

TVET CERTIFICATE IV in NETWORKING

NETWORK MAINTENANCE

NEWNM401

Perform network maintenance

Competence

Credits: 12

Learning hours:70



Sector: ICT

Sub-sector: NETWORKING

Module Note Issue date: July, 2020

Purpose statement

This core module describes the skills, knowledge and attitude required to make a preparation effectively in the computer networks maintenance and networking fields by applying relevant technical knowledge and technical skills in: Network installation, maintenance, selection, and optimization of computer systems, computer networks and associated hardware and software systems. The learner also will have an ability to conduct standard tests and measurements and, to conduct, analyzes, interpret experiments and write technical Report.

Table of Contents

Elements of competence and performance criteria		Page No.
Learning Unit	Performance Criteria	
1. Conduct site survey and analyze the site infrastructure	1.1. Efficient Study of the network structure and the environment	3
	1.2. Adequate verification of network security	
	1.3. Proper verification of the network status	
	1.4. Appropriate identification and selection of tools and materials to be used according to the network status	
2. Determine and implement solutions	2.1. Proper description of network maintenance	69
	2.2. Relevant application of curative maintenance if any	
	2.3. Relevant application of preventive maintenance	
3. Document the work done	3.1 Systematic implementation of SOHO and Enterprise wireless	90
	3.2 Relevant application of security to the technology applied	
	3.3 Efficient test of access point and verifying wireless connection and security arrangements Efficient Troubleshooting of WLAN Problems	

Total Number of Pages: 106

Learning Unit 1: Conduct Site Survey

LO1.1: Study network structure and the environment

- Content/Topic 1: Identification of network components

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Examples of network devices: Desktop computers, laptops, mainframes, and servers, Firewalls, Bridges, Repeaters, Network Interface cards, Switches, hubs, modems, and routers, Smart phones and tablets, Webcams.

Servers, Client computers, Transmission Media ,Network printers and other peripherals, Network Interface Card, Local Operating System and network Operating System.

- **Servers** - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, For example: file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers.
- **Clients** - Clients are computers that access and use the network and shared network resources.
- **Transmission Media** - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.
- **Shared printers and other peripherals:** Is hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.
- **Network Interface Card:** The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network.

PCI Network Interface Card



Short for network interface card, the NIC is also referred to as an Ethernet card and network adapter. It is an expansion card that enables a computer to connect to a network; such as a home network, or the Internet using an Ethernet cable with an RJ-45 connector.

How does a computer with a network card connect to a network?

Network cards can communicate with each other over the same network using a network switch, or if two computers are directly connected.

Local Operating System: A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, Unix, Linux, Windows 2000, Windows 98, and Windows XP etc.

Network Operating System: The network operating system is a program that runs on computers and servers, and allows the computers to communicate over the network.

- **Content/Topic 2: Identification of common network problems**

1. Computer Viruses

Causes

Viruses can come from a wide range of sources, such as e-mail attachments, malicious software, online advertisements, and even social media. Some of the most common ways to get computer viruses include:

- **Opening links/attachments from spoof or unknown links**

These emails are spoofed to look legitimate but have a link or attachment that when opened will infect your computer.

- **Downloading software from malicious sites**

Viruses are not just procured from problematic sites, it is common for viruses to be embedded anywhere on the internet. It is important to double check all downloads on your machine.

- **Online ads**

Malvertising is a very common way to procure viruses to your system. Trusted ads on websites can later be infected with malicious codes.

- **Social Media**

Social media is a big time place for hackers. While users tend to be more comfortable clicking links on social media platforms links that require additional plug-ins can be patched with viruses.

Solutions

Step 1: Check the severity of the infection by running a complete network scan to find malicious files or programs. Make sure that your antivirus and anti-malware programs are up to date and able to scan hidden files, the root directory, and all running programs. Also, try to have your antivirus/anti-malware software scan your e-mail inbox for any malicious materials.

Step 2: Back up all of your system files using the necessary tools. Running a complete system backup will ensure that your data isn't lost and that the network will remain stable. The Windows' "System Restore" option will allow you to set up a restoration that can often be useful in an emergency.

Step 3: Confine all suspicious, irregular files. Isolating them will prevent their exchanging with other files or your network system. Then, disinfect or completely wipe all quarantined files. Manually delete any emails that were identified by your antivirus software.

2. Unable to connect to the Internet

Causes

Wireless networks encounter problems, and being unable to connect your device is a big one. Using a wireless network is great for mobility, but can hinder your productivity when it decides to malfunction. There are a few different reasons why your wireless network is having connectivity issues, such as the wireless router or the network card

Solutions

Step 1: If your router won't connect to the internet, try putting your computer or device right next to the router. If this causes your equipment to connect, then the system hardware may have been the issue. If this didn't fix the problem, proceed to Step 2.

Step 2: Update the network card. Sometimes, your network card will receive a strong signal, but won't be able to transmit it quickly and effectively resulting in the need for network troubleshooting. Updating the driver might solve the problem entirely, but if it doesn't, you might need to contact your IT department or provider and consider replacing the hardware altogether.

3. Duplicated IP Address

Causes

- Your system administrator could have assigned two computers on a local area network (LAN) the same static IP address.
- Your internet service provider accidentally assigned two people the same IP address.
The network's Dynamic Host Configuration Protocol (DHCP) server has allowed the same dynamic address to be assigned to multiple computers automatically.
- Your system administrator has assigned a static IP address to a computer within the local network's DHCP range, and the same address is automatically given by the local DHCP server.
A small error window just popped up on your screen saying that your IP address is already in use. How is this even possible and what causes this IP address conflict? Well, there are a few reasons why this can happen:

Solutions

Windows - If you have a dynamic IP address:

Step 1: Click the "Start" button and click "Run". Enter "cmd" into the text box and click "OK". The Windows command prompt will open.

Step 2: Type "ipconfig/renew" into the command prompt and press "Enter". This will refresh your dynamic IP address.

Step 3: Check your network connection. Your computer will receive an available IP address that isn't already taken.

Windows – if you have a static IP address:

Step 1: Right click "Network Neighborhood" on your desktop. On Windows 7 or Windows Vista, this will be labeled "Network". Next, click "Properties".

Step 2: Right click onto your network card and click "Properties". In most cases, your network card will be labeled "Local area LAN Connection."

Step 3: Select "TCP/IP" in the list and then, click the "Properties" button under the list of options. Enter in a new IP address in the opened window. Click "OK" to confirm the changes you've made.

Mac

Step 1: Click on "System Preferences" in your dock. Then, click on "Network".

Step 2: Select "Wi-Fi" on the left side of the window. Then, click "Advanced", which is located on the bottom right.

Step 3: On the next page, select the "TCP/IP" tab and then click "Renew DHCP Lease" on the right side of the window.

4. Slow Performance

Causes

This happens especially when a computer first turns on or connects to a network. In most cases, this is caused by heavy bandwidth usage. In other instances, it can be caused by lack of hard drive space, running too many applications at once, having too many browser tabs open at one time, or even just a dusty room! The solution for this issue depends on the root of the problem. Once you've gotten rid of some of your browser's extensions, eliminated applications you aren't using, or identified the application that's eating up all of your processing power, you should be able to see a huge difference in your computer's processing speed. (You can do this by using the Task Manager for Windows or the Activity Monitor for Mac to see which applications are slowing you down).

Solutions

Note: Be sure to enforce proper network use by making sure that users aren't viewing too much digital content via streaming or continuously downloading large files. Doing so will help you keep your bandwidth use under control. However, if you find that your employees are utilizing the network correctly, it might be time to upgrade your network to meet your business needs. If you feel that the sluggishness of your applications is due to another issue, proceed to Step 1.

Step 1: Try restarting your PC. Sometimes, a quick reset will fix any and all issues right away. Doing so will clear your system memory (RAM). If this works, remember to shutdown your PC when it's not in use. If this doesn't help, proceed to Step 2.

Step 2: Now, it's time to check on your hard drive and make sure that it's not approaching the end of its lifespan. So, let's run a hard drive check:

Windows

Right click on "Drive". Then, click "Properties" and then click "Tools". Click "Check Now". Select "Scan for and attempt recovery of bad sectors". Doing this will stop your computer from tapping into any malfunctioning areas of the hard drive.

Mac

Click "Applications" from the "Finder", then "Utilities", and then "Disk Utility". Highlight the hard drive that's giving you trouble and then select "First Aid". If your hard drive is healthy, but you think it's becoming too full with data, proceed to Step 3.

Step 3: Get rid of unnecessary files from programs that have gone unused. System backups and restore points can eat up a lot of space, so don't hang onto more versions of this software than you need. You might also consider uploading your data onto the cloud to save your hard drive.

Step 4: If you've completely deep-cleaned your computer and checked all of the possible issues above, but your computer is still running slowly, it might be time to upgrade your RAM so that your computer has

more memory. Certain programs take more RAM to run properly than others and if you don't have enough RAM ready, your computer will not be able to handle it. Look into RAM upgrade options.

5. IP Address Exhaustion

Causes

So, your network seems to have gone down. Your operating system has sent you an alert stating that the address was not received from the DHCP server. You've just checked the network adapter status and noticed that there's actually no IP address to be found.

There are a few different reasons why this could happen. It could be that the DHCP server is out of addresses, the device might be set to use a static address rather than a DHCP address, or maybe the DHCP request from the device never made it to the server.

Solutions

Step 1: Check the network interface card (NIC). You can find this by opening the control panel, then the device manager. Then, select "Hardware and Sound" and then select "Device Manager". Expand the Network Adapters item to view all network adapters, although you will most likely only have one. Verify that your system is configured to utilize DHCP.

Step 2: Check the switch to see which virtual LAN (VLAN) the port is set as a member. Verify that other devices on this particular VLAN are able to get an IP address. If they can't, the issue is that the network is not sending DHCP requests to the server. If this issue is taking place with more than one device, then the issue is likely the server itself.

6. VPN Errors

Causes

The Problem: I got an error message saying that my device was "unable to establish the VPN connection" or error 800. Your virtual private network (VPN) works to provide a safe connection between a local client and a remote server. When you can't connect to a VPN, you'll receive an error message that usually states something along the lines of "VPN error 800 – Unable to establish the VPN connection". This can happen if the client device disconnected from the local network, the network's firewall is blocking the VPN traffic, or if the name/address specified for the VPN server was incorrect.

Solutions

Step 1: Check the connection between the client and server. Attempt to connect to the server from a different client device to verify whether the network issue is a widespread issue or if it is affecting only one client.

Step 2: Verify that the name entered on the client side matches the server name given by the VPN administrator. In some instances, users can specify an IP address rather than a name, while it's more typical for users to mistype the address than the name. VPN servers can also change their IP addresses in some instances, especially DHCP networks.

Step 3: If the first two steps didn't clear up the issue, now it's time to make sure that the firewall isn't blocking your connection with the VPN. Do so by temporarily disabling it to retry the connection. If this solves the problem, you need to update the firewall settings specific to the port numbers that the VPN on the network is using to prevent this issue from happening again. If none of this troubleshooting solved the issue, it could be possible that the server is overloaded with clients or that it is offline. Check with your IT department to see what can be done.

7. Connection Errors and Network Connectivity

Causes

The Problem: My network has limited connectivity or no connectivity at all. Connection issues are some of the most annoying, frustrating network issues of all. These issues can be a result of all types of glitches and issues within the computer and/or the network itself.

Solutions

Step 1: Restart your computer. A quick reboot can often be a life-saver. If you've already tried this or restarting the computer didn't fix anything, proceed to Step 2.

Step 2: Restart your router or modem. DO NOT reset the router or modem or restore its settings back to factory default. Simply turn the router or modem off and back on. If this doesn't work or only works for a moment, keep going to Step 3.

Step 3: If you are connected to your network via Ethernet cable, unplug the cable and then reattach it. If needed, replace your network cable with a new or different cable to see if this was the cause of the issue.

Step 4: If you're connected via Wi-Fi when you see this error, it's a possibility that the network adapter is attempting to conserve power. Stop this by finding the Network and Sharing Center in the Control Panel. Right click "Wi-Fi Connection", select "Properties", click "Configure" and find the "Power Management" tab. Click and uncheck the option that allows your computer to turn off device to conserve power.

Step 5: If you've tried all of this and there's still no connection, unplug your router and connect your computer directly to your modem. If this solves the issue, then your router is likely to be malfunctioning. If not, contact the router manufacturer for support. If the error remains and the network is still down, reach out to your internet service provider for help.

Workstation

A workstation is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems.

Network administration - A network is a system consisting of one or more workstations connected to a server to share resources.

Common resources include printers, storage devices, and folders containing data that many users need to use. The network is used to create centralized access (secure access) to shared resources. Currently the entire network is using the largest shared resource, the World Wide Web.

This article will show the five most common errors with Windows network and workstation systems, and provide some information to help you overcome or mitigate the impact of these problems.

5. Initial configuration error

The first problem makes the network unstable because of an error when configuring the network, configuring the system and configuring the resource usage. A network system usually has too many components while the scale and number of users can increase making it more complex and thus the problem is always permanent. With the development of telecommunications in the past 10 years, and the development of the hardware and software market, many users have installed the system and the network themselves, even without a certain knowledge of the network.

If we want to install and configure Windows or a Linksys router, we need some understanding of this work. For example, if you want to connect your computer to the Internet, then at least we need to know something about the TCP / IP address scheme, DHCP protocol, cable, .

When installing the system, the main problems that caused it were power failure, incorrect cable setup (or Wifi configuration), missing or misconfigured protocols (such as IP) and problems with Windows systems. (as network services are misconfigured). Another problem to consider is to configure the workstation method to access shared resources, such as network printers. If a server is used to provide centralized access, then we need to configure properties on the print server, or if the print server is located and controlled on a server We need to configure the workgroup or the relationship between the client and the server. The relationship between the workstation and the server is one of the major obstacles for people working with network-connected Windows workstations. After completing the configuration and testing

the network, we need to store configuration information so that when problems arise we can quickly detect the cause of the error.

If you want to use Wifi connections through cable connections, the initial design and configuration is very important. OSI Model is very useful when troubleshooting these problems. First, cable connection is often accompanied by a physical error, such as a broken cable, affected by distance or power problem, incorrect connection (wrong type or point), or simply a cable Fully connected. Signal interference is a common problem, especially when the cable is pulled over a power source or light source (with fiber optic cable). Wifi connections are often more complicated because they need the support of software and hardware (such as drivers or application software).

4. Issues of rights, licenses and licenses

If we have configured everything correctly and all the workstations are connected without any problem, is there any mistake? The answer is yes. The first problem must be mentioned with Windows workstations is permissions, licenses and licenses. This is when we cannot access the server, or we cannot access resources even though we are logged into the server.

When encountering this problem, we need to change some configuration. There are some things that we need to pay attention to. First, the Windows system forces us to change passwords periodically. In other words, after an unused period, some accounts become obsolete or forget their password. If this happens we can fix it ourselves instead of asking the admin. We only need to access the account and log in the information in Windows to reconfigure the necessary items. In addition, we may be using a working group without centralized source access control and having to log into multiple systems just to use one resource. Workgroups cause a lot of problems for this reason, so we should not use a workgroup with a network of 10 or more computers.

If you can log in and check, we can use Windows Event Viewer to detect errors in the network. Failure to access resources over the network is a common mistake and can be easily overcome by a more appropriate structure, or a plan to restore forgotten login information.

3. Network performance

Perhaps this is the most common incident. With Windows operating systems, there are many good weaknesses that affect performance. For example, if we configure a computer without taking into account the applications that will be operated over the network. The most common applications often require a

relationship between the client and the server, which means that the workstation installed on the Windows desktop must communicate and transfer data over the network to operate. If the network performance is affected, it is because the network is too slow, or the application has not been deployed to the network. Fixing this kind of problem is quite complicated, usually we have to analyze it carefully and need to use a tool like package analyzer.

The problem of speed and latency may be due to slow connections, or because a network loads too much data. For example, if using a gigabit Ethernet card for servers, cable connections will speed up to 1000 Mbps. Some users are unaware that switching to Wi-Fi will have a significant impact on network communication because many home Wi-Fi systems will not have transmission speeds greater than 100 Mbps.

Also, using an access server instead of a network switch can cause big problems with speed and latency. The use of non-hierarchical structures in which the main component of the network operates at the highest speed and the access layers in this main component operating at a slower rate may create bottlenecks. Two-way settings and unmatched speeds on NIC cards are also common causes of network performance problems. And using a converter to create a loop may cause the network to crash completely.

Windows home users always face Internet problems. If you have checked hardware and software that we cannot fix these problems, it may not really be a problem. Sometimes, problems arise from the provider's service. In those cases, we need to contact the supplier to find a solution.

Other issues affecting network performance are security issues that prevent access to resources, or make services inoperable.

The Internet browser application may also cause problems especially when infected with a virus or the settings in this application have blocked the page being accessed. For example, in Internet Explorer 8, if we use all security settings, such as a Phishing Filter, the time it takes to determine the page will increase and as a result slow down the session. counter. There is also a reason when people blame the network when something goes wrong, because that's always the obvious. However, in reality, the network is just one of the many causes of the problem, in which system resources, through communication, . can cause the network to be slow. As we operate many applications and services through a link that cannot be processed, the system will freeze if those applications respond poorly.

2. Problems with TCP / IP and other protocol issues

There are many reasons why the protocol becomes a problem in the network, these issues include: ISP protocol issues, DHCP, APIPA, DNS, IP address and use of a protocol other than TCP / IP in the network. We can solve TCP / IP related problems by:

Using a updated network topology, although the network has only a few computer systems. Using graphics is useful when troubleshooting network problems, or you can easily add a new server to the network without causing problems. Even if we use DHCP, we need to consider using IP tools like tracert, netstat, ping and pathping, and there are many other tools that we can use when troubleshooting other problems.

If you have not configured a network protocol, you cannot communicate over the network. There are many protocols in TCP / IP, such as DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System) which are the culprits that often cause connectivity problems, as well as network performance problems. For example, if the workstation cannot connect to the server that provides it for the IP address, the workstation will be disconnected from the network. If this problem occurs, APIPA (Automatic Private IP Addressing) will give this workstation a different IP address (possibly not routing or not routing in the network) which will cause many troubles. Workstations always try to connect. If a physical connection (such as a cable and a power source) is disconnected, or the system cannot be logged on or the network is available, or the protocol is incorrectly configured, we will not be able to connect or connect limit.

DHCP can cause some performance problems if the clients cannot determine the server to get the IP address. What DHCP must handle is a DNS server address for disconnected workstations, and these workstations will have to search the server list to find a suitable server. This process raises some network performance issues. It is difficult for us to find out the cause of DNS failure if we do not understand its working method on the system. Suppose we want to access quantrimang.com.vn page, the workstation will need a IP address to communicate with ISP. In addition, it needs to know which DNS server contains information about quantrimang.com.vn website. If these servers do not allow access, or there is a problem with this page, then we can implement the following two methods to overcome this problem. First, configure another DNS server to troubleshoot problems for ISPs. For example, we can open the Command Prompt and then use the nslookup command to find the current DNS settings. If you are connected to the Internet, the ISP will send this information from a DHCP server. If the ISP then changes the DNS server, the client will not be able to respond to that information until the connection session ends, or we make a new connection. In addition, we can use the nslookup command to change the primary DNS to use and test another DNS to see if the DNS server has a problem.

Dynamic DNS is also the cause of network problems if we configure it incorrectly.

1. Common security incidents

The most common network problem with Windows clients is due to the poor services and features of security applications. In fact, all infections come from inside the network, or through Wifi connections when not using security tools to control, monitor and block Wifi. However, this does not mean that the PC or router cannot be secure. Currently, most hardware and software are integrated with some security support. Routers today function as a firewall, IDS (intrusion detection systems), and provide many detailed records of data transmitted through it. Intrusion is a common form of attack. That's when someone connects to your Wifi network and access resources in it.

Security for Wifi networks is not simple. Some of the previous tools like WEP keys are very easy to overcome. In addition, another popular method is to use the workstation's MAC addresses in the access point list to allow only some users. However, if there is no additional security measure for the system, there is no guarantee that this method is completely secure.

Whether we choose to use Windows Firewall or some third-party software, we should consider using a tool as a basic method to protect the server. Network intrusion detection tools can help secure data and prevent what signs of tampering.

