phone to the cloud automatically
- An application may back up specific content (for example Google Photos) or the entire phone

Failed Login Attempts Restrictions

- If the wrong password is entered multiple times, the phone is automatically erased
- The number of failed login attempts is typically 10, but the number of attempts can be configured by the user
- After a shorter number of failed login attempts (such as 5), the phone prevents additional log ins for a period of time. For example, after 5 failed login attempts, you can't enter another login for 30 minutes

Antivirus/Anti-malware

- Norton and other antivirus apps ere available for Android phones
- Blackberry phones have a built-in anti-malware program
- iOS phones don't have antivirus

Patching/OS Updates

- OS updates are released regularly for Android and iOS devices
- Updates provide additional features and fix security issues

- The updates typically download automatically and can be installed at the user's option
- Updates for apps are also made available by each app developer
    - An Android phone may automatically update Apps

Biometric Applications

- Allows a user to log in to their device through a fingerprint, facial recognition or other biometric (as previously mentioned)

Full Device Encryption

- Encrypts the contents of the device
- Enabled by default on newer Android and iOS devices
- If device encryption is not enabled, a hacker can bypass the lock screen password and access the data directly

Multifactor Authentication

- Requires a user to enter their username, password, and a one-time password
- The one-time password is automatically generated by an app or a key fob
- Even if a hacker can guess the username/password, they won't be able to log in
- Not common for mobile devices, but common for many web-based applications (such as banking apps, healthcare apps, etc.)

Authenticator Application

- Most common authenticator app is Google Authenticator
- Syncs with the server that you are trying to access
- Displays the one-time passcode, which you can copy or enter
- Can add multiple accounts to the app

Trusted Source vs Untrusted Source

- A trusted source is one that you trust (may allow data/applications to be accessed/installed)
    - Example might be a corporate server
    - May authenticate with a certificate that proves its identity

- An untrusted source is one that you don’t trust (don’t allow data/applications from an untrusted source to be accessed/installed)

Firewall

- Configure the firewall to prevent unauthorized access
- Firewalls are not common on mobile devices

Policies and Procedures

- BYOD vs Corporate-Owned
    - BYOD = Bring Your Own Device
        - A user can bring their own device to work and use it for work-related purposes
        - Advantages
            - Cheaper for the company, since they don’t have to supply/maintain mobile devices
            - User can use a device that he/she is comfortable with
            - User can carry one device instead of two (a personal and a corporate device)
        - Disadvantages
            - Many different devices will be in use and the company will have trouble supporting all of them
            - The user might be mixing personal and work data
            - Difficult to control the user devices or apply policies to them
    - Corporate-Owned
        - The company supplies all devices to the users
        - Advantages
            - Company has a limited number of different device models to support
            - Company can control the data/policies of each device
        - Disadvantages
            - Users will be required to use the devices supplied by the company
- Profile Security Requirements
    - Can enforce different requirements on a mobile device
    - Profile security is enforced by a mobile device management app/script
    - Examples of policies that can be applied
        - Password/lock screen/minimum password complexity
        - Remote wipe
        - Inability to install applications
        - Automatically install specific apps

- Connect only to specific Wi-Fi networks
- Enable/disable specific items such as the camera, location services, etc.

2.9 Given a scenario, implement appropriate data destruction and disposal methods.

- *Physical destruction*
  - *Shredder*
  - *Drill/hammer*
  - *Electromagnetic (Degaussing)*
  - *Incineration*
  - *Certificate of destruction*
- *Recycling or repurposing best practices*
  - *Low-level format vs. standard format*
  - *Overwrite*
  - *Drive wipe*

HDD Destruction

Shredder	Most expensive destruction method Guaranteed to destroy the drive and data, especially where the drive is solid state and/or contains a hybrid chip
Drill/Hammer	Can be used to smash the drive Can be messy and unsafe It's possible to recover data from flash memory chips (solid state and hybrid drives)
Electromagnetic (Degaussing)	Requires a special degausser Not guaranteed to work Will not work with non-magnetic drives (solid state drives) Drive can be reused after degaussing
Incineration	May cause pollution Can be complicated Guaranteed to destroy the drive and data, especially where the drive is solid state and/or contains a hybrid chip
Certificate of Destruction	Provide drives to third-party data destruction firm The firm will erase the data and provide a certificate of destruction Outsourcing the data destruction is not a good idea if the data is sensitive, because the third party may lose or leak the data

Recycling or Repurposing

Low-Level Format vs Standard Format	A low-level format erases all the data on the drive. The drive is overwritten with 0s, and the file system is recreated A standard format erases the partitions, and recreates the file system but does not affect the data. It's possible to use a data recovery tool and recover files.
Overwrite	Write 0's over all of the data on the hard disk drive Every bit is covered with a 0, which erases the data Can take several hours There are different erasing standards (some require three or five overwrite passes) A software program can overwrite the data and confirm that it was completed successfully
Drive Wipe	Send a command to the hard disk drive The hard drive will execute its own built-in erasing program and verify that it was completed successfully

2.10 Given a scenario, configure security on SOHO wireless and wired networks.

- *Wireless-specific*
  - *Changing default SSID*
  - *Setting encryption*
  - *Disabling SSID broadcast*
  - *Antenna and access point placement*
  - *Radio power levels*
  - *WPS*
- *Change default usernames and passwords*
- *Enable MAC filtering*
- *Assign static IP addresses*
- *Firewall settings*
- *Port forwarding/mapping*
- *Disabling ports*
- *Content filtering/parental controls*
- *Update firmware*
- *Physical security*

SOHO Wireless Security

- A typical ISP modem/router will have a default SSID
    - Change the SSID to something that people can't guess
- Set the Wi-Fi encryption to the highest available setting
    - Choose WPA2/WPA3 and AES if possible
- Disable the SSID broadcast
    - Your Wi-Fi network will appear as a "Hidden Network"
    - You must know what the SSID is in order to connect to it
- Antenna and access point placement
    - Install the access point in a secure location
    - Make sure that the antennas are pointed in the recommended direction (ensure best possible signal)
- Radio power levels
    - Adjust the radio power levels so that the Wi-Fi signal stops at the perimeter of the building
    - This prevents people outside the building from being able to access your network
    - Some access points don't allow you to adjust the power level
- WPS
    - Wireless Protected Setup
    - Allows you to connect a Wi-Fi device to the router by pressing a button on the router
        - The router and other device will sync
    - Disable WPS where possible

Other Security Procedures

- Change default username/password
    - A router/modem will have a default username/password
    - The username/password might be “admin” and “password” or “admin” and “admin”
    - The default username/password is written on a sticker affixed to the modem
    - You should change it so that users can’t access the setup page
- Set encryption
    - Encrypt all Wi-Fi traffic via WPA2 or similar (as mentioned earlier)
- Enable MAC filtering
    - Make a list of the MAC addresses of authorized devices
    - Block other devices from connecting to the Wi-Fi (if the MAC is not on the list)
    - Also block devices from connecting to the switch of the MAC does not match
- Assign Static IP
    - Assign Static IPs to shared resources such as servers, printers, scanners, and cameras
    - Allow other devices such as computers to connect over DHCP
- Firewall
    - Enable the firewall and configure as appropriate (see previous sections)
- Port Forwarding
    - Allows you to forward traffic from one external port to an internal port
    - Not recommended
    - Use a VPN where possible
- Disable Ports
    - Disable ports on a switch that are not in use
    - Can only be done on managed switches
    - This prevents people from plugging unauthorized devices into the switch
- Content Filtering/Parental Controls
    - Allows you to block harmful/malicious/inappropriate content
    - Performed at the router level or at the computer level
    - A router might not be able to accurately filter traffic
    - Filtering can be bypassed with a VPN
- Update Firmware

  - Update the firmware on all network devices and do so regularly
  - Cloud managed devices such as Meraki and Ubuquiti can automatically download the latest firmware from the cloud
  - Other devices may require you to manually download and update the firmware
- Physical Security
  - Enforce physical security on the network equipment
  - This may not be practical for a small office / home office

Part I 220-1002 3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot Microsoft Windows OS problems.

- Common symptoms
    - Slow performance
    - Limited connectivity
    - Failure to boot
    - No OS found
    - Application crashes
    - Blue screens
    - Black screens
    - Printing issues
    - Services fail to start
    - Slow bootup
    - Slow profile load
- Common solutions
    - Defragment the hard drive
    - Reboot
    - Kill tasks
    - Restart services
    - Update network settings
    - Reimage/reload OS
    - Roll back updates
    - Roll back devices drivers
    - Apply updates
    - Repair application
    - Update boot order
    - Disable Windows services/applications
    - Disable application startup

- Safe boot
- Rebuild Windows profiles

Common Symptoms

Note that we are only concerned with "software" causes in this section. Many issues can be caused by software or hardware.

Problem	Possible Cause	Possible Solution
Slow Performance	Why is the computer slow? Too many applications open? The hardware is not adequate for the activity? The HDD is fragmented (files are broken into multiple parts)	Reboot the computer; rebooting the computer will resolve many issues Find out if there are background tasks/services that are slowing the computer down and disable them Upgrade the computer hardware Run the disk defragmenter
Limited Connectivity	Limited connectivity is when the computer is not connected to the internet, but the computer does not report a disconnected ethernet cable The computer may be configured with a static IP when it requires DHCP, or configured with DHCP when it requires static The computer may have the wrong static IP settings	Configure the computer to have DHCP or static as appropriate Configure the correct static IP settings Disable the firewall if necessary

	A network firewall is blocking the computer The firewall on the computer is blocking traffic	
Failure to Boot	Computer may be booting from the wrong drive/boot source The OS is corrupted	Attempt to reboot again, because this issue resolves itself sometimes Make sure that you are booting from the correct drive Reimage the computer if other methods don’t work
No OS Found	Computer may be booting from the wrong drive/boot source The OS is corrupted	Attempt to reboot again, because this issue resolves itself sometimes Make sure that you are booting from the correct drive Reimage the computer
Application Crashes	Missing a driver or component Application file is corrupted New update is incompatible with application	Identify if there is an error message related to the application and install the correct driver/component Repair/reinstall the application Roll back to a previous update

Blue Screen	Look up the reason for the blue screen and then act as appropriate Can be caused by invalid drivers	A blue screen that does not reoccur can be ignored Update drivers/software
Black Screen	Computer will not boot	Check that the issue is not hardware related (monitor, graphics card, etc.) Reinstall operating system
Printing Issues	Incorrect printer driver installed Printer not configured correctly Printer IP address is not set correctly	Determine if the issue is with the printer not connecting, or the print quality is affected If the issue is with the print quality, check the printer (as described in previous sections) If it’s a network printer, check to see if the printer has the correct IP address set, and check if you can ping it/reach it from the computer. If not, set the correct IP address and make sure that the network is configured correctly Make sure that the correct driver is installed

