



205 Westwood Ave
Long Branch, NJ 07740
1-877-742-TEST (8378)
Fax: (732) 222-7088
salesteam@Tequipment.NET



Filtering Link Aggregation Taps

FATAP-1000 SERIES
FATAP-2000 SERIES
FASTAP-4X4

FlowControl™

USER GUIDE

PN 2840523
March 2007

© 2007 Fluke Corporation. All rights reserved. Printed in USA.
All product names are trademarks of their respective companies.

COMPLIANCE TESTING

CAUTION

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE

*This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to **Part 15** of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at one's own expense.*

CE CERTIFICATIONS

This equipment has been tested and found to meet the radiated and conducted emission limits for a **Class B** product of **EN 55022** to the **EMC Directive 89/336/EEC** requirements.

This equipment has been tested and found to meet the immunity levels for **Class 1**, tested to **level 2** for **EN 6100-4-2**, tested to **level 3** for **EN 61000-4-3**, tested to **level 2** for **EN 61000-4-4**, and tested to **level 3** for **EN 61000-4-5** to the **EN 50082-1** requirements and meets the **Class A** requirements for **EN 61000-3-2** and **EN 61000-3-3**.

This equipment has completed the Product Safety Review and found to meet the **Low Voltage Directive 72/23/EEC (1993)** requirements.

Limited Warranty & Limitation of Liability

Each Fluke Networks product is warranted to be free from defects in material and workmanship under normal use and service. The warranty period for the mainframe is one year and begins on the date of purchase. Parts, accessories, product repairs and services are warranted for 90 days, unless otherwise stated. Ni-Cad, Ni-MH and Li-Ion batteries, cables or other peripherals are all considered parts or accessories. The warranty extends only to the original buyer or end user customer of a Fluke Networks authorized reseller, and does not apply to any product which, in Fluke Networks' opinion, has been misused, abused, altered, neglected, contaminated, or damaged by accident or abnormal conditions of operation or handling. Fluke Networks warrants that software will operate substantially in accordance with its functional specifications for 90 days and that it has been properly recorded on non-defective media. Fluke Networks does not warrant that software will be error free or operate without interruption.

Fluke Networks authorized resellers shall extend this warranty on new and unused products to end-user customers only but have no authority to extend a greater or different warranty on behalf of Fluke Networks. Warranty support is available only if product is purchased through a Fluke Networks authorized sales outlet or Buyer has paid the applicable international price. Fluke Networks reserves the right to invoice Buyer for importation costs of repair/replacement parts when product purchased in one country is submitted for repair in another country.

Fluke Networks warranty obligation is limited, at Fluke Networks option, to refund of the purchase price, free of charge repair, or replacement of a defective product which is returned to a Fluke Networks authorized service center within the warranty period.

To obtain warranty service, contact your Technical Assistance Center. Support information can be found in the System Recovery section at the end of this manual. Fluke Networks assumes no risk for damage in transit. Following warranty repair, the product will be returned to Buyer, transportation prepaid (FOB destination). If Fluke Networks determines that failure was caused by neglect, misuse, contamination, alteration, accident or abnormal condition of operation or handling, or normal wear and tear of mechanical components, Fluke Networks will provide an estimate of repair costs and obtain authorization before commencing the work. Following repair, the product will be returned to the Buyer transportation prepaid and the Buyer will be billed for the repair and return transportation charges (FOB Shipping point).

THIS WARRANTY IS BUYER'S SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY.

Since some countries or states do not allow limitation of the term of an implied warranty, or exclusion or limitation of incidental or consequential damages, the limitations and exclusions of this warranty may not apply to every buyer. If any provision of this Warranty is held invalid or unenforceable by a court or other decision-maker of competent jurisdiction, such holding will not affect the validity or enforceability of any other provision.

FLUKE NETWORKS P.O. BOX 777 EVERETT, WA 98206-0777 USA

Table of Contents

COMPLIANCE TESTING	ii
CERTIFICATIONS	ii
LIMITED WARRANTY & LIMITATION OF LIABILITY	iii
PREFACE	2
<i>FATAP-1000 / FATAP-2000 / FASTAP-4X4 series</i>	2
<i>FlowControl™</i>	2
<i>Audience</i>	2
UNPACKING	3
<i>Universal Packing List</i>	3
<i>Network Port and Tap / Monitor Port specifications</i>	3
OVERVIEW	4–6
<i>FATAP/FASTAP Panel Descriptions</i>	5–6
HARDWARE INSTALLATION	7–8
<i>Copper Ethernet networks</i>	7–8
<i>Fiber Networks</i>	9–10
<i>Tap / Monitor Ports</i>	11
<i>Management Ports</i>	12
FLOWCONTROL™	13–56
<i>Installation</i>	13–14
<i>Getting Started</i>	15
<i>IP Configuration</i>	16–30
<i>Networking</i>	31–33
<i>Interface</i>	34–51
<i>Filtering</i>	52–56
APPENDIX	57–62
<i>Frame and Data Packets</i>	57–59
<i>HyperTerminal</i>	60–61
<i>General Specifications</i>	62

Table of Contents continued

CARE AND MAINTENANCE	63
<i>Avoiding rough handling</i>	63
<i>Cleaning carefully</i>	63
<i>Providing adequate ventilation</i>	63
<i>Safety information</i>	63
<i>Service and adjustment</i>	63
CONTACTING FLUKE NETWORKS	64

Preface

Like many network security managers, you are constantly aware of how critical your network's security is to your company's bottom line. Your network's copper and fiber links are not only the backbone for high-volume traffic, but they also have the capacity to transfer proprietary data and support unauthorized bandwidth use. With the Fluke Networks series of Filtering Link Aggregation Taps, you can now filter and monitor your network's traffic with seamless transparency, protecting your company's most valuable assets.

FATAP-1000, FATAP-2000 AND FASTAP-4X4 SERIES

Each Filtering Link Aggregation Tap provides the means for meeting whatever network filtering, port assignment, and traffic monitoring requirements you may have. It also enables the sharing of multiple network tools between single network segments. With a Filtering Link Aggregation Tap, your monitoring tools can be quickly and effectively deployed to easily verify network security, expanding visibility to the farthest reaches of your network.

FLOWCONTROL™

FlowControl™ is the versatile monitoring utility bundled with the Fluke Networks series of Filtering Link Aggregation Taps. FlowControl™ is used to administrate, filter, aggregate, monitor, and log network traffic passing through the Filtering Link Aggregation Tap. These are typically installed between two nodes in an enterprise network, such as between a firewall and router.

Network data passing through the Tap are mirrored and, by using FlowControl™, can be routed to selected external network appliances that are connected to the FATAP/FASTAP's tap/monitor ports. The FATAP/FASTAP's ports, located exclusively on the front panel, enables easy rack access for configuration and patching of intrusion detection systems (IDS), forensic data analyzers, application monitors, and other detection devices.

By assigning the FATAP/FASTAP to an IP address, a network administrator can manage multiple FATAP/FASTAP units within a large network by configuring each with FlowControl™. This enables centralized management and ease of access from a remote location, such as a laptop.

AUDIENCE

This guide is written for the user who is connecting and managing a Fluke Networks Filtering Link Aggregation Tap for use with the included FlowControl™ configuration utility. The user should be comfortable with working in a Windows® environment, understands how networks operate, and has experience with administering network analyzing devices.

This user guide is written to quickly assist you with getting to know your new Filtering Link Aggregation Tap. We welcome any comments or suggestions you may have pertaining to this user guide.

Unpacking

UNIVERSAL PACKING LIST

- (1) Filtering Link Aggregation Tap
- (2) 100–240V AC power cords
- (1) DRL434-6 Serial-to-USB configuration cable
- (1) CAT-5E Ethernet 3' cable
- (1) Installation CD-ROM: FlowControl™ management utility
- (1) User's Guide

FATAP-1000 SERIES MODELS

FATAP-1000BT FATAP-1000SX
 FATAP-1000LX

FATAP-2000 SERIES MODELS

FATAP-2000BT FATAP-2000BT/SX
 FATAP-2000SX FATAP-2000BT/LX
 FATAP-2000LX

FASTAP SERIES MODEL

FASTAP-4X4

NETWORK PORT AND TAP / MONITOR PORT SPECIFICATIONS

MODEL	AVAILABLE NETWORK PORTS(S)	AVAILABLE TAP / MONITOR PORTS	TAP / MONITOR PORT CONFIGURATION OPTIONS
FATAP-1000BT	1 @ 10/100/1000BASE-T	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-1000SX	1 @ 1000SX multi-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-1000LX	1 @ 1000LX single-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-2000BT	2 @ 10/100/1000BASE-T	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-2000SX	2 @ 1000SX multi-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-2000LX	2 @ 1000LX single-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-2000BT/SX	2 @ 10/100/1000BASE-T 2 @ multi-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FATAP-2000BT/LX	2 @ 10/100/1000BASE-T 2 @ single-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); option of adding up to 4 single-/multi-mode fiber ports
FASTAP-4X4	4 @ 10/100/1000BASE-T or optional single- / multi-mode fiber	4 ports	4 @ 10/100/1000BASE-T (standard); or optional single- / multi-mode fiber

Overview

The Fluke Networks Filtering Link Aggregation Tap features exceptional network aggregation and filtering versatility, enabling superior 24/7 management and analysis of network traffic. This flexibility allows dedicated devices to handle routing, firewalls, and subnet switching operations while filtered traffic can be directed to any desired monitoring device.

Every Filtering Link Aggregation Tap model creates a duplicate of every data packet passing through the tap, redirecting the duplicated stream to the FATAP's tap / monitor ports. This feature permits live monitoring of traffic with gigabit (10/100/1000BASE-T) Ethernet monitoring devices or, optionally, up to four fiber monitoring devices.

By using the bundled FlowControl™ management software, network administrators can readily customize traffic flow from each network to specific monitoring devices, eliminating the inconvenience of having to add or remove physical links whenever more than one monitoring device is present.

Every Filtering Link Aggregation Tap model supports link aggregation, allowing for bi-directional, full-duplex network traffic to be directed to a single Network Interface Card (NIC). Moreover, traffic can be simultaneously directed from two network taps to a single monitoring device. The potent filtering capabilities enable explicit monitoring of only that network traffic which is desired for further analysis.

The Fluke Networks series of Filtering Link Aggregation Taps is available in nine configurations. All models feature gigabit Ethernet network ports, and can support up to four tap devices. If fiber monitoring needs are required, up to a total of four single- or multi-mode fiber transceivers can be optionally installed into the Filtering Link Aggregation Tap.

Overview FATAP/FASTAP Panel Descriptions

FATAP-1000 SERIES

Figure 1 shows the FATAP-1000BT front panel display. This example is equipped with a standard 10/100/1000BASE-T copper network port, and four optionally installed fiber tap / monitor ports alongside four standard copper tap / monitor ports.

NOTE

Fiber pair models (FATAP-1000SX and FATAP-1000LX) are similar, but feature multi-mode and single-mode fiber taps, respectively.

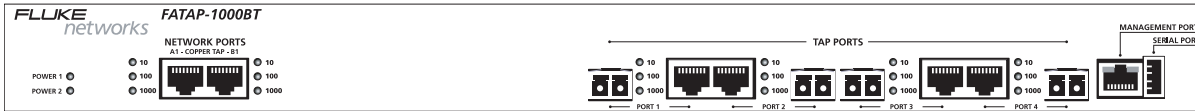


Figure 1. FATAP-1000BT front panel display with optional fiber tap / monitor ports installed.

NOTE

Copper tap / monitor ports are standard on every Filtering Link Aggregation Tap model, while individual fiber tap / monitor ports can optionally be added as needed.

The rear access panel for all Filtering Link Aggregation Tap models is shown below in **Figure 2**.

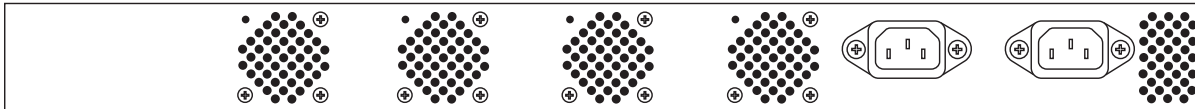


Figure 2. Filtering Link Aggregation Tap rear access panel, featuring outlets for both primary and redundant AC power supplies.

Overview FATAP/FASTAP Panel Descriptions

FATAP-2000 SERIES

Figure 3 shows the FATAP-2000BT/SX front panel display. This example is equipped with two standard 10/100/1000BASE-T copper network ports, two fiber network ports, and four optionally installed fiber tap/monitor ports alongside four standard copper tap/monitor ports.

Other FATAP-2000 series models are similar features, but are equipped with alternate tap configurations. Refer to the Network Port and Tap / Monitor Port Specifications table on page 3 for model specifications.

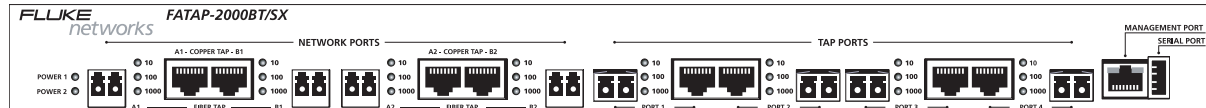


Figure 3. FATAP-2000BT/SX front panel display with optional fiber tap / monitor ports installed.

NOTE

Copper tap / monitor ports are standard on every Filtering Link Aggregation Tap model, while individual fiber tap / monitor ports can optionally be added as needed.

FASTAP-4X4 SERIES

Figure 4 shows the FASTAP-4X4 front panel display. This model is equipped with four standard 10/100/1000BASE-T copper network ports, four optional fiber network ports, and four optionally installed fiber tap/monitor ports alongside four standard copper tap/monitor ports.

NOTE

The FASTAP-4X4 is designed for use with SPAN / Mirror port connectivity on the network side. By contrast, in-line applications should use one of the FATAP series models.

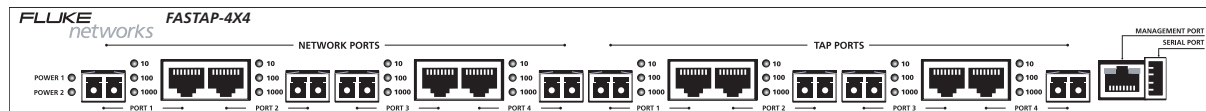


Figure 4. FASTAP-4X4 front panel display with optional fiber tap / monitor ports installed.

Hardware Installation Copper Ethernet Networks

COPPER PORT CONNECTION INSTRUCTIONS

The installation procedure described below applies to FATAP-1000, FATAP-2000 and FASTAP series models featuring 10/100/1000BASE-T copper network ports. Refer to page 9 for FATAP/FASTAP models equipped with fiber network ports.

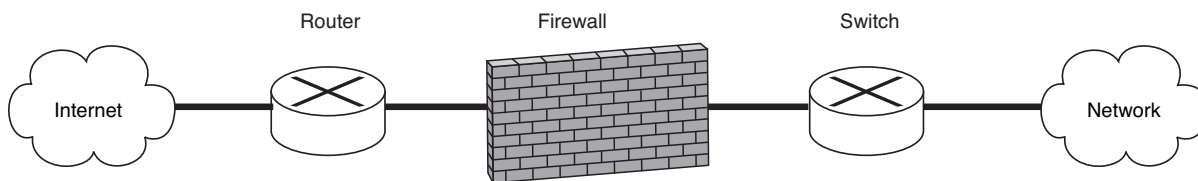


Figure 5. Typical 10/100/1000BASE-T copper network schema

Figure 5 presents a common network situation: incoming traffic from the internet is first routed, then sent through the firewall before being distributed to the network via switching.

To install the Filtering Link Aggregation Tap using copper Ethernet ports:

1. Determine where along the network traffic monitoring is needed.

NOTE

The Filtering Link Aggregation Tap may be placed anywhere along a copper network, depending on what kind of traffic monitoring is required.

2. Turn on the Filtering Link Aggregation Tap by plugging each of the FATAP/FASTAP's AC power cords into separate power circuits. Each **POWER** LED indicator on the left side of the FATAP/FASTAP's front panel will illuminate, verifying that primary and redundant power supplies are active.
3. At the juncture where the FATAP/FASTAP will be added to the network, disconnect the copper network cable. For instance, if the FATAP/FASTAP is to be installed between router and firewall, disconnect the cable from the firewall.
4. Connect the existing cable between the first device (e.g., router) and **NETWORK PORT A1** on the FATAP. (or **NETWORK PORT 1** on the FASTAP).

