# AC 2007-944: VISUAL ROUTE AND VIRTUAL NETWORK COMPUTING EXERCISES FOR COMPUTER NETWORK COURSES

**Veeramuthu Rajaravivarma, Central Connecticut State University**

Dr. V. Rajaravivarma is currently with the Computer Electronics and Graphics Technology department at Central Connecticut State University, New Britain, CT. He is a Professor and Program Coordinator of Computer Engineer Technology. He is Vice-Chair and past Treasurer of the IEEE-Connecticut Section. Previously, he was with Tennessee State University, Morehead State University, and North Carolina A&T State University. Dr. Rajaravivarma received a B.E. in Electronics & Communication Engineering from University of Madras,India, earned an Electrical Engineering M.A.Sc. from University of Windsor,Canada, and completed a Ph.D. in Electrical Engineering from Tennessee Technological University. E-mail: RajaravivarmaV@ccsu.edu

**G. Thomas Bellarmine, Florida A&M-Florida State University**

Dr. G. Thomas Bellarmine is currently working at Florida A&M University as Associate Professor teaching Electronic and Computer Engineering Technology courses. He obtained his BSEE degree from Madras University and MSEE degree from Madurai Kamaraj University. He did his PHD in Elecrical Engineering at Mississippi State University and M.S. in Computer Science from The University of West Florida. He is currently an IEEE Senior Member and a Member in ASEE. He is also a Registered Professional Engineer. Email: Thomas.bellarmine@famu.edu

# Visual Route and Virtual Network Computing Exercises for Computer Network Courses


## Abstract

Knowledge of networking concepts (network usage) has become crucial in today's world where all of us use different types of networks in our day-to-day life. But in a field like networking, real understanding can be achieved only by hands-on exercises. In this article, six lab exercises on Visual Route and Virtual Network Computing software suites are discussed, and how they could be further enhanced by teaming them with firewall hardware/packet sniffers, or with firewall software such as Zone Alarm. This work can be expanded with discussions of other networking concepts and technologies that will enhance one's networking experience.


## Introduction

Visual Route is an easy to use graphical user interface that integrates various tools such as traceroute, ping, and whois (the most common commands taught in a networking course) to check Internet connectivity, and displays the actual route of connections and IP address locations on a global map (Exercise 2, Exercise 3). Visual Route presents a general analysis of the specific traceroute in terms of the following:

- The total number of hops encountered
- The average response time of each hop
- The time it takes for a DNS lookup
- The TTL value of packets received
- The exact place where a problem occurred
- The type of Web Server running at the destination site
- The general idea of throughput achieved
- A graphical representation of the entire path taken to reach the destination server
- A route table which displays detailed information about each hop such as the node names, their location, and the major network backbone in use at these nodes.

Clicking on any node names gives the whois information associated with that node which provides an instant contact for reporting a problem. It also has the ability to track emails. Incorporating a firewall will help to solve the security issue and make Visual Route better. Because of the packet filtering provided by firewalls, it is possible for the user to allow or deny transferring data from a specific IP address. A packet sniffer or a network analyzer could be integrated with Visual Route to enhance its functionality. This analyzer would read and capture the packets that pass through a network segment (Exercise 4). By using information from the captured packets, a packet sniffer can identify erroneous packets, and can use the data to determine the bottlenecks in the network and show the overall network performance.

Virtual Network Computing (VNC) is a remote control software that allows you to view, access, and run files on one computer (the "server") using a small and simple program (the "viewer") on another machine, anywhere on the Internet. It can be used for collaboration and sharing in schools, universities and enterprises, for providing computer support to the remotely located family member, for remote system administration, IT support, and helpdesks, and for telecommuting. It does not store any state for the VNC viewer. If a user's connection to the server is broken, then all the user needs to do is to reconnect to the server and continue the work. Reconnecting will not cause any loss of data. Also, the user may reconnect from any other machine, as well, and the cursor will still be in the same place for the user to continue. VNC uses a protocol that is simple, open, and platform-dependent. The sixth lab exercise discusses how VNC works, and shows how to run a VNC server and/or viewer.

VNC, however, is not a very secure protocol. Zone Alarm firewall software prevents any unauthorized inbound or outbound access, and keeps the user's virtual network connection safe and secure. Zone Alarm firewall is an award-winning firewall that has an easy-to-use interface, uses superior technology, and a free download available for the individual user. This is discussed in seventh lab. VNC is freely and publicly available and is in widespread active use by millions throughout industry, academia and privately [1]. VNC is a desktop sharing system that uses the Remote Frame Buffer (RFB) protocol to take complete control of a remote computer. The keyboard presses and mouse clicks are transmitted from one computer (the viewer) to the other (the server) over a network.

The set of laboratory exercises *on* Visual Route and Virtual Network Computing (VNC) software suites discussed in this article are:

1. Study the basic commands of networking
2. Implement traceroute for specific website name using Visual Route.
3. Implement ping for specific IP address using Visual Route
4. Study the basics of packet sniffing.
5. Create a remote-sharing environment for group projects using VNC.
6. Learn the basics of firewall software, such as Zone Alarm.

The minimum hardware requirements for Visual Route are Windows (all versions), a 1.x GHz processor, 128 MB RAMS, and 10 MB free disk space. A 2.x GHz processor, 512 MB RAM, and 100 Mb free disk space is recommended. For a full installation of both VNC's server and viewer, the requirement is 1.6 MB of disk space, but compact or custom installation will need lesser disk space. The Windows viewer, for example, is only about 150K in size and can even be run from a floppy. The Java viewer is less than 100K. Both software packages also support MAC OS, Linux, and UNIX. Visual Route is a Java based application, and requires a Java VM (Virtual Machine) [2].

**Visual Route Applications**

Visual Route is a GUI application with the following features (a snapshot of the software is provided in "Exercise 2" below):

- **Graphical User Interface:** Visual Route has a graphical user interface which makes it easier and more convenient to use.
- **Tabbed Interface:** Simultaneous traces to different sites can be performed through the tabbed interface. Each trace is performed in a different tab. Clicking on the particular tab opens the route related to that tab. From the File Menu, one may also select to open new tab or close a current tab.
- **Whois Information:** By a single click on the Node Name and the Network columns, the whois information related to that host is displayed.
- **Database Updater:** There is an option named "Database Updater" in the Tools Menu of Visual Route. This enables a user to add a node name convention, IP address (for adding a single host or a range of hosts with similar IP addresses) or for setting a default home location (to specify that all traces begin from the same geographic location).
- **Email Tracker:** By entering an email address in the address field, one can trace the location of a specific mail server [3].