Services Fail to Start	A specific service may rely on another service. This is known as a dependency Check that the failed service is not relying on another failed/offline service	Repair the windows installation/file Uninstall and reinstall the service, if it belongs to a specific application
Slow Bootup	Too many start up items Disk is defragmented	Delete unnecessary start up items Defragment the computer
Slow Profile Load	Disk is defragmented Profile has too much data or is corrupted	Defragment the disk Delete the profile and rebuild it

Common Solutions

Defragment Hard Drive	Applies to HDDs not SSDs A file may be fragmented (broken into pieces) and the pieces are scattered randomly throughout the drive). Thus, it takes longer for the computer to find the file (it must find multiple pieces and put them back together) Defragmenting makes the file continuous
Reboot	Rebooting the computer resolves many issues There can be many unnecessary programs occupying the memory, and they will close when the computer is rebooted
Kill Tasks	A task that has crashed can be killed Launch the Task Manager and end the task Killing the task could cause data to be lost
Restart Services	A service that has crashed or is not responding can be restarted Go to Services, find the service, and restart it
Update Network Settings	Limited connectivity can be resolved by updating network settings Set the network to static/DHCP as appropriate Set the static IP configuration
Reimage/Reload OS	Use this as a last resort Sometimes, the issue cannot be determined (random error messages, slow computer, etc.),

	in which case, reimaging the computer is the best approach
Roll Back Updates	A new update may not be compatible with the hardware/software and cause errors The update itself may have bugs Roll back the update to prior to when the errors occurred
Roll Back Device Drivers	A new driver may not be compatible with the hardware/software Roll back the driver to prior to when the errors occurred
Apply Updates	Errors can be resolved by updates Apply updates to drivers, the operating system, and/or software programs
Repair Application	If an application is corrupted, repair the application (from Add/Remove Programs) Some applications don't provide a repair option, in which case, you must uninstall and reinstall it
Update Boot Order	If the computer isn't booting from the correct drive, update the boot order to the correct drive
Disable Windows Services/Applications	Disable services that are causing issues Disable applications that are causing issues This isn't an ideal option because some applications/services may be necessary
Disable Application Startup	Disable applications that automatically load with Windows

Safe Boot	Safe Boot Safe Boot loads Windows with only minimal applications/drivers Once Windows has loaded with Safe Boot, enable applications and drivers one at a time until the error reappears The last thing that you enabled is the cause of the issue Safe Boot is only for diagnostics and isn't an option to use regularly
Rebuild Windows Profile	Delete the Windows profile and allow it to rebuild

3.2 Given a scenario, troubleshoot and resolve PC security issues.

- Common symptoms
    - Pop-ups
    - Browser redirection
    - Security alerts
    - Slow performance
    - Internet connectivity issues
    - PC/OS lockup
    - Application crash
    - OS updates failures
    - Rogue antivirus
    - Spam
    - Renamed system files
    - Disappearing files
    - File permission changes
    - Hijacked email
        - Responses from users regarding email
        - Automated replies from unknown sent email
    - Access denied
    - Invalid certificate (trusted root CA)
    - System/application log errors

Common Symptoms

Pop-ups	A pop-up ad can be a normal part of browsing a website Install a pop-up blocker if you don’t want to see pop-ups Some pop-ups appear automatically (without interaction from a website) if a user has installed some adware/malware In that case, you must remove the adware
Browser Redirection	The browser automatically redirects to a malicious website Check that the browser homepage is set to a legitimate site, and if not, reset it If you can’t reset the browser homepage, you might have malware which you should remove
Security Alert	Identify the cause of the security alert and act accordingly Windows will provide a security alert when you try to run a program that is not trusted Verify the source and purpose of the program before allowing it Some security alerts are false positives
Slow Performance	In this circumstance, the slow performance is assumed to be caused by malware (although many other issues can cause slow performance) Malware may be running in the background Identify malware in Task Manager and/or run a system scan

Internet Connectivity Issue	Identify malware that is blocking the internet connection This is not a common symptom
PC/OS Lockup	Malware may have corrupted some system files or overloaded the system, which leads to a lock-up Delete/disable the malware and repair system files/applications
Application Crash	Malware may have corrupted some system files or overloaded the system, which leads to a lock-up Delete/disable the malware and repair system files/applications
OS Update Failure	OS Update failures are caused by many issues The update may have been interrupted and/or may not be compatible with the existing hardware/software Attempt to restart the update and/or remove incompatible hardware/software
Rogue Antivirus	A rogue antivirus program is a virus that pretends to be an antivirus program Some antivirus programs are fake (they don't scan for viruses or are not effective, but they pretend to be effective) Remove the antivirus program and only install an antivirus program from a legitimate source
SPAM	Unsolicited commercial e-mails You can't prevent people from sending SPAM

	It is easier to safeguard your e-mail Install a SPAM filter and/or block e-mails from senders who are known to e-mail SPAM
Renamed System File	Malware may have renamed the system file A user typically won't have permission to rename a system file Run a system scan and remove any malware
Disappearing Files	Malware may delete system files Run a system scan and remove the malware Restore the files Make sure to perform regular back ups
File Permission Changes	Malware may have changed the permissions Run a system scan and remove the malware Correct the permissions Determine if the file permissions have allowed third parties to access the files without permission
Hijacked E-mail – Responses from users regarding email	Your actual e-mail account has been hijacked (a hacker will use your e-mail account to send messages to people). Change your password and enable 2FA if possible. The hacker either has accessed your account online (knows your e-mail username/password), or has accessed your account through your computer (has access to your computer) Run a malware scan and make sure that your firewall is set up correctly.

Hijacked E-mail – Automated replies from unknown sent e-mail	Your actual e-mail account has not been hijacked. Instead, a hacker has created messages that appear to be from you (they have your e-mail address/name in the header). Enable digital signatures in your e-mail so that hackers can't spoof your e-mail address.
Access Denied	You don't have permission to do a certain thing (access a file, access a resource, install a program, change a setting, etc.) Adjust the settings so that you have permission
Invalid Certificate (trusted root CA)	The certificate is not trusted The name on the certificate doesn't match what it is supposed to Obtain a new certificate from the issuer
System/Application Log Error	Check the log to see what the error is Investigate the cause of the error and take corrective action There are literally millions of scenarios here

3.3 Given a scenario, use best practice procedures for malware removal.

1. Identify and research malware symptoms.
2. Quarantine the infected systems.
3. Disable System Restore (in Windows).
4. Remediate the infected systems.
    a. Update the anti-malware software.
    b. Scan and use removal techniques (safe mode, pre-installation environment).
5. Schedule scans and run updates.
6. Enable System Restore and create a restore point (in Windows).
7. Educate the end user

Malware Removal

Identify Symptoms	How do you know that this is malware vs a legitimate program? What kind of malware is it? A trojan, a virus, spyware, etc.? Need to figure out exactly what the infection is so that you can understand how to remove it Also need to understand the larger implications (is the company a target of some hackers? has any user data been compromised?)
Quarantine the Systems	Isolate the systems from the network so that the malware does not spread That might require you to physically disconnect the computer
Disable System Restore	Disable system restore The malware might be saved in system restore
Remediate the Infected system	Remove the malware The more deeply embedded the malware, the more difficult it is to remove Some malware (such as macro viruses, or adware) can be removed by deleting the file and/or uninstalling the program from the control panel. This would apply to adware that the user voluntarily installed. More complicated malware infects system files and must be deleted with an antivirus program Some malware is so complex that an antivirus program can't remove it

	You may try to remove the malware by booting from a recovery USB/DVD, or by reimaging the computer A very rare type of malware can infect device firmware (including the BIOS). This type of malware can't be removed without replacing the hardware
Schedule Scans/Updates	Make sure that the antivirus program you installed is up to date and schedule regular scans
Enable System Restore/Create a Restore Point	Enable system restore and create a restore point This ensures that you have a restore point where the system is clean Also ensures that system restore is functioning (we disabled it in the previous step)
Educate the End User	It is easier and more cost-effective to educate the end user than to come back and remove more malware Show the end user how to detect malware (suspicious e-mail attachments, adware programs, etc.) so that they don't install them in the future

3.4 Given a scenario, troubleshoot mobile OS and application issues.

- Common symptoms
  - Dim display
  - Intermittent wireless
  - No wireless connectivity
  - No Bluetooth connectivity
  - Cannot broadcast to external monitor
  - Touchscreen non-responsive
  - Apps not loading
  - Slow performance
  - Unable to decrypt email
  - Extremely short battery life
  - Overheating
  - Frozen system
  - No sound from speakers
  - Inaccurate touch screen response
  - System lockout
  - App log errors

Mobile OS Issues

Dim Display	The backlight is defective. Replace the back light. The screen brightness is set to a low. Increase the brightness. The device has a light sensor (it automatically dims the screen in low-light conditions). The sensor might be dirty or damaged. Clean/replace the sensor.
Intermittent Wireless	The wireless card/antenna is damaged. Replace the wireless card/antenna. The device is not within range of a wireless network. Improve the wireless network and/or move to within range of a network.
No Wireless Connectivity	The wireless card/antenna is damaged. Replace the wireless card. The device is not within range of a wireless network. Improve the wireless network and/or move to within range of a network. The device only supports 2.4Ghz networks, and the available networks are 5Ghz. Replace the device/wireless card with one that is capable of 5Ghz connectivity.

	The wireless settings on the device are not configured correctly. Configure the correct SSID/password.
No Bluetooth Connectivity	The device is not within range of a Bluetooth device. Move to within range of a Bluetooth device. The device does not support Bluetooth. Replace the device with one that supports Bluetooth. The device is not synced with a Bluetooth device. Sync the devices.
Cannot broadcast to External Monitor	The device and/or external monitor does not support broadcasting. Replace the devices with ones that support broadcasting. The device and/or external monitor are not configured correctly. Configure the device and/or external monitor.
Touchscreen Non-Responsive	The touchscreen is dirty or defective. Repair or replace the touchscreen.
Apps Not Loading	The device is overloaded or has crashed. Reboot the device. The App is corrupted. Uninstall and reinstall the App.
Slow Performance	The device is overloaded. Reboot the device.