Hardware Installation Copper Ethernet Networks

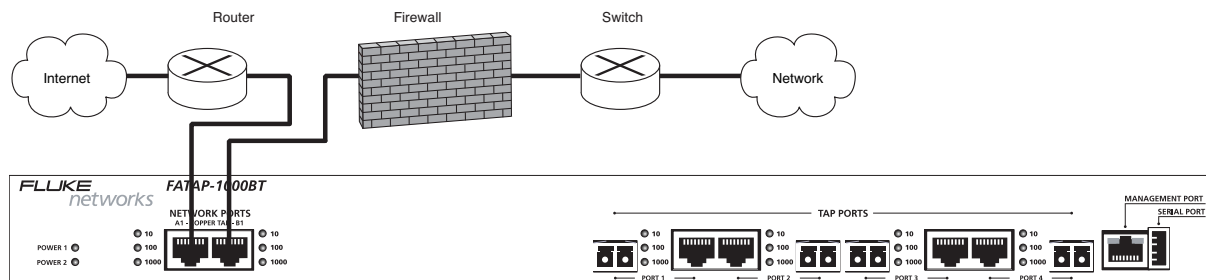


Figure 6. Insertion of Filtering Link Aggregation Tap: connecting router to **NETWORK PORT A1** and firewall to **NETWORK PORT B1** on FATAP-1000BT unit, closing the network connection.

5. Using a separate cable, connect **NETWORK PORT B1** to the second device (e.g., firewall), as shown in **Figure 6**.
6. To verify whether the FATAP is properly connected, check the LED panel indicators located on either side of **NETWORK PORT A1** and **NETWORK PORT B1**; both should be illuminated. Solid LEDs indicate the current network speed setting, while a flashing LED indicates network activity.

NOTE

On models equipped with both copper and fiber network ports, the LED indicators for 10Mbps and 100Mbps will only illuminate when a copper network port is installed on a 10/100BASE-T network; the 1000Mbps LED indicator will illuminate when network ports are connected to fiber or 1000BASE-T copper connections.

The network port functionality on each copper-equipped Filtering Link Aggregation Tap is default configured to a full-duplex setting of 1000Mbps. This speed setting can be adjusted to the network environment by using the FlowControl™ management utility.

On Filtering Link Aggregation Tap models that are equipped with two copper network ports (e.g., FATAP-2000BT, FATAP-2000BT/SX, and FATAP-2000BT/LX), the above steps can be repeated for monitoring another network segment on **NETWORK PORT 2**, such as between firewall and switch.

IMPORTANT

In the event that the Filtering Link Aggregation Tap loses both primary and redundant power while in use, network traffic will not be disrupted. The FATAP is designed to operate passively whenever power is absent, allowing network traffic to pass through without interruption. Port monitoring functionality, however, will be unavailable until primary and/or redundant power is restored.

Hardware Installation Fiber Networks

FIBER TAP CONNECTION INSTRUCTIONS

The installation procedure described below applies to FATAP-1000, FATAP-2000 and FASTAP series models featuring either single-mode (LX) or multi-mode (SX) fiber network ports. Refer to page 7 for FATAP/FASTAP models equipped with copper Ethernet network ports.

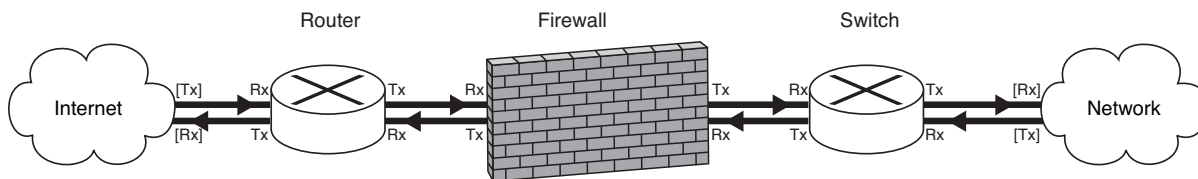


Figure 7. Typical fiber network schema

Figure 7 presents a typical fiber network scenario: incoming traffic from the internet is received by the router (Rx), which sends (Tx) to the firewall (Rx); the firewall then transfers (Tx) data to the internal network. Outgoing traffic from the internal network travels along a separate, but parallel return path via the firewall (Rx), which sends the traffic (Tx) to the router (Rx) to be sent (Tx) back to the internet.

To install the Filtering Link Aggregation Tap on a fiber network:

1. Determine where along the network traffic that monitoring is needed.

NOTE

The Filtering Link Aggregation Tap may be placed anywhere along a fiber network, depending on what kind of traffic monitoring is required.

2. Turn on the Filtering Link Aggregation Tap by plugging each of the FATAP's AC power cords into separate power circuits (**Figure 2**). Each **POWER** LED indicator on the left side of the FATAP's front panel will illuminate, verifying that primary and redundant power supplies are active.
3. At the juncture where the FATAP will be added to the network, disconnect the **Tx** and **Rx** fiber pair connectors from one device. For instance, if a FATAP series unit is to be installed between the router and the firewall, disconnect the fiber pair connection from the firewall.

Hardware Installation Fiber Networks

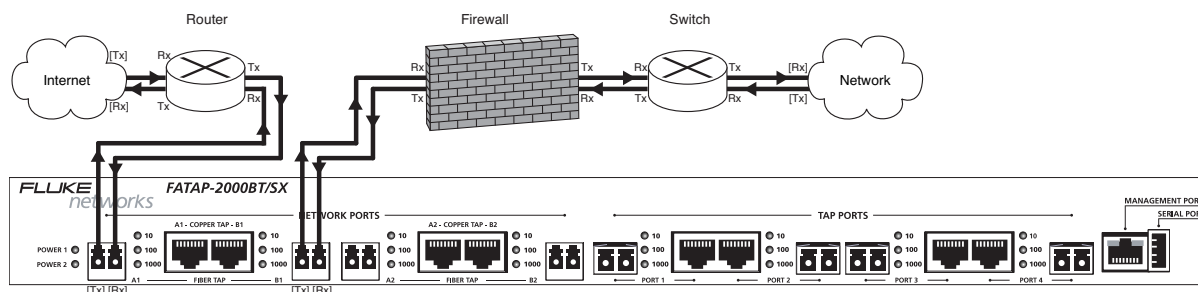


Figure 8. Connecting router (Tx) fiber cable to the **NETWORK PORT A1** (Rx) port on the FATAP-2000BT/SX. Using the other half of the fiber pair, connect the **NETWORK PORT A1** (Tx) port to the router's (Rx) port to establish a parallel connection.

4. As shown in **Figure 8**, connect the fiber pair between the first device (e.g., router) and **NETWORK PORT A1** on the FATAP, ensuring that the (Tx) port from the first device is attached to the (Rx) port on **NETWORK PORT A1**, while the (Tx) connector from **NETWORK PORT A1** is connected to the (Tx) connector on the first device.
5. Using a separate fiber pair, connect **NETWORK PORT B1** on the FATAP to the second device (e.g., firewall), ensuring that the (Tx) connector from the FATAP is attached to the (Rx) connector on the second device, while the (Tx) connector from that device is connected to the FATAP's **NETWORK PORT B1** (Rx).
6. To verify whether the FATAP is properly connected, check the LED panel indicators located on either side of **NETWORK PORT A1** and **NETWORK PORT B1**; both should be illuminated. Solid LEDs next to **1000Mbps** confirm a successful connection, while flashing LEDs indicate network activity.

NOTE

On FATAP-2000 series models equipped with combined copper and fiber network ports (e.g., FATAP-2000BT/SX and FATAP-2000BT/LX), both sources can be simultaneously connected to a single network port. The Filtering Link Aggregation Tap allows source traffic on either channel to pass through without disrupting the other. Only one source per network port, however, can be monitored by the tap / monitor ports at any given time. The FlowControl™ configuration utility manages control over FATAP monitoring options. Copper network ports are monitored by default.

On FATAP-2000 series models that are equipped with two fiber network ports (e.g., FATAP-2000SX, FATAP-2000BT/LX, etc.), the above steps can be repeated for monitoring another network segment on **NETWORK PORT 2**, such as between a firewall and a switch.

NOTE

In the event that a Filtering Link Aggregation Tap loses both primary and redundant power while in use, network traffic will not be disrupted. The FATAP is designed to operate passively whenever power is absent, allowing network traffic to pass through without interruption. Port monitoring functionality, however, will be unavailable until primary and/or redundant power is restored.

Hardware Installation Tap / Monitor Ports

TAP / MONITOR PORT CONNECTION INSTRUCTIONS

Figure 9 shows a network monitoring scenario using a FATAP-2000BT/SX Filtering Link Aggregation Tap equipped with four optional fiber tap/monitor ports. Each tap/monitor port is connected to various monitoring and analyzing devices.

IMPORTANT

When adding a fiber monitoring device, verify that the FATAP's **TAP** (Tx) fiber port is connected to the external monitoring device's (Rx) fiber port, while the external device's (Tx) fiber port is connected to the FATAP's **TAP** (Rx) port.

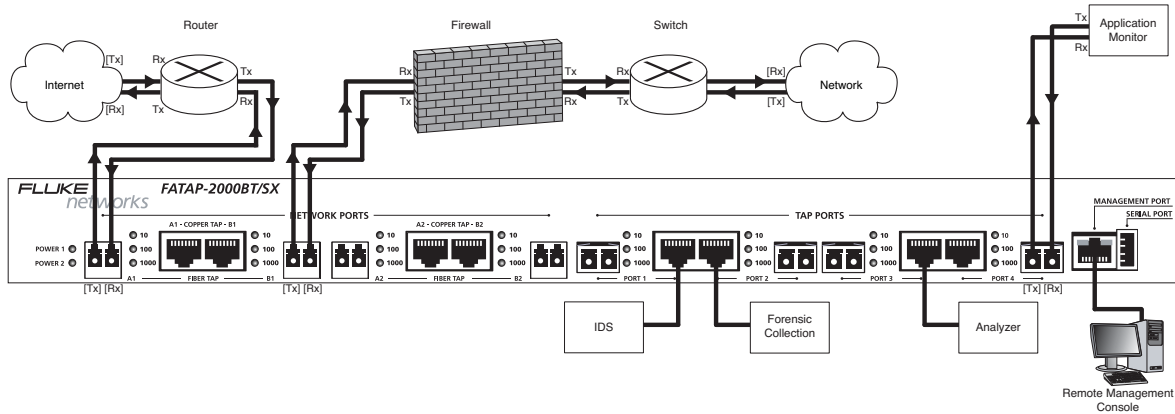


Figure 9. FATAP-2000BT/SX Filtering Link Aggregation Tap application with tap / monitor ports connected to monitoring devices

NOTE

Any combination of monitoring devices may be used with a Filtering Link Aggregation Tap. With optional fiber tap / monitor ports installed, both copper and fiber connections on one tap / monitor port can be attached to different monitoring devices; however, only one device per tap / monitor port — either copper or fiber — can be selected at a time. Tap / monitor port device selection is managed by the FlowControl™ monitoring utility.

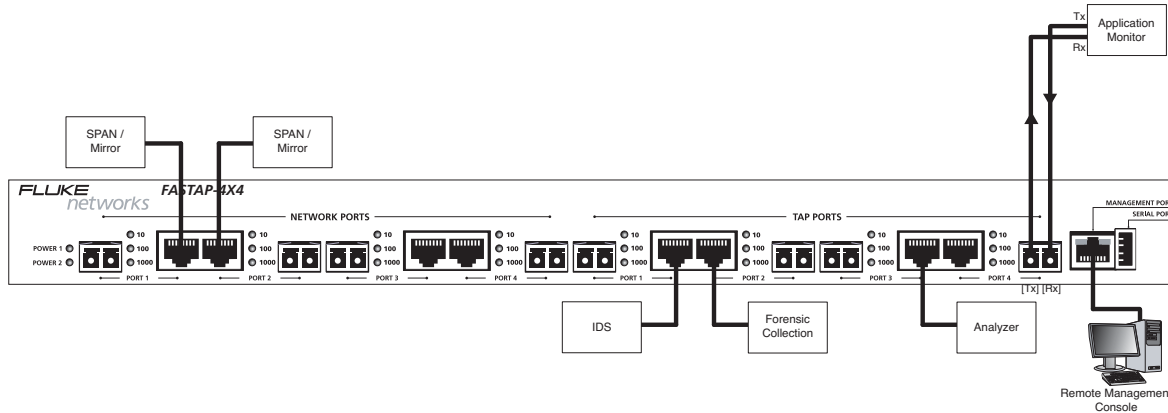


Figure 10. FASTAP-4X4 Filtering Link Aggregation Tap with tap / monitor ports connected to SPAN / Mirror devices

Hardware Installation Management Ports

REMOTE MANAGEMENT CONTROL

Once all desired monitoring devices (e.g., IDS, analyzers, forensic collection, etc.) are connected to the Filtering Link Aggregation Tap's tap/monitor ports, use a CAT-5E Ethernet cable to connect the **MANAGEMENT PORT** (located at far right on the FATAP's front panel, next to the **SERIAL PORT**) to the remote management console (e.g., the computer or local network from which the FlowControl™ monitoring utility will be managed). Built-in LEDs on the **MANAGEMENT PORT** will illuminate once a connection is established with the remote management environment.

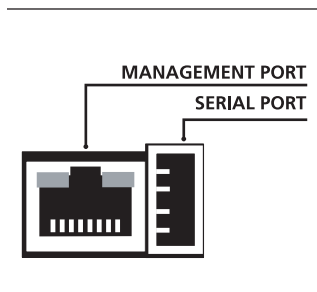


Figure 11. **MANAGEMENT PORT** (10/100BASE-T Ethernet) and **SERIAL PORT** (6-pin USB-style).

DIRECT FATAP / FASTAP CONNECTION

A direct link between the management console (e.g., a laptop with FlowControl™ installed) and the Filtering Link Aggregation Tap is required for specific configuration steps — such as assigning an IP address to the FATAP/FASTAP (see page 16). Connect the included DRL434-6 serial cable's USB connector to the **SERIAL PORT** on the FATAP/FASTAP (at far right on the FATAP front panel, **Figure 11**, next to the **MANAGEMENT PORT**), and the 9-pin connector into the serial port on the management console.

FlowControl™ Installation

Installing the FlowControl™ Software

The FlowControl™ software is used to configure the Filtering Link Aggregation Tap. This section covers the installation of the FlowControl™ software application.

1. Insert the FlowControl™ CD into your computer's optical drive.
2. Browse to your computer's optical drive. Double-click on the setup application to begin installation.
3. Some computers are protected against unverified applications. FlowControl™ is a safe and secure application. Click Install to continue the installation process.
4. A progress bar shows the status of the installation (**Figure 12**).

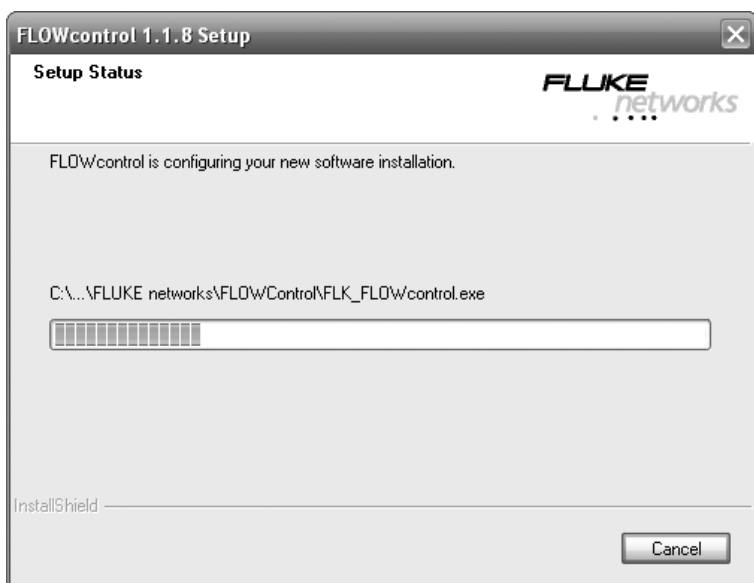


Figure 12. FlowControl™ installation setup progress

FlowControl™ Installation



Figure 13. FlowControl™ startup splash screen

5. Congratulations, you have successfully installed FlowControl™. FlowControl™ starts automatically after installation. The FlowControl™ icon is displayed while the application is launched on your computer.
6. You are at the FlowControl™ main screen. Refer to **FlowControl™ Getting Started** on page 15 to learn how to use the FlowControl™ application.



