

A Study on Virtual Network Computing In RDP

Geethamani G.S¹, Mohamed Haris.W²

¹Assistant Professor, Dept of IT

²Dept of IT

^{1,2}Hindusthan College of Arts and Science, Coimbatore

Abstract- A remote desktop protocol is computer software that allows a user to control a computer remotely. There are two ways this can be done. Either by copying what is shown on the remote computer to the local computer or by copying the instructions that draw the screen. The normal pc desktop can be taken remotely and we can access from any part of the world using internet and wap support service. The operations such as accessing the internet, sending emails, and also system controls like shutdown, log off, restart through the mobile Phone. The remote desktop connection can be made wireless and can be accessed from any part of the world. In this paper, we will enlist the process to access the desktops of remote computer systems with the use of a android based cellular phone. This process will be carried out using Virtual Network Computing based architecture. A user will be able to access and manipulate the desktops of remote computers through a VNC viewer that will be provided on the user's cell-phone. Conditions that must be followed are that a VNC server must be installed on the person's computer which will be monitored and it must be connected to a Wi-Fi network. The user can access and manipulate the desktop within the Wi-Fi range irrespective of various platforms like windows, mac or linux.

attached to a system. The cellular customer can see and maneuver the desktop on the cellular handset.

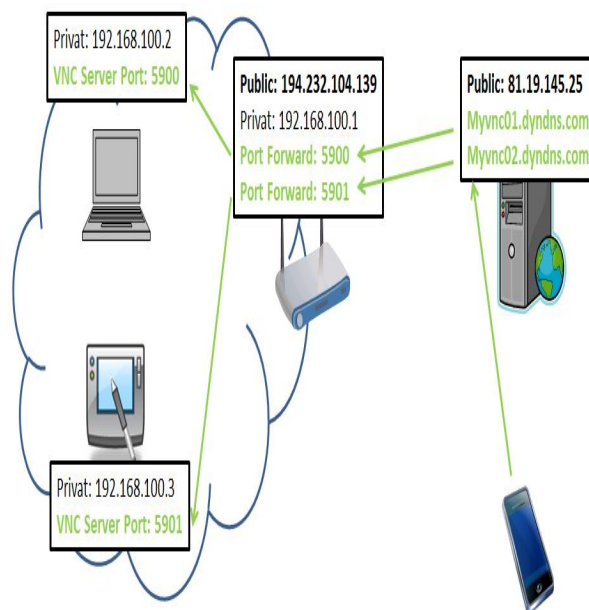


Fig 1: VNC

Keywords- VNC,RFB,Android, Java,Wi-Fi, Desktop.

I. VNC

Virtual Network Computing (VNC) is a pixel-based desktop sharing system. It uses the remote framebuffer (RFB) protocol to transmit its images. 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. It is, in spirit, a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is management, but from anywhere on the Internet and as of a wide variety of machine architectures. Virtual network computing based architecture for accessing the desktop of various remote systems (such as MS Windows, Macin-tosh, and UNIX systems) from a cellular handset. It is tacit that the remote computer system is running a VNC server and that it is

II. EXISTING SYSTEM

- 1) In the existing system we make use of BLUETOOTH to right to use the organization contents in a mobile.
- 2) In this, only particular application can be accessed.
- 3) The files of the system can be alive accessed just within short distances.

III. PROPOSED SYSTEM

Virtual Network Computing is a graphical desktop sharing system providing remote control via network. It supports a controlling functionality by usage of a graphical screen update from a controlled device and capturing a mouse and/or a keyboard. VNC system is based on RFB (Remote Frame Buffer) protocol to transmit all information between connected devices. Transmission is running on one port from range 5900-5906 using TCP/IP protocol. VNC system required two type of application for a proper work - server application

for a machine under control and client - for a supervisor (controlling) device. Client side is called viewer because of its functionality. Controlling machine is responsible for viewing a shared desktop (or screen in general) and capturing and converting all user activity into the RFB protocol[7] messages. On the other side, server must to interpret all events received from client and inject them into self system. Server should also response to graphic screen update request by sending back a desktop view to connected client. The cellular user can see and manipulate the desktop on the cellular phone. The same cellular phone to talk someone, the user must terminate the network connection.

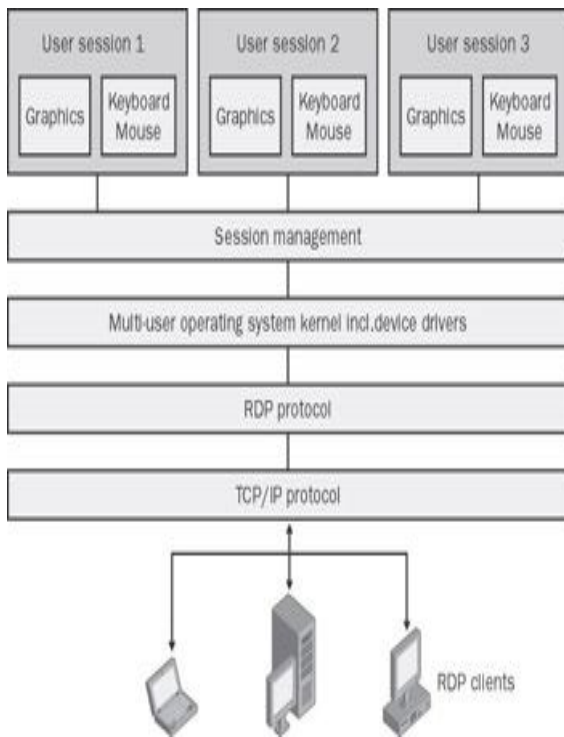


Fig 1: VNC Architecture

IV. 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. 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.
10. It is stateless, that is, the data can be apprehended efficiently from one system to another devoid of any interrupt.