	The device is overloaded. Consider uninstalling unnecessary apps, and/or remove unnecessary data.
Unable to Decrypt E-mail	The password has changed. Check that you have the correct credentials.
Extremely Short Battery Life	The battery has failed, or the device is overloaded/overused. Replace the battery.
Overheating	The device will overheat when overused. Consider purchasing a more powerful device
Frozen System	The system is overloaded with too many applications Reboot the device If the frozen system continues, uninstall unneeded applications and/or delete unneeded files
No Sound from Speakers	The volume is turned down or on mute. Enable the volume. The speakers are damaged. Replace the speakers.
Inaccurate Touch Screen Response	The touchscreen should be calibrated.
System Lockout	The user has entered an incorrect password. Determine the password. Use a tool to unlock the device, if possible.

App Log Errors	Check the log to see what the error is Investigate the cause of the error and take corrective action There are literally millions of scenarios here

3.5 Given a scenario, troubleshoot mobile OS and application security issues.

- Common symptoms
    - Signal drop/weak signal
    - Power drain
    - Slow data speeds
    - Unintended Wi-Fi connection
    - Unintended Bluetooth pairing
    - Leaked personal files/data
    - Data transmission over limit
    - Unauthorized account access
    - Unauthorized location tracking
    - Unauthorized camera/ microphone activation
    - High resource utilization

Symptoms, Causes, and Resolution

- Most of these issues are caused by bloatware (useless applications that drain system resources)
- The unauthorized application causes the damage

Signal Drop/Signal Weak	Damage to phone/phone antenna preventing good signal	Repair or replace phone
	Phone in area with weak signal	If signal is Wi-Fi, may need to consider upgrading Wi-Fi If signal is from cellular network, may need to move to area with stronger signal
Power Drain	Phone battery is worn out	Replace battery or phone
	Applications running in the background are causing power drain	Find out if applications are causing drain. Phone settings will show you which applications consume battery life. Remove unnecessary applications
Slow Data Speeds	Phone in area with weak signal	If signal is Wi-Fi, may need to consider upgrading Wi-Fi If signal is from cellular network, may need to move to area with stronger signal
Unintended Wi-Fi Connection	User connected to Wi-Fi accidentally	Delete/forget unintended connection

		Consider implementing mobile device management software to prevent further issues
	Malicious application connected to Wi-Fi	Delete malicious application Consider implementing mobile device management software to prevent further issues Consider wiping phone and reloading
Unintended Bluetooth Pairing	User connected to Bluetooth accidentally	Disconnect and forget Bluetooth connection User may have confused which device he wanted to connect to
	Malicious application caused connection	Delete malicious application Consider implementing mobile device management software to prevent further issues Consider wiping phone and reloading
Leaked Data	User accidentally leaked data via e-mail or other method	Educate user about proper security Consider implementing data leak prevention software Notify affected users/customers about leak

	Malicious Application	Delete malicious application Consider implementing mobile device management software to prevent further issues Consider wiping phone and reloading Notify affected users/customers about leak
	User Account Hacked	Change passwords Educate user about choosing more difficult password Implement 2FA if possible Notify affected users/customers about leak
Data Transmission Over Limit	User has used too much data	Investigate which applications are using the data Educate user about best practices User may be connected to cellular when Wi-Fi networks are available
	Background application used the data	Investigate which applications are using the data Delete unnecessary applications Consider implementing mobile device management software to prevent further issues

Unauthorized Account Access	Malicious application installed which provided access	Delete malicious application Consider implementing mobile device management software to prevent further issues Consider wiping phone and reloading Notify affected users/customers about leak
	User account hacked	Change passwords Educate user about choosing more difficult password Implement 2FA if possible Notify affected users/customers about leak
Unauthorized Location Tracking	Malicious Application	Delete malicious application Consider implementing mobile device management software to prevent further issues Consider wiping phone and reloading
Unauthorized Camera Activation	Malicious Application	Delete malicious application Consider implementing mobile device management software to prevent further issues

		Consider wiping phone and reloading
High Resource Utilization	Background Applications	Investigate which background applications are using more resources and remove them
	Phone is not powerful enough for user requirements	Consider purchasing a more powerful device if existing device is not adequate

Part J 220-1002 4.0 Operational Procedure

4.1 Compare and contrast best practices associated with types of documentation.

- Network topology diagrams
- Knowledge base/articles
- Incident documentation
- Regulatory and compliance policy
- Acceptable use policy
- Password policy
- Inventory management
    - Asset tags
    - Barcodes

Documentation Types

Network Topology Diagram	Shows how network devices are connected together May be a high-level (showing main devices such as switches and routers May show IP addresses and port numbers This diagram should be kept confidential, and updated any time the network changes
Knowledge Base	Store knowledge, standard operating procedures, user manuals, etc. The knowledge base is typically online and can be searched When you solve a problem, you should create an article in the knowledge base explaining how you solved it Other users/IT personnel can access the knowledge base to solve the problem
Incident Documentation	Each incident should be documented A ticketing system such as Service Now can be used When a user reports an issue, a ticket or incident is created An incident can be assigned to the appropriate member of the IT department Each time an update happens to the incident, it can be logged Other users working on the same incident can view the full history
Regulatory & Compliance Policy	Must comply with applicable laws and regulations

	Create a policy that complies with the government regulations in your jurisdiction and make sure that people follow it The policy should contain concrete steps May need to consult with a lawyer
Acceptable Use Policy	Acceptable Use Policy lists what users can and cannot do The policy may vary from organization to organization In a business, the policy should be that technology can only be used for work-related purposes Some businesses may allow limited personal use of the technology, provided that the personal use does not impact the business Other parts of the policy include: no accessing inappropriate or illegal content, no software piracy, no pornography, etc.
Password Policy	Enforce a password policy Common policy may require a password to contain letters, numbers, special characters, etc. Policy may require users to change their passwords every 90 days, and not use easy to guess passwords such as their names The password policy can be enforced by the Active Directory
Inventory Management – Asset Tags/Barcodes	Each piece of IT hardware should be tagged with an Asset Tag/barcode

	The Asset Tag identifies the hardware throughout its lifecycle from purchase to disposal The organization can track where the item is and which department it is assigned to Asset Tags help the organization reduce costs

4.2 Given a scenario, implement basic change management best practices.

- Documented business processes
- Purpose of the change
- Scope the change
- Risk analysis
- Plan for change
- End-user acceptance
- Change board
    - Approvals
- Backout plan
- Document changes

Change Management

To learn more about Change Management, consult the PMBOK (Project Management Body of Knowledge)

Each time we change something in the organization, we should follow this procedure

- We should have a clearly documented policy for each thing we do (a documented business process)
- We should identify the purpose of the change. Why are we changing this thing? What benefit will it bring us, or what harm will it reduce? *For example, we want to upgrade our network. It will bring us faster speeds, better security, and improved performance.*
- What is the scope of the change? Exactly what are we going to do? We must define the scope of work clearly.
- Risk Analysis. What are the risks? A risk can be negative or positive. *It will cost money to change the network equipment. We risk downtime during the change, and there is a possibility that the upgrade doesn't go as planned, leaving users without internet.*
- Plan for change. How will we implement the change? We should clearly write out our steps.
- End-user Acceptance. The people who are affected by the change must accept our plan and risk analysis.
- Change Board. Also known as a Change Control Board. The board decides whether to approve or reject the change. The board is made up of stakeholders from the organization.
- Backout Plan. We should always have a plan to go back to the old setup in case the change fails. The change may fail during implementation or later down the road. *For example, we might change the network equipment and realize in the middle of the upgrade that some new equipment is missing or defective. We should have a plan to revert to the old configuration.*
    - We should have specific criteria for when we are going to roll back. It might be a time, cost, or other measure.
    - *For example, the network appears to be functioning early in the upgrade, but during testing we discover that some resources are inaccessible.*
- Document Changes. Write down the changes that are made so that others can reference them.

4.3 Given a scenario, implement basic disaster prevention and recovery methods.

- Backup and recovery
  - Image level
  - File level
  - Critical applications
- Backup testing
- UPS
- Surge protector
- Cloud storage vs. local storage backups
- Account recovery options

How do we back up data?

There are two ways (we can image an entire hard disk drive or back up individual files)

Image the data

- Can image an entire hard disk drive
- Known as a bare metal back up
- We are taking all the raw data, including deleted data
- Not possible/practical to restore individual files from an image (must restore the entire drive)
- If the entire server/computer fails, we can restore from back up to the previous configuration, including files, applications, user accounts, and settings
- We may need to shut down the server to perform the back up
- If the server has virtualization, then we don't need to shut down the server

File level

- We back up individual files
- If a file is modified or deleted, we can restore individual files
- File level back-ups won't restore settings or applications

Critical Applications

- It is difficult to back up an application because an application is more than just files (it may contain registry settings, log files in hidden directories, services, sockets, etc.) When you install an application, it modifies other settings on the computer. If you simply back up the program files, the application may not operate.
- To back up a critical application, consider using a server application such as VMWare, which can virtualize a server. VMWare can allow an application to run on multiple physical servers, even servers that are in different geographic locations. If a server fails, VMWare can fail over to the other server without affecting users' access to the application

Back up testing

- Verify that the back up is completed properly and that all files are there
- Just because a back up appears to be running doesn't mean that it is working
- You should attempt to restore a back up and make sure that it works

UPS

- Provides us with power in case of an outage
- Needed for network equipment
- How much capacity do we need? Calculate the amount of power required to run the equipment multiplied by the amount of time we need to run the equipment
- A UPS can be connected to the network for monitoring purposes
- A UPS can be built into the building or can be a rack-mounted component
- A UPS may have some outlets that provide a battery back up and other outlets that only provide surge protection

Surge Protector

- Provides protection for power surge only, not for power failure
- A surge protector protects computer equipment from a high-power surge
- There is a limit to the voltage that it can protect from
- Many surge protectors come with a connected equipment guarantee (if the equipment is damaged when connected to a surge protector, the manufacturer will reimburse you for the replacement cost)

Cloud Storage v Local Storage

- People assume that Local Storage doesn't cost anything, but local storage costs include electricity, cooling, maintenance, and server management. There are many hidden costs
- Cloud storage likely costs you a fee per GB per month (for storage), and a fee per GB for downloading/uploading the data
- Cloud storage can provide users in many locations with access to the files
- Local storage won't protect you from natural disasters such as fires or floods
- Cloud storage relies on vendors. If a vendor goes out of business, you may lose access to your data.
- Cloud storage may have higher latency than local storage; however, cloud vendors have excellent networks

