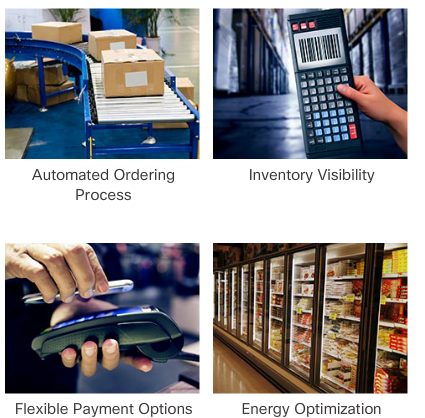
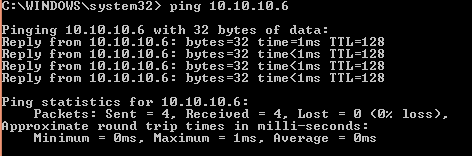
Network troubleshooting tools are necessary for every network administrator in order to make sure network is working fine. Today we are living the modern era of computing most of the task are being done with the help of computing devices so as a good system Administrator you must be familiar with applications as well how to troubleshoot them .



There are few basic commands you should be familiar with if you want to troubleshoot your network.

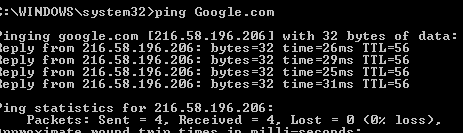
Ipconfig (Quick way to find IP address)

Although you can get IP address of your machine from the control panel but it requires few clicks. The Ipconfig is the best way determines your machine IP address and other information. And that IP address you can use further to check the connectivity for example you want to check the connectivity between two PC on your network just Ping the IP address of other PC from the command prompt if it is successful shows connection is established successfully.

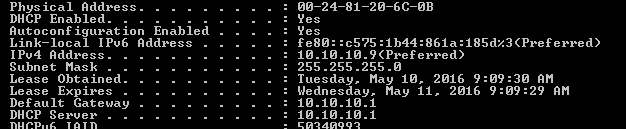


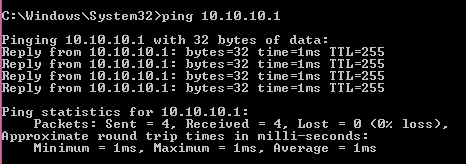
If you are experiencing issues connecting to website you can type ping then Name of website the website will respond and will let you know that it has received packets?

You will be able to see if any packets did not arrive to particular website perhaps you are experiencing connectivity issues.



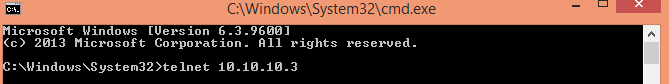
Always it is good practice if you have network connectivity first try to ping to your default gateway it will tells either the problem is occurring after the gateway means on our side or Problem is on the side of service provider and in order to check the default gateway just enter the command “ipconfig / all” without quote .

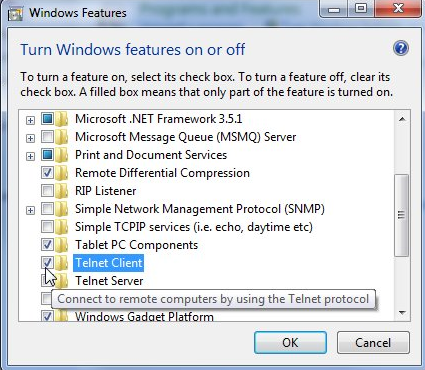
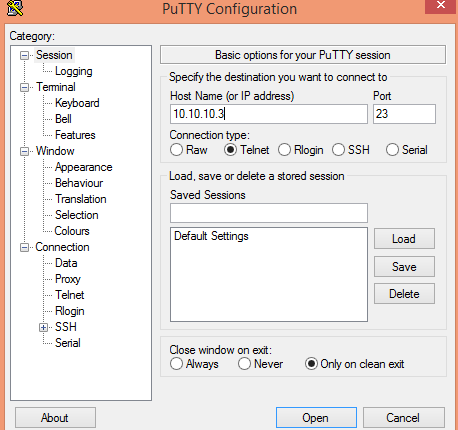




**Telnet**

Telnet is a network protocol that works at Layer one of OSI Model (Physical layer) it allows to log on to other PC or switch remotely . The telnet client is not installed by default you have to install it from the control Panel once installed you can use the telnet command to connect to telnet server by using command or can use popular software known as putty or can type IP address of remote machine followed by Telnet .