As mentioned earlier, Visual Route displays a graphical representation (over a global map) of the entire path taken to reach the destination server. The following features are available for the global map.

- **Multiple Maps:** There are three different maps available with Visual Route. One may also choose to add or download a new map or to add map points to a custom map.
- **IP's Geographical Location:** Visual Route is able to identify the geographical location in terms of city/country or state of the destination IP address.

The **traceroute function** of Visual Route has the following **features:**

- **Traceroute History:** Visual Route maintains and provides a database to recall the previous traceroute and its performance.
- **Compare traceroutes:** The File Menu in Visual Route has an option called "Compare Traceroutes". This is used to compare the results of the specified traceroutes for performance and network problems by opening them side by side.
- **Continuous Traceroutes:** The Options Menu in Visual Route has an option called "Continuous Trace Preferences" which allows the user to update the trace continuously or to refresh the trace after every specified number of minutes.
- **Traceroute Table:** This table lists all the routers (hops) between the source and destination and also gives the performance at the specific router.

Visual Route provides the following **types of analysis:**

- **Performance Analysis:** In the general analysis section of the result of trace, there is a performance analysis which helps in identifying poor connections and provides analysis for them.
- **DNS Analysis:** It measures the performance (time taken) of the Internet domain name lookup.
- **TTL Analysis**: It gives the TTL (Time to Live) for the packets received from the destination host. Hence, it measures network time to live.
- **Connection Analysis:** It identifies poor performance routers on the network if there are any.

- **Latency Measurement:** The round trip time from all hosts to destination is calculated by adding each one of them and displayed. This is a measurement of latency.
- **Packet Loss Measurement:** This feature measures the network quality for all the packets that are dropped (if any).

The following **features** are available for the **"ping" command:**

- **Ping Grapher:** This feature plots the live performance of a connection over time on a graph with history.
- **Ping Grapher History:** It maintains provides a database to recall the previous ping grapher data.

Finally, the **Visual Route Server** has the following **capabilities/functionalities:**

- **Browser Integration:** By accessing the Visual Route server with a web browser, remote users throughout the world can view connection results from the server back to themselves or from the server to any Internet address. A toolbar button is now provided for Firefox and Internet Explorer [4].
- **Server Side Ping Grapher:** The ping grapher facility is also supported in the web browser.
- **Reverse Tracing:** Reverse Tracing allows a remote user to connect to the Visual Route's support workstation. After connecting, the Visual Route support technician can trace any connection path directly from the user's desktop. So, with the help of this capability, the support technician can instantly see the analysis of the connectivity from the client location to the application with which the client has the problem and pinpoint the connectivity issue.
- **Deploy Anonymous Remote Agents:** Agents are light weight programs that can be installed on remote computers, which may be connected to the Visual Route server. This feature of Visual Route supports multiple and simultaneous reverse traceroutes between the clients and the server [5].

**Applications of Visual Network Computing**

- **Sharing.** VNC allows a person working at one location to completely control another computer located anywhere, across a network, as if he/she were sitting in front of the other computer.
- **Troubleshooting.** VNC allows users to help troubleshoot the computer of a less-technically-savvy family member or friend, who lives across the globe. In other words, sitting at your desk in Baltimore, you could use VNC to take control of your mother's PC in London and show her how to install and use some new software package by actually doing it yourself [6].
- **Hot desking and telecommuting.** VNC allows employees to access their office desktop and servers from any other machine in the company, or from other branch offices, or from home, without having to worry about the type of computers or architectures used.
- **IT support/ System administration.** VNC allows system administrators and IT support technicians to take complete control of employees' machines to identify,

and fix problems. This way, administrators can support employees working in other buildings, offices, or from home.

- **Collaboration.** VNC is an invaluable tool for creating a collaborative environment for educational or business purposes. For instance, students can view and respond to instructors' mouse-clicks; instructors can help students debug programs et al.

Research on VNC helped put together its most important features. Information that differentiates from other remote sharing systems was gathered from the following web pages:

http://www.realvnc.com/why.html
http://www.csd.uwo.ca/staff/magi/doc/vnc/

- **It is fully platform-independent.** A desktop running on a Linux machine may be displayed on a Windows PC, on a Solaris machine, or on any number of other architectures.
- **No state is stored at the viewer.** This means you can leave your desk, go to another machine, whether next door or several hundred miles away, reconnect to your desktop from there and finish the sentence you were typing. Even the cursor will be in the same place. If your PC crashes or is restarted, all the remote applications will not die, they go on running.
- **It is small and simple.** The Windows viewer, for example, is about 150K in size and can be run directly from a floppy. There is no installation needed. *The entire Java viewer is substantially less than 100K and takes less time to download than the images on some web pages.*
- **It is sharable.** One desktop can be displayed and used by several viewers at once, allowing CSCW-style applications.
- **It is free!** You can download it, use it, and redistribute it under the terms of the GNU Public License. Also, the original VNC source code is open source under the same license.

## Laboratory Exercises

To better understand Visual Route and VNC, the following six lab exercises are recommended:

***Exercise 1: Study the basic commands of networking***

These basic networking commands are very handy in troubleshooting problems such as connectivity issues.