Account Recovery Options

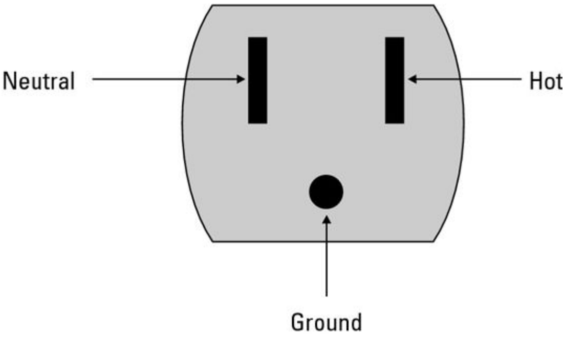
- How do users get back into their accounts when they forget their passwords?
- The administrator can manually reset the password
    - Least complicated system
    - Can cause a delay if the administrator is busy
    - Can overwhelm the administrator if there are many users
- A self-service password reset function is the best way
    - The user clicks on a link, and receives a password reset link via e-mail (or SMS if the user is attempting to reset their e-mail password)
    - Automatic and instant
    - Potential for abuse

4.4 Explain common safety procedures.

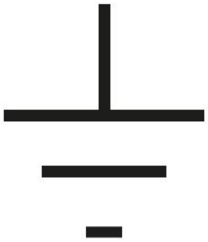
- Equipment grounding
- Proper component handling and storage
  - Antistatic bags
  - ESD straps
  - ESD mats
  - Self-grounding
- Toxic waste handling
  - Batteries
  - Toner
  - CRT
  - Cell phones
  - Tablets
- Personal safety
  - Disconnect power before repairing PC
  - Remove jewelry
  - Lifting techniques
  - Weight limitations
  - Electrical fire safety
  - Cable management
  - Safety goggles
  - Air filter mask
- Compliance with government regulations

Equipment Grounding

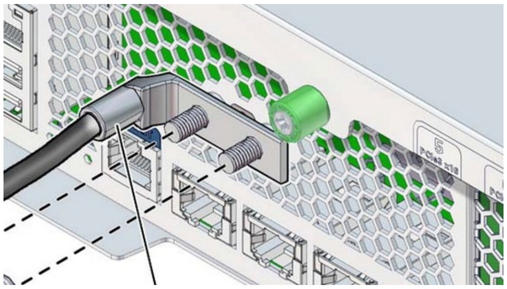
- When we construct a building, the electricians install a "grounding rod", which is a long rod in the ground. That's why it is called a ground
- Electrical outlets throughout the entire electrical system are connected to the grounding rod through a ground wire
- Most appliances contain a third prong, which is connected to the ground wire. If there is a fault in the wiring, a lightning strike, or some other electrical issue, the electricity flows into the ground wire, and literally into the ground. This protects us against electric shocks and fire



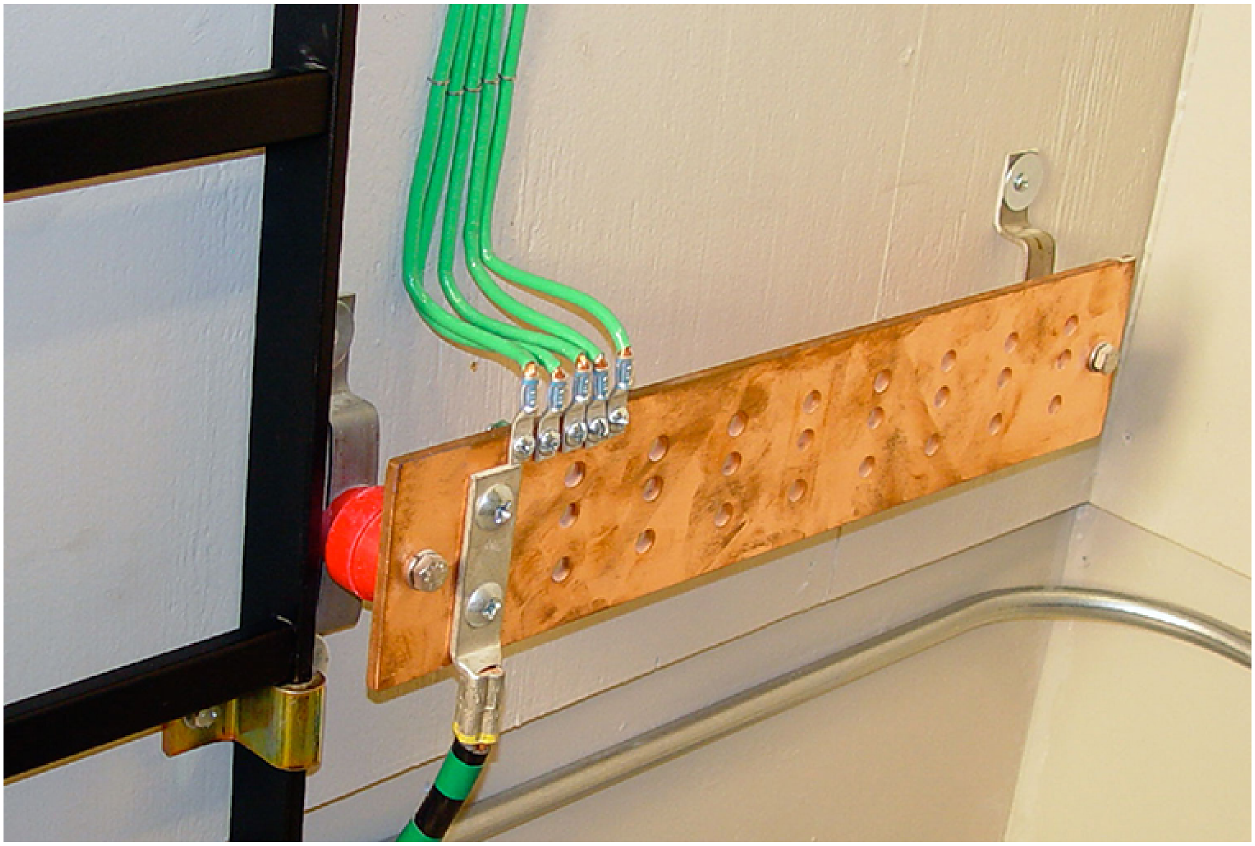
- Some devices contain additional grounding requirements. You will see a ground symbol on the chassis



  - If you see this symbol, you should connect the ground port on the device to the building ground



    - In a server room, a electrician will typically install a grounding bar
        - The bar is usually copper
        - Grounding wire is usually copper, with a green plastic coating
        - The thickness of the wire depends on the amount of equipment connected and the amount of current that is expected to flow through the wire
        - In theory, it is safe to touch the ground wire, but you probably shouldn't do it
        - Always check for current before touching any electrical wire and consult a qualified electrician



- Server racks should always be grounded
    - If the rack has a ground symbol, connect the ground wire to that
    - If the rack doesn't have a ground symbol, connect the ground wire to a hole on the rack
        - Scrape the paint off the rack first, so that the ground wire contacts the bare metal of the rack

Proper component handling and storage

- Some electronic devices (hard drives, PCI cards, etc.) can be damaged by electric shocks or static electricity
  - These devices should be stored inside antistatic bags
  - Bags are available in a wide variety of sizes

- ESD strap
  - Wear an ESD wrist strap when you are working with sensitive electronic components
  - The strap takes static electricity from you and passes it to the ground
  - You must connect the other end of the strap to a ground source

- ESD mat
  - An ESD mat transfers static electricity to the ground
  - The ESD mat allows you to work on a cellular phone or other computer equipment
  - The mat may also allow you to connect a wrist strap

- Self-grounding
  - You can self ground yourself before working with computer equipment
  - Self-ground by touching something metal
  - The metal will absorb any static in your body

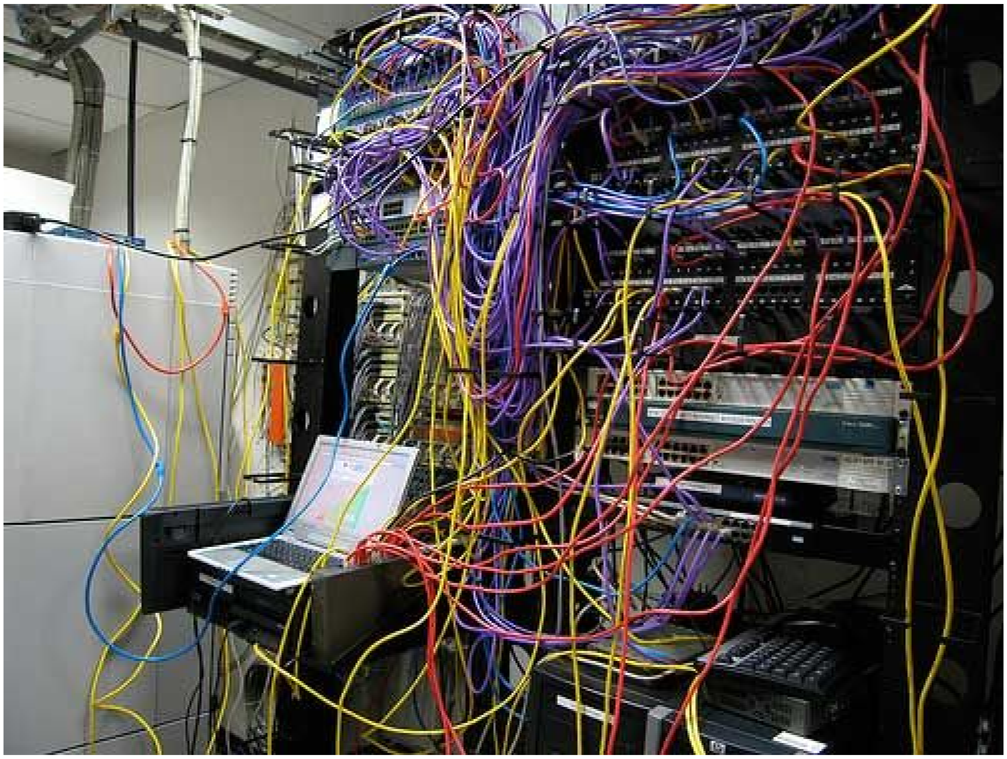
Toxic Waste Handling

- Batteries
    - Put in the trash
    - Check local regulations and recycling programs. Some communities will accept used batteries for recycling
- Used toner cartridges
    - Put in the trash
    - Send back to manufacturer (manufacturers may pick up waste toner cartridges for free; they will refill them)
- CRT Monitors
    - CRT monitors contain lead
    - Contact a recycling agency or local municipality
- Cell phones & tablets
    - Donate them if data leaks are not a risk and if the devices are still functioning
    - Send to a recycling agency

