FLUKE networks

OptiView™ Console SwitchTap™

Background

Switch technology is everywhere. The price of switches has steadily dropped over the past few years, making switched links to the desktop a possibility for companies all over the world. Although switching provides considerable bandwidth to the end user, it has made troubleshooting and monitoring increasingly difficult. This is true even for dedicated monitoring devices, and especially protocol analyzers.

Switch operation

The topology of the network changes every time a device is inserted or removed. Switches keep up with these changes by updating their internal switch forwarding tables. These store information about all of the devices the switch knows about. After a switch learns the MAC (Media Access Control) address for a device (or host) attached to any of its ports, it forwards traffic addressed to a particular device directly to the corresponding port. Other ports and other devices, including analyzers, do not see this traffic. If a switch has not learned what to do with a particular address, it will forward that traffic to all the ports. Broadcast frames are also forwarded to all ports. Multicast frames are forwarded to one or many ports depending on the multicast address. Because of these rules, a device that is attached to a particular switch port will only receive:

- Broadcast frames.
- Multicast frames the host is supposed to receive.
- Unicast frames addressed to that host.
- Frames with a destination address that is currently unknown to the switch.

The limited amount of traffic, if any, forwarded to a passive monitoring device or analyzer would not be very useful.

Enter mirroring

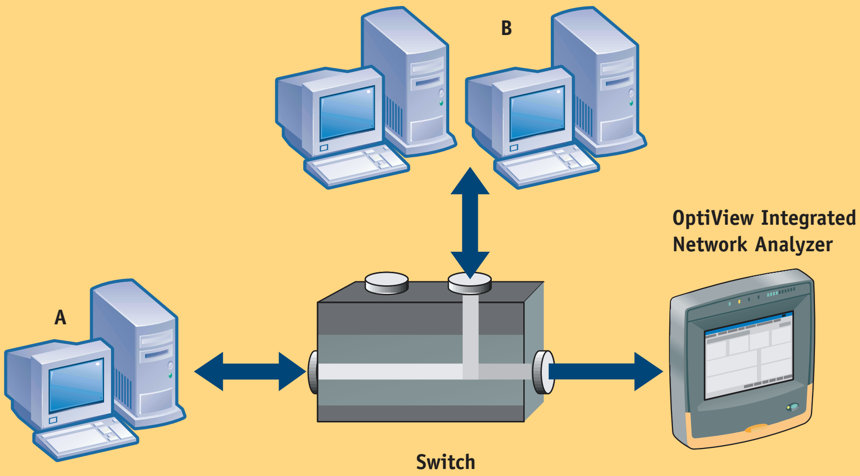
Most switch manufacturers recognized this issue and built a diagnostic feature into their switches. This feature is known as mirroring or Spanning (Switch Port Analyzer). Mirroring is when a switch port is configured to see the traffic of another port(s) on the same switch. The switch does this by copying frames to the mirror port.

In **Figure 1**, the OptiView™ analyzer is connected to a port that is configured to receive the frames that are sent to or from the port that has host A attached. The OptiView can now capture the traffic between hosts A and B. The port OptiView is attached to is the mirror port. Hosts A and B are both unaffected by the mirror port.

Mirroring can also be done with VLANs instead of individual ports. Typically, a mirror configuration is done by either Telneting to the switch or by using the switch's RS232 console port. A useful feature of port mirroring is that an analyzer, such as the OptiView™ Workgroup Analyzer or OptiView Integrated Network Analyzer, can be connected to a port that is configured as a mirror port. When there is a need to monitor or troubleshoot the network, a network engineer can remotely configure a mirror session and remotely monitor or troubleshoot the problem. Nobody has to be physically present and no cabling has to be changed or added.

As powerful as port mirroring is, it should be used with caution. Incorrectly mirroring a port can create loops in the network architecture, flood users with unwanted traffic, or make devices unreachable. This can result in unintentional but negative consequences.

