



Comtech EF Data is an  
AS9100 Rev B / ISO9001:2000 Registered Company



# *FX Series*

Administrator Guide

Version 6.1.1

**IMPORTANT NOTE:** The information contained in this document supersedes all previously published information regarding this product. Product specifications are subject to change without prior notice.

MN-FXSERIESADM6 Revision 5



## Table of Contents

Table of Contents .....	iii
Table of Figures .....	viii
<b>Using This Document.....</b>	<b>X</b>
Document Organization .....	x
Contacting Product Support .....	xi
FX Series End User License Agreement .....	xii
Patents and Trademarks .....	xiv
Conventions and References .....	xv
Comtech EF Data Warranty Policy.....	xvi
Release Notes .....	xviii
Version 6.1.1 Functionality Enhancements .....	xviii
Version 6.1 Functionality Enhancements.....	xviii
Version 6.0.3 Functionality Enhancements .....	xix
Version 6.0.2 Functionality Enhancements .....	xx
Version 6.0.1 Functionality Enhancements .....	xx
<b>1 Overview - FX Series .....</b>	<b>22</b>
1.1 Stampede FX Series Product Line Update .....	22
1.2 Technologies that Optimize Satellite Bandwidth Acceleration.....	23
1.3 Single-Sided Solution .....	25
1.3.1 Load Balancing via WCCP .....	25
1.3.2 Source IP Preservation .....	25
1.3.3 Connection Management .....	26
1.3.4 QoS with ACM option .....	26
1.3.5 GZIP Compression.....	26
1.3.6 Image Reduction and Smoothing .....	27
1.3.7 Static Caching .....	27
1.3.8 TCP Optimization .....	28
1.4 Two-Sided Solution.....	29
1.4.1 Cache Differencing .....	29
1.4.2 Multiplexing of Large Data Objects .....	29
1.4.3 Microsoft™ Update Caching.....	30
1.4.4 Network Protocol Optimization .....	30
1.4.5 Dynamic Data Deduplication .....	30
1.4.6 Header Compression/Packet Aggregation .....	30
1.4.7 Multicator .....	31
1.5 FX Series ADC Appliance .....	32
1.5.1 Theory of Operation.....	32
1.5.2 Reporting.....	32
1.5.3 Deployment Options.....	32
1.6 FX Series Remote Appliance.....	33
1.6.1 Theory of Operation.....	33
1.6.2 TCP Optimization and Data Compression .....	33
1.6.3 Reporting.....	34
1.6.4 Deployment Options.....	34
1.7 Mesh Networking with the FX Series .....	35
1.7.1 Theory of Operation.....	35
1.7.2 Mesh Capability with two FX Series appliances at each node.....	35
1.8 FX Series Appliances Data Sheet.....	38

1.8.1	Single Sided with the Application Delivery Controller (ADC)	38
1.8.2	Two Sided with the ADC and the Remote	38
1.8.3	FX Series Hardware Specification	39
1.8.4	FX-4010 Physical Description	40
1.8.5	FX-1005 Physical Description	41
1.8.6	FX-1010 Physical Description	43
1.8.7	Hardware Mounting Options for FX Series FX-1005	45
<b>2</b>	<b>Pre-Installation Information</b>	<b>46</b>
2.1.1	Unpacking	46
2.1.2	User Interfaces	46
2.1.3	Documentation	47
2.2	Configure Appliance Management Address - All Installation Patterns	47
<b>3</b>	<b>FX Series Network Installation Patterns</b>	<b>48</b>
3.1	FX Series Installation Pattern (In-Path Bridged)	48
3.1.1	Cable the Appliance	48
3.1.2	Configure the Appliance	48
3.2	FX Series Installation Pattern (Routed)	49
3.2.1	Cable the Appliance	49
3.2.2	Configure the Appliance	49
3.3	FX Series Installation Pattern (WCCP)	50
3.3.1	Cable the Appliance	50
3.3.2	Configure the Appliance	50
3.4	Installation of Two FX Series Appliances in a Mesh Configuration	52
3.4.1	Configure the appliances	52
3.4.2	Mesh installation with Redundancy capability	52
<b>4</b>	<b>FX Series Network Settings</b>	<b>53</b>
4.1	Standard Network Configuration Overview	53
4.2	Basic Network Interfaces	55
4.2.1	Management Interface	55
4.2.2	Auxiliary Interface	56
4.2.3	Management Static Routes	56
4.3	Host Settings	57
4.3.1	Host Networking Settings	57
4.3.2	Host File Entries	58
4.4	In-Path Interface	59
4.4.1	In-Path Interface Definition	59
4.5	LAN Interfaces	61
4.5.1	LAN Interface Definition	61
4.5.2	Configure SNMP Settings	62
4.6	Configuring Quality of Service with ACM	64
4.6.1	Overview	64
4.6.2	Configure Dynamic ACM Parameters	65
4.6.3	QoS Filter Definitions	68
4.6.4	QOS Queue Definitions	70
4.7	FX Series Multicator Overview	73
4.7.1	Theory of Operation	74
4.7.2	Multicator Settings	75
4.7.3	Multicator General Setup (required for all roles)	77
4.7.4	Multicator Controller Configuration Setup	78
4.7.5	Multicator Receiver Configuration Setup	78

4.7.6	Multicator Transmitter Configuration Setup .....	78
4.8	Redundancy.....	79
4.8.1	Redundancy Configuration Settings.....	79
4.8.2	Configuring Key-Exchange .....	80
4.8.3	Example 1:1 redundancy with fail over setup scenario .....	81
4.8.4	Synchronizing Configurations in a WCCP Cluster .....	82
4.9	WCCP .....	83
4.9.1	WCCP Configuration Considerations .....	84
4.9.2	WCCP Cisco Device configuration .....	84
4.9.3	Web Cache Communication Protocol Parameters .....	84
4.9.4	WCCP Router Configuration and Status Monitoring .....	86
4.9.5	WCCP IP Spoofing Configuration for Routers.....	87
4.9.6	WCCP IP Spoofing Configuration for Switches .....	89
4.9.7	LAN and In-Path Interface Requirements for WCCP .....	90
4.9.8	Configuring WCCP on earlier models .....	90
<b>5</b>	<b>FX Series ADC Specific Settings .....</b>	<b>91</b>
5.1	Overview .....	91
5.1.1	General Settings.....	92
5.1.2	Object Retrieval Logging .....	93
5.1.3	Traffic Interception.....	93
5.1.4	System Time .....	94
5.1.5	Software Updates .....	94
5.1.6	Administration .....	94
5.1.7	Other .....	94
5.2	Port Definitions .....	95
5.2.1	In-Path Interface: .....	95
5.2.2	Example Port Definitions .....	96
5.2.3	Setting up an HTTP Forward Proxy .....	96
<b>6</b>	<b>FX Series Remote Specific Settings .....</b>	<b>97</b>
6.1	FX Remote Settings Overview .....	97
6.2	FX Series Remote Configuration Settings.....	98
6.2.1	FX Series Remote General Settings .....	99
6.2.2	System Time .....	99
6.2.3	Traffic Interception.....	99
6.2.4	Administration .....	100
6.2.5	Other .....	100
6.2.6	Configuration Notes .....	101
6.3	FX Series Remote In-Path Interfaces.....	102
6.3.1	Best Practices for Routed Mode Configurations .....	102
6.3.2	Add In-Path Interfaces .....	102
<b>7</b>	<b>FX Series Status .....</b>	<b>105</b>
7.1	FX Series ADC Status .....	105
7.1.1	FX Series ADC Real-Time Monitor .....	105
7.2	QOS Status Monitor.....	108
7.2.1	QOS Status Monitor Options .....	108
7.2.2	QOS Status Matrix .....	109
7.2.3	Modem Status: .....	111
7.2.4	Output Data Rate: .....	111
7.2.5	FX Series ADC Current Statistics.....	112
7.3	FX Series Remote Status .....	116