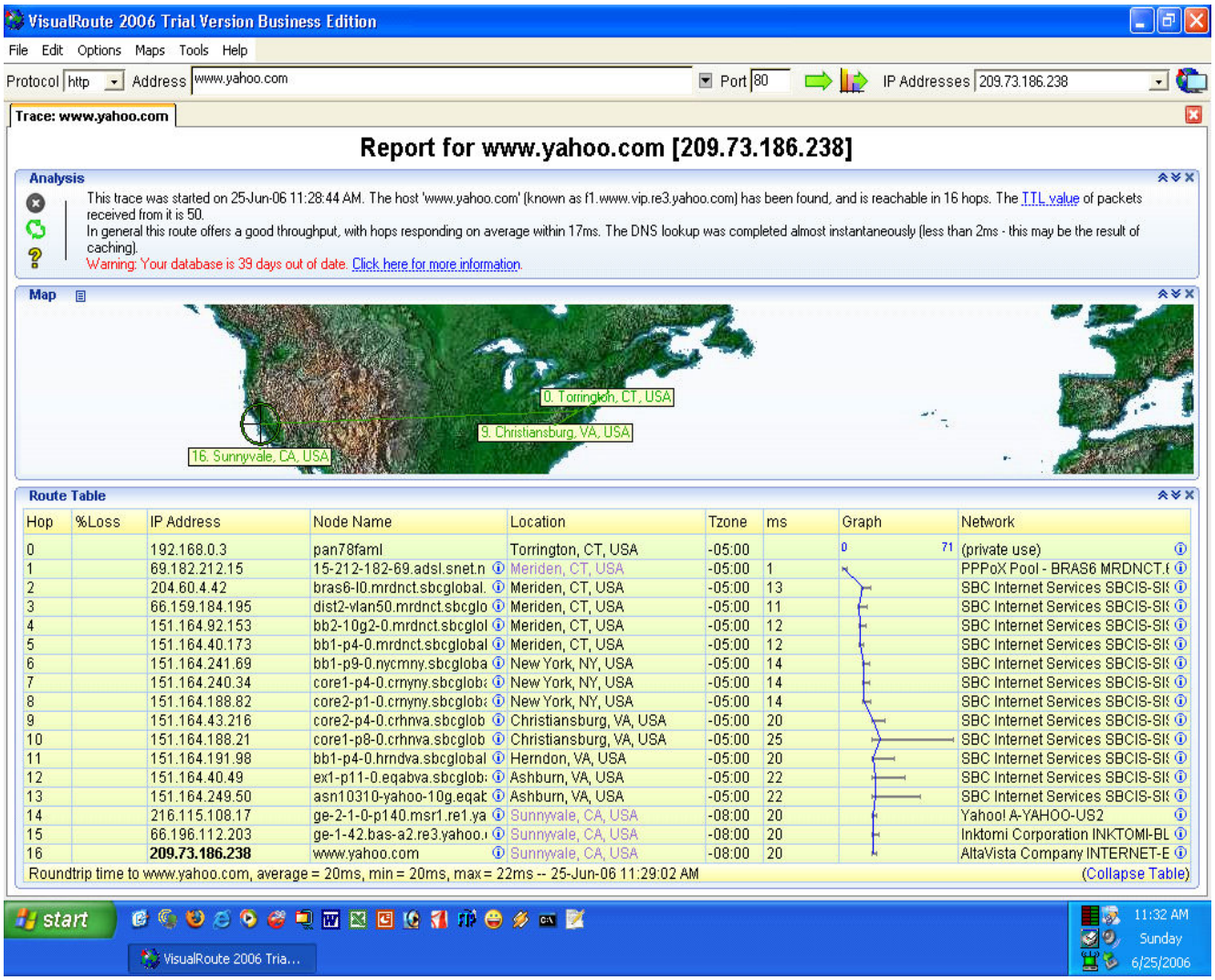
- Traceroute: This is a computer network tool that shows the actual route taken by packets across an IP network [3]. To perform a traceroute, user can simply type "tracert <server>" at a DOS prompt where "<server>" is an IP address or a domain name of the server to which the network route needs to be traced. A successful traceroute will list all hops (IP address and hostname) taken by a packet from the source to the destination server. Traceroute determines the path taken to the destination server by sending packets with different Time to Live

(TTL) values to it (the TTL is used as a hop counter). Each router along the path decrements the TTL value in an IP packet by at least 1 before forwarding it. When the TTL becomes 0, the router returns an "ICMP Time Exceeded" message to the source. The maximum number of hops is 30 by default. Traceroute continues until the destination or the maximum number of hops is reached [7].

- Ping: This is a computer network tool that is used to test whether a specific node is alive or not. It sends ICMP "echo request" to the destination host and then waits for ICMP "echo response" replies. It displays the ping statistics which includes the average round trip time in ms. and the number of packets lost and received [8]. To ping a server, simply type "ping <server>" at a DOS prompt where "<server>" is an IP address or a domain name of the server to be pinged.
- Whois: This is TCP based query response protocol that queries a database to determine the owner of a given domain name, an IP address, or an autonomous system on the Internet. It also provides contact information for that particular IP address or domain name [9]. There are various free "whois" utilities available for the Windows platform.

