

Working With Wireshark



The Problem

It is vital that your network operate as efficiently and smoothly as possible. But in such a complex environment, knowing what is going on is no easy task. After all, there is a lot to keep you up at night...hardware malfunctions, software bugs, user errors, network attacks, viruses, spyware...all these things can put a real crimp in your network performance. Having a big picture view of your network operation makes it much easier to notice something out of whack. You can spot trends, identify anomalies, and plan for the future. In this game, knowledge really is power.

A key tool for getting to know your network is the protocol analyzer. A protocol analyzer decodes and displays information about packets traversing your network.

One of the foremost protocol analyzers in use today is Wireshark, formerly Ethereal, (www.wireshark.org). Wireshark is an open source project licensed under the GNU General Public License, and is well-known for its robust features and capabilities. Wireshark is very good at decoding and displaying network traffic data.

Unfortunately, Wireshark's effectiveness as a troubleshooting tool is dependent on your ability to select the proper network traffic sample to analyze, assuming you have been lucky enough to see the data live, or preserve the traffic you need. This can be a daunting task on a busy network. If you miss the packet "needle" in the network "haystack", it's gone forever.

The Solution

Solera Networks improves the Wireshark solution through its DS series of deep packet capture and stream-to-storage appliances. Solera DS appliances function as network traffic recorders, capturing and storing all network data—every single packet—through a passive network connection. Solera DS appliance features include the following:

- Performs complete packet capture, including both packet header and payload
- Connects passively to the network and has no effect on live network traffic
- Supports sustained capture rates up to an astounding 10 Gbps
- Provides onboard storage capacity of up to 16TB per appliance and virtually unlimited storage capacity with external SAN connectivity
- Filters and throttles playback as needed for your particular analysis

Solera Networks DS appliances deliver a historical network record you can really dig into. No constraints, no time limits, and no lost data. Your DS appliances can save the traffic you need even before you know there is a problem. The network data is there when you need it.

The following is just some of what Wireshark can do:

- Recognizes hundreds of protocols
- Performs live capture and offline analysis
- Browses captured traffic via GUI, or the TTY-mode TShark utility
- Offers powerful display filters
- Provides comprehensive VoIP analysis
- Supports multiple capture file formats, including libpcap, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer®, and NetXray®
- Reads data from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI.
- Supports decryption for several protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Exports packet information to XML, Post Script®, CSV, or plain text

For more information about Wireshark, visit www.wireshark.org.

Working with Wireshark – Procedure at a glance



The DS appliance lets you deliver captured network traffic to Wireshark in two different ways: write the traffic out to a Snapshot file (in standard PCAP format), or regenerate (replay) the network traffic directly to Wireshark. Either way, you can finally study historical network traffic in context, dissect events, understand root causes, and plan improvements.

Use the DS appliance's Web Console to create a Snapshot file or setup traffic regeneration. For detailed instructions, see the Web Console User Guide.

1. Connect the DS Appliance to Your Network and Start Recording Traffic Connect to the network through either a network tap or switched port analyzer (SPAN). The Web console Record page lists all available Ethernet ports. Click the Record button next to the active port from which you want to capture traffic. This is the Capture Interface.

2. Review Packet Filters The DS appliance lets you create filters to restrict the type and volume of network data it captures. Review filters carefully to make sure no previously defined filter prevents you from capturing the desired data.

3. Configure Captured Traffic Playback To create a Snapshot file: Open the Web Console Playback page and select the PCAP tab. Select the Capture Interface as the Snapshot file source interface, then specify a starting time and either an ending time or a file size for the Snapshot. If desired, you can apply a filter to the network traffic captured by the Snapshot file.

To regenerate captured traffic: Connect a separate Ethernet port on the DS appliance to the network segment on which you want to replay the network traffic. Open the Web console Playback page and assign the Capture Interface to a virtual interface, then use the Web console's Regeneration page to link the virtual interface to the Regeneration Interface.

4. Analyze Captured Traffic with Wireshark Analyze a Snapshot file: Open the Web Console Playback page and select the PCAP tab. Click the Download button to save the Snapshot file to a location of your choosing. Launch Wireshark and open the Snapshot file to analyze its contents.

Analyze regenerated traffic: Connect Wireshark to the Regeneration Interface. As the DS appliance regenerates the traffic, Wireshark sees the traffic as live data that you can analyze as needed.

5. Analyze Regenerated Traffic Connect your monitoring and analysis tools to the regeneration interface. Now you can view, test, and analyze the regenerated network traffic and the connected tools and systems can't distinguish the regenerated network traffic from live data.

Conclusion

The complexity of today's network environments makes tools like Wireshark critical to maintaining network performance and limiting exposure to internal and external threats. Solera Networks deep packet capture and stream-to-storage appliances remove obstacles and boundaries associated with using only a small sample of data with the Wireshark protocol analyzer, so you can better utilize it to understand your network's big picture.

For more information about solutions from Solera Networks, visit: www.soleranetworks.com/solutions

© 2008 Solera Networks. All rights reserved. Solera Networks, Solera DS Series, DeepSee, Solera V2P Tap, DS 1150, DS 3150, DS 5150, and See everything. Know everything. are registered trademarks of Solera Networks. All other company names, brand names and product names are the property and/or trademarks of their respective companies.

Contact Solera Networks

Solera Networks Headquarters

355 South 520 West, Suite 225
Lindon, Utah 84042
1 877-5SOLERA (877-576-5372)
1+ 801-623-5705 • 1+ 801-623-5706 fax
Email: info@soleranetworks.com

Solera Networks Japan, Inc.

Shinjuku Park Tower N30F
3-7-1, Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-1030
1+ 81-3-5326-3367 • 1+ 81-3-5326-3001 fax
Email: info@soleranetworks.co.jp



See everything. Know everything.™