
Southern Polytechnic State University

Electrical and Computer Engineering Technology Department

ECET 4820 Laboratory Exercise 5: Introduction to TCP/IP

Objective:

The main objective of this laboratory exercise is to familiarize the student on how to set up the TCP/IP protocol on a PC running the Windows 7 Professional and the Ubuntu Linux operating systems. Useful tools for working with TCP/IP will also be introduced. As part of this laboratory exercise, students will operate Linux as a virtual machine within the Windows environment. The software implementing the virtual machine is Oracle VirtualBox.

The TCP/IP protocol is a set of protocols (or *suite* of protocols) used as the primary protocol of the Internet. As the Internet continues to grow, the TCP/IP protocol continues to develop and will become more and more important as a part of the Internet. It is important to understand the basics of the protocol as Internet usage is increasing rapidly.

Prelab:

Review this entire procedure to have an understanding of what you will be doing in lab. Use your textbook or the Internet to look up information on the utilities **ping** and **tracert** (or **tracert**). Your laboratory instructor may ask you questions about these utilities.

Instructions:

In step 1, you will boot the computer to Windows. Steps 2-6 provided detailed instructions for installing the TCP/IP (IPv4) protocol on a computer running Windows 7 Professional. Step 7 shows how to set up Client for Microsoft Networks to enable logging in to a Windows domain.

1. If your computer is not already running in the Windows environment, boot or reboot it and select Windows 7 at the boot loader menu.

Installing TCP/IP on a Windows 7 Computer Manually:

2. a) Once the computer has been started and logged into, open the **Control Panel**:
 - i) Click **Start**.
 - ii) Click **Control Panel**.
 - iii) Click **Network and Sharing Center**
 - iv) Click **Change Adapter Settings**.
- b) Right-click the **Local Area Connection** icon and select **Properties**.

Note: if you have more than one **Local Area Connection** icon, make sure the one you click on is the one associated with the Ethernet connection from your computer to the lab network.
- c) The TCP/IPv4 protocol may not appear. *If it does not*, perform step d), otherwise go to step 2.
- d) Add the TCP/IPv4 protocol if it is not already visible in the **Properties** box:
 - i) Click **Install**.
 - ii) Double-click **Protocol**.
 - iii) Select **Internet Protocol (TCP/IP)** from the list and then click **OK**. After a short time, you will see TCP/IP appear in the **Local Area Connection Properties** box.

3. The IP address is the identification for a computer on the Internet.
 - a) Click on TCP/IPv4 entry in the **Local Area Connection Properties** box to highlight it. Then click the **Properties** button. A properties sheet will appear for the protocol setup.
 - b) The first step is to assign the IP address to the computer. Have your instructor give you an IP address to use. It will be in the form aaa.bbb.ccc.ddd
 - c) Click **Use the following IP address** and enter this value in the **IP address** field.
 - IP Address _____.
4. The subnet mask should be set for a Class C range of addresses. Have your instructor give you a subnet mask to use and enter it into the **Subnet mask** field.
 - Subnet Mask _____.
5. The default gateway is the device that a computer communicates through, usually in order to get to the rest of the Internet. That device is typically a router.
 - a) Obtain the value to enter for the default gateway from your instructor. Enter the value under **Gateway** and click add. Record this value:
 - Gateway _____.
6. A DNS server allows a computer to resolve an address to a numeric IP number. This must be done for any connection to be made using TCP/IP. The **Host** and **Domain** are used to identify your computer to the DNS server. To establish DNS:
 - a) Select **Use the following DNS server addresses**.
 - b) Obtain the DNS server's IP address from your instructor. Enter it into the **Preferred DNS Server** field and click Add.
 - DNS Server _____.
7. If a Windows workstation is configured for local network access, it is either a member of a workgroup or a domain. Microsoft domains are managed by one or more Domain Controller computers. When a user logs in to the domain through the workstation, the resources of the domain are available to that user. If the workstation is a member of a workgroup, each workstation in the workgroup is a "peer." That is, there is no domain controller or central resource management. This procedure will cause a network login box to appear when the workstation boots up.
 - a) Return to the **Local Area Connection Properties** box. If the **Client for Microsoft Networks** already appears, go to step 8.
 - b) With none of the **Components** highlighted, click **Install**.
 - c) Click on **Client**, then **Add**.
 - d) Click on **Client for Microsoft Networks**; then click **OK**. **Do not install Client Service for NetWare**. After a short time you will be asked to restart your computer. Click **Yes** to restart.
 - e) Restart your computer if it asks you to.
8. Log off or restart your computer so you see a logon box. To see where you would specify whether your computer logs on to a workgroup or a domain, do the following. **You will not make changes to the settings**.
 - a) Right click on the **Computer** icon on the desktop and then click properties. The **System Properties** box will appear. Note: if you do not see the Computer icon on the desktop, right click on your desktop, then click **Personalize**→**Change desktop icons**, then select Computer and Network and click **OK**.

