

Virtual Network Computing- A Prodigious Technology For Remote Desktop Sharing

Harshita Tomar*, Gunjesh Sahney**

*(Department of Computer Science, Guru Gobind Singh Indraprastha University, New Delhi)

** (Department of Electronics and Communication, Guru Gobind Singh Indraprastha University, New Delhi)

ABSTRACT

Virtual Network Computing abbreviated as V.N.C. is a stupendous technology adverted for remote desktop sharing. It is envisioned as an open source research project in the late 1990's which was spawned at the Oracle Research Lab. It is an intelligible protocol, based on a graphic primitive. This efficacious application is mainly contemplated for triggering and controlling remote desktop with in a network. This protocol is intrinsically used for prospecting Graphical User Interface desktops on remote machines within a LAN or over a WAN and providing access to home computing environments. Usually applications on a network can be accessed and executed by users as per the permissions ascribed by the administrator but impotent to access the desktop. The "VNC" is one such application that helps in catering the imperative facilities for inducing specific applications on a remote machine. The ingenuousness and candor makes this protocol competent, robust and puissant. The VNC protocol is utterly independent of operating system, windowing system, and applications dissonant from other remote display protocols such as the XWindow System and Citrix's ICA. The VNC server is used for sharing and dispensing its screen where as, the VNC client ganders and collaborates with the server.

Keywords: Virtual network computing, remote frame buffer, Computer Supported Cooperative Work, RealVNC

I. Introduction

Virtual network computing is one of the most congruous outgrowth of supervising a computer at a secluded spot via internet by prospecting the computer. They can aspect files, prosecute programs, delete stuff, etc. conversely the computer can be used exactly by various bystanders although a bit slower. A replica of the desktop of the server is consorted to our computer and we can contrive in the server computer by fabricating events in the viewer computer. Internet is wielded as the transmission medium between the server and the viewer computer. The supervising is done with a bolster of mouse events as the operating system is graphical user interface. When a mouse event is betiding on a particular pixel, then it is dispatched by the viewer to the server and the modification is consorted to the viewer. So the user will not grope that two computers are operating here and will get a feel that the server is used by himself. There can be an aberration in the speed of VNC and any other remote desktop software sometimes performing cogently just like the local computer but other times exhibiting sluggish responsiveness due to network latency. Programming of VNC client is quite facile; intensification only on the frame buffer and TCP/IP transmission is desired. Programmers need to be conscientious while programming for client and ensures that client side must be as simple as possible. [1]

The section I of this paper familiarizes the given topic in concoction with illuminating the background information. The rest of the paper is structured as superseded; section 2 concisely explicates the installation procedure of V.N.C., section 3 and 4 deal with the working of V.N.C. and security issues respectively. The advantages and disadvantages of this process are elucidated in section 5 and 6 respectively, followed by the applications in section 7 and conclusion in the terminating section.

II. Installation Procedure

1. Firstly one needs to visit Real VNC to attain a copy of the VNC software which is complimentary for exclusive use.
2. Next, Install VNC on all machines which you plan to access remotely.
3. Select "service mode" during installation. This accredits VNC to run as a Windows service, which offers resource-management benefits.
4. After this, confirm the execution of VNC on all machines. If the service is active and running, an icon in the system tray showing the letters "VNC will be displayed".
5. To access another machine from your current location, Click Start > All Programs > RealVNC > VNC Viewer 4 > Run VNC viewer to access another machine from your current location. A small input box will emerge.
6. Next, type the IP address of the familiar remote computer and click OK. This will lead to establishment of successful connection. [5]