If the router being used has a firewall capability, we can use it to create log files that can monitor what is happening on the network. Firewall systems such as Windows Firewall can also perform this function on the server.

Antivirus software (as well as Network Access Protection or NAP) can be used to reduce performance and connectivity issues. Currently most types of viruses and worms often attack networks and servers.

Care should be taken to check and monitor security tools when implemented. If you do not often do this, it is best to use a number of different tools (Defense in Depth - use multiple security tools simultaneously), then check the logs when a problem occurs.

Conclude

The above are the 5 most common network problems with Windows clients. The purpose of the article is to provide some information about the causes and remedies. As we can see, working on the network always has many problems and risks, from slow connections to becoming victims of an attack. Perhaps it is

impossible to avoid incidents with the network, but if we recognize the cause of these incidents, we can minimize their impact.

Operating System

An operating system, or "OS," is software that communicates with the hardware and allows other programs to run. ... Every desktop computer, tablet, and smartphone includes an operating system that provides basic functionality for the device. Common desktop operating systems include Windows, OS X, and Linux.

The operating system manages a computer's hardware resources, including:

1. Input devices such as a keyboard and mouse
2. Output devices such as display monitors, printers and scanners
3. Network devices such as modems, routers and network connections
4. Storage devices such as internal and external drives

How to troubleshoot operating system problems and tools used

BSOD

The blue screen of death is a Windows stop error that clearly points onto hardware malfunction or spoilt device drivers. One may decide to start in safe mode or carry out some System Restore.

Failure to boot

Failure of one's computer to boot can be as a result of a corrupt operating system or some possible changes in one's system's boot order. One can go to the BIOS setup and try to look at the boot sequence. If that does not work, then one should consider reinstalling the Windows operating system since the problem could be far much serious.

Improper shutdown

At times, one's computer may shutdown improperly due to instances of power loss or crushing. In case of such an incidence, restarting the computer might not take one directly to Windows and therefore one should run Windows Error Recovery which automatically checks the file system and drives for any problems. With that, all system files are placed in their right positions and Windows now starts without any problems.

Spontaneous shutdown/restart

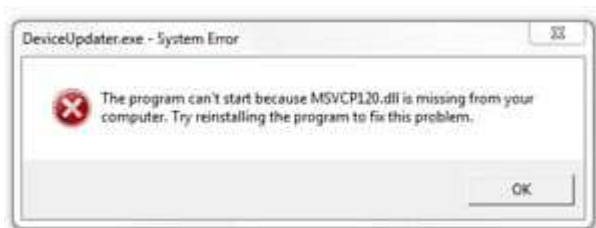
This is a problem that mostly occurs in instances where one's computer keeps looping over the start-up process where it appears to be starting and then restarts. In such a case, the first step should be to try and establish the occurrence point of the problem either in the course of the BIOS check where the Power on Self-test is undergoing among some other possible reasons. Once that is established, then one can easily decide if the problem is hardware related or related to the Windows configuration.

RAID not detected during installation

This is an error message that tends to appear when one are installing an operating system and some of the files required are not found. In such a case, one might open the registry in safe mode to check for the files or restart the installation process with a new installation media.

Device fails to start

Failure of one's device can be very frustrating. In most cases, it normally results from a computer crash or some other hardware related problems. In such a case, try to carry out hardware diagnostics so as to try and establish the problem. One can also decide to boot the computer from a Windows installation media to try and get one's computer to restart.



Missing dll message

The missing dll message mainly appears when the dynamic link libraries are missing. This could be as a result of using many third party applications leading to much redundancy in all the applications. DLLs have many different versions and therefore a lack of update can lead to such a pop-up message. Overwriting older versions with new versions can be very dangerous since there can be some possible malfunction.

Services fail to start

At times, starting one's system might become a problem due to the fact that one can receive a pop-up message informing one that there is a failure in the starting of one or more services. Since it is very difficult to establish the problem, some information should be collected. One can manually start services at the Windows services so as to see if any of them will fail.

In addition to manually starting the services, try to look at processes the services depend on since the process may have to start so that the service can also begin running. One might also need to install a special type of software that will manage the service, rebuilt it and reconfigure it so that every inch of that service starts properly.

Compatibility error

The Windows operating system compatibility error mainly appears when some of the old application versions are not working properly after a windows upgrade. In such cases, Windows has an in-built capability that allows one to change the compatibility of the applications. One can also choose to run the program in its compatibility mode so as to choose the most appropriate operating system for the application. In some cases, the old and out-dated applications can also run in a new version of Windows as long as they are in their compatibility mode.

Slow system performance

A slow system performance is a problem that can be fixed by making sure that one has installed the latest versions of all items running in one's computer system such as the operating system, drivers and applications. All security patches should be up to date and all Windows updates should be functional. Slow system performance could be as a result of some in-built configurations such as running the CPU slowly when on battery and not on power. Malicious software could also be a cause of slow system performance hence a computer scan can be very essential.

Boots to safe mode

The safe mode boot option is one that is usually available prior to starting the operating system. When one presses F8, one receives a menu of advanced options from where one can choose to boot one's computer in safe mode. By using the safe mode boot for one's operating system, one should be in a position to enable network drivers among some many other functions. In addition, booting through the safe mode may not boot the desktop but takes one directly to the command prompt rather than heading to the graphics display.

File fails to open

In a Windows operating system, all files normally have distinct file extensions such as .docs and .ppt. A file with a specific file extension can only be opened by an application designed to open it. Trying to open a file whose file extension is not compatible with a certain program can result into an error message of the file failing to open. Installation of the specific application to open specific file extensions can be a solution. In other cases, some modifications can be made on the applications inside Windows.

Missing NTLDR

Missing NTLDR message is one that is very common on older versions of Windows such as the Windows XP operating system. NTLDR files are very crucial and highly important boot files for one's computer and their deletion means that one's system will not start. To deal with this, one should start the computer with a boot disk so that one can copy back the deleted files onto the hard drive, then carry out a system restart and the Windows operating system begins to run.

Missing Boot.ini

The missing operating system message mainly appears in instances where one is trying to access a drive that is configured as a boot device but with the absence of a boot loader in one's computer. With such an error message, one may need to get into the recovery console environment and run the check disk command to check if the OS is in one's computer. In other case, one should only carry out updates on the Master Boot Record and everything gets right on track.

Missing operating system

When the operating system isn't installed or it is corrupted, then this message appears and this message indicated that one has to do something about the installation of new windows.

Missing Graphical Interface

The missing graphical interface normally results into a dark screen that appears in instances where Windows does not start up. User interfaces and login screens are absent and therefore there could be a problem with the video system. One should try to update the video driver or start the system in graphics mode for lower resolution graphics so as to get to a point of loading the new drivers.

Graphical Interface fails to load

The graphical interface probably fails to load due to the absence of the necessary graphics drivers or a problem with the video hardware. In such a case, try updating the video drivers or install a new version of the drivers.

Invalid boot disk

The invalid boot disk error message mainly appears when there is a problem with one's operating system's boot order. On receiving such a message, make sure that no USB device is plugged in since the BIOS might be configured to boot from external USB devices instead of the local drive. In addition, one can make modifications onto the BIOS configuration so as to modify the devices that should boot first on one's

computer.

Tools

Here are the tools used for the fixation;

Fixboot

Fixboot command is used when one want to create a new boot sector for the operating system. By using this command, one might want to write some new booting sector in a particular partition. When using this command, one might also require using the DISKPART command so as to identify the part or section of the disk onewants to write the new boot sector.

Recovery console

This is a powerful troubleshooting tool that gives one the mandate to change things on the operating system without having to start windows. It is however a very dangerous commands to use. This is a command that gives one complete control of the operating system in such a manner that one can make changes to it before it starts.

Fixmbr

The Fixmbr command is one that one can access from the command prompt. This is a troubleshooting command that one should use when the need to build another Master Boot Record arises. One can also make changes on the drive's configurations, repartitions and reformats.

Sfc

The SFC operating system troubleshooting tool is one that one should prior to using one's system again in case one have ever been a victim of malware infection or hard drive corruption. This is the System File Checker command which is able to carry out integrity scans on all the system files so as to check the validity of the operating system files. In case some malware infection replaced or brought about some damage to one of the system files, the System File Checker will identify it and prompt one to recover the file so as to put the appropriate one in place.

Repair disks

The system repair disk is a troubleshooting environment that is available for windows where onereceives the option to create a system recovery option, backup and restore options. There are many options normally available in this such as repair/start-up, system restore, image recovery among many others. In the repair disk option, one can also launch the system recovery options and commence all one's troubleshooting.

Pre-installation environments

The pre-installed windows environment is an option that is mainly used when going through some recovery options or when setting up windows vista and 7. This is an environment where the desktop is usually unavailable. One can easily come up with one's own windows pre-installation environment. In addition, some of these PE tools can be downloaded and burnt onto a DVD ROM hence no need to come up with one.

MSCONFIG

The MSCONFIG troubleshooting tool is an acronym for the Microsoft System Configuration Utility. This is a troubleshooting utility that one should use in instances where one's operating system is experiencing start-up problems, if the desktop is not loading or some possible malfunction of some applications. With this utility, one are in a position to carry out some diagnostic activities through which all processes are broken down so as to establish where the problem is. This is a utility that gives one the ability to control all the boot process activities such as enabling and disabling the loading of some applications. In addition, one can make modifications and changes to some operating services if onedoes not want them to load when the operating system starts.

DEFRAG

The DEFRAG tool is another important operating system troubleshooting tool. This mainly stands for defragmentation which means putting files and folders in a proper order. Through defragmentation, one is able to bring many split files into one location for continuous viewing. This is a troubleshooting tool that one should use when one are encountering problems with accessing hard drive files especially if the files are stored in different locations on the hard drive thus making the process of reading each file a challenge. This is a process that one can set to occur automatically using the task scheduler.

REGSRV32

The regsvr32 also known as the Microsoft Registry Server is a troubleshooting utility that tends to alter contents of the registry. With this application, one can easily make some DLL registration in addition to deregistration from the operating system. The Microsoft Registry Server performs registry updates when one are troubleshooting problems related to dynamic link libraries that are used by the Windows operating system. . Once it updates, it informs the operating system of the DLL's location, its version among other information required by the application so as to use the dynamic link library.

REGEDIT

With the computer registry being an important aspect of the operating system, it is one of the most important places one should not miss when carrying out operating system troubleshooting. This is because it is in the registry where much information concerning applications, system configurations, services and running drivers is stored making it a very large and important database. In the registry, there is a program known as regedit or Registry Editor where one can gain full access to edit registry information. One can back up registry information, add keys and also delete keys.

Event viewer

The event viewer is somewhat a special troubleshooting tool in that it is the one that enables one to see activities that are happening simultaneously in the OS. Since it's very difficult to establish all that's happening in the OS, the event viewer is a place where one are able to see all that's happening in the operating system. For instance, one may have a driver that is not properly functional and one can easily view it at the event viewer. The event viewer also keeps track of information on activities that occurred some period ago.

Safe mode

The safe mode boot option is one that is usually available prior to starting the operating system. When one presses F8, one receives a menu of advanced options from where one can choose to boot one's computer in safe mode. By using the safe mode boot for one's operating system, one should be in a position to enable network drivers among some many other functions. In addition, booting through the safe mode may not boot the desktop but takes one directly to the command prompt rather than heading to the graphics display.

Command prompt

The command prompt is considered to be one of the most powerful OS troubleshooting tools. The command prompt is a platform that can be accessed without necessarily having to start the operating system. In Windows XP version, one can access it from the installation media while in Windows 7 and Vista one can use the system recovery options to get to the command prompt. In the command prompt, one can make modifications to the operating system only if one is conversant with the modifications one is making. It can be very dangerous to go to the command prompt, make some alterations on operating files or even delete them and then recovering them becomes a problem. Through the command prompt, one has complete control of the operating system since one can replace OS files and move them around since the OS is not yet booted.

Emergency repair disk

Emergency repair disk should be carried out when there is an urgent need to carry out diagnosis on a drive that is not properly functional. One should use the system recovery option or repair disk option for this.

Automated system recovery

An automated system recovery can be induced by running one's computer in safe mode and then selecting the system recovery option and the operating system moves to a specific restoration point.

Generally, troubleshooting of operating system problems is an easy activity only when the right troubleshooting tools are used. It is therefore important that one is familiar with all the troubleshooting tools.

Memory (RAM)

RAM or Random Access Memory is the main memory of any computer. The main work of RAM is to store temporary data for the computer. Many people mistake RAM for permanent data storage. But, it is actually temporary data storage. All the data in RAM is temporary.

RAM is a very important component of your computer. You can ignore your broken Smartphone screen for a long time. But, you simply can't ignore your computer RAM. It also has the highest failure rate among all other computer components. If your RAM is not working properly, then apps won't run smoothly on your computer. Your operating system will work very slowly. Also, your web browser will become slower. It will take more time to open. But, most people don't know if their computer is suffering from any RAM problem. Some common symptoms of a RAM problem are:

1. Diminishing Performance of your System

If your computer performance is diminishing over time, then your computer probably has memory issues. Your computer will boot up at a normal speed. But, after using it for a while it will become slow. This problem mostly happens due to slow **RAM**. Try using heavy apps like Photoshop or play heavy games like PUBG. If your RAM is not working properly, then you will see a sudden decrease in the performance of your computer.

Sometimes these problems arise due to leakage of memory also. Thus, many people don't know how to test this problem. One thing you can do is restart your computer. But, this time don't open any apps on

your computer. If you are facing similar problems without any software running, then your RAM is facing some problems.

2. Frequent Crashes

Your computer can crash due to many reasons. But, it is important to pinpoint the exact reason. If these crashes are occurring randomly, then your RAM is facing some problems. For example, if your computer is crashing on opening heavy apps, then your hardware is probably failing. But if these crashes are occurring without any prior warning, then your RAM is not working properly.

3. Corrupted Files

If you are suddenly seeing your data files getting corrupted, then your system is suffering from RAM problem. This problem will only accelerate in the future. You will start seeing more and more files getting corrupted. Hence, this problem will only get worse with time. The main reason behind this problem is that your RAM is changing your hard drive structure. It is degenerating old files in your hard disk. Soon your computer won't boot once your main drive files get corrupted.

4. Video Card is not loading

If you've ever turned on a computer, then you must have heard a loud beep. This loud beep indicates that your computer has recognized your media and video hardware. If you don't hear this beep during the boot process, then your computer is suffering from RAM problem. Your operating system will also show you an on-screen message after the booting process.

If your computer is only suffering from this problem, then there is no guarantee that your RAM is malfunctioning. Sometimes these problems can occur due to corrupted video cards. On a Mac computer, a triple loud beep during the startup signifies that a RAM problem has occurred.

5. Incorrect RAM Display

You can easily check the amount of RAM in your system.

If you are using Windows, then you can follow below steps to check the RAM of your system:

1. Open Control Panel in your computer.
2. Navigate to the System section of Control Panel.
3. You will see the amount of RAM installed in your systems.

If you are using Mac, then you can follow below steps to check the RAM of your system.

1. Click on Apple icon and after that open click on the about this Mac.
2. After that, click on the Overview tab.
3. You will see an overview of your Mac stats, including the amount of RAM installed in your system.

If your system is showing less RAM, then your laptop computers might have memory issues.

6. Your system will freeze

If your windows computer is freezing for minutes at a time, then your system might be facing RAM problems. It may take even 3-4 minutes to open a browser like Chrome. This problem might be occurring due to malware or virus. Thus, first, you should check your computers with antivirus. If this problem still persists, then your RAM is probably facing problems.

What Causes RAM Problems?

- Sometimes power surges can damage your computer components like RAM or hard disk. Make sure to plug your computer into a surge protector. This will protect your cheap computer components from getting damaged.
- Even excessive heat can damage your computer components. Sometimes individual components can overheat, or even heat from other components can cause damage to other components.
- If you have accidentally restarted any computer part, then it may cause damage to your RAM due to excessive heat.
- Sometimes your memory module may have a fault that slipped through quality control. These errors can get worse over time. This is the most common reason behind a damaged RAM.

Even if one or two memory slots on your motherboard are not working properly, then it will hinder your RAM performance. This can also damage your memory stick in the long run.

How to Diagnose RAM Errors

There are various methods using which you can diagnose RAM problems. If you think that your computer is facing some memory problem, then you can follow the below methods to make it clear:

- The easiest way to Diagnose RAM Error is by using the Windows Memory Diagnostics Tool. It is provided by Windows. First, open Control Panel in your computer. After that, search for Windows Memory Diagnostic and open it. You can run the test immediately by restarting your computer. At the bottom of the screen, you'll see a Status field. If any problem is detected, then you will see it in the Status field.
- If you have two memory sticks, then you can take out one stick of RAM at a time. This is the ideal method to check for memory problems. After removing one stick, you can restart your computer. If your computer is working properly, then one of your RAM stick is not working properly. You can get it replaced.

If your computer is suffering from memory problems then you should check your RAM sticks for dirt. Most times your RAM stops working due to excessive dust. Hence, it is a good idea to clean your RAM every once in a while. If the problem still persists, then you should take professional help. You can get your RAM replaced in around \$75. Sometimes the problem is with RAM modules. In such cases, it is always good to take professional help.

Server:

What is server problem?

The biggest problem that can affect a server is a total crash. A physical problem such as a fire or flood might cause you to completely lose your server. A cyber attack may cause your server to shut down completely. Hardware and software failures can also lead to a full shutdown.

Common Server Errors And How To Fix Them

Whether you're experiencing slow-loading web pages or your site has completely crashed, server errors can be disastrous to your business. If your clients are unable to access your website, they'll quickly move on to one of your competitors, leaving you with a loss of revenue and a potentially damaged reputation. All of the interruptions to the working day may also lead to your employees feeling demotivated and being less productive. You need to ensure you can rely on your network in order for your business to perform well. So we've listed some common errors of servers and server rooms, as well as how you can solve them.

Server Errors That Can Affect Your Website

Having a managed host run your web services is an effective way to prevent common server errors. That way, if something bad happens, you'll have a dedicated team on hand who will be able to resolve any issues before they take effect.

Here are some common server errors that affect websites:

- **Slow page loading**

If it takes longer than three seconds for a webpage to load, more than 50 per cent of users admit to abandoning it in favour of a competitor. There are many factors that can cause slow page loading, including site usage, complicated forms, image rendering, videos that play automatically as well as the user's own web browser. One way you can combat this and keep people returning to your site is to invest in the support of a dedicated managed web service. That way your website will have round-the-clock protection.

- **Viruses and cyber attacks**

With cyber attacks and computer viruses more rife than ever these days, it's vital that your business devises and implements a security policy. You'll need to ensure you go the extra mile to protect your customer's data, otherwise you risk damaging your reputation as well as losing significant revenue. Have a process in place to protect against the loss of customer's personal details as well as payment information.

- **High traffic**

A high volume of traffic to your website is usually a good sign, pre-empting an increase in revenue and sales for your business. Sometimes though, a sudden spike can cause your site to crash, leading to customers experiencing issues with accessing your site. This is more common during events such as Black Friday and Cyber Monday but it's something to be aware of. Employing a dedicated managed hosting provider will allow the impact of high levels of traffic to be controlled. Your dedicated team will also be able to make slight changes to your site to resolve any issues.

- **Hardware or software failure**

All businesses are likely to encounter problems with hardware or software at some point –and when such issues arise, you'll want to ensure your website is back up and running in as short a time as possible. A combination of a fully managed solution and a state-of-the-art data centre can help with this.

- **Site outages**

The biggest problem you'll potentially encounter with your server is a complete site outage. From physical causes (flood and fire) to cyber attacks, hardware or software failures, a website crash could leave your site unavailable to users for quite some time. Significant downtime incurs huge costs for businesses – even more so if the majority of your revenue comes from online sales and services.

How to troubleshoot common server errors

Before tackling server errors, it's a good idea to check your PC's overall health, and use software such as CCleaner to clean and optimise your computer.