Figure 1



Limitations to mirroring/spanning

One factor to consider when using a diagnostic tool, such as the Fluke Networks OptiView, on a mirror port is that it may not be able to access the network. The rules and limitations governing mirror port configuration vary among switch vendors and models. Depending on the switch, a mirror port can be configured as “receive-only” or “receive/transmit.” If the mirror port is “receive-only,” then OptiView will be unable to fully discover the network because it cannot use any of its active discovery techniques. This will hinder its effectiveness when troubleshooting. If the OptiView is unable to answer queries, the OptiView Remote User Interface will not work. A user might be able to transmit to the OptiView, but he would not be able to receive a response back from the analyzer.

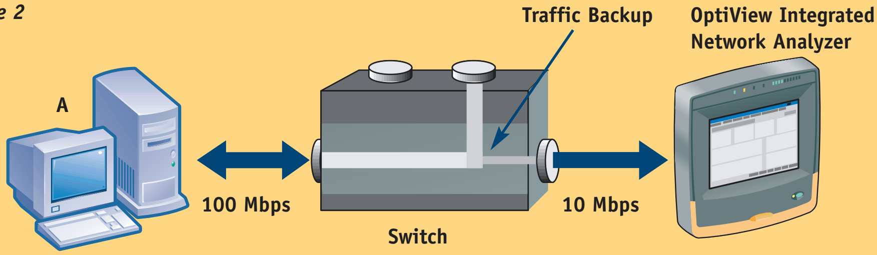
Another factor to consider with mirroring is the speed of the mirror port. The port speed must be fast enough to keep up with all traffic coming from the source port(s). For example, if host A is on a heavily utilized 100 Mbps link and the OptiView is on a 10 Mbps link, the capacity of the 10 Mbps port may by exceeded and frames destined for the analyzer are dropped (see Figure 2).

Somewhat less obvious, but just as important, is that if the mirrored traffic comes from a 100 Mbps full-duplex link, the aggregate amount of traffic can theoretically reach 200 Mbps. Since full duplex allows traffic to flow simultaneously in both directions, it effectively doubles the available network bandwidth. Each of the paths (the TX and RX connections) can carry 100 Mbps of traffic. If the aggregate amount of traffic exceeds 100 Mbps, the switch will again drop all excess traffic going to the mirror port without providing any indication that traffic was dropped. Therefore, it is critical that all mirrored traffic “fit” into a single 100 Mbps mirror port transmit path.

In situations where mirroring a port is used for troubleshooting slow links, it is important to remember the forwarding operation of the switch. Most switches perform store-and-forward switching at wire speed as the default state. This forwarding method performs full error checking on a frame before sending it on its way, so collisions and errors are not propagated onto other segments.

Under normal operation, traffic forwarded from the source port(s) will also be sent to the mirror port. This causes troubleshooting to be a bit difficult. If a segment is slow because of excessive collisions or errors, copying “all” traffic from that segment to a mirror port probably will not include these bad frames – unless the switch is using a low-latency forwarding technique and the error occurred after the forwarding decision was made. Some vendors no longer offer low-latency forwarding on their products, making it impossible to detect the collisions and errors with OptiView without introducing a hub on the suspected segment. When using a mirror function on a switch for testing and monitoring, it is important to know the actual forwarding technique being employed by the switch. One place to get this information is to review the switch documentation.

Figure 2



SwitchTap

SwitchTap reduces the time and effort required to safely configure port mirroring on supported LAN switches. Integrated with the OptiView Console application, SwitchTap provides an intelligent user interface approach to show where devices are connected. Discovered devices can be searched and selected by device type (e.g. “Routers” or “Servers”) or by the discovered device name or IP address. With SwitchTap, individual ports or even entire VLANs can be mirrored to the analyzer. Safety features, such as automatic analyzer port discovery and spotting potentially troublesome configurations, are built in.

