

Assignment No. 07

Aim: Introduction to server administration (server administration commands and their applications) and configuration of

a. Telnet

b. FTP

c. DHCP

Theory :

Introduction:

A server administrator, or admin has the overall control of a server. This can be in the context of a business organization, where often a server administrator oversees the performance and condition of multiple servers in the business, or it can be in the context of a single person running a game server. The admin for a server typically represents the owners and financiers of the server. Alternatively, an owner can grant administrator rights to a regular player (or clan member) on the server.

The Server Administrator's role is to design, install, administer, and optimize company servers and related components to achieve high performance of the various business applications supported by tuning the servers as necessary. This includes ensuring the availability of client/server applications, configuring all new implementations, and developing processes and procedures for ongoing management of the server environment. Where applicable, the Server Administrator will assist in overseeing the physical security, integrity and safety of the data center/server farm.

a) Telnet:

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). Telnet was developed in 1968 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards. Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration (including systems based on Windows NT). However, because of serious security issues when using Telnet over an open network such as the Internet,

its use for this purpose has waned significantly in favor of SSH. The term telnet may also refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. Telnet is also used as a verb. To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "To change your password, telnet to the server, log in and run the passwd command." Most often, a user will be telnetting to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

History and standards: Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

Security: When Telnet was initially developed in 1969, most users of networked computers were in the computer departments of academic institutions, or at large private and government research facilities. In this environment, security was not nearly as much a concern as it became after the bandwidth explosion of the 1990s. The rise in the number of people with access to the Internet, and by extension the number of people attempting to hack other people's servers, made encrypted alternatives necessary.

b) FTP:

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server. FTP is built on client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different. The first FTP client applications were command-line applications developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as Web page editors.

History of FTP server: The original specification for the File Transfer Protocol was written by Abhay Bhushan and published as RFC 114 on 16 April 1971. Until 1980, FTP ran on NCP, the predecessor of TCP/IP. The protocol was later replaced by a TCP/IP version, RFC 765 (June 1980) and RFC 959 (October 1985), the current specification. Several proposed standards amend RFC 959, for example RFC 2228 (June 1997) proposes security extensions and RFC 2428 (September 1998) adds support for IPv6 and defines a new type of passive mode.

Protocol overview:

- i) **Communication and data transfer:** FTP may run in active or passive mode, which determines how the data connection is established. In both cases, the client creates a TCP control connection from a random unprivileged port N to the FTP server command port 21. In active modes, the client starts listening for incoming data connections on port N+1 from the server (the client sends the FTP command PORT N+1 to inform the server on which port it is listening).
- ii) **Login:** FTP login utilizes a normal username and password scheme for granting access. The username is sent to the server using the USER command, and the password is sent using the PASS command. If the information provided by the client is accepted by the server, the server will send a greeting to the client and the session will commence. If the server supports it, users may log in without providing login credentials, but the same server may authorize only limited access for such sessions.
- iii) **Anonymous FTP:** A host that provides an FTP service may provide anonymous FTP access. Users typically log into the service with an 'anonymous' (lower-case and case-sensitive in some FTP servers) account when prompted for user name. Although users are commonly asked to send their email address instead of a password, no verification is actually performed on the supplied data. Many FTP hosts whose purpose is to provide software updates will allow anonymous logins.

c) DHCP :

The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Overview: Dynamic Host Configuration Protocol is used by computers for requesting Internet Protocol parameters, such as an IP address from a network server. The protocol operates based

on the client-server model. DHCP is very common in all modern networks ranging in size from home networks to large campus networks and regional Internet service provider networks. Most residential network routers receive a globally unique IP address within the provider network. Within a local network, DHCP assigns a local IP address to devices connected to the local network. When a computer or other networked device connects to a network, its DHCP client software in the operating system sends a broadcast query requesting necessary information. Any DHCP server on the network may service the request. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers.

History: DHCP was first defined as a standards track protocol in RFC 1531 in October 1993, as an extension to the Bootstrap Protocol (BOOTP). The motivation for extending BOOTP was that BOOTP required manual intervention to add configuration information for each client, and did not provide a mechanism for reclaiming unused IP addresses. DHCP development culminated in RFC 2131 in 1997, and remains as of 2014 the standard for IPv4 networks.

Printouts to be taken:

a) Install Telnet Server

Applies To: Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Vista

The Telnet Server service is not installed by default on Windows 7, Windows Server 2008 R2, Windows Vista or Windows Server 2008. The procedures to install Telnet Server vary based on the operating system you are using:

- Install Telnet Server by using a command line
- Install Telnet Server on Windows Server 2008 R2 and Windows Server 2008
- Install Telnet Server on Windows 7 and Windows Vista

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

Install Telnet Server by using a command line

On Windows 7, Windows Server 2008 R2, Windows Server 2008, or Windows Vista you can use the following command line procedure to install Telnet Server.

To install Telnet Server using a command line

1. Open a command prompt window. Click **Start**, type **cmd** in the **Start Search** box, and then press **ENTER**.
2. Type the following command:
3. `pkgmgr /iu:"TelnetServer"`
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. When the command prompt appears again, the installation is complete.

Install Telnet Server on Windows Server 2008 R2 and Windows Server 2008

On Windows Server 2008, you can use the Role Management tool to install optional components.

To install Telnet Server on Windows Server 2008 R2 and Windows Server 2008

1. Start Server Manager. Click **Start**, right-click **Computer**, and then click **Manage**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. In the **Features Summary** section, click **Add features**.
4. On the **Select Features** page, select **Telnet Server**. You can also select **Telnet Client** if you want.
5. Click **Next**, and then on the **Confirm Installation Options** page, click **Install**.
6. On the **Installation Results** page, click **Close**.
7. Close **Server Manager**.

Install Telnet Server on Windows 7 and Windows Vista

On Windows Vista, you can use the Windows Features tool to install optional components.

To install Telnet Server on Windows 7 and Windows Vista

1. Click **Start**, and then click **Control Panel**.
2. On the **Control Panel Home** page, click **Programs**.
3. Under the section titled **Programs and Features**, click **Turn Windows features on or off**.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. In the **Windows Features** list, select **Telnet Server**, and then click **OK**.

Install Telnet Client

Applies To: Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Vista

Telnet Client is not installed by default on Windows 7, Windows Server 2008 R2, Windows Vista, or Windows Server 2008. The procedures to install Telnet Client vary based on the operating system you are using:

- Install Telnet Client by using a command line
- Install Telnet Client on Windows Server 2008 R2 or Windows Server 2008
- Install Telnet Client on Windows 7 or Windows Vista

Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.

Install Telnet Client by using a command line

On Windows 7, Windows Server 2008 R2, Windows Server 2008 or Windows Vista you can use the following command line procedure to install Telnet Client.

To install Telnet Client by using a command line

1. Open a command prompt window. Click **Start**, type **cmd** in the **Start Search** box, and then press **ENTER**.
2. Type the following command:
3. `pkgmgr /iu:"TelnetClient"`
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. When the command prompt appears again, the installation is complete.

Install Telnet Client on Windows Server 2008 R2 or Windows Server 2008

On Windows Server 2008, you can use the Role Management tool to install optional components.

To install Telnet Client on Windows Server 2008 R2 or Windows Server 2008

1. Start Server Manager. Click **Start**, right-click **Computer**, and then click **Manage**.
2. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
3. In the **Features Summary** section, click **Add features**.