Set up weekly automatic scans to run and repair issues affecting your computer's performance and health to keep it running smoothly and problem-free. Here's an easy step-by-step guide to doing this:

1. Download a PC repair and optimiser tool such as WinThruster
2. Click *start scan* to discover registry issues that may be causing problems
3. Click *repair all* to fix these issues

Now it's time to tackle any server errors. Here's what you may encounter and how to fix it:

- **404 error**
 - **Problem:** page not found, indicating a problem with the server due to broken or dead links
 - **Solution:** reload the page and check you typed in the correct URL, try to access the homepage, try using a different browser, clear your browser's cache memory and cookies
- **400: Bad Request**
 - **Problem:** either the server couldn't process your request or the website you're looking for is down
 - **Solution:** check the URL is correct or use another browser. Alternatively, the site might be temporarily down – wait and try again later
- **408: Request Timeout**
 - **Problem:** if the website is taking too long to respond, the server will stop trying and display a 408 error
 - **Solution:** check your internet connection as it may be lagging temporarily. Wait and try again in a few minutes
- **401: Unauthorised**
 - **Problem:** webpage requires authentication
 - **Solution:** log into the website and try again
- **502: Bad Gateway**
 - **Problem:** two servers are unable to communicate effectively
 - **Solution:** try using a different web browser, clear your browser's cache or cookies to remove any corrupt files
- **403: Forbidden**
 - **Problem:** you do not have permission to access the webpage
 - **Solution:** try logging in to see if that works

Common server room problems

Sometimes, server errors can happen in the server room. Here are the most common errors to watch out for:

- **Temperature is too hot**

It's vital that the server room is temperature-controlled. You'll need to ensure the air surrounding your hardware is between 68 and 72 degrees to prevent damage to the servers. Don't forget to take outside temperatures into account too, such as direct sunlight. Servers also generate heat so it's important that you have adequate cooling measures in place.

- **Insufficient ventilation**

In addition to temperature control, you'll also need to account for sufficient space around each piece of equipment to allow the air to properly circulate. If ventilation is poor it can lead to inadequate cooling. For small server rooms, make use of dedicated server racks to stack up your servers.

- **Poorly controlled humidity**

Pay attention to the humidity level in your server room. High levels can cause rust, corrosion, fungus and short-circuiting. Too little moisture can be equally as problematic, potentially leading to electrostatic discharge which in turn causes damage to the system. Be sure to position your servers away from pipes in the building just in case they spring a leak.

- **Vibrations and jostling**

Many environmental hazards can affect your server functionality, resulting in data loss. Whether your hardware is subject to scratches, jostling or vibrations, all of these factors can lead to issues. It's a good idea to keep any servers away from busy hallways or outside walls to reduce the impact of these factors.

- **Clutter**

A tidy, orderly server room is essential for reducing risks. Make sure all cords are kept untangled and keep wires neat so nobody will trip over them. You can use a power distribution unit to help you with this.

- **Power outages**

Keep a UPS (uninterruptible power supply) or a standalone generator as handy power backups in the event of a power outage. Most of the time server functionality will be restored with a full system reboot but if

that doesn't work, it's helpful to have a backup plan in place. Be sure to monitor and test those systems regularly to ensure they're fully functioning. Look out for depleted batteries, failure to start or low fuel levels.

- **Intentional acts**

A breach of security can lead to problems with your server. You'll need to ensure physical and digital means of protection are put in place to prevent disgruntled employees from accessing the server room as well as to reduce the likelihood of a cyber attack on the system. Install security cameras outside the server room and fit combination code locks on the server room door as well as on server racks.

- ✓ **Network operating system (NOS):**

A network operating system (NOS) is an operating system that manages network resources: essentially, an operating system that includes special functions for connecting computers and devices into a local area network (LAN).

- ✓ **System Clock**

System Clock is an electronic device in a computer that issues a steady high-frequency signal that synchronizes all the internal components; is A time-of-day clock in a computer system.

Reasons why your computer clock falls behind

As with many PC issues, there is rarely a single possible cause for each error. For that reason, it is important to keep an open mind and investigate all possible angles.

Indeed, some people often find that a problem goes away for a short time, only to crop up again. This proves there would likely be an underlying problem you may have yet figured out.

Dead CMOS battery

The time and date settings for all PCs are stored on the CMOS chip that is fixed to the PC's motherboard. These settings are part of the BIOS, which also define the relationships between all the peripheral devices connected to your computer.

The BIOS checks all system configurations, including the date and time before it can even load the Windows OS.

The CMOS battery uses a small battery so the BIOS settings remain active when the PC is switched off. This battery usually runs for between two and 10 years before it needs to be replaced.

So, if your clock can't seem to keep the correct time and the PC is fairly old, there is a strong chance the CMOS battery may be failing. The clock essentially stops the point you switch off the PC.

Wrong or corrupted BIOS settings

Even after replacing your CMOS battery the clock may still display the wrong time, especially on startup. You may want to check if the CMOS chip is getting power from the battery.

You could be dealing with a loose battery. A quick fix will be to remove the battery and lift the negative power pin upwards a bit. Also press the positive pin down before replacing the battery, making sure the battery has firm connections.

However, even that may not fix the problem. At this point, the problem could be a result of a corrupted or out of date BIOS. Try resetting the BIOS values, including the date and time settings. Or, if the computer is quite old and does not update automatically, consider installing a more up-to-date BIOS.

Wrong time zone

If your clock is set to the wrong time zone, you will find that, even after correcting the time, the clock will fall behind the next time you boot. Depending on what time zone it is set to, it may even be ahead by a few hours.

Usually, if the clock is set to the wrong time zone, the minutes are usually correct while the hour value will be behind or ahead. Where the CMOS battery is the issue both the hour and minute values are usually wrong.

Remove PC Errors

Run a PC Scan with Restoro Repair Tool to find errors causing security problems and slowdowns. After the scan is complete, the repair process will replace damaged files with fresh Windows files and components.

Disclaimer: to remove errors, you need to upgrade to a paid plan.

Fix PC Errors

Malware infection

Now, this one should worry you. Chiefly because a virus or malware is rarely deployed to just throw your time off. The frequently wrong time and date is often a symptom of a more serious problem. The malware may be targeted right at the BIOS or at the Windows OS itself. Either way, the effect will be damaging.

Now that we are up to speed with what could be causing your PC's clock to fall behind, let's go through the possible solutions you could try to fix the problem.

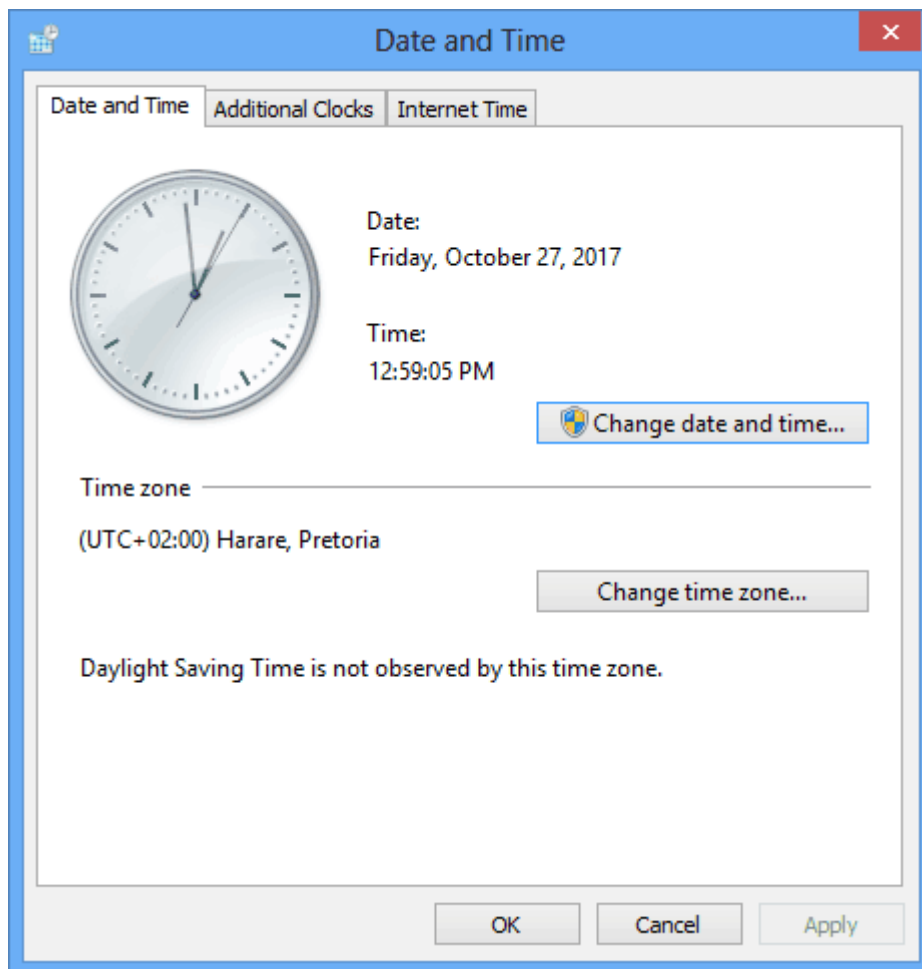
Solution 1 – Synchronize your PC's clock with the default Microsoft Time Server

The best way to set your time on automatic update is perhaps to synchronize your PC's clock with an internet time server. This way, you don't always have to correct your time every time you boot your computer.

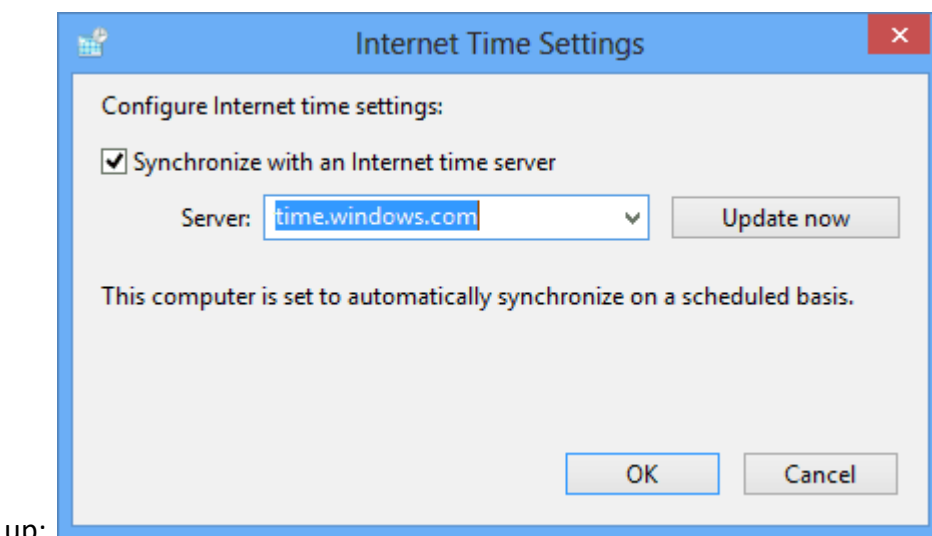
Being a Windows PC, the first option ought to be Microsoft's own time server. Follow the following steps to synchronize your PC's clock and date settings with the Microsoft Time Server;

1. Restart your computer in Safe mode,
2. Click the time tab in the bottom right corner of your screen,

3. Click **Change and time settings...** at the bottom of the pop-up window,



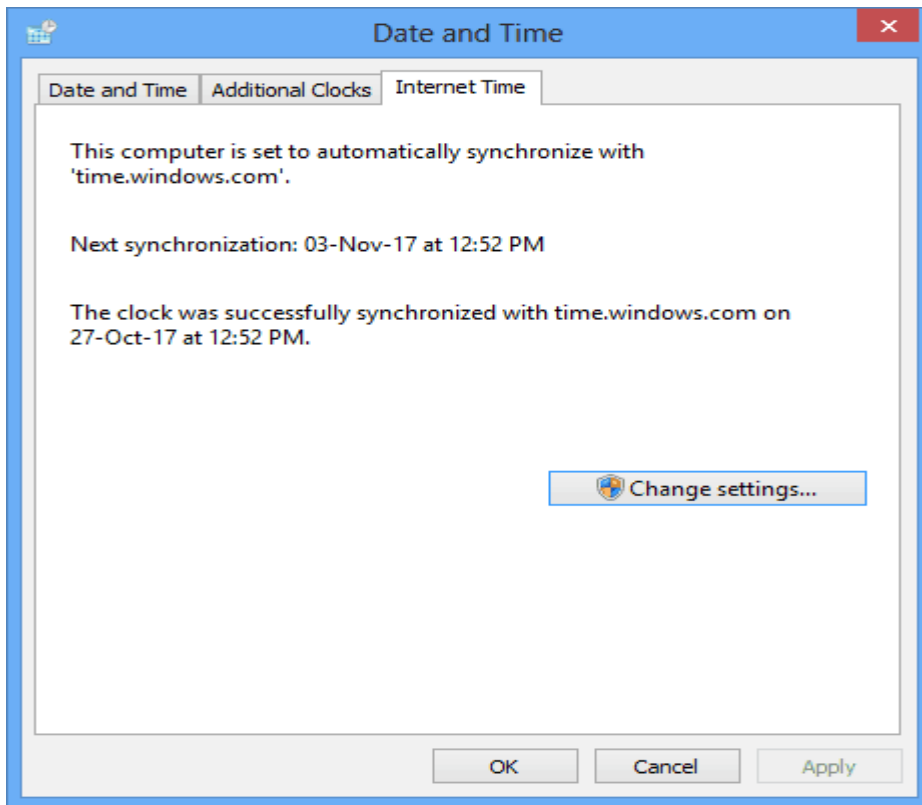
4. Click on the **Internet Time** folder. This small screen will come



up;

5. Select the **time.windows.com** server using the down arrow as shown in the image above. Click **Update now**,

6. After you click **OK**, this confirmation screen will come up;



As you can tell from the image above, this **internet time** is not updated on startup. Rather, the synchronization happens after a set period of time. This is thus not an adequate fix if your PC's time is falling behind or slowing as a result of a dead CMOS battery.

Solution 2 – Update your BIOS

Sometimes an outdated or corrupted BIOS may be the reason your PC's clock is falling behind. BIOS corruption may be a result of improper shutdowns, where you pull the computer from the power source without properly shutting down the PC first. Getting into the habit of doing a proper shutdown should easily fix this issue.

However, in the event your BIOS is now outdated, the only option may be to update. Get in touch with your PC's manufacturer and find out if there is an updated version available. You can also find such information on their website.

Remember resetting or flashing your PC's BIOS so you can correct the time and date settings from there is an option, but it is fraught with risks. This isn't something you should do if you are unsure of what to do. It can easily harm your computer. Consult a professional technician.

Solution 3 – Replace your CMOS battery

Let's face it, if your CMOS battery is now flat, your PC's clock is always going to fall behind. You will have to constantly update it and, at the same time, grapple with all manner of errors. The more permanent fix is to just replace the battery with a new one.

The CMOS's battery slot is normally fitted to the computer's motherboard. But it can be a little tricky to remove and replace the battery on some PCs. If you have one of those computers it is best you take the computer to a repair technician.

However, the CMOS battery is fairly easy to replace on most modern desktop PCs. It is with laptops that the process may get a bit tricky. Just remember to properly shutdown the PC and disconnect it from its power source before you disassemble it. Again seek help from a professional if you are unsure of what to do.

Solution 4 – Clean your computer of viruses and malware

If, after trying all of the above solutions, your PC's clock continues to slow or fall behind, there is a probability your PC may have been infected by a virus. In case you hadn't updated your anti-malware software or installed one, now is the time to do it.

If you had up-to-date security software installed, you may also consider upgrading it. To ensure the malware does not evade your anti-malware software, or launch on startup, start and install the software in Safe Mode.

This way, all non-essential programs, including malware and viruses, don't get to launch. You can then properly scan and clean your PC without interference from the malware.

Microsoft has its own free Malware Removal Tool. But, if you want to go premium, there are several good options you can choose from, including Malwarebytes and others. Otherwise, be vigilant with how you use your computer to protect your it against virus and malware infection.

✓ **CPU Usage:** The CPU (Core Processing Unit) is the brain of your computer.

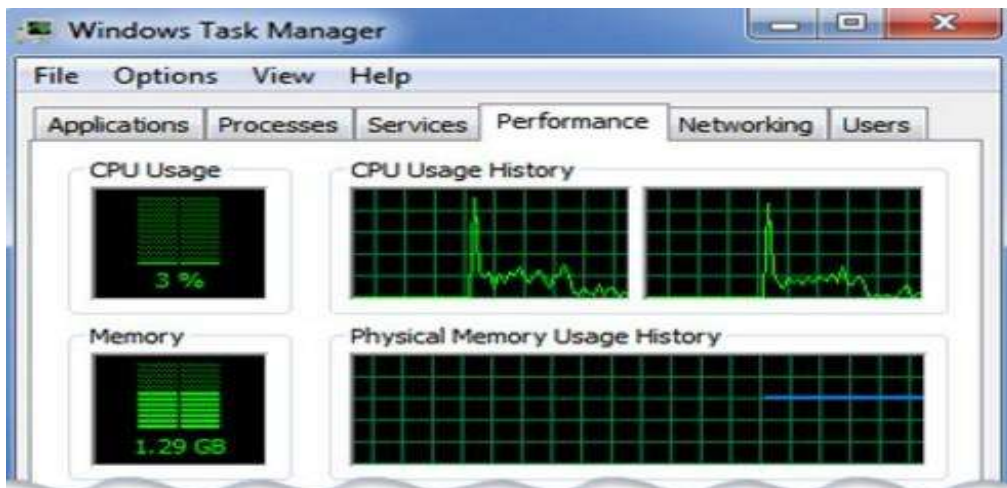
CPU usage refers to your computer's processor and how much work it's doing. A high reading means your computer is running at the maximum level or above normal level for the number of applications running.

CPU usage is a term used to describe how much the processor is working. A computer's CPU usage can vary depending on the types of tasks that are being performed by the processor. CPU usage can be monitored to see how much of the processor's capacity is in use.

Check CPU Usage in Task Manager

Use the Performance tab in Task Manager to view how your computer's central processing unit (CPU) is being used by Windows and other programs running on your computer

1. Open Task Manager by right-clicking the taskbar and then clicking Task Manager.
2. Click the Performance tab.



✓ Hard drive

A hard disk drive (sometimes abbreviated as hard drive, HD, or HDD) is a non-volatile memory hardware device that permanently stores and retrieves data on a computer.

Non-volatile means data is retained when the computer is turned off.

A hard disk drive is also known as a hard drive.

All computers have a hard drive installed in them, which is used to store files for the operating system, software programs, and a user's personal files. A computer cannot function without a hard drive installed, as it requires one to function properly.

❖ Where is the hard drive found in a computer?

All primary computer hard drives are found inside a computer case and are attached to the computer motherboard using an ATA, SCSI, or SATA cable. Hard drives are powered by a connection to the PSU (power supply unit).

❖ What is stored on a hard drive?

A hard drive can be used to store any data, including pictures, music, videos, text documents, and any files created or downloaded. Also, hard drives store files for the operating system and software programs that run on the computer.

❖ What are the sizes of hard drives?

The hard drive is typically capable of storing more data than any other drive, but its size can vary depending on the type of drive and its age. Older hard drives had a storage size of several hundred MB (megabytes) to several GB (gigabytes). Newer hard drives have a storage size of several hundred gigabytes to several TB (terabytes). Each year, new and improved technology allows for increasing hard drive storage sizes.

✓ How to Check Your Hard Drive Usage

Your hard drive usage could be too high and on its way to a crash. Here's how to check if it's working too hard.

Your hard drive is the main storage of your computer. It holds your pictures, videos, office or business software among everything else running on your PC. If you've already scanned for malware, removed unnecessary programs and toolbars, checked your CPU and your memory then it may be time to check your hard drive. Programs malfunctioning in the background can read and write unnecessarily from your hard causing your computer to slow down.



✓ Firewalls And Filters

Firewalls

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely.

Types of Firewalls:Let's quickly discuss the three basic types of network firewalls: packet filtering (stateless), stateful, and application layer.

1. Packet filtering, or stateless, firewalls work by inspecting individual packets in isolation. As such, they are unaware of connection state and can only allow or deny packets based on individual packet headers.

2. Stateful firewalls are able to determine the connection state of packets, which makes them much more flexible than stateless firewalls.

