Understanding Virtual Network Computing

VNC is a free, open-source remote control and monitoring tool. It consists of viewer and server components, and its platform-independence adds greatly to its usefulness.

By Phil Morris
Technical Journalist

A number of commercial products are currently available which allow remote viewing / control of the desktop of a host machine. However, VNC differs from these in a number of ways. Firstly, it is free; secondly, it is open source (available for redistribution and modification under the GNU General Public Licence); and thirdly, it is platform-independent, so adding greatly to its versatility.

VNC began its life at the Olivetti and Oracle Research Laboratory (ORL) as their Teleporting System - this allowed the interface of an X Windows application to be displayed on a remote machine. However, this had relatively heavy resource and bandwidth requirements, plus the X security model was an issue. In 1994 the Videotile was built by ORL - this was a display device with Pen, LCD screen and ATM connection. The VNC Protocol was developed from the Videotile, utilising the method of only transmitting the parts of the screen that changed, so greatly reducing bandwidth. In 1995 the Videotile mechanism was implemented in Java, so allowing anyone with a Java-equipped Web browser to access remote desktops running the relevant server software. It was now possible to access remote desktops from anywhere in the world, so providing far greater flexibility. The VNC Protocol was then fully developed, so leading to the VNC viewers and servers described here. In January 1999, AT&T acquired ORL, so making VNC a project of AT&T Labs, Cambridge, UK.

Two Components

VNC consists of two main programs: the viewer and the server. The viewer is a small program (150 KB in size for the Win32 version) which allows the remote PC to connect to and view / control the desktop of the remote machine. No installation is necessary for the viewer - the relevant program for the operating system of choice is simply run on the remote machine. The server does require an installation process which differs according to the operating system - the Win32 version, for example, entails the use of a setup program, installation of the WinVNC Service, plus the installation of the VNC hooks via a registry file. These two programs are explained in greater detail below.

The VNC protocol is based on the concept of a Remote FrameBuffer (RFB), and because it works at the framebuffer level it is versatile across a range of windowing and operating systems and applications. It will operate over any reliable transport protocol (such as TCP / IP). Because of the low bandwidth requirements it is a true thin-client protocol and will run on a wide range of hardware. The server by necessity has more overheads than the viewer, but even this shouldn't stop it from operating well on any PC available today.

VNC Servers

The main server program needs to be run on the host machine so viewers have something to connect to. The server is currently available for X (Unix), Windows and PPC Macintosh. There is also a version called rfbcounter, which is a simple server produced with the aim of demonstrating that things other than desktops can be displayed. Under Windows, the server can be run as an application or service, but for various reasons it is recommended to run it as a service (for example, a user doesn't then need to be logged into the server machine before a viewer can access it). Once installed, the server can be set up to allow viewers to access it.

I will use the Windows version as an example. In this case, all the default settings can be used for an easy test startup, and the only thing that you will need to do is enter a password for viewer access. Failure to do so will result in a dialog box with a security warning message which then takes you back to the Properties page (see Figure 1), so forcing a password to be entered. Besides the options available via the Properties page, various command-line options are also available. It is prohibitive to list them all here, so instead I have listed a few examples:

`-install` installs the WinVNC Service

`-kill` kills a running copy of WinVNC

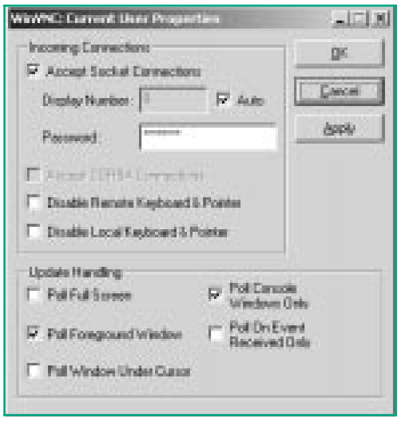
`-about` shows the About box

It is also possible to run WinVNC from the command line with multiple options, so combining commands on one line. Quite a number of advanced settings are also available under WinVNC, but these are somewhat more fiddly to configure because the registry needs to be edited. Ways of simplifying this process are currently being looked into for implementation into future revisions.