Figure 14. FlowControl™ main screen

The default username is **Administrator** and the default password is **admin**. The Administrator has “super-user” privileges and can limit access of other accounts. See the **Utilities** pull-down menu section for changing user account information.

Configuring the IP Address of a Filtering Link Aggregation Tap

1. You may want to record the IP address(es) of your Filtering Link Aggregation Tap here for easy reference in the future:

DEVICE IP ADDRESS LOG

LOCATION	SUB-LOCATION	FILTERING LINK AGGREGATION TAP MODEL NUMBER	IP ADDRESS

2. You may want to record your Username and Password information here for easy reference in the future:

ADMIN LOGIN INFORMATION

USERNAME	
PASSWORD	

3. You may connect your PC to your Filtering Link Aggregation Tap:
 - With the provided serial cable & HyperTerminal
 - With the provided serial cable & the FlowControl™ software
 - With a cross-connect LAN cable & the FlowControl™ software
4. An agent stores the specific connection information that your PC uses to connect to a Link Filtering Aggregation Tap.
5. Default agents allow for serial connections to the Filtering Link Aggregation Tap
6. Additional agents must be created to allow for LAN connections
7. This section provides information on configuring the IP address only. For more information regarding the creation of connection agents, see page 31.
8. The default IP Address for the Filtering Link Aggregation Tap is **192.168.1.1**. This address will most likely need to be modified in order for the Filtering Link Aggregation Tap to be available via your local network.
9. The default user name is **Administrator**, and default password is **admin**.

FlowControl™ IP Configuration

Configuring the IP Address of a Filtering Link Aggregation Tap

The Filtering Link Aggregation Tap is assigned an IP address by default. It is likely that the IP address must be changed before the Filtering Link Aggregation Tap can be integrated into your local network. A new IP address can be assigned by using either Microsoft's HyperTerminal or FlowControl™.

NOTE

*The initial setup may have already been completed. If your Filtering Link Aggregation Tap already has an IP address for your network, please turn to **Using the FlowControl™ Software** on page 24.*

If you need to modify the IP address of your Filtering Link Aggregation Tap, continue with one of the sections below.

CONFIGURING THE IP ADDRESS: HYPERTERMINAL

The IP address of your Filtering Link Aggregation Tap can be configured via a serial connection. A serial connection can be made with Microsoft's HyperTerminal application that is typically available on Windows PCs.

1. First, you must connect your PC and your Filtering Link Aggregation Tap. Using the provided cable (DRL 434-6), connect the 9-pin end to the serial port on your PC, and connect USB end to the serial port on your Filtering Link Aggregation Tap as shown below in **Figure 15**:

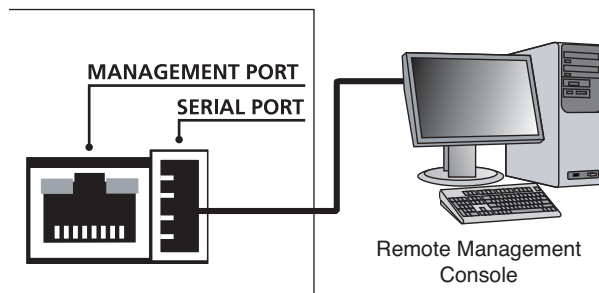


Figure 15. FATAPI/FASTAP-series serial connection with a PC device

FlowControl™ IP Configuration

2. Open the HyperTerminal Application on your PC by selecting **Start > All Programs > Accessories > Communications > HyperTerminal**.
3. Name a New HyperTerminal Connection (**Figure 16**). Click **OK**.



Figure 16. HyperTerminal **Connection Description** window

4. On the **Connect To** window, create a serial link by selecting the **COM** port assigned to the Serial Port on your PC from the **Connect using** pull-down menu. Click **OK**.



Figure 17. HyperTerminal **Connect To** window

FlowControl™ IP Configuration

5. Next, configure the **COM** Properties. The correct settings to communicate with your Filtering Link Aggregation Tap are shown below. Once all settings are configured correctly, click Apply, and then click OK.

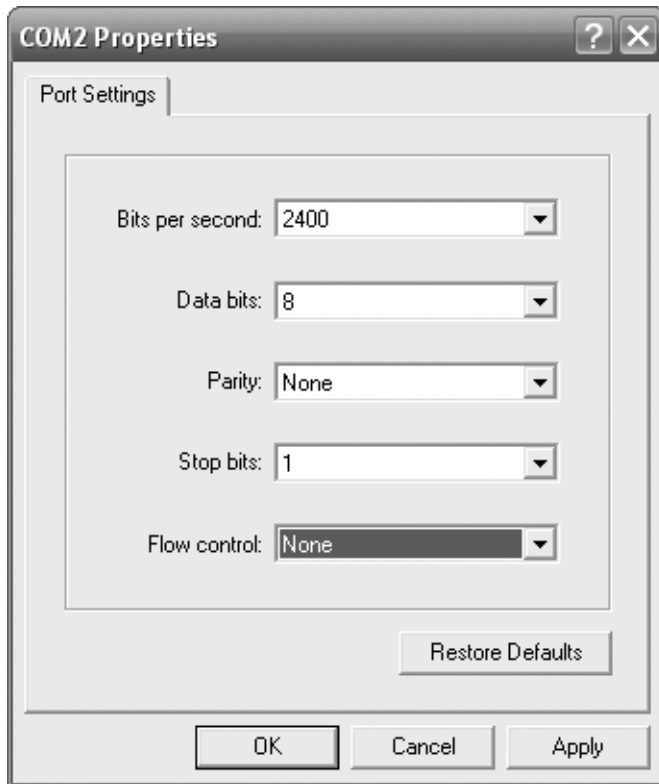


Figure 18. HyperTerminal **COM Properties** window

FlowControl™ IP Configuration

6. Log in to the Filtering Link Aggregation Tap. The default user name is **Administrator** and the default password is **admin**.

NOTE

Sometimes it is necessary to press the **Enter** key once to obtain the HyperTerminal prompt.

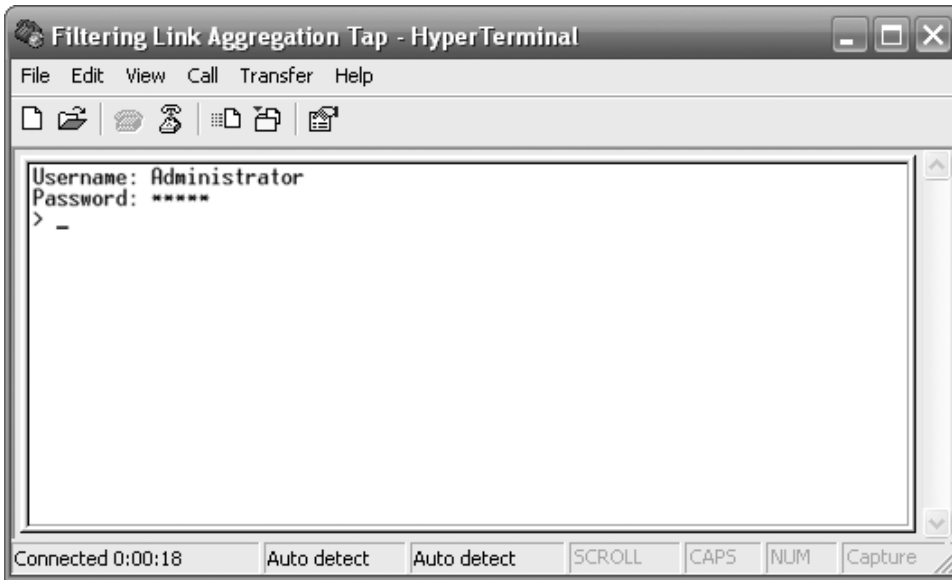


Figure 19. HyperTerminal **Login** window

FlowControl™ IP Configuration

7. You are now connected to your Filtering Link Aggregation Tap. Type **HELP** to see a list of available commands.

```
Filtering Link Aggregation Tap - HyperTerminal
File Edit View Call Transfer Help
[Icons]
Username: Administrator
Password: *****
> HELP
CLEAR SYSLOG - Clear Syslog Records
EXIT - Terminate HyperTerminal Session.
HELP - Display Commands.
SET IP ADDRESS xxx.xxx.xxx.xxx - Set IP address.
SET IP BROADCAST xxx.xxx.xxx.xxx - Set broadcast IP.
SET IP DEFAULT GATEWAY xxx.xxx.xxx.xxx - Set Default Gateway.
SET IP SUBNET xxx.xxx.xxx.xxx - Set Subnet Mask.
SET SYSLOG ENABLE (ON/OFF) - Enable Syslog
SET SYSLOG IP ADDRESS xxx.xxx.xxx.xxx - Set SysLog Server address.
SET TCP PORT xxxxx - Set TCP Port.
SHOW - Show current settings.
> _
Connected 0:01:54 Auto detect Auto detect SCROLL CAPS NUM Capture
```

Figure 20. Filtering Link Aggregation Tap **Commands** window

FlowControl™ IP Configuration

8. Set the IP address by typing **SET IP ADDRESS x.x.x.x**, where **x.x.x.x** corresponds to a valid IP address for your network. Press the Enter key to continue.
9. Set the subnet mask by typing **SET IP SUBNET x.x.x.x**, where **x.x.x.x** corresponds to your network's subnet mask. Press the Enter key to continue.
10. Set the default gateway (if needed) by typing **SET IP DEFAULT GATEWAY x.x.x.x**, where **x.x.x.x** corresponds to your network's default gateway. Press the Enter key to continue.

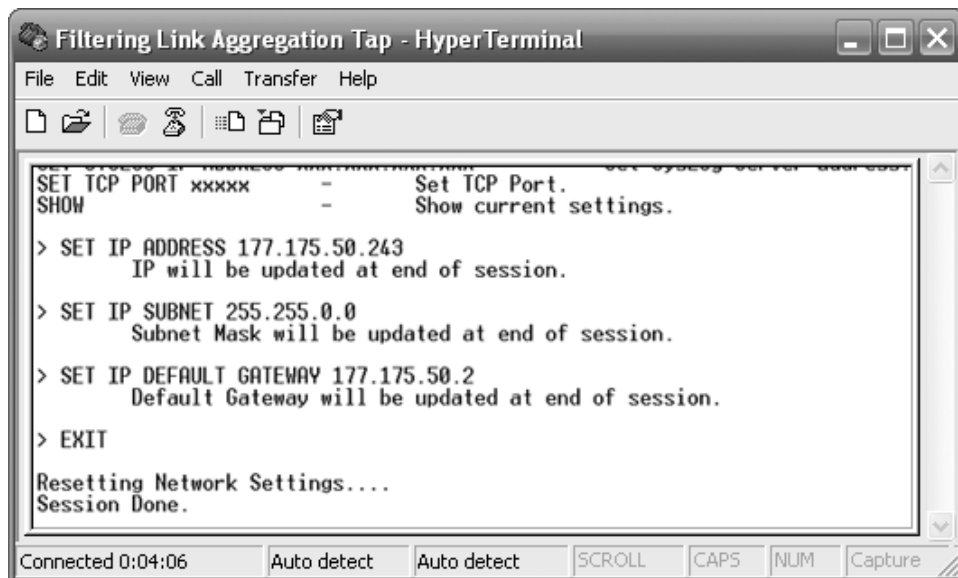


Figure 21. Filtering Link Aggregation Tap **Configuration** window

11. Type **EXIT** to save the network address changes and reboot the Filtering Link Aggregation Tap.

NOTE

During the reboot process (approximately 45 seconds), several unreadable characters will be displayed in the HyperTerminal window. These characters can be ignored.

FlowControl™ IP Configuration

12. When the reboot is complete, the stream of characters will stop. At this time, press the Enter key, and then type **SHOW** to review the network address settings. Verify that the settings are correct.

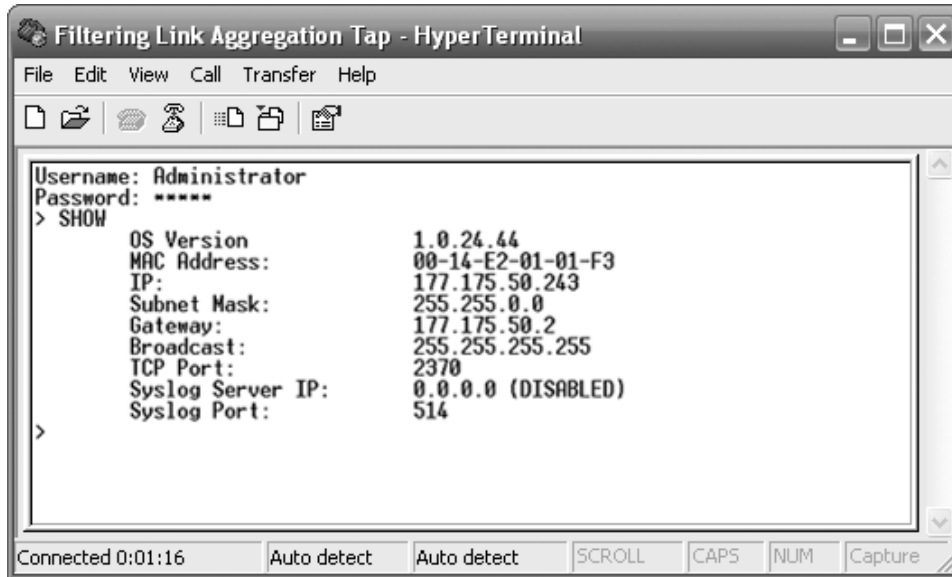


Figure 22. Filtering Link Aggregation Tap **SHOW** window

13. Disconnect the Serial Cable from your Filtering Link Aggregation Tap.

FlowControl™ IP Configuration

CONFIGURING THE IP ADDRESS: FLOWCONTROL™ VIA SERIAL CONNECTION

The IP address of the Filtering Link Aggregation Tap can also be modified using a serial connection with the FlowControl™ software application. Using FlowControl™ with a serial connection is only recommended during initial configuration.

1. First, you must connect your PC to your Filtering Link Aggregation Tap. Using the provided cable (DRL434-6), connect the 9-pin end to the serial port on your PC, and connect USB end to the serial port on your Filtering Link Aggregation Tap as shown below:
2. Start the FlowControl™ software application.
3. From the main FlowControl™ Main Window, expand Local Connectivity, then select the local COM port you are using on your PC.



Figure 23. FlowControl™ local connectivity

4. To connect using your PC's COM port, select **Agent > Connect**. You will be presented with the login screen. The default user name is Administrator and the default password is admin.

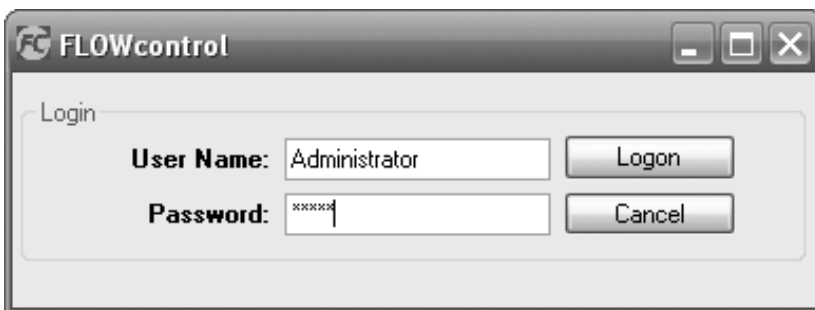


Figure 24. FlowControl™ login window

FlowControl™ IP Configuration

5. After logging in (approximately 150 seconds), the FlowControl™ main window appears. An image of the Filtering Link Aggregation Tap is displayed across the top of the window. The image displayed will automatically update to the correct image. An FSS-2000BT/SX is shown below.

NOTE

The FlowControl™ activity is shown across the bottom of the Main Window.