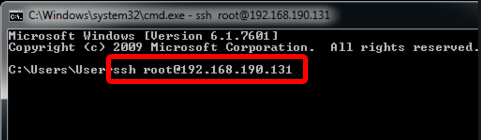
 For example if you want to make remote connection with 10.10.10.3 just type Telnet 10.10.10.3 in the comman prompt.



Telnet is not only used for PC’s to PC’s remote connection it can also be used to make remote connection with switches , routers , and servers .For example one of your company server is located at Kualalumpur and second one at Lahore(Pakistan) in order to make configuration changes in server located at Lahore you have no need to travel to Server location just have to telnet the IP address of remote host and can make the required configuration changes.

**SSH (secure Shell)**

Secure shell is like Telnet but it is more secure all the information being transmitted is encrypted while in telnet information including username and passwords are in plain text this is the reason they can be compromised and hackers can use it for their own purposes.



While root shows the username at the remote host and **192.168.190.131 is the IP address of remote host.**

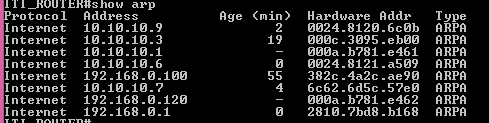
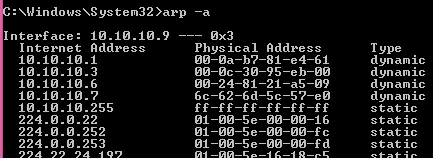
**Currently there are two versions of SSH version 1 and version 2. Version one is less secure as compared to version 2.**

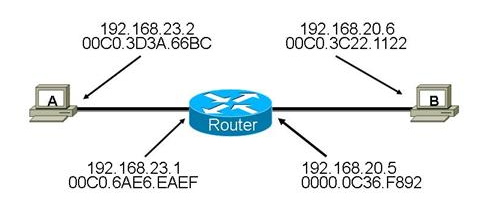
**SSH version 1 transfer speed is about 4 times than SSH version 2 most of the latest networking devices like Switch , routers support the SSH version2.**

**Address resolution protocol (ARP)**

ARP (address resolution protocol) is used to map between IP (internet protocol) and MAC (media access control) of devices in LAN (local area network) from the table we can check which devices are connected to our network and which ones are disconnected. In cisco router or switch we can check the ARP table by using the command “show arp” without quote.

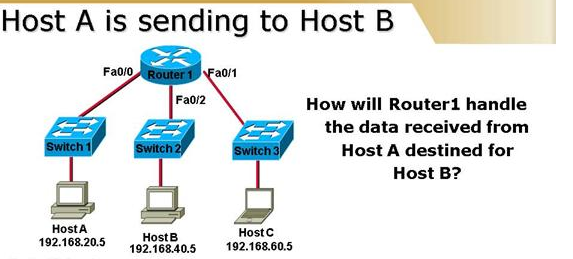
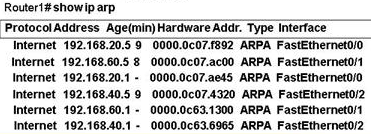
On window operating system this information can be viewed by using the command “arp -a” without quote .





Consider this example PC A want to communicate with PC B so at the Beginning The MAC address of PC A Will **be 00C.3D3A.66BC** and destination MAC address will be **00C0.6AE6.EAEF** but when the Packet will exit the router source Mac address be changed to exit interface of Router **0000.0C36.F892** and destination MAC address will be **00C0.3C11.1122 while the IP address will never be changed.** And function is performed by **using the ARP (Address resolution protocol).**

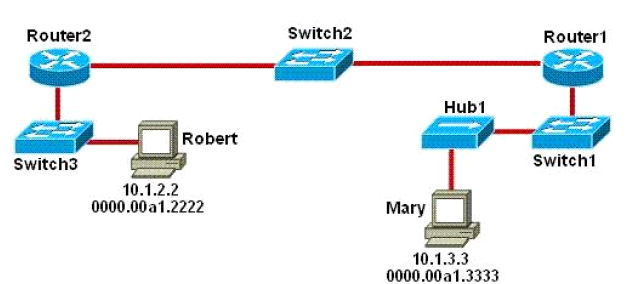
**When HOST A want to communicate with B** first it will use ARP to find the Destination MAC address and that one will be inbound MAC address of Router in our exampl**e 00C0.6AE6.EAEF.** When Packet will arrives at outbound interface of Router it will again perform ARP(Address resolution protocol ) to determine the Destination MAC(media access control) address of destiny. And Thus Source MAC address will be changed to **0000.OC36.F892 and destination MAC address will be 00C0.3C22.1122**

**Another example**

As from the output mentioned above we can observer IP address of HOST B (192.168.40.5) is mapped with MAC address of 0000.0C07.4320 from the interface fa0/2 so the data will be forwarded to interface fa0/2 only.