VNC Viewers

The viewer is run on the remote machine that will be connecting to the server. The viewer is currently available for X (Unix), Windows, Java, Macintosh (requires MacOS 7.1 or greater plus Open Transport 1.1.1 or greater) and WindowsCE (requires Windows CE 2.0 or later). The following information covers the use of the Windows VNCviewer. No installation or configuration is necessary - the executable is simply run from hard drive or floppy disk, either by double-clicking the icon or typing in the name of the VNC executable via the command line. Once started, a dialog box is displayed prompting for the name or IP address of the server (see Figure 2). After this, the user is prompted for the session password (as previously configured via the server software). Successful authentication brings up a virtual display of the server's desktop. As can be seen in Figure 2, an Options button is available - clicking on this displays the options which can be seen in Figure 3.

Out of all the available options, View Only is the one that is the most interesting, since it allows the viewer to view activity on the server without the server being controlled in any way by the viewer. This is especially useful for monitoring purposes (monitoring a backup program running on a server, for example) or for "spying" purposes - ie, keeping tabs on how users are utilising their machines. This latter use would no doubt create some controversy in some circles - after all, no-one likes to be spied on - but it does have a valid use in certain circumstances. Once connected to the server, the viewer can control it as if the user was sitting at the remote machine. I found the speed to be good on a 10 Mbits / second LAN. Various options are available via a pull-down menu which allows the user to change certain functions once connected. These are as shown in Figure 4. If started via the command-line then various options can be input at that stage without the need for



WinVNC: Current User Properties

Incoming Connections

☑ Accept Socket Connections

Display Number: 0 ☑ Auto

Password: ********

□ Accept CORBA Connections

□ Disable Remote Keyboard & Pointer

□ Disable Local Keyboard & Pointer

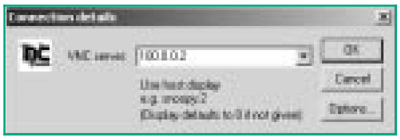
Update Handling

□ Poll Full Screen ☑ Poll Console Windows Only

☑ Poll Foreground Window □ Poll On Event Received Only

□ Poll Window Under Cursor

Figure 1 - The Windows VNC server.

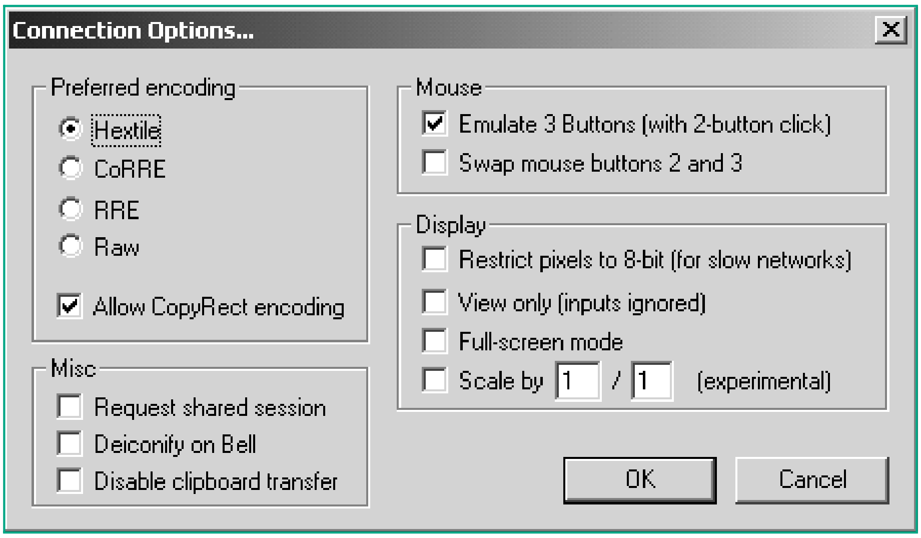


Connection details

VNC server: 10.0.0.2

Use host:display
e.g. snoopy:2
(Display defaults to 0 if not given)

Figure 2 - Connection Details dialog box.