SwitchTap supports the following switches:

Cisco

Catalyst 2900
Catalyst 2900XL
Catalyst 3500XL
Catalyst 5000
Catalyst 5505
Catalyst 6000
Catalyst 6009
Catalyst 6509
Catalyst 2926
Catalyst 2900MXL
Catalyst 5000
Catalyst 5502
Catalyst 5509
Catalyst 6006
Catalyst 6506

Extreme*

Extreme Summit
Extreme Black Diamond**
Extreme Alpine

Nortel

BayStack 450

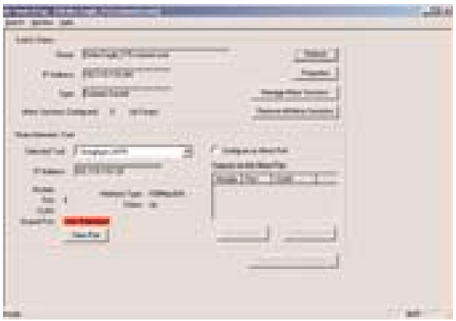
***Note**: If you select a switch that is not supported by the application, you will see the message “Unsupported Switch” in the Type field of the Switch Status window. Use the Select Switch feature to pick a different switch.*

* *For Extreme switches, you should always use the same PC you used to configure a mirror session to also remove that session. If you use a different PC to remove the mirror session, the switch must be reset in order to regain use of the port. If you find it necessary to remove a mirror session from a different PC, you can use Telnet or the Web browser to reconfigure the switch port, or you can cycle power on the switch to restore the previous configuration.*

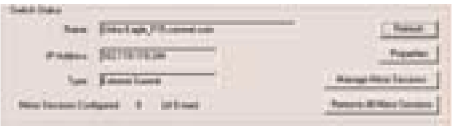
** *If VLANs are configured on the Extreme Black Diamond, both the Network Inspector application and the OptiView analyzer may not correctly identify the switch slots/ports. In this situation, it is recommended to Telnet to the switch to configure mirror sessions.*

SwitchTap features

The following window shows the SwitchTap application's main window with a configured mirror session:

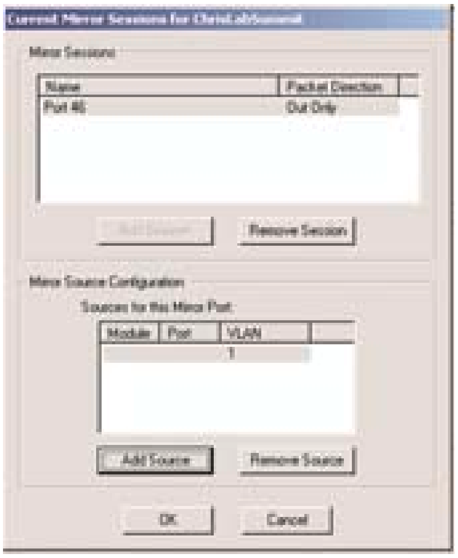


The Switch Status window shown below gives information about the selected switch.



- **Name** is the "best name" as determined by the OptiView Console application.
- **IP Address** is the IP Address for the switch.
- **Type** is the type of switch as determined by the OptiView Console application. You can use the Properties button to set or change the type.
- **Mirror Sessions Configured** gives the number of configured mirror sessions for the switch and the maximum number possible (in parentheses). **Note**: The number of mirror sessions shown is the number that has been configured, not the number that has been "applied" (i.e. activated).
- **Refresh** button causes the application to read the mirror status information for the currently selected switch. If a mirror session has been configured, but not applied, then that configuration will be reset.
- **Properties** opens the Switch Properties dialog box where you can specify or change the switch type. You can also enter the passwords necessary to access and change the switch configuration. The Telnet Password (Login for Extreme switches) allows access to the switch. The Enable Password (Password for Extreme switches) allows the configuration to be changed. Both passwords are required to configure and run a mirror session.
- **Manage Mirror Sessions** opens the Current Mirror Sessions dialog box for the selected switch.

You can use this to add or remove a mirror session and also to view the current mirror session(s) for the selected switch. The switch name is indicated in the title bar of the dialog box.