3. Application firewalls go one step further by analysing the data being transmitted, which allows network traffic to be matched against firewall rules that are specific to individual services or applications.

In addition to firewall software, which is available on all modern operating systems, firewall functionality can also be provided by hardware devices, such as routers or firewall appliances..

Firewall Rules

As mentioned above, network traffic that traverses a firewall is matched against rules to determine if it should be allowed through or not. An easy way to explain what firewall rules looks like is to show a few examples.

Suppose you have a server with this list of firewall rules that apply to incoming traffic:

1. Accept new and established incoming traffic to the public network interface on port 80 and 443 (HTTP and HTTPS web traffic)
2. Drop incoming traffic from IP addresses of the non-technical employees in your office to port 22 (SSH)
3. Accept new and established incoming traffic from your office IP range to the private network interface on port 22 (SSH)

Note that the first word in each of these examples is either "accept", "reject", or "drop". This specifies the action that the firewall should do in the event that a piece of network traffic matches a rule.

Accept means to allow the traffic through,

Reject means to block the traffic but reply with an "unreachable" error, and

Drop means to block the traffic and send no reply.

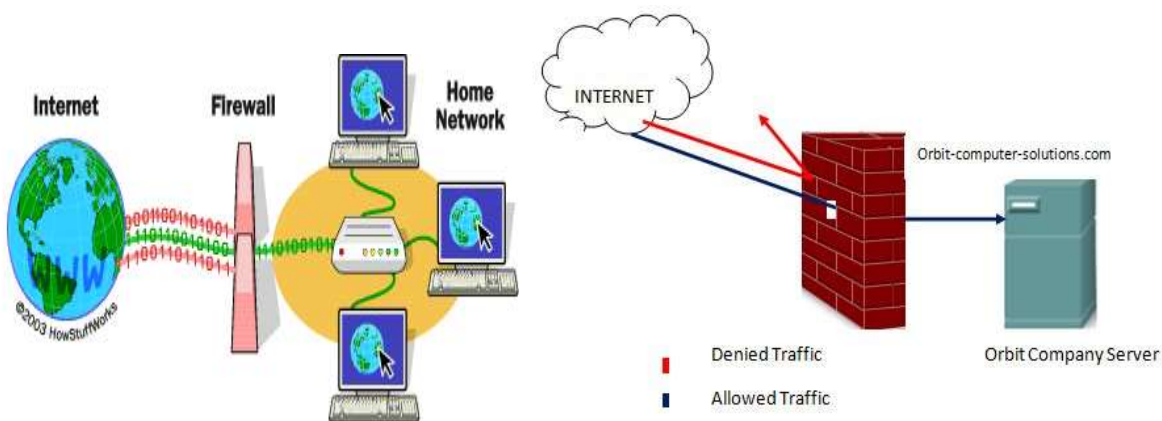
The rest of each rule consists of the condition that each packet is matched against.

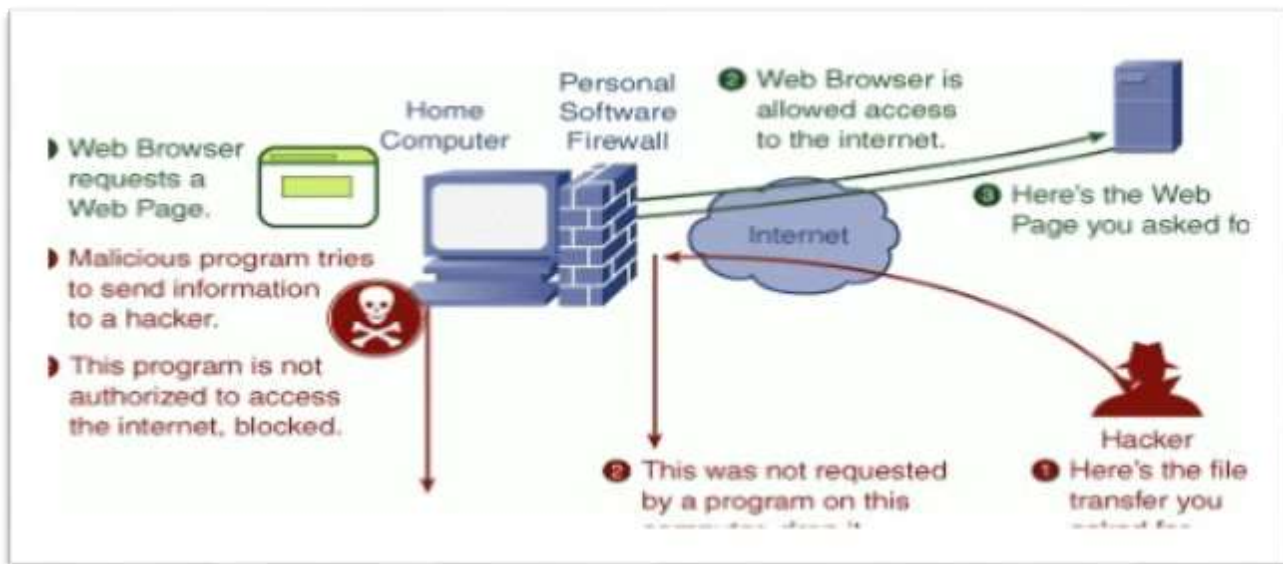
As it turns out, network traffic is matched against a list of firewall rules in a sequence, or chain, from first to last. More specifically, once a rule is matched, the associated action is applied to the network traffic in question. In our example, if an accounting employee attempted to establish an SSH connection to the server they would be rejected based on rule 2, before rule 3 is even checked. A system administrator, however, would be accepted because they would match only rule 3.

What Firewalls Do?

Basically, firewalls need to be able to perform the following tasks:

- Defend resources
- Validate access
- Manage and control network traffic
- Record and report on events
- Act as an intermediary
- Always active connection - means that your computer is vulnerable every time when it is connected to the internet.





How does a firewall work?

To start, a firewalled system analyses network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does this by allowing or blocking specific data packets — units of communication you send over digital networks — based on pre-established security rules.

A firewall works like a traffic guard at your computer's entry point, or port. Only trusted sources, or IP addresses, are allowed in. IP addresses are important because they identify a computer or source, just like your postal address identifies where you live.

What does a firewall do?

A firewall acts as a gatekeeper. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources.

A firewall acts as a barrier or filter between your computer and another network such as the internet. You could think of a firewall as a traffic controller. It helps to protect your network and information by managing your network traffic, blocking unsolicited incoming network traffic, and validating access by assessing network traffic for anything malicious like hackers and malware.

Your operating system and your security software usually come with a pre-installed firewall. It's a good idea to make sure those features are turned on. Also, make sure your security settings are configured to run updates automatically.

What a personal firewall can do ?

- Stop hackers from accessing your computer.
- Protects your personal information.
- Blocks “pop up” ads and certain cookies.
- Determines which programs can access the Internet.
- Block invalid packets.



Firewall rules:

- Determine what traffic your firewall allows and what is blocked.
- Examine the control information in individual packets, and either block or allow them according to the criteria that you define.
- Control how the firewalls protect your network from malicious programs and unauthorized access.

Managing your firewall rules across your devices and throughout your network is critical to network security.

Firewalls weakness / limitations

1. Firewalls cannot protect against what has been authorized
2. It cannot stop social engineering attacks or an unauthorized user intentionally using their access for unwanted purposes
3. Firewalls cannot fix poor administrative practices or poorly designed security policies
4. It cannot stop attacks if the traffic does not pass through them
5. They are only as effective as the rules they are configured to enforce.

Filters

Filters as the name suggests, they filter the frequency components. That means, they allow certain frequency components and / or reject some other frequency components.

Filters are application programs used in a firewall for examining packets on their arrival at the firewall. Filters help with firewall security in that they route or reject the packets based on defined rules.

✓ **Virtual Private Network (VPN) Software :**

Virtual private networks, or VPNs, connect users to private, secure networks. Companies hoping to increase security or restrict user access to sensitive data can utilize VPNs to set up gated, internal networks. Individuals can also use VPNs to secure networks and encrypt certain data (individuals interested should look explore the best free VPN options in 2018. If a company has a large number of users accessing their network remotely, a VPN will ensure no unapproved users have access to data. Employees may connect at airports, hotels, or libraries using unfamiliar and unsecured connections, but a VPN will prevent hackers or other criminals from accessing sensitive company data. These tools also encrypt IP addresses, mask locations, and can bridge connections between devices. These products often contain firewalls to prevent viruses, hacks, and other threats. Many network security packages include VPNs, but offer significant additional functionality and security than a standalone VPN.

To qualify for inclusion in the Virtual Private Network (VPN) category, a product must:

Connect devices to private networks using encryption and security mechanisms

Ensure only authorized access to private networks and sensitive data

Sniff network traffic at the packet level to encrypt data

Route connections to secure networks through tunnelling protocols

Why do you need a VPN service?

Surfing the web or transacting on an unsecured Wi-Fi network means you could be exposing your private information and browsing habits. That's why a virtual private network, better known as a VPN, should be a must for anyone concerned about their online security and privacy.

Think about all the times you've been on the go, reading emails while in line at the coffee shop, or checking your bank account while waiting at the doctor's office. Unless you were logged into a private Wi-Fi network that requires a password, any data transmitted during your online session could be vulnerable to eavesdropping by strangers using the same network.

The encryption and anonymity that a VPN provides helps protect your online activities: sending emails, shopping online, or paying bills. VPNs also help keep your web browsing anonymous.

How a VPN protects your IP address and privacy

VPNs essentially create a data tunnel between your local network and an exit node in another location, which could be thousands of miles away, making it seem as if you're in another place. This benefit allows online freedom, or the ability to access your favorite apps and websites while on the go.

Here's a closer look at how a virtual private network works. VPNs use encryption to scramble data when it's sent over a Wi-Fi network. Encryption makes the data unreadable. Data security is especially important when using a public Wi-Fi network, because it prevents anyone else on the network from eavesdropping on your internet activity.

There's another side to privacy. Without a VPN, your internet service provider can know your entire browsing history. With a VPN, your search history is hidden. That's because your web activity will be associated with the VPN server's IP address, not yours. A VPN service provider may have servers all over the world. That means your search activity could appear to originate at any one of them. Keep in mind, search engines also track your search history, but they'll associate that information with an IP address that's not yours. Again, your VPN will keep your online activity private.

VPN privacy: What does a VPN hide?

A VPN can hide a lot of information that can put your privacy at risk. Here are five of them.

1. Your browsing history

It's no secret where you go on the internet. Your internet service provider and your web browser can track just about everything you do on the internet. A lot of the websites you visit can also keep a history. Web browsers can track your search history and tie that information to your IP address.

Here are two examples why you may want to keep your browsing history private. Maybe you have a medical condition and you're searching the web for information about treatment options. Guess what? Without a VPN, you've automatically shared that information and may start receiving targeted ads that could draw further attention to your condition.

Or maybe you just want to price airline tickets for a flight next month. The travel sites you visit know you're looking for tickets and they might display fares that aren't the cheapest available.

These are just a few isolated examples. Keep in mind your internet service provider may be able to sell your browsing history. Even so-called private browsers may not be so private.

2. Your IP address and location

Anyone who captures your IP address can access what you've been searching on the internet and where you were located when you searched. Think of your IP address as the return address you'd put on a letter. It leads back to your device.

Since a VPN uses an IP address that's not your own, it allows you to maintain your online privacy and search the web anonymously. You're also protected against having your search history gathered, viewed, or sold. Keep in mind, your search history can still be viewed if you are using a public computer or one provided by your employer, school, or other organization.

3. Your location for streaming

You might pay for streaming services that enable you to watch things like professional sports. When you travel outside the country, the streaming service may not be available. There are good reasons for this, including contractual terms and regulations in other countries. Even so, a VPN would allow you to select an IP address in your home country. That would likely give you access to any event shown on your streaming service. You may also be able to avoid data or speed throttling.

4. Your devices

A VPN can help protect your devices, including desktop computer, laptop, tablet, and smart phone from prying eyes. Your devices can be prime targets for cybercriminals when you access the internet, especially if you're on a public Wi-Fi network. In short, a VPN helps protect the data you send and receive on your devices so hackers won't be able to watch your every move.

5. Your web activity — to maintain internet freedom

Hopefully, you're not a candidate for government surveillance, but who knows. Remember, a VPN protects against your internet service provider seeing your browsing history. So you're protected if a government agency asks your internet service provider to supply records of your internet activity. Assuming your VPN provider doesn't log your browsing history (some VPN providers do), your VPN can help protect your internet freedom.

How can a VPN help protect against identity theft?

Identity theft occurs when thieves steal your personal information and use it to commit crimes in your name — like taking over or opening new accounts, filing tax returns in your name, or renting or buying property. A VPN can help protect against identity theft by helping protect your data. It creates an encrypted tunnel for the data you send and receive that's out of reach of cyberthieves.

If your smartphone's Wi-Fi is enabled at all times, your device could be vulnerable without you ever knowing it. Everyday activities like online shopping, banking and browsing can expose your information, making you vulnerable to cybercrime.

A VPN can protect the information you share or access using your devices. That's especially important when using a public Wi-Fi network, where a cyberthief on the same network could capture your login credentials and the credit card number you type in when you shop online.

You can't prevent identity theft. No one can. Some security aspects — like a data breach at an organization where you have an account — are out of your control. But a VPN can help safeguard the information you send from and receive on your devices.

What should you look for in VPN services?

The VPN market is crowded with options, so it's important to consider your needs when you're shopping for a VPN.

Think about what is important to you. Do you want to be able to surf the web anonymously by masking your IP address? Are you afraid that your information could be stolen on public Wi-Fi? Are you a frequent traveler who wants to be able to watch your favorite shows while you're on the go.

A good VPN can help you check all three boxes, but here are some other points to consider.

How to choose a VPN

A smart way to stay secure when using public Wi-Fi is to use a VPN solution. But what's the best way to choose a virtual private network? Here are some questions to ask when you're choosing a VPN provider.

1. **Do they respect your privacy?** The point of using a VPN is to protect your privacy, so it's crucial that your VPN provider respects your privacy, too. They should have a no-log policy, which means that they never track or log your online activities.

2. **Do they run the most current protocol?** OpenVPN provides stronger security than other protocols, such as PPTP. OpenVPN is an open-source software that supports all the major operating systems.
3. **Do they set data limits?** Depending on your internet usage, bandwidth may be a large deciding factor for you. Make sure their services match your needs by checking to see if you'll get full, unmetered bandwidth without data limits.
4. **Where are the servers located?** Decide which server locations are important to you. If you want to appear as if you're accessing the Web from a certain locale, make sure there's a server in that country.
5. **Will you be able to set up VPN access on multiple devices?** If you are like the average consumer, you typically use between three and five devices. Ideally, you'd be able to use the VPN on all of them at the same time.
6. **How much will it cost?** If price is important to you, then you may think that a free VPN is the best option. Remember, however, that some VPN services may not cost you money, but you might "pay" in other ways, such as being served frequent advertisements or having your personal information collected and sold to third parties. If you compare paid vs. free options, you may find that free VPNs:

✓ **Network Adapter/Network Interface card(NIC)**

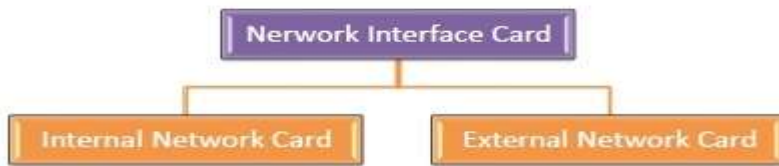
A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

NIC cards are of two types –



Internal Network Cards

In internal network cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).



External Network Cards

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.



- Content/Topic 3: Identification of Network Devices

Hubs, Switches, Routers and Gateways

1. Hub: Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network.

Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as Switches and Routers.

2. Switch: On a network, a switch is a hardware device that filters and forwards network packets, but often not capable of much more. A network switch is more advanced than a hub but not as advanced as a router. The picture shows an example of a NETGEAR 5 port switch.

NETGEAR 5 Port Network Switch



Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network.

- ✓ Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

3. Router: A router is hardware device designed to receive, analyze and move incoming packets to another network.

The picture shows the Linksys BEFSR11 wireless router and is what many home routers resemble.

Linksys Wireless Router



There are two types of Router: **wired and wireless**. The choice depends on your physical office/home setting, **speed** and **cost**.

In the above example, of a home network, there are two different types of a router: the router and the wireless router. In this example:

The router allows all the computers and other network devices to access the Internet.

The wireless router allows a laptop to wirelessly connect to the home network and access the internet as well.

Below are some additional examples of different types of routers used in a large network.

➤ **Brouter**

Short for bridge router, a brouter is a networking device that serves as both a bridge and a router.

➤ **Core router**

A core router is a router in a computer network that routes data within a network, but not between networks.

➤ **Wireless router**

For information on a wireless router (Wi-Fi router), it's like the access point.

4. Gateway

In computer networking and telecommunications, a gateway is a component that is part of two networks, which use different protocols. The gateway will translate one protocol into the other. A router is a special case of a gateway.

Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of the router or switch as it communicates using more than one protocol.

Both the computers of internet users and the computers that serve pages to users are host nodes. The nodes that connect the networks in between are gateways.

These are gateway nodes:

The computers that control traffic between company networks, The computers used by internet service providers (ISPs) to connect users to the internet gateway must be implied on larger networks to interconnect them.

✓ **Network emulators**

Network emulation is a technique for testing the performance of real applications over a virtual network. This is different from network simulation where purely mathematical models of traffic, network models,

channels and protocols are applied. The aim is to assess performance, predict the impact of change, or otherwise optimize technology decision-making.

✓ **Methods of emulation**

Network emulation is the act of introducing a device to a test network (typically in a lab environment) that alters packet flow in such a way as to mimic the behaviour of a production, or live, network such as a LAN or WAN. This device may be either a general-purpose computer running software to perform the network emulation or a dedicated emulation device which usually does link emulation.

It is commonly known that networks are imperfect private or public. They introduce delay, errors and drop packets.

The primary goal of network emulation is to create an environment whereby users can connect the devices, applications, products and/or services being tested in order to validate their performance, stability, or functionality against real-world network scenarios. Once tested in a controlled environment against actual network conditions, users can have confidence that the item being tested will perform as expected.

• **Network Address Translation (NAT)**

To access Internet, one public IP address is needed but as you use private IP address in our private network, translation of private IP address to a public IP address is required.

Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.

✓ **Network Address Translation (NAT) working**

Generally, the border router is configured for NAT i.e. the router which has one interface in local (inside) network and one interface in global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to local (private) IP address.

✓ **There are 3 Types of NAT:**

1. Static NAT – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e. one-to-one mapping between local and global address.

This is generally used for Web hosting.

2. Dynamic NAT – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address.

3. Port Address Translation (PAT) – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address.

Advantages of NAT

- NAT conserves legally registered IP addresses.
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunnelling protocols such as IPsec.
- Also, router being a network layer device should not tamper with port numbers (transport layer) but it has to do so because of NAT.

✓ VPN or Virtual Private Network

A **Virtual Private Network** is a connection method used to add security and privacy to private and public networks, like Wi-Fi Hotspots and the Internet.

The reasons for using a VPN are:

To protect your online information and to visit websites that may be restricted due to your geographic location.

1. Protect Yourself: When left unprotected, your private data, such as bank account information and credit card numbers, can fall into the wrong hands. A good VPN will encrypt your data, so even if you connect to a public Wi-Fi, your private data is guaranteed to be protected.

2. Hide your IP address: Connecting to a Virtual Private Network often conceals your real IP address.

3. Encrypt data transfers: A Virtual Private Network will protect the data you transfer over public Wi-Fi.

4. Mask your location: With a Virtual Private Network, users can choose the country of origin for their Internet connection.

5. Access blocked websites: Get around website blocked by governments with a VPN.

The two most common types of VPNs are:

1. Remote access VPN

Remote access VPN clients connect to a VPN gateway server on the organization's network. The gateway requires the device to authenticate its identity before granting access to internal network resources such as file servers, printers and intranets.

2. Site-to-site VPN

In contrast, a site-to-site VPN uses a gateway device to connect an entire network in one location to a network in another location. End-node devices in the remote location do not need VPN clients because the gateway handles the connection.

✓ VPN software?

VPN software is a tool that allows users to create a secure, encrypted connection over a computer network such as the Internet.