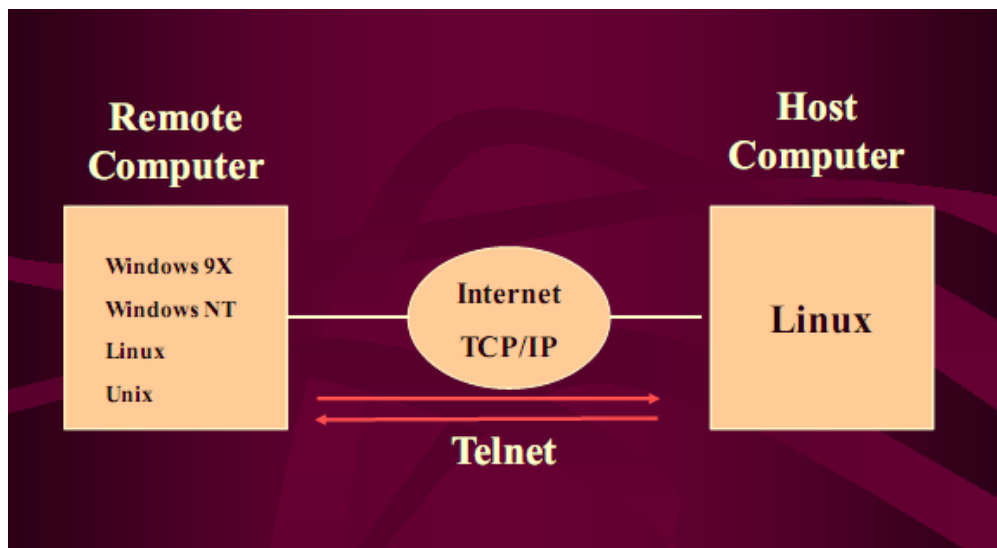
4. In the **Add Features Wizard**, select **Telnet Client**, and then click **Next**.
5. On the **Confirm Installation Options** page, click **Install**.
6. When installation finishes, on the **Installation Results** page, click **Close**.

Install Telnet Client on Windows 7 or Windows Vista

On Windows 7, Windows Vista, you can use the Windows Features tool to install optional components.

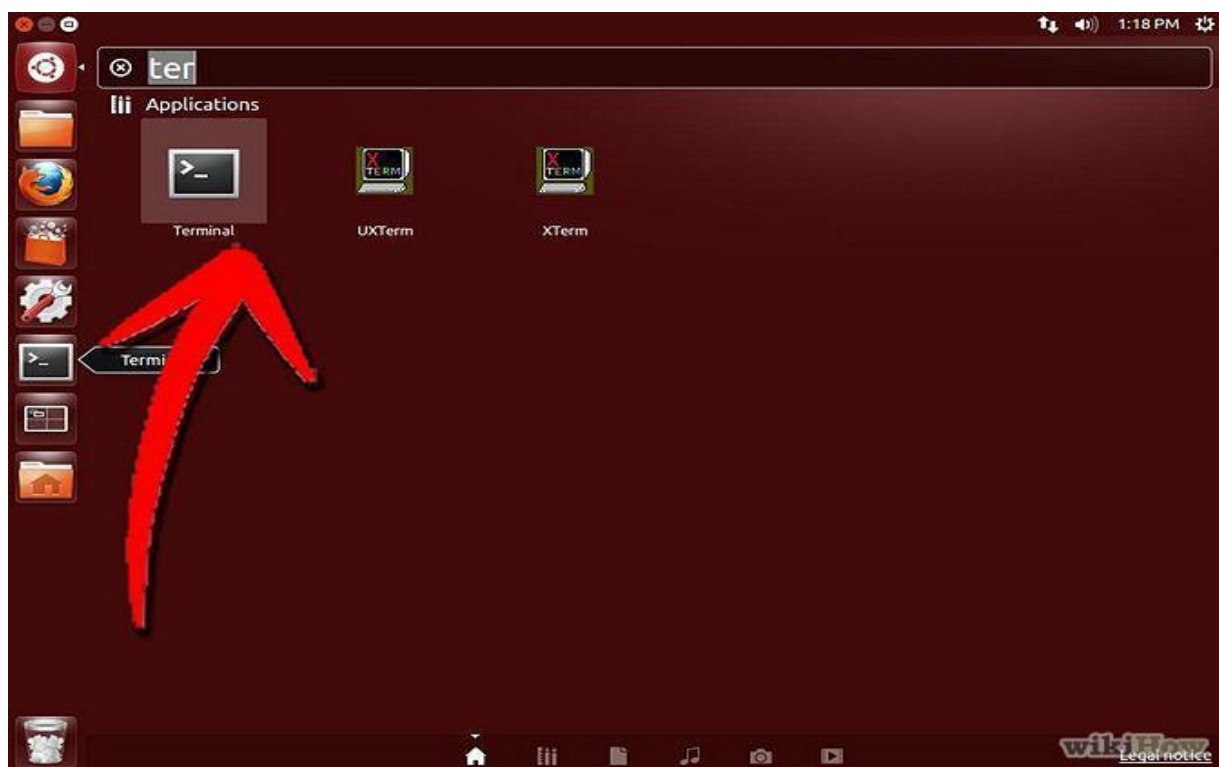
To install Telnet Client on Windows 7 or Windows Vista

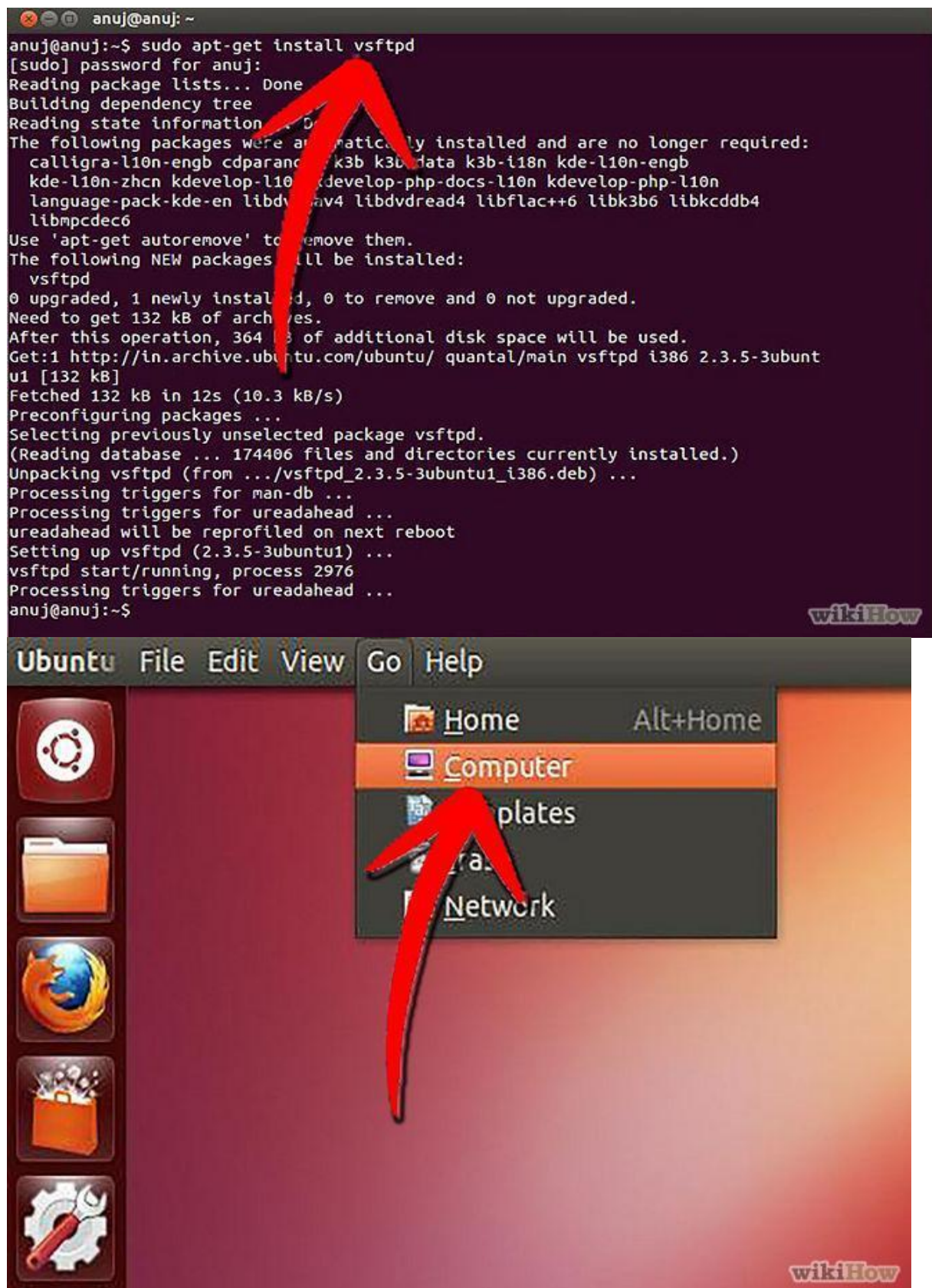
1. Click **Start**, and then click **Control Panel**.
2. On the **Control Panel Home** page, click **Programs**.
3. In the **Programs and Features** section, click **Turn Windows features on or off**.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. In the **Windows Features** list, select **Telnet Client**, and then click **OK**.