In case if **ARP cache** is empty Router will first perform ARP (Address resolution protocol) in order to map MAC address with IP address then it will forward to that particular interface.

**Quick Quiz**



Refer to exhibit and tell which three devices will be using destination mac address of packet to determine the forward path?

**Answer with explanation**

**Switch1, switch2, switch3**

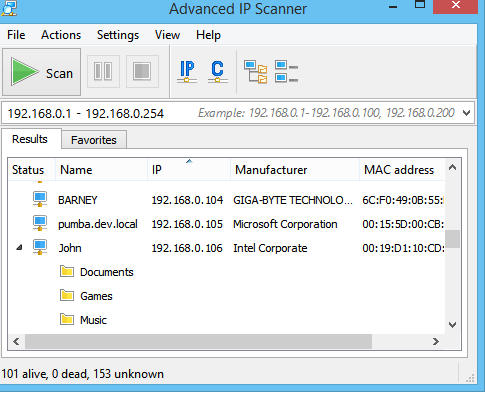
Switches used the destination mac address information for forwarding traffic while router uses IP address for forwarding decision. Local area network Employs layer 2 switches and bridges to forward and filter network traffic. Switches are bridges are able to listen to traffic on wire to examine the source and destination MAC address. Being able to listen to traffic also allows the switches and bridges to compile MAC address take to better filter and forwarding network traffic.

When a switch or bridge is listening to network traffic, it receives each frame and compares it to the MAC address table. By checking the MAC address table the switch/bridge is able to determine which port frame came in on if the SOURCE MAC address is not present in MAC table it is added to MAC address table And if the destination MAC address is not present in MAC address table the frame is forwarded to all ports except the port from which frame was received.

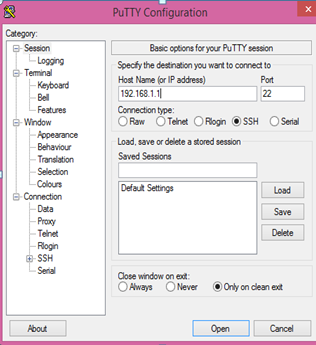
**Advanced IP Scanner**

**Advanced IP scanner is a free tool that scans your LAN or WI-FI network and provides the information about the devices connected to it. It can also shutdown networked computer remotely, also wake them if your network card supports WAKE-ON-LAN standard.**

**By using the IP scanner we can get the IP( internet protocol) as well MAC(media access control) address of devices on our network and by looking at MAC address table and computer names we can get the information of all devices connect to network.**



**And from the PC on which IP Scanner is installed we can Do telnet, SSH, ping and tracert also the details about that particular PC can be seen remotely.**

**SSH(secure shell) : Secure shell works like Telnet but in Telnet all data is sent in clear text so if someone from outside get access to network He/she can see the sensitive information being transferred over network . While in SSH data being sent and received is encrypted so outsiders cannot read it a free software known as putty can also be used to establish SSH connection with PC, switch, Router or Server. The older version of IOS does not support SSH they only support Telnet.**

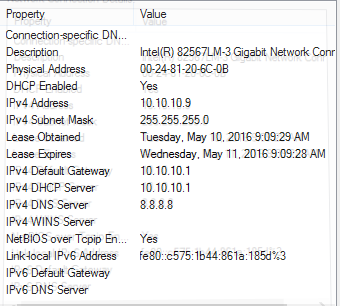
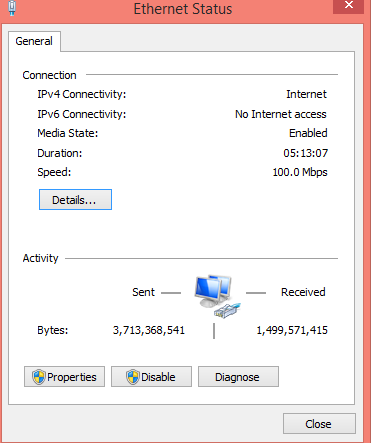
**DNS problems**