Current Mirror Sessions for ChrisLabSummit
Mirror Sessions
Add Session
Remove Session
Mirror Source Configuration
Sources for this Mirror Port
Add Source
Remove Source
OK
Cancel

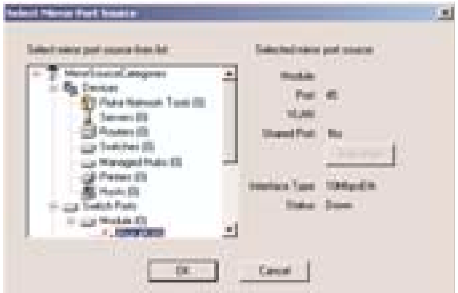
Name	Packet Direction
Port 46	Out Only

Module	Port	VLAN
		1

Mirror Sessions

Shows all of the configured mirror sessions for the selected switch. For each mirror session the following information is provided: **Note**: The mirror sessions shown are those that have been configured, not just the ones that have been applied (i.e. activated).

- **Name** is a combination of the switch module number, port number, and VLAN number for the selected destination (mirror) port.
- **Packet Direction** indicates whether traffic is permitted in both directions (In and Out) on the port, or Out only.
- **Add Session** brings up the Select Mirror Port Destination dialog box, which you can use to configure the mirror port for the selected switch. **Note**: Add Session is available only if the maximum number of Mirror Sessions Configured has not been reached.



Use the **MirrorPortCategories** tree to select the switch port to be used as the mirror port. Alternately, you can select a **Device** from the tree and the switch port that it is connected to will be configured as the mirror port.

Once you have selected a mirror port, the port information will be displayed to the right of the list. The **View Port** button will be available if the selected port has other devices connected to it. **View Port** presents a tree-like view of the devices on the selected switch port.

The **Accept Incoming Packets** checkbox will be available if the selected switch allows bi-directional traffic on a mirror port.

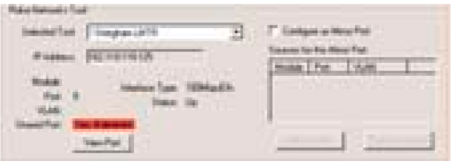
Caution: Be very careful about configuring a mirror port that allows Out traffic only. If it is a shared port, you may create problems for your network.

The **Restrict Source Ports to Single VLAN** checkbox will be available if the selected switch has multiple VLANs configured. **Note**: You must still select the **Apply Mirror Configuration** button to make the configured mirror session active.

- **Remove Session** deletes the selected mirror session.
- **Remove All Mirror Sessions** will cause all mirror sessions (both configured and applied) to be terminated (with a confirmation prompt) for the selected switch.

Fluke Networks Tool

The **Fluke Networks Tool** window shown below gives information about the selected tool.



- **Selected Tool** shows the Fluke Networks Tool which was highlighted in order to invoke the SwitchTap application. This tool may be either:

  a) The Fluke Networks Tool which was highlighted in order to invoke the SwitchTap application.

-or-

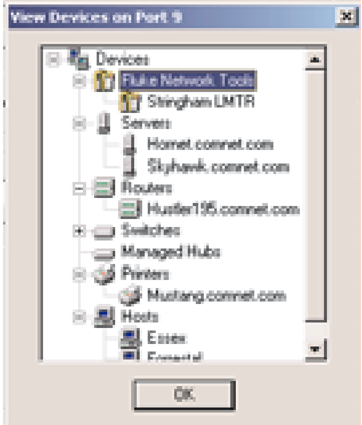
  b) The Fluke Networks Tool which is attached to a port on the same switch and shares its connection with the fewest number of other devices. This best-fit suggestion is made by OptiView Console when the SwitchTap application is invoked from a selected source port instead of a selected destination tool.

If the OptiView Console determines that there is another switch connected to the same port as the selected Fluke Networks Tool, the name shown in the **Selected Tool** field will be preceded by an exclamation point (!).

Caution: Use great care when creating a mirror session on a port that is shared with other devices, especially switches. Careless application of a mirror session could cause severe problems for your network. For example, selecting a shared port that has a switch on it as a mirror destination could isolate all devices on that port from the rest of the network; or if the mirror destination port has key servers or a critical router on it, workgroups or entire sites could be isolated.