Connection Options...

Preferred encoding

● Hextile

○ CoRRE

○ RRE

○ Raw

☑ Allow CopyRect encoding

Misc

□ Request shared session

□ Deiconify on Bell

□ Disable clipboard transfer

Mouse

☑ Emulate 3 Buttons (with 2-button click)

□ Swap mouse buttons 2 and 3

Display

□ Restrict pixels to 8-bit (for slow networks)

□ View only (inputs ignored)

□ Full-screen mode

□ Scale by 1 / 1 (experimental)

Figure 3 - Connection Options dialog box.

making menu selections. As with the server description, it is prohibitive to list them all here, but some examples are shown in Figure 5. In use I found that blocks of pixels sometimes appeared on the screen as a new area was being drawn, but these were erased by the program once the display had finished updating itself. Because of bandwidth restrictions it is obviously not recommended to run programs on the server that constantly move a lot of graphics around (games, for example), but that shouldn't present a problem as that isn't what the program was designed for. It is a remote control and monitoring tool - not a means of remotely playing games.

During the hours I have spent experimenting with the Windows viewer I didn't find any glaring restrictions or omissions; I ran a number of programs and all performed as expected. Some didn't redraw correctly after dragging and dropping data, but a simple click on the Screen Refresh option within the viewer soon remedied that. The only thing I found offputting (as indicated above) was the drawing of such items as pull-down menus - during this process parts of the image can appear to be temporarily corrupted as they are drawn. This is not a major problem as, once the drawing is finished, they look as they should, but it takes some getting used to.

Out of all the viewers, the one I find the most interesting is the WindowsCE implementation - the portability of the CE machine coupled with the ability to connect to and control any host has the potential to be extremely useful. For example, imagine being able to dial into work from the CE machine and connect to the VNC server running under X Windows on a Unix server.

Security

Due to the potentially sensitive nature of any data and the possibilities of unscrupulous persons remotely viewing or controlling sensitive servers or desktops,

Common Uses For VNC

- **Workstation to Workstation (Windows)** - In a PC support environment this would arguably be the most useful. With the server software loaded onto each machine on the network, and the viewer on restricted machines (or carried around on a floppy disk by support personnel) it would be easy for remote diagnostics to be carried out on PCs that were located remotely (perhaps many miles away), either via the company WAN or a dial-up connection to the remote PC. The issue of monitoring / spying also crops up here - if it is suspected that a member of staff is not utilising his / her time correctly, then the viewer, if connected in View Only mode, can easily "snoop" on the user. This could be done by a technician, or even someone senior who might not have the relevant technical skills; in View Only mode no real technical skills are required to start up, view, and subsequently shut down the software.
- **Workstation to Server** - This would enable a viewer on any type of workstation (or WindowsCE machine) to connect to a server running one of the supported operating systems, so allowing remote control (or monitoring) of that server. The most common uses here would be for server control / monitoring from the support person's desk while at work, or when dialling into the server from home (the viewer software being run on a laptop, desktop or WindowsCE machine).
- **Workstation to Workstation (cross-platform)** - Because server and viewer software is also available for the Macintosh machines it is now possible to remotely run, for example, a non-Windows-compliant application on a Windows machine, so enabling a vast array of Macintosh software to effectively be "run" on Windows PCs (albeit a little slowly and with some obvious restrictions on functionality).
- **Thin Client** - As VNC is Thin Client software it is possible for an older, poorly-specified PC to connect to a better-specified "server" PC and remotely run software that would not have been possible on the lesser PC, either due to memory, hard drive or power restrictions. However, although it is possible to connect from multiple machines, all these machines will only be able to monitor / control the one Windows desktop - ie, VNC does not turn a server into a true multi-user server in the way that the Citrix products can. The X-based VNC server is more flexible in this respect.