**Sometimes connectivity problems occur because of DNS (domain name system) issues sometimes either DNS server is not available or DNS is not configured properly. DNS is a protocol that converts Domain names in to IP address.**

**Many times if you open web browser, go for URL and URL fails to bring up a website this problem is usually caused by DNS(domain name server) but before Blaming to DNS server start troubleshooting by checking the Layer 1 (Physical layer) then check the network connectivity.**

**It can be checked just right click on your network either it is WIFI or Cable connection and Go to open network and sharing center from here click on your network. From the output we can observe that connection is established there is no problem at Layer 1(Physical Layer) .**

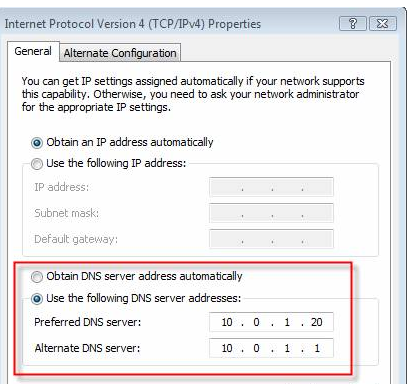
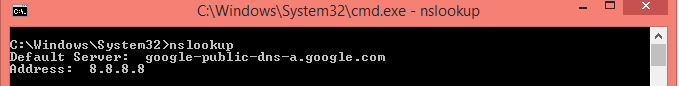
**In order to check the further details click on Details and further information can be retrieved .**



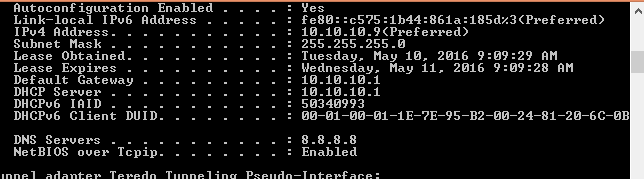
**DNS information can be configured or can be retrieved from DHCP (Dynamic host configuration Protocol) if want to use two DNS server it is also permitted in window system.**

**Usually we use DNS server (8.8.8.8) which is the DNS server of Google DNS server can also be installed locally on server being used at Our LAN that will decrease the DNS query response time.**

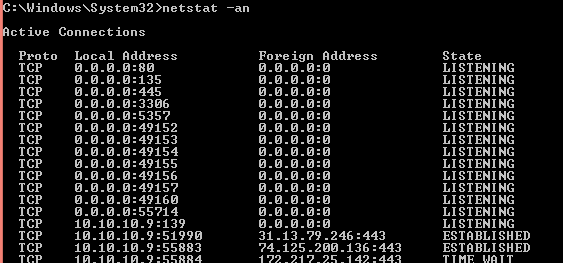
**You can get the information about your DNS server by using the command “nslookup” without quote in the command prompt.**



**OR The information about DNS can be found by using simple command “ipconfig /all” without quote**



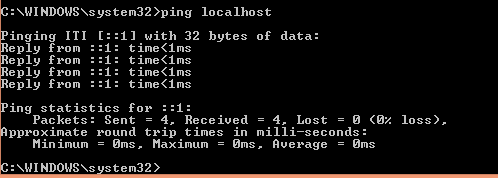
**Netstat (network statistics)**

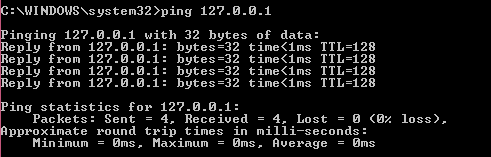
**Another useful command that can be used for displaying all sort of network traffic it can be used with different options . One of them is Netstat –an which will displays a list of all open network connections on your computer along with port number they are using and the foreign IP address they are connected to .**

**Loopback address**

Loopback address is a special type of IP address that is designed for software loopback interface of machine. It is always a good practice you check the connectivity to your network interface card **(127.0.0.1) that is also known as loopback address before addressing the other connectivity issues. These loopback addresses are very useful in routing can also be used to identify Routers and switches.**

**IN IPV6 (internet protocol version 6) this loopback address is :: 1/128 can also be written as ::1.it will verify our that network card is capable of pinging itself using the ping command.**





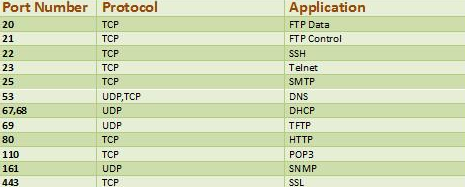
**Verifying connections**

 If you are using a laptop with a wireless network, look for laptop WIFI (wireless fidelity) button and make sure it is turned on. Many Laptops have a Wi-Fi button that allows the wireless network to turn ON or OFF.