Personal Safety

- Always disconnect the power before repairing any electronic device
    - Some devices have redundant power supplies (multiple electrical plugs), which should be disconnected
    - Some devices have battery power, which should be disconnected
    - Devices may contain capacitors, which could create electric shocks even after the battery and power supplies have been disconnected. Be cautious not to touch any capacitators.
    - An exception can be made for hot-swappable components (such as replacing a hard disk drive on a server)
- Remove jewelry before repairing a device
    - The jewelry could get caught and cause personal injury
    - The jewelry could conduct electricity
- Lifting Techniques
    - Follow proper lifting techniques
    - Lift with your legs, not your back
    - Have good posture
    - Don't twist
    - Go slowly
    - If you're carrying something, make sure that there are no obstructions in the path ahead of you
- Weight Limitations
    - Don't lift more than you can handle
    - Ask for help or use a tool such as a dolly or cart
- Electrical Fire Safety
    - Inspect power cords and outlets to make sure that they are not damaged before using them
    - Use three-pronged electrical cords with equipment, because they provide grounding
    - Keep an electrical fire-rated fire extinguisher nearby
- Cable Management
    - Cables should be neat and labelled

  - Proper cable management should start when equipment is installed
  - Tangled cables are difficult to trace and can present a tripping hazard



- Safety Goggles
  - Wear them
  - Your eyes are sensitive and it's impossible to predict when harm to them could occur
  - The tiniest spec of metal or loose wire could come out of nowhere, and cause blindness
- Air Filter Mask
  - Known as a respirator
  - Protects you from harmful fumes, gases, and other contaminants
  - Wear it when it is required
  - Make sure to use the correct filter for the hazard you encounter (there are different filter types for different hazards)

4.5 Explain environmental impacts and appropriate controls.

- MSDS documentation for handling and disposal
- Temperature, humidity level awareness, and proper ventilation
- Power surges, brownouts, and blackouts
    - Battery backup
    - Surge suppressor
- Protection from airborne particles
    - Enclosures
    - Air filters/mask
- Dust and debris
    - Compressed air
    - Vacuums
- Compliance to government regulations

MSDS Documentation - Canada

- MSDS means Material Safety Data Sheets
- Any material (chemical) covered by WHMIS (Workplace Hazardous Materials Information System) must have an MSDS
- An employer is required to provide an MSDS in the workplace for any material that a worker or contractor is exposed to
- MSDS are provided by the supplier of the material
- It’s your right to view the MSDS
- MSDS contain
  - Product Information: product identifier (name), manufacturer and suppliers’ names, addresses, and emergency phone numbers
  - Hazardous Ingredients
  - Physical Data
  - Fire or Explosion Hazard Data
  - Reactivity Data: information on the chemical instability of a product and the substances it may react with
  - Toxicological Properties: health effects
  - Preventive Measures
  - First Aid Measures
  - Preparation Information: who is responsible for preparation and date of preparation of MSDS

MSDS Documentation – United States

- In the United States, they are called SDS (Safety Data Sheets)
- Employer is required by law to provide the SDS to employees
- It's your right to view the SDS
- Most important is that you know how to properly handle the material safely and dispose of it. That includes safety protection.
- Contain 16 sections
    - Section 1 – Identification: Product identifier, manufacturer or distributor name, address, phone number, emergency phone number, recommended use, and restrictions on use.
    - Section 2 – Hazard(s) identification: All hazards regarding the chemical and required label elements.
    - Section 3 – Composition/Information on ingredients: Information on chemical ingredients and trade secret claims.
    - Section 4 – First-aid measures: Required first aid treatment for exposure to a chemical and the symptoms (immediate or delayed) of exposure.
    - Section 5 – Fire-fighting measures: The techniques and equipment recommended for extinguishing a fire involving the chemical and hazards that may be created during combustion.
    - Section 6 – Accidental release measures: Steps to take in the event of a spill or release involving the chemical. Includes: emergency procedures, protective equipment and proper methods of containment and cleanup.
    - Section 7 – Handling and storage: Precautions for safe handling and storage, including incompatibilities.
    - Section 8 – Exposure controls/Personal protection: OSHA's permissible exposure limits (PELs), threshold limit values (TLVs), appropriate engineering controls, and personal protective equipment (PPE).
    - Section 9 – Physical and chemical properties: The chemical's characteristics.
    - Section 10 – Stability and reactivity: Chemical stability and possible hazardous reactions.

- Section 11 – Toxicological information: Routes of exposure (inhalation, ingestion, or absorption contact), symptoms, acute and chronic effects, and numerical measures of toxicity.
- Section 12 – Ecological information: How the chemical might affect the environment and the duration of the effect.
- Section 13 – Disposal considerations: Describes safe handling of wastes and methods of disposal, including the disposal of any contaminated packaging.
- Section 14 – Transportation information: Packing, marking, and labeling requirements for hazardous chemical shipments.
- Section 15 – Regulatory information: Indicates regulations that apply to chemical.
- Section 16 – Other information: Includes date of preparation or last revision.

Temperature, humidity level awareness, and proper ventilation

- In any building or workplace, there are three HVAC requirements
    - Temperature – the temperature of the room should be comfortable for the occupants. In a server room, the temperature should be 68° to 75°F (20° to 24°C) so that the equipment can be cooled properly.
    - Humidity – the humidity (water content in the air) should be comfortable for the occupants. Server room humidity should be set between 45% and 55%. If the humidity is too high, water content will corrode the equipment.
    - Proper Ventilation – the building requires fresh air. The amount of fresh air required depends on the number of occupants. In a server room, proper air circulation is necessary. Hot air is ejected from the room and cool air is brought in.

Power surges, brownouts, and blackouts

- Use a battery backup and surge suppressor where necessary
- They were covered in the previous section
- A power surge is when too much power comes in. A power surge can damage the electrical equipment. Prevent power surges by installing surge protectors
- A brownout is when the voltage in the electrical system drops. It is caused when the power company can't supply enough electricity to keep up with demand. It may cause electrical equipment to slow down or stop working until proper power is restored.
- A blackout is when no power is received. It is caused by damage to the electrical system
    - Blackouts and brownouts can't be prevented
    - If you install a UPS (a battery backup), your equipment will continue to operate even in the event of a blackout/brownout
    - A battery lasts for a limited amount of time, but can be supplemented by an electrical generator

Protection from airborne particles

- Air filters can remove harmful airborne particles
  - An air filter is connected to the building's ventilation system
- You may also perform work inside a hood if the work you're performing is particularly harmful

Dust and debris

- Dust can plug fans and other components of electronic devices
- Dust prevents proper ventilation and can cause equipment to overheat or jam
- The best way to remove dust is to prevent it from contacting electronics
    - Use a proper filter in your HVAC system
- If you still have dust in your equipment, you can remove the dust with a compressed air can or a vacuum

4.6 Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.

- Incident response
  - First response
    - Identify
    - Report through proper channels
    - Data/device preservation
  - Use of documentation/ documentation changes
  - Chain of custody
    - Tracking of evidence/ documenting process
- Licensing/DRM/EULA
  - Open-source vs. commercial license
  - Personal license vs. enterprise licenses
- Regulated data
  - PII
  - PCI
  - GDPR
  - PHI
- Follow all policies and security best practices

Incident Response

- Identify the affected devices and materials
- Report the activity to the proper channels
- Who you should report to depends on the policies of your employer and the jurisdiction that you're in
    - Your boss/manager
    - Legal department
    - Police/law enforcement
    - Government regulator
- Preserve the device so that the data is not deleted
    - Devices should be disconnected from the network so that they can't be modified
    - Phones may be placed in a Faraday bag so that they do not communicate. Avoids the risk of being erased remotely
- Document everything that you see, including the date/time, and who you spoke with
- Chain of custody
    - Record who had possession of the device at what time
    - This means that we know where the device was all the time
    - If we left the device unattended, how do we know that somebody didn't modify the contents?

Software Licensing

- Open Source License
    - Open Source means that the source code is available to you.
    - Allows you to modify the software
    - It doesn't mean that the software is free (although most Open Source applications are free)
    - There may be certain terms and conditions
        - Must keep the author's name in the software
        - You can modify the software and redistribute it, but not allowed to sell it
        - Free for non-commercial use
- Commercial License
    - Must pay for the software
    - Can use the software for commercial use
    - The source code is not available
- Personal License
    - Used by you for personal use
    - Can be used for educational purposes
    - May be prohibited from using the software for commercial purposes
- Enterprise License
    - Used in a large company
    - License may be per user, per person, or company-wide
- Other License Types
    - Per use – the license is for one use of the software. You must purchase a license for each time you operate the software
    - Per person – the license is for each person who uses the software. If 100 people need to use the software, then you will require 100 licenses.
    - Per user – the license is for each simultaneous user. If 100 people need to use the software, but only 10 people need to use the software at the same time, you only need 10 licenses. Typically, the software licenses are stored on a license server. A user can borrow a license from the server, use the software, and then return the license.

- Company-wide – anybody in the organization can use the software
- Per server or per core – you require a license for each server or processor core. The more cores you have, the more licenses that you will require. This is a common license scheme for database and server applications
- USB Dongle – the license is stored on a USB key. You must connect the USB key to the computer in order to use the software
- Cloud – many companies are switching to cloud licenses, where you are required to pay per month for the software. This is also known as Software as a Service. It reduces up-front costs for the software, but increases total overall costs.