- b) Determine the name of the domain or workgroup your computer is a member of from the **View basic information about your computer** information.

Domain or Workgroup Name: _____

Configuring TCP/IP on a Ubuntu Linux Computer Manually

You will configure the TCP/IP stack on a Ubuntu Linux virtual machine running in VirtualBox. First, VirtualBox must be started and then Ubuntu will be booted from VirtualBox. Next, the TCP/IP address will be configured manually.

9. In this step, you will start VirtualBox and the Ubuntu operating system (OS).
- Double click on the **Oracle VM VirtualBox** icon. The **Oracle VM VirtualBox** window will appear. It should look similar to that of Fig. 1.
 - In the right panel, if you highlight the guest Ubuntu operating system a set of **Details** regarding its virtual machine configuration will appear.
 - Scroll down in the **Details** pane until you see the **Network** heading. The information displayed will tell you which NIC card hardware is emulated by Ubuntu. You may also see (NAT) or (Bridged ...) in parenthesis.

If you see NAT, this means that the guest operating system Ubuntu will communicate through VirtualBox to the Windows host operating system using network address translation with the VirtualBox hypervisor acting as a “router” to move network traffic back and forth to Ubuntu from Windows’ network card driver.

If you see Bridged ..., VirtualBox places a device driver on the host OS that filters traffic going to/from the guest. It effectively causes the guest to have a “virtual” network card on the host’s machine. Therefore, the guest OS operates on the same IP

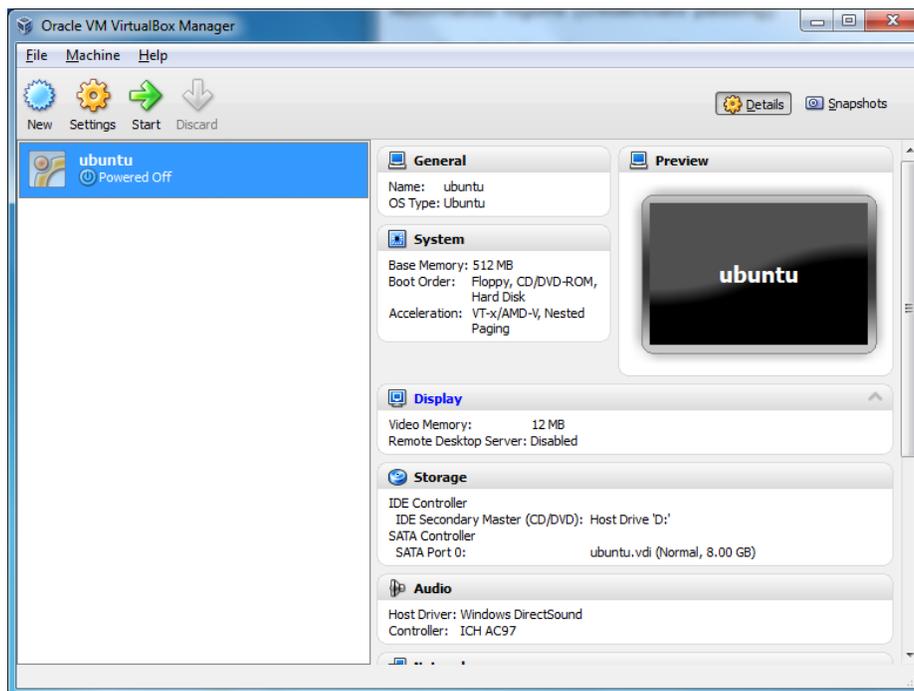


Fig. 1. VirtualBox window showing virtual machine details for Ubuntu OS.

network that the host does.

The third way to implement networking is to operate an internal network among the various guest virtual machines.

NAT is the default networking configuration for VirtualBox guest operating systems. You can change the networking configuration once the guest OS is booted. In this lab exercise, we will select Bridged networking.

