Wireshark

Version: 3514

Table of Contents

Wireshark

Wireshark is the world's foremost network protocol analyzer. This additional service also includes TShark which from the command line lets you capture packet data from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file. To install the Wireshark add-on package use the following procedure.

- Ensure a DNS server is configured and the router has access to the Internet.
- Ensure you are running the latest version of the ImageStream Linux 4.4 or 5.0 OS. If you are running 4.4, update your router software to the latest distribution by typing the following command from the command line:

```
update 4.4.0
```

- When the update is finished, reboot the router.
- When the router is booted, follow the procedures to enable the addon_hd feature (add-on hard drive) appropriate for your router (See "Setting up the add-on hard drive service" - Setup) if this has not already been done.
- Drop to a bash shell command line (3. Advanced, 1. Bash shell).

- Run the Wireshark installation script (/usr/share/init.d/wireshark install).

```
# /usr/share/init.d/wireshark install
Add-on hard drive service is running.
  Mounting add-on program partition read-write...  done.
Downloading software... done.
Installing software... done.
Cleaning up... done.
  Mounting add-on program partition read-only...  done.
Configuration saved to flash
```

- Start Wireshark (can also be done from the menus: 1. Configuration, 9. Add-on package configuration, 6. Wireshark, 3. Start the Wireshark service).

```
# Start wireshark
Starting the Wireshark service...Stopping ssh...done.
Starting ssh...done.
done.
```

- Enable the Wireshark service on boot (can also be done from the menus: 1. Configuration, 9. Add-on package configuration, 6. Wireshark, 1. Enable the Wireshark service on boot).

```
# Enable wireshark
wireshark enabled on boot.
```

- Confirm tshark runs from the command line.

```
# tshark -v
TShark 1.0.0
Copyright 1998-2008 Gerald Combs <gerald@wireshark.org> and contributors.
```

```
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
Compiled with GLib 2.16.3, with libpcap 0.9.5, with libz 1.2.3, without POSIX
capabilities, without libpcre, without SMI, without ADNS, without Lua, without
GnuTLS, without Gcrypt, without Kerberos.
NOTE: this build doesn't support the "matches" operator for Wireshark filter
syntax.
Running on Linux 2.6.23.9-rc1a, with libpcap version 0.9.5.
Built using gcc 3.3.4.
```

A tshark command line for the RTP streams analysis we use:

```
tshark -i eth0 -a duration:600 -q -p -o rtp.heuristic_rtp:TRUE -z rtp,streams -f udp
```

In this example eth0 is the interface being monitored. Other params are:

-a duration:600 - stop and produce report after 10 minutes -q - don't print one line synopsis of each packet -p - don't bother enabling promiscuous mode on the interface -o rtp.heuristic_rtp:TRUE - ignore broken streams (caused by start/stop cap in middle of stream) -z rtp,streams - when capture complete, run the rtp streams analysis and output results -f udp - only process udp packets to reduce tmp file size

During and after this command is run, a file exists called /tmp/etherXXXX(random) that is equivalent to doing a tshark -w file or tcpdump -w file. The file must be manually deleted after tshark returns to avoid filling the disk.