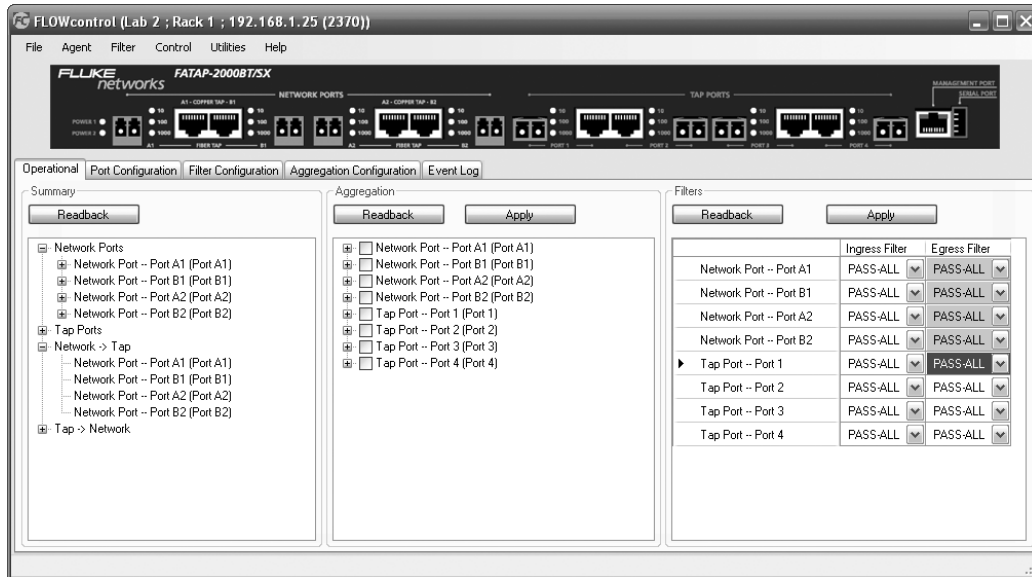
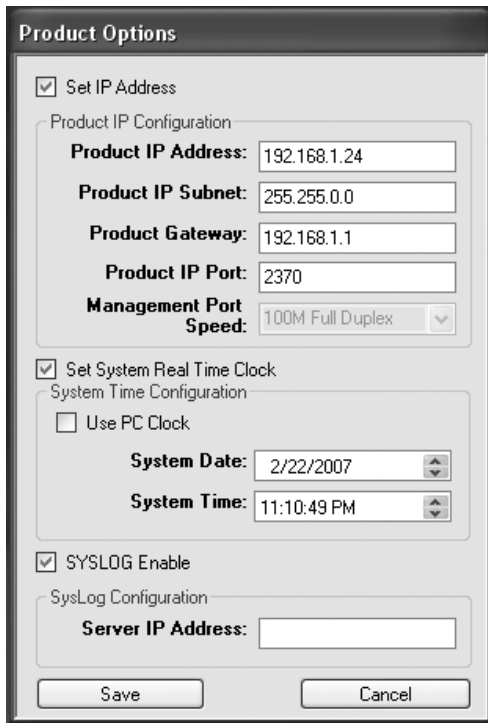


Figure 25. FlowControl™ main window, connected to the FATAP-2000BT/SX

6. To correctly integrate your new Filtering Link Aggregation Tap into your network, you must assign it a valid IP address for your network. To do this, select **Utilities > Options** to open the Product Options window.

FlowControl™ IP Configuration



The screenshot shows a 'Product Options' dialog box with the following sections and fields:

- Set IP Address
 - Product IP Configuration
 - Product IP Address: 192.168.1.24
 - Product IP Subnet: 255.255.0.0
 - Product Gateway: 192.168.1.1
 - Product IP Port: 2370
 - Management Port Speed: 100M Full Duplex (dropdown menu)
- Set System Real Time Clock
 - System Time Configuration
 - Use PC Clock
 - System Date: 2/22/2007 (calendar icon)
 - System Time: 11:10:49 PM (clock icon)
- SYSLOG Enable
 - SysLog Configuration
 - Server IP Address: (empty text field)

Buttons: Save, Cancel

Figure 26. Product Options window

7. Enter the desired IP address and subnet mask. If your network is segmented into multiple subnets, you may provide the Filtering Link Aggregation Tap with a default gateway (such as the IP address of a local router) to use when communicating with non-local devices. If you don't need a default gateway, leave it blank.
8. Save the new information by clicking on Save.
9. From the FlowControl™ main window select **Agent > Disconnect** to disconnect the serial connection to the Filtering Link Aggregation Tap.

You must now create an agent that allows for communication between your PC and your new Filtering Link Aggregation Tap via your LAN. Please refer to page 27 to create a connection agent.

FlowControl™ IP Configuration

CONFIGURING THE IP ADDRESS: FLOWCONTROL™ VIA LAN CONNECTION

If your PC does not have a 9-pin serial connection, you can perform the initial configuration of the Filtering Link Aggregation Tap via an Ethernet LAN connection. To do this, you must be able to temporarily change the IP Address of your PC and you must have a cross-connect LAN cable.

1. The default IP address of a Filtering Link Aggregation Tap is **192.168.1.1** with a netmask of **255.255.255.0**.

NOTE

192.168.1.1/24 specifies the IP address **192.168.1.1** and the netmask (**/24**). The **/24** netmask can also be written as **255.255.255.0**.

2. Temporarily set the IP address of your PC to **192.168.1.2/24**.
3. Connect your PC to the Filtering Link Aggregation Tap via a cross-connect LAN cable.

NOTE

Some newer PCs may have Network Interface Cards that automatically detect when a cross-connection is necessary. In some cases, a cross-connect LAN cable will not work. If you have trouble establishing a connection between your PC and the Filtering Link Aggregation Tap, you may want to try using a normal (straight-through) LAN cable.

4. Start the FlowControl™ software application.

FlowControl™ IP Configuration



Figure 27. FlowControl™ main window

5. To configure a new Filtering Link Aggregation Tap you must first define a connection agent. Agents are connection profiles used by your PC to connect to various Link Filtering Aggregation Tap. To create your first agent, select **Agent > Add** to open the Product Configuration window and add a new agent. When using your Filtering Link Aggregation Tap the first time, create an agent with the default IP address of the Filtering Link Aggregation Tap (**192.168.1.1**). The IP address must be changed later to an appropriate IP address for your network. You may enter the desired location & sub-location information at this time, this information will help you distinguish one Filtering Link Aggregation Tap from another.

IMPORTANT

The IP address must be changed later to an appropriate IP address for your network.

FlowControl™ IP Configuration

6. Enter the default IP Address (**192.168.1.1**) and port for your new agent on the Product Configuration window as shown below. Also you must enter a descriptive name for this connection agent. If you are on the same network as your Filtering Link Aggregation Tap, the Get Product button retrieves the FATAP/FASTAP-series model information. The location information will be user specific. If you will be installing and configuring several new Filtering Link Aggregation Tap, then you may wish to name this agent "New_FATAP_Install" or similar so you can re-use it later.

The screenshot shows the 'Product Configuration' dialog box. It is divided into several sections. At the top, there is a checkbox for 'Connect Serially' which is unchecked. Below this is the 'Product Configuration' section, which includes an 'IP Address' field containing '192.168.1.1', a 'Port' dropdown menu set to '2370', and a 'Get Product' button. The next section is 'Location Configuration', featuring a dropdown menu set to '<New>', a 'Name' field containing 'Lab 1', and a large empty 'Description' text area. Below that is a checked checkbox for 'Use Sub Location'. The final section is 'Sub Location Configuration', which has a dropdown menu set to '<New>', an empty 'Name' field, and another large empty 'Description' text area. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Figure 28. FlowControl™ Product Configuration window

7. When all the information has been entered correctly, select Save. This creates the new agent. Once a new agent is created, the agent will appear in the list of agents shown on the main FlowControl™ window.
8. To connect to a Filtering Link Aggregation Tap using an agent, expand the list of agents until the IP Address and Port appear. Click on the desired Address (Port): and select **Agent > Connect**.

FlowControl™ IP Configuration

- 9. You will be presented with the login screen. The default username is **Administrator** and the default password is **admin**. After logging in (approximately 8 seconds), the FlowControl™ the Main Window appears. An image of the Filtering Link Aggregation Tap is displayed across the top of the window. The image displayed will automatically update to the correct image. A FATAP-2000BT/SX is shown below.

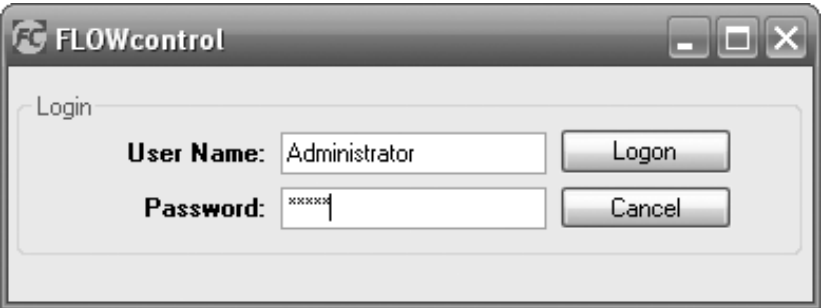


Figure 29. FlowControl™ login window

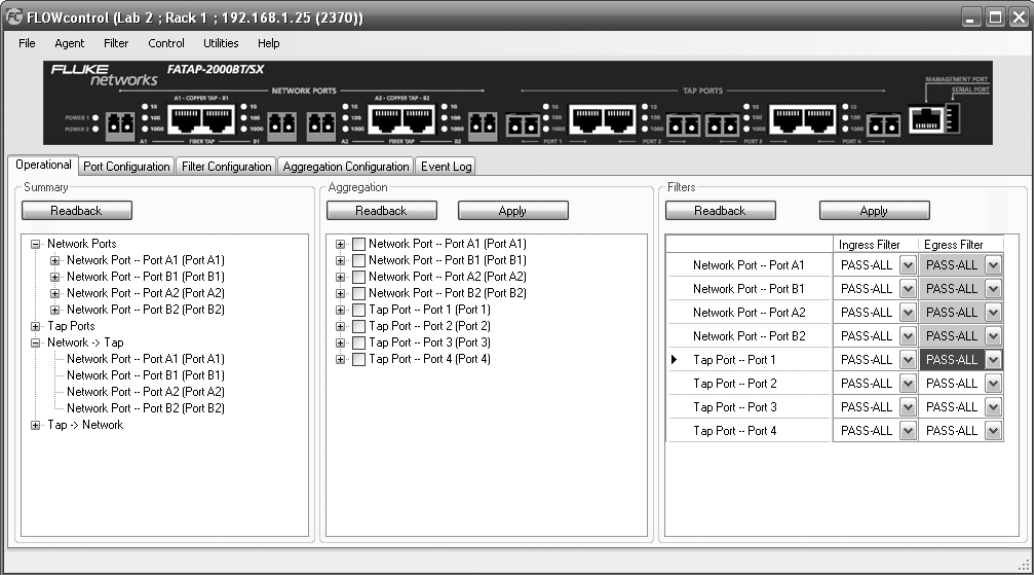
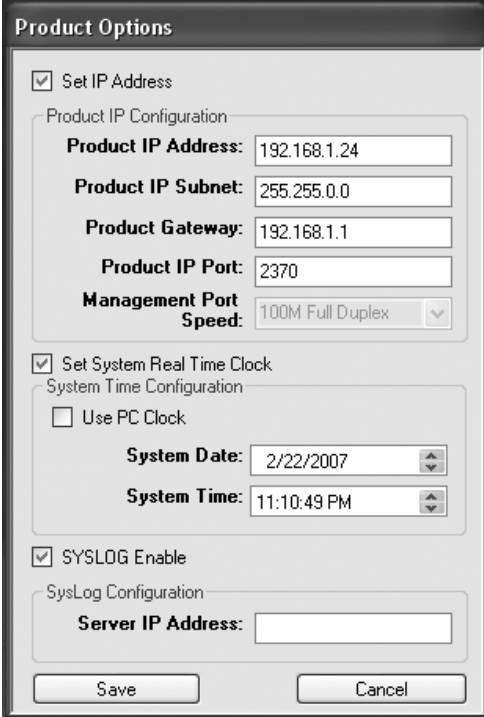


Figure 30. FlowControl™ main window, connected to the FATAP-2000BT/SX

FlowControl™ IP Configuration

10. To correctly integrate your new Filtering Link Aggregation Tap into your network, you must assign it a valid IP address for your network. To do this, select **Utilities > Options** to open the Product Options window.



The screenshot shows the 'Product Options' window with the following settings:

- Set IP Address
 - Product IP Configuration
 - Product IP Address: 192.168.1.24
 - Product IP Subnet: 255.255.0.0
 - Product Gateway: 192.168.1.1
 - Product IP Port: 2370
 - Management Port Speed: 100M Full Duplex
- Set System Real Time Clock
 - System Time Configuration
 - Use PC Clock
 - System Date: 2/22/2007
 - System Time: 11:10:49 PM
- SYSLOG Enable
 - SysLog Configuration
 - Server IP Address: [Empty]

Buttons: Save, Cancel

Figure 31. Product Options window (**Utilities > Options**)

11. Enter the desired IP address and subnet mask. If your network is segmented into multiple subnets, you may provide the Tap with a default gateway (such as the IP address of a local router) to use when communicating with non-local devices. If you don't need a default gateway, leave it blank.
12. Save the new information by clicking on **Save**.
13. Select **Agent > Disconnect** to disconnect from the Filtering Link Aggregation Tap. The FlowControl™ window should now be displayed.

Your Filtering Link Aggregation Tap now has a unique IP address for your network. The agent needs to be updated to allow for communication between your PC and your new Filtering Link Aggregation Tap. When initially created, the agent made use of the default IP address of **192.168.1.1**. You must change this IP address to the new address you assigned to your Filtering Link Aggregation Tap. Please refer to Section 5, Using the FlowControl™ Software, to update the connection agent.

FlowControl™ Networking

USING THE FILTER PRODUCT CONSOLE SOFTWARE

By now, you have created at least one Network Tap, installed the FlowControl™ software on your PC, and assigned an IP address to your Filtering Link Aggregation Tap. Now you are ready to define the routes and filters that will allow you to send tapped network traffic to your monitoring devices.



Figure 32. FlowControl™ main window

CREATING A CONNECTION AGENT

Once your Filtering Link Aggregation Tap has been installed and correctly configured with an IP address, you must create an agent on your PC using the FlowControl™ software. An agent is a local configuration that allows your PC to connect to the Filtering Link Aggregation Tap.

1. To create a new Agent, select **Agent > Add** from the main FlowControl™ window to bring up the Product Configuration window.

FlowControl™ Networking

2. Enter the IP address and Port for your new agent on the Product Configuration window as shown below. Also you must enter a descriptive name for this connection agent. If you are on the same network as your Filtering Link Aggregation Tap, the **Get Product** button retrieves the FATAP/FASTAP-series model information.

The screenshot shows a 'Product Configuration' dialog box. At the top left, there is a checkbox for 'Connect Serially' which is unchecked. Below it is the 'Product Configuration' section with an 'IP Address' field containing '192.168.1.25' and a 'Port' dropdown menu set to '2370'. A 'Get Product' button is located below the port field, and a text box below it displays 'FATAP-2000BT/SX'. The 'Location Configuration' section has a dropdown menu set to 'Lab 2', followed by 'Name' and 'Description' text boxes. The 'Sub Location Configuration' section has a checked checkbox for 'Use Sub Location', a dropdown menu set to 'Rack 1', and 'Name' and 'Description' text boxes. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Figure 33. FlowControl™ Product Configuration window

NOTE

The Location and Sub-Location information will be displayed on the main FlowControl™ window. Using descriptive terms here will allow you to easily keep track of all the Filtering Link Aggregation Tap in your network.

3. When all the information has been entered correctly, select Save. This creates the new agent. Once a new agent is created, the agent names will appear in the list of agents shown on the main FlowControl™ window.

FlowControl™ Networking

- To connect to a Filtering Link Aggregation Tap, expand the list of agents on the Main Window. Select the **Address (Port)** of the desired Filtering Link Aggregation Tap. Select **Agent > Connect**.