***Exercise 2: Implement traceroute for specific website name using Visual Route***

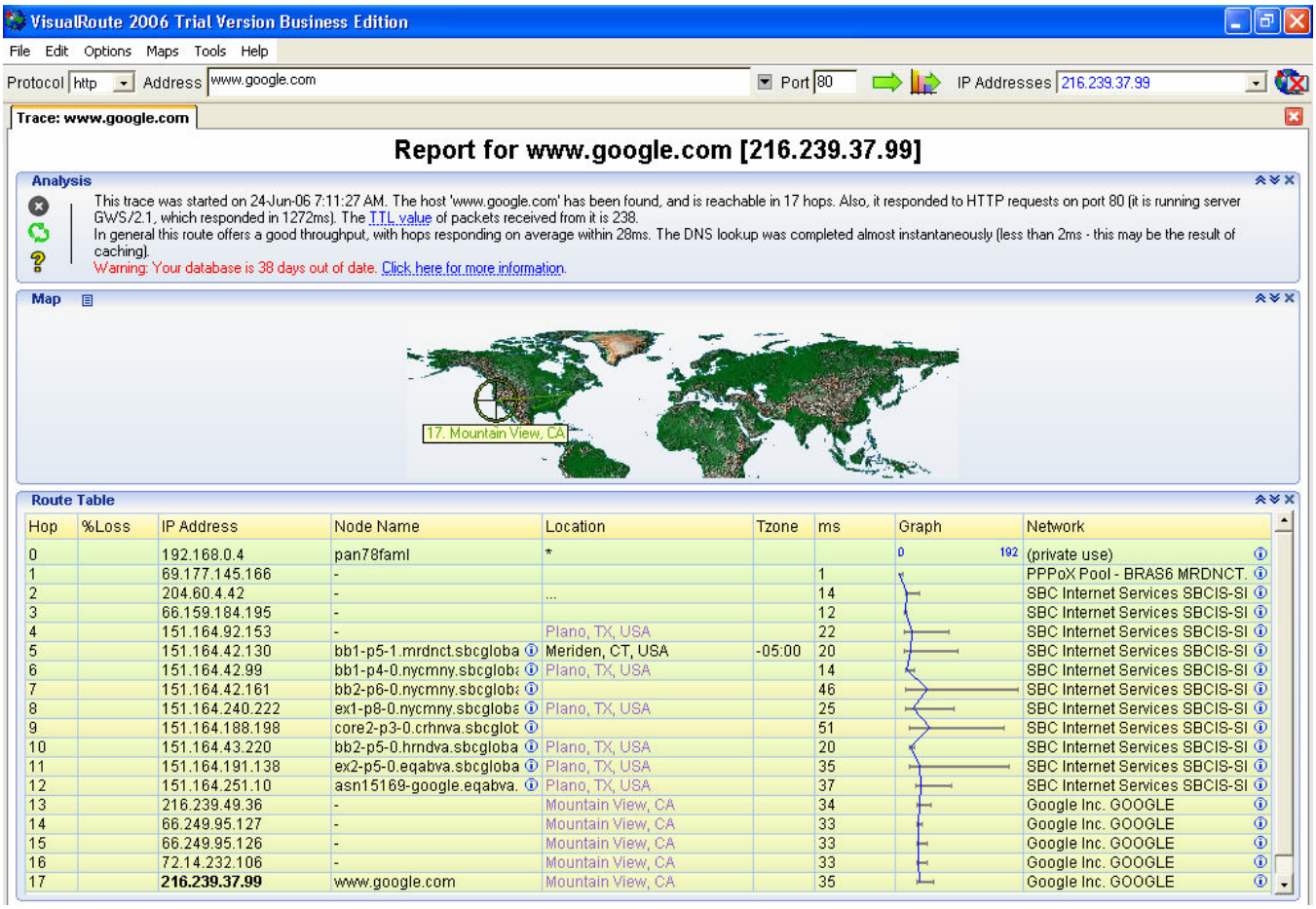
For this exercise, we will perform a traceroute to www.yahoo.com using Visual Route. Consider the following snapshot of the Visual Route software suite.




Note that the Protocol is "http" and that Address is www.yahoo.com with Port 80 (default for HTTP). The "Analysis" section shows the number of hops taken to reach the destination, the TTL value of the packets received, and the throughput analysis. The "Map" section charts the path from source to destination on a global map. Finally, the "Route Table" section shows the details of the traceroute with the following information: Hop Number, % Loss, IP Address, Node Name, Location (of the node at this hop), Tzone (Time Zone), Response time of this hop in millisecond, Graph (graphical representation of the response time), and Network (the name of the network on which the host lies).

***Exercise 3: Implement ping for specific IP address using Visual Route***

In this exercise, we perform a ping using an IP address of www.google.com 216.239.37.99 instead of a website name.