7.3.1	FX Series Remote Real-Time Monitor .....	116
7.3.2	FX Series Remote Current Status Reports .....	118
<b>8</b>	<b>FX Series Optimization Settings .....</b>	<b>120</b>
8.1	Configure Application Policies .....	120
8.1.1	FX Series Optimization Summary .....	121
8.1.2	Single-Sided Optimizations: .....	121
8.1.3	Two-sided Optimizations .....	121
8.1.4	Authorization Realms.....	122
8.1.5	Web Application Policies .....	124
8.1.6	Authorization realm .....	125
8.1.7	Enable Acceleration .....	125
8.1.8	Caching .....	125
8.1.9	Content Validation.....	125
8.1.10	Image Optimization .....	126
8.1.11	Back-End Server Interface Options .....	127
8.1.12	When Application Policies Take Effect: .....	127
8.2	Web Application Firewall Features .....	128
8.2.1	Buffer Overflow Prevention: .....	128
8.3	Setting up Basic Web Application Policies .....	129
8.3.1	How to Set the Policy Header .....	129
8.3.2	Set Specific Users Access .....	130
8.3.3	Restrict acceleration for specific sites, or users .....	131
8.3.4	Set Specific Optimization Techniques.....	131
8.4	Layer 5 Application Policies .....	132
8.4.1	Certified Applications .....	132
8.4.2	Configuring Other Applications .....	132
8.4.3	Configuring Layer 5 Optimizations .....	133
8.4.4	Layer 5 Protocols.....	134
8.4.5	ToS handling method .....	134
8.4.6	Layer 5 Acceleration - Theory of Operation.....	135
<b>9</b>	<b>FX Series Operations Features.....</b>	<b>136</b>
9.1	Basic Operations Functions .....	137
9.1.1	Backup/Restore Configuration Files .....	137
9.1.2	Disaster Recovery Procedure .....	137
9.1.3	Change Password.....	138
9.1.4	Manage Licenses / Fast Codes .....	138
9.1.5	Shutdown/Restart Appliance .....	139
9.2	Packet Capture .....	140
9.3	Update Software.....	142
9.3.1	Upload and Apply Server Installation Image Version 6.02+:.....	142
9.3.2	Download and Apply Image from ADC (FX Remote Only): .....	142
9.3.3	Software Update Discussion .....	142
9.3.4	Recommended Process for Software Upgrades .....	143
9.4	Updating FX Series Appliance Software at 5.78.0 or earlier .....	144
9.4.1	Base Platform Image (BPI) Upgrade Process .....	144
9.4.2	Upgrade Kit and Prep .....	144
9.4.3	The Upgrade Process .....	144
9.5	Updating FX Series Appliance Software to Version 6.1 .....	146
9.5.1	User Interfaces .....	146
9.5.2	Determine the Current Software Version .....	146
9.5.3	Screen print version information for reference .....	146
9.5.4	Determine the Available Upgrade Versions .....	147

9.5.5	Download the files to your desktop or other convenient location. ....	147
9.5.6	Check for new software: .....	147
9.5.7	Installing the Latest Software Version .....	147
9.5.8	Install the FX Platform Image Update .....	147
9.5.9	Upload and Apply FX Platform Image Update:.....	147
9.5.10	Verify Update Success .....	148
9.6	FX Series Documentation.....	149
9.6.1	On the Comtech EF Data web site: .....	149
9.6.2	On the appliance:.....	149
<b>10</b>	<b>Appendix .....</b>	<b>150</b>
10.1	FX Series Console Management Functions.....	150
10.1.1	Main Menu .....	150
10.1.2	Configure Appliance.....	150
10.1.3	Show Status.....	151
10.1.4	Diagnose Network Connectivity .....	151

## Table of Figures

Figure 1-1 FX Series Multicator Theory of Operation .....	31
Figure 1-2 FX Series Basic Mesh Connectivity Diagram .....	35
Figure 1-3 FX Series Hub Spoke Mesh Connectivity Diagram .....	36
Figure 1-4 FX Series Mesh with Redundancy Connectivity Diagram.....	37
Figure 1-5 FX Series Appliances Data Sheet.....	38
Figure 1-6 FX Series Hardware Specifications.....	39
Figure 1-7 FX Series FX-4010 Back Panel .....	40
Figure 1-8 FX Series FX-1005 Front Panel .....	41
Figure 1-9 FX Series FX-1005 Rear Panel .....	42
Figure 1-10 FX Series FX-1010 Front Panel.....	43
Figure 1-11 FX Series FX-1010 Rear Panel.....	44
Figure 3-1 FX Series Mesh Connection Diagram .....	52
Figure 4-1 FX Series Standard Configuration Screen .....	53
Figure 4-2 FX Series Basic Network Interfaces Screen.....	55
Figure 4-3 FX Series Host/DNS Settings Screen .....	57
Figure 4-4 FX Series In-Path Interfaces Definition Screen .....	59
Figure 4-5 FX Series LAN Interfaces Screen .....	61
Figure 4-6 FX Series SNMB Configuration Screen.....	63
Figure 4-7 FX Series Quality of Service Menu .....	64
Figure 4-8 FX Series Dynamic ACM Configuration Screen.....	65
Figure 4-9 FX Series ACM QOS Status by VSAT Modem Screen.....	67
Figure 4-10 FX Series QoS Filters Configuration Screen .....	68
Figure 4-11 FX Series Quality of Service Queues .....	70
Figure 4-12 FX Series QoS Queues Configuration Screen .....	71
Figure 4-13 FX Series Multicator Theory of Operation .....	74
Figure 4-14 FX Series Multicator Configuration Screen (Controller Settings) .....	75
Figure 4-15 FX Series Multicator Transmitter/Receiver Configuration Settings .....	76
Figure 4-16 FX Series Redundancy Screen .....	79
Figure 4-17 FX Series ADC WCCP Definitions Screen .....	83
Figure 5-1 FX Series ADC Configuration Menu.....	91
Figure 5-2 FX Series ADC General Settings Screen.....	92
Figure 5-3 FX Series ADC Port Definitions Screen .....	95
Figure 6-1 FX Series Remote Main Index Screen .....	97
Figure 6-2 FX Series Remote Configuration Screen.....	98
Figure 6-3 FX Series Remote General Settings Screen.....	99
Figure 6-4 FX Series Remote In-Path Interfaces Screen .....	102
Figure 7-1 FX Series Status Menu.....	105
Figure 7-2 FX Series ADC Real-Time Monitor Screen .....	105
Figure 7-3 FX Series QOS Status Monitor Screen .....	108
Figure 7-4 FX Series ADC Current Status Screen .....	112
Figure 7-5 FX Series Remote Real-Time Monitor Screen.....	116
Figure 7-6 FX Series Remote Current Status Screen.....	118
Figure 8-1 FX Series ADC Features Menu .....	120
Figure 8-2 FX Series ADC Application Policy Menu .....	120
Figure 8-3 FX Series Application Policy Applicability .....	129
Figure 8-4 FX Series Authorization Realm Screen .....	130
Figure 8-5 FX Series Specific Optimization Techniques Configurations .....	131
Figure 8-6 FX Series Layer 5 Policy Configuration Screen .....	132
Figure 8-7 FX Series TCP/UDP Ports Table .....	135



