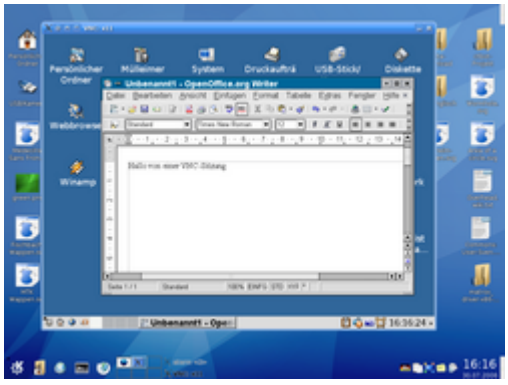
VNC

By Contributors to Wikimedia projects

Published: 2003-10-28 · Archived: 2026-04-06 00:45:44 UTC

From Wikipedia, the free encyclopedia

Virtual Network Computing logo



VNC in KDE 3.1

VNC (**Virtual Network Computing**) is a graphical desktop-sharing system that uses the Remote Frame Buffer (**RFB**) protocol to remotely control another computer. It transmits the keyboard and mouse input from one computer to another, relaying the graphical screen updates, over a network.[1] Popular uses for this technology include remote technical support and accessing files on one's work computer from one's home computer, or vice versa.

VNC is platform-independent, with clients and servers for many GUI-based operating systems and for Java. Multiple clients may connect to a VNC server at the same time. There are a number of variants of VNC[2] which offer their own particular functionality; e.g., some optimised for Microsoft Windows, or offering file transfer (not part of VNC proper), etc. Many are compatible (without their added features) with VNC proper in the sense that a viewer of one flavour can connect with a server of another; others are based on VNC code but not compatible with standard VNC.

VNC was originally developed at the Olivetti & Oracle Research Lab in Cambridge, United Kingdom, whose developers subsequently created RealVNC Ltd and claimed VNC and RFB as registered trademarks in the US and some other countries. The original VNC source code and many modern derivatives are open source under the GNU General Public License.

The Olivetti & Oracle Research Lab (ORL)[3] at Cambridge in the UK developed VNC at a time when Olivetti and Oracle Corporation owned the lab. Developers who worked on VNC while at the AT&T Research Lab include Tristan Richardson (inventor), Andy Harter (project leader), Quentin Stafford-Fraser, James Weatherall and Andy Hopper.[4] The name *Virtual Network Computer/Computing* (VNC) originated with ORL's work on a thin client called the Videotile, which also used the RFB protocol. The Videotile had an LCD with pen input and a fast ATM connection to the network. At the time, *network computer* was commonly used as a synonym for a thin client; VNC is essentially a software-only (i.e. virtual) network computer.[*citation needed*]

In 1999, AT&T acquired the lab, and in 2002 closed down the lab's research efforts. Following this, several members of the development team (including Richardson, Harter, Weatherall and Hopper) formed RealVNC in order to continue working on open-source and commercial VNC software under that name. As of 2013, RealVNC Ltd claims the term "VNC" as a registered trademark in the United States and in other countries.[5]

The original GPLed source code has fed into several other versions of VNC. Such forking has not led to compatibility problems because the RFB protocol is designed to be extensible. VNC clients and servers negotiate their capabilities with handshaking in order to use the most appropriate options supported at both ends.

Design and operation

[edit]

The VNC server is the program on the machine that shares some screen (and may not be related to a physical display: the server can be "headless"), and allows the client to share control of it. The VNC client (or viewer) is the program that presents the screen data originating from the server, receives updates from it, and presumably controls it by informing the server of collected local input. The VNC protocol (RFB protocol) is very simple, based on transmitting one graphic primitive from server to client ("Put a rectangle of pixel data at the specified X,Y position") and event messages from client to server.

In the normal method of operation a viewer connects to a port on the server (default port: 5900). Alternatively (depending on the implementation) a browser can connect to the server (default port: 5800). And a server can connect to a viewer in "listening mode" on port 5500. One advantage of listening mode is that the server site does not have to configure its firewall to allow access on port 5900 (or 5800); the duty is on the viewer, which is useful if the server site has no computer expertise and the viewer user is more knowledgeable.