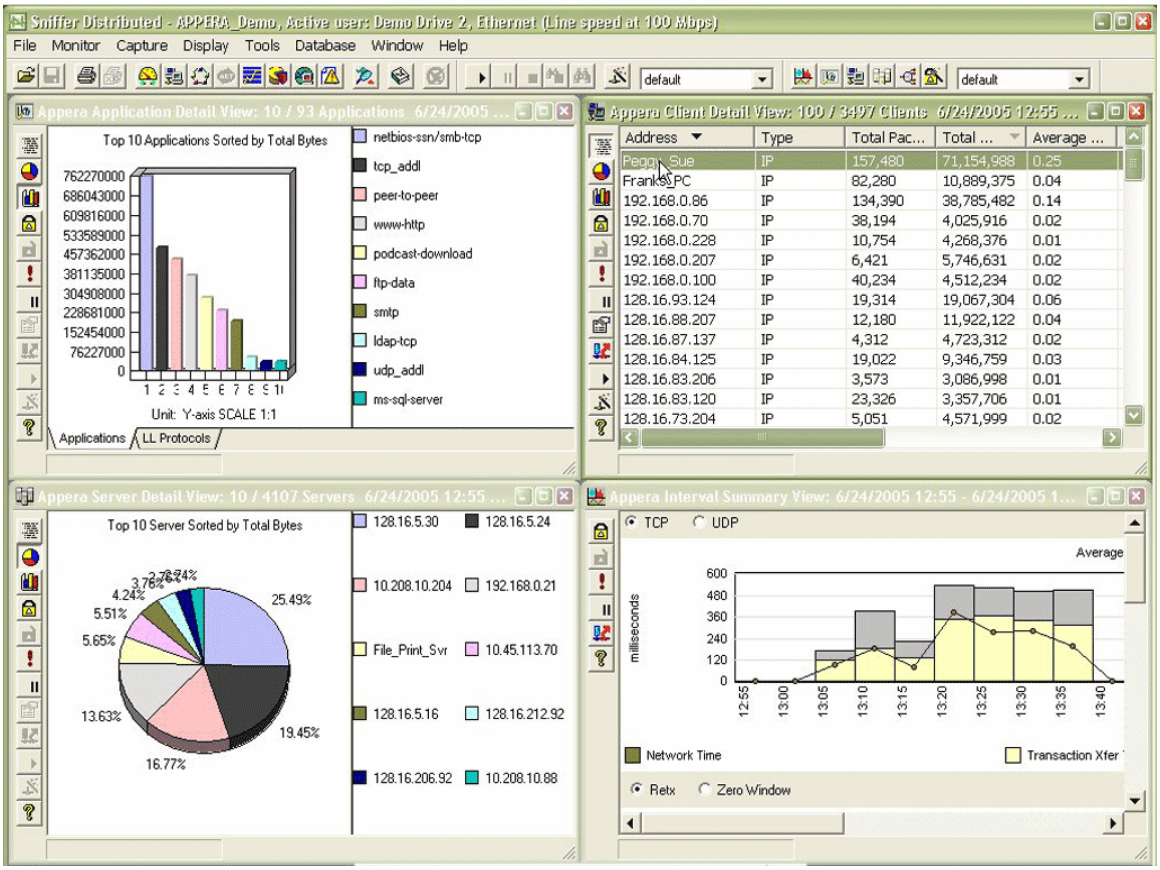



The results of the ping command for a specific IP address (as shown in the above Figure) is also similar to the Traceroute command. It displays three sections Analysis, Map and Route Table. In the first section, the number of hops taken to reach the destination IP address, the TTL value of the packets received, and the overall throughput analysis are displayed. In the second "Map" section, the entire route from the source to destination is displayed on a global map. Finally, the third "Route Table" section displays the route specifics like Hop Number, % Loss, IP Address, Node Name, Location (of the node at this hop), Tzone (Time Zone), Response time of this hop in millisecond, Graph (graphical representation of the response time), and Network (the name of the network on which the host lies).

### *Exercise 4: Study the basics of packet sniffing*

The packet sniffer/protocol analyzer software is capable of passively reading and capturing all data that is transmitted over a network segment [10]. As data passes through the seven layers of the OSI Reference Model, packets of data are encapsulated with header and trailer control information used by the various network devices in-route to the packet's final destination [11]. It's the job of the packet sniffer to capture and decode these bits of information and present them in a readable form. Hence, it helps to locate security lapses or simple troubleshooting of a misbehaving network.

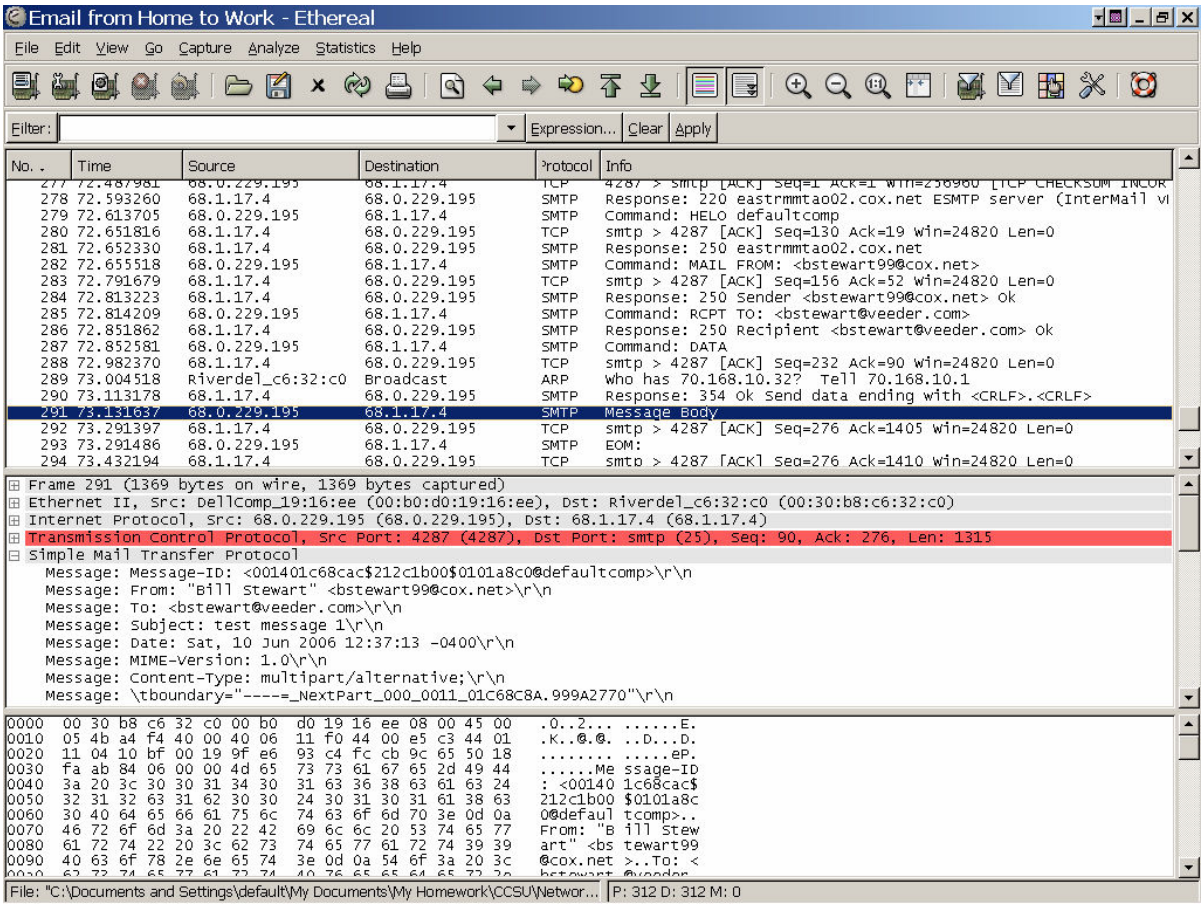
Several types of analyzers are available on the market. One such analyzer such as Network General's Sniffer application will break down network performance into graphs and charts that can pinpoint problem areas at a glance [see the figure below].




**Network General's Sniffer**

***Ethereal***

Yet another tool that can be used for packet sniffing is Ethereal, which would perform packet capture and decode for network troubleshooting and network analysis. Ethereal, is free open-source software that can be downloaded from the Internet and installed on a PC in minutes. There are hundreds of protocols involved in data transmission and Ethereal is capable of decoding nearly 800 of them, including the most popular such as FTP, HTTP, SMTP, and TCP. The three frame graphical layout of the main Ethereal window shows the captured packets in the top frame followed by a detailed frame that breaks the packet into its OSI layers. For example, an email transmission will display a link-layer (identified as Ethernet II), an Internet Protocol, a Transmission Control Protocol record, and finally the SMTP application data. Each layer can be "drilled down" to show the details of the protocol [figure shown below]. The third frame on the screen, known as the "byte detail", translates the protocol data into both hexadecimal and ASCII format.




