En informática, Computación de red Virtual (VNC) es un sistema gráfico Compartir escritorio que utiliza el Protocolo RFB a control remoto de otro equipo. Transmite los eventos del teclado y el ratón de un ordenador a otro, retransmitir las actualizaciones de pantalla de gráficos en la otra dirección, en una red.

VNC es independiente de la plataforma, un visor VNC en un sistema operativo puede conectarse a un servidor VNC en el mismo o cualquier otro sistema operativo. Hay clientes y servidores para muchos sistemas operativos basados en GUI y Java. Varios clientes pueden conectarse a un servidor VNC al mismo tiempo. Populares usos de esta tecnología incluyen soporte técnico remoto y acceder a archivos en el equipo de trabajo desde el equipo de casa, o viceversa.

VNC fue desarrollado originalmente en el Laboratorio de investigación de Olivetti en Cambridge, Reino Unido. El original VNC código fuente y muchos derivados modernos son código abierto bajo la Licencia Pública General de GNU.

# VNC en KDE.

Hay una serie de variantes de VNC que ofrecen su propia función particular; por ejemplo, algunos optimizado para Microsoft Windows, ofrece transferencia de archivos (no forma parte de VNC adecuada), etc. Muchos son compatibles (sin sus características añadidas) con VNC correcta en el sentido de que un espectador de un sabor puede conectar con un servidor de otro; otros son basada en código VNC pero no compatible con VNC estándar.

VNC y RFB son marcas registradas de RealVNC Ltd. en Estados Unidos y en otros países.

# Historia

VNC fue creado en la Olivetti & Oracle Research Lab (ORL), que entonces era propiedad de Olivetti y Oracle Corporation. En 1999 de AT & t adquirió el laboratorio y en 2002 cerró los esfuerzos de investigación del laboratorio.

Los desarrolladores que han trabajado en VNC mientras todavía en el AT & T Research Lab:

Tristán Richardson (inventor)

Andy Harter (líder del proyecto)

Quentin Stafford-Fraser

James Weatherall

Tras el cierre de ORL en 2002, varios miembros del equipo de desarrollo (incluyendo Harter, Weatherall, Richardson y Hopper) forman RealVNC para seguir trabajando en código abierto y software comercial de VNC bajo ese nombre.

Se han desarrollado varias otras versiones de VNC desde el código fuente original de GPL. Tal duplicidad no ha conducido a problemas de compatibilidad porque el protocolo RFB está diseñado para ser extensible. Servidores y clientes VNC negocian sus capacidades cuando handshaking para utilizar las opciones más adecuadas compatibles en ambos extremos.

El término "VNC" ahora es una marca registrada de RealVNC Ltd. en los Estados Unidos y otros países.

# Etimología

El nombre de ' equipo de la red Virtual/Informática ' proviene del trabajo de ORL en un cliente ligero llamado el Videotile que también utiliza el Protocolo RFB. Esto fue esencialmente un LCD con un bolígrafo y una rápida conexión ATM a la red. Al tiempo, equipo de la red fue comúnmente utilizado como sinónimo de "cliente ligero". VNC es esencialmente una sólo software (es decir) versión virtual de este equipo de la red.

Operación

Un sistema VNC consta de un cliente, un servidor y un protocolo de comunicación.

El VNC server es el programa en el equipo que comparte su pantalla. El servidor permite pasivamente al cliente tomar el control de la misma.

El cliente VNC (o visor) es el programa que mira, controla e interactúa con el servidor. El cliente controla el servidor.

El Protocolo VNC (RFB) es muy simple, basado en una primitiva gráfica del servidor al cliente ("poner un rectángulo de datos de píxeles en el especificado X, posición Y") y mensajes de eventos desde el cliente al servidor.

En el modo normal de funcionamiento un visor se conecta a un puerto en el servidor (puerto 5900 predeterminado). Como alternativa un navegador puede conectarse al servidor (dependiendo de la aplicación) (por defecto el puerto 5800). Y un servidor puede conectarse a un visor en modo “escuchando" en el puerto 5500. Una ventaja del modo escucha es que el sitio del servidor no tiene que configurar el cortafuegos para permitir el acceso en el puerto 5900 (o 5800); la responsabilidad recae en el espectador, que es útil si el sitio del servidor sin experiencia en equipo, mientras que se espera que el usuario visor estar más informados.

El servidor envía pequeños rectángulos del framebuffer al cliente. En su forma más simple, el protocolo VNC puede utilizar una gran cantidad de ancho de banda, por lo que han ideado varios métodos para reducir la sobrecarga de comunicación. Por ejemplo, existen diversas codificaciones (métodos para determinar la manera más eficiente para transferir estos rectángulos). El protocolo VNC permite que el cliente y el servidor negociar Qué codificación se utilizará. La codificación más simple, que es apoyado por todos los clientes y servidores, es la codificación raw donde píxel se envían datos en orden de izquierda a derecha scanline , y después la pantalla completa original ha sido transmitida, sólo transfiere rectángulos que cambiar. Esta codificación funciona muy bien si sólo una pequeña porción de la pantalla cambia de un fotograma al siguiente (como un puntero de ratón mover en un escritorio, o se escribe en el cursor de texto), pero las demandas de ancho de banda llegar muy altas si un montón de píxeles cambia al mismo tiempo, como al desplazar una ventana o un video de pantalla completa de visualización.