Figure 9-1 FX Series Operations Menu .....	136
Figure 9-2 FX Series Backup and Restore Screen .....	137
Figure 9-3 FX Series Change Passwords Screen .....	138
Figure 9-4 FX Series Upgrade Fast Codes Screen .....	138
Figure 9-5 FX Series Shutdown/Restart Appliance Screen .....	139
Figure 9-6 FX Series Packet Capture Screen .....	140
Figure 9-7 FX Series Update Software Screen .....	142
Figure 9-8 FX Series Software Version Display Screen .....	146

# Using This Document

This guide was prepared to assist you in the installation, configuration and management of the FX Series Appliances. This document contains the same information that is available thru the on-line help contained with the FX Series web based administrative screens. This document supports Release 6.1 of FX Series Appliances.

---

## Document Organization

### Release Notes

This section delineates the major changes from the prior release.

### Theory of Optimization

This section discusses the characteristic of data transmission that will cause slow response and higher bandwidth requirements. It also delineates techniques that can reduce the slowness and help reduce bandwidth requirements.

### FX Series Technology

This section provides a brief description of the hardware and optimization techniques available through the FX Series of appliances.

### FX Series Installation Patterns

This section provides instruction on how to install the available configurations for all FX Series appliances.

### FX Series Basic Network Settings

This section discusses how to set the basic networking parameters, such as Management Interface, Host Settings, SNMP Settings, Multication, Quality of Service and High Availability.

### FX Series ADC Specific Network Settings and Performance

This section discusses ADC specific network settings and current performance status, including General Settings, In-Path Settings and WCCP.

### FX Series Optimization

This section discusses optimization issues and definitions of optimization techniques available on the FX Series appliances for web based or enterprise applications.

### FX Series Remote Specific Network Settings and Performance

This section discusses Remote specific network settings and current performance status, including General Settings and In-Path Settings.

### FX Series Operations

This section discusses tools to perform operational tasks, including Backups, License Management, Shutdown/Restart, and Updating Software for all FX Series Appliances. This section also describes how to obtain FX Series documentation downloads for the FX Series Appliances.

## Symbols used in this manual:



Important Note



Informational Note

---

## Contacting Product Support

Comtech EF Data Product Support representatives for FX Series Products are available. **For all product support, please call:**  
**+1.240.243.1880**  
**+1.866.472.3963 (toll free USA)**

Comtech EF Data offers an annual subscription plan providing unlimited telephone support for the coverage period, software upgrades and other important support provisions. Contact Technical Support for more information.

---

## FX Series End User License Agreement

This is a legal agreement between you (either an individual or an entity) and Comtech EF Data Corporation.

### **HARDWARE LICENSE and WARRANTY**

This product is covered by Comtech EF Data's standard H/W warranty

### **SOFTWARE LICENSE**

This SOFTWARE is protected by the copyright laws of the United States and international copyright treaties as well as other intellectual property laws and treaties. This SOFTWARE product is licensed not sold.

The FX Series Appliance SOFTWARE you have licensed is defined as the SOFTWARE which operates on an appliance. The FX Series Client SOFTWARE you have licensed is defined as the SOFTWARE which operates on an intelligent, single computer, for use in accessing and accelerating Web, Browser or TCP-based applications.

**GRANT OF LICENSE:** You have the right to install the FX Series Appliance SOFTWARE on all appliances for which you have licensed copies. For each copy of the FX Series Client SOFTWARE this license confers you have the right to install the SOFTWARE on a designated computer for use in accessing and accelerating Web, Browser or TCP-based applications. The SOFTWARE is in "use" on a computer when it is loaded into temporary memory (i.e. RAM) or installed into permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. You may not install the SOFTWARE on more appliances or on more computers than you have licensed copies.

Additionally, you have the right to make one (1) archival copy of the SOFTWARE for each appliance and for each computer which has the SOFTWARE installed in accordance with the terms of this Agreement and subject to the Use Restrictions as set forth below. The copyright notice, as contained in the original CD-ROM, must be affixed to any archival copy.

**COPYRIGHT:** The SOFTWARE is owned by Comtech EF Data Corporation or its suppliers and is protected by United States copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE like any other copyrighted material (e.g., a book or musical recording). You may not copy any of the written materials accompanying the SOFTWARE.

**OTHER RESTRICTIONS:** You may not rent, lease or sublicense the SOFTWARE, but you may transfer the SOFTWARE and accompanying written materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement. You may not modify, create a derivative work, reverse engineer, decompile, or disassemble the SOFTWARE. If the SOFTWARE is an update or has been updated, any transfer must include the most recent update and all prior versions. This license and your right to use the SOFTWARE automatically terminate if you fail to comply with any provision of this license agreement.

**SUPPORT AND UPGRADES:** This Agreement does not entitle Licensee to any support, upgrades, patches, enhancements or fixes for the Product (collectively, "Support"). Licensee must make separate arrangements for Support and pay any fees associated with such Support. Any software upgrades, patches, enhancements or fixes provided as part of Support for the Software that may be made available by Comtech EF Data's Maintenance agreement shall become part of the Software and subject to this Agreement.

### **LIMITED WARRANTY**

**LIMITED WARRANTY:** Comtech EF Data warrants that (a) the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt provided that it is used on the computer hardware and with the operating system for which it was designed.

Any implied warranties on the SOFTWARE are limited to ninety (90) days. These warranties commence on the date you first obtain the product and extends only to you, the original customer. Some states/countries do not allow limitations on duration of implied warranty, so the above limitations may not apply to you.

**CUSTOMER REMEDIES:** Comtech EF Data's entire liability and your exclusive remedy shall be, at Comtech EF Data's option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet Comtech EF Data's Limited Warranty and which is returned to Comtech EF Data with a copy of your receipt. IN NO CASE WILL COMTECH EF DATA'S LIABILITY EXCEED THE AMOUNT OF THE LICENSE FEE. This Limited Warranty is void if failure to the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or thirty (90) days, whichever is longer. Outside the United States, these remedies are not available without proof of purchase from an authorized non-U.S. source.

**NO OTHER WARRANTIES:** The warranty and remedies set forth above are exclusive and in lieu of all other, oral or written, expressed or implied. Comtech EF Data disclaims all other warranties, expressed or implied, including, but not limited to, implied warranties or merchantability and fitness for a particular purpose, with regard to the SOFTWARE, and the accompanying written materials. Comtech EF Data does not warrant that the SOFTWARE's functions will meet your requirements or that its operation will be uninterrupted or error free. This limited warranty gives you specific legal rights. You may have others which vary from state/country.

**NO LIABILITY FOR CONSEQUENTIAL DAMAGES:** In no event shall Comtech EF Data be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this Comtech EF Data product, even if Comtech EF Data Inc. has been advised of the possibility of such damages. Because some states/countries do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

**EXPORT:** You acknowledge that the laws and regulations of the United States restrict the export and re-export of the SOFTWARE. You agree that you will not export or re-export the SOFTWARE in any form without the appropriate United States and foreign government approval.