DRM

- DRM is Digital Rights Management
- A software company can include DRM to prevent you from copying, printing, modifying, or sharing the data
- DRM can be applied to videos, images, PDF documents, and software programs
- Removing DRM is illegal

EULA

- EULA is End User License Agreement
- You must accept the End User License Agreement to use the software
- The agreement might limit what you can do with the software or how you can use it

Regulated Data

- Regulated data is data that is subject to government or industry regulations
- Regulated data should be encrypted
- Only authorized people should be able to access the regulated data. They should only be able to access the data that is required for them to do their jobs
- Document who accessed the data, what they accessed, and when they accessed it
- If you store data that belongs to a customer, you may be required to provide the customer with a copy of their data upon request
- The government may inspect your data or data storage systems
- PII
  - Personally Identifying Information
  - Information that could identify a person
  - Includes drivers license, date of birth, social security number, address, name, etc.
  - Storage is subject to local and national privacy laws
- PCI
  - Payment Card Industry
  - Includes credit card numbers and expiry dates
  - Must comply with PCI regulations
  - The credit card industry has specific requirements for what data you can store and for how long
- GDPR
  - General Data Protection Regulation
  - European regulation
  - Applies to any company that stores data belonging to a resident of the European Union
  - Requirements
    - You must have consent to store or process the data
    - You must have data protection procedures built in to your business procedures
    - Citizens have a right to access the data that you are storing about them
    - Citizens have a right to request that you erase their data

  - You can be fined if you fail to comply with GDPR
- PHI
  - Protected Health Information
  - Includes medical records, test results, prescriptions, diagnostics, etc.
  - In the United States, PHI is subject to the HIPAA law (Health Information Portability & Accountability Act)
    - Patients have a right to access their PHI
    - You must protect the PHI
    - You can be fined for failing to comply with HIPAA

Best Practices

- Make sure that you comply with the regulations imposed by your employer and/or your client
- Make sure that you comply with the applicable laws and regulations
- Consider
  - You are subject to the laws of the city, county, state, province, and country that you're physically and/or legally present in
  - If you're storing data belonging to foreigners, you may be subject to foreign laws. For example, if you're located in the United States, but your customers are in Belgium, and you're storing the data in the United States, you might be subject to US law and Belgian law.
  - You are subject to the laws of the region where you store your data. If you're located in Canada, and store data on behalf of Canadians, but you store the data in servers located in the United States, you may be subject to Canadian law and US law.
  - A jurisdiction may not allow you to store data outside of its jurisdiction. For example, the province of Alberta, Canada may require you to store personal data on servers located in Canada. It might be illegal to store personal data belonging to Canadians on servers located in the United States.
  - A jurisdiction may require you to store the data on servers that are physically in your possession. That means you won't be able to store data on servers operated by third parties (such as Azure or AWS).
- Security
  - Encrypt the data at rest and when transmitted
  - Use two-factor authentication
  - Log all access to the data

4.7 Given a scenario, use proper communication techniques and professionalism.

- *Use proper language and avoid jargon, acronyms, and slang, when applicable*
- *Maintain a positive attitude/ project confidence*
- *Actively listen (taking notes) and avoid interrupting the customer*
- *Be culturally sensitive*
  - *Use appropriate professional titles, when applicable*
- *Be on time (if late, contact the customer)*
- *Avoid distractions*
  - *Personal calls*
  - *Texting/social media sites*
  - *Talking to coworkers while interacting with customers*
  - *Personal interruptions*
- *Dealing with difficult customers or situations*
  - *Do not argue with customers and/or be defensive*
  - *Avoid dismissing customer problems*
  - *Avoid being judgmental*
  - *Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)*
  - *Do not disclose experiences via social media outlets*
- *Set and meet expectations/timeline and communicate status with the customer*
  - *Offer different repair/ replacement options, if applicable*
  - *Provide proper documentation on the services provided*
  - *Follow up with customer/user at a later date to verify satisfaction*
- *Deal appropriately with customers' confidential and private materials*
  - *Located on a computer, desktop, printer, etc.*

How to deal with customers

- Remember that a typical end user is not experienced with technology.
- When the technology breaks, the end user might be frustrated because the problem is affecting their personal life or their business. A customer may have lost many important files for example.
- Treat the customer the way you want to be treated. Explain the situation to them, but do so at their level
- Be positive and project confidence. If you panic, the customer will panic. Do not panic. Appearance is everything.
- Listen to the customer. The customer has many clues about what went wrong and can help you find the solution or explain how something was connected.
- Be culturally sensitive. The customer may have an ego, or a title such as "Dr., Mr. etc."
- Be on time. People are busy. Call ahead of time, if you will be late.
- Don't interrupt by using your phone or making personal calls.

How to deal with difficult customers

- Don’t argue with the customer
- Don’t dismiss the customer’s problems
- Don’t gossip about the customer on the internet
- Don’t judge or be condescending
- Try to paraphrase what the customer tells you to make sure that you understood it correctly

Set Expectations

- Can the problem be fixed? If the customer has trouble installing a software program, it can probably be fixed. If the computer caught fire and there was no back up, it is probably unlikely that you will recover the data.
- If it can be fixed, how much will it cost? That includes labor, software, and hardware. If the cost is too expensive, consider alternative solutions that are within the customer's budget.
- If it can be fixed, how long will it take? The customer may need a solution quickly. Is there a temporary solution that can make the customer operational quickly, while you work on a proper fix?
- Give the customer several options (for hardware)
  - Option to repair the device. Consider that the customer may not have the budget to replace it.
  - Option to replace the device, if it is old. Customer may be interested in a replacement.
  - Option to use genuine parts or generic parts. Discuss the risks with using non-genuine parts if the device is still under warranty.
  - Device may be under warranty. Sending it back to manufacturer can be cheaper, but slower.
- Document what you did
  - Keep documentation for yourself and other technicians
  - Keep documentation for the customer in simple terms
- Follow Up
  - Ensure that the customer is satisfied
  - Many unsatisfied customers don't complain, they just go away. This is bad for business.

Confidentiality

- Consider that the customer may have confidential information
  - Intellectual property or trade secrets
  - Medical records
  - Financial information
  - Personal photos
  - Other sensitive information
- You can't disclose information you see without permission
- You shouldn't remove data from the client's site without their express written consent, and only if it is encrypted. You could be liable if the data is lost.

4.8 Identify the basics of scripting.

- *Script file types*
  - *.bat*
  - *.ps1*
  - *.vbs*
  - *.sh*
  - *.py*
  - *.js*
- *Environment variables*
- *Comment syntax*
- *Basic script constructs*
  - *Basic loops*
  - *Variables*
- *Basic data types*
  - *Integers*
  - *Strings*

Script Files

A script file is a set of commands stored in a text file. The extension of the file allows the computer to determine the type of language it was written in. Make sure that you use the correct extension. You can execute a script file by running it.

Script files are used for

- Automating processes that need to run regularly. Instead of entering the commands manually, you can run the script
- Can be deployed for software installation (for example install a printer on many users). You can create a script to install the printer, send the file to each user, and have them run it.

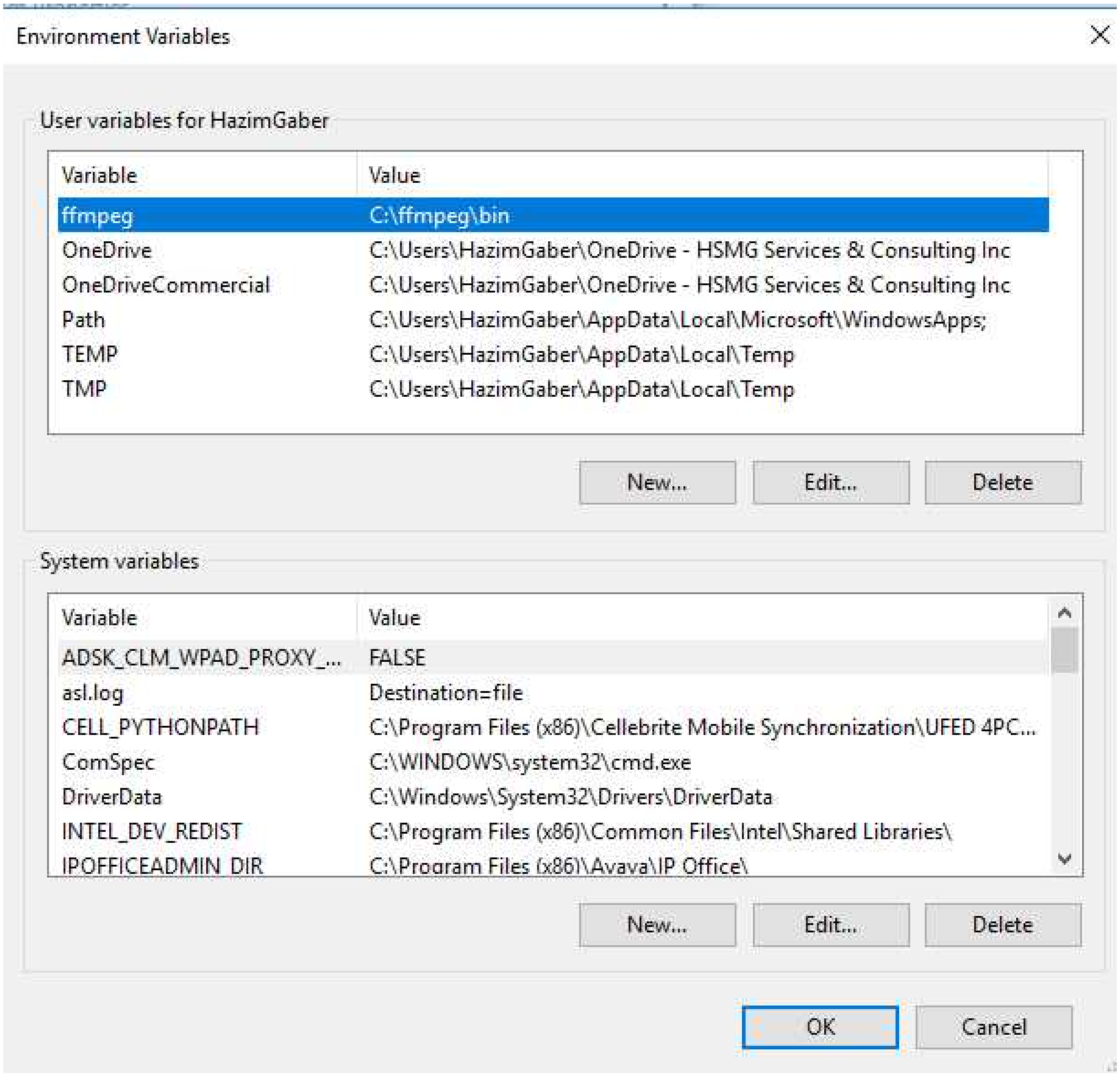
Script Types

BAT	Batch File Contains Windows commands Can operate on all versions of Windows and DOS
PS1	PowerShell Contains Windows PowerShell scripts Can operate on all versions of Windows from Windows XP onward Supports “piping”; allows you to forward the output of one command to the input of another command Use PowerShell to connect to and configure other remote resources • Azure • Exchange Server • SQL Server • Windows Server • SCCM • SharePoint
VBS	Visual Basic A Visual Basic script runs on Windows through the Windows Script Host Contains more features than BAT or PS1 scripts Can be used to introduce malware
SH	Bash Shell Contains UNIX commands Can operate on all versions of UNIX Contains more advanced features than BAT, such as arrays

PY	Python Script Runs on UNIX or Windows if Python is installed on the system
JS	JavaScript A JavaScript script runs on Windows through the Windows Script Host Contains more features than BAT or PS1 scripts Can be used to introduce malware JavaScript is also used for websites and apps