The server sends small rectangles of the framebuffer to the client. In its simplest form, the VNC protocol can use a lot of bandwidth, so various methods have been devised to reduce the communication overhead. 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 they will use. The simplest encoding, supported by all clients and servers, is *raw encoding*, which sends pixel data in left-to-right scanline order, and after the

original full screen has been transmitted, transfers only rectangles that change. This encoding works very well if only a small portion of the screen changes from one frame to the next (as when a mouse pointer moves across a desktop, or when text is written at the cursor), but bandwidth demands get very high if a lot of pixels change at the same time (such as when scrolling a window or viewing full-screen video).

VNC by default uses TCP port 5900+*N*,[6][7] where *N* is the display number (usually :0 for a physical display). Several implementations also start a basic HTTP server on port 5800+*N* to provide a VNC viewer as a Java applet, allowing easy connection through any Java-enabled web-browser. Different port assignments can be used as long as both client and server are configured accordingly. A HTML5 VNC client implementation for modern browsers (no plugins required) exists too.[8]

Although possible even on low bandwidth, using VNC over the Internet is facilitated if the user has a broadband connection at both ends. However, it may require advanced network address translation (NAT), firewall and router configuration such as port forwarding in order for the connection to go through. Users may establish communication through virtual private network (VPN) technologies to ease usage over the Internet, or as a LAN connection if VPN is used as a proxy, or through a VNC repeater (useful in presence of a NAT).[9] [10]

In addition, the display that is served by VNC is not necessarily the same display seen by a user on the server. On Unix/Linux computers that support multiple simultaneous X11 sessions, VNC may be set to serve a particular existing X11 session, or to start one of its own. It is also possible to run multiple VNC sessions from the same computer. On Microsoft Windows the VNC session served is always the current user session.[*citation needed*]

In July 2014 RealVNC published a Wayland developer preview.[11][12]

By default, RFB is not a secure protocol. While passwords are not sent in plain-text (as in telnet), cracking could prove successful if both the encryption key and encoded password were sniffed from a network.[13] For this reason it is recommended that a password of at least 8 characters be used. On the other hand, there is also an 8-character limit on some versions of VNC;[14] if a password is sent exceeding 8 characters, the excess characters are removed and the truncated string is compared to the password.[15]

UltraVNC supports the use of an open-source encryption plugin which encrypts the entire VNC session including password authentication and data transfer.[16] It also allows authentication to be performed based on NTLM and Active Directory user accounts.[17] However, use of such encryption plugins makes it incompatible with other VNC programs. RealVNC offers high-strength AES encryption[18] as part of its commercial package, along with integration with Active Directory.[19] According to TightVNC, TightVNC is not secure as picture data is transmitted without encryption. To circumvent this, it should be tunneled through an SSH connection[20] (see below).

VNC may be tunneled over an SSH or VPN connection which would add an extra security layer with stronger encryption.[21]

An additional security concern for the use of VNC is to check whether the version used requires authorization from the remote computer owner before someone takes control of their device. This will avoid the situation where the owner of the computer accessed realizes there is someone in control of their device without previous notice.

Functionality for this security feature has been implemented into certain VNC servers, such as RealVNC, and UltraVNC.[17][22]

Xvnc is the Unix VNC server, which is based on a standard X server. To applications, Xvnc appears as an X "server" (i.e., it displays client windows), and to remote VNC users it is a VNC server. Applications can display themselves on Xvnc as if it were a normal X display, but they will appear on any connected VNC viewers rather than on a physical screen.[23] Alternatively, a machine (which may be a workstation or a network server) with screen, keyboard, and mouse can be set up to boot and run the VNC server as a service or daemon, then the screen, keyboard, and mouse can be removed and the machine stored in an out-of-the way location.