- ✓ **So why use VPN?** Online privacy and security is the most sensible reason for one to adopt VPN software. A key feature of a VPN is its ability to hide your real IP address by providing you with a temporary one. This makes all your online activities a secret, making it impossible to trace your location. This essentially answers the question, what is VPN?

What are the benefits/advantages of using a VPN?

1. Security, security: Your data will be encrypted which means hackers won't be able to access it. If you're using a closed network for work, you can keep it completely private. That means security for yourself, your business and any sensitive materials will stay in your possession. The encryption keeps you and your data safe.

2. Online anonymity: If you want to browse websites in complete privacy, you need to be using a VPN. The VPN acts like a mask to allow you to anonymously conduct your business online. VPN will allow you to access websites and web applications undetected.

3. Remote access to your network: After you've set up your VPN, you can connect to it remotely from anywhere with an internet connection. You can securely log into your network and access the information, documents, etc you need. For business, this will increase productivity. For users who use a VPN for privacy, this means you won't have to send an email or attachment that can be intercepted. You can keep all of your data in a closed network that only you have access to.

4. Share files in your network: This is similar to the last point, but after you've set up your VPN you can access share files with others. That means members of your network will easily be able to access and transfer files among themselves.

5. Change your IP address and the server location: You can change the location of your IP address or “hide” your IP address/location.

6. Performance: Sometimes the servers available to us are not optimal. You might find that connecting via VPN can improve speed and performance as you search the internet. It certainly will be better than a proxy network. VPN services are taking performance very seriously. In the past, VPN’s could be slow, lag and you’d lose connections constantly. New developments have made those inconveniences a thing of the past. And, in many cases, using a VPN can result in better performance.

- **Content/Topic 1: Identification of components, tools and equipment to be used**

- ✓ **Networking components**

Computer networks share common devices, functions, and features including servers, clients, transmission media, shared data, shared printers and other hardware and software resources, network interface card(NIC), local operating system(LOS), and the network operating system (NOS).

Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few. Sometimes it is also called host computer, servers are powerful computer that store data or application and connect to resources that are shared by the user of a network.

Clients - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (users) of the network, as they request and receive services from the servers. These days, it is typical for a client to be a personal computer that the users also use for their own non-network applications.

Transmission Media - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called transmission medium channels, links or lines.

Shared data - Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.

Shared printers and other peripherals - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

Network Interface Card - Each computer in a network has a special expansion card called a network interface card (NIC). The NIC prepares (formats) and sends data, receives data, and controls data flow between the computer and the network. On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.

Local Operating System - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, UNIX, Linux, Windows 2000, Windows 98, and Windows XP etc. The network operating system is the software of the network. It serves a similar purpose that the OS serves in a stand-alone computer

Network Operating System - The network operating system is a program that runs on computers and servers that allows the computers to communicate over the network.

Hub - Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer requests information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Switch - Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port.

Unlike a hub, switch doesn't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights.

Router - When we talk about computer network components, the other device that used to connect a LAN with an internet connection is called Router. When you have two distinct networks (LANs) or want to share a single internet connection to multiple computers, we use a Router. In most cases, recent routers also include a switch which in other words can be used as a switch. You don't need to buy both switch and router, particularly if you are installing small business and home networks. There are two types of Router: wired and wireless. The choice depends on your physical office/home setting, speed and cost.

LAN Cable -A local area Network cable is also known as data cable or Ethernet cable which is a wired cable used to connect a device to the internet or to other devices like computer, printers, etc.

✓ Networking tools

A computer networking tool is any type of software that assists in the creation, maintenance, or distribution of a wireless network. Also, computer networking tools aid in a website's creation, maintenance, advertising, security, and modification. They are responsible for the maintenance of local area networks, especially in situations that involve dozens or hundreds of computers within the same network. Computer networking tools are used for both domestic and commercial purposes and are available on sale or for free. Every software listed in this article is a free computer networking tool that anyone can use for any purpose.

- DNS Lookup
- Email Checker
- HTTP Headers
- IDN and Punycode Conversion
- NS Lookup
- Online Ping
- Spam Blacklist Checker
- Traceroute
- URL Encode and Decode
- WHOIS Search

We've been providing these free of charge for over twenty years, so don't hesitate to take advantage of any of these! If you want to know a bit more about these tools, read on.

DNS Lookup

The DNS Lookup tool retrieves domain name records for the domain name that you provide. You can use this to help diagnose problems and see if the problem originates from the domain name server — if you cannot return a domain's records, you'll know where to begin troubleshooting!

This tool returns only address (A) records. For other types of domain name records, use NsLookup.

NsLookup

The NsLookup tool allows you to provide a hostname and request one or more types of DNS records (e.g., A, NS, CNAME records).

Email Checker

The Email Checker allows you to test the validity and reachability of an email address. It makes sure that the email is syntactically valid and that it is available via an SMTP server. If you're trying to cull false email addresses from your email list or something similar, this tool will be helpful.

HTTP Headers

The HTTP Headers tool allows you to see what headers are returned by a web server for a specific domain name or IP Address. If you notice odd behavior with your HTTP connections, you can use this tool to troubleshoot the top-level domain. Alternatively, you can use it to check for redirection — minimizing these optimizes any links you might be using.

IDN and Punycode Conversion

If you are working with domain names that contain non-English characters, you'll need to convert the domain name into punycode, which can then be provided to the DNS server. In some circumstances, you might need to convert punycode back to the original domain name. The IDN to Punycode and Punycode to IDN tools will help you with these tasks.

Online Ping

To determine if a server is responding to requests, you can use Online Ping. You provide an IP address or a domain name, and you can see if the host is responding or not.

Spam Blacklist Checker

With the Spam Blacklist Checker, you can check to see if a domain name (regardless of whether you own it or not) has been put on a spam blacklist. This can be helpful if you aren't receiving mail or are sending mail that isn't being received by the intended recipients.

Traceroute

If you are curious as to what path your requests are taking, as well as how long it takes to get from point A to point B (as well as intermediary stops), you can use the Traceroute tool. This can help you with things like:

- Determining if there's a specific server (or node) that is slow or unreachable
- Figuring out who hosts a specific resource and where the host is located
- Checking the reachability of your site

URL Encode and Decode

If you need to include special characters in your URL, you'll need to encode them so that the URL remains valid. You can do this with URL Encode. Conversely, if a URL contains special characters and has been encoded, yet you want to see it in a more human-readable form, use URL Decode to standardize the URL.

WHOIS Search

If you are curious as to who the responsible party (or parties) is behind a domain name, the WHOIS query will allow you to query multiple domain registrars' databases. If the owner has chosen to hide their information, you can nevertheless return forwarding information.

✓ **Network equipments**

Networking hardware, also known as network equipment or computer networking devices, are electronic devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network.

There are different types of network devices used in a computer network which include the following.

- Network Hub.
- Network Switch.
- Modem.
- Network Router.
- Bridge.
- Repeater.

LO1.2 Verify network security

- **Content/Topic 1: Verification of network security**

✓ **AUTHENTICATION**

In computing, authentication is the process of verifying the identity of a person or device. A common example is entering a username and password when you log in to a website. Entering the correct login information lets the website know 1) who you are and 2) that it is actually you accessing the website.

While a username/password combination is a common way to authenticate your identity, many other types of authentication exist.

✓ **Importance of Authentication**

Authentication is important because it enables organizations to keep their networks secure by permitting only authenticated users (or processes) to access its protected resources, which may include computer systems, networks, databases, websites and other network-based applications or services.

Once authenticated, a user or process is usually subjected to an authorization process as well, to determine whether the authenticated entity should be permitted access to a protected resource or

system. A user can be authenticated but fail to be given access to a resource if that user was not granted permission to access it.

The terms authentication and authorization are often used interchangeably; while they may often be implemented together the two functions are distinct.

While authentication is the process of validating the identity of a registered user before allowing access to the protected resource, authorization is the process of validating that the authenticated user has been granted permission to access the requested resources. The process by which access to those resources is restricted to a certain number of users is called access control. The authentication process always comes before the authorization process.

✓ **CONFIDENTIALITY**

Confidentiality is the protection of personal information. Confidentiality means keeping a client's information between you and the client, and not telling others including co-workers, friends, family, etc.

Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

Confidentiality is one of the five pillars of Information Assurance (IA). The other four are authentication, availability, integrity and no repudiation.

✓ **Examples of maintaining confidentiality include:**

1. Individual files are locked and secured
2. Support workers do not tell other people what is in a client's file unless they have permission from the client
3. Information about clients is not told to people who do not need to know
4. Clients' medical details are not discussed without their consent
5. Adult clients have the right to keep any information about themselves confidential, which includes that information being kept from family and friends.

✓ **The types of information that is considered confidential can include:**

1. Name, date of birth, age, sex and address
2. Current contact details of family, guardian etc
3. Bank details
4. Medical history or records
5. Individual personal plans

6. Assessments or reports

✓ **NETWORK AUDITING**

Network auditing is the collective measures done to analyze study and gather data about a network with the purpose of ascertaining its health in accordance with the network/organization requirements.

Network auditing works through a systematic process where a computer network is analyzed for:

- Security
- Implementation of control
- Availability
- Management
- Performance

Network auditing is a process in which your network is mapped both in terms of software and hardware. The process can be daunting if done manually, but luckily some tools can help automate a large part of the process. The administrator needs to know what machines and devices are connected to the network. He should also know what operating systems are running and to what service pack/patch level. Another point on the checklist should be what user accounts and groups are on each machine as well as what shares are available and to whom. A good network audit will also include what hardware makes up each machine, what policies affect that machine and whether it is a physical or a virtual machine. The more detailed the specification the better.

LO1.3 Verify network status

- **Content/Topic 2: Verification of network status**
- ❖ Network connectivity verification tools
- ✓ **Ping**

What is Ping?

Ping is a tool that sends test packets through the network to a destination of your choice and measures the response time.

The ping command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

For example, you might find that there are no responses when pinging a network printer, only to find out that the printer is offline and its cable needs replaced. Or maybe you need to ping a router to verify that your computer can connect to it, to eliminate it as a possible cause for a networking issue.

Ping Command Availability

The ping command is available from within the Command Prompt in Windows 10, Windows 8, Windows 7, Windows Vista, and Windows XP operating systems. The ping command is also available in older versions of Windows like Windows 98 and 95.

You can use ping to:

1. Test if your website or web server is reachable

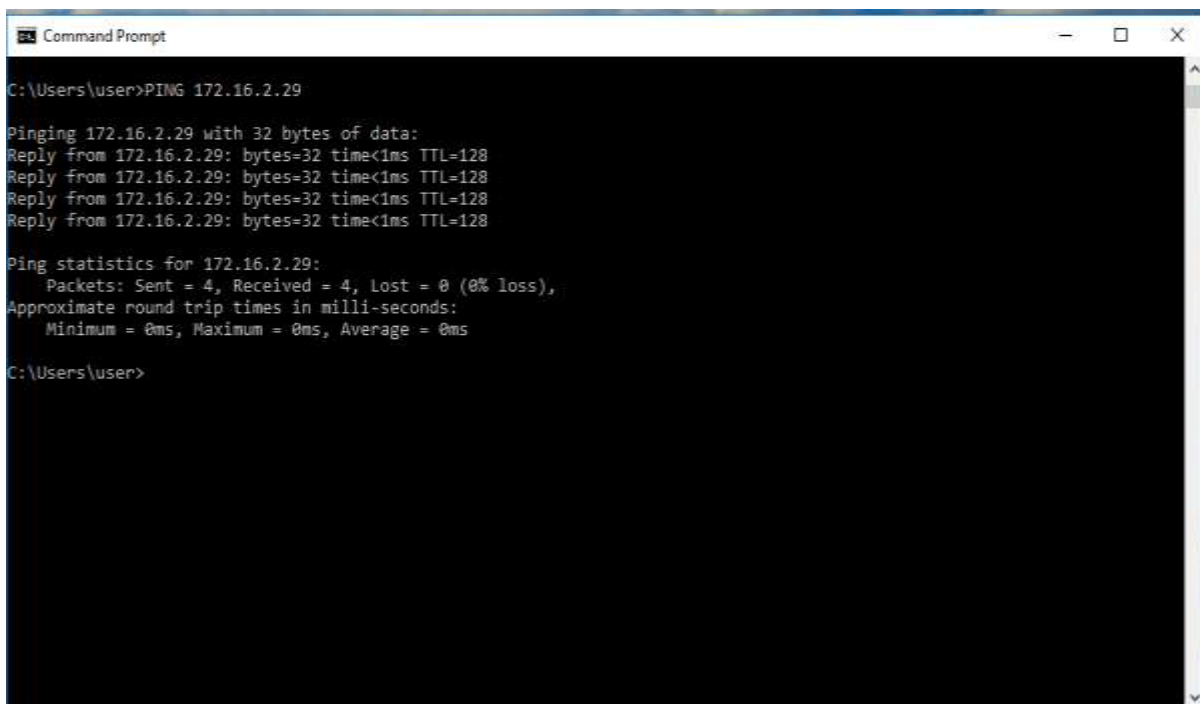
2. Test the internet connection latency

3. Check if you are experiencing lag or packet loss

How to use Ping? Use your search to find your Command Prompt – just type 'cmd' and then open the app.

Type ping, followed by a domain name or IP address like so: ping 172.16.2.29

Windows will stop your test after the 4th attempt



```
Command Prompt

C:\Users\user>PING 172.16.2.29

Pinging 172.16.2.29 with 32 bytes of data:
Reply from 172.16.2.29: bytes=32 time<1ms TTL=128
Reply from 172.16.2.29: bytes=32 time<1ms TTL=128
Reply from 172.16.2.29: bytes=32 time<1ms TTL=128
Reply from 172.16.2.29: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.2.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>
```

How to read ping results in Microsoft Windows: Each line has several components with the following meaning:

C:\Users\user>PING 172.16.2.29

Pinging 172.16.2.29 with 32 bytes of data:

Reply from 172.16.2.29: bytes=32 time<1ms TTL=128

Reply from 172.16.2.29: bytes=32 time<1ms TTL=128

Reply from 172.16.2.29: bytes=32 time<1ms TTL=128

Reply from 172.16.2.29: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.2.29:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>

PING (172.16.2.29):– If you ping a domain name, before the test, the tool will identify that domain name's IP address.

time=1 ms – This is the amount of time it took for 1 test packet to be sent from your device, reach the destination and reach you back.

32 bytes – this is the size of the test packet

TTL=128 – this is your test's 'time to live'. The TTL (Time to live) defines for how long the packet will travel before it dies

4 packets transmitted, 4 packets received, 0.0% packet loss – The amount of sent and received packets, and % packet loss.

Successful test: You are looking at consistent low response time – the time values are close. The amount of transmitted and received packages match and there is no packet loss. (It is not uncommon for the first ping attempt to fail - it is not an indication of a problem.)

There is an issue: Highly fluctuating time values, timeouts and more than the occasional packet loss.

Unfortunately, the ping command only tells you there are issues along the way. It does not tell you whether the issues are with your router, your internet service provider or your hosting

✓ Show commands

The show commands are very useful Cisco IOS commands. The Cisco Router show commands can be used to examine nearly everything about a Cisco router and its configuration. Following table lists important Cisco Router Show commands and their use.

1. show version: Start simple; this command gives uptime, info about your software and hardware and a few other details.

Example: Router# show version

2.showip interface brief: This command is great for showing up/down status of your IP interfaces, as well as what the IP address is of each interface. It's mostly useful for displaying critical info about a lot of interfaces on one easy to read page.

3.show interface: This is the more popular version of the command that shows detailed output of each interface. You'll usually want to specify a single interface or you'll have to hit 'page down' a lot. This command is useful because it shows traffic counters and also detailed info about duplex and other link-specific goodies.

Example: Router#show interfaces

4. Showip interface: This often overlooked command is great for all the configuration options that are set. These include the switching mode, ACLs, header compression, ICMP redirection, accounting, NAT, policy routing, security level, etc. Basically, this command tells you how the interface is behaving.

Example: Router# show ip interface brief

5. Showip route: provides information about the interfaces on a router, including the logical (IP) address and status.

6. Showarp:Displays the ARP table of the router "OmniSecuR1". ARP table is the table which contains the resolved IPv4 address to MAC address mappings.

Example: Router# show arp

7.show running-config: This is an easy one. It tells you how the box is configured right now. Also, "show startup-config" will tell you how the router will be configured after the next reboot.

8.show port: Similar to the show interface command on routers, this command gives you the status of ports on a switch.

9. Showvlan: With the trend toward having lots of VLANs, check this command to make sure your ports are in the VLANs you think they are. Its output is very well designed.

10. Show tech-support: This command is great for collecting a lot of info. It basically runs a whole bunch of other show commands, and spits out dozens of pages of detailed output, designed to be sent to technical support. But, it's also useful for other purposes.

✓ Trace route

A traceroute is a function which traces the path from one network to another. It allows us to diagnose the source of many problems.

Note: To be effective, the traceroute must be run during a time when you are experiencing the problem, from a computer that is experiencing the problem.

A trace when you are able to connect, or one from another computer, is not helpful. Therefore, you should try to connect to your site again just before you run it. If the problem is no longer occurring, you will have to wait until the next time the problem occurs (if there is a next time) before running your traceroute.

To run traceroute on Windows: Open the command prompt.

Go to Start > Run.

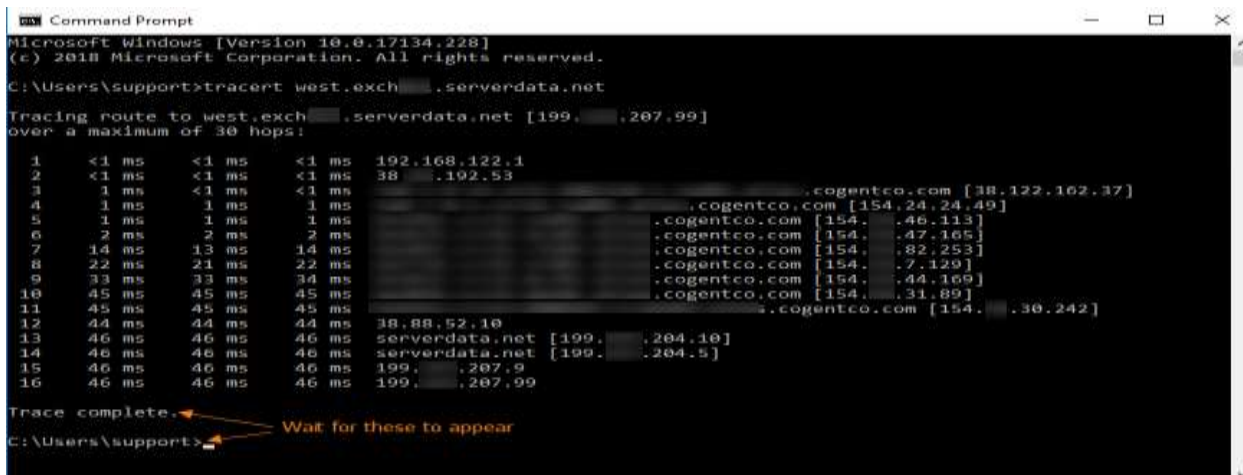
Type cmd and press the Enter key.



In the command prompt, type: `tracert hostname`

where hostname is the name of the server connection you are testing. See the section determining

hostname below for help with the hostname.



```
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\support>tracert west.exch.serverdata.net

Tracing route to west.exch.serverdata.net [199.207.99]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.122.1
  1  <1 ms    <1 ms    <1 ms    38.192.53
  2  <1 ms    <1 ms    <1 ms    .cogentco.com [38.122.162.37]
  3  <1 ms    <1 ms    <1 ms    .cogentco.com [154.24.24.49]
  4  <1 ms    <1 ms    <1 ms    .cogentco.com [154.46.113]
  5  <1 ms    <1 ms    <1 ms    .cogentco.com [154.47.165]
  6  <1 ms    <1 ms    <1 ms    .cogentco.com [154.82.253]
  7  14 ms    13 ms    14 ms    .cogentco.com [154.7.129]
  8  22 ms    21 ms    22 ms    .cogentco.com [154.44.169]
  9  33 ms    33 ms    34 ms    .cogentco.com [154.31.89]
 10  45 ms    45 ms    45 ms    .cogentco.com [154.30.242]
 11  45 ms    45 ms    45 ms    38.88.52.10
 12  44 ms    44 ms    44 ms    serverdata.net [199.204.10]
 13  46 ms    46 ms    46 ms    serverdata.net [199.204.5]
 14  46 ms    46 ms    46 ms    199.207.9
 15  46 ms    46 ms    46 ms    199.207.99
 16  46 ms    46 ms    46 ms    199.207.99

Trace complete.
C:\Users\support>
```

You may have to wait up to a minute or more for the test to complete. It will generate a list of the connections along the way and some information about the speed of the steps along the way.