Hence, packet sniffers would allow troubleshooting and analysis of a particular network. It would therefore allow the user to see all traffic passing in the network. Hence, if a packet sniffer is integrated with the Visual Route, the captured data packets from the packet sniffer could be checked to see if they were erroneous. Also, the overall network performance and the bottlenecks in the network can be detected [12].

***Exercise 5: Create a remote-sharing environment for group projects using VNC***

In this exercise, we create a remote-sharing environment that can be used for group projects using a Windows VNC server and viewer. If you need to understand how VNC works, please refer to Appendix A.

***Running a Windows VNC server***

1. Download and install the VNC server for Windows by running the Setup program. This will add the VNC services to your Startup Menu.
2. Start the VNC service or run the VNC server depending on the edition downloaded. The first time one will be prompted to enter a password, as shown in Figure 1. This is the password through which the intended user would be authenticated to connect to the server from a remote location. Click OK and the VNC server should start running. A small icon of VNC on your system tray, as shown in Figure 2. Right-clicking on that icon will control most aspects of the VNC server, as shown in Figure 3.

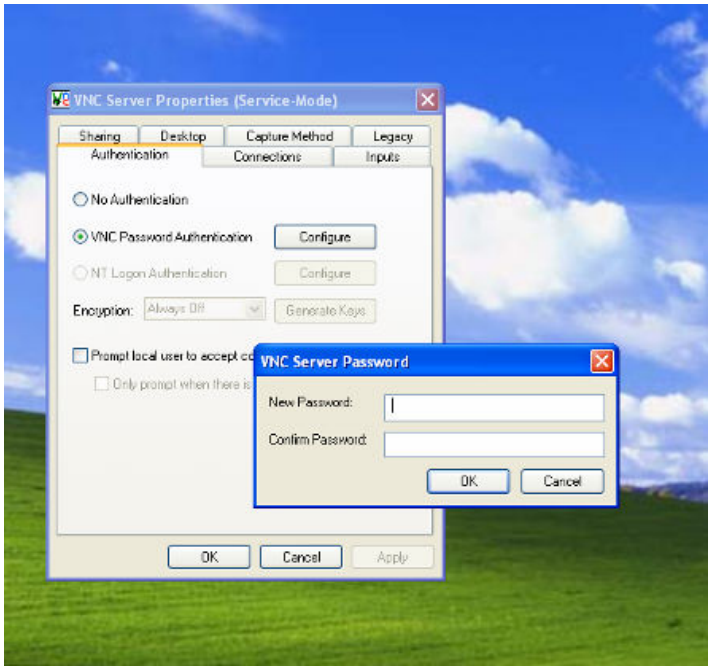



Figure 1. Setting up a password for VNC Server.


Figure 2. VNC icon on system tray.

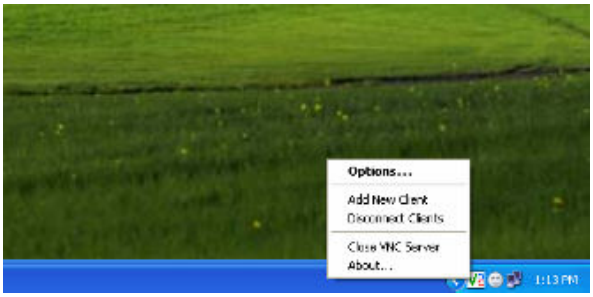



Figure 3. Right-clicking on VNC icon.

3. The VNC server is installed.
4. By placing mouse on the VNC Icon an IP address can be noted. This would be needed for the viewer to connect to the server.

***Running a VNC viewer***

1. Download and install the VNC viewer by running the Setup program. This will add the VNC viewer services to your Start Menu.
2. Select the "Run VNC Viewer" option from Start Menu.
3. You would be prompted to specify the details of the server you are trying to connect to. A window, as shown in Figure 4, will be displayed. You may enter the IP address of the server (that was noted down when running VNC server) and click OK, or use the host name and display number. The second option will work if there is a DNS service available on the network.


Figure 4. Connection details of a VNC Viewer.

4. VNC Viewer options can be set by clicking on the options button. Figure 5 shows the default settings of a VNC viewer. One can change these based on the level of interactivity and security.
5. When prompted, enter the password to be authenticated to connect to the VNC server, as shown in Figure 6. Enter the VNC server's password and click OK. Now, the display window of server machine is shown in Figure 7.
6. Now, once connected, the server machine can be accessed. All mouse clicks and keyboard presses on this window will be reflected on the server machine. You are now free to interact with your server machine.

VNC servers and viewers for other operating systems may be installed and run in a similar fashion.

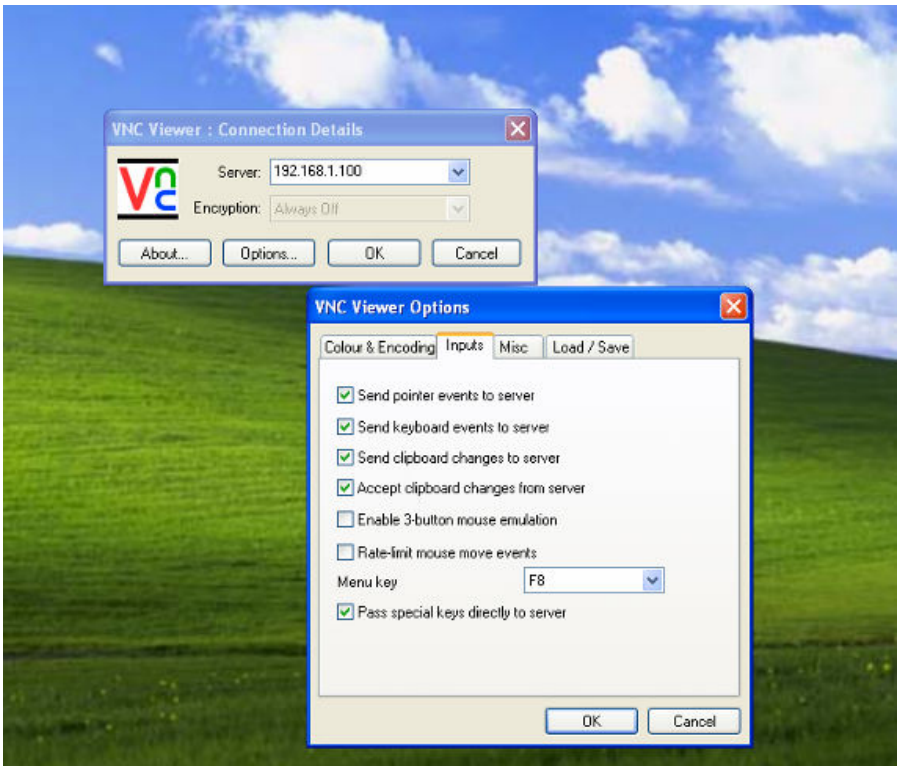



Figure 5. VNC Viewer: Options.