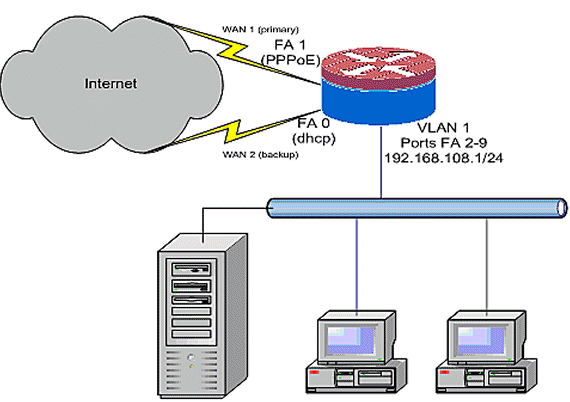
**Firewall**

**If your computer utilizes a firewall make sure all the required ports are open especially the port 80 which is HTTP (hypertext transfer protocol) port it is closed we can’t use the HTTP services.**



If possible disable or disconnect the firewall at the time of troubleshooting the network connectivity.

**Internet is not working**

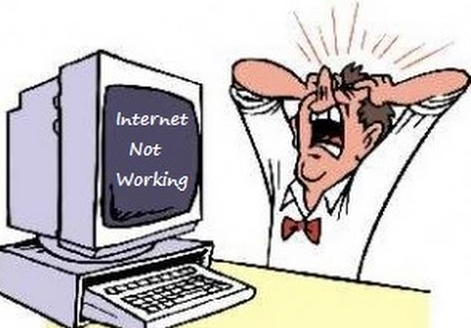
**if you are able to ping to router but still unable to connect to internet , it shows either your router is improperly configured or the ISP(internet service provider) is having issues.**

**The router address can be found by using the command (ipconfig) .**

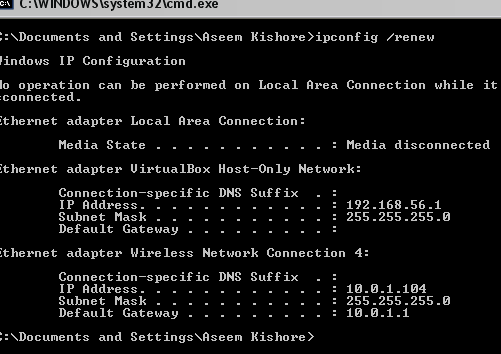
**If your internet has been working but recently stopped working give it few minutes to make sure it is not a temporary outage. If after waiting a few minutes you still have problems follow the steps below.**

1. **Turn off the power to computer/laptop and leave it off.**
2. **Unplug the power cable to your router and cable modem or DSL modem.**
3. **Leave the power cables disconnected for 10-15 seconds plug your modem again, and plug your router again.**
4. **Finally turn on your computer and see if you can ping to your router if it is successful then ping to** [**www.Google.com**](http://www.Google.com)**.**
5. **If your ping to** [**www.Google.com**](http://www.Google.com) **is successful it means your connection is established.**

**While pinging if you are not getting reply from** [**www.Google.com**](http://www.Google.com) **means your router or modem is not reaching the internet, make sure your router has DHCP enabled and default gateway is properly configured.**



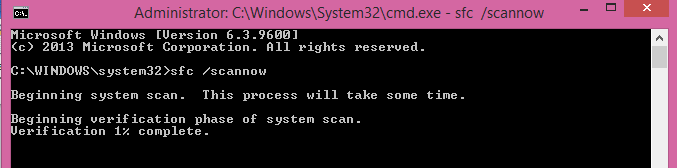
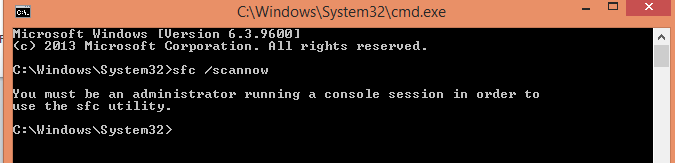
**Renew your IP Address**

 **Sometimes by renewing the IP(internet protocol) address can resolve the IP address problem can it can be done using the command ipconfig/renew and all the information related to IP address will be renewed by DHCP(dynamic host configuration protocol) .**