Environmental Variable

- A Windows computer will contain a set of environment variables
- Can view environment variables from the system properties
- An application will query the environmental variable to understand where it needs to store files (for example, where the location of the temp directory is)
- Environment variables are required for some apps to work properly
- A script can reference an environment variable by enclosing the name of the variable with % signs, such as %variablename%
- You can edit the variables from the system properties or from the command line
  - setx variablename "value"



User variables for HazimGaber

Variable	Value
ffmpeg	C:\ffmpeg\bin
OneDrive	C:\Users\HazimGaber\OneDrive - HSMG Services & Consulting Inc
OneDriveCommercial	C:\Users\HazimGaber\OneDrive - HSMG Services & Consulting Inc
Path	C:\Users\HazimGaber\AppData\Local\Microsoft\WindowsApps;
TEMP	C:\Users\HazimGaber\AppData\Local\Temp
TMP	C:\Users\HazimGaber\AppData\Local\Temp

System variables

Variable	Value
ADSK_CLM_WPAD_PROXY_...	FALSE
asl.log	Destination=file
CELL_PYTHONPATH	C:\Program Files (x86)\Cellebrite Mobile Synchronization\UFED 4PC...
ComSpec	C:\WINDOWS\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
INTEL_DEV_REDIST	C:\Program Files (x86)\Common Files\Intel\Shared Libraries\
IPOFFICEADMIN_DIR	C:\Program Files (x86)\Avaya\IP Office\

Comment Syntax

- Comments are important. You will forget what the script does, so it's always good to explain it with comments.
- Comments are ignored by the operating system when executing the script

BAT	Comments start with REM For example This is the command REM This is the comment
PS1	Comments start with #

	For example This is the command #This is the comment
VBS	Comments start with a ‘ For example This is the command ‘This is the comment
SH	Comments start with # For example This is the command #This is the comment
PY	Comments start with # For example This is the command #This is the comment
JS	Comments start with // For example This is the command //This is the comment

Basic Script Constructs

IF Statement	If (some condition is true) {perform this action} Elseif (some other condition is true) {perform this other action} Else {perform this action} An if statement tells the computer to perform an action if a condition is true The if statement contains an "if" section It may contain one or more elseif sections, and it may contain an else section The computer only executes one section. It checks the if and elseif conditions in order. The else is executed if none of the other statements are true. It is possible to write an if statement with no else statement
For	For (condition) {perform this action} The action inside the for loop is executed a specific number of times The for loop performs the action as many times as the for loop requires The for loop increments each time it is executed

	For ($i = 1; $i < 10; $i++) We start counting at 1, and we stop when we reach 10
While Loop	While (condition) {perform this action} While (coffee cup is not full) {add 1 mL of coffee} {check if the coffee cup is full} The while loop contains one condition The while loop performs the action until the condition becomes false The action in the while loop could make it the condition false
Nesting	We can nest multiple if statements, while loops and for loops together It is a good practice to indent statements so that it is easy to see where they belong If (condition is true) If (other condition is true) For (some other condition) (perform this action)
Operators	We can use AND, OR, and NOT to have different/multiple conditions

	If (condition is true AND other condition is true) If (condition is true OR other condition is true) If (condition is true AND other condition is NOT true)

Function	If we want to use the same set of code in multiple places, we can create a function
	A function takes some inputs, performs some operations, and then returns some outputs
	Function (inputs) {
	    (do some thing)
	    (return some outputs)
	}
	Later in our code, we can reference our function
	For example, we can create a function that converts a temperature from Celsius to Fahrenheit
	We store this function in our code
	FunctionConvertTemperature (Celsius temp) {
	    Equation to convert Temperature
	    Return Fahrenheit Temperature

	}
	Anytime we need to convert the temperature, we just call the function, without needing to repeat the code
	FahrenheitTemp = FunctionConvertTemperature (Celsius temp)

Variables

- A variable holds data that could change
- An array is like a variable with more than one dimension
- You must give the variable a name
- Some languages are strict with variables
    - The first time you write the name of the variable, the language automatically recognizes it. You may have to declare the variable before you can use it if the language is strict.
    - You must declare the type of data the variable will hold. Some languages do not require or enforce this.

Basic Data Types

When we create a variable, we tell the computer what kind of data type the variable will hold. Consider rounding errors when declaring and adding variables.

Boolean	This is the smallest variable It can be set as true or false True is equivalent to 1 and False is equivalent to 0 In a comparison we can ask if the Boolean variable is False, or if it is equal to 0
Integer	Whole Number that could be positive or negative For example, -5, 100, 200, 234234234 There are limits to the size of the number Can use integers, singles, and doubles in math equations
String	A non-numeric value A number could be stored as a string Computer understands it as "words" Can't use a string in a math equation
Single/Double/Float	A numeric value with decimals There are limits to the size (number of digits) that can be contained in the variable. It depends on the language

Consider this equation where we add two strings

String1 = "1"
String2 = "1"

String1 + String2 = 11

When we add two string variables, even if they are numbers, the strings are connected together

Integer1 = “1”

Integer2 = “1”

Integer1 + Integer2 = 2

Integer1 = “1”

Answer variable is an integer

Single2 = “0.1”

Answer variable = Integer1 + Single2 = 1

When we add an integer to a single, we receive a variable that is a single. In a strict language, it depends on what the answer variable is typed as.

Answer variable is a single

Single2 = “0.1”

Answer variable = Integer1 + Single2 = 1.1

4.9 Given a scenario, use remote access technologies.

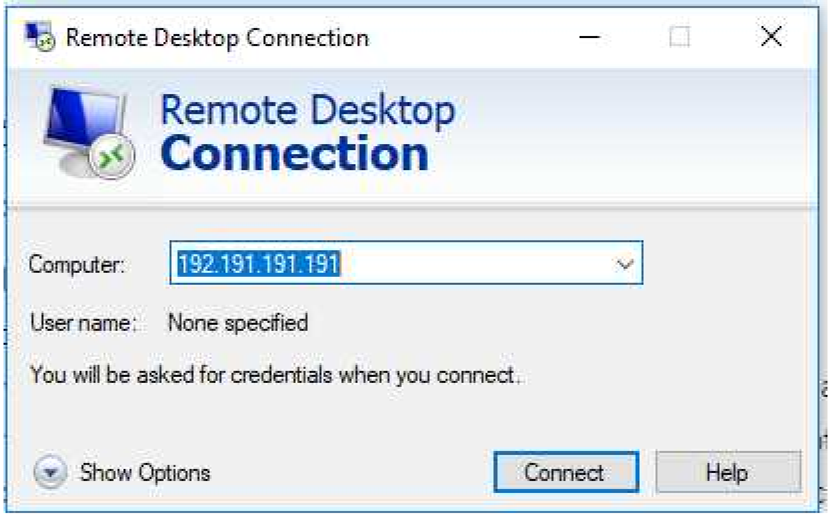
- *RDP*
- *Telnet*
- *SSH*
- *Third-party tools*
    - *Screen share feature*
    - *File share*
- *Security considerations of each access method*

Why are remote access tools necessary?

- We don’t always have physical access to the device. For example, we might need to access a server located in a far away data center.
- We have physical access, but the server is headless. For example, we have a rack full of servers, but no monitor. It’s easier to access the servers remotely from a laptop.
- It is more cost effective. It might be cheaper and faster to obtain remote access to a computer than to drive to the client. This is especially true when a help desk must support geographically diverse clients. For example, the help desk is in India and the clients are located all over the United States.
- We need to multi-task. We want to work on many devices at the same time, and the devices are far apart.

What is RDP?

- Remote Desktop Protocol
- Developed by Microsoft.
- Allows you to connect to a Windows machine
    - Install xrdp on a UNIX machine to connect via RDP
- The machine that you connect to must have RDP enabled (requires Windows Professional)
- You can share
    - Hard Drives
    - Printers
    - Audio
    - Clipboard (can copy to/from host/remote computer)
- You launch RDP and enter the IP address / hostname



Remote Desktop Connection

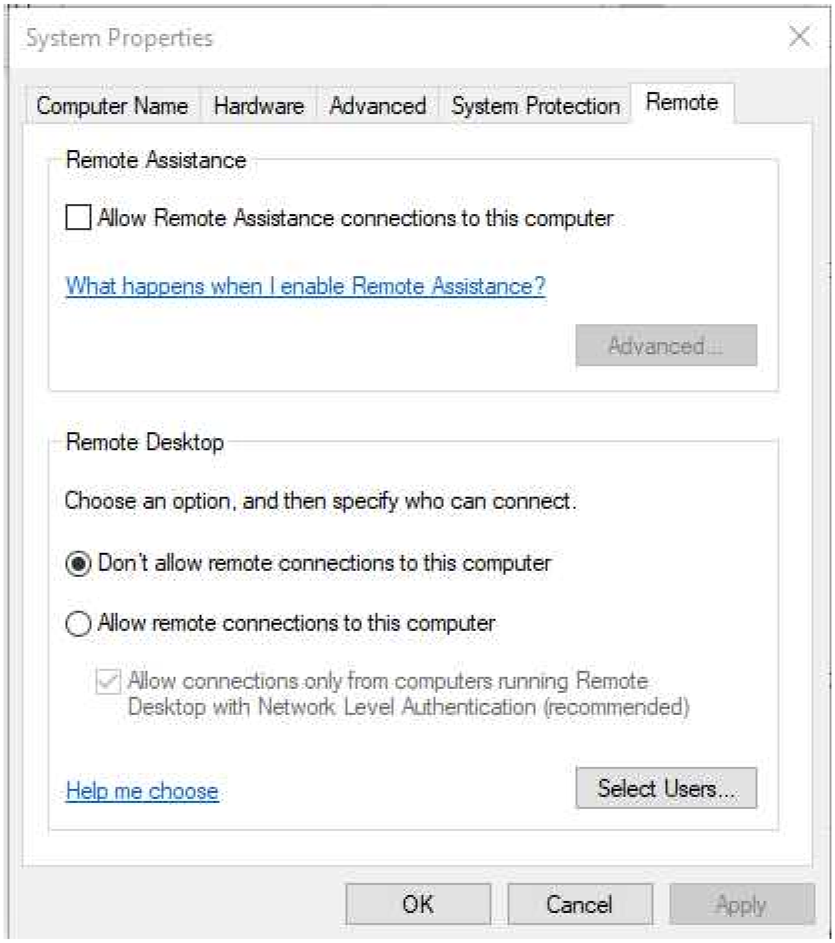
Computer: 192.191.191.191

User name: None specified

You will be asked for credentials when you connect.

