Ethereal and VNC

Table of Contents

Ethereal

What is Ethereal?

Every network manager at some time or other needs a tool that can capture packets off the network and analyze them. In the past, such tools were either very expensive, propietary, or both. However, with the advent of Ethereal, all that has changed.

Ethereal is perhaps one the best open source packet sniffers available today.

Platforms Ethereal runs on

Ethereal currently runs on most UNIX platforms and the various Windows platforms. It requires GTK+, GLIB and libpcap in order to run.

Where to get Ethereal

You can get the latest copy of the Ethereal from the Ethereal Website: http://www.ethereal.com. The website allows you to choose from among several mirrors for downloading.

Obtaining the source and binary distributions

You can obtain both source and binary distributions from the Ethereal web site: http://www.ethereal.com. Simply select the download link, and then select either the source package or binary package of your choice from the mirror site closest to you.

Installing Ethereal under Windows

In this section we explore installing Ethereal under Windows from the binary packages. You must follow two steps:

1. Install WinPcap. There are instructions at the WinPcap web site for installing it under Windows 9X, Windows NT and Windows 2000. These are located at: http://netgroup-serv.polito.it/winpcap/install/Default.htm.

2. Install Ethereal. You may acquire a binary installable of Ethereal at http://www.ethereal.com/download.html#binaries. Download the installer (after installing WinPcap) and execute it.

Starting Ethereal

You can start Ethereal from the command line under UNIX, but it can also be started from most Window managers as well.

Ethereal is comprised of three main windows, or panes.

1. The top pane is the packet list pane. It displays a summary of each packet captured. By clicking on packets in this pane your control what is displayed in the other two panes.

2. The middle pane is the tree view pane. It displays the packet selected in the top pane in more detail.

3. The bottom pane is the data view pane. It displays the data from the packet selected in the top pane, and highlights the field selected in the tree view pane.

In addition to the three main panes, there are four elements of interest on the bottom of the Ethereal main window.

A. The lower leftmost button labeled "Filter:" can be clicked to bring up the filter construction dialog.

B. The left middle text box provides an area to enter or edit filter strings. This is also where the current filter in effect it displayed. You can click on the pull down arrow to select past filter string from a list.

C. The right middle button labeled "Reset" clears the current filter.

D. The right text box displays informational messages. These message may indicate whether or not you are capturing, what file you have read into the packet list pane if you are not capturing. If you have selected a protocol field from the tree view pane and it is possible to filter on that field then the filter label for that protocol field will be displayed.

The Ethereal menus

The Ethereal menu sits across the top of the Ethereal window.

It contains the following items:

File

> This menu contains menu-items to open and reread capture files, save capture files, print capture files, print packets, and to quit from Ethereal.

Edit

> This menu contains menu-items to find a frame and goto a frame,mark one or more frames, set your preferences, create filters, and enable or disable the dissection of protocols (cut, copy, and paste are not presently implemented).

Capture

> This menu allows you to start and stop captures.

Display

> This menu contains menu-items to modify display options, match selected frames, colorize frames, expand all frames, collapse all frames, show a packet in a separate window, and configure user specified decodes.

Tools

> This menu contains menu-items to display loaded plugins, follow a TCP stream, obtain a summary of the packets that have been captured, and display protocol hierarchy statistics.

Help

> This menu contains the About Ethereal... menu item and access to some basic Help.

Ethereal preferences

There are a number of preferences you can set from one place. Simply select the Preferences... menu item from the Edit menu, and Ethereal will pop up the Preferences dialog box.

The Ethereal Preferences dialog box is a tabbed dialog box that allows you to set preferences for each of the following elements:

Printing

> This tab allows you to define the default printing command that Ethereal will use as well as the default output file name when you print to a file.

Columns

> This tab allows you to select which columns appear in the Packet List Pane.

TCP Streams

> This tab allows you to change the foreground and background colors used by the **Follow TCP Stream**.

GUI

> This tab allows you to configure various characteristics of the GUI.

Other tabs

> The remaining tabs allow you to configure various preferences for the dissection of various network protocols.

Files used by Ethereal

Ethereal uses a number of files while it is running. Some of these reside in $HOME/.ethereal and are used to maintain information between runs of Ethereal, while some of them are maintained in system areas.

The following are some of the files accessed by Ethereal:

$HOME/.ethereal/preferences

> This file contains all your Ethereal preferences, including defaults for capturing and displaying packets. It is a simple text file containing statements of the form **variable: value**.

