

# Regenerating Network Traffic



## Solera Networks—See everything. Know everything.

Today's complex network infrastructure is ripe for trouble: Network components overload or malfunction; crackers exploit hardware and software weaknesses to attack your network; network users expose organizations to security and liability risks. Unless you've got a bottomless IT budget, you need a way to manage the flood without breaking the bank.

Fortunately, there are a lot of tools out there that monitor, analyze, and warn you about what's happening on your network. Unfortunately, the effectiveness of all of these tools is dependent on their ability to keep up with the volume of network traffic, and your ability to respond to their warnings. As traffic increases, alerts, log entries, and reports can pile up. Worse still, most monitoring and analysis tools cannot capture every aspect of your network environment when a problem occurs, limiting your ability to study root causes, look for trends, and effectively plan for network updates and security.

## The Solera Networks Solution

Solera Networks addresses these deficiencies 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.

The DS appliance also gives you the ability to regenerate, or replay, network traffic almost instantaneously so you can effectively dissect network events, understand their root causes, and plan improvements. A Solera DS appliance lets you use your monitoring and analysis tools more effectively by directing the appropriate network data to each tool. You can recreate network traffic flow for any purpose, and ensure that all data related to a given event is available.

For example, sophisticated network crackers “test” your network security by attacking at different times and in different ways, and once they get in, they often siphon data off slowly instead of trying to grab everything at once. Viewed separately, these individual events might be dismissed, but recreating the complete network flow that contains these events allows you to analyze them more closely, and develop an effective response to the attack.

Major features of Solera DS series appliances include the following:

- Connects passively to the network connection and has no effect on live network traffic
- Performs complete packet capture, including both packet header and payload
- Supports sustained capture rates up to an astounding 10 Gbps
- Nearly infinite data storage capacity through both onboard drives, and iSCSI/fibre channel SAN options
- Immediate or delayed playback to one or more virtual network interfaces
- Throttle playback to stream packets at a speed appropriate to your needs

A few of the network monitoring tools available to you include:

- **Protocol Analyzer:** Protocol analyzers, or sniffers, let you monitor and dissect traffic to see exactly what is happening on your network.
- **Intrusion Detection:** Monitors your network for attacks and break-ins.
- **HTTP and Communications Monitoring:** Tracks specific network communications such as HTTP, Instant Messaging, and Email.
- **Operating System Detection:** Identifies and tracks all systems that connect, or attempt to connect, to your network.

For information about specific third-party applications that work with Solera Networks DS appliances, see [www.soleranetworks.com/solutions/apps](http://www.soleranetworks.com/solutions/apps).

## Configuring Network Traffic Regeneration – Procedure at a glance

Installing and configuring a Solera DS appliance is relatively simple. You can have a DS appliance installed and capturing network traffic in less than 30 minutes.

The configuration process utilizes a Web Console for easy administration. The process of configuring the DS appliance for traffic regeneration involves the following general steps. For detailed instructions, see the Solera Installation and User Guide.

**1. Connect the DS Appliance to your network** Solera DS appliances provide multiple Ethernet ports that you can use to connect to your network. You can connect to multiple networks simultaneously, if desired. Use copper or SR fiber cables to connect to the network through either a network tap or switched port analyzer (SPAN). SPAN ports must first be configured to mirror packets from other selected ports of the network router or switch.

**2. Start Recording Network Traffic** The web console Record page lists all available Ethernet ports. Simply click the Record button next to the active port through which you want to capture traffic. This is the Capture Interface.

**3. Review Packet Filters** Solera DS appliances let you create filters to restrict the type and volume of network data captured on each interface. Review filters carefully to make sure that no previously defined filter prevents you from capturing the desired data.

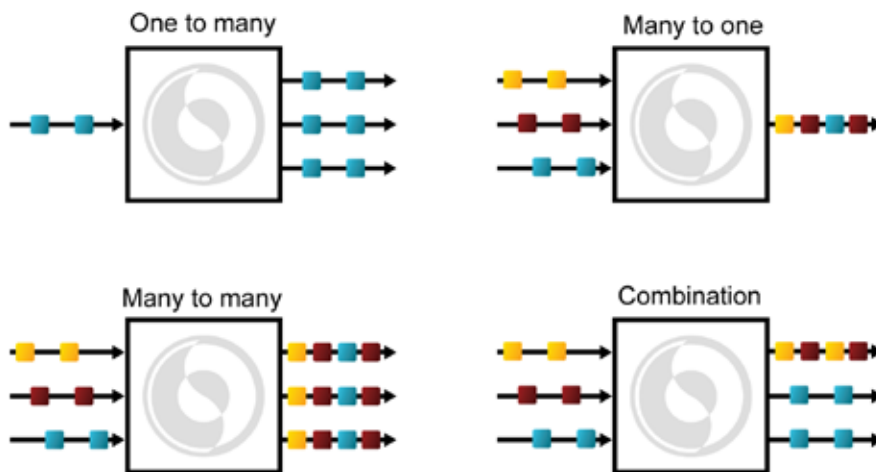
**4. Start Regenerating Captured Traffic** The Playback page lets you configure data playback. Simply assign the capture interface to a virtual port; use IFP ports for general network traffic, and IFT ports for time-sensitive traffic such as VoIP. You can even select to review packets from a specific period of time.

Once you have verified the virtual interface mapping, use the Regeneration page to select the virtual interface and a corresponding Ethernet port to act as the regeneration interface. You can also specify a specific data transmission speed, if necessary. Click Start to begin regenerating network traffic.

**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 traffic monitoring and analysis critical to maintaining network performance and limiting exposure to internal and external threats. Solera Networks deep packet capture and stream-to-storage appliances let you regenerate network traffic at will so you can study network events and trends in their original context, without affecting the performance or operation of your live network.



© 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](mailto: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](mailto:info@soleranetworks.co.jp)



See everything. Know everything.™