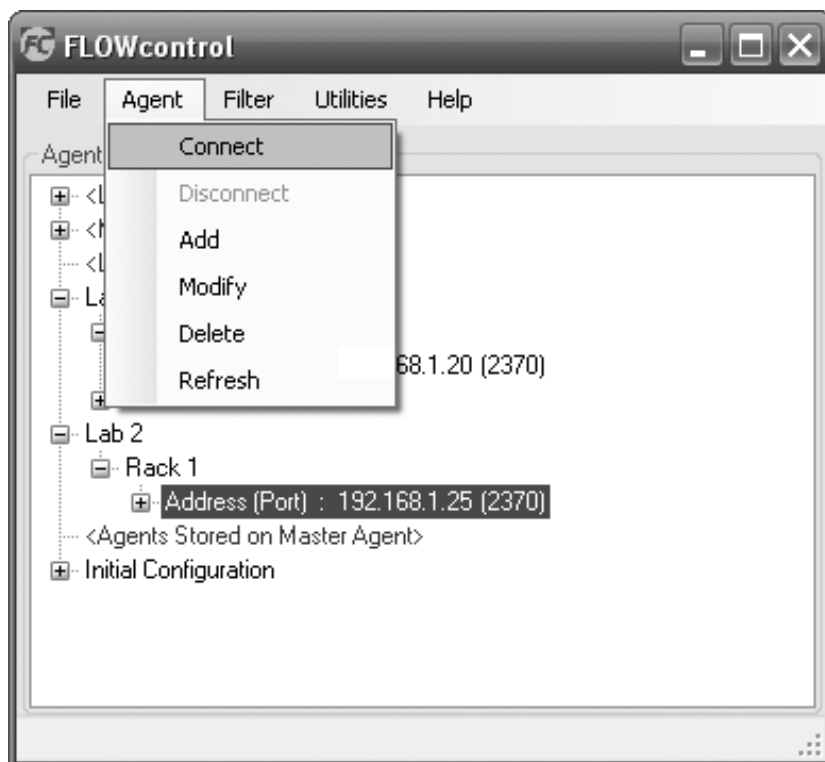


Figure 34. FlowControl™ **Agent** -> **Connect** command

- You will be presented with the login screen. The default username is **Administrator** and the default password is **admin**. After logging in, the FlowControl™ Main Window appears. An image of the Filtering Link Aggregation Tap is displayed across the top of the window. The image displayed will automatically update to the correct image. A FATAP-2000BT/SX is shown in **Figure 36**.

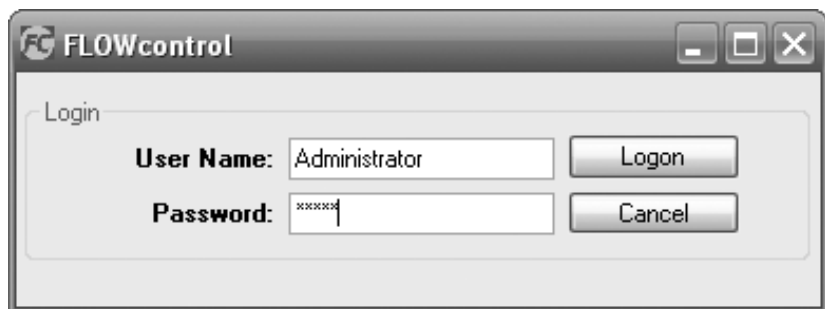


Figure 35. FlowControl™ login window

FlowControl™ Interface

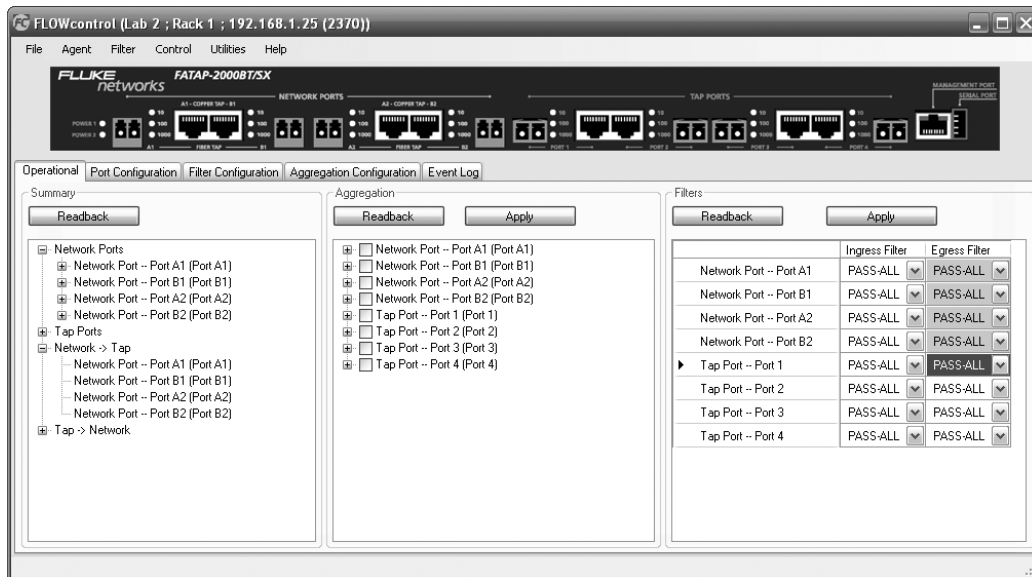


Figure 36. FlowControl™ main window, connected to the FATAP-2000BT/SX

PULL-DOWN MENUS

Upon logging in, the user is presented with the main FlowControl™ window. Six pull-down menus that control basic functions are always available across the top of the FlowControl™ main window. The pull-down menus — **File**, **Agent**, **Filter**, **Control**, **Utilities**, and **Help** — are described in this section.

FILE PULL-DOWN MENU

The **File** pull-down has one option, **Exit**, which closes FlowControl™.



Figure 37. FlowControl™ File pull-down menu

FlowControl™ Interface

AGENT PULL-DOWN MENU

The Agent pull-down allows the user to open and close the connection between the PC and the Filtering Link Aggregation Tap.

Agent > Connect / Disconnect



Figure 38. FlowControl™ Agent pull-down menu

FILTER PULL-DOWN MENU

The **Filter** pull-down is used with the **Filter Configuration** tab to open, save, import and export filters. External filter files are stored as *.rec files (default file is filt.rec) and can only be used by the FlowControl™ software application. By exporting your filter definitions to a file, you could reuse them when you connected to another Filtering Link Aggregation Tap device.



Figure 39. FlowControl™ Filter pull-down menu

Filter > Open and **Save** are used to open and save both basic and advanced filters. These selections are only available when the **Filter Configuration > Basic** or **Advanced** tab is selected.

Filter > Import is used load filters saved on your PC. **Filter > Export** is used save the filters you create on your PC.

Filter > Open / Save / Filter Definitions > Import / Export to File

FlowControl™ Interface

CONTROL PULL-DOWN MENU

The **Control** pull-down allows the user to apply new configuration settings to the connected Filtering Link Aggregation Tap or readback the current settings from the connected Filtering Link Aggregation Tap. The configuration settings in question are dictated by the tab selected (Operational, Port Configuration, Filter Configuration, etc).

Control > Apply / Readback



Figure 40. FlowControl™ **Control** pull-down menu

UTILITIES PULL-DOWN MENU

The **Utilities** pull-down allows the user to customize the connected Filtering Link Aggregation Tap. Selecting **Utilities > Upgrade** allows the user to upgrade the operational software files used by the Filtering Link Aggregation Tap. The user may select to upgrade files for the microprocessor or filter engine. These actions should only be taken at the direction of Fluke Networks Technical Support personnel.



Figure 41. FlowControl™ **Utilities** pull-down menu

Selecting **Utilities > Options** allows the user to change the IP address of the connected Filtering Link Aggregation Tap, direct the event log (syslog) to an external destination, require login access be granted locally from the Filtering Link Aggregation Tap, and define the value of the time stamps applied to event log entries. The system data and time are based on your PC's date and time. The user can adjust time stamps if desired (e.g., EST vs. GMT).

FlowControl™ Interface

Utilities > Options

The screenshot shows a window titled "Product Options" with the following configuration options:

- Set IP Address
 - Product IP Configuration
 - Product IP Address: 192.168.1.24
 - Product IP Subnet: 255.255.0.0
 - Product Gateway: 192.168.1.1
 - Product IP Port: 2370
 - Management Port Speed: 100M Full Duplex
- Set System Real Time Clock
 - System Time Configuration
 - Use PC Clock
 - System Date: 2/22/2007
 - System Time: 11:10:49 PM
- SYSLOG Enable
 - SysLog Configuration
 - Server IP Address: [Empty field]

Buttons: Save, Cancel

Figure 42. Product Options window (Utilities > Options)

The **Utilities > User Accounts** option allows the user to define new login accounts, modify existing accounts, and add personal contact information to existing accounts. For each account, the Administrator can define access rights. In this manner, the Administrator can limit what configuration options are available to certain login accounts.

FlowControl™ Interface

Utilities > User Accounts

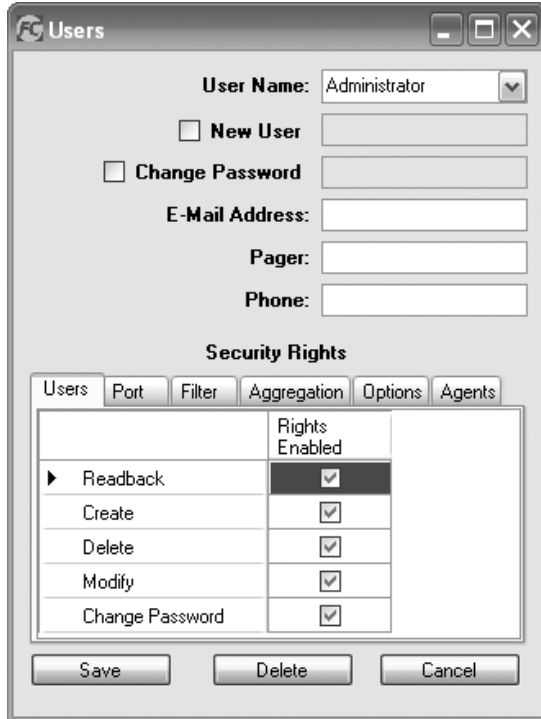


Figure 43. User Accounts window (Utilities > User Accounts)

HELP PULL-DOWN MENU

The **Help** menu provides links to information that may assist you while you are using your Filtering Link Aggregation Tap.

Help > About / Quick Connect Guide / User Guide / Website}

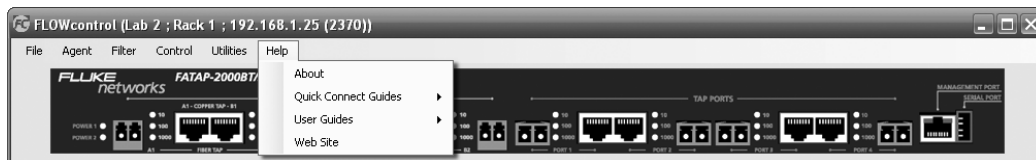


Figure 44. FlowControl™ Help pull-down menu

FlowControl™ Interface

CONFIGURATION TABS

OPERATIONAL TAB

From the Operational Tab, the user can check the current status of the **NETWORK PORT** and **TAP** ports available on the connected Filtering Link Aggregation Tap by clicking the **Readback** button. The user must click Readback to view the status of the connected Filtering Link Aggregation Tap. The user can change the configuration by making changes and clicking the **Apply** button. The window is split into three sections: Summary, Aggregation, and Filters.

The Summary section allows the user to visualize the number of network and tap/monitor ports available. Ports on the Filtering Link Aggregation Tap are not configurable – each port is a part of a **NETWORK PORT** or it is a **TAP** port. **NETWORK PORTS** consist of **A** and **B** ports. All FATAP/FASTAP-series models have **NETWORK PORT 1** with ports **A1** and **B1**; FATAP-2000 series models have a second **NETWORK PORT** with ports **A2** and **B2**.

All models have four tap/monitor ports.

The Aggregation section allows the user to configure the routes that are used by the connected Filtering Link Aggregation Tap. The user can modify the routes by expanding the list of possible routes for a port, then selecting the desired check-boxes. By default, the ports for a single **NETWORK PORT** are routed to each other (these routes cannot be modified). In the figure below, ports **A1** and **B1** make up **NETWORK PORT 1**. Ports **1, 2, 3,** and **4** are the available **TAP** ports.

To route full-duplex traffic from **NETWORK PORT 1** to **TAP 1**, expand **NETWORK PORT A1** and select **TAP 1**. Then expand **NETWORK PORT B1** and select **TAP 1**. Then apply the changes by clicking the Apply button. **TAP 1** is then going to receive the full-duplex network traffic from Network Tap 1. All full-duplex traffic from **NETWORK PORT 1** is then forwarded to **TAP 1**.

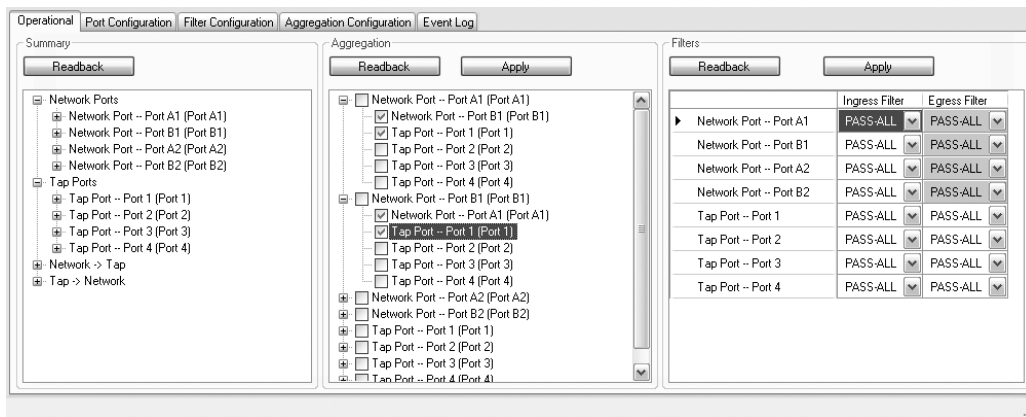


Figure 45. FlowControl™ Operational tab

The Filter section allows the user to apply any defined filter to any of the ports of the connected Filtering Link Aggregation Tap. The user can set the filters to **PASS-ALL**, **PASS-NONE**, or any filter defined on the Filter Configuration tab.

FlowControl™ Interface

PORT CONFIGURATION TAB

The **Port Configuration** tab allows the user to view or modify the port settings for all the available ports of the connected Filtering Link Aggregation Tap. **Port Name**, **Media**, and **Port Speed** can all be selected by the user. FATAP-2000BT/LX and FATAP-2000BT/SX models feature both fiber and copper media availability for all ports, including **NETWORK PORTS**. Other models only have both fiber and copper media available for the **TAP** ports. In each case, **Copper** is the default media type.

To use a fiber connection for a port that allows for both media types, you must access the **Port Configuration** and modify the **Media Preference** to **Fiber**. The Port Type cannot be modified, as it is dependent upon which model of Filtering Link Aggregation Tap you are connected to.

IMPORTANT

*Be sure that the correct speed setting is used consistently across Network Taps. Both the **A** and **B** ports of any **NETWORK PORT** must have the same speed setting. Also be sure to only send an appropriate amount of traffic to any connected monitoring device. A 10BASE-T network analyzer cannot handle all (unfiltered) traffic from both sides of a full-duplex 100BASE-T Network Tap. If you direct more traffic to a device than its link can handle, your monitored traffic will suffer from randomized packet loss.*

The **Readback** button allows the user to view the current settings of the connected Filtering Link Aggregation Tap, while the **Apply** button allows the user to send new configurations to the connected Filtering Link Aggregation Tap.