#### **U.S. GOVERNMENT RESTRICTED RIGHTS**

The SOFTWARE and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer SOFTWARE clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer SOFTWARE-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Comtech EF Data (Stampede), 80A Rhoads Center Drive, Dayton, Ohio 45458. This Agreement is the entire agreement between you and Comtech EF Data relative to the SOFTWARE and supersedes all prior written statements, proposals or agreements relative to its subject matter. If you acquired this product in the United States, this Agreement is governed by the laws of the State of Ohio. Should you have any questions concerning this Agreement, or if you desire to contact Comtech EF Data, address your questions to: Attention: Contracts Division.

---

## Patents and Trademarks

See all of Comtech EF Data's Patents and Patents Pending at <http://patents.comtechedata.com>.  
Comtech EF Data acknowledges that all trademarks are the property of the trademark owners.

Webmin is a web-based system administration tool created by Jamie Cameron. All recent versions of Webmin may be freely distributed and modified for commercial and non-commercial use.

Copyright© 2001-2004 SUSE LINUX SUSE and its logo are registered trademarks of SUSE AG. Linux is a trademark of Linus Torvalds.

Portions Copyright© 1991-1997, Thomas G. Lane. All rights reserved.  
All trademarks or registered trademarks are the property of their respective owners.  
Stampede and Acceleration On-Demand are registered trademarks of Comtech EF Data/Stampede

© 2013 Comtech EF Data/Stampede. All rights reserved.  
US Patent #5,682,514, #5,835,943. #6,012,085, #6,122,637, #6,339,787, #6, 615,275, #7,359,926,  
#7,543,072

Under the copyright laws, this documentation may not be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, without the prior written consent of Comtech EF Data/Stampede.

Comtech EF Data  
2114 West 7th Street  
Tempe AZ 85281

WORLD WIDE WEB: <http://www.comtechedata.com>

---

## Conventions and References

### **Metric Conversion**

Metric conversion information is located on the inside back cover of this manual. This information is provided to assist the operator in cross-referencing non-Metric to Metric conversions.

### **Recommended Standard Designations**

Recommended Standard (RS) Designations have been superseded by the new designation of the Electronic Industries Association (EIA). References to the old designations may be shown when depicting actual text displayed on the Web Server (HTTP) or Command Line Interface pages for the FX Series appliance).

### **Trademarks**

Product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

### **Environmental**

The FX Series Appliance must not be operated in an environment where the unit is exposed to extremes of temperature outside the ambient range 0° to 50°C (32° to 122°F); precipitation, condensation, or humid atmospheres above 95% relative humidity; altitudes (unpressurized) greater than 2000 meters; excessive dust or vibration; flammable gases; or corrosive or explosive atmospheres. Operation in vehicles or other transportable installations which are equipped to provide a stable environment is permitted. If such vehicles do not provide a stable environment, safety of the FX Series appliance may not be guaranteed.

---

## Comtech EF Data Warranty Policy

Comtech EF Data products are warranted against defects in material and workmanship for a specific period from the date of shipment, and this period varies by product. During the warranty period, Comtech EF Data will, at its option, repair or replace products that prove to be defective. Repairs are warranted for the remainder of the original warranty or a 90 day extended warranty, whichever is longer. Contact Comtech EF Data for the warranty period specific to the product purchased.

For equipment under warranty, the owner is responsible for freight to Comtech EF Data and all related customs, taxes, tariffs, insurance, etc. Comtech EF Data is responsible for the freight charges only for return of the equipment from the factory to the owner. Comtech EF Data will return the equipment by the same method (i.e., Air, Express, Surface) as the equipment was sent to Comtech EF Data.

All equipment returned for warranty repair must have a valid RMA number issued prior to return and be marked clearly on the return packaging. Comtech EF Data strongly recommends all equipment be returned in its original packaging.

Comtech EF Data Corporation's obligations under this warranty are limited to repair or replacement of failed parts, and the return shipment to the buyer of the repaired or replaced parts.

### Limitations of Warranty

The warranty does not apply to any part of a product that has been installed, altered, repaired, or misused in any way that, in the opinion of Comtech EF Data Corporation, would affect the reliability or detracts from the performance of any part of the product, or is damaged as the result of use in a way or with equipment that had not been previously approved by Comtech EF Data Corporation.

The warranty does not apply to any product or parts thereof where the serial number or the serial number of any of its parts has been altered, defaced, or removed.

The warranty does not cover damage or loss incurred in transportation of the product.

The warranty does not cover replacement or repair necessitated by loss or damage from any cause beyond the control of Comtech EF Data Corporation, such as lightning or other natural and weather related events or wartime environments.

The warranty does not cover any labor involved in the removal and or reinstallation of warranted equipment or parts on site, or any labor required to diagnose the necessity for repair or replacement.

The warranty excludes any responsibility by Comtech EF Data Corporation for incidental or consequential damages arising from the use of the equipment or products, or for any inability to use them either separate from or in combination with any other equipment or products. A fixed charge established for each product will be imposed for all equipment returned for warranty repair where Comtech EF Data Corporation cannot identify the cause of the reported failure.

### Exclusive Remedies

Comtech EF Data Corporation's warranty, as stated is in lieu of all other warranties, expressed, implied, or statutory, including those of merchantability and fitness for a particular purpose. The buyer shall pass on to any purchaser, lessee, or other user of Comtech EF Data Corporation's products, the aforementioned warranty, and shall indemnify and hold harmless Comtech EF Data Corporation from any claims or liability of such purchaser, lessee, or user based upon allegations that the buyer, its agents, or employees have made additional warranties or representations as to product preference or use.



The remedies provided herein are the buyer's sole and exclusive remedies. Comtech EF Data shall not be liable for any direct, indirect, special, incidental, or consequential damages, whether based on contract, tort, or any other legal theory.

### **RMA Policy**

To return a Comtech EF Data product (in-warranty and out-of-warranty) for repair or replacement, please follow these guidelines.

Contact the Comtech EF Data Customer Support Department during normal business hours. Be prepared to supply the Customer Support representative with the model number, serial number, and a description of the problem. Request a Return Material Authorization (RMA) number from the Comtech EF Data Customer Support representative.

Pack the product in its original shipping carton/packaging to ensure that the product is not damaged during shipping.

Ship the product back to Comtech EF Data. (Shipping charges should be prepaid.)

### **Online RMA Support**

An RMA number can be requested electronically by accessing Comtech EF Data's online Support page ([www.comtechefdata.com/support.asp](http://www.comtechefdata.com/support.asp)). From this page:

Click the Service hyperlink, and then read the Return Material Authorization section for detailed instructions on Comtech EF Data's return procedures.

Click [Send RMA Request] on the Support page or the RMA Request hyperlink provided in the Service | Return Material Authorization section; fill out the *Billing Information*, *Return Information*, and *Unit to be Returned* sections completely, then click [Send email]

**Or –**

**Send an e-mail** providing this same detailed information to the Customer Support Department at [service@comtechefdata.com](mailto:service@comtechefdata.com).

*Some Stampede products, programs, or services referred to in this publication may not be available in all countries in which Stampede does business. Additionally, some Stampede products, programs, or services may not be available for all operating systems or all product releases. Contact your Comtech EF Data/Stampede representative to be certain the items are available to you.*

## Release Notes

### Version 6.1.1 Functionality Enhancements

Package Release 6.1 is the latest WANOP firmware for the FX Series platforms. These new features have been developed in response to customer feedback and market analysis for the purpose of increasing the interoperability of the FX Series with other CEFD products and to broaden the scope of environments where FX Series can be deployed.