Connection options - brings up options as displayed in Figure 3.

Connection info - displays host name, address, pixel size, etc.

Request Screen Refresh - refreshes the screen to alleviate any corruption.

Full Screen - utilises more of the screen; not necessary unless scrollbars have appeared due to the server screen size being larger than the current window size of the viewer.

Send CTL-ALT-DEL - send this key sequence for logging in purposes under NT, for example.

CTRL Down, CTRL Up, ALT Down, ALT Up - send these key sequences if required.

New connection - connects to another server (closes the existing session).

Save Connection Info As - saves the current connection data to a file.

Figure 4 - Options in the viewer.

`-shared` leaves open any existing server connections so the desktop can be "shared" with other users. For security reasons this is usually not possible, but this command overrides the default setting.

`-8bit` any colour depths are usually allowed, with translation to lower bits automatically carried out as required. This overrides the default, so making it useful for lower-speed lines (such as modem dial-ups).

`-emulate3` emulates three buttons on a two-button mouse (simultaneously clicking both buttons emulates the third).

`-fullscreen` causes the viewer to start in full-screen mode instead of windowed.

`-listen` with this set, the server can initiate connections to the viewer.

Figure 5 - Command-line startup options for the viewer.

security is naturally an important issue. This is well covered by VNC, with the flexibility to use third-party security in addition if required. Out of the box, VNC uses a random challenge-response system; this provides the basic authentication that allows a viewer to connect to a server, and the password is not sent over a network. However, once connected, all the traffic is unencrypted, so could be snooped with the right tools. VNC's documentation recommends that, if higher security is important, the VNC protocol is "tunnelled" via a more secure channel such as SSH (Secure SHell). SSH is easily and freely available in the Unix community, and Clients are available for Macs, Windows, etc. However, SSH servers for these platforms are only available commercially, and a cheaper alternative is to route the connection via a Unix machine. All this is outlined in the VNC documentation, along with pointers to various Web resources, including the SSH FAQ.

It recently transpired that a security hole has been found in Windows-based VNC server (3.3.3r7 or previous). From various Web discussions on this it looks as if it is fairly low risk, primarily because a registry key needs to first be created to enable the debug logging, plus the VNC Web server port needs to be open. More details can be found at **www.core-sdi.com/advisories/vnc_servebo_advisory.htm**, along with a listing of a patch and an ftp site where it can be downloaded.

Documentation

The provided documentation is good, but isn't particularly detailed. It is supplied as it is seen on the VNC Web site - ie, in HTML. A general overview and history of VNC is also available as a PDF document, but this hasn't apparently been updated since 1998. Don't let this put you off, though, as it is a good, informative read. Finally, the VNC publicity video is available to download; it runs for eight minutes and is available in RealPlayer format in varying sizes depending on the line speed (which accordingly affects the quality). See the Resources section below for information on where to find these videos.

Conclusion

VNC is a very impressive product, especially considering that it's free. Quite apart from that, its main advantage over its commercial competitors is that it is open source, so anyone with programming skills can contribute towards it and so make it an even better, more flexible product. Even in its current form, its remote control applications are almost limitless, and it will no doubt find many uses and supporters in a typical support environment. Definitely a program to try out and evaluate for yourself.

PCNA

Web Resources

Home pages
www.uk.research.att.com/vnc/index.html

Documentation
www.uk.research.att.com/vnc/docs.html

PDF document (different to the main documentation)
ftp://ftp.uk.research.att.com/pub/docs/att/tr.98.1.pdf

VNC Publicity Video
www.uk.research.att.com/vnc/videos.html

FAQ
www.uk.research.att.com/vnc/faq.html

Mailing Lists
www.uk.research.att.com/vnc/join.html

VNC Channel in IRC
www.chaosreigns.com/vnc_irc.html (channel #VNC)

Email the developers directly
vnc@uk.research.att.com