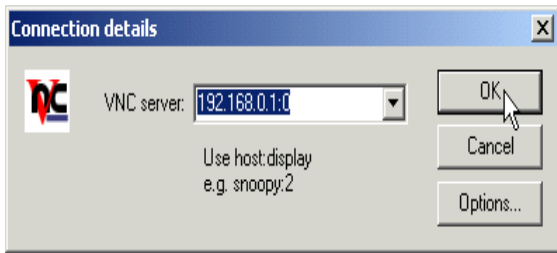


Fig.1 Connection details

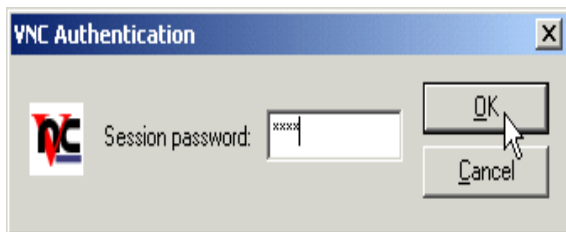


Fig.2 VNC authentication

III. Working of VNC

The protocol concedes the server to amend the frame buffer demonstrated on a viewer. It has capability to germane on all operating systems, windowing systems and applications as it serves at the frame buffer level. It comprises of X/Unix, Windows 3.1/95/NT, Macintosh and might also include PDAs and any other accessories dwelling any mode of communications link. This protocol will regulate any reliable carriage like TCP/IP. To work with VNC, run a server and then associate a viewer to it initially. From web, packages for the platforms to be used can be obtained and installed later. The current VNC software desires a TCP/IP connection between the server and the viewer. [4]



Fig.3 VNC setup

3.1 Rectangular update

Around a single graphics primitive: "put a rectangle of pixel data at a given coordinates " the display view of the protocol is placed. This might be an improficient approach to draw erratic user interface components instead we can elect the relevant provision for each rectangle we dispatch and make the gilt edged

use of network bandwidth, client drawing speed and server processing speed because we have assortments of disparate encoding strategy for the pixel data. The lowest prevailing denominator is the so-called raw encoding, where the rectangle is basically a pixel data transported in left-to-right scan line manner. All clients and servers must reinforce this encoding.

3.2 Adaptive update

An array of rectangles of pixel data synthesizes a frame buffer update. An update exhibits a modification from one valid frame buffer state to another. Therefore, an update is complementary with a frame of video. It diversifies in the way that it frequently impinges only a small space of the frame buffer. Each rectangle may be encoded using a divergent pattern. The update protocol is demand-driven by the client in other words an update is only delegated by the server as an acknowledgement to an unequivocal request from the client. All screen varies since the clients, last request are commingled into a single update. This provides the protocol an adaptive quality: the lethargic the client and the network, the lower the rate of updates.

3.3 Input protocol

The input viewpoint of the VNC protocol relies on a definitive workstation model of a keyboard and multi button pointing device. Whenever the user constrains a key/pointer button/ moves the pointing device the client circulates input events to the server. Input events can also be amalgamating from other nonstandard I/O devices.

3.4 RFB protocol

RFB is a simple remote frame buffer protocol for remote access to graphical user interfaces that obliges a client to glimpse and control a window system on a distinct computer. RFB befits to all windowing systems and applications as it works at the frame buffer level. It describes the communication between an RFB client and RFB server.

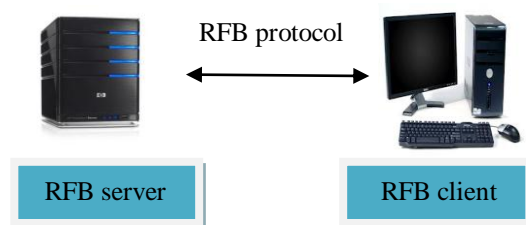


Fig.4 RFB protocol

3.5 Connection Setup and Shutdown

To domiciliate a client-server connection, the server initially requests authentication from the client making use of challenge-response VNC server VNC viewer VNC protocol scheme; the client normally oblige the user to enter a password . The server and client then interchange messages to negotiate desktop

size, pixel format, and encoding schemes. The client appeals for an update for the entire screen and the huddle commences. Both the sides can leave the connection at any time without offshoot because of the stateless nature of the client.

3.6 Running a viewer

VNC can be executed from the command line with the windows viewer, but more customarily run it from the VNC group displayed at the Start Menu. In this situation, the host name has to be stimulated and number should be displayed: Enter it and click OK. Password will be required to proceed further, after which the remote display can be beamed. When a Windows or Mac server is associated then the displayed number will be 0, unless and until it is changed. If the machine operating the server lacks a proper DNS entry then no one will be able to access the name and have to compensate it. This can be administered on most platforms by contriving file which maps names onto IP addresses.