This release adds the following new features:

- Quality of Service
  - QoS only license is now rate limited at 700 Mbps instead of 500 Mbps
  - New protocol filter options for SCTP, PTPv1, PTPv3
  - Added support for VLAN priority in the QoS filters
- FAST Codes
  - This release introduces new “trial license” Fast Codes for 30/60/90 day for Packet Compression and WANOP.
- Reporting
  - The Status->View Current Status->ACM QOS->By VSAT Modem has two changes.
    - New column header for 'Queue Name' indicates which queue a filter is directed
    - 'Filter Hits' column header has been changed to 'Filter Matches'

### Version 6.1 Functionality Enhancements

These new features have been developed in response to customer feedback and market analysis for the purpose of increasing the interoperability of the FX Series with other CEFD products and to broaden the scope of environments where FX Series can be deployed.

This release adds the following new features:

- Enhanced QOS Monitor Functionality
  - CurrentStatus-> ACM QOS-By VSAT modem.
    - This now shows ingress packets and bytes which will be non-zero if packet compression is happening.
  - CurrentStatus->ACM QOS-Throughput by QOS Queue.
    - This now shows packet compression savings percentage.
  - Configuration->QOS-Queues pick list.
    - This function has been dramatically reworked. You can now change CIR, MIR, Priority, and enable/disable packet compression directly from the view.
- Enhanced SNMP Functionality
  - MIB
    - Entirely new MIB which allows full management of the FX.
    - Same MIB is used for both FX-Remote and ADC.
  - New wramp SNMP configuration wizard

Now prompts for destination 'trap' community and 'read/write' community. (previous MIB was not read/write and did not emit traps (traps are an SNMP term for alerts))

- Enhanced Operations Functionality

Operations->Shutdown Restart.

Now has new 'Restart acceleration service and reset cache. This is now the only way to completely reset the cache files

- Status Monitor Enhancements

Real-Time Monitor

Real-time monitor now does a 'quick' reset of cache that does not require reboot.

CurrentStatus->NetworkStatus-Of WAN Interface.

New status feature that is the only way to ascertain the MAC address of the WAN interface.

- Header Compression/Packet Aggregation

FX aggregates packets into an Ethernet frame and sends it to a peer, where the packets are restored.

- The default for DDS has been changed to 'Enabled' on the ADC. Previously it was 'Disabled' by default.

### Version 6.0.3 Functionality Enhancements

These features have been developed in response to customer feedback and market analysis for the purpose of increasing the interoperability of the FX Series with other CEFD products and to broaden the scope of environments where FX Series can be deployed.

This release adds the following new features:

- Multiprotocol Label Switching (MPLS) is now supported in ACM Filter Definitions.  
If MPLS is selected, then the "MPLS Label" and "MPLS experimental bits" fields will be enabled as filter criteria.
- The default for Dynamic ACM Polling Method Parameters is changed.  
The default setting is now the Modem type, with the pull-down choices including:  
CDM-750, CDM-625, CDM-760, CDM-800, CDM-840, and CTOG-250.  
The default is the CDM-750
- L5 functionality has been enhanced with the following improvements  
Pre-connect option has been removed from the L5 form  
Enable acceleration has been added to the L5 form  
The ability to define a "\*" policy for L5. A "\*" is a port range of 1-65535.
- Other changes include:  
VLAN Mode has been added to the general screen for (Trunk or Access)  
Fail-to-Wire option has been added to the general screen (on or off)  
ACM QoS Section of the Current Status screen has an added report "Throughput by QoS with an updated description of "By Modem"

## Version 6.0.2 Functionality Enhancements

These features have been developed in response to customer feedback and market analysis for the purpose of increasing the interoperability of the FX Series with other CEFD products and to broaden the scope of environments where FX Series can be deployed.

This release adds the following new features:

- **Mesh Network Configuration**  
Mesh network optimization is now supported with two appliances at each site.
- **Multicator modifications**  
Configuration settings have been simplified and located on one main screen on the Web Admin Guide. The Multicator icon will appear on a single screen if an in-path interface is enabled.
- **QOS modification for FTP**  
FTP is now an option on the QOS filter screen. If FTP is selected, the FX automatically tracks the data ports associated with FTP transfers by monitoring the activity on the FTP control port, which is defaulted to port 21 upon initial selection. The FTP control port may be changed.
- **WCCP is now enabled on FX Series Remote**  
WCCP functionality for the FX Series Remote is now available and follows the configuration/installation patterns which have been available on the FX Series ADC.
- **Redundancy modifications**  
The process for setting up these options has been simplified.
- **Installation patterns**  
Installation patterns have been updated to include the FX Remote WCCP and Mesh configurations.

## Version 6.0.1 Functionality Enhancements

This release added the following features:

### **Management Port**

This release supports a dedicated management port. The administrative WEB GUI has been enhanced to configure management port settings. Management traffic flows over a separate routing table from the accelerated data traffic. The Administrative Web GUI can now optionally run over HTTP/S.

### **Trunked VLAN Support**

FX Series supports a trunked network, where multiple 802.1Q tagged VLANs flow thru the same physical connection. To accomplish this, many aspects of the FX Series Remote FX Series ADC data interception and acceleration was modified to retain the VLAN properties. Any accelerated data is transmitted over the network on the same VLAN as the original, non-accelerated data.

. FX Series Release 6.0.1 provides:

- Support for 1024 active VLANs for IDs 2-4095.
- Support Virtual Routing and Forwarding (VRF) environments.
- Support display of tallies on a per-VLAN basis at ADC only (not RCO).
- Accelerated VLAN traffic will maintain original VLAN affinity.

- Private HTTP caches on a per VLAN basis
- Cached HTTP data will be segregated between VLANs.

VLAN addition and deletion configuration changes can be made without service loss or downtime. A restart is not required for the changes to take effect.

### **Transparency**

FX Series Release 6.0.1 provided:

- Ability to communicate between appliances using the same port as the original client connection.
- Ability to communicate between appliances using the original client source addresses.
- Ability to support active-active ADC configurations.
- Ability to optionally disable multiplexing of client connections.

### **Dynamic ACM QoS**

- Special support was added to FX Series Release 6.0.1 ADC to continuously acquire the data rate of a modem via SNMP connection. When the data rate changes the QoS rules are dynamically adjusted. New fields were added to the Dynamic ACM page to configure the IP address of the modem, and user name and password.

### **FAST Code Support**

In prior releases, a “license” file was uploaded to the FX to enable functionality.

In FX Series Release 6.0.1 and above, this methodology is now superseded by FAST Codes.

The FX Series CLI and Administrative Web GUI have been enhanced to allow Fast code upgrades.

### **Routed Mode Deployment Option**

The main configuration screen now allows you to put the FX in either “bridged” or “routed” mode. In routed mode, policy based routing (PBR) must be set up on the Cisco router to specifically direct traffic to the FX Series Appliances.

### **Reliable Multicast Fan-Out**

“Multicator” feature is a powerful new content distribution system. This feature allows a user to upload a file to an FX device via ftp, the file is then reliably multicast to a group of receivers. The receivers then upload the content to a local ftp server. The Multicator employs the “Content Distribution Control Protocol” (CDCP) to ensure that only one multicast transmission is in progress.