V. 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.

VI. SECURITY ISSUES

VNC has a miscellany of serious security issues elucidated below: 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. 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]

VII. RFB PROTOCOL

The VNC server and client communicate using a protocol called RFB (Remote Frame Buffer). The basic idea of this protocol is to communicate changes to the screen contents from the server to the client using various RFB encodings. RFB also allows mouse and keyboard input on the client to be transmitted to the server, so that the client can not only passively observe the server's desktop, but actively interact with it. 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 benefits 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.

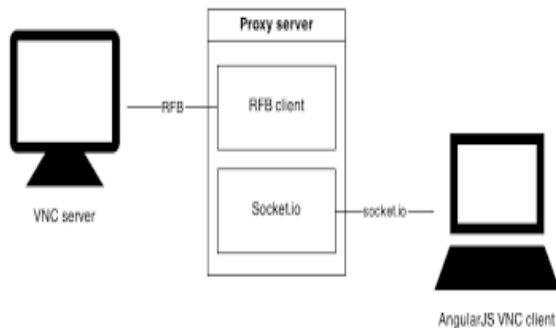


Fig 2: RFB Protocol

IX. RFB PROTOCOL IMPLEMENTATION STEPS

There are three stages to the RFB protocol implementation. First is the handshaking phase, the purpose of which is to agree upon the protocol version and the type of security to be used. The second stage is an initialization phase where the client and server exchange ClientInit and ServerInit messages. The final stage is the normal protocol interaction. Handshaking begins by the server sending the client a ProtocolVersion message. This lets the client know which is the highest RFB protocol version number supported by the server. The client then replies with a similar message giving the version number of the protocol which should actually be used (which may be different to that quoted by The ProtocolVersion message consists of 12 bytes interpreted as a string of ASCII characters in the format "RFB xxx.yyy\n" where xxx and yyy are the major and minor version numbers, padded with zeros. The server). A client should never request a protocol version higher than that offered by the server.

A. ClientInit:

Shared-flag is non-zero (true) if the server should try to share the desktop by leaving other clients connected, zero

(false) if it should give exclusive access to this client by disconnecting all other clients.

B. ServerInit:

After receiving the ClientInit message, the server sends a ServerInit message. This tells the client the width and height of the server's framebuffer, its pixel format and the name associated with the desktop.

C. Client to server messages:

The client to server message types defined are:

Table 1: Client Server Message Types

Number	Name
0	SetPixelFormat
1	SetEncodings
2	FramebufferUpdateRequest
3	KeyEvent
4	PointerEvent
5	ClientCutText

X. 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. 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. Next step will be implementing this system over Internet. The same RFB protocol will be used for the data transfer. The VNC architecture will be used for implementation of the system. Thus the extended scope of this system will prove to be helpful in providing mobility and accessing the remote desktop over the internet. Effortless access to the potent UNIX system is another advantage. Remote access is made attainable to the extensive platforms.

REFERENCES

- [1] ArchanaJadhav1 ,Vipul Oswal2,Sagar Madane3 ,Harshal Zope4,Vishal Hatmode5 “VNC ARCHITECTURE BASED REMOTE DESKTOP ACCESS THROUGH ANDROID MOBILE PHONES” International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2012 .
- [2] Remote Control of Mobile Devices in Android Platform Angel, Gonzalez Villan , Student Member, IEEE and JosepJorbaEsteve,Member, IEEE.
- [3] Virtual Network Computing,Tristan Richardson, Quentin StaffordFraser,Kenneth R. Wood and Andy Hopper,Reprint from IEEE Internet Computing Volume 2, Number 1 January/February 1998.
- [4] T. Richardson, \The RFB Protocol", Tech. rep., RealVNC Ltd,2007 .
- [5] The RFB Protocol,TristanRichardson,RealVNC Ltd(formerly of Olivetti Research Ltd / AT&T Labs Cambridge) ,Version 3.8,Last updated 26 November 2010.
- [6] R.Manikandasamy”Remote Desktop Connection Using Mobile Phone”International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 8, August 2013.
- [7] H.Kawashima, K. Koshiha, K. Tuchimochi, K. Futamura, M. Enomoto, and M. Watanabe, “Virtual PC-type thin client system,” NEC TECHNICAL JOURNAL,(SEP-2007).
- [8] P. Simoens, F. A. Ali, B. Vankeirsbilck, L. Deboosere, F. De Turck, B. Dhoedt, P. Demeester, and R. Torrea-Duran,“Cross-Layer Optimization of Radio Sleep Intervals to Increase Thin Client Energy Efficiency,” IEEE COMMUNICATIONS LETTERS, (DEC- 2010).
- [9] V. Rivoira and F.Pascali, “HSDPA: High-speed internet over your mobile phone”, IEC newsletter, (June -2007).
- [10] Michael Lloyd Lee, “J2ME VNC”, codigofonte, (February-2005).
- [11]HarshitaTomar ,GunjeshSahney ,”Virtual Network Computing- A Prodigious Technology For Remote Desktop Sharing”HarshitaTomar et al Int. Journal of Engineering Research and Applications . www.ijera.com ISSN : 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013.
- [12] 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). "Xbased VNC server". Virtual Network Computing. Archived from the original on 2007-03-19. Retrieved 2007-03-24
- [13]IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 22788727Volume 6, Issue 5 (Nov. - Dec. 2012), PP 16-20 Virtual Network Computing

Based Droid desktop VaidehiMurarka, Sneha Mehta,DishantUpadhyay, AbhijitLal .