Send us the complete results (every line) for analysis. Select tracert results using your mouse cursor and right click on it to copy in into clipboard. You can now paste it into a document and send to Support.

✓ NS lookup

The nslookup (which stands for name server lookup) command is a network utility program used to obtain information about internet servers. It finds name server information for domains by querying the Domain Name System.

How to Use nslookup in Windows: To use the Windows version of nslookup,

Open Command Prompt and type nslookup to get a result similar to this one but with entries for the DNS server and IP address that your computer is using:

This command identifies which DNS server the computer is currently configured to use for its DNS lookups. As the example shows, this computer is using an Open DNS server.

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify.

For example, if you entered "whatis.com" (which is one of the TechTarget sites), you would receive as a response our IP address, which happens to be 65.214.43.37

Or if you entered "65.214.43.37", it would return "sites.techtarget.com".

Nslookup sends a domain name query packet to a designated (or defaulted) domain name system (DNS) server. Depending on the system you are using, the default may be the local DNS name server at your service provider, some intermediate name server, or the root server system for the entire domain name system hierarchy.

Network monitoring

Network monitoring is a computer network's systematic effort to detect slow or failing network components, such as overloaded or crashed/frozen servers, failing routers, failed switches or other problematic devices. In the event of a network failure or similar outage, the network monitoring system alerts the network administrator (NA). Network monitoring is a subset of network management.

Network monitoring is generally carried out through software applications and tools. Network monitoring services are widely used to detect whether a given Web server is functioning and connected properly to networks worldwide. Many servers that perform this function provide a more complete visualization of both the Internet and networks.

1.4. Appropriate identification and selection of tools and materials to be used according to the network status.

- Topic 1: identification and selection of tools and materials to be used according to the network status

What kinds of tools do I need?

Every network administrator or manager worth his or her salt knows that it takes preparation and knowledgeable responses to keep your system running smoothly. When it comes to managing your network, you need the kinds of tools that will allow you to:

- Monitor
- Track
- Alert
- Troubleshoot
- Modify and correct

In order to effectively do all of these things, you will need both hardware and software tools that are proven reliable and picked with your network's specific design requirements in mind.

What features should those tools have?

Your system needs to monitor bandwidth and usage trends, set up alerts for faults and capacity, track the IPs of connected devices and monitor user traffic—and ALL of these features should be transparent and traceable using a variety of custom reporting tools including those that make it easier to convey information to your less technical minded departments and decision makers.

✓ **Hardware Tools:**

The following are the tangible, hands-on tools you should have available for your use when managing and maintaining your network. While virtually monitoring your system is made easier with the right software, the network itself still lives and breathes through the technological foundation you've built here in the real world.

- **Butt Set**

Used in telephony, a butt set allows you to test your network's phone lines using alligator clips and a handheld set.

- **CableCertifier**

Want to verify your cable's bandwidth and frequency? A cable certifier can help you confirm that your CAT 5e cable meets proper specifications, supporting speeds of 1000 Mbps.

- **Cable Tester**

A cable tester can help you verify that your cable is wired correctly or to troubleshoot suspected faulty cables, allowing you to identify short or open cables. Fluke Networks is a great resource for high quality cable testing and diagnostic hardware.

- **Crimper**

You'll need a crimper to attach cables and connectors.

- **TonerProbe**

Need to find the other end of a cable? Then a toner probe's your new best friend, allowing you to place a tone on one end of the wire to find the corresponding tone on the other end with a speaker and contact probe. This excellent troubleshooting tool can also be used to identify cable continuity because a short or open cable will not complete the circuit and produce the tone.

- **Environmental monitor**

your environmental monitor will log the conditions (temp and humidity) of the room in which your sensitive network equipment resides. An excellent tool for monitoring the conditions in

your data center(s) and/or server rooms, an environmental monitor can help you identify those issues that could potentially cause problems for your equipment helping you to sidestep a down. Tracking these logs can also assist you in ferreting out potential environmental causes of problems like random reboots or overheated systems. AVTECH makes a wide range of tools to monitor your environmental and power status in server rooms.

- **Loop back plug**

Want to test your data ports and NIC jacks? A loop back plug can help you verify that data is flowing properly on that port, both sending and receiving.

- **Multimeter**

Your multimeter can help you with continuity checks, measuring voltages, amperage, and resistance. Touch the probes to two ends of a wire and listen for the multimeter's characteristic beep. No beep? Your cable has a break in continuity—it's that simple.

- **OTDR & TDR**

The optical time domain reflectometer (OTDR) and time domain reflectometer (TDR) work similarly, allowing you to isolate the locations of breaks, measuring the distance between cable ends by sending a signal down the cable and measuring how long it takes to return or reflect the signal back from a break. Both are invaluable in troubleshooting breaks and even more minor disruptions in the electrical flow of your cables. OTDR works on fiber optic cables.

- **Punch Down Tool**

Allowing you to “punch down” connecting cables to wiring blocks or terminate cables to jacks with a small amount of pressure, the punch down tool is spring loaded and a must have for all those maintaining a network.

- ✓ **Hardware or Software Tools:**

Some tools offer an opportunity for choice between hardware or software to do the same job, which you choose will depend on your network's needs, budget, and priorities.

- **Protocol Analyzer aka “Packet Sniffer”**

Want to hunt down an unauthorized application or suspected attack on your network? Send in the sniffer. Protect your network by analyzing traffic, troubleshooting problems or suspicious activity using a protocol analyzer. While many folks view a hardware-based protocol analyzer solution as superior to

software solutions, the cost difference and network priorities of your organization may make a software solution a better choice for you.

Software Tools:

While there are many all-in-one solutions available to help you monitor, analyze, and maintain your network – we'll leave the choice of which to use up to you. Here is a list of the most common tools your network management software should contain and how they can assist you in doing what you do.

- **Bandwidth Monitor**

Monitor the average BPS and utilization percentage of interfaces, identifying traffic bottlenecks in a switch or router in real-time with this vital bandwidth tool. Presented in an easy-to-understand graphical format.

- **Network Monitor**

Continuously monitoring device response time, your network monitor alerts you via email, reporting node status and prioritizing severity. Ipswitch creates industry leading tools to visualize and monitor your network.

- **Port Scanner**

Track down unknown or unwanted services running on your system using a port scanner to scan for port status, associating ports with known services.

- **Switch Port Mapper**

Manual cable tracing is both time consuming and a total drag, save yourself from tedium and identify each switch port a device is connected to within a switch using a switch port mapper. Useful in helping you quickly assess port availability and gain real-time operational status and speeds of each port.

- **System Details Update**

Streamline your system details update process using this handy tool that lets you to view, scan, modify, and update the details on a range of devices all at once.

- **TCP Reset**

Providing a list of all established TCP connections in a device, the TCP reset lets you verify legitimate connections and reset those that are unwanted or unauthorized.

- **Wake-On-LAN**

Wake it up when you're on the go-go. Wake-on LAN allows you to remotely "wake" or boot up a

machine in low power mode on the network with the use of a remote command. Solarwinds provides free tools to manage your network power consumption and use wake-on-lan technology to save energy and remotely control system power.

Learning Unit 2: Determine and Implement Solutions

LO2.1. Apply network preventive maintenance

- Content/Topic 1: Introduction to network preventive maintenance

What is preventative maintenance?

In order for your network to work properly, every piece of the network must work properly. Preventative maintenance is concerned with anything that can be done to prevent any component of your network from failing. This includes:

- ✓ **Client computers** (also referred to as workstations) – PCs, Apples, laptops.
- ✓ **Servers** – the computers controlling specific parts of the network
- ✓ **Peripherals** – devices such as printers, whiteboards or scanners that are connected to client or server computers
- ✓ **Devices** such as hubs, switches, bridges and routers that are used to control the network
- ✓ The equipment used to connect the network together, whether cables or wireless devices, or a combination of the two
- ✓ The software running on all this equipment

Why use preventative maintenance?

Implementing a preventative maintenance programme will enable you to detect and prevent many problems before they become incidents by ensuring that the individual items that comprise your network are operating as reliably as possible.

Some of the benefits of preventive maintenance

1. Reduced network downtime
2. Eliminating premature replacement of parts
3. More economical use of technical staff because they are working to a schedule rather than on reacting to repair breakdowns
4. Lower repair costs, because there will be fewer secondary failures (when parts fail in service they often damage other parts)
5. Reduced product rejects, rework and scrap, owing to better overall equipment condition
6. Improved safety conditions and quality.

Who uses preventative maintenance?

Internal or external technical support staff carries out most of the preventative maintenance activities in the school. If your school's technical support is provided by an external party, you can use the information on preventative maintenance tasks to ensure that they are performing the tasks necessary to keeping your network running at maximum performance.

How does preventative maintenance work?

There are three main elements to preventative maintenance: design, maintenance and preparation. The preventative maintenance process flowchart illustrates this.

1.Design

This involves setting up the network in such a way as to minimize the possibility of component or network failure. Examples:

- Ensuring that servers have an uninterruptible power source
- Installing a firewall to keep the network secure
- Putting in adequate ventilation for heat sensitive devices

2. Maintenance

This means carrying out periodic maintenance tasks on network equipment to reduce the risk of early component failure. Examples:

- Keeping print heads clean in printers
- Blowing dust out of PCs
- Checking disk space and keeping track of system logs

3. Preparation

This entails putting systems in place to minimize the impact on the network when components do fail.

Examples :

- Maintaining a stock of spare equipment
- Keeping detailed documentation on network components so that they can be quickly rebuilt
- Backing up critical data (and testing the back-ups)
- Knowing who is responsible for each part of the school network

- **Content/Topic 2: Preventive network maintenance tasks**

1. Regular Cleaning

When does it need to be done?

The frequency of maintenance activities will also be determined by the type and quantity of equipment covered by the schedule. The following list is only a rough guide to appropriate timings for general activities.

Daily

- Check server error and usage logs to identify potential problems.

Weekly

- Check disk space on servers.
- Clean paper dust out of printers.
- Ensure that antivirus software is up to date.

Monthly

- Check batteries on laptops and mobile devices.

Quarterly (four times a year)

- Clean dust out of workstations.
- Clean keyboards, mice and other moving parts.

2. Back up and security system

What is a backup?

Backup refers to the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or catastrophe.

Security

Data security refers to the protection of data from unauthorized access, use, change, disclosure and destruction and includes network security, physical security, and file security.

Storage & Backup

Data storage refers to holding your data files in a secure location that you can readily and easily access.

Data backup, in contrast, refers to saving additional copies of your data in separate physical or virtual locations from data files in storage.

Your data is the basis of your research. If you lose your data, recovery could be slow, costly, or impossible. It is important that you secure, store, and backup your data on a regular basis.

Why should you secure and backup your data?

- Accidents
- Malicious damage/modification to data
- Theft of valuable data

Keeping reliable backups is an important part of data management. Regular backups protect against the risk of damage or loss due to hardware failure, software or media faults, viruses or hacking, power failure, or even human errors.

Backup options

- Hard drives - personal or work computer
- Departmental or institution server
- External hard drives
- University archives

Backup storage for PCs and mobile devices

PC users can consider both local backup from a computer's internal hard disk to an attached external hard drive or removable media, such as a thumb drive (a flash drive or USB stick).

Another alternative for consumers is to back up data from smart phones and tablets to personal cloud storage, which is available from vendors such as Box, Carbonite, Dropbox, Google Drive, Microsoft OneDrive and others.

3.Network upgrading

In computers, an upgrade is a new version of addition to a hardware or, more often, software product that is already installed or in use. Upgrades may be sold as specially labeled, less expensive "upgrade" packages (as, for example, Microsoft's Office suite products) to existing users alongside versions of the product that are made for sale to first-time users.

Upgrading is the process of replacing a product with a newer version of the same product. In computing and consumer electronics an upgrade is generally a replacement of hardware, software or firmware with a newer or better version, in order to bring the system up to date or to improve its characteristics.

4.Requirements for scalability

Scalability is the ability of something to adapt over time to changes. The modifications usually involve growth, so a big connotation is that the adaptation will be some kind of expansion or upgrade.

Scalability is an attribute that describes the ability of a process, network, software or organization to grow and manage increased demand. A system, business or software that is described as scalable has an advantage because it is more adaptable to the changing needs or demands of its users or clients.

Scalability [in telecommunication and software engineering] indicates the capability of a system to increase performance under an increased load when resources (typically hardware) are added

Dimensions of Scalability:

- Size (more CPUs)
- Other Resources (Memory)
- Software (Versions,...)

A system is described as scalable if it remains effective when there is a significant increase in the number of resources and the number of users.

5.Requirements for availability

Availability, in the context of a computer system, refers to the ability of a user to access information or resources in a specified location and in the correct format.

When a system is regularly non-functioning, information availability is affected and significantly impacts users. In addition, when data is not secured and easily available, information security is affected, i.e., top secret security clearances.

Another factor affecting availability is time. If a computer system cannot deliver information efficiently, then availability is compromised.

Data availability must be ensured by storage, which may be local or at an offsite facility. In the case of an offsite facility, an established business continuity plan should state the availability of this data when onsite data is not available. At all times, information must be available to those with clearance.

6.Applications software updating

System Software Updates: You always want to keep your system updated as much as possible as updates most often focus on bug fixes (A bug fix is a change to a system), so your system will run better, and additional security.

The process is similar on Windows computers. To update your system software on Windows, just follow these steps:

1. Click the Windows icon in your task bar to open up the Start menu. (If you don't already know, this icon is in the bottom left corner of your screen.)
2. Click "All Programs."
3. Click, "Windows Update."
4. After Windows Update opens, click "Check for Updates" on the top left side of the window.
5. Once Windows finishes checking for updates, click the "Install" button.
6. When the updates have finished installing, restart your computer (if prompted).

Software Update (Mac) and Windows Update (Windows) will periodically run all by themselves and ask you to update. Nonetheless, you may not notice this or ignore it from time to time, so it's good to check yourself once in a while.

5. Applications software deployment

Deployment, in the context of network administration, refers to the process of setting up a new computer or system to the point where it is ready for productive work in a live environment.

Installing, setting up, testing and running. Is widely used with computers as an alternate to the word "implementation." For example, "XYZ software deployment" is the same as saying "XYZ software implementation." To "deploy" something is to "get it installed and running."

Deploy can refer to any type of installation. For example, this could be setting up a new LAN, building a server, installing software, etc.

Deploy: To install, test and implement a computer system or application.

Release: make a particular software version available to public.

Software deployment is all of the activities that make a software system available for use.

Software deployment brings many key advantages to enterprises. Tasks like installing, uninstalling and updating software applications on each computer are time consuming. Software deployment services reduce the time and make the process error free.

The software can be easily controlled and managed through deployment. You can also monitor software information and the actions of users.

Software deployment includes all the process required for preparing a software application to run and operate in a specific environment. It involves installation, configuration, testing and making changes to

optimize the performance of the software. It can either be carried out manually or through automated systems.

The big advantages of Software deployment:

1. Time saving
2. Enhance security
3. Monitor user actions
4. Effective software updates

✓ Software deployment

What is Software Deployment?

Software Deployment is the process of remotely installing software on multiple or all the computers within a network simultaneously, from a central location. The word "Software Deployment" is generally used in the context of a large network (more than 20 computers). Software Deployment comprises but is not limited to the following activities:

1. Creating and maintaining up-to-date and ready-to-install software packages
2. Configuring the target computers before the installation or uninstallation of the package
3. Installing or uninstalling the software on the target computers
4. Configuring the target computers post installation or uninstallation
5. Upgrading existing software.

Steps for software deployment

A smooth software deployment process is vital for the smooth operation of any organization. The software deployment process can be handled manually or through automation if you have an IT Team or IT Consultant. Software deployment process mainly consists of 3 stages: development, testing and monitoring. Deployment tools can be used to bath deploy software on multiple computers with options to customize and select permission roles.

These are the main stages of software deployment:

1. **Deployment.** You need to decide on the method of deployment and the configuration metrics that you will require. You will need to budget enough time to the development stage and test deploy codes to server or client ends. It has to be remembered that the objective is to achieve successful deployment and release of the software, not meet a time deadline.
2. **Testing.** Statistics and analytics can be drawn from comprehensive or customized reports gathered from software distribution systems. It can be used to monitor user activities around the particular software on workstations. This can assist in establishing a controlled work environment where the actions of users can be monitored by the enterprise.
3. **Monitoring.** Software distribution gives comprehensive deployment options and ways to customize installation. Packages can be distributed to users in less time, so they are up and running within hours instead of days. Software installations can be done remotely saving both time and effort. The process can be done without constant monitoring, so your IT team can focus on performing activities that can benefit your business in the long-term.

LO2.2: Apply network curative maintenance

- Content/Topic 1: Introduction to network curative maintenance

The curative maintenance

The curative maintenance can be considered as repair of defective or damaged equipment.

It can be associated to other types of maintenance: preventive or corrective maintenance.

It is generally related to the end of the life of a machine or one of its components.

The Most Common Computer Network Problems and Their Solutions

1. Cable Problem: Cables that connect different parts of a network can be cut or shorted. A short can happen when the wire conductor comes in contact with another conductive surface, changing the path of the signal.

Cable testers can be used to test for many types of cable problems such as: Cut cable, incorrect cable connections, Cable shorts, Interference level, Connector Problem

2. Connectivity Problem: A connectivity problem with one or more devices in a network can occur after a change is made in configuration or by a malfunction of a connectivity component, such as hub, a router or a Switch.

3. Software Problem: Network problems can often be traced to software configuration such as DNS configuration, WINS configuration, the registry etc.

4. Duplicate IP Addressing: A common problem in many networking environments occurs when two machines try to use the same IP address.

5. Printing problems Symptom: Printing does not consistently work on the network. A printer may appear available, but print jobs that are sent to it are not completed.

Cause: Determine if only one user is experiencing this problem or if several people have the same issue. If only one user is having the issue, it may be that the PC is not mapped correctly to the print server. If this is not the cause, the network between client and printer may be to blame. Packet loss can cause printing problems, as well as network connectivity problems on the printer itself.

Resolution: Check the printer configuration to make sure it has a good IP address and can access the print server if it is external to the printer. At times, updating the printer driver has resolved printing issues. Overall, be sure that traffic is getting to and from the printer on the network and that all printer drivers are up to date.

At some point in time, we all have faced the same “No Internet” error message.

Some people decide to play the dinosaur video game, and others do nothing, then there are the ones that love to dig down into the nature of the problem.

✓ Usage of Troubleshooting tools

What is Troubleshooting?

Troubleshooting is a form of problem solving, often applied to repair failed products or processes on a machine or a system. It is a logical, systematic search for the source of a problem in order to solve it, and make the product or process operational again. Troubleshooting is needed to identify the symptoms.

Difference between maintenance and troubleshooting?

The difference between maintenance and troubleshooting is that **maintenance** means to look after something so that it stays in good condition **while troubleshooting** is trying to figure out why something is not working as it should.

Troubleshooting is finding an existing problem and maintenance is preventing a potential problem.

All the tools and commands work in many Operating Systems, including Windows and Major Linux variations. Although they have the same fundamentals, they have differences in their implementation. Most of the tools require you to open the Command Prompt “cmd” in Windows, the “terminal” in MacOS, or the “shell” in Linux. Others are web-based, and others require you to download an executable file.

The network troubleshooting software described in the following list are the favorites among any experienced IT specialist:

1. Ipconfig/Ifconfig

Gathering information is the most important step when troubleshooting.

The ipconfig command stands for IP configuration and is used in Windows OS.

The ifconfig stands for interface configuration and is used in Linux and MacOS. Both display all current TCP/IP configuration for all currently connected networks.