### **Base Platform Image ‘3’ Upgrade Kit**

The new features of Release 6 require new software packages and a new kernel from previous FX releases. This upgrade kit will define procedures for updating existing FX appliances from a USB flash drive.

### **Management via SSH**

The Base Platform Image “3” provides support over SSH and will also allow the Administrative WEB GUI to function over SSL.

# 1 Overview - FX Series

## 1.1 Stampede FX Series Product Line Update

### Value Proposition

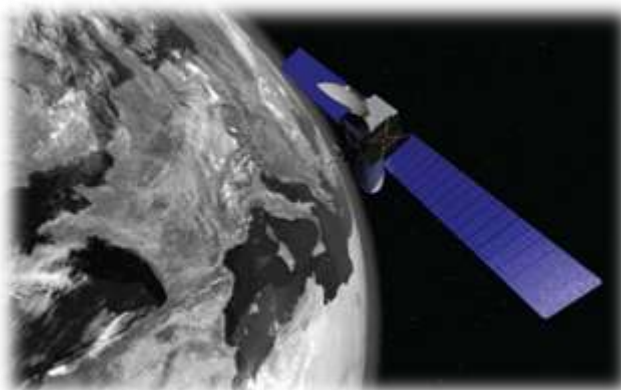
**“Reduce OPEX, Improve User Experience”**

**Reduce OPEX by:**

- Shrinking the Data
- Keeping the Pipe Full

**Improve User Experience by:**

- Getting the Data there faster
- Getting the Right Data there



### The Challenges for ISPs with Satellite Links

Data consumed by individual users and enterprises is increasing exponentially. ISPs must cost-effectively keep up with the enormous demand for limited bandwidth - while conserving it.

### Assuring Delivery of Web Applications for Bottom Line Results

Data center simplification and the growing migration to web-enabled applications are driving the need for a new class of multi-function optimization devices. The Stampede FX Series combines both one-sided application delivery and two-sided WAN optimization into a single platform. The FX Series delivers unprecedented application performance, optimization, transparency, availability and management for existing networks.

### Productivity and Performance

The Stampede FX Series WAN optimization improves access to your applications by reducing the amount of data transferred on the link through use of various compression and caching schemes as well as accelerating reliable protocols.

As a two-sided FX Series implementation, the FX Series Remote resides at the remote site providing TurboStreaming, Dynamic Cache Differencing, Adaptive Compression, Persistent Connections, Dynamic Data De-duplication, and Header Compression/Package Aggregation.

#### Typical Users

- Internet Service Providers (ISPs)
- Enterprise
- Offshore/Maritime
- Telecommunications Operators
- Satellite Operators
- Managed Service Providers

#### Common Applications

- High-speed content delivery
- HTTP and TCP optimization & acceleration
- Corporate networks
- Mobile Backhaul

#### Key Benefits

- Provides up to 80% bandwidth savings in both directions
- Provides up to N times efficiency when using the Multicator
- Enables measurable reduction in response time for users
- Delivers CAPEX for OPEX payback typically in 3-4 months
- Scales easily for small, medium and high volume networks
- Ensures the best traffic flow with Advanced Traffic Shaping
- Matches the modem link rates with ACM tracking
- Real time voice sessions with the use of Header Compresses/Package Aggregation.

## 1.2 Technologies that Optimize Satellite Bandwidth Acceleration

### Traffic Shaping with ACM Tracking

Traffic is classified and prioritized by protocol, source/destination subnets, source/destination ports, VLAN, MPLS labels/EXP and DSCP bits. Classified traffic is then shaped to the link rate based upon priority, CIR and MIR. Link rate is either configured at setup or optionally read from the modem in real time. Reading from the modem in real time allows the output rate to track the actual link rate for an ACM modem, which changes based upon changing link conditions. While it is possible to configure this with other modems, it is designed to work with the CDM-750 and CDM-625 modems. This feature is available as either stand-alone, or as part of the full WAN optimization product.

### Transparent Assured Delivery

With flexible options for in-line or Cisco's Web Cache Communication Protocol (WCCP), the FX Series devices deliver unprecedented transparent optimization. End-to-end assurance is maintained for all applications providing complete transparency and the ability for existing Quality of Service (QoS) and network visibility management programs to continue monitoring the health of your network.

### Optimize VLAN Trunked Data

All appropriate Layer 5 and Layer 7 optimizations are available for tagged VLAN data, preserving or recreating the VLAN tags for optimized traffic. This includes HTTP caching as well as de-duplication. Caches are maintained by appliance and by VLAN. Appropriate traffic can be shared between VLANs on the same appliance. In addition, the FX-1010 will support up to 8 LAN ports, each of which is tagged and passed to the WAN trunk.

### Multicator

The FX Series supports a reliable multicast. This is designed to work in a mesh network, but will also work in a hub/spoke network. In the mesh, any device can be a transmitter with the remaining devices being receivers. Multiple devices can be transmitters. The transmitter function is time shared, with a second device being given permission to transmit after the first is complete. This can work in a hub-spoke network where typically the ADC would be the transmitter, although this is not required. The process is to FTP a file from the client into the transmitter's inbox, that file is transmitted reliably in a multicast to all of the receivers. Once transmitted, the receivers FTP the file to a specified server.

### Redundancy and Fail Over

Redundancy is critical to 24/7 availability, and the FX appliance is designed to handle redundancy and fail over in two different ways; inline and routed. The inline configuration is used when operating in conjunction with a CEFD modem operating with 1:1 redundancy. WCCP (Web Caching Communication Protocol) is used in routed mode to allow N devices to serve the function of any M devices, resulting in M: N redundancy. The inline configuration has a primary and a redundant device in series, the redundant takes over whenever the primary fails.

### Management

The FX platforms provide total insight through real-time information including over 100 real-time statistics providing extensive details on all inbound and outbound traffic. Historical data for days or months are easily viewed via online graphs, simplifying capacity planning, trending, network issues, and application troubleshooting. Management information can be obtained via an intuitive Web GUI or SNMP. The updating for the FX Series Remotes is automatic. The FX Series remotes poll the FX Series ADC for updates. When the ADC is updated; each remote will download the update and automatically update itself.

## Flexibility

The FX Series platforms provide a comprehensive range of flexible options for total transparent 24/7 operation within your existing or growing network infrastructure. No matter what your application acceleration or WAN optimization requirements are today or in the future, the FX Series platform solutions will handle all your business critical applications with ease. Whether your installation requires small, medium or large branches or the consolidation of multiple remote or enterprise data centers, we have the solution for your organization's needs.

## Compatible with Advanced VSAT Solutions

The Stampede FX Series products can be added to an Advanced VSAT Solutions network for WAN optimization and application acceleration. The results can be significant improvements in user experience and a reduction by 20-80% in required bandwidth for TCP traffic.

## Solutions

Deploy the Stampede FX Series (ADC) as a single-sided solution to optimize traffic from your outbound channel. For a two-sided solution, add the FX Series Remote (REM) appliance and achieve the ultimate in application acceleration and WAN optimization.

## Header Compression/Packet Aggregation

As real time traffic moves to IP, there is a proliferation of traffic with small payloads. In this case, the header bytes can be 2 to 4 times the number of payload bytes. For small voice packets, compression can result in reducing the required data rate to 30 – 50% of the original. The FX aggregates packets into an Ethernet frame and sends it to a peer, where the packets are restored. Header compression is integrated into the traffic shaping, and maximum latency per queue can be set. Header Compression is available as a standalone function with ACM QoS.