You can use ▼ to open the pull-down menu and select a different Fluke Networks Tool.

- **IP Address** shows the IP Address for the selected Fluke Networks Tool.
- **Module** shows the module number (if configured) of the selected switch that the Fluke Networks Tool is located on.
- **Port** shows the port number of the selected switch that the Fluke Networks Tool is located on.
- **VLAN** shows the VLAN number (if configured) of the selected switch that the Fluke Networks Tool is located on.
- **Shared Port** indicates whether the switch port is shared with other devices. The field is highlighted in red if there are other switches on the port, yellow if there are other devices but no detected switches.
- **Interface Type** indicates the speed and type of the selected switch port that the Fluke Networks Tool is located on.
- **Status** indicates the port status (Up or Down)
- **View Port** presents a tree-like view of the devices on the selected switch port.



- **Configure as Mirror Port** – Use this checkbox to configure the selected switch port as a mirror port. The configuration change will not take effect until the **Apply Mirror Configuration** button is selected.
- **Sources for this Mirror Port** displays any sources configured for a mirror session. This selection is grayed out until the **Configure as Mirror Port** checkbox is selected.
- **Add Source** pops up the **Select Mirror Port Source** dialog box, which presents a tree-like view of possible sources for the configured mirror port. Selecting a source will cause all traffic on the same port as the selected device to be mirrored to the configured mirror port. You can use the **Add Source** button repeatedly to direct traffic from multiple ports to the mirror port.
- **Remove Source** will remove the highlighted source from the mirror session.

Apply Mirror Configuration

Any configured mirror session will not take effect until the **Apply Mirror Configuration** button is selected. Any configured but not yet applied sessions will be removed by application of the **Refresh** button in the **Switch Status** window. Deselecting the **Configure as Mirror Port** checkbox will also remove unapplied sources.

Using SwitchTap

The ability to create and use a mirror session on any given switch is strictly a function of the features of the switch. The SwitchTap application provides a convenient user interface for creating, managing, and disabling mirror sessions. Creating and using mirror sessions provides a very powerful tool for monitoring and troubleshooting the performance of your network. However, as with any tool, there are inherent risks involved with its use. It is important that you understand mirroring principles and the configuration of your network when configuring and applying a mirror session.

Choosing the appropriate mirror port is critical. Using a shared port increases the risk of flooding a portion of your entire network with unwanted traffic, creating traffic routing loops, or incapacitating network devices. Because the configuration of any individual network is so unique, it would be impossible to provide an entire list of potential configuration issues to avoid. Some general guidelines to follow are:

- Read the documentation for your switch. Understand the features and limitations of each one. Features may vary even with switches from the same manufacturer or even different firmware versions running on the same switch.
- The best-case scenario is that you choose a mirror port that has a single network analysis tool on it such as a Fluke Networks OptiView Workgroup Analyzer. Use the management port to control the analyzer remotely, making sure that management port is not part of the mirror session. Connect the Network Under Test port to the mirror port of the switch. Refer to the documentation of the analyzer for more information on its use.
- Not accepting incoming packets on the mirror port is useful to prevent inadvertent routing loops. However, if the mirror port is a shared port this will prevent any device on that port from sending out information on the network.
- It is best if the mirror port and the source port are configured for the same VLAN.
- Some switches may not let you mix VLANs. Even if the mirror port is not a shared port, some switches may prevent a source port from mirroring its traffic if the source port is on a different VLAN.

Problems

If you configure a mirror session that causes network problems, it is important that you know how to quickly remove the mirror session:

- Use the **Remove All Mirror Sessions** button to disable all mirror sessions for the selected switch.
- Manually disconnect the port from the network. This gives you more time to remove and correct the problem. Make sure that you select the correct cable or you may affect network functionality for other users.
- Communicate directly with the switch using Telnet or Web access. Refer to your switch documentation for instructions on how to do this.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

©2003 Fluke Corporation. All rights reserved.

Printed in U.S.A. 4/2003 1676322 A-ENG-N Rev B