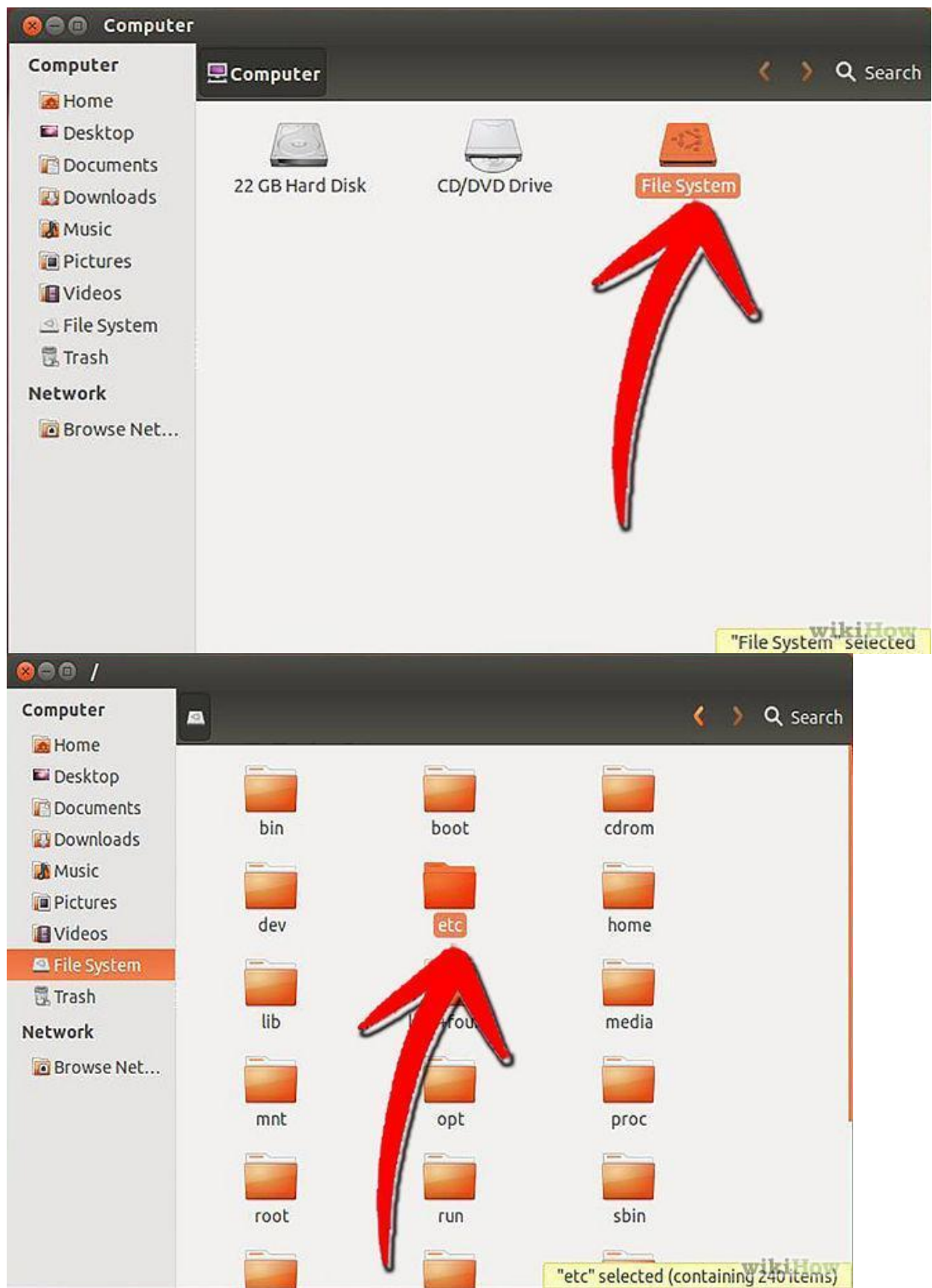


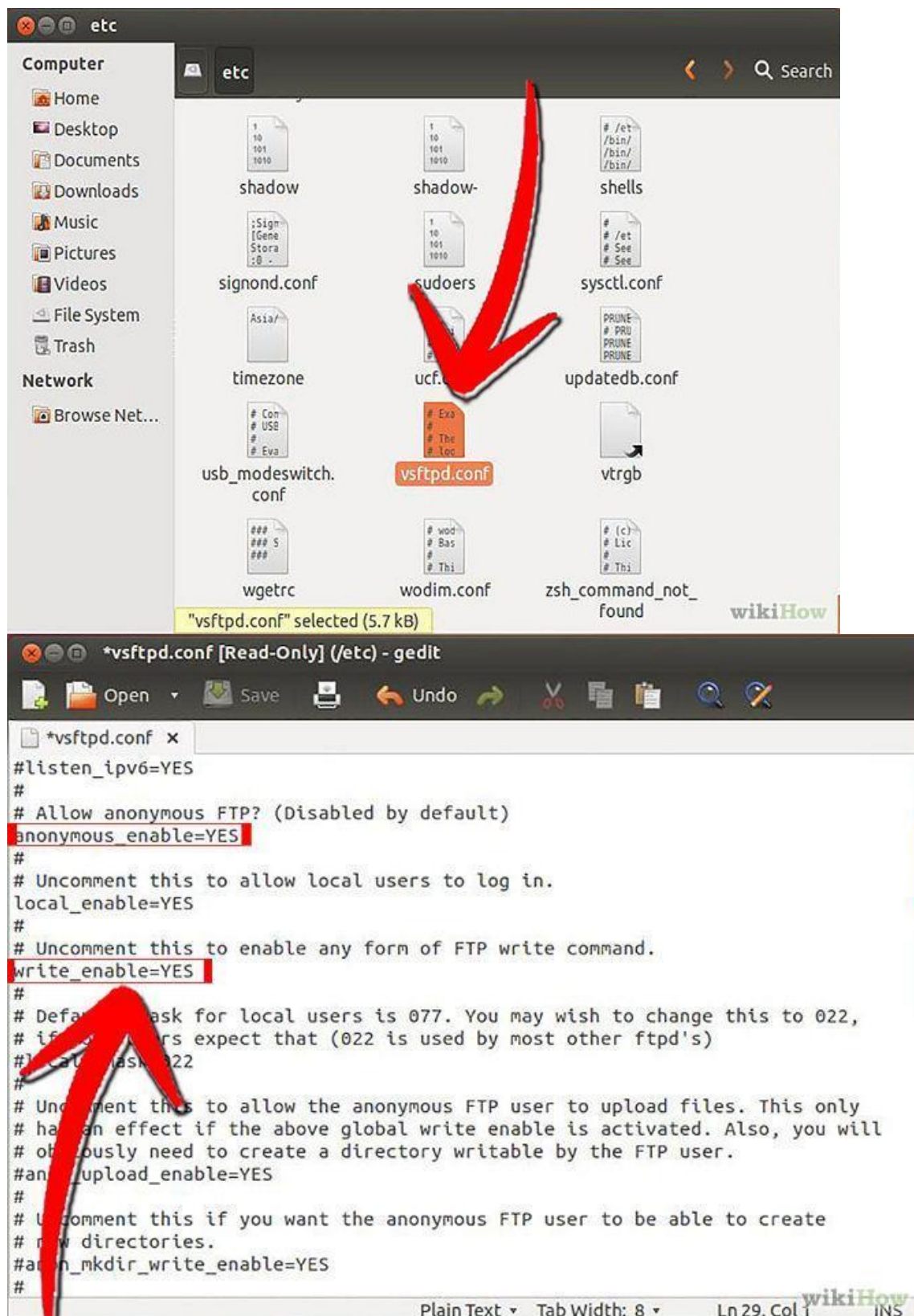
b) FTP Installation:

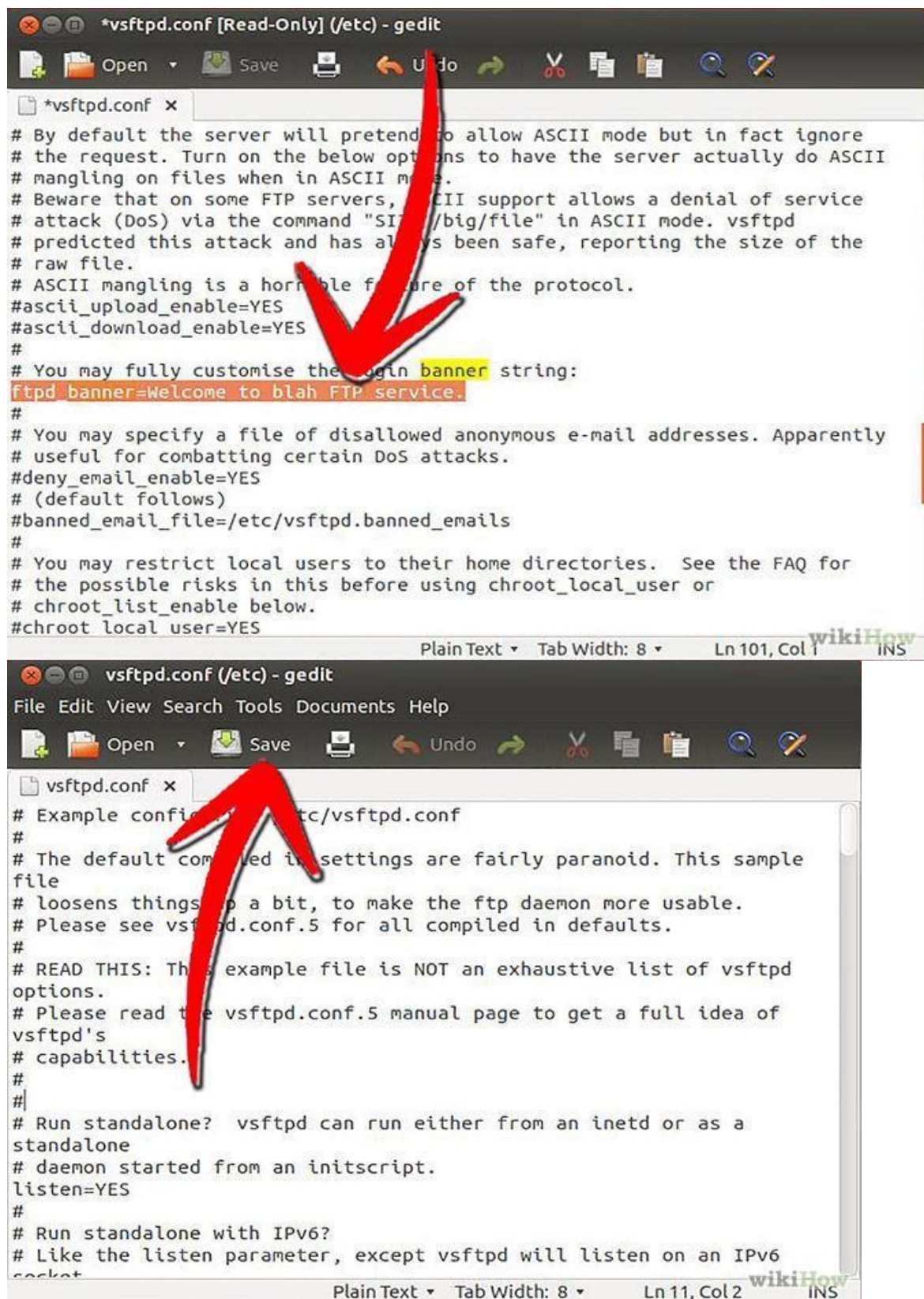
1

Boot up Ubuntu Linux.



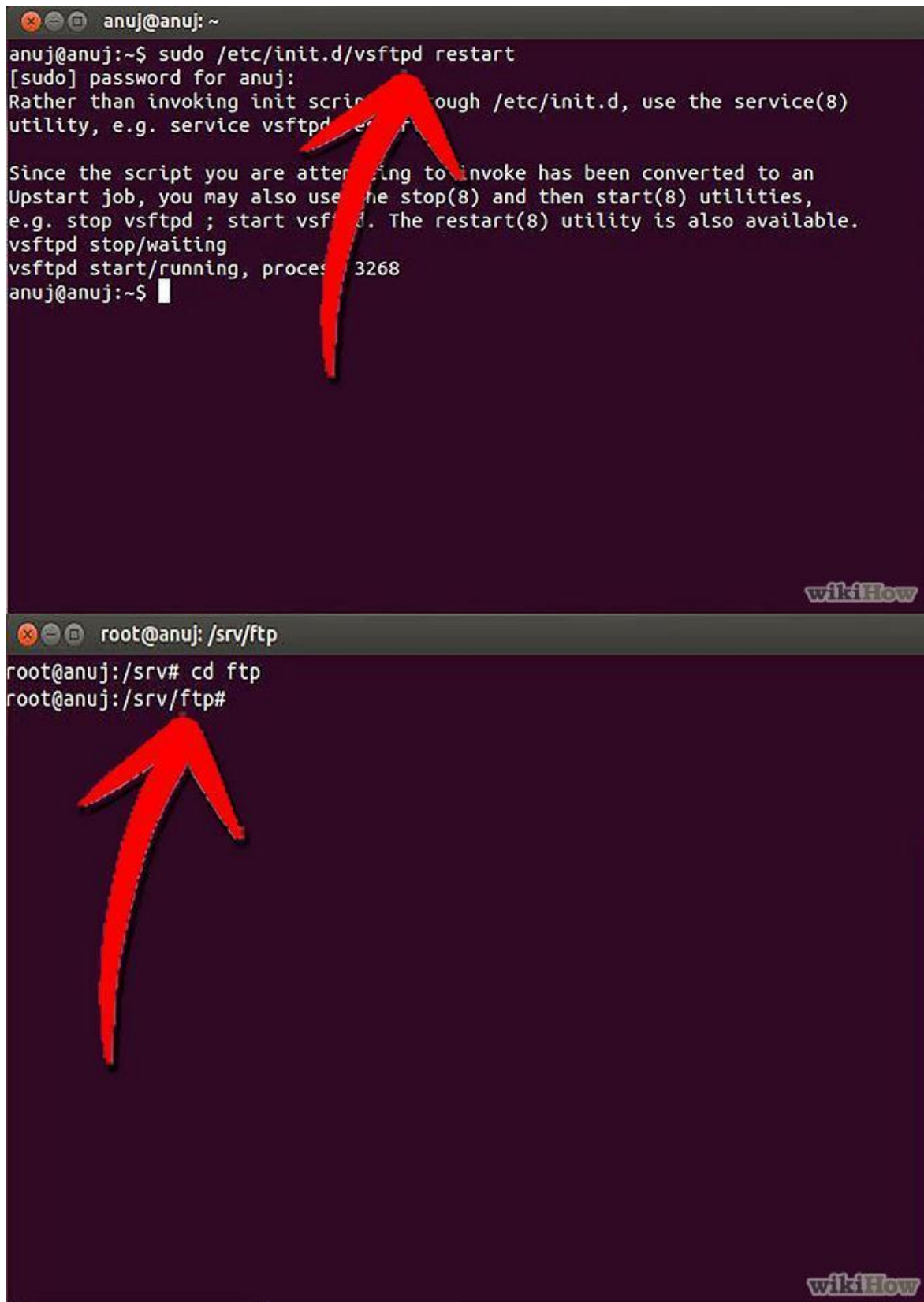






```
*vsftpd.conf [Read-Only] (/etc) - gedit
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SITE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories. See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#chroot local user=YES

vsftpd.conf (/etc) - gedit
File Edit View Search Tools Documents Help
# Example configuration file for vsftpd. See /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd
# options.
# Please read the vsftpd.conf.5 manual page to get a full idea of
# vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a
# daemon started from an initscript.
listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6
# socket.
```