## 1.3 Single-Sided Solution

### 1.3.1 Load Balancing via WCCP

The Web Cache Communications Protocol (WCCP) allows satellite network service providers to transparently inject acceleration into their satellite network infrastructure by redirecting traffic flows in real-time to network devices such as the FX Series. WCCP has built-in load balancing, scaling, fault tolerance, and service-assurance (failsafe) mechanisms to ensure network devices can scale and have high-availability. For fault tolerance, if one of the FX Series appliances incurs a hardware failure, the WCCP-enabled router will stop sending traffic to that device and redirect traffic to the other FX Series appliances with zero down-time.

Load balancing via WCCP intelligently distributes the TCP and HTTP workload across multiple FX Series appliances. For flexible scalability, service providers can simply add an FX Series appliance to the cluster, and WCCP will split the traffic load among all the FX Series appliances. Up to thirty-two FX Series appliances can be set up within a cluster and dynamically load balanced.

WCCP enables network service providers to implement the FX Series into their network with greater deployment flexibility, without requiring the FX Series to be physically in-line. The FX Series can be deployed "virtually" in-line, hence, not all traffic is required to pass through the FX Series appliance. The network administrator programs the router to redirect traffic to the FX Service appliance in-bound and out-bound based on the router policies. This allows the administrators to make changes to their network environment by simply changing the router policies.

Stampede's FX Series (running WCCP) localizes content, and responds to content requests in order to reduce the amount of data going over the WAN. This improves application delivery response times, and allows the WAN link to support more traffic. Using WCCP, traffic is transparently redirected to the FX Series appliance for TCP and HTTP acceleration, compression, caching and other optimization services.

With WCCP configured, the router redirects traffic to the FX Series to perform the application acceleration and WAN optimization functions. When an end-user makes a request, the router intercepts the request, and redirects the request to the FX Series inside a generic routing encapsulation (GRE) frame to prevent any modifications to the original packet. The FX Series with WCCP can be used to transparently route traffic, so that you don't have to make changes to Web browsers, and configure the FX Series as a proxy server to offload servers, accelerate application delivery and optimize the network.

### 1.3.2 Source IP Preservation

Source IP Preservation is a technology that is used to support security policies that require a specific source IP address, or range of IP addresses. It is also used to prevent the FX Series appliance from being blacklisted.

For example, in the event where a situation is deemed inappropriate, such as a SPAM event, the sending device Source IP address will be blacklisted. To avoid this problem, the FX Series uses the end-user's Source IP address when making a request to a Web or application server. The FX Series configuration method makes implementing Source IP Preservation easy within a WCCP or inline environment. The FX Series is usually configured to use the IP address of the client when making requests to content servers, whereas, other FXs make requests to Web servers using their own IP address. IP addressing problems can occur when, for example, an end-user is involved with illegal online activity and the IP address of the FX is recorded in the Web server's logs. If the IP address of the FX is used to make the client request to the server, it will likely be placed on a blacklist, and therefore cause considerable network problems. By spoofing the IP address of the client, the FX Series is able to avoid this problem.

### 1.3.3 Connection Management

Connection management removes the burden of establishing and terminating TCP connections from the web servers, allowing the server to handle more traffic. Stampede manages network connections in several ways to optimize the flow of data and reduce the impact on the network, application servers and end-user devices. The FX Series appliance maintains a consistent pool of connections between itself and the servers. The servers are then offloaded from managing the connections, and are isolated from inadvertent session disconnects.

With Stampede's FX Series Remote appliances working with the FX Series head-end appliance, a persistent connection between the client and server is always maintained, even when the browser may close and reopen a session. These sessions are also multiplexed across multiple connections, improving throughput and response time. This persistent connection is extremely important for AJAX and Web 2.0 applications which constantly open and close sessions as they poll and access various Web services. Stampede eliminates this potentially network intrusive overhead.

### 1.3.4 QoS with ACM option

The Quality of Service Function with ACM option is intended to work with EF Data modems that support ACM. The FX Series ADC and Remote have the ability to read the current data rate from the modem, and will adjust the output data rate to match the modem data rate. The FX Series data rate is calculated based a per Ethernet frame basis.

The FX is also designed to work with the modem in a 1:1 Redundant with fail over mode and work with the modems when they are in a 1:1 redundant configuration.

#### **Output Data Rate**

All data rates are Ethernet frame rates. The total data rate is a parameter that can be set, or under the optional ACM mode, can be updated dynamically and continuously from the modem in the link.

#### **Traffic Classification**

Traffic can be classified on combinations of Protocol, VLAN, Source/Destination IP Port number, Source/Destination subnet, MPLS labels/EXP and DSCP bits. Classified traffic is directed into specified Queues. Queues are assigned priority.

#### **Traffic shaping**

Traffic is shaped using drain algorithms on the specified queues. Queues of equal priority are treated in a fair-weighted manner. Connections within a specified Queue are also treated in a fair-weighted manner.

The drain algorithms are strict priority or Min-Max. In Strict Priority, available bandwidth is allocated on the basis of priority.

Min-Max gives more control. Bandwidth is allocated up to a committed information rate based upon priority. Once the committed information rate is reached for all classes, excess bandwidth is allocated based on the same priority, up to a defined maximum for each Queue.

### 1.3.5 GZIP Compression

The most common use of compression in Web environments is accomplished by enabling GZIP functionality at the Web server. GZIP compression is handled on-the-fly from the servers to the clients. This reduces bandwidth consumption and improves application delivery and client response time. The FX Series uses GZIP compression to reduce the payload size to deliver more data across the satellite link, enabling more applications to be delivered and the ability to support more users. GZIP compression

removes non-essential information from data being moved from one location to another, and then reassembles the data to its original form after the transfer is complete.

Squeezing the data reduces network traffic and accelerates the delivery of time-sensitive information. GZIP compression uses standard techniques to compress data sent to browsers. While compression exists in many forms throughout Web deployments, the FX Series is able to more effectively apply compression resulting in better compression ratios. GZIP is not normally used for attachment compression or for inbound compression from the browser. In addition, GZIP cannot be used to compress HTTP headers or image data. In a single-sided mode, the FX Series appliance utilizes GZIP to compress information that can be processed by standard browsers.

Stampede utilizes various compression techniques to reduce the amount of data that must be sent across the network. In two-sided deployment, the FX Series bi-directional compression provides compression for:

- All HTTP Headers
- Application Cookies
- All Text and Data Objects
- JPEG files with Image Reduction, yielding very acceptable quality
- All attachments and file uploads and downloads

### 1.3.6 Image Reduction and Smoothing

Image Reduction and Smoothing reduces the amount of data required to represent an image without significantly altering the visual perception of the image. This is accomplished in two ways. Smoothing reduces the high frequency components or the sharpness of an image. A moderate amount of smoothing can significantly reduce the amount of data. The quality factor of a JPEG image relates to the precision of the samples. Sample precision can be reduced without visible detection.

The goal of the JPEG quality and smoothing values is to reduce the amount of data while maintaining a usable image. Depending on the JPEG, the compression is often in the range 9:1. A number between 1 and 100 specifies the tradeoff between size of the jpeg data and quality of the original image. A higher number will retain a higher quality but will not conserve as much bandwidth. If no value is specified then the FX Series value is inherited from a higher level policy; a default value of 50 is used if no higher level policy is defined. Images that have been transformed are typically not significantly changed by running through the algorithm again. What this means is that if an image has been compressed with particular smoothing and quality factor, if the same factors are used again, the image is not significantly changed.