Figure 6. VNC Viewer: Password Authentication.

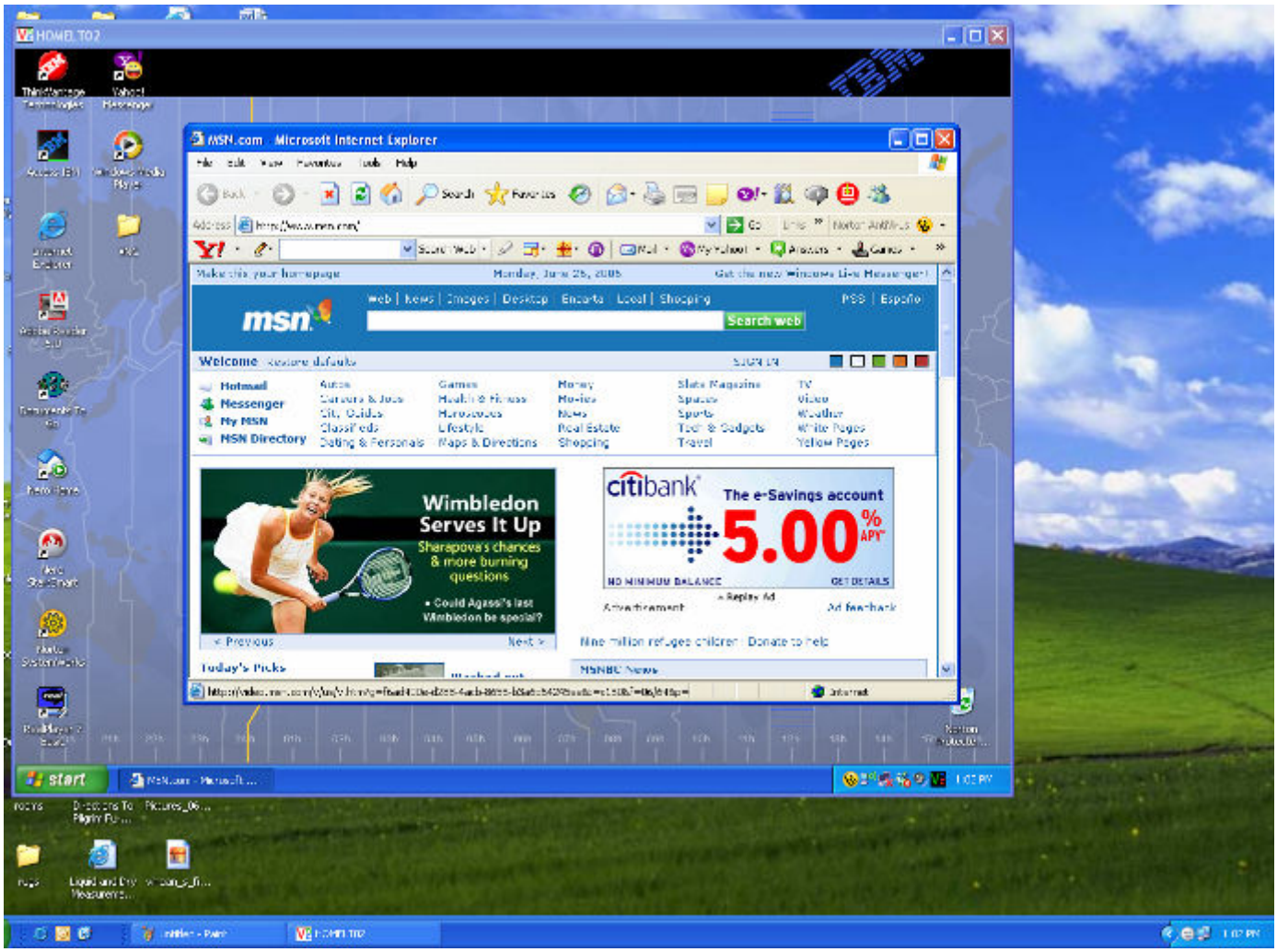



Figure 7. Display window of Server machine on the remote Viewer machine.

### *Drawbacks and Suggestions*

VNC has some known bugs. Some have been fixed and the others have workaround options that are recommended. VNC is not a very secure protocol. Encoded passwords are used but sniffing of both the encryption key and encoded password is possible and could make the system vulnerable. A suggestion is to use long passwords which are at least 8 characters long. For more secure connections, however, VNC may be used over VPN or SSH connections, which would enable extra security, and a stronger encryption. UltraVNC, a flavor of VNC, allows the use of open-source encryption plug-ins that encrypt the entire VNC session and also provide password authentication and a secure data transfer. UltraVNC also allows authentication by the use of NTLM (NT LAN Manager, a computer networking security protocol) and Active Directory (a directory service used to store information about the network resources) user accounts.VNC allows remote access to remote users. A good way to secure your computer against unwanted and unauthorized access is to block the port used by VNC by a firewall, making it impossible for intruders to break into the service. Firewall software, such as Zone Alarm,

can also be used to prevent unauthorized access. For academic use, firewall software is an easy and effective way to achieve a secure connection. The next exercise discusses the basics of firewall software.