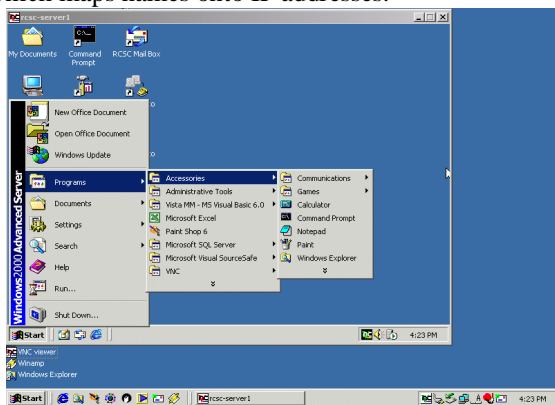


Fig.5 Virtual desktop

3.7 VNC servers

Writing a VNC server is marginally arduous than writing a viewer due to the fact that the protocol is originated to view the client as uncomplicated as possible. It depends upon the server to execute any mandatory translations. Large number of VNC servers for different users can be operated by a single UNIX machine, each depicting a distinct VNC desktop. Each desktop is similar to a virtual X display having a root window consisting of several X applications. The Windows VNC server was even more difficult to construct. To monitor display updates and the model of multi user operations windows has fewer places to insert hooks into the system. Our current server simply replicates the real display to a remote client.

3.8 Running a windows server

Build in the Windows server, WinVNC, by running the Setup program comprised in the distribution. This will contrive a VNC group in the Start Menu. Build in the default registry settings by making use of the option in the VNC group. Run the WinVNC server. If WinVNC is being used first time on the machine then password is needed to be set, which will be required further. Normally all the other

options should be kept on default settings. Click OK and the server should be running. A small icon will be installed on the system tray and by right-clicking on this most aspects of the server can be controlled.

IV. Security Issues

VNC has a miscellany of serious security issues elucidated below:

1. VNC communication is not comprehensively encrypted, though the password that is availed to control the computer is encrypted. This might not appertain to the organization; after all, standard email and web access is not encrypted either, and substantial skill is required for someone to ambush VNC and attain profound and pragmatic information.
2. Security for sensitive information is not provided by VNC. Nevertheless, where the use of VNC is justified by the business case, steps should be adopted for securing default installation. Guidance on curtailment of some of the risks is provided by this technical note.
3. There is no guarantee for a secured deployment of the product by using the information within this document.[11]

V. Advantages

1. One of the major benefits of this process is the liberty to excerpt your favorite computing environment.
2. It is minuscule and elementary which serves as another great advantage.
3. Effortless access to the potent UNIX system is another advantage.
4. Remote access is made attainable to the extensive platforms.
5. Another benefit is for server administrators to analyze and maintain a server remotely.
6. It is usually used for controlling a proper functional system over a network from a disparate computer.
7. The VNC protocol is very utilitarian and robust as a cross platform explication.
8. Interchangeability is a clear advantage.
9. Unrecompensed, that is, it is free of cost and can be downloaded freely and used.
10. One of the prevalent benefits of VNC is that it is sharable which means that a single desktop can be exposed and used by various beholders at once, allowing Computer Supported Cooperative Work (CSCW) applications.
11. It is stateless, that is, the data can be apprehended efficiently from one system to another devoid of any interrupt.
12. Data can be accessed conveniently and efficiently without any need for installation. [13]

VI. Disadvantages

1. One of the major deprivations is that in comparison to business settings, VNC is not flexible.

2. A connection to VNC server can be contrived only through a direct IP address which makes both local and remote access arduous to set up.
3. VNC is network resource intensive.
4. In case of low bandwidth connection, an abominable situation emanates which means that a good bandwidth is required for its decorous functioning.
5. It is devoid of any modem access or features which is a detriment.
6. Display can be a bit sluggish, convulsive and incomplete.
7. File systems are apportioned between distinctive operating systems.
8. Exceptional multi-user support is not bestowed for accessing non-Unix platforms.
9. Various other mechanisms are obligatory for transferring files.
10. There is dearth of prevalent concept of several user accesses in PC/MAK.