$HOME/.ethereal/filters

> This file contains all the filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
"<filter name>" <filter string>
```

$HOME/.ethereal/colorfilters

This file contains all the color filters that you have defined and saved. It consists of one or more lines, where each line has the following format:

```
@<filter name>@<filter string>@[<bg RGB(16-bit)>][<fg RGB(16-bit)>]
```

/usr/share/ethereal/plugins, /usr/local/share/ethereals/plugins, $HOME/.ethereal/plugins

Ethereal searches for plugins in the directories listed above. They are searched in the order listed.

/etc/ethers, $HOME/.ethereal/ethers

When Ethereal is trying to translate Ethernet hardware addresses to names, it consunts the files listed above in the order listed. If an address is not found in /etc/ethers, Etherereal looks in $HOME/.ethereal/etheres

Each line in these files consists of one hardware address and name separated by whitespace. The digits of hardware addressses are spearated by colons (:), dashes (-) or periods(.). The following are some examples:

```
ff-ff-ff-ff-ff-ff    Broadcast

c0-00-ff-ff-ff-ff    TR_broadcast

00.2b.08.93.4b.a1    Freds_machine
```

/usr/local/etc/manuf

Ethereal uses the file listed above to translate the first three bytes of an Ethernet address into a manufacturers name. This file has the same format as the ethers file, except addresses are three bytes long.

$HOME/.ethereal/ipxnets

Ethereal uses the above file to translate IPX network numbers into names.

An example is:

```
C0.A8.2C.00    HR

c0-a8-1c-00    CEO

00:00:BE:EF    IT_Server1

110f           FileServer3
```

The Ethereal section above is comprised of unmodified excerpts from **Ethereal User's Guide: V1.1 for Ethereal 0.9.7** to which the following license applies.

The GNU Free Document Public License

Copyright

Version 1.1, March 2000

Copyright (C) 2000 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

TightVNC

VNC (Virtual Network Computing) is a client/server software package allowing remote network access to graphical desktops. With VNC, you can access your Internet-connected machine from anywhere. VNC is free (released under the GNU General Public License) and available on most platforms.

An enhanced version of VNC, TightVNC, contains new features, improvements, optimizations and bugfixes. TightVNC is compatible with standard VNC.

TightVNC is used to perform remote control and administration tasks in Windows, Unix and mixed network environments. It is helpful in distance learning and remote customer support.

The following are instructions on installation, remote upgrade, running the server and viewer, and uninstalling.

Installation

TightVNC is available in the self-installing form, starting from its 1.2.1 release. Run the executable to install. The installation wizard will allow you to choose an installation directory and a name for the TightVNC group under the **Start->Programs** menu. By default, TightVNC installs into the Program Files\TightVNC directory, but you may choose any other location during installation.

Upgrading Remotely

TightVNC servers can be upgraded remotely, starting from its 1.2.5 version, meaning that the TightVNC installation can be performed in an active TightVNC session. You cannot replace the executable files in place while the TightVNC service is running, so the installer will copy the new files to a temporary location, and these new files will replace the older versions during the next reboot. The installer prompts for reboot if unable to replace the executables.

Reboot the computer before using this feature. If you want to access your computer after the reboot, run WinVNC as a service, not in the application mode.

Note: There is no warranty of absolute reliability of the remote upgrade procedure. Close all running applications (besides the WinVNC service) before launching the TightVNC installer to minimize risks.

Running the Server and Viewer

Like normal VNC, TightVNC is comprised of the server (WinVNC), which shares the screen of the machine on which it's running, and the viewer, which shows the remote screen received from the server. To get started, run a server on the machine to be accessed remotely and connect to it with a viewer. TightVNC Win32 distribution includes both the server and viewer parts.

Running a Server (WinVNC)

WinVNC can run in the application mode and as a Windows service. In the application mode, the server runs only during the current user session and closes on logout. To start WinVNC in the application mode, choose **Start ->Programs->TightVNC->Launch TightVNC Server**.

Right-click the tray icon to bring up a menu with the following options.

- **Properties** - displays the Properties dialog, allowing the user to change WinVNC parameters.
- **Add New Client** - allows outgoing connections from the server to any viewer started in "listening" mode.
- **Kill All Clients** - disconnects all currently connected clients from the server.
- **Disable New Clients** - disables new client connection to the server.
- **About WinVNC** - shows the "About..." box.
- **Close** – shuts down the server.

Running a Viewer

To view and control a remote desktop on which a TightVNC server is running, run the TightVNC viewer.

Choose one of the following under **Start->Programs->TightVNC**:

- **TightVNC Viewer** - for a slow network connection to the server (best compression)
- **TightVNC Viewer** - for high-speed networks (fast compression)
- **TightVNC Viewer** - starts the viewer in Listen Mode.

After starting the viewer, enter the host name and optional display number of the remote server you want to access at the prompt.

Note: The TightVNC server displays the IP address as the mouse passes over its tray icon.

Uninstalling

Uninstall TightVNC using Add/Remove Programs under Control Panel. You may also remove the directory into which you have installed it (e.g. C:\Program Files\TightVNC).

Note: The TightVNC installation program does not copy files into the system directory. Before uninstalling, check that WinVNC is not running and not installed as a service.

Reference: http://www.tightvnc.com/winst.html