If your network is using a DHCP (Dynamic Host Configuration Protocol) Server to assign IPs to all hosts, then ipconfig is mandatory when troubleshooting. It also comes in handy when the IPs are statically assigned because there might not be proper documentation, or the IP address changed.

The ipconfig gives out all the network adapter's information (when used without arguments), such as:

- IPv4/IPv6 Address
- Subnet Mask
- Default Gateway

Aside from showing information, the Ipconfig command can also release IP addresses, renew DHCP configuration, flush DNS cache, register DNS, and more.

ipconfig /all

This command will display all information, including adapter description, MAC address, DHCP Server, Lease information, and more.

ipconfig /renew

This command will renew the IP information for a specific adapter. Use it, when you suspect that there is an IP address conflict.

2. Ping

A good Ping represents a healthy network connection, a bad ping means a delay or packet loss, and an unresponsive ping represents no connection.

In networking, ping is a method that sends an ICMP (Internet Control Message Protocol) echo request to a destination and waits for the response (echo reply). While the source of the ping is waiting, a delay timer is counting the time it takes for the packet to go and come back.

With Ping you can perform a basic connectivity test between source and destination. If the target does not respond to the request, the connection is unavailable.

3. Tracert / Traceroute

In networking, a route towards a destination is made out of hops. Each hop is a device capable of routing and forwarding packets.

The traceroute tool gives out information on each hop that leads to a destination, something that can never be done with traditional ping.

You can use traceroute when you think that a problem extends beyond the local network and you want to find information about the path, which includes all the devices that forward your packet to the destination. The traceroute will give out IPs, hostnames, and response time of each hop.

How does Traceroute Work?

Just like Ping, Traceroute also uses ICMP requests and replies. The difference is that it performs it, using a concept known as, hop limit. To get information from each device, it limits the next hop by modifying the TTL, for example, it sends an ICMP Echo request TTL=1, then the hop drops the package and returns a TIME EXCEEDED. The source of the traceroute interprets this as the first hop, records the IP/hostname information and sends the second packet by increasing the TTL to 2, and so on.

To find information about traceroute type “tracert -help” in Windows or “traceroute” in Mac or Linux.

4. Nslookup

Anyone using the Internet will indirectly use DNS. If you type google.com from your browser, the DNS will convert the name “google.com” to a machine-readable IP, so that your packet can be forwarded correctly.

How does your computer find its way to google.com?

First, your computer checks its DNS cache, which is a memory of recent DNS lookups.

If it does not find the name on the cache, it will send the request to the DNS Server.

If you are in a SOHO (Small Office Home Office) network, you might not have to deal with a DNS Server, and leave those problems to your ISP. But enterprise networks usually use a DNS server to convert all their internal server IPs to names.

Why is NSLookup Important?

The command nslookup (Name Server Look Up) is a way to find out if the DNS Server (not the cache) is resolving names. If it can't translate a name, then there is likely a DNS issue.

Although ping and traceroute can resolve a domain name to an IP, they work based on NetBIOS information. The nslookup will consult the configured DNS server directly.

5. Netstat

If you are connected to the Internet, there are probably some applications taking advantage of your connection. Not only your web browser is creating a link to a remote server, but also online video games, downloading software, and probably some background processes that you might be unaware of, such as backdoors or Malware.

Netstat stands for Network Statistics. It gives detailed information about the state of all the current network connections on the computer.

Netstat is a fantastic tool for troubleshooting because It can let you see what ports are open and listening on your device and the remote servers that are creating a connection to your computer with the ports that they are using.

6. Route

With some tools listed before, such as "traceroute," you learned how to analyze routes on a hop-by-hop basis. You are troubleshooting a "No Internet" issue, and you can quickly figure out the path that the packet is taking is not going through your Internet Gateway.

All your traffic is being re-routed somewhere else, and you don't know why.

The "route print" command shows all configured routes on your machine. Route Print is a Windows command and is the equivalent for "Netstat -nr" in MacOS and Linux, showed before.

7. Subnet Calculator

Unless you do it every single day, subnetting is a skill that takes time to master. Some network professionals can create subnets without a pen, paper, and calculator. They have been doing it for a while, that their minds can create subnets quickly.

But those that don't have the skills need speed and error-less subnetting.

A subnet calculator will let you divide your network into subnets. It will help you define IP subnets, masks, and subnet addresses. Give it a range of IP addresses or CIDR notations, and it will create a list of subnets for you.

When you use a calculator, you can customize the output of the list of subnets. For example, you can vary the number and the size of subnets available in your network.

A favorite subnet calculator among network admins and engineers is Solar Winds Advanced Subnet Calculator. It is free, easy-to-use, lightweight, and fully compatible with Windows OS.

Among its key features are:

- Calculates IPs
- Creates Subnets
- Calculates CIDR
- Creates a list of subnets.
- Resolves DNS.
-

8. SpeedTest

Network admins use online speed tests to check the real bandwidth or throughput of an Internet connection. These tests are capable of measuring the time it takes to download or upload from the Internet to a specific host.

The results of these tests are great for testing newly deployed connections, making sure that the Internet Service Provider “ISP” is giving the offered bandwidth, or making sure that an SLA (Service-Level-Agreement) is met.

- Content/Topic 2: Curative Network maintenance tasks.

The curative maintenance can be considered as repair of defective or damaged equipment.

It can be associated to other types of maintenance: preventive or corrective maintenance.

It is generally related to the end of the life of a machine or one of its components.

Problem identification

What Is Problem Identification?

Problem Identification consists of: Clearly identifying the root cause of a problem.

Developing a detailed problem statement that includes the problem’s effect on a population’s health

Why Is Problem Identification Important?

You need to make sure you are identifying the true, underlying problem causing the public health issue—and this is not always obvious.

How Do You Identify The Problem?

1. Identify the root cause of the problem by collecting information and then talking with stakeholders. Combining existing research and information from your stakeholders can offer some insight into the problem and its causes. Consider data sources that could help you more clearly define the problem. Start by doing an environmental scan, a literature review, and if necessary, surveys in the community.

2. Develop your problem statement.

Describe how the problem occurs, how serious it is, and its outcomes and impacts. Doing this can also help you identify any gaps in the data you have gathered. The problem statement you develop might include:

- Who is affected
- How big is the problem
- What contributes to the problem
- When and where the problem is most likely to occur.

How Do You Know You Have Successfully Completed Problem Identification?

You collected information about the problem by combining existing research and information from your stakeholders, and you collected new data from the community if necessary

You involved all relevant stakeholders when defining the problem

The data you collected identifies the root cause of the problem and provides a complete picture of it

Your problem statement includes:

- ✓ Who is affected?
- ✓ How big the problem is?
- ✓ What contributes to the problem?
- ✓ When and where the problem is most likely to occur?
- ✓ You framed the problem in a way that helps illuminate possible policy solutions

Curative Maintenance for the IT Monitoring Of Your Infrastructure

The Pentalog IT team provides its customers with an assortment of curative maintenance solutions to help them increase the availability, performance and security of their IT infrastructure, environment and services.

Here are just a few examples:

- Registration of tickets declared by mail
- Registration of tickets detected following monitoring
- Feedback on tickets
- Virtual machine (VM) restart
- Service (web, database) restart
- Intervention on network alert
- Intervention on application server alert
- Drawing up operational procedures

LO2.3: Test Network

- Content/Topic 1: Testing Network

Why network test?

Think of all the problems you face when you try to connect to a network. You may have seen instances where you may be doing everything right but still unable to connect.

Let's take another case where you want to launch a website and want to be sure the server responds, how do you really validate and test before launching.

To help us find out & troubleshoot network issues, monitor network speeds, and other network management, we find 100's of tools available these days.

In general, testing is finding out how well something works. In terms of human beings, testing tells what level of knowledge or skill has been acquired.

In computer hardware and software development, testing is used at key checkpoints in the overall process to determine whether objectives are being met.

For example, in software development, product objectives are sometimes tested by product user representatives. When the design is complete, coding follows and the finished code is then tested at the unit or module level by each programmer; at the component level by the group of programmers involved; and at the system level when all components are combined together. At early or late stages, a product or service may also be tested for usability.

Network testing: is the actual measurement and recording of a network's state of operation over a period of time. It involves recording the current state of network operation to serve as a basis for comparison or control.

Here are a few simple tests you can conduct to make sure your network is functional.

- **Check the physical connections.**

Check that the Link light — the little red or green light next to the RJ-45 port — is lit on every computer. You must check this light both on the computer itself and on the switch or router the computer is plugged into. If this light is not on, you have a connection problem — most likely a bad cable.

- **Verify that you can log on.**

When you're sure the physical connections are good, you should attempt to log on to each of your network computers using a valid domain user account.

- **Check the network configuration.**

Click the Start button, type `cmd` and press Enter. Then, enter the command `ipconfig /all` and press Enter.

- This command will spit out numerous lines of information. The line you're looking for should resemble this:

```
IPv4 Address. . . . . : 192.168.1.125(Preferred)
```

If this part of the output does not show a valid IP address, you need to check that your IP configuration is set correctly and that your DHCP server is working.

- **Verify that the computers can ping each other.**

Another basic test you should perform is to use the ping command from a command prompt to make sure that the computers on your network can contact one another.

Do several ping tests. First, make sure that TCP/IP is up and running by having the computer try to ping itself. Open a command prompt and type `ping localhost`. The output from this command will indicate whether or not the ping was successful.

Next, try to ping your servers by name. For example, if your file server is named `FileServer01`, use the command `ping FileServer01`.

- Content/Topic 2: Description of Types of network test

Software testing can be categorized according to the various broad testing goals that are the focus of the individual tests.

At a conceptual level, the kinds of automated application testing you can perform using Silk Test Classic in a networked environment is:

- ✓ Functional
- ✓ Configuration
- ✓ Concurrency

The ordering of this list conforms to the incremental functional testing methodology supported by Silk Test Classic.

Each stage of testing depends for its effectiveness on the successful completion of the previous stage. Functional, configuration, and concurrency testing are variations of regression testing, which is a prerequisite for any type of load testing.

You can use Silk Performer for load testing, stress testing, and performance testing.

You can perform functional testing with a single client machine.

You can perform the first four types of test with a testbed containing only two clients. The last two testing types require a heavy multi-user load and so need a larger testbed.

The first four types of test

1. **Concurrency Testing** : Describes how you can test two clients using the same server.
2. **Configuration Testing** : Describes how you can test that every possible client platform can operate with every possible server platform.
3. **Functional Testing** : Describes how you can test the functional operation of a single instance of an application.
4. **Peak Load Testing** : Describes how to place a load on the server for a short time to emulate the heaviest demand that would be generated at peak user times.
5. **Volume Testing** : Describes how you can place a heavy load on the server, with a high volume of data transfers.

- **Content/Topic 3: Description of Network testing tools**

Network testing tools and equipment makes it easy for skilled networking technicians to locate problems in your network setup and apply fixes as needed. These precise network tools are exactly what you need to ensure that your network continues to operate at peak performance.

Testing equipment can help identify issues before they noticeably affect your company, allowing you to keep systems operational and prevent downtime.

Accurate analysis

networking testing equipment includes probes and multimeters that help you analyze specific energy flows in your network's systems. These analytical tools can read current and voltage and help skilled electricians or network technicians identify faults or short circuits. .

Prepare for Upgrades

networking testing equipment can also help you prepare your network for system upgrades. These tools let you check power lines and other transmission cables and wires for problems before you begin installing upgrades that may be damaged by faults or other common network problems. When you are ready to upgrade to the latest networking technology using existing wiring, check out available power line adapters.

Repair Tools

Testing equipment also includes cutters, line strippers, and other tools that help make repairs as easy as possible. The right tools can make a major difference when you are trying to repair problems in your electrical or data transmission cables.

Repair tools allow your company's skilled networking technicians to fix problems without needing to hire outside contractors or rent equipment.

1. Elegant



Wire Tracker, ELEGANT RJ11 RJ45 Cable Tester Line Finder Multifunction Wire Tracker Toner Ethernet LAN Network Cable Tester for Network Cable Collation, Telephone Line Tester.

This is a pretty straight forward network cable debug tool. Essentially one end is the transmitter and the other end is the scanner. It will let you know specifically which wire there is an issue with which is very useful when putting your own connectors on a cable.

This instrument is a multi-functional handheld cable testing tool. Work perfect when RJ11 RJ45 cable is on power. It has a wide application with reinforced cable types and multiple functions. It is a necessary testing tool for telecommunication engineering, wiring engineering, and network maintenance person.

2. Meterk Wire Tracker RJ11 RJ45 Line Finder Handheld Cable Tester Multifunction Cable Check Wire Measuring Instrument for Network Maintenance Collation, Telephone Line Test.



Tracer function: Tracer function is it can help you quickly find the line pairs in many pairs, this instrument is suitable for RJ45 interface internet cable, RJ11 interface telephone line, for other metal wire hunt through **adapter**.

Telephone line test: the work of the telephone line of the detection of various states, only the transmitter can be detected, such as determining TIP or PING line, to determine the work of the telephone line idle, ringing and off-hook state.



3. 50 Pieces Network Tool Repair Kit, Ethernet LAN Cable Tester Computer Maintenance Coax Crimper Tool for RJ-45/11/12 Cat5/5e with Connector Accessories and Socket Set.

Fully demagnetized tools offer you full protection of computer hard drive or magnetic media from damage.

4. Network Cable Tester AT226-C Multi-functional LCD for RJ45, RJ11, BNC, Metal Cable, PING/POE

Tracker NF-8601W



Poe function: Identify which pins are providing power and detect how much voltage.

PING function:to test network performance, data packet, min & max time.

AC Filter:Tone traces cable with complete AC Interference Rejection.

Hub blink: For locating network port by the flashing port light on Hub / Switch.

Additional Benefits:TF function to import and export data from computer (160 sets, txt format).

1. PoE / PING testing.

2. Trace targeted cable among lots of unknown cables;
3. Port flash function help trace LAN cable connected to switcher or router visually, no need of receiver.
4. Capable of scanning cable on PoE switch without damaging the device.
5. Locate faults for RJ11/RJ45/BNC Cable.
6. measure cable length accurately
7. Voltage detecting function.
8. 8remotes included, improving work efficiency.
9. Memory and storage function, export or upload the data from PC.
10. Built-in Lithium battery and color screen.

Other testing tools you may know:

1. Flent (Flexible Network Tester)

This is a tool which allows experimental evaluations of the network instead of simulation. This is a python wrapper and allows running tests on multiple tools, maintains information on which tool to run in a configuration file.

2. Netalyzer

If you're looking for a network debugging tool, this is a good choice. This tool lets user test internet connections to identify problems and output in the form of the detailed report show security/performance issues.

3. FortiTester

This is a very powerful tool which lets users measure the performance of network devices.

4. Simple Port Tester

This is very handy and simple tool which lets the user find out if ports are open or not. This allows testing multiple ports through a specific IP address.

5. Network Monitor

This tool is a great tool for monitoring Network, can be used to isolate and fix issues before they are seen by real users. It also has a feature which lets users customize alerts and notifications.

6. NetCrunch

This tool supports monitoring Network Infrastructure, Virtual machines and Windows.

7. NetflowAnalyzer

This is a network traffic analytics tool which can provide information on real-time bandwidth performance. Besides network forensics and network analysis, it also helps user optimize bandwidth usage.

8. Network Security Auditor

This is a suite of more than 45 network tools & utilities and allows activities like monitoring, network auditing, and vulnerability scanning. This allows checking for all methods which hackers can use to attack. It also comes with firewall systems, real-time monitoring, and packet filtering.

LEARNING UNIT 3: DOCUMENT THE WORK DONE

LO3.1: Document on network status

- Content/Topic 1: Description of network status before and network infrastructure

✓ Document on network status

What should you document?

Proper documentation should be created as you work. Don't wait until everything is in place before starting to document what you've done. It's much easier to document in the moment than trying to remember what you did later. Make documentation a habit and make it part of your process. Don't risk potentially embarrassing situations because of the lack of network documentation.

But, what should you document?

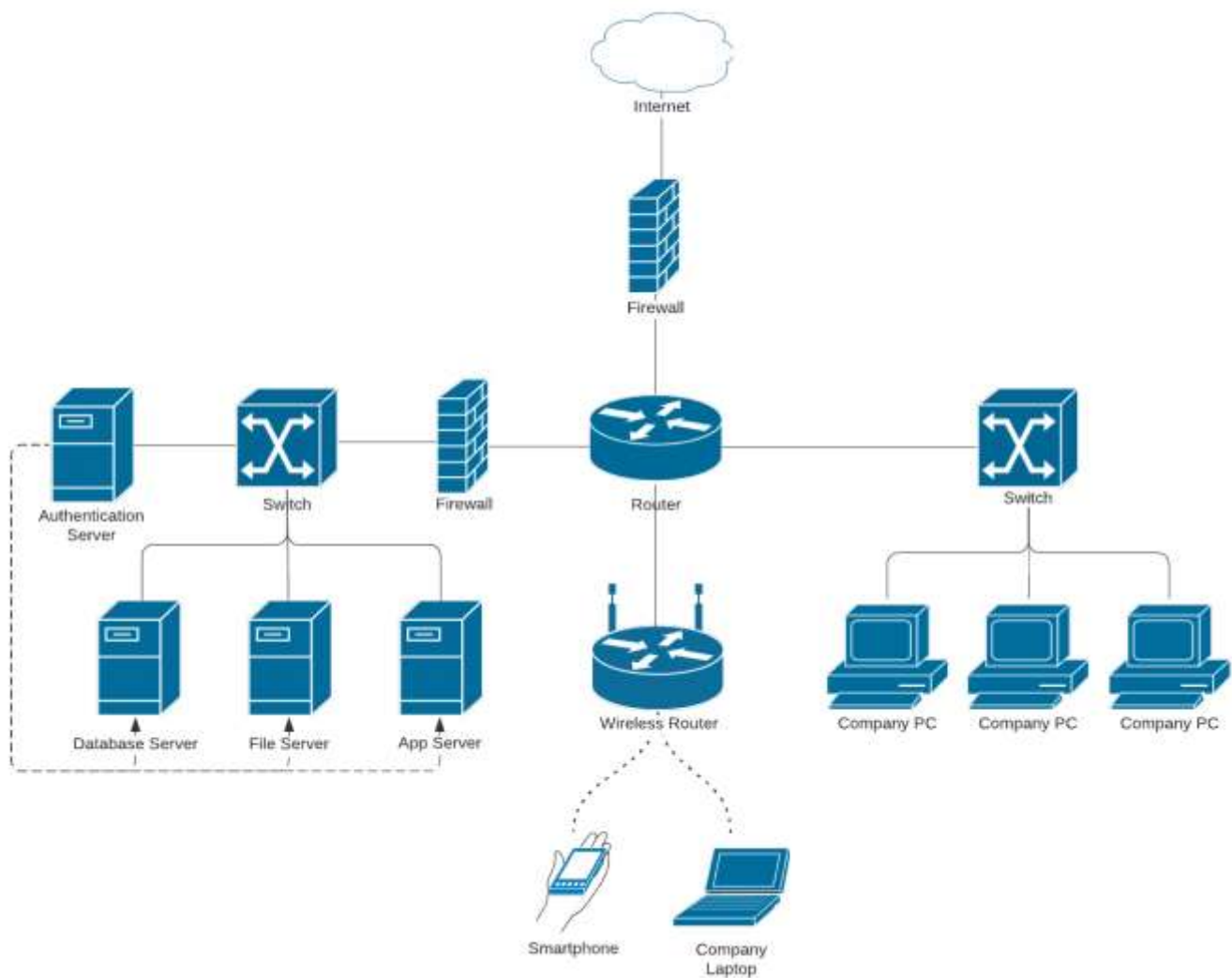
Your goal with network documentation should be to ensure that your company retains all the knowledge that went into creating the network as well as how to maintain and upgrade it.

You should seek input from your IT team, other network administrators in various departments throughout your organization, and managers to determine what you should document. The following are just a few examples of the types of information you should record to help your network to stay in good working order (plus you'll find templates to help you start your own documentation).