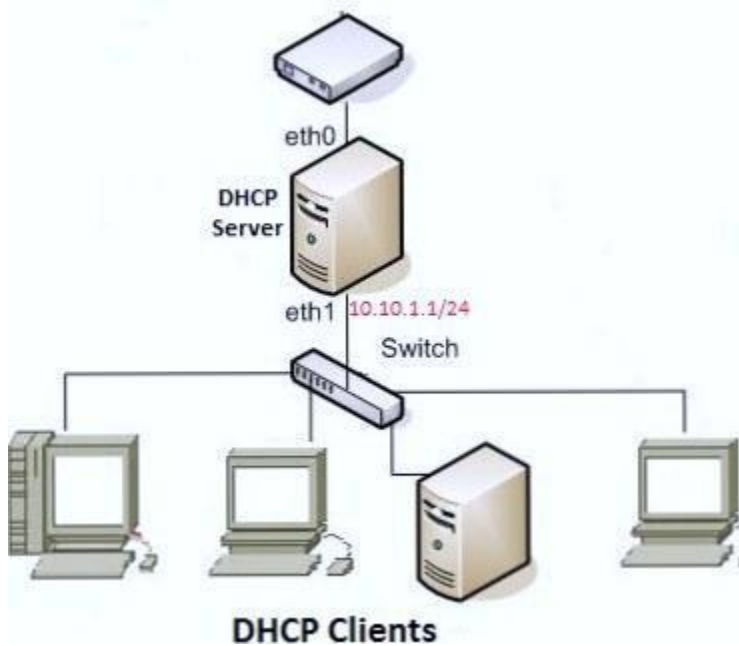


The image consists of two terminal window screenshots. The top screenshot shows a user named 'anuj' at a prompt 'anuj@anuj: ~'. They execute the command 'sudo /etc/init.d/vsftpd restart'. The terminal output shows a password prompt, followed by a message advising to use 'service(8)' instead of '/etc/init.d'. It then shows 'vsftpd stop/waiting' and 'vsftpd start/running, process 3268'. A red arrow points from the 'restart' command to the 'service(8)' advice. The bottom screenshot shows a root user at a prompt 'root@anuj: /srv/ftp'. They execute 'cd ftp' and the prompt changes to 'root@anuj: /srv/ftp#'. A red arrow points from the 'cd ftp' command to the new prompt. Both screenshots have a 'wikiHow' watermark in the bottom right corner.

```
anuj@anuj:~$ sudo /etc/init.d/vsftpd restart
[sudo] password for anuj:
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service vsftpd restart
Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the stop(8) and then start(8) utilities,
e.g. stop vsftpd ; start vsftpd. The restart(8) utility is also available.
vsftpd stop/waiting
vsftpd start/running, process 3268
anuj@anuj:~$
```

```
root@anuj: /srv/ftp
root@anuj: /srv# cd ftp
root@anuj: /srv/ftp#
```

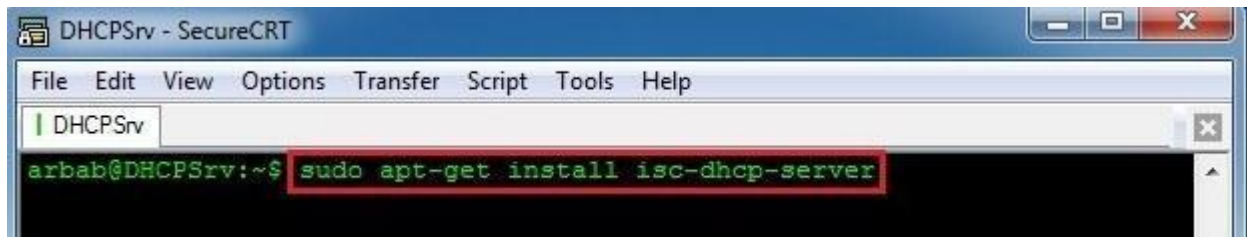
c) DHCP Installation:



Ubuntu as DHCP Server:

To install dhcp server, enter the following command at a terminal prompt:

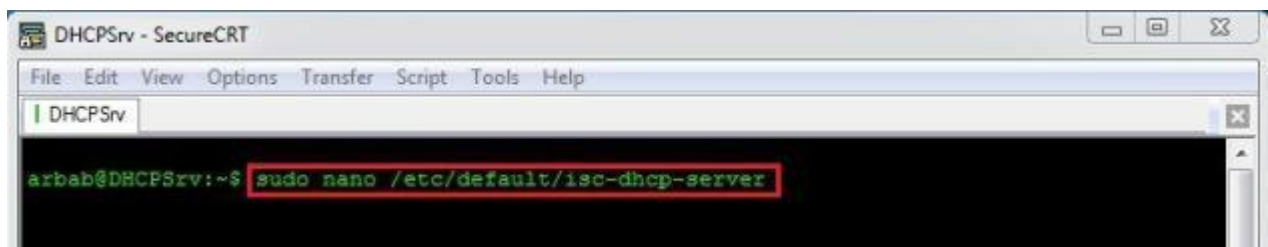
```
sudo apt-get install isc-dhcp-server
```



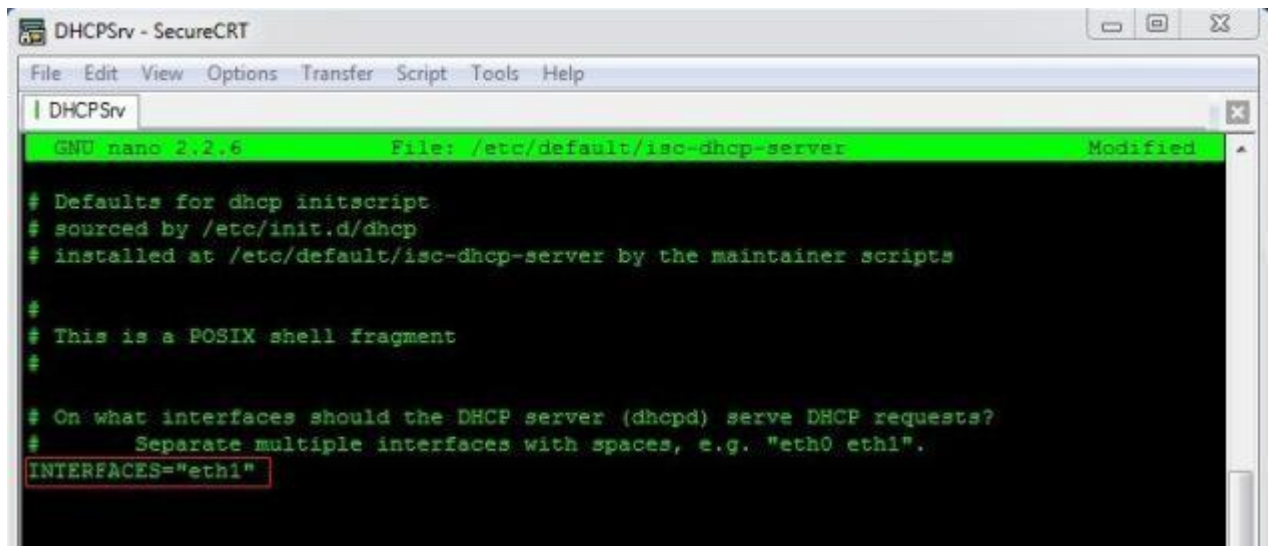
If there is more than one network card(s) in your Ubuntu server, then you have to select the network card on which your server will be listen for dhcp request. (By default, it listens on **eth0**).