- c) Boot the Ubuntu guest OS by selecting it in the left pane and clicking the **Start** arrow. Ubuntu will boot in a separate scalable window that appears similar to the one in Fig. 2.
 - i) Note the drop down menus **Machine**, **View**, **Devices**, and **Help** are associated with VirtualBox and not Ubuntu.
 - ii) Click **Devices**→**Network Adapters**. In the **Adapter 1** tab, make sure the **Attached to:** selection is **Bridged Adapter**. Under **Name**, select the adapter used by the computer to connect to the lab network. Click **OK**.
 - iii) If you made changes to the networking mode and/or adapter, you need to reboot Ubuntu.
10. In this step, you will configure the protocol stack through the Ubuntu graphical user interface (GUI).
- a) Click **System**→**Preferences**→**Network Connections**. The **Network Connections** window will appear.
 - b) Click on **Auto eth0** and then select **Edit**. Ubuntu defaults to using DHCP (the Auto method) to obtain an IP address.

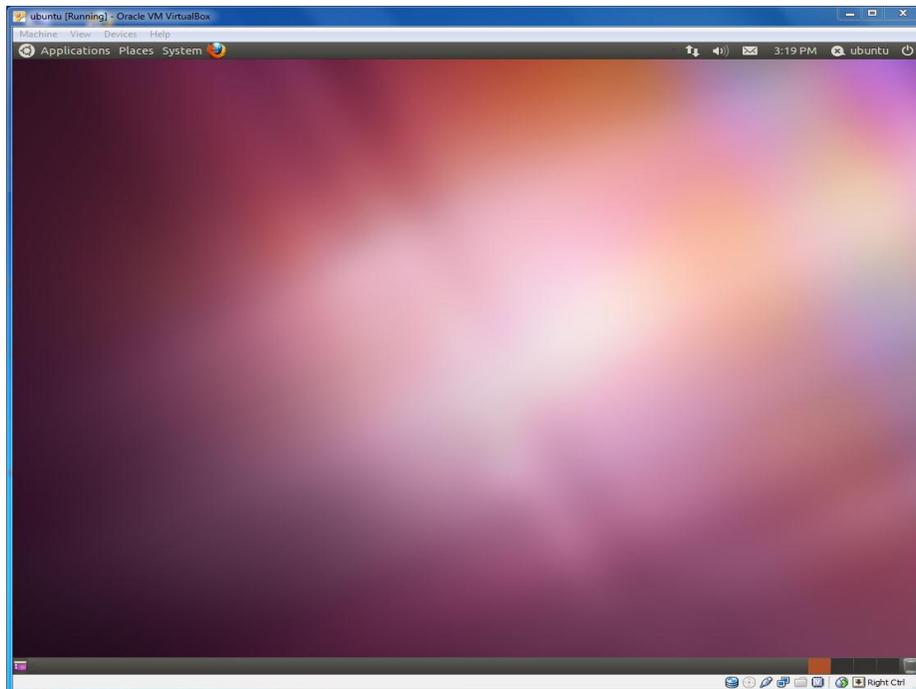


Fig. 2. VirtualBox guest OS window with Ubuntu running.

- c) Click the **IPv4 Settings** tab.
- d) Under **Method**, select **Manual**.
- e) In the **Addresses** box area select **+Add**, then select **Address**. Type in the IP address, subnet mask, and default gateway values specified by your instructor. Also record these values below.
 - IP Address _____.
 - Subnet Mask _____.
 - Gateway _____.
- f) In the **DNS Servers** box, enter the IP address(s) of the DNS server(s) specified by your instructor. Leave the **Search Domains** box empty.
- g) Reboot Ubuntu to make the changes take effect.

Testing the TCP/IP Protocol Configuration:

11. Once configuration is complete, it is advisable to always test the setup. There are several simple utilities that can be used to test TCP/IP; they are:

- Ipconfig (Windows) or Ifconfig (Linux)
 - Ping
 - Traceroute
- a) The **ipconfig** command is a Windows utility that displays the IP configuration of the computer. The utility must be run from the **Command Prompt** window.
- i) Click **Start→Programs→Accessories→Command Prompt**. Note: you can add a shortcut to the **Command Prompt** window to the desktop for convenience.
 - ii) Type **ipconfig** on the command line. What is displayed?
 - iii) Ipconfig has other capabilities. Type **ipconfig /?** to see a list of options. Use one of the command line options to find your Ethernet adapter's hardware address.
- Ethernet address: _____
- b) The **ifconfig** command is a Linux utility that is considerably more versatile than its Windows counterpart. The utility must be run from the Linux **terminal** window.
- i) Click **Applications→Accessories→Terminal**.
 - ii) Type **ifconfig** at the prompt. What general information is displayed? Is it the same information as displayed by **ipconfig** in Windows?
Determine the Ethernet address associated with your address identified as eth0.
 - iii) Type **ifconfig --help** to see what other capabilities the command has. Determine whether or not **ifconfig** can be used to assign an ip address to an interface.
- Ethernet address: _____
- Is this the same Ethernet address as found from the Windows **ipconfig** command?
- c) **Ping** is a utility used to query a computer's status. If a response is returned when **ping** is executed, the computer is at least powered-up and on the network. No response indicates the computer being pinged is turned off, is not on the network, or has problems of some type. Note that pings are blocked from leaving the campus network and only a few campus addresses can be pinged.