***Exercise 6: Learn the basics of firewall software***

Firewalls determine which traffic to allow or deny based on the network layer it operates on [13]. Firewall software is software that protects a computer connected to a public network from unauthorized access by hackers. There are two kinds of firewall software: basic firewalls and dynamic firewalls. Basic firewall software monitors the communication that flows between your computer and the Internet. When it sees any suspicious inbound requests from unknown sources, it automatically identifies it and also effectively blocks it. Dynamic firewall software, on the other hand, not only protects your computer from unauthorized inbound accesses/ requests but also protects your PC from unauthorized outbound communication. Also, basic firewalls keep your computer's door always open to the Internet, but dynamic firewalls open your computer's door to the Internet only when needed, and close the door immediately after the authorized requests. Therefore dynamic firewalls provide more security and protection than basic firewalls. A widely-used and effective dynamic firewall, available freely, is Zone Alarm. It has an easy-to-use interface, it is compatible with Windows operating systems and all anti-virus software, and protects the computer without slowing it down or using much of its resources [14]. "Zone Alarm's intrusion blocking systematically identifies hackers and blocks their access attempts. Stealth Mode automatically makes your computer invisible to anyone on the Internet". Overall, it keeps the user's network connection safe and secure.

As VNC accepts keyboard presses and mouse clicks from remote users who get authenticated by providing connection details and a password, the virtual connection is vulnerable to unauthorized intrusions. It is therefore very important to make the connection secure by following one or more suggestions outlined above in the "Drawbacks and Suggestions" section of exercise 6. As mentioned before, for academic use, an effective but affordable solution is to team VNC with firewall software. The important point to remember when selecting firewall software for securing VNC is that VNC needs firewall software that not only checks any inbound accesses but also validates any outbound communication. This means the essential requirement of dynamic firewall software. Zone alarm firewall is a good choice for VNC as it validates both inbound and outbound communication, does not slow down the connection, does not require much of the computer's resources, and is also available freely.

**Conclusion**

The paper presents a set of laboratory exercises for learning two software tools, VNC and Visual Route, and the logic behind combining both tools for increased security. These exercises are designed by the author(s) using the open source network testing tools to complement the existing laboratory exercises in networking courses.

Visual Route is a software suite that helps to understand various networking commands such as traceroute, ping, and whois, and has various features that provide an in-depth analysis and understanding of specific networking concepts. Visual Route's graphical user interface is easy, clear and convenient to operate. Integrating a Firewall provides improved security and incorporating a Packet Sniffer or Network Analyzer can provide additional functionalities such as detecting erroneous packets to determine the bottlenecks in the network. VNC is a software suite that provides a virtual, remote-sharing environment for its users. Its services and unique features have led to its active, wide-spread usage by millions in Universities, in homes, and in the industry. It has a few drawbacks, but use of the recommended solutions will ensure a safe and secure connection for all users. Overall, smart usage of the VNC service can let us connect across the globe in a few clicks!! This article provides an in-depth discussion of two software suites – Visual Route and VNC. It discusses how the two software suites can be made more secure by teaming them up with firewall hardware, firewall software, and/or packet sniffers. This work can be expanded with discussions of other networking concepts and technologies that will enhance one's networking experience.

**Bibliography**


[1] http://www.realvnc.com/what.html
[2] http://www.visualroute.com/support/index.html
[3] http://en.wikipedia.org/wiki/Traceroute
[4] http://www.visualroute.com/ed_webaccess.html
[5] Visual Route Software help http://visualroute.visualware.com/
[6] http://www.realvnc.com/how.html
[7] http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/tracert.mspx?mfr=true
[8] http://en.wikipedia.org/wiki/Ping
[9] http://en.wikipedia.org/wiki/Whois
[10] Feldman, Jonathan. "Network Protocol Analyzers" Available online at http://www.samspublishing.com/articles/article.asp?p=30166&seqNum=1
[11] Cisco Networking Academy Program CCNA 1 and 2 Companion Guide Revised Third Edition , Cisco Press, Indianapolis, IN. 2005
[12] http://en.wikipedia.org/wiki/Ethereal_%28software%29
[13] Firewall Q&A http://www.vicomsoft.com/knowledge/reference/firewalls1.html
[14]http://www.zonelabs.com/store/content/support/zasc/whyZoneAlarm.jsp?dc=12bms&ctry=US&lang=en&lid=zasupp_k
[15] http://en.wikipedia.org/wiki/VNC


## Appendix A

***How VNC works?***

Different versions of VNC software are available to support different architectures and operating systems. Different operating systems on which VNC can be run are: Windows

2000, Windows Me, Windows NT, Windows CE, Windows 9.x, Macintosh, Linux, and UNIX. VNC also has a Java viewer that allows any kind of desktop to be viewed with a Java-capable browser. There are VNC clients for Pocket-PC devices as well. VNC consists of two components, a client and a server. The server is the program on the computer that shares its screen/resources, and the client (or viewer) is the program that watches, interacts, and uses the resources of the server. A VNC viewer on any operating system can connect to a VNC server running on any other operating system. Also, VNC allows multiple clients to connect to a single VNC server at the same time.

"VNC is a very simple protocol, based on one graphic primitive: 'Put a rectangle of pixel data at a given x, y position'. That is, the server sends small rectangles of the frame buffer to the client. This in its simplest form uses a lot of bandwidth, so various methods are used to reduce it. For example, there are various *encodings* - methods to determine the most efficient way to transfer these rectangles. The VNC protocol allows the client and server to negotiate which encoding will be used. The simplest encoding, which is supported by all clients and servers, is the *raw encoding* where pixel data is sent in left-to-right scanline order, and after initial setup, then only transfers rectangles that change. Because of that, this encoding works very well if only a small portion of the screen changes from one frame to the next (like a mouse pointer moving across a desktop, or text being written at the cursor), but bandwidth demands get very high if a lot of pixels change. (Full screen video is the most radical example of this.)" [15]

By default, VNC uses ports 5900 to 5906. However, if needed, these ports can be changed. Windows-based computers use only a single port as they lack the multi-session features of UNIX-based machines. So, by default, the display number for Windows-based computers is 0 and that maps to TCP port 5900. Depending on the application, one may decide to download just the VNC viewer or both the VNC server and viewer. Download the VNC that is compatible with your operating system/architecture. One can download from www.realvnc.com/download.html.
Depending on the level of security and features, one can choose form the following:

- Free edition
- Personal edition
- Enterprise edition