You can change this by editing `/etc/default/isc-dhcp-server` file:

```
sudo nano /etc/default/isc-dhcp-server
```



Change “**eth0**” to the interface on which you want that your server will listen for dhcp request (In my case, it is **eth1**):



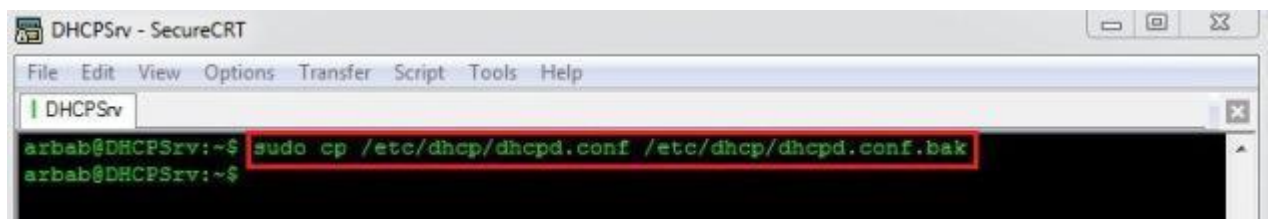
```

DHCPsrv - SecureCRT
File Edit View Options Transfer Script Tools Help
| DHCPsrv
GNU nano 2.2.6 File: /etc/default/isc-dhcp-server Modified
# Defaults for dhcp initscript.
# sourced by /etc/init.d/dhcp
# installed at /etc/default/isc-dhcp-server by the maintainer scripts
#
# This is a POSIX shell fragment
#
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth1"

```

It's always a good practice to make a backup copy of */etc/dhcp/dhcpd.conf* file:

```
sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.bak
```



```

DHCPsrv - SecureCRT
File Edit View Options Transfer Script Tools Help
| DHCPsrv
arbab@DHCPsrv:~$ sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.bak
arbab@DHCPsrv:~$

```

Now we will change the default configuration by editing */etc/dhcp/dhcpd.conf*, I normally delete everything inside the file and manually add the configuration that suits my needs :-)

```
sudo nano /etc/dhcp/dhcpd.conf
```



```

DHCPsrv - SecureCRT
File Edit View Options Transfer Script Tools Help
| DHCPsrv
arbab@DHCPsrv:~$ sudo nano /etc/dhcp/dhcpd.conf

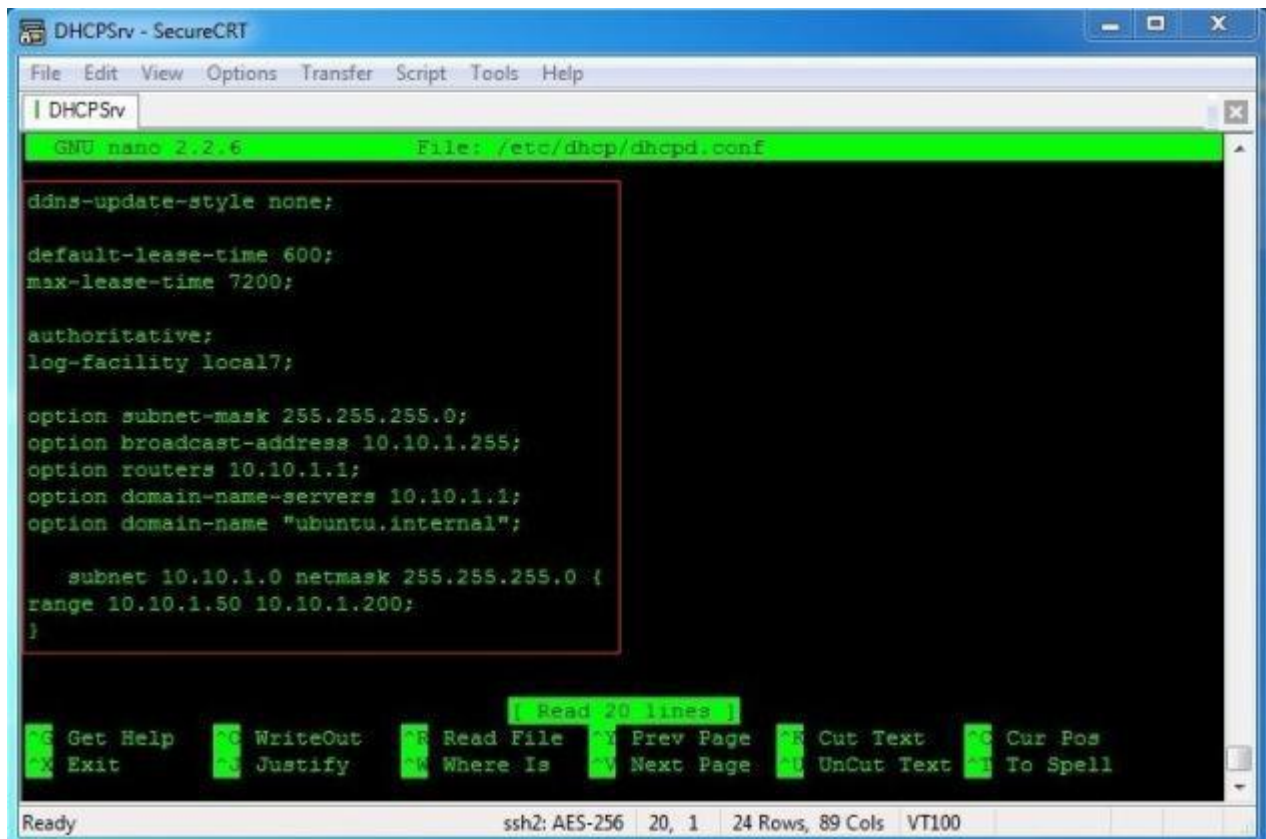
```

Here is my *dhcpd.conf* file, you need to change it according to your needs:

```

ddns-update-style none;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
option subnet-mask 255.255.255.0;
option broadcast-address 10.10.1.255;
option routers 10.10.1.1;
option domain-name-servers 10.10.1.1;
option domain-name "ubuntu.internal";
subnet 10.10.1.0 netmask 255.255.255.0 {
range 10.10.1.50 10.10.1.200;
}

```

```
GNU nano 2.2.6 File: /etc/dhcp/dhcpd.conf

ddns-update-style none;

default-lease-time 600;
max-lease-time 7200;

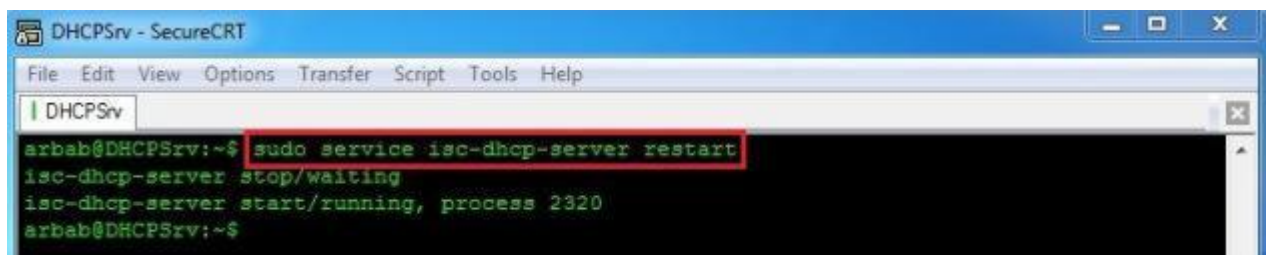
authoritative;
log-facility local7;

option subnet-mask 255.255.255.0;
option broadcast-address 10.10.1.255;
option routers 10.10.1.1;
option domain-name-servers 10.10.1.1;
option domain-name "ubuntu.internal";

    subnet 10.10.1.0 netmask 255.255.255.0 {
range 10.10.1.50 10.10.1.200;
    }
```

Restart dhcp service using the following command:

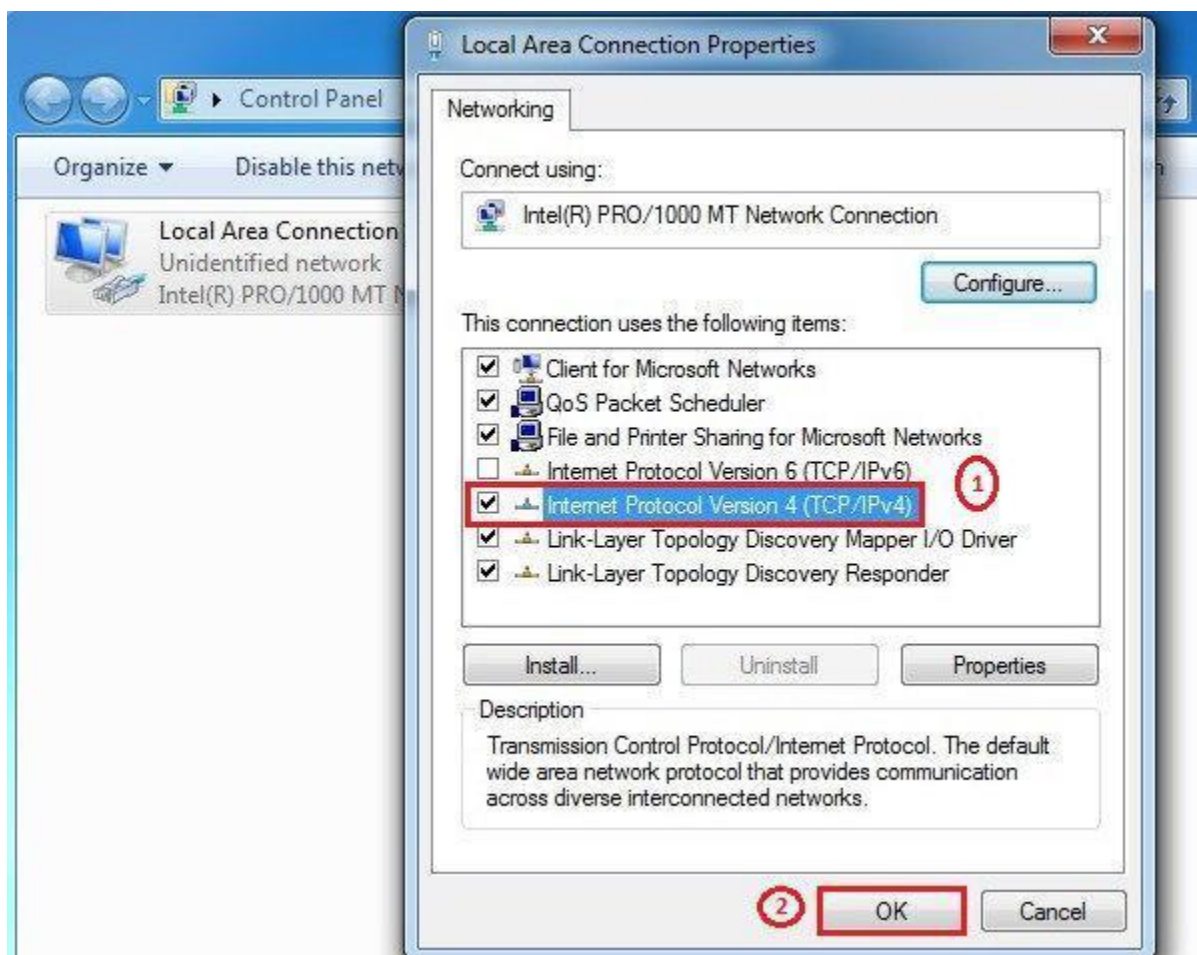
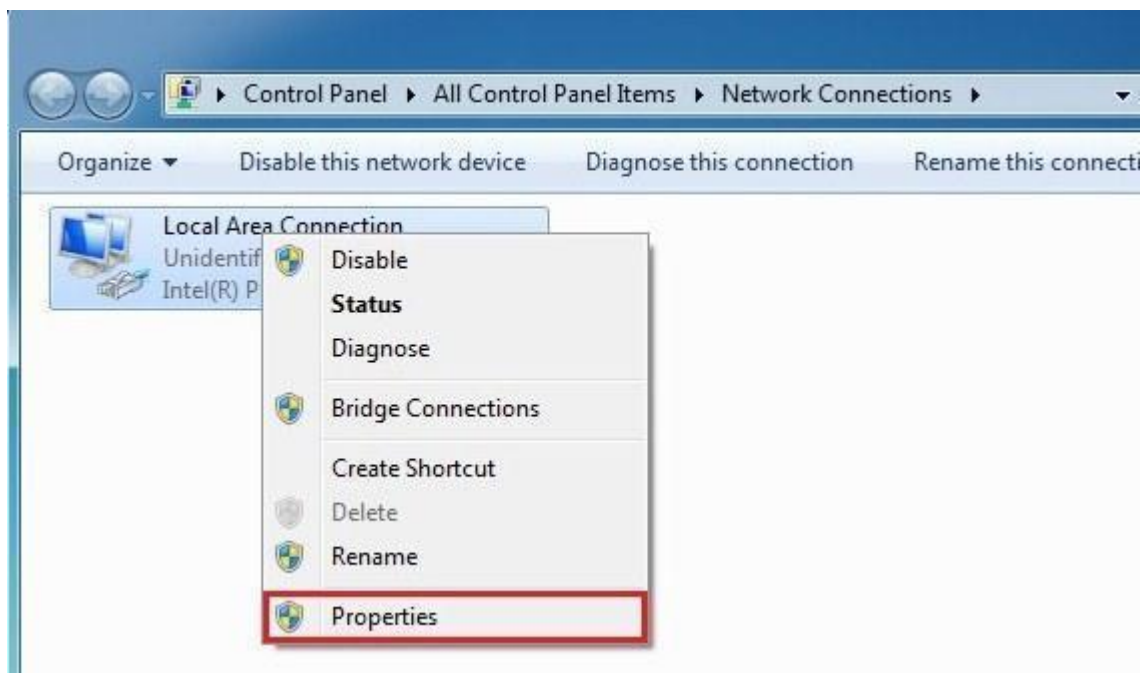
```
sudo service isc-dhcp-server restart
```

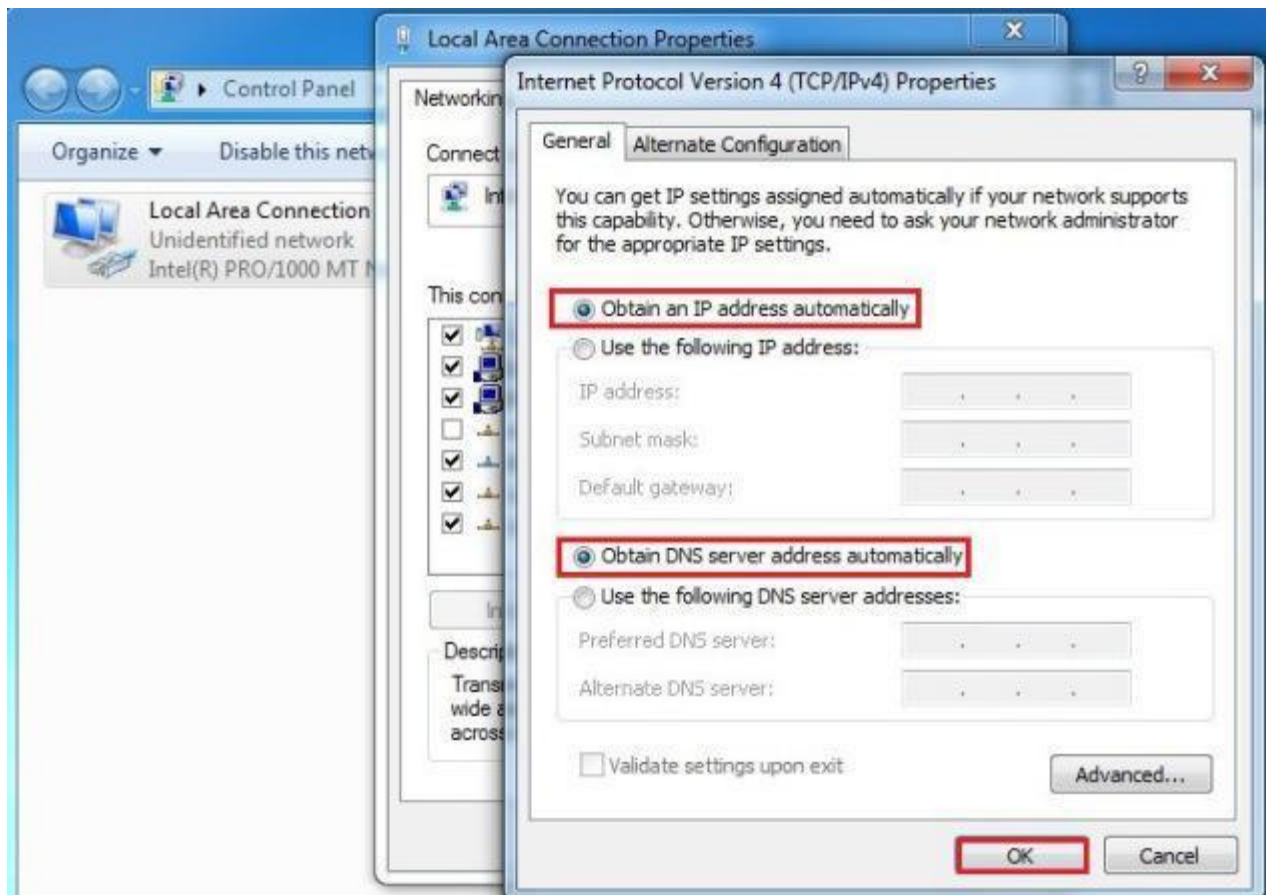


```
arbab@DHCPsrv:~$ sudo service isc-dhcp-server restart
isc-dhcp-server stop/waiting
isc-dhcp-server start/running, process 2320
arbab@DHCPsrv:~$
```