**SFC /Scannow**

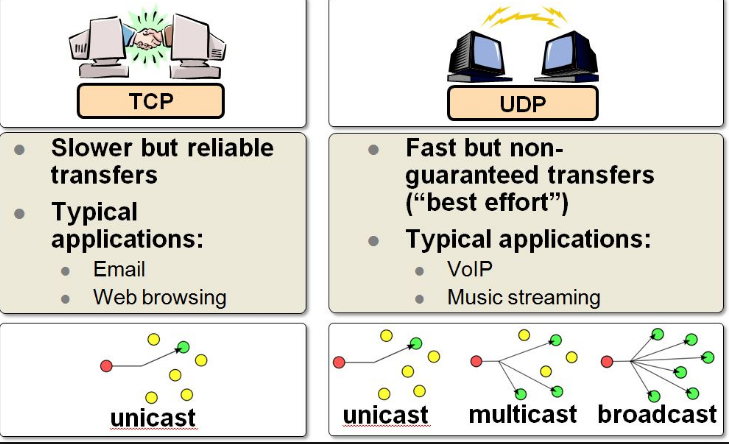
**If your PC has been feeling buggy or having trouble during startup, it is possible that window system have become corrupt , gone missing or even have been changed by a software installation somewhere along the line .So that command can be used to fix these issues furthermore this command can be used to scan the system.**

**Remember you have to open command prompt in Administrator mode else this command will not work.**



**TCP (Transmission control Protocol)**

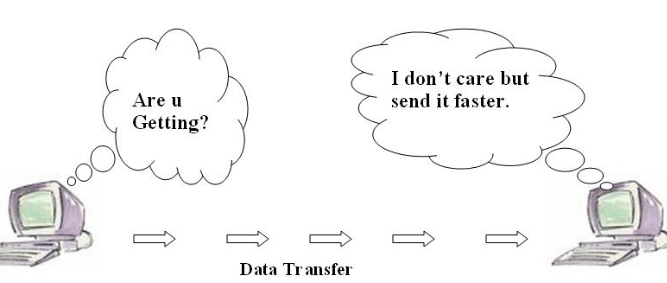
**TCP is a standard that defines how to establish and maintain a network conversation via which application programs can exchange the data. TCP works with internet protocol (IP) in TCP communication a dedicated connection must be established between sender and receiver.**



**UDP (user data gram protocol)**

**UDP is alternative communication protocol to TCP used primarily for establishing low latency and loss tolerating connections between applications on the internet. Sometimes connection to internet or any service is denied because of access list so make sure your connection is allowed by access list. The required TCP or UDP port is allowed to pass the traffic over the internet.**

**Always remember TCP is connection oriented while UDP is connection less in TCP dedicated connection is established to move data from sender side to destination host while in UDP it can take several paths to reach the destination.**

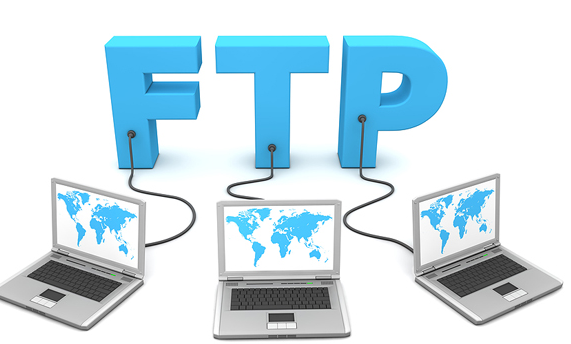
**In TCP during the communication if some packets are lost they need to retransmit again while in UDP (user datagram protocol) there is no need to transmit the lost data again.**

**Quick Quiz**

**(1) Which protocol is used to transfer the files between the end systems?**

1. FTP (File transfer protocol)
2. DNS(Domain Name system)
3. HTTP(Hypertext transfer protocol)
4. SMTP(Simple mail transfer protocol)

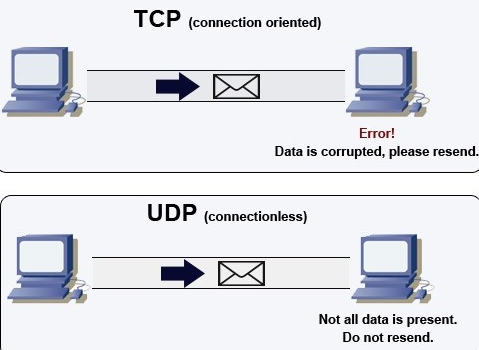
**Answer: FTP is acronym for File Transfer Protocol FTP is used to transfer the files between the computers on network you can also use to download online software archives.**