VNC por defecto utiliza el puerto TCP 5900++N, donde n es el número de visualización (normalmente: 0 para una visualización física). Varias implementaciones también iniciar una básica HTTP del servidor en el puerto 5800++n para proporcionar un visor VNC como un applet de Java, que permite una conexión sencilla a través de cualquier navegador web habilitado para Java. Las asignaciones de puertos diferentes pueden utilizarse como cliente y servidor están configurados en consecuencia.

El uso de VNC por Internet funciona bien si el usuario tiene una conexión de banda ancha en ambos extremos. Sin embargo, requiera configuración avanzada de NAT, firewall y router como puerto de reenvío para la conexión a recorrer. Algunos usuarios pueden optar por utilizar instantáneas aplicaciones de redes privadas, como las aplicaciones de Red privada Virtual (VPN), como Hamachi hacer uso por Internet mucho más fácil. Alternativamente, se puede establecer una conexión VNC como una conexión LAN si VPN se utiliza como proxy.

Tenga en cuenta que el equipo del servidor VNC se ejecuta sobre no necesita tener una pantalla física. Xvnc es el servidor Unix VNC, que se basa en un estándar del servidor X. Para aplicaciones Xvnc es un "servidor X" (es decir muestra cliente Windows), y a los usuarios remotos de VNC es un servidor VNC. Aplicaciones pueden mostrar propios en Xvnc como si se tratara de una normal x pantalla, sino aparecerá en cualquier visores VNC conectados en lugar de en la pantalla física. También puede configurarse una máquina (que puede ser una estación de trabajo o un servidor de red) con pantalla, teclado y ratón para arrancar y ejecutar el servidor VNC como un servicio o daemon, entonces pueden eliminarse la pantalla, el teclado y el ratón y la máquina se almacena en una ubicación fuera de la forma.

Además, la pantalla que se sirve por VNC no es necesariamente la misma pantalla vista por un usuario en el servidor. En los equipos Unix/Linux que soportan múltiples simultáneas X 11 sesiones, VNC puede establecerse para servir a un particular existentes X 11 sesión, o para iniciar uno de los suyos. También es posible ejecutar múltiples sesiones VNC desde el mismo equipo. En Microsoft Windows el VNC sesión sirvió es siempre la sesión del usuario actual.

VNC es comúnmente usado como un sistema de escritorio remoto multiplataforma. Por ejemplo, Apple Remote Desktop para Mac OS X (y más recientemente, "volver a mi Mac" en 'Leopardo' - Mac OS X 10.5) interopera con VNC y se conectará al escritorio actual del usuario de Linux si se sirve con x11vnc, o a un independiente 11 X sesión si uno es servido con TightVNC. En Linux, TightVNC se conectará a una sesión de Mac OS X servida por Apple Remote Desktop si está habilitada la opción de VNC o a un servidor VNC que se ejecuta en Microsoft Windows.

Seguridad

De forma predeterminada, VNC no es un protocolo seguro. Aunque las contraseñas no se envían en texto sin formato (como en telnet), agrietamiento puede resultar exitosa si la clave de cifrado y codificación de contraseña son inhalados desde una red. Por esta razón se recomienda que se utilice una contraseña de al menos 8 caracteres. Por otro lado, también hay un límite de 8 caracteres en algunas versiones de VNC; Si una contraseña se envía como superior a 8 caracteres, se eliminan los caracteres exceso y se compara la cadena truncada con la contraseña.

Sin embargo, VNC puede ser entubado en una conexión SSH o VPN que añadir una capa de seguridad adicional con cifrado más fuerte. SSH clientes están disponibles para todas las plataformas principales (y muchas plataformas de menores); SSH túneles se pueden crear desde UNIX clientes, Microsoft Windows clientes, clientes de Macintosh (incluyendo Mac OS X y sistema 7 y hasta) – y muchos otros. Hay aplicaciones de freeware que creación instantáneas túneles VPN entre equipos.

UltraVNC es compatible con el uso de un plugin de cifrado de código abierto que cifra toda la sesión VNC, incluida la transferencia de datos y autenticación de contraseña. También permite autenticación a realizarse basándose en las cuentas de usuario NTLM y Active Directory. Sin embargo, el uso de estos plugins de cifrado hacer incompatibles con otros programas VNC. RealVNC ofrece un cifrado de alta resistencia como parte de su paquete comercial. Workspot publicado parches de cifrado AES VNC.

Limitaciones

Unicode no se admite en VNC versiones 3.x y menor, por lo que es imposible transferir texto del Portapapeles fuera del conjunto de caracteres Latin-1.

El protocolo VNC es base de píxel. Aunque esto lleva a la gran flexibilidad (es decir,-puede mostrarse cualquier tipo de escritorio), a menudo es menos eficaz que las soluciones que tengan una mejor comprensión del diseño gráfico subyacente como X 11 o Protocolo de escritorio remoto de Windows. Estos protocolos envían primitivas gráficas o comandos de alto niveles en una forma más simple (por ejemplo, "ventana abierta"), Considerando que RFB sólo envía los datos de píxel crudo.