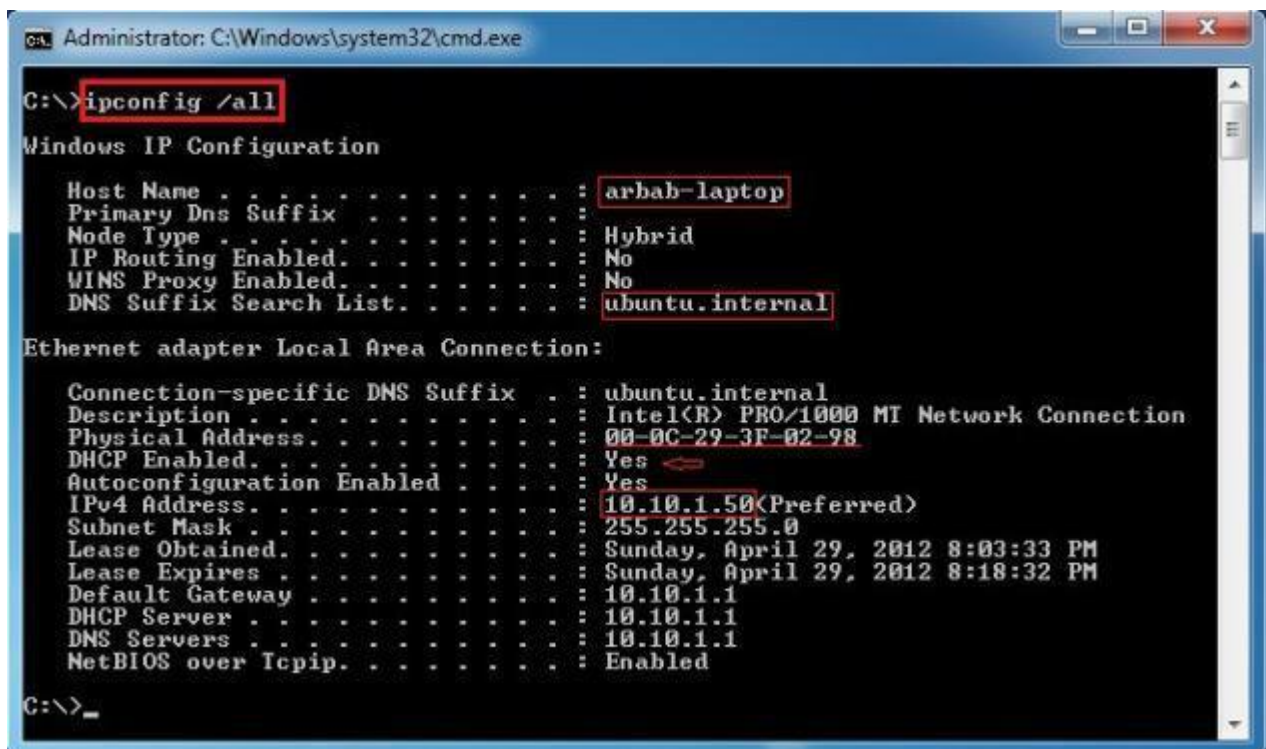
Configure Windows as DHCP Client:

Just follow these steps, in order to configure your Windows machine as DHCP client (In my case, it's Windows 7):





To check the IP Address on Windows 7:



To Check the DHCP Leases on Ubuntu Server:

`sudo tail /var/lib/dhcp/dhcpd.leases`

```

arbab@DHCPsrv:~$ sudo tail /var/lib/dhcp/dhcpd.leases
lease 10.10.1.50 {
  starts 0 2012/04/29 15:03:36;
  ends 0 2012/04/29 15:13:36;
  cltt 0 2012/04/29 15:03:36;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:3f:02:98;
  uid "\001\000\014) ?\002\230";
  client-hostname "arbab-laptop";
}
arbab@DHCPsrv:~$

```

Server Commands:

Some useful networking commands you can enter at the command prompt include the following:

Command Name	Description
net	Used to start, stop, and view many networking operations
ipconfig	Displays the IP address and other TCP/IP configuration information for your workstation
hostname	Displays the Microsoft networking computer name; available only in Windows NT, 2000, and XP
lpq	Displays the print queue status of an LPD printer; available only in Windows NT, 2000, and XP
ping	Verifies existence of remote host (connectivity)
nbtstat	NetBIOS over TCP/IP; gives statistics and technical NetBIOS information for the TCP/IP layer
netstat	Returns protocol statistics and current TCP/IP connections
ipxroute	Displays and modifies IPX routing tables
route	Manipulates TCP/IP routing information
tracert	Displays route taken by an ICMP to a remote host
finger	Displays information about the user; finger is turned off in IU's ADS Domain
arp	Displays or modifies information in the ARP (Address Resolution Protocol)

cache	
getmac	Lists the MAC (Media Access Control) Address on the computer network interfaces; available in Windows XP only

Linux Network Commands:

The network commands chapter explains various tools which can be useful when networking with other computers both within the network and across the internet, obtaining more information about other computers. This chapter also includes information on tools for network configuration, file transfer and working with remote machines.

Command Name	Description
Netstat	Displays contents of /proc/net files. It works with the LINUX Network Subsystem, it will tell you what the status of ports are i.e. Open, closed, waiting, masquerade connections. It will also display various other things. It has many different options.
Tcpdump	This is a sniffer, a program that captures packets off a network interface and interprets them for you. It understands all basic internet protocols, and can be used to save entire packets for later inspection.
Ping	The ping command (named after the sound of an active sonar system) sends echo requests to the host you specify on the command line, and lists the responses received their round trip time. You simply use ping as: ping ip_or_host_name
Hostname	Tells the user the host name of the computer they are logged into. Note: may be called <i>host</i> .
Traceroute	<i>traceroute</i> will show the route of a packet. It attempts to list the series of hosts through which your packets travel on their way to a given destination. Also have a look at <i>xtraceroute</i> (one of several graphical equivalents of this program).
Findsmb	<i>findsmb</i> is used to list info about machines that respond to SMB name queries (for example windows based machines sharing their hard disk's).
Ifconfig	This command is used to configure network interfaces, or to display their current configuration. In addition to activating and deactivating interfaces with the “up” and “down” settings, this command is necessary for setting an interface's address information if you don't have the <i>ifcfg</i> script.

Conclusion:

Thus we have performed the server administration tasks in the Network Laboratory in which we have learned how to

1. Install Telnet Server and Client
2. Install and maintain FTP Server and Client
3. Perform the installation of DHCP Server and Client and how to manage the network with DHCP and Static IP