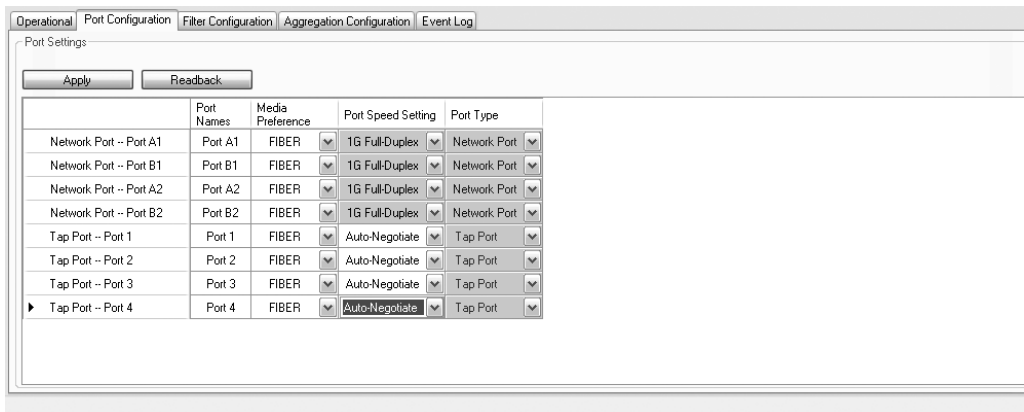


Figure 46. FlowControl™ **Port Configuration** tab

FlowControl™ Interface

FILTER CONFIGURATION TAB

The **Filter Configuration** tab provides the user with many filtering options. The screen is split into two sections. On the left side, **Saved Filters**, **Basic**, and **Advanced** tabs are available. Each allows the user to configure specific kinds of filters. On the right side, the **Filter Functions** section provides a tabular representation of the filters applied to each port as ingress and/or egress filters.

The **Saved Filters** tab allows the user to select a filter that has been defined previously. Any saved filter can be selected, and then applied to one of the ports of the connected Filtering Link Aggregation Tap.

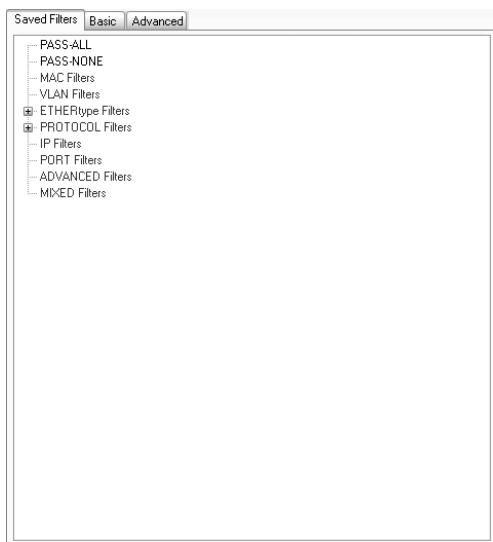


Figure 47. FlowControl™ Port Configuration tab

FlowControl™ Interface

The **Basic** tab, provides the user with many filtering options that may be used on a regular basis. These filters include the **Pass-ALL** and **Pass-NONE** options. These first two options completely enable or completely disable traffic flow to a particular port. The other options require some configuration; selecting one of these options results in a new set of options being displayed for the user.



Figure 48. FlowControl™ **Filter Configuration** -> **Basic** tab

FlowControl™ Interface

The third **Basic** filter option is **MAC Address Filtering**. Selecting this box allows the user to create a configurable filter based on the Media Access Control (MAC) Addresses of the networked computers.

NOTE

The MAC Address is a unique, 48-bit hardware address assigned permanently to every network interface card; it is typically written as 12 hexadecimal digits (e.g., **0F : 98 : AF : 2D : 7C : 11**).

A filter can be defined to Include the traffic that meets the requirements of the filter, or the filter can be defined to Exclude the traffic that meets the requirements of the filter. A filter can be defined for a single MAC address or for a range of MAC addresses.

The screenshot shows the 'Basic' tab of the 'MAC Address' configuration section. It includes checkboxes for 'Pass-ALL Filtering', 'Pass-NONE Filtering', and 'MAC Address Filtering' (which is checked). The 'MAC Address Filtering' option is set to 'INCLUDE'. Below this, there are two sections for 'Source MAC Address' and 'Destination MAC Address'. Each section has a dropdown menu for 'SINGLE' or 'ANY' and a text input field. A direction selector (arrow) is located between the two sections. At the bottom of the configuration area, there are 'Add' and 'Delete' buttons. Below the configuration area is a table with the following columns: 'Lower Range Source MAC', 'Equation', 'Upper Range Source MAC', 'Direction', and 'Lower Range Destination MAC'. The table is currently empty. At the bottom of the interface, there are several other filter options: 'VLAN Filtering', 'Frame Type Filtering', 'Protocol Filtering', 'IP Address Filtering', and 'Port Filtering', all of which are unchecked.

Figure 49. FlowControl™ **Filter Configuration** -> **Basic** -> **MAC Address** tab

The Source Address (the sending machine) and the Destination Address (the intended recipient) can be configured separately. Selecting a Single address of Any applies the filter to all detected traffic. After creating an Include/Exclude- Source-Destination rule, the user can Add the rule. Multiple rules can be created and added. The Arrow selection box allows the user to quickly change a defined rule. By default, the arrow points to the right, which filters for packets from the Source Address to the Destination Address. By selecting the left-pointing arrow, the user can quickly filter for packets sent from the Destination Address to the Source Address.

Lastly, by selecting the arrows pointing in both directions, the user can create a rule that looks for any packet exchanged between the two sets of Addresses — regardless which is the source and which is the destination.

FlowControl™ Interface

The fourth **Basic** Filter option is **VLAN Filtering**. By using this option, the user can create configurable filters that include or exclude traffic based on the VLAN ID assigned to the Source of the network traffic. Rules can be created for single IDs or for a range of IDs. Multiple rules can be created and applied as a single filter.

The screenshot shows the 'Basic' tab of the 'Saved Filters' configuration window. The 'VLAN Filtering' checkbox is checked. Below it, the 'VLAN ID' section has a dropdown menu set to 'INCLUDE' and another dropdown set to 'SINGLE'. There are 'Add' and 'Delete' buttons. Below these is a table with columns for 'Starting Value', 'Equation', and 'Ending Value'. At the bottom, there are checkboxes for 'Frame Type Filtering', 'Protocol Filtering', 'IP Address Filtering', and 'Port Filtering', all of which are currently unchecked.

Figure 50. FlowControl™ **Filter Configuration** -> **Basic** -> **VLAN Filtering** tab

The fifth **Basic** filter option is **Frame Type Filtering**. This option allows the user to create configurable filters to include or exclude specific types of frames. The available frame types include **0x0800 (IP)** and **0x8137 (IPX)**. Using these options, the user can include or exclude IP or IPX traffic as desired.

The screenshot shows the 'Basic' tab of the 'Saved Filters' configuration window. The 'Frame Type Filtering' checkbox is checked. Below it, the 'Frame Type' section has a dropdown menu set to 'INCLUDE' and another dropdown set to '0x0800 (IP)'. Below these are checkboxes for 'Protocol Filtering', 'IP Address Filtering', and 'Port Filtering', all of which are currently unchecked.

Figure 51. FlowControl™ **Filter Configuration** -> **Basic** -> **Frame Type Filtering** tab

FlowControl™ Interface

The sixth **Basic** filtering option is **Protocol Filtering**. This option allows the user to create configurable filters to include or exclude specific network protocols. The network protocols available for filtering include TCP and UDP.



Figure 52. FlowControl™ **Filter Configuration** -> **Basic** -> **Protocol Filtering** tab

FlowControl™ Interface

The seventh **Basic** filtering option is **IP Address Filtering**. This option allows the user to create configurable filters that include or exclude traffic based on the source and destination IP addresses. The configuration of this filter is similar to that of the MAC Address Filtering.

The user can create multiple rules; each rule can include the traffic that meets the filter requirements, or exclude the traffic that meets the filter requirements. The Source and Destination addresses can be a single IP address, or a range of IP addresses. The Arrow selection box allows the user to quickly change a defined rule. By default, the arrow points to the right, which filters for packets from the Source Address to the Destination Address. By selecting the left-pointing arrow, the user can quickly filter for packets sent from the Destination Address to the Source Address.

The screenshot shows the 'Basic' tab of the 'IP Address Filtering' configuration window. It features a list of filter types on the left, with 'IP Address Filtering' selected and set to 'INCLUDE'. Below this, there are fields for 'Source IP Address' and 'Destination IP Address', each with a 'SINGLE' dropdown and an 'ANY' button. A central arrow dropdown is currently set to '---->'. Below these fields are 'Add' and 'Delete' buttons. At the bottom, there is a table with columns for 'Lower Range Source IP', 'Equation', 'Upper Range Source IP', 'Direction', and 'Lower Range Destination IP'. The table is currently empty. At the very bottom, there is a 'Port Filtering' checkbox.

Figure 53. FlowControl™ **Filter Configuration** -> **Basic** -> **IP Address Filtering** tab

Lastly, by selecting the arrows pointing in both directions, the user can create a rule that looks for any packet exchanged between the two sets of Addresses – regardless of which is the source and which is the destination.

FlowControl™ Interface

The last **Basic** filtering option is **Port Filtering**. With this option, the user can create configurable filters that include or exclude traffic based on the Source and Destination Ports. The user can create multiple rules.

Each rule can include the traffic that meets the filter requirements, or exclude the traffic that meets the filter requirements. The Source and Destination can include a single port number or a range of port numbers. The Arrow selection box allows the user to quickly change a defined rule. By default, the arrow points to the right, which filters for packets from the Source Address to the Destination Address. By selecting the left-pointing arrow, the user can quickly filter for packets sent from the Destination Address to the Source Address.

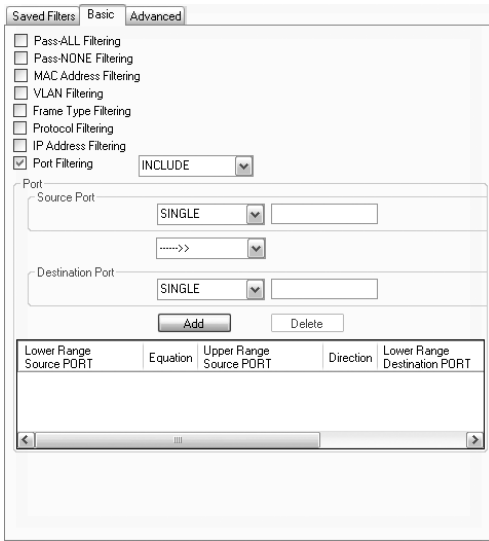


Figure 54. FlowControl™ **Filter Configuration** -> **Basic** -> **Port Filtering** tab

Lastly, by selecting the arrows pointing in both directions, the user can create a rule that looks for any packet exchanged between the two sets of Addresses – regardless of which is the source and which is the destination.

FlowControl™ Interface

The **Advanced** filter tab should only be used to create very specific filters. The **Advanced** tab provides the user with the ability to filter network traffic based on the bit masks of the individual frames.

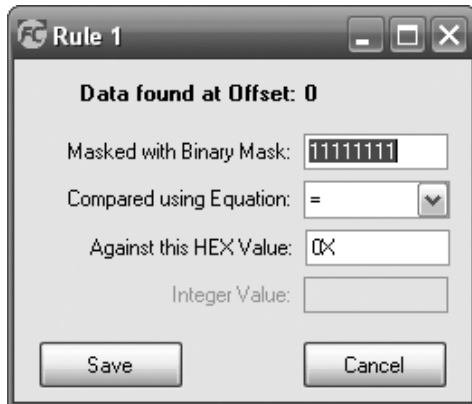


Figure 55. FlowControl™ Filter Configuration -> Advanced rule creation window

Within any frame, the user can add a rule for the value of any byte within the frame. The rules must be defined at offsets of whole words. Rule 1 and Rule 2 both allow for data filters for the bytes at offsets of 0 through 63. In **Figure 55**, a filter has been added that requires the fifth byte of data (offset by 4 bytes) must represent a value of **0x1A** or less. To add such a rule, select the desired byte, right click, and then select **Add**.

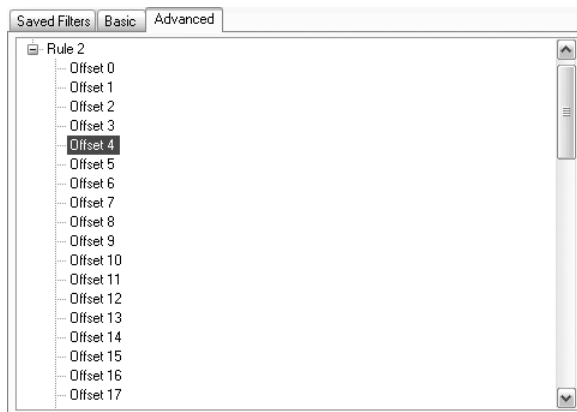


Figure 56. FlowControl™ Filter Configuration -> Advanced tab

The Binary Mask can be used to limit the filter to consider only a portion of the selected byte. A "1" in the Binary Mask includes that bit against the filter value, while a "0" excludes that bit from consideration. For example, a Binary Mask of "00001111" would result in the last four bits of the selected byte being compared to the value of **0x1A**. A single filter can be defined for each byte. Before creating an Advanced filter, be sure you understand the structure of the data frames that you would like to filter.

NOTE

Refer to Appendix A for a closer look at the structure of some standard frames.

FlowControl™ Interface

On the right side of the **Filter Configuration** tab is the **Filter Functions** section. This section allows the user to apply a Saved, Basic, or Advanced filter, defined on the left side of the window to any appropriate port. **NETWORK PORTS** can only have Ingress Filters applied, whereas **TAP** ports can have either Ingress and/or Egress Filters applied.

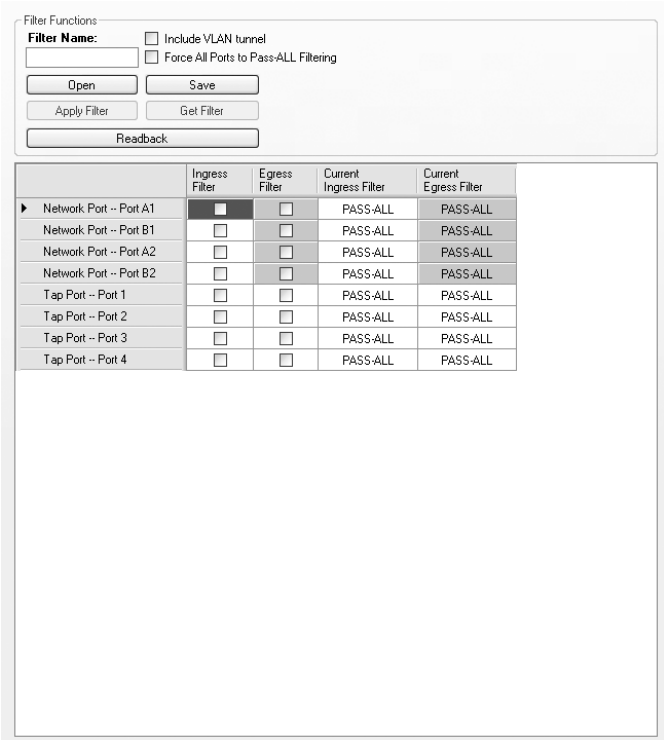


Figure 57. FlowControl™ **Filter Functions** window

FlowControl™ Interface

AGGREGATION CONFIGURATION TAB

The Aggregation Configuration tab allows the user to modify the routes used by the Filtering Link Aggregation Tap. By default, the **A** and **B** ports of any **NETWORK PORT** are routed to each other. This setting cannot be changed, or else the **NETWORK PORT** would cause a break in the network. The Filter Product Console software does not allow the user to make this change. The **Readback** button allows the user to view the current aggregation configuration. After making changes, the user must click the **Apply** button for the changes to take effect.

The user can also create routes from any **NETWORK PORT** to any **TAP** port. Traffic from a **NETWORK PORT** can be routed to multiple **TAP** ports if desired. Additionally, traffic from multiple **NETWORK PORT** can be routed to a single **TAP** port. When connected to an FATAP-2000 series model, all four **NETWORK PORTS** — **A1**, **B1**, **A2**, and **B2** — could be routed to a single **TAP** port if desired.