Users commonly deploy VNC as a cross-platform remote desktop system. For example, Apple Remote Desktop for Mac OS X (and "Back to My Mac" in versions 10.5 through 10.13) interoperates with VNC and will connect to a Unix user's current desktop if it is served with x11vnc, or to a separate X11 session if one is served with TightVNC. From Unix, TightVNC will connect to a Mac OS X session served by Apple Remote Desktop if the VNC option is enabled, or to a VNC server running on Microsoft Windows.[24]

Open source programs or libraries which implement VNC include: KRDC, Krfb, Libvncserver, Remmina, TigerVNC, TightVNC, TurboVNC, UltraVNC, Veyon, Vinagre, VirtualGL, x11vnc and xpra.

- RealVNC
- RFB (protocol)
- SPICE
- TigerVNC
- UltraVNC

1. ^ *Richardson, T.; Stafford-Fraser, Q.; Wood, K. R.; Hopper, A. (1998). "Virtual network computing" (PDF). IEEE Internet Computing. **2**: 33–38. CiteSeerX 10.1.1.17.5625. doi:10.1109/4236.656066.*
2. ^ *"The VNC family of Remote Control Applications: a list of VNC variants". Archived from the original on 7 December 2023. Retrieved 4 June 2009.*
3. ^ *"VNC Frequently Asked Questions (FAQ)". 1999. Archived from the original on 15 August 2000.*
4. ^ *"RealVNC Executive Profiles". Archived from the original on 15 May 2016. Retrieved 23 June 2011.*
5. ^ Copyright and trademarks RealVNC. Accessed Feb 23, 2018.
6. ^ *"Frequently asked questions".*
7. ^ *"UltraVnc Configuration". Archived from the original on 3 July 2011. Retrieved 19 April 2009.*
8. ^ *"noVNC". GitHub.*
9. ^ *"OpenWRT VNC repeater".*
10. ^ *"uVNC repeater". Archived from the original on 5 December 2023. Retrieved 11 April 2017.*
11. ^ *"VNC® Wayland Developer Preview". 8 July 2014. Archived from the original on 14 July 2014. Retrieved 10 July 2014.*
12. ^ *"RealVNC Wayland developer preview email". freedesktop.org. 9 July 2014.*
13. ^ *Richardson, Tristan; Levine, John R. (March 2011). The Remote Framebuffer Protocol (Report). Internet Engineering Task Force.*
14. ^ *"Remote Access with VNC [EECS Technical Database]". wiki.eecs.yorku.ca. Retrieved 6 July 2025.*
15. ^ *"vncpasswd". tigervnc.org. Retrieved 6 July 2025.*

16. ^ *"SecureVNC Plugin - UltraVNC VNC OFFICIAL SITE, Remote Desktop Free Opensource"*. *uvnc.com. Retrieved 6 July 2025.*
17. ^ Jump up to: **a** **b** *"UltraVNC Server Configuration - UltraVNC VNC OFFICIAL SITE, Remote Desktop Free Opensource"*. *uvnc.com. Retrieved 6 July 2025.*
18. ^ *"Setting up VNC Connect for Maximum Security"*. *RealVNC Help Center. 21 March 2024. Retrieved 6 July 2025.*
19. ^ *"Setting up Single sign-on Authentication"*. *RealVNC Help Center. 2 May 2024. Retrieved 6 July 2025.*
20. ^ How secure is TightVNC? TightVNC Frequently Asked Questions. TightVNC.com Accessed Feb 23, 2018
21. ^ *Wallen, Jack (17 January 2019). "How to connect to VNC using SSH". TechRepublic. Retrieved 6 July 2025.*
22. ^ *"Requiring Connection Approval From a Remote Computer Owner"*. *RealVNC Help Center. 31 May 2022. Retrieved 6 July 2025.*
23. ^ *AT&T Laboratories Cambridge (1999). "X-based VNC server". Virtual Network Computing. Archived from the original on 19 March 2007. Retrieved 24 March 2007.*
24. ^ *"OnlineVNC Server for Windows OSes"*.

Wikimedia Commons has media related to VNC.

- RFB 3.8 Protocol Standard
- AT&T VNC Archived 16 October 2008 at the Wayback Machine: Original AT&T-Cambridge VNC website

---

Source: https://en.wikipedia.org/wiki/Virtual_Network_Computing