Try steps i) and ii) below for both Windows and Linux. Note that to stop a ping display in Linux, you must type ctrl-C. Try steps iii) and iv) for Windows only.

- i) From a command prompt, type **ping**. What is displayed (do not list the response)?
- ii) Type **ping localhost**. What information is returned? What is the **localhost**?
- iii) Ping the IP address specified by your instructor. Record the first three lines from the ping output.

- iv) Modify your line to ping the address 20 times. Write that command below.

- d) **Traceroute** is a utility to check a connection from one computer on a network to another computer on a network. It makes a trace from the initiating computer to the destination computer, showing all intermediate nodes. Both Windows and Linux have the capability of executing traceroutes with the Linux command being more versatile. Unfortunately, trace routes are blocked from leaving the SPSU campus, so the most interesting trace is implemented from a web site to demonstrate the utility's function.

Perform the following steps in Windows only.

Type **tracert** on the command line in the **Command Prompt** window. This will show the options for the utility.

Have your instructor give you an IP address or World Wide Web address to trace.

Open a web browser and go to **http://network-tools.com** and select the **Trace** option.

Type **www.telstra.net** on the input line. Record the information indicated below from your trace. Include all information on the lines for the first and last hops.

Total number of hops including first and last: _____

First Hop: _____

Domain name of domain just before last hop: _____

Last Hop: _____

Greatest time difference between hops: _____

Why is this time difference so large?

Find the contact name and phone number for the domain just before the last hop. Hint: Perform an Internet search on **whois**.

Determining Workstation Network Statistics

12. You can use the command **netstat** and its options to determine network parameters and statistics associated with your workstation. Both Windows and Linux have versions of this command. You will use the Windows version here and you will also use a free utility TCPView.
- a) Open a Command Prompt window.
 - b) Type **netstat /?**.
 - c) Determine which switch to use to find out how many IP packets were received by your workstation. How many were received? **Have your instructor verify your results.**

 - d) Use **netstat** to determine the all of the types of ICMP messages received by your computer.

 - e) Type **netstat -r**. What information is displayed? Copy the IPv4 table displayed or print it out.

 - f) Open your web browser and connect to **www.yahoo.com**. What port(s) is your computer listening on for this connection?

 - g) Close the connection to Yahoo and see what happened to your open ports.

 - h) Start the TCPView program to view the open ports. What additional information about the ports does it display that Netstat does not?

Automatic IP Address Assignment

13. Most networks implement Dynamic Host Configuration Protocol to assign IP addresses to hosts. When a computer boots, the DHCP client broadcasts a request for a DHCP server to send it an IP address, DNS server address, etc.
- a) Open the **Network Connections** box and the **Local Area Connection Properties** box as before.
 - b) Double left-click on the **Internet Protocol** entry to open its **Properties** box. Select **Obtain an IP Address Automatically** and **Obtain DNS Server Address Automatically**.
 - c) Click on **OK** until the **Local Area Connection Properties** box is closed.
 - d) Your configuration will be verified using **Net Shell** commands below.

Using the Network Services Shell

14. The network services shell (Netsh) is activated from the command prompt and allows you to perform a considerable number of diagnostic queries. The reference at the end of the lab instructions describes the commands you can use in the Netsh.
 - a) First, open the **Administrative Tools** window in the **Control Panel**.
 - b) Select **Services** and ensure that the **Routing and Remote Access** service is in **Manual** mode and is **Started**.
 - c) Open a **Command Prompt** window and type **Netsh** at the prompt. The **netsh>** prompt will appear.
 - d) Type **help** to show a list of commands to get an idea of what you can do in the Netsh mode.
 - e) Type **interface ipv4 show ipaddress** at the prompt to display the IP address assigned by DHCP.
 - Was the IP address the same as the one you entered manually?
 - f) Type **interface ipv4 show interface** at the prompt to display interface information.
 - i) Determine the maximum transmission unit for your Ethernet connection
 - ii) Determine the speed of your interface.