- You are required to enter your username and password (on the remote computer)
- RDP uses TCP port 3389

- Remote computer must have RDP enabled (in system properties)



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

☐ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

● Don't allow remote connections to this computer

○ Allow remote connections to this computer

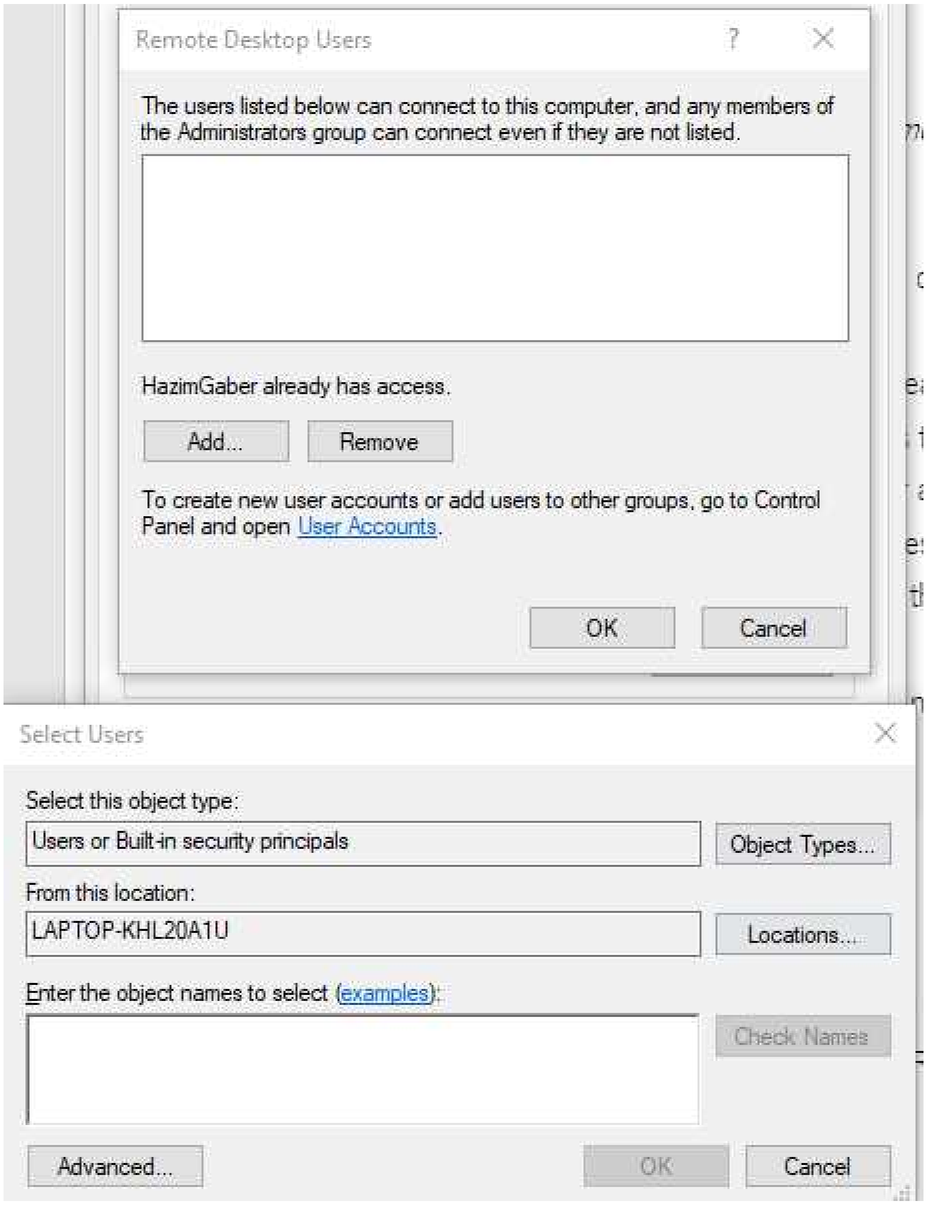
☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

OK | Cancel | Apply

- You can choose which users are able to connect (Administrators have access by default)



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

HazimGaber already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

Select Users

Select this object type:

Users or Built-in security principals

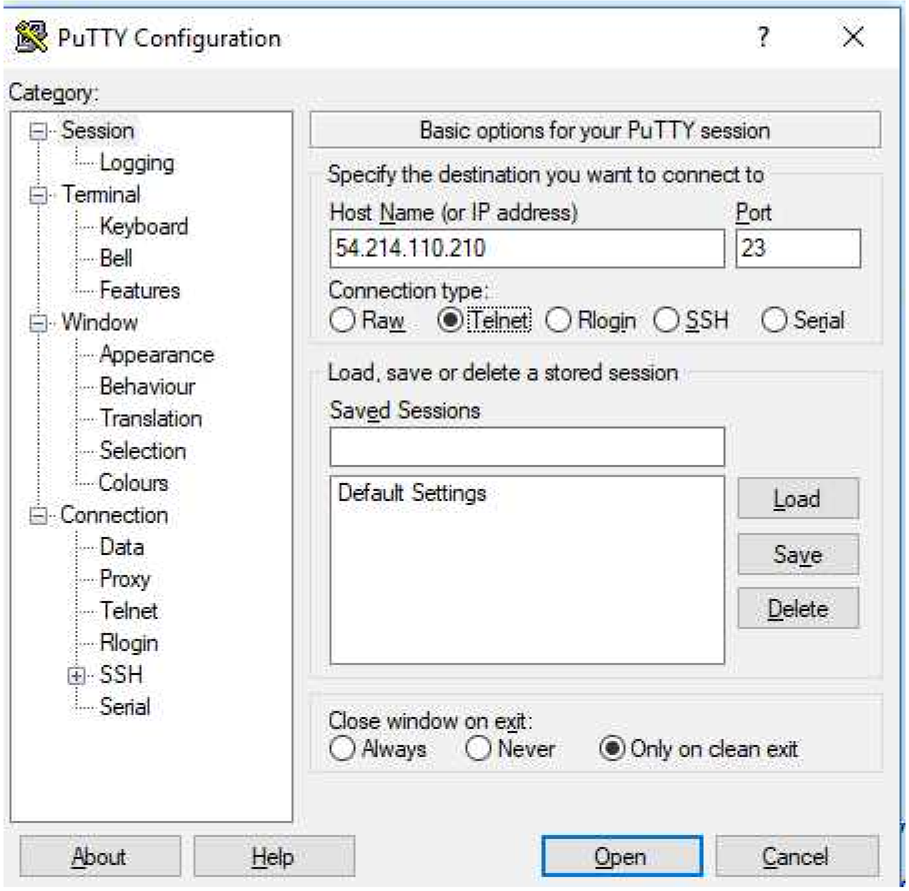
From this location:

LAPTOP-KHL20A1U

Enter the object names to select (examples):

Telnet

- Unlike RDP, Telnet only offers a text connection (a command line interface, not a GUI)
- You can use PuTTY to connect via Telnet
- Telnet is not common
- Telnet does not encrypt traffic



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 54.214.110.210

Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

SSH

- SSH replaced Telnet
- SSH provides secure authentication
  - Authenticates the user so that only authorized users can access the resource
  - Authenticates the resource, so that the identify of the resource is confirmed to the user
- Uses Port 22
- SSH itself is good for connecting to UNIX machines
- You can start a graphical user interface through SSH if you have the correct programs installed

SCCM Remote Control

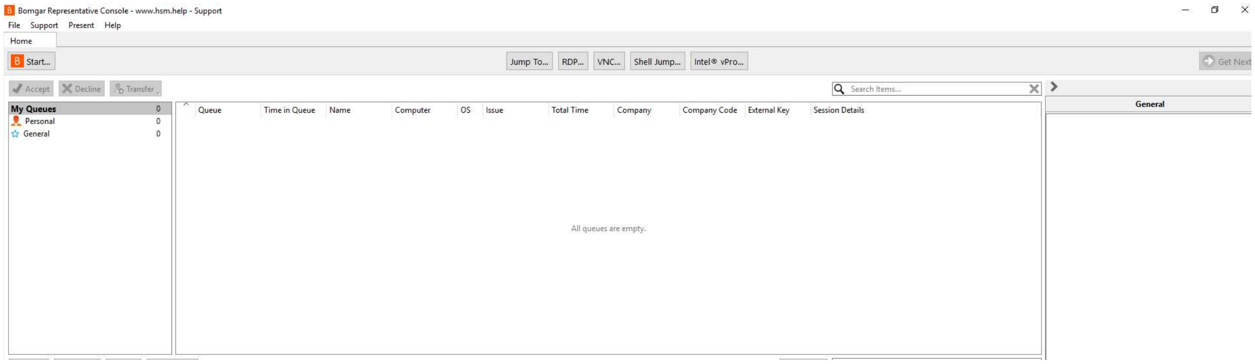
- SCCM Remote Control tool allows you to connect to a remote computer
- The advantage is that you can log the user off and stay connected (if you want to log off and log back on as an admin)
- SCCM works only on the corporate network

iLO

- Many servers have iLO or iDRAC, which allows remote access to the server
- The iLO/iDRAC card is a separate card “a mini server”
- Can manage BIOS of server, reboot server, etc.

Third-party tools

- There are many third-party tools for remote access
- GoToMeeting, Bomgar, TeamViewer, LogMeIn
- Advantage
    - Can collaborate with multiple support agents
    - Can transfer a session to another, more experienced agent
    - Easy to use interface
    - Can record remote sessions
    - Can do special things like reboot the computer and stay connected
    - Can "pin" a client so that you can connect without having the user present (easier than explaining to the user how to connect)
- Disadvantages
    - Can be expensive
    - Bomgar costs $2000+ per user per year; other programs are less expensive, but have less features
    - Your data goes through a third party server, which could be a security risk (Bomgar sells an appliance that you can host)
    - Can be difficult to explain to a user how to download the remote software and connect



My Queues	0
Personal	0
General	0

Queue	Time in Queue	Name	Computer	OS	Issue	Total Time	Company	Company Code	External Key	Session Details

All queues are empty.

Security Considerations

- In order to connect to an RDP session from a remote network, you would need to forward traffic to the client. That exposes the machine to the internet, where it can be hacked. The best option is to set up a VPN, and not expose the machine.
- Third party tools may have security holes or undiscovered bugs.
- Telnet has no security
- SSH has good security
- Bomgar and some other third-party tools support two-factor authentication