**(2) Which protocol is used to established dedicated connection between the hosts**

1. TCP(Transmission control protocol)
2. DHCP(Dynamic host configuration protocol)
3. ARP(Address resolution Protocol)
4. RARP(Reverse Address resolution protocol)

**Answer: TCP is used to establish dedicated connection between two hosts. It provides reliable transfer of file unlike UDP which does not guarantee the delivery of packets.UDP (User datagram protocol) is also referred as “Best effort delivery”.**

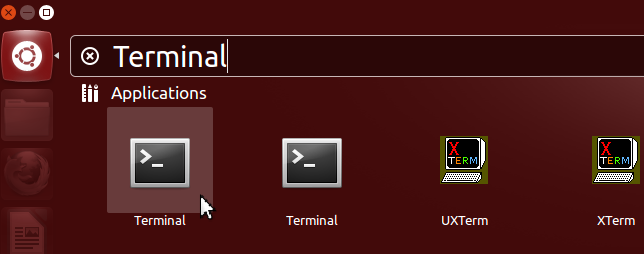


**Linux Terminal**

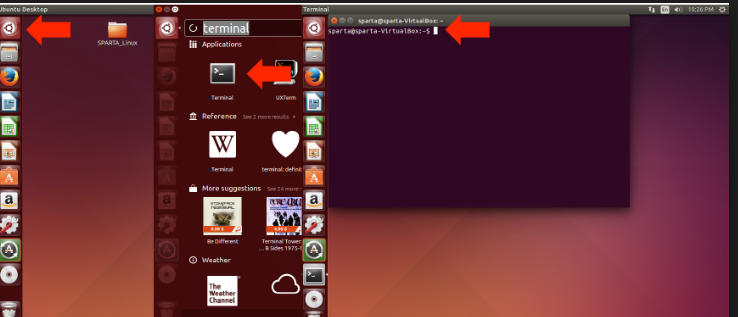
**Linux terminal is same like CMD (command prompt) in window based system in Linux or Unix based system we use the Terminal. Here you have to type the command in order to give instructions to computer. Today most of the established organization uses Linux based system instead of window based system because Linux based system have free source code anyone can update and make changes .Another important feature of Linux based system is Security these system are more secure than window based system .**

**Starting Terminal**

**Utility is a default desktop environment in order to open the Terminal the easiest option is to use the search option or you may click on “more app” button , click the “see more results” and in the installed section you can find the list of applications installed in the system.**

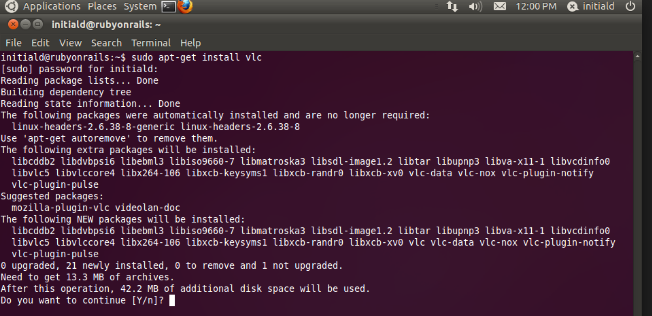


**Another easiest way that can be used on some versions of Linux operating system(like 16.04) is just right click on desktop it will give the option of open terminal just click on it Linux terminal will be open.**



**Linux terminal has wide range of commands that can be used to accomplish the various task unlike windows operating system in Linux based system we can install , uninstall the program or Packages using the command line and much more .**

**For example to install VLC media player on your Linux based system there is no need to go Online to search the VLC , then download and then to follow some steps to install the software.**



**The commands used in Linux are different than commands used in CMD(command prompt) in window based system .**

**For example to find the IP address of computer in CMD (command prompt) we use the command of Ipconfig while in Terminal we have to use the “ifconfig” without quote.**