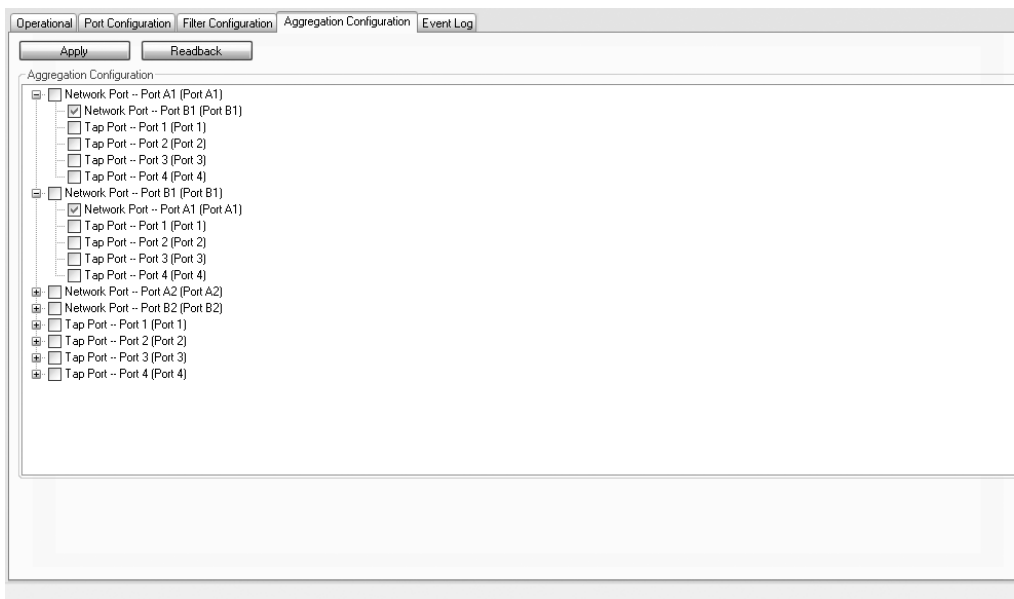


Figure 58. FlowControl™ Aggregation Configuration tab

When routing **NETWORK PORTS** to **TAP** ports, be aware of the connection speed limitations on the devices connected to the **TAP** port. If four 1000BASE-T Network Tap ports are routed to a single 100BASE-T monitoring device, you may experience random packet loss. Random packet loss may lead to inconsistent network monitoring results.

FlowControl™ Interface

EVENT LOG TAB

The **Event Log** tab allows the user to quickly monitor any actions or events that have occurred with the connected Filtering Link Aggregation Tap. Each entry in the event log captures the time of the event, the user who made the change, the IP address of the Filtering Link Aggregation Tap, and a brief description of the event itself. This information allows the user to track any changes that may have been made to the connected Filtering Link Aggregation Tap.

Event Time	User	Event Facility	Event Severity	Event Description
Feb 17 13:31:55	NO USER	17	1	192.168.1.28 FATAP-2000BT/SX: Power Reset
Feb 17 13:50:20	NO USER	17	1	192.168.1.28 FATAP-2000BT/SX: Power Reset
Feb 17 13:54:46	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 1A
Feb 17 13:54:48	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 1B
Feb 17 13:54:49	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 2A
Feb 17 13:54:51	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 2B
Feb 17 13:54:52	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 1
Feb 17 13:54:54	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 2
Feb 17 13:54:55	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 3
Feb 17 13:54:57	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 4
Feb 17 13:54:58	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Memory Allocation Change
Feb 17 13:54:58	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Memory Allocation Change
Feb 17 13:54:58	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Memory Allocation Change
Feb 17 13:54:59	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Memory Allocation Change
Feb 17 13:55:25	NO USER	17	1	192.168.1.25 FATAP-2000BT/SX: Firmware Upgrade
Feb 17 13:55:32	NO USER	17	1	192.168.1.25 FATAP-2000BT/SX: Firmware Upgrade
Feb 17 13:56:19	NO USER	17	1	192.168.1.25 FATAP-2000BT/SX: Power Reset
Feb 17 13:56:57	Administrator	17	1	192.168.1.25 FATAP-2000BT/SX: Administrator: Port Media/Speed Change on Port 1A

Figure 59. FlowControl™ Event Log tab

The event log will also alert the user to any operating errors that may have been encountered during the normal operation of the Filtering Link Aggregation Tap.

FlowControl™ Filtering

EXAMPLE USE OF FILTER PRODUCT CONSOLE: PRINTER TRAFFIC

As an example, the following steps outline how to: create a network tap; create a filter that passes only traffic being sent to a known destination; and route the filtered traffic to a connected monitoring device.

In this example, we are interested in monitoring the network traffic being sent to a network printer. The printer has a fixed IP address of **10.10.5.5**.

NOTE

*This section outlines the procedure to configure a hypothetical network **NETWORK PORT**. This information is presented only to offer an example of how you could create a useful Network Tap. This exact procedure may not apply to your network.*

The example network is a 100BASE-T network, and we will use a FATAP-2000BT Filtering Link Aggregation Tap. The first thing we need to do is physically create the Network Tap. The network printer is originally connected to a 100BASE-T LAN switch. Disconnect the printer from the LAN Switch, and create the Network Tap.

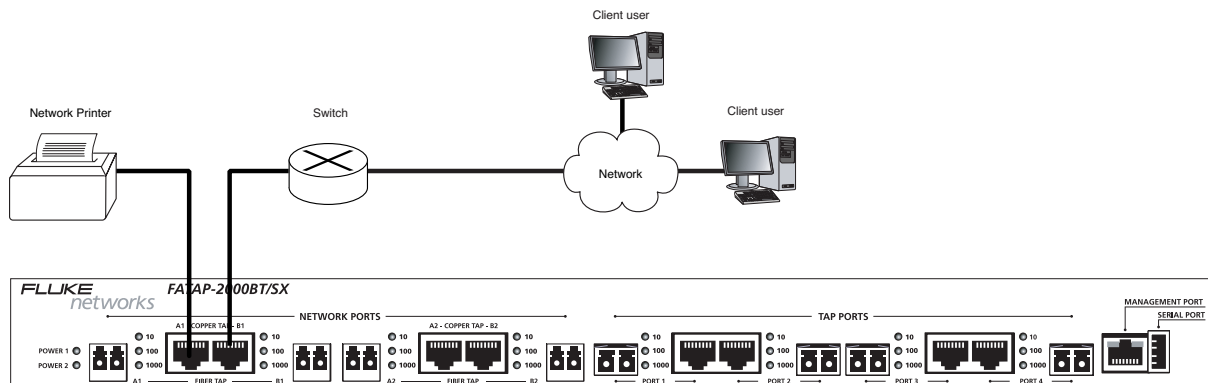


Figure 60. FATAP-2000BT/SX network printer application

FlowControl™ Filtering

Once the Network Tap has been created, the Network PCs can access the printer just like normal. The Network Tap is passive and will not disrupt the network in any way. Next, connect the monitoring device, a 10BASE-T half-duplex LAN analyzer to, in this case, **TAP 1**. Once all the physical connections have been made and verified, you are ready to create the route and apply the filter.

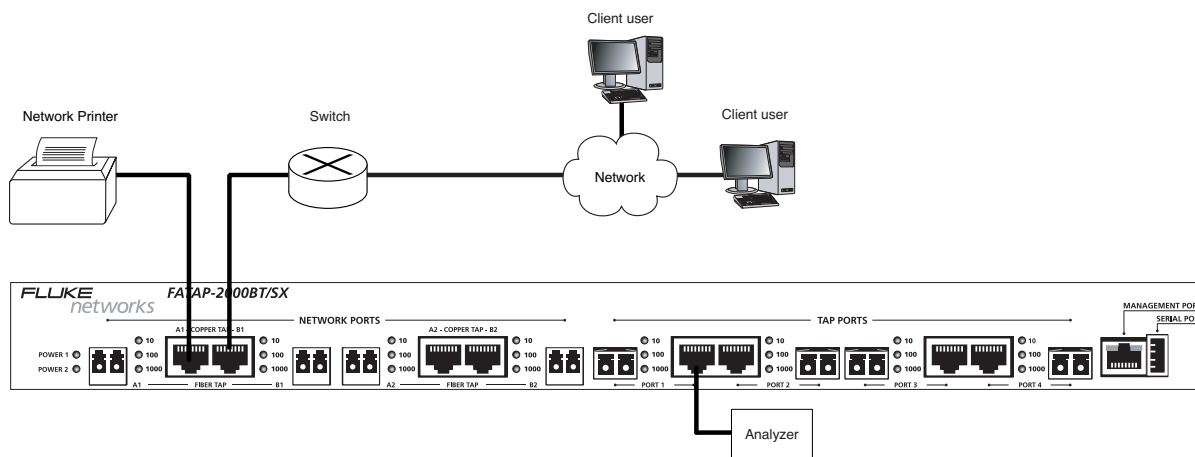
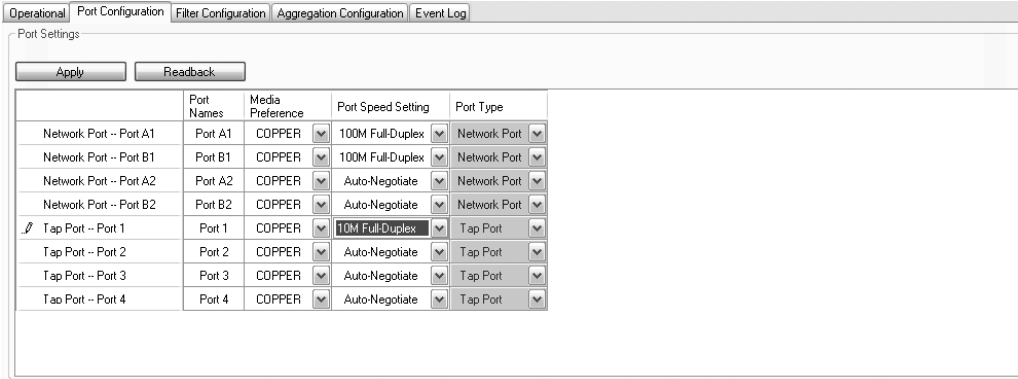


Figure 61. FATAP-2000BT/SX network printer application with network analyzer

FlowControl™ Filtering

To create the route, connect your PC to the Filtering Link Aggregation Tap, log in to the **Filter Product Console**, and click on the **Port Configuration** tab. By default, the Media Preference for each port is **Copper**, and the port speed is set to **Auto-Negotiate**. For this example, set the port speed to **100BASE-T Full-Duplex** for the Network Tap, and **10BASE-T Full-Duplex** for the **TAP** port. Once the changes have been made, click **Apply**.



The screenshot shows the 'Port Configuration' tab in the Filter Product Console. It features a 'Port Settings' section with 'Apply' and 'Readback' buttons. Below is a table with columns for Port Names, Media Preference, Port Speed Setting, and Port Type. The 'Tap Port -- Port 1' row is highlighted, showing its speed setting is '10M Full-Duplex'.

Port Names	Media Preference	Port Speed Setting	Port Type
Network Port -- Port A1	COPPER	100M Full-Duplex	Network Port
Network Port -- Port B1	COPPER	100M Full-Duplex	Network Port
Network Port -- Port A2	COPPER	Auto-Negotiate	Network Port
Network Port -- Port B2	COPPER	Auto-Negotiate	Network Port
Tap Port -- Port 1	COPPER	10M Full-Duplex	Tap Port
Tap Port -- Port 2	COPPER	Auto-Negotiate	Tap Port
Tap Port -- Port 3	COPPER	Auto-Negotiate	Tap Port
Tap Port -- Port 4	COPPER	Auto-Negotiate	Tap Port

Figure 62. FlowControl™ **Port Configuration** tab: Network Printer Application

FlowControl™ Filtering

Next, create the route by clicking on the **Aggregation Configuration** tab. Ensure that both ports of **NETWORK PORT 1**, ports **A1** and **B1**, are configured to forward traffic to **TAP 1** as shown in **Figure 63** below. Once you have made the configuration changes, click **Apply**.

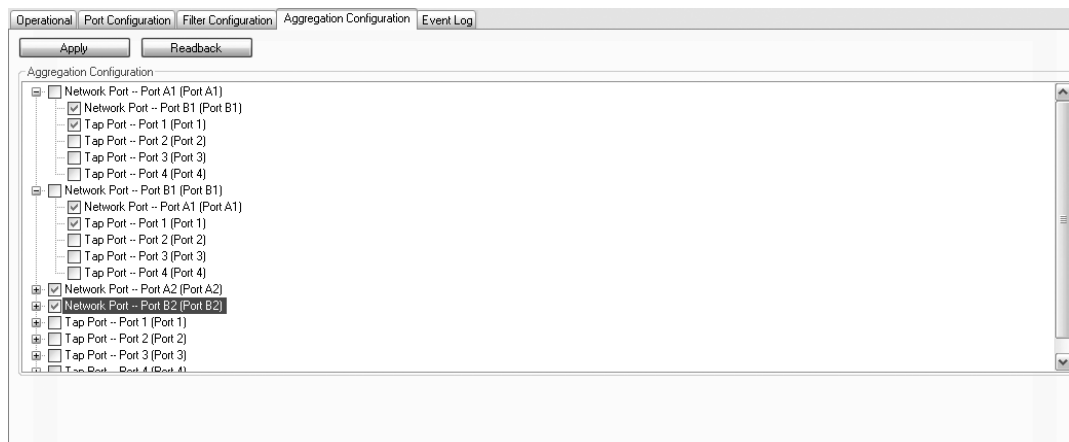
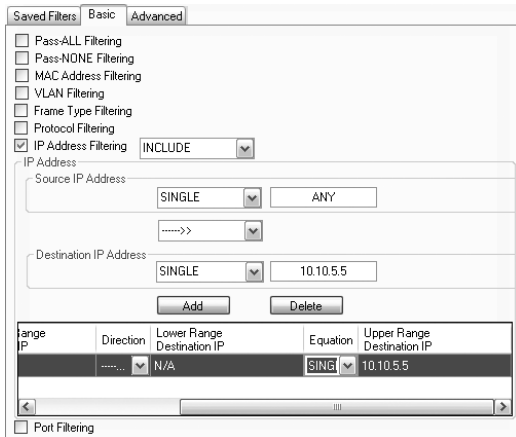


Figure 63. FlowControl™ **Aggregation Configuration** tab: Network Printer Application

Now, a copy of the network traffic should be flowing to the connected LAN Analyzer. However, the 10BASE-T half-duplex LAN Analyzer connection cannot support all of traffic on the full-duplex 100BASE-T network. To prevent this over-subscription problem, a filter can be created that sends only the traffic of interest to the LAN Analyzer.

FlowControl™ Filtering

To create such a filter, click on the **Filter Configuration** tab. Select the **Basic** tab, and then check the **IP Address Filtering** check-box. To view only that traffic that is being sent to the network printer, configure the filter so that it includes traffic sent from any source IP address to the destination IP address of the network printer. Once you have configured the rule, click **Add**. Under the **Filter Functions** section on the right side of the window, name the new filter **printer_traffic** and click **Save**.



Range IP	Direction	Lower Range Destination IP	Equation	Upper Range Destination IP
	----->	N/A	SING	10.10.5.5

Figure 64. FlowControl™ **Filter Configuration** tab: Network Printer Application

Now the new filter is available, and can be applied to the various ports. Click on the **Operational** tab. The new **printer_traffic** filter can be applied to the **NETWORK PORT A1** and **NETWORK PORT B1** from the pull-down menu under the **Filters** section. Once configured correctly, click the **Apply** button. Also verify that the Aggregation and Summary sections show the correction information by clicking the **Readback** button for each section.

The LAN Analyzer should now only receive the traffic being sent to the network printer.

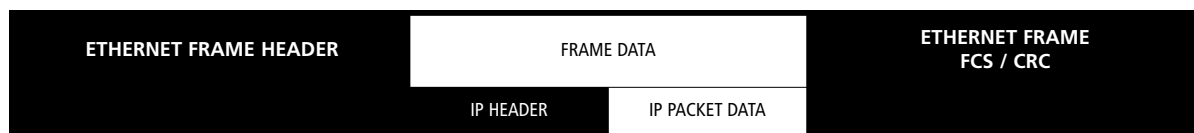
Appendix Frame and Data Packets

Description of Frames and Packets

This section provides a description of an Ethernet frame and an Internet Protocol (IP) packet to aid the users with the creation of Advanced bit mask filters. Advanced Filters are discussed on page 48 of this document. Typically, Layer 2 Ethernet frames are used to transport Layer 3 IP packets.