Network topology

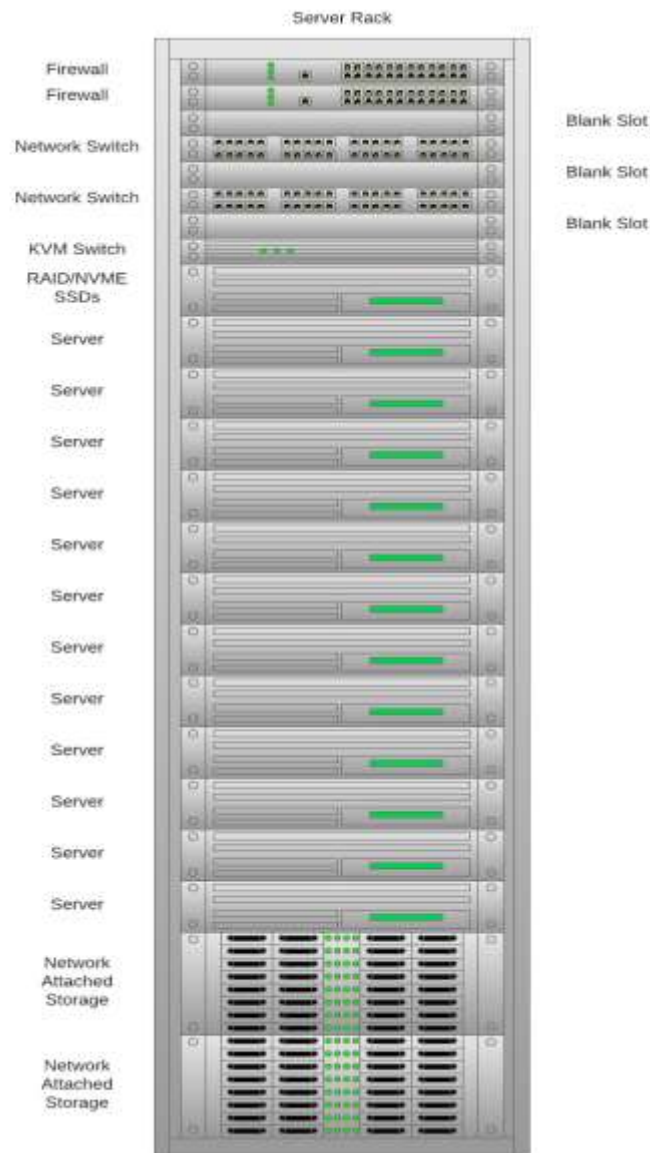
The topology is the physical or logical map of your network. It lets you visualize how the resources in your network are connected. Knowing the topology helps you to determine where new hardware can fit in your network.

Basic Small Company Network Diagram



Server rack diagram

This type of diagram shows the organization of equipment on your server rack, including components such as monitors, hard drives, power strips, routers, etc. Server rack diagrams can help you determine the size of rack you'll need during the design process but also see where computers and other devices connect to the server when you're troubleshooting.



Server Rack Diagram.

Hardware directory

This directory documents the hardware pieces of your network and should include information about serial numbers and descriptions of physical configurations. This information helps you to locate and fix hardware problems that occur.

Software directory

This directory represents your software inventory. It lets you know where all of the software applications that are authorized for use in your organization are located, what the names of these applications are, on which computers they are installed, proof of software license for each application, and service level agreements for those applications.

In large organizations, maintaining a software directory can be a daunting task. But if you are ever subject to a software audit, you will be glad you took the time to document what you have, where it is, and how many licenses you have so you can prove that your company is in compliance.

Wi-Fi diagram

You may find it useful to document or diagram how your wireless network is laid out. The diagram can include:

- The number of routers, switches, and servers used in your wireless network
- A map of physical access points to help you track down problems
- Radiofrequency patterns
- Security measures such as employee and guest SSIDs

IP address allocation

You should keep a detailed list of internal and external IP address assignments to help as you design network expansions and recycle IP addresses to be allocated to other locations. Documenting your allocation process gives you an understanding of subnet size, subnet assignments, and the devices that have been assigned to specific IP addresses or to a dynamic range of addresses. This documentation helps you to define allocation standards going forward.

An asset management diagram can give you a bird's-eye view of your organization. This customizable template can give your IT team a quick overview of employee location, asset tags, physical Wi-Fi access points, IP addresses, software installations, and so on.

Cable diagram

Documenting where and how the cables run through your building can help when troubleshooting and diagnosing network problems. The diagram should map jack numbers to physical locations.

Recovery plan

Do you know what you are going to do if you need to restore lost data? How do you preserve data from failing hardware? Do you know where your backups are housed? You need to document details of where backup data is located, how often backups occur, which type of data gets backed up, and how backups are accessed and restored to those who need it.

A step beyond a recovery plan, a fault-tolerant system is designed to give you uninterrupted service in the event that one or more network component fails. Even if you experience a catastrophic failure, the fault-tolerant system should let your employees remain productive and working without any knowledge that there has been a system failure.

A fault-tolerance plan should include:

An analysis of the business impact in the event of a failure.

Outline potential threats and the impact they may have on your business.

Assess how likely it is that these threats will occur.

Consider the effects if you don't have a fault-tolerant plan in place (lost sales, lost productivity, lost development, and so on).

Planned redundancies. Duplicating everything in preparation for potential disasters can be costly. Be sure to understand which business-critical assets and systems must start up immediately. Let the data and systems that are not mission-critical wait to come back online after proper fixes have been put in place.

The location of your fault-tolerant system, whether in the cloud or on-premises.

Improve your documentation process

While it may seem like no one reads your network documentation, network diagrams are essential to understanding existing technology, communicating with stakeholders, onboarding new employees, troubleshooting issues before they escalate, and creating a vision for future innovation.

Get started with the templates above or learn more about how Lucidchart can help your team with understanding complex systems.

Here is a list of activities to be performed while documenting the work done:

- ✓ Description of network status before
- ✓ Status of network infrastructure
- ✓ describe problems found
- ✓ Review of user manual and previous report
- ✓ Suggestion of solutions on problems found

- ✓ Description of solution implementation
- ✓ Description of procedures of the task accomplished
- ✓ Network Devices, equipment and materials used
- ✓ Description of the network status after work
- ✓ Write Technical journal and recommendation report

LO3.2: Report on the work done

- **Content/Topic 1: Reporting the work done**

A report is a document that presents information in an organized format for a specific audience and purpose. Although summaries of reports may be delivered orally, complete reports are almost always in the form of written documents.

According to the Business Dictionary, a report is a document containing information organized in a narrative, graphic, or tabular form that is prepared on periodic, regular, or as required basis.

Types of reports include memos, minutes, lab reports, book reports, progress reports, justification reports, compliance reports, annual reports, and policies and procedures.

Here are the main sections of the standard report writing format:

- **Title Section:** The title of report is necessary to orient the reader. This includes the name of the author(s) and the date of report preparation.
- **Summary:** There needs to be a summary of the major points, conclusions, and recommendations. It needs to be short as it is a general overview of the report. Some people will read the summary and only skim the report, so make sure you include all the relevant information. It would be best to write this last so you will include everything, even the points that might be added at the last minute.
- **Introduction:** The first page of the report needs to have an introduction. You will explain the problem and show the reader why the report is being made. You need to give a definition of terms if you did not include these in the title section, and explain how the details of the report are arranged.
- **Experimental details:** This is the part that you need to state every detail of the experiment, starting from the equipment that you used to the procedure for the test.
- **Results:** This is where you are expected to explain the results that you obtained. You should give clear explanation so that the reader cannot ask themselves any question on your results.

- **Body:** This is the main section of the report. There needs to be several sections, with each having a subtitle. Information is usually arranged in order of importance with the most important information coming first.
- **Conclusion:** This is where everything comes together. Keep this section free of jargon as most people will read the Summary and Conclusion.
- **Recommendations:** This is what needs to be done. In plain English, explain your recommendations, putting them in order of priority.
- **Appendices:** This includes information that the experts in the field will read. It has all the technical details that support your conclusions.

Remember that the information needs to be organized logically with the most important information coming first.

LO3.3 Write technical journal and recommendation

- Content/Topic 3: Writing technical journal and recommendation

One of the main forms of communication in engineering is the technical report. In the workplace, the report is a practical working document written by engineers for clients, managers, and other engineers.

This means every report has a purpose beyond the simple presentation of information. Some common purposes are:

- To convince the reader of something. For example:
 - to convince a government agency of the effect of a particular course of action
 - to convince a client that your solution will fulfill their needs
 - to convince the public that a proposed project will bring benefits
- To persuade the reader to do something. For example:
 - to persuade a government or council to adopt a particular course of action
 - to persuade a client to choose one design over another
 - to persuade an organisation to partner with your company on a project
- To inform the reader about something (usually for a further purpose). For example:
 - to provide a government department with information they will base policy on
 - to instruct other engineers who will work from your plans
 - to present the outcomes of a project to stakeholders

Basic report structure

Most reports contain the sections listed below. Where each report will differ is in the body; the sections you decide to include will depend on the type of report and the specific topic. You will usually be expected to decide on the structure of the body yourself. The best way is to put yourself in the place of the reader.

Ask yourself:

What does the reader need to know first?

What is the most logical way to develop the story of the project?

A report usually has the following components.

- ✓ **Title page**
- ✓ **Summary**
- ✓ **Table of contents**
- ✓ **Introduction**
- ✓ **Body of the report**
- ✓ **Conclusions and recommendations**
- ✓ **References and appendices**

Title page

This page gives:

- the title of the report
- the authors' names and student IDs
- the unit name and code, the department, and university
- the date of submission.

The title of the report should indicate exactly what the report is about. The reader should know not only the general topic, but also the specific aspect of the topic addressed in the report. Compare the following pairs of report titles:

Weak titles	Strong titles
Bridge analysis	Analysis of a prestressed concrete bridge
Internet based ATIS	An evaluation of Internet based Automated Traveler Information Systems

Summary

The Summary is usually written last of all. It provides a brief overview of the substance of the report. It is a stand-alone document generally used by busy managers who might not have time to read the full report. That's why it is usually referred to as the Executive Summary in the workplace.

The Summary is not an introduction to the topic. It should focus on what you did, how you did it, and the main outcomes and significance of your work.

The Summary:

- states the topic of the report
- briefly outlines your approach to the task (if applicable)
- focuses on the results or outcome of the project, the findings of your investigation: or the key aspects of your design
- states the significance or implications of the results.

The Summary does NOT:

- provide background information on the topic
- explain the motivation for the project
- refer to figures, tables or references contained in the report.

Length: $\frac{1}{4}$ to $\frac{1}{2}$ a page is sufficient for most undergraduate reports.

How NOT to write the summary

A common mistake is to describe the type of information in the report, rather than summarise the information itself.

Acknowledgements

In major projects you will possibly need assistance or advice from others, such as industry mentors or laboratory staff, who may have made an extra effort to help you. You may acknowledge such assistance in a short paragraph on the page after the Summary.

- Give the person's full name, position and affiliation.
- State their contribution clearly and briefly.

- Use formal language.



Thanks to my supervisor Dr. Hessami for being so patient and to Rod from the chemical engineering lab for putting me right on how to use the equipment. Without your help this project might never have got off the ground.



I would like to thank my supervisor, Dr. Josie Carberry for her encouragement and guidance throughout the project, and also MrRafiqBakti, Supervisor Monash University Wind Tunnel for his help setting up my experiments.

Table of contents

The Contents page sets out the sections and subsections of the report and their corresponding page numbers. It should clearly show the structural relationship between the sections and subsections. A reader looking for specific information should be able to locate the appropriate section easily from the table of contents.

Sections are numbered using the decimal point system. Section numbers appear on the left margin, page numbers on the right.

Here is an example from a final year project report.

CONTENTS

1.0	INTRODUCTION	1
2.0	PROJECT REQUIREMENTS	3
3.0	SYSTEM SPECIFICATIONS	4
4.0	SETTING UP A LINUX BASED VIDEO CAPTURE SYSTEM	5
4.1.	SELECTING AND INSTALLING THE OPERATING SYSTEM.....	5
4.2.	INSTALLING FEDORA CORE 1	6
4.3.	INSTALLING VIDEO CAPTURE DRIVERS VIA THE LINUX KERNEL.....	7
4.4.	IMPLEMENTING THE VIDEO4LINUX API	8
4.5.	INSTALLING OPENGL AND GLUT	14
4.6.	CREATING SIMPLE GLUT PROGRAMS FOR VIDEO OUTPUT.....	16
4.7.	USING GLUI TO CREATE GUIs	17
5.0	IDENTIFYING THE TARGET IN A FRAME	19
5.1.	OBJECT RECOGNITION FROM COLOUR.....	19
5.2.	SEGMENTATION FOR NOISE REDUCTION	24
5.3.	EDGE DETECTION AND SEPARATING MULTIPLE OBJECTS.....	29
6.0	DETERMINING ATTITUDE	33
6.1.	DISTINGUISHING BETWEEN OBJECTS	33
6.2.	LOCATING THE CENTRE OF AN OBJECT	37
6.3.	USING CORRELATIONS TO EXTRACT 3D INFORMATION.....	39
7.0	RECOMMENDED IMPROVEMENTS	62
8.0	CONCLUSIONS	64
9.0	REFERENCES	65

Introduction

The Introduction tells the reader what the report is about. It sets the project in its wider context, and provides the background information the reader needs to understand the report.

The Introduction:

- introduces the topic of the report in context
- explains the problem and/or motivation for the project
- states the aim/s of the project
- indicates the purpose of the report
- briefly outlines the report structure (not necessary in a short report).

Length: $\frac{1}{2}$ to $\frac{3}{4}$ of a page is sufficient for most undergraduate reports.

In a short report, the technical background necessary to understand the problem may be included in the Introduction. In longer reports this may be summarized in the Introduction and presented in detail in a separate section.



When writing the Introduction, take care not to confuse the report with the project. The project is the work you did; it had an aim, motivation and an outcome. The report is the mode of communicating that work to the reader.

Body of the report

The Introduction and Conclusions act as a frame for the body of the report, which is where you present your own work. The information should be organised so that the reader can follow the development of your project. You will therefore need to put some thought into ordering the sections and choosing concise but informative headings and subheadings.

The body of the report:

- presents the information from your research, both real world and theoretical, or your design
- organises information logically under appropriate headings
- conveys information in the most effective way for communication by means of:
 - figures and tables
 - bulleted or numbered lists
 - formatting to break up large slabs of text.

Presentation conventions and section headings

Provide informative headings

Headings should tell the reader exactly what type of information is contained in the section. They should be specific and content-focused rather than just labels. Devising informative headings as opposed to label headings right from the planning stage will help you to clarify exactly what you want to achieve in each section and subsection.

Compare these pairs of headings:

Uninformative headings	Informative headings
Consumption patterns	Changes in water consumption patterns
Survey results	Turning movement survey results
Overview	Overview of the organisation
Management	Management style and method

Conclusions and recommendations

The Conclusions and Recommendations may be combined or, in long reports, presented in separate sections. If there are no recommendations to be made as a result of the project, just call this section Conclusions.

The Conclusions section sums up the key points of your discussion, the essential features of your design, or the significant outcomes of your investigation. As its function is to round off the story of your project, it should:

- be written to relate directly to the aims of the project as stated in the Introduction
- indicate the extent to which the aims have been achieved
- summarise the key findings, outcomes or information in your report
- acknowledge limitations and make recommendations for future work (where applicable)
- highlight the significance or usefulness of your work.

The conclusions should relate to the aims of the work:

Recommendations

Recommendations are often included with a report's conclusion, although they serve different purposes. Whereas a conclusion offers you the opportunity to summarize or review your report's main ideas, recommendations suggest actions to be taken in response to the findings of a report. You can regard recommendations as a prompt to action for your readers. As you have seen from your planning, your report structure should lead up to the recommendations and provide justification for them. Just as a

proposal grows from your project's goals and objectives, a report should actually grow backwards from your recommendations. Having your recommendations accepted then becomes part of your purpose.

What makes a good recommendation? Effective recommendations:

- describe a suggested course of action to be taken to solve a particular problem;
- are written as action statements without justification;
- are stated in clear, specific language;
- should be expressed in order of importance;
- are based on the case built up in the body of the report; are written in parallel structure.

A word of caution about writing recommendations: you should always consider your relationship with the reader first. If you have no authority to make recommendations, the reader may be hostile to their presence.

Have a look at the following examples from different types of reports. Many of the recommendations included here are well written but a few contain some significant shortcomings. Position your cursor over the excerpts to see our comments.

Example of recommendations

Letter to Jill Bremerton, M.D.
December 14, 2013
page 2

general-purpose tablets can meet our standards for ease of disinfection or durability, and we are not sure whether they have sufficient battery life.

We recommend one of two courses of action: reconsidering the cost criterion or testing a representative sample of general-purpose tablets for disinfection and the other technical characteristics and letting the clinical staff try them out.

We appreciate the trust you have shown in inviting us to participate in this phase of the feasibility study, and we would look forward to working with you on any follow-up activities. If you have any questions or comments, please contact Jeremy Elkins, at jelkins@rrmc.org or at 444-3967, or Eloise Carruthers, at ecarruthers@rrmc.org or at 444-3982.

The major recommendation. The writers ask their supervisor if she will reconsider whether the hospital can afford tablets specifically designed for health-care environments. That's not insubordination. Just be polite about it.

A polite offer to participate further or to provide more information.

tablets, nearly half own an iPad and nearly half an Android tablet, most consider themselves expert users of their tablets, and more than two-thirds already use them in the clinical setting; by a slim margin, they would prefer a hospital-supplied model for tablet use to a BYOD model. Our research on the two models for making tablets available also found more advantages and fewer disadvantages to the hospital-supplied model.

Our principal finding regarding tablets themselves is that the best tablets for our use would be those designed and built for health-care applications. These tablets are rugged and easy to disinfect, and they offer a wealth of hardware and software options that would streamline our daily tasks without introducing any risks either to patient care or to data privacy. Unfortunately, purchasing enough of these tablets for all clinical staff would exceed our budget. To determine whether any of the general-purpose tablets meet all our needs, we would need to conduct hands-on testing regarding disinfection, battery life, durability, and several other technical criteria.

We recommend, first, that we reassess whether the budget will permit consideration of any of the health-care-specific tablets. If that is not possible, we recommend that we ask manufacturers of a small set of general-purpose tablets to let us test their products and invite our clinical staff to demo them. This option would yield data that would help us decide how to proceed.

In the following sections, we provide additional details about our research methods, the results we obtained, the conclusions we drew from those results, and our recommendation.

Notice the writers' use of the phrase "we recommend." Repeating key terms in this way helps readers understand the logic of a report and concentrate on the technical information it contains.

An advance organizer for the rest of the report.

References and appendices

✓ References

All information, methods, data, diagrams and maps, whether obtained or based on the work of others, must be acknowledged using one of the referencing styles recommended for engineering.

✓ Appendices

Appendices contain material that is too detailed to include in the main report, such as long mathematical derivations or calculations, detailed technical drawings, or tables of raw data. The content should be summarised and referred to at the appropriate point in the the body of the report.

The conventions for appendices are as follows:

- each appendix must be labelled with a number (or letter) and title
- the appendix numbers and titles must be listed on the Contents page under the heading Appendices (if more than one) or Appendix (if only one)
- Each appendix must be referred to by number (or letter) at the relevant point in the text.

REFERENCES

1. Computer Network. (2010, February 2). In Wikipedia, the Free Encyclopedia. Retrieved February 3, 2010,
2. Bradley, T. (2010). Introduction to Firewalls. (2010) In About.com: Internet/Network Security . Retrieved,
3. Mitchell, B. (2010). Computer and Wireless Networking Basics. Retrieved March 1, 2010, from About.com:
4. Mitchell, B. (2010). Introduction to Client Server Networks. Retrieved March 1, 2010, from About.com: <http://>
5. <https://www.amazon.com/slp/network-testing-tools/drzmzp8nera39tf>
6. <http://documentation.microfocus.com/help/index.jsp?topic=%2Fcom.borland.silktest.classic.doc%2FSTCLASSIC-B12DC3CE-THE-KINDS-OF-NETWORK-TESTING-YOU-CAN-PERFORM.html>
7. <https://www.softwaretestinghelp.com/network-testing-tools/>
8. https://www.cdc.gov/policy/polaris/policyprocess/problem_identification.html