VII. Applications

1. Pragmatic for accessing important information.
2. It is used for downloading and checking-up emails.
3. Telephone answering machine can be dialed and reprogrammed through a graphical interface with an aid of modem.
4. Any processing or computation can be initiated or halted.

VIII. Conclusion

VNC is an ultra-thin and meager client system based on an elementary display protocol. The default installation of VNC is inherently insecure and precarious. It has the potential to significantly deteriorate a system's complete level of security. Consequently it is essential that the business benefits be deemed to justify the additional risks introduced by installing VNC onto critical servers. A multifarious business benefits are there in using VNC for access to remote systems, but on the other hand a number of risks are present which needs to be managed properly and precisely. In particular, potential procurers of VNC need to be cognizant that VNC does not cater towards the security for sensitive information. VNC installation can be hardened, but even if this is undertaken, some issues still need to be addressed and appraised in any risk assessment. Even in its prevailing form, its remote control applications are almost inexhaustible, and many users and supporters in a typical support environment can be found. VNC means really here, virtually there. [14]

References

- [1] http://www.webopedia.com/TERM/V/virtual_network_computing.html

- [2] A. Boukerche, R. W. N. Pazzi, and J. Feng, "An end-to-end virtual environment streaming technique for thin mobile devices over heterogeneous networks," *Computer Communications*, vol. 31, no. 11, pp. 2716–2725, JUL 15 2008.
- [3] Md. Sanullah Baig, Rajasekar M. and Balaji P, Department of Computer Science and Engineering, Gojan School of Business and Technology, Chennai-600052, India "Virtual Network Computing." *VNC – How it works. 1999. AT&T Laboratories Cambridge. 5Jul.2001*
<http://www.uk.research.att.com/vnc/howitworks.html>
- [4] Virtual Network Computing Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood and Andy Hopper Reprint from *IEEE Internet Computing Volume 2, Number 1 AT&T Laboratories Cambridge (1999). "X-based VNC server". Virtual Network Computing. Archived from the original on 2007-03-19. Retrieved 2007-03-24*
<http://www.yolinux.com/TUTORIALS/VNC.html>
- [5] <http://www.yolinux.com/TUTORIALS/VNC.html>
- [6] <http://www.cl.cam.ac.uk/research/dtg/attarchived/vnc/>
- [7] *IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 5 (Nov. - Dec. 2012), PP 16-20 Virtual Network Computing Based Droid desktop* Vaidehi Murarka, Sneha Mehta, Dishant Upadhyay, Abhijit Lal
<http://www.realvnc.com/docs/rfbproto.pdf>
- [8] <http://www.realvnc.com/docs/rfbproto.pdf>
- [9] *Internet Engineering Task Force (IETF) T. Richardson, J. Levine Category: Informational RealVNC Ltd. ISSN: 2070-1721 March 2011*
- [10] Richardson, T., Stafford-Fraser, Q., Wood, K. and Hopper, A., "Virtual Network Computing", *IEEE Internet Computing, Vol. 2 No. 1*, Jan/Feb. 1998
- [11] <http://searchnetworking.techtarget.com/definition/virtual-network-computing>
- [12] http://compnetworking.about.com/od/softwareapplicationstools/g/bldef_vnc.htm
- [13] *International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011 DOI: 10.5121/ijnsa.2011.3101 1 Virtual machines and networks – installation, performance, study, advantages and virtualization options* Ishtiaq Ali and Natarajan Meghanathan
- [14] http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=656066&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D656066



Harshita Tomar Bachelors of Technology (B.Tech), Department of Computer Science, Guru Tegh Bahadur Institute of Technology, GGSIPU, New Delhi.



Gunjesh Sahney Bachelors of Technology (B.Tech), Department of Electronics and Communication, Guru Tegh Bahadur Institute of Technology, GGSIPU, New Delhi.