The table below shows how an IP packet is encapsulated inside an Ethernet frame. Not all network traffic is the same, and there are many available networking protocols. Because many networks rely upon Ethernet at Layer 2 and IP at Layer 3, a brief description of each is provided in this appendix.

ETHERNET FRAME ENCAPSULATION OF AN IP PACKET



On the next few pages, a more detailed description of the various fields that make up Ethernet frames and IP packets is provided. There are many types of Ethernet in use throughout the world; the most common types are Ethernet II and IEEE 802.3, although IEEE 802.3 SNAP and wireless IEEE 802.11 are also in use. The IP packet is the basic packet format used to transmit and receive data across local and wide-area networks. Both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) messages are sent via IP packets.

The Filter Product Console software allows the user to create Advanced Filter rules that are applied to the first 64 Bytes of any frame or packet. A full Ethernet frame header consists of 16 Bytes (only 13 for the older and shorter Ethernet II format). An IP packet header consists of an additional 23 Bytes. To create a filter that checks the Type of Transfer Protocol field for IP packets encapsulated in Ethernet frames, an offset of 25 Bytes would be used. An offset of 25 Bytes means the filter would skip over the first 16 Bytes of Ethernet frame (the entire header), and then skip over the first 9 Bytes of the IP packet header. The Type of Transfer Protocol field is the 10th Byte of the IP packet header, which means it has an offset of 9 Bytes from the beginning of the IP header. The Type of Transfer Protocol field is also on the 26th Byte of the Ethernet frame. Right-clicking on the offset of 25 Bytes on the Filter Product Console's Advanced Filter screen, and selecting **Add**, allows for the creation of a rule for the content of the Type of Transfer Protocol (in this case).

Using a similar method, it is possible to create an Advanced Filter that examines any combination of bits, fields, and values within the first 64 Bytes of any transmitted package. Before creating such a filter, you must first understand the format of the protocol(s) in use.

Appendix Frame and Data Packets

ETHERNET FRAME FORMATS

- Bytes 0–13 are the Data Link Header. This is used in all formats.
- Bytes 14–16 are the Logical Link Control (LLC) Header. This is used in the IEEE 802.3, IEEE 802.3 SNAP, and IEEE 802.11 formats.
- Bytes 17–21 are the Sub-Network Access Protocol (SNAP). This is used in IEEE 802.3 SNAP format only.

NOTE

Bytes 17 through 21 can be used to transmit the Sub-Network Access Protocol (SNAP) header. If this is used (only in IEEE 802.3 SNAP), bytes 17–19 are the Vendor's Code, while Bytes 20 and 21 are the frame's Ethertype. Using this format, the data will begin with Byte 22.

BIT-MAPPING OF AN ETHERNET FRAME

BYTE 0		BYTE 1		BYTE 2		BYTE 3	
Bits 0–3	Bits 4–7	Bits 8–11	Bits 12–15	Bits 16–19	Bits 20–23	Bits 24–27	Bits 28–31
DESTINATION MAC ADDRESS: BYTES 0–5							
BYTE 4		BYTE 5		BYTE 6		BYTE 7	
Bits 32–35	Bits 36–39	Bits 40–43	Bits 44–47	Bits 48–51	Bits 52–55	Bits 56–59	Bits 60–63
DESTINATION MAC ADDRESS: BYTES 0–5				SOURCE MAC ADDRESS: BYTES 6–11			
BYTE 8		BYTE 9		BYTE 10		BYTE 11	
Bits 64–67	Bits 68–71	Bits 72–75	Bits 76–79	Bits 80–83	Bits 84–87	Bits 88–91	Bits 92–95
SOURCE MAC ADDRESS: BYTES 6–11							
BYTE 12		BYTE 13		BYTE 14		BYTE 15	
Bits 96–99	Bits 100–103	Bits 104–107	Bits 108–111	Bits 112–115	Bits 116–119	Bits 120–123	Bits 124–127
FRAME LENGTH [does not include preamble, CRC, DLC Addresses, or the Length Field itself; the range is 64–1518 Bytes, not used in Ethernet II format.]				DESTINATION SERVICE ACCESS POINT (DSAP) [not used in Ethernet II format]		SOURCE SERVICE ACCESS POINT (SSAP) [not used in Ethernet II format]	
BYTE 16		BYTE 17*		BYTES 18 ~ 1497			
Bits 128–131	Bits 132–135	Bits 136–139	Bits 140–143	Bits 144 ~ 33rd-from-Last			
CONTROL [specifies the type of Frame being sent; not used in Ethernet II format]		DATA [where IP header data may begin]					
4TH-TO-LAST BYTE		3RD-TO-LAST BYTE		2ND-TO-LAST BYTE		LAST BYTE	
Last 32 Bits							
FRAME CHECK SEQUENCE (FCS) [also known as CYCLICAL REDUNDANCY CHECK (CRC)]							

Appendix Frame and Data Packets

BIT-MAPPING OF AN IP PACKET

BYTE 0		BYTE 1		BYTE 2			BYTE 3
Bits 0–3	Bits 4–7	Bits 8–11	Bits 12–15	Bits 16–19	Bits 20–23	Bits 24–27	Bits 28–31
IP VERSION	IP HEADER LENGTH	TYPE OF SERVICE [not used]		TOTAL LENGTH OF DATAGRAM [header & data]			
BYTE 4		BYTE 5		BYTE 6		BYTE 7	
Bits 32–35	Bits 36–39	Bits 40–43	Bits 44–47	Bits 48–51	Bits 52–55	Bits 56–59	Bits 60–63
16-BIT PACKET IDENTIFICATION NUMBER				ROUTING FLAGS	FRAGMENTATION OFFSET [used when a router fragments the original packet into multiple packets]		
BYTE 8		BYTE 9		BYTE 10		BYTE 11	
Bits 64–67	Bits 68–71	Bits 72–75	Bits 76–79	Bits 80–83	Bits 84–87	Bits 88–91	Bits 92–95
TIME-TO-LIVE (TTL) [number of permitted router hops]		TYPE OF TRANSFER PROTOCOL USED		16-bit HEADER CHECKSUM			
BYTE 12		BYTE 13		BYTE 14		BYTE 15	
Bits 96–99	Bits 100–103	Bits 104–107	Bits 108–111	Bits 112–115	Bits 116–119	Bits 120–123	Bits 124–127
32-BIT SOURCE IP ADDRESS							
BYTE 16		BYTE 17*		BYTE 18		BYTE 19	
Bits 128–131	Bits 132–135	Bits 136–139	Bits 140–143	Bits 144–147	Bits 148–151	Bits 152–155	Bits 156–159
32-bit DESTINATION IP ADDRESS							
BYTE 20		BYTE 21		BYTE 22		BYTE 23	
Bits 160–163	Bits 164–167	Bits 168–171	Bits 172–175	Bits 176–179	Bits 180–183	Bits 184–187	Bits 188–191
OPTIONS [if any] for the IP PACKET							
BYTE 24		BYTE 25		BYTE 26		BYTE 27	
Bits 192–195	Bits 196–199	Bits 200–203	Bits 204–207	Bits 208–211	Bits 212–215	Bits 216–219	Bits 220–223
START OF TRANSMITTED DATA							

Appendix HyperTerminal

HyperTerminal Commands

In FlowControl IP Configuration section, starting on page 16, only the commands to configure the IP address of the Filtering Link Aggregation Tap are discussed. As shown in that section, you may use the supplied serial cable and a PC equipped with a DB-9 serial port to configure your Filtering Link Aggregation Tap. The connection between the PC and the Tap is depicted below in **Figure 65**.

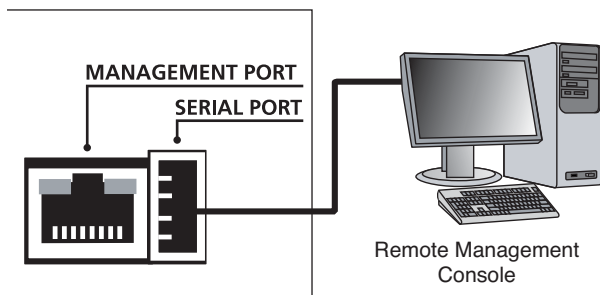


Figure 65. FATAP / FASTAP-series serial connection with a PC device

To ensure proper communication, the HyperTerminal connection must use the same configuration settings as the Filtering Link Aggregation Tap. Through HyperTerminal, configure the COM port on the PC as show below in **Figure 66**.

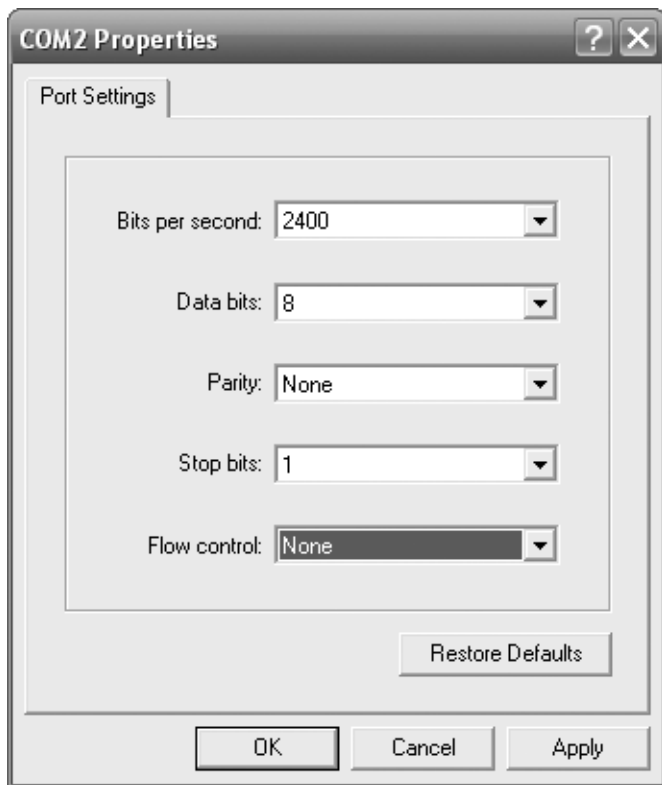


Figure 66. HyperTerminal COM Properties window

Appendix HyperTerminal

Once you have connected, many commands are available for use. In the following table, a brief description of the each of the commands and configuration options is provided.

NOTE

The default user name is **Administrator** and the default password is **admin**.

HYPERTERMINAL COMMANDS

COMMAND	SYNTAX	FUNCTION
CLEAR SYSLOG	—	Clears the system log record stored on the Filtering Link Aggregation Tap.
EXIT	—	Terminates the HyperTerminal session.
HELP	—	Shows list of available commands and options.
QUIT	—	Terminates the HyperTerminal session.
SET IP ADDRESS	x.x.x.x	Sets the IP address of the Filtering Link Aggregation Tap.
SET IP BROADCAST	x.x.x.x	Sets the broadcast address used by the Filtering Link Aggregation Tap (typically the 255 node)
SET IP DEFAULT GATEWAY	x.x.x.x	Sets the IP address of the default gateway used by the Filtering Link Aggregation Tap to access non-local networks (typically, a local router)
SET IP SUBNET	x.x.x.x	Sets the IP subnet mask used for the local network (typical Class C network uses 255 . 255 . 255 . 0)
SET TCP PORT	xxxxxx	Sets the TCP port number used by the Filtering Link Aggregation Tap. Port numbers range from 1 to 65535, with many ports being reserved for well-known uses: port 21 is used for FTP and port 80 is used for HTTP. If you select a well-known port number, you may experience minor network problems.
SHOW IP	—	Shows the current settings for the IP address, subnet mask, and default gateway.

Appendix Product Specifications

GENERAL SPECIFICATIONS

FEATURE	SPECIFICATION
NETWORK PORT PHYSICAL CONNECTIONS BT COPPER PORTS SX FIBER PORTS LX FIBER PORTS	RJ45 connector; CAT5E cable; 10/100/1000Mbps (auto-sensing) short-haul, multi-mode fiber; 50 or 65 microns; 1000Mbps long-haul, single-mode fiber; 9 microns; 1000Mbps
TAP / MONITOR PORT PHYSICAL CONNECTIONS COPPER (BT) PORTS FIBER (SX/LX) PORTS	RJ45 connector; CAT5E cable; 10/100/1000Mbps (auto-sensing) LC connector allowing for SX or LX; 1000Mbps
NOMINAL POWER REQUIREMENTS	Two internal, redundant 100–240V AC at 1.5A power supplies Certified by UL, CUL, and TUV; CE approved
OPERATING TEMPERATURE	0° to 40°C (32° to 104°F)
STORAGE TEMPERATURE	-30° to 65°C (-22° to 149°F)
HUMIDITY	Less than 95% non-condensing
DIMENSIONS	(H) 76mm x (W) 457mm x (D) 229mm (H) 3.00" x (W) 18.00" x (D) 9.00"
WEIGHT	unit: 3.18kg (7lbs)

Care and Maintenance

Each Filtering Link Aggregation Tap is designed to be maintenance free. Treat it with care to ensure the best performance. The suggestions below will help you fulfill the obligations of the warranty and enjoy the tap for many years.

AVOIDING ROUGH HANDLING

Although each Filtering Link Aggregation Tap model can absorb shock and vibration, avoid dropping it. If you must ship the tap, use the original packaging or the ruggedized transit case.

CLEANING CAREFULLY

To clean your Filtering Link Aggregation Tap, use a soft, slightly damp cloth. To remove any stains, use a mild soap. Never use detergents, solvents, or abrasive cleaners on the tap.

PROVIDING ADEQUATE VENTILATION

Always place the Filtering Link Aggregation Tap in an area where there is sufficient space in front and behind the unit to provide adequate ventilation.

SAFETY INFORMATION

To avoid possible electric shock or personal injury, the following general safety precautions must be observed during all phases of operation, service, or repair of your Filtering Link Aggregation Tap. Failure to comply with these precautions or with specific warnings in this guide violates the safety standards of design, manufacture and intended use of the tap. Fluke Networks assumes no liability for the customer's failure to comply with these requirements.

WARNINGS

If this product is used in a manner not specified by the manufacturer, the protections provided by the product may be impaired. Do not use the tap if it is damaged. Before using, inspect the case. Look for cracked or missing case parts. Pay particular attention to the insulation surrounding the connectors.

Do not operate the tap around explosive gas, vapor or dust. When servicing the tap, use specified replacement parts only. Do not connect a telephone line to the tap. Provide adequate ventilation in front of and behind the tap.

SERVICE AND ADJUSTMENT

Service and adjustment of your Filtering Link Aggregation Tap should be performed by trained Fluke Networks service personnel only. If you experience a problem with the tap, visit the Fluke Networks website at <http://www.flukenetworks.com>, send email to support@flukenetworks.com, or contact your nearest Fluke Networks Service Center to report the problem (see **Contacting Fluke Networks** for a list of telephone numbers).

If the tap requires repair, service center personnel will provide you with shipping information and repair prices. If the tap is covered under warranty, it will be promptly repaired or replaced (at Fluke Networks' option) and returned to you, postage paid, at no charge. See the registration card for warranty terms. If the warranty has lapsed, Fluke Networks will repair the tap for a fixed fee and return it, postage paid, to you.

Contacting Fluke Networks

To contact Fluke Networks, visit our website at <http://www.flukenetworks.com/> or send email to support@flukenetworks.com.

For operating assistance in the USA, call **1-800-283-5853**.

To order accessories or to find out the location of the nearest Fluke Networks distributor or service center, call:

- Australia: 61 (2) 8850-3333 or 61 3 9329 0244
- Beijing: 86 (10) 6512-3435
- Brazil: 11 3044 1277
- Canada: 1-800-363-5853
- Europe: +44 1923 281 300
- Hong Kong: 852 2721-3228
- Japan: +81-3-3434-0181
- Korea: 82 2 539-6311
- Singapore: +65-6738-5655
- Taiwan: (886) 2-227-83199
- USA: 1-800-283-5853
- Anywhere in the world: +1-425-446-4519

Visit our website for the latest list of phone numbers.



205 Westwood Ave
Long Branch, NJ 07740
1-877-742-TEST (8378)
Fax: (732) 222-7088
salesteam@Tequipment.NET