**Information security**

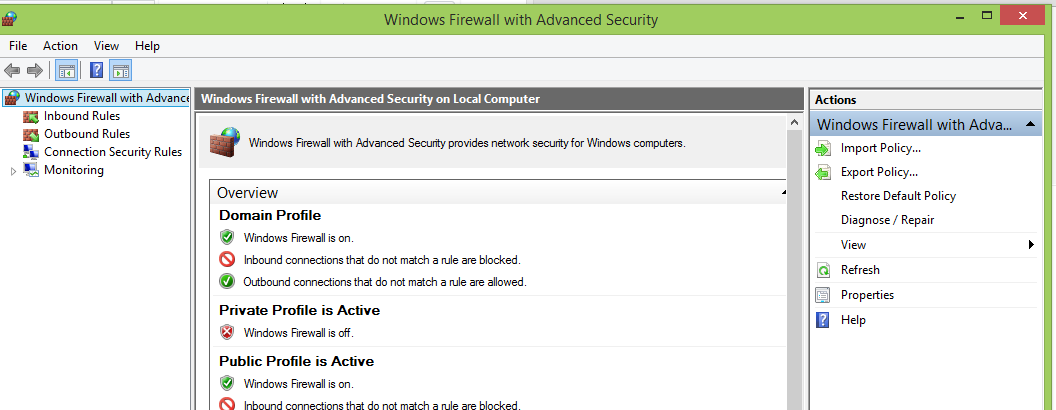
**It is the process of protecting the data from those who has malicious intent.**

**“Think like a hacker and Defend like a Ninja”**

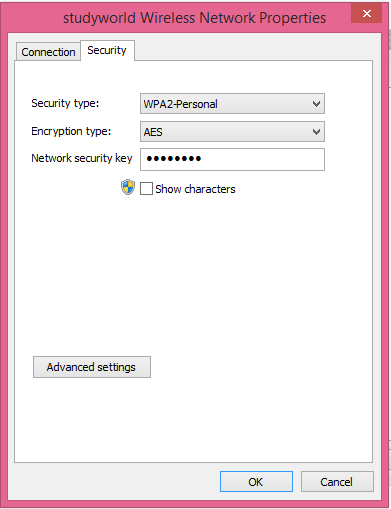
**In order to protect your computer from viruses, spies, warms, and outsiders the following steps can be taken in order to mitigate the risk.**

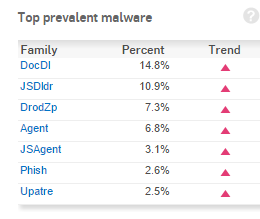
1. **Install a firewall:**

**A firewall is a software or piece of hardware that blocks hackers from entering and using your computer. In window based operating system it is already installed you can define your own rules based on requirements. You can also install additional firewall.**



1. **Use Anti-virus software: It will protect your computer from viruses that can destroy your data, slow down or even crash your computer. The most commonly used anti-virus software includes Avast anti-virus, Antiwar, NOD32 and etc.**
2. **Use Anti-spy software: spyware is a software that is installed without your knowledge or consent that can monitor your activities.**
3. **User Strong password and keep it to yourself: Hackers are constantly trying to find flaws or holes in operating system and browsers. In order to protect your OS (operating system) and information inside it use a strong password.**
4. **Secure your wireless network: if you use a wireless in your home or office be sure to take precautions against hackers. Encryption wireless communication is first step. WPA (wireless protected access) is better than WEP (wired equivalent Privacy).**





**6. be careful if your share files: Many consumers enjoy sharing digital files, such as music, movies, photos and software’s. Files sharing can pose several risks. When connected to file-sharing network you may allow others to copy files that you do not intend to share so are careful.**

Quick Quiz

(1) What are two common practices that make your password vulnerable?

1. Changing password very frequently
2. Using SHA-256 to encrypt your password
3. Using the same password for many accounts.
4. Using password with complex mix of characters.

Explanation: B and D are true if we will encrypt our password it will be converted into different symbols that can’t be interpreted by human. Also if the password is the mixture of numbers and characters it will be more difficult to guess and break it.

(2) What is the purpose of DNS (domain name system)?

1. To translate domain name into IP (internet protocol).
2. Is used for clock synchronization
3. Is used to assign automatically IP (internet protocol) address to PCs.
4. None of the above

(3) In Linux which command performs the same function as Ipconfig?

Answer: In Linux we use “ifconfig” instead of ipconfig.

(4) What is the syntax to install program from terminal in Linux based system?

1. Sudo apt-get install package name
2. Yum –get install package name
3. Sudo apt-get remove package name
4. None of them

Answer: in order to install package in Linux based system we use the command **Sudo apt-get install package name A is correct.**

**(5)** Write-down three difference between TCP(transmission control protocol) and UDP(user datagram protocol**)**

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| Connection oriented | Connectionless |
| Reliable | Not reliable |
| Acknowledgement Segments | No acknowledgements |