Questions:

1. What is a hypervisor?
2. What is the purpose of Client for Microsoft Networks?
3. Why is DHCP a good choice for assigning IP addresses on large networks?
4. Briefly explain what the DNS server's purpose is. That is, elaborate on what it is doing when given an address to lookup (such as www.spsu.edu).
5. Interpret the ping output you obtained.
6. From the IPv4 routing table printed after typing the netstat -r command, interpret each of the Network Addresses except for the 0.0.0.0 address. Note that the Network Address column contains a list of addresses that your computer might try to reach.
7. How might the information displayed by the netstat -r command be used to troubleshoot TCP/IP network problems?
8. Why is it useful to have a tool showing you which ports TCP/IP has open on your computer?
9. The Linux ifconfig command does not display the configured default gateway like the Windows ipconfig command does. Perform some research and determine a Linux command that will display the default gateway.

Report:

Discuss the results obtained in the lab exercise. Answer the questions. Make conclusions regarding your results.

Reference:

W. Stanek, Microsoft Windows Command-Line Administrator's Pocket Consultant, Redmond, WA, Microsoft Press, 2004.

Southern Polytechnic State University

Electrical and Computer Engineering Technology Department

ECET 4820 Laboratory Exercise: Introduction to TCP/IP Instructor Guide

Instructor's Guide

1. The Sept 2012 update changed the instructions to support Windows 7.
1. A major change in the Sept 2010 update was instruction on the protocol stack configuration of Linux Ubuntu which runs as a virtual machine in VirtualBox. This helps students become more familiar with and less intimidated by Linux.
2. The Linux guest OS network interface is set up as Bridged in the lab so that it appears to have a separate NIC on the network. You must assign it a different IP address than the Windows NIC has. Thus each computer in lab will have 2 IP addresses. Be careful that you do not inadvertently assign the same IP address to more than one machine.
3. In Windows 7, to change the TCP/IP stack, *the student must have administrator privileges on the local computer*. Having administrative privileges on the domain is useless since you have no network configuration. You must do this ahead of time.
4. To remove the TCP/IP stack configuration, uninstall TCP/IP and Client for Microsoft network.
5. Connect a projector to a computer's monitor so you can show them what the netstat -r display looks like and explain the routing table.
6. Make sure the student is supplied with the following information:
 - IP Address (should be on each machine)
 - Gateway
 - Subnet mask
 - DNS server IP address
 - WINS server IP address
7. Any lecture before lab begins should be an overview of TCP/IP, perhaps a quick review of what was discussed about it in class so far. Emphasis should be on:
 - It's purpose
 - Where it's used
 - The main parts of it
 - The purpose of the two tools (ping and traceroute)
8. Students should check their connectivity to the link leading to the campus network.
9. You might wish to cover DNS servers, gateways, and subnet masks in detail; they are a bit difficult to comprehend.
10. When they are pinging a server, have them ping the campus DNS server.
11. To run DHCP, you can either use the campus DHCP server or set up a server in the lab. The small lab Linksys router can do this function. **Make sure that if a lab DHCP server is used that there is no connection to the campus network except through a router. It is important that the lab DNS server not interact with clients on the campus network.**

Answers to Questions

1. A hypervisor is a virtual machine manager that controls access of the virtual machine to the host OS hardware.
2. Client for MS Networks is the software allowing Windows to communicate with other Windows computers on a workgroup or domain.
3. DHCP allows easy IP address management.
4. Understanding the translation of an address such as *www.spsu.edu* to a numeric IP address is important. The student should state this fact and prove their knowledge that a machine is not assigned a name address, but a numeric address.
5. The successful ping output gives the response time from the ping attempt and the TTL setting it used when it started.
6. The routing table has a number of entries. They should say that 0.0.0.0 is the network associated with the default gateway; 127.0.0.0 is the computer's internal TCP/IP network with gateway 127.0.0.1. When they ping 127.0.0.1, they are testing their computer's TCP/IP stack. They should see their computer as gateway address on network 168.28.186.0. Their computer's external network 168.28.186.0 is reached through their own NIC card as the gateway address. Address 224.0.0.0 is a multicast address. In essence, they need to see the relationship between the address they are trying to reach Network Address and the one used to get there Gateway Address. Packets going to any address not specifically listed in the table are going to be sent to the Default Gateway.
7. Netstat -r shows the routing table. If the default gateway is unreachable or does not appear in the table, the workstation cannot reach the outside network.
8. Open ports are an opening for hackers.
9. The route command will do it; so will netstat -r.