### 1.3.7 Static Caching

Caching brings information closer to the end-user by storing recently accessed data in local memory or on hard disk, reducing the time it takes to bring back needed information, Improving the users' experience by speeding the page load times. While today's browsers maintain their own cache, they tend to be overly conservative. This means they will error on the side of requesting a new piece of data or object, usually when it really hasn't been changed. This not only impacts response time to the end-user, but also saturates bandwidth with unnecessary data transmissions.

The FX Series uses caching to maintain copies of routinely accessed data to eliminate unnecessary requests to Web and application servers, and from going over limited satellite links. By keeping local copies of frequently requested content, the FX Series allows organizations to significantly reduce their upstream bandwidth usage and cost, while improving performance. The FX Series acts as an intermediary from end-users requesting content (such as a file, web page, or other resource) from servers.

Some of the key benefits include:

- Reducing bandwidth consumption
- Keeping servers behind the FX Series anonymous for security purposes
- Delivering fast access to content

### 1.3.8 TCP Optimization

Advanced protocol optimizations drive significant improvements in bandwidth efficiencies and time savings (reducing payload and latency). WAN optimization and application acceleration technologies are deployed to improve satellite network performance and increase the amount of applications and users that can be delivered over the satellite link. The FX Series manages all TCP sessions, and handles the establishing and tearing down of TCP connections locally (at LAN speeds) to avoid satellite network congestion problems. This helps to increase link utilization and improve the user experience. TCP termination offloads the responsibility from servers having to handle the overhead imposed by the volume of TCP connections from web applications.

Additionally, application level multiplexed TCP streams take advantage of all other TCP or protocol optimization done at the link level, and application-level handshakes are eliminated by consolidating transaction requests.

Benefits include:

- Increases server capacity
- Reduces the amount of traffic sent over satellite links
- Keeps the satellite links maximized for optimum utilization
- Dramatically reduces transaction TCP turns (requests and responses) that bottleneck satellite links

## 1.4 Two-Sided Solution

### 1.4.1 Cache Differencing

Cache Differencing takes the concept of caching one step further and maintains identical copies of the browser's cache at the local device and on the FX Series appliance. The FX Series then uses intelligent differencing technology to understand what data has actually changed, and then transfers only the changed data. The local device functions normally, but with less data being transferred, you realize improved utilization of the satellite network, and increased end-user productivity.

Traditionally, pages can be marked as cacheable and will have expiration dates. When they expire they must be retrieved from the original server, resulting in additional traffic and data being transmitted across the satellite network. Within a two-sided environment, the FX Series Remote appliance caches all pages returned to the browser (even pages that are marked as non-cacheable) and performs validation when needed to ensure that no stale data is returned to the browser. When the browser asks for a page or an item that has expired or been marked as non-cacheable, the FX Series remote appliance sends a validation request to the FX Series appliance at the head-end. If the FX Series appliance is aware of the last page the client cache contains and can compute differences in the page, it sends just the differences to an expired page or non-cached page. If the differences are too big, or if the FX Series appliance no longer has retained the last version that the client has, then the entire page is returned and subsequently cached for future possible differencing. The client in turn reconstructs the requested page, caches it, and returns it to the browser. Checksums are calculated by the FX Series appliance at the head-end and verified at the FX Series remote appliance so that pages will never be delivered incorrectly. While this technique adds value on expired pages, it is extremely effective for dynamic page generation.

An important aspect of Stampede's Cache Differencing is the ability to perform differencing not only on HTML GET requests but also on POST requests. This is significant because a) responses to posts are always marked non-cacheable, and b) most applications that are based on SOAP and XML (including most AJAX applications) issue SOAP requests via the HTML POST command.

### 1.4.2 Multiplexing of Large Data Objects

The FX Series multiplexes large data objects using Comtech EF Data's patented TurboStreaming™ (multiplexed TCP sessions, patent # 7,543,072) that enables HTTP browser traffic to be intermixed across multiple "pipelines". All browser activity is optimized, including the network-intensive polling associated with Web 2.0 and AJAX applications. A key advantage of TurboStreaming is that communication resources can be shared across multiple applications, and all HTTP requests and responses from any application (including multiple browsers) are intermixed simultaneously across multiple concurrent sessions.

TurboStreaming serves as a platform for the consolidation and aggregation of all Web-based traffic from a given user. Multiple HTTP protocol streams are logically aggregated across a few TCP sessions. Individual objects or pieces of objects can be split into any size and then multiplexed with other object data and reconstructed as needed SNSPs that deliver mixed payloads consisting of business-critical applications and data, streaming media, and other network-intensive traffic. The end result is improved throughput and faster response time for the end-user.

TurboStreaming enables the browser to open multiple pipelines (10s or even 100s) that communicate with the FX Series remote appliances. All of this data, from all browsers and all browser windows, is intelligently multiplexed over multiple TCP sessions back to the head-end FX Series appliance. This fully utilizes all available bandwidth, and enables the browser to function at its full potential. This is only possible because of advanced, industry leading two-sided acceleration technology.

### 1.4.3 Microsoft™ Update Caching

Intelligently caches Microsoft® updates on the client side saving significant bandwidth attributed to "Patch Tuesday". The FX Series caching methodology handles the rather complicated procedures employed by Microsoft and other AV vendors to request updates by requesting "partial objects". This reduces the amount of data sent over satellite links to reduce bandwidth consumption and provide faster response times for end-users.

The FX Series Remote can dramatically curb bandwidth consumption by caching software updates published frequently by Microsoft, Symantec, Adobe, Apple and many other leading software vendors. The delivery of these updates is performed when software that resides on client devices downloads the new content in the background by requesting "partial content" over HTTP. The complex nature of "partial-content" HTTP requests thwarts the capabilities of most caching devices, however the FX Series Remote appliance caching engine can handle these requests. Once the content is cached by the FX Series Remote, subsequent retrievals by the updating agents that request "partial-content" will be satisfied by the FX Series Remote appliance, eliminating the need to repetitively transfer the same updates over satellite links.

### 1.4.4 Network Protocol Optimization

The FX Series provides application-aware modules for HTTP, CIFS, MAPI, POP3, SMTP, and FTP that dramatically reduce costly handshakes and intelligently apply compression to lower bandwidth consumption and reduce latency.

Stampede specializes in optimizing protocols by consolidating multiple transactions into a single transaction, which eliminates round-trips, performing cache differencing on dynamically generated content, and bi-directional data compression. In addition, our patented technology (TurboStreaming) enables the transfer of previously compressed objects up to 5 times faster through intelligent multiplexing across multiple TCP sessions.

- TCP and HTTP applications have chatty protocols that put added delay in satellite networks, as do delay-sensitive such as Microsoft Exchange and CIFS.
- IT managers are placing thousands of applications on their satellite links. Many of these applications are mission-critical, and compete over a limited amount of bandwidth.

### 1.4.5 Dynamic Data Deduplication

Dynamic Data Deduplication segments the incoming data stream, uniquely identifies the data segments, and then compares the segments replacing repetitive streams of payload data with signatures prior to transmission over the satellite links. This feature is not application protocol specific and can be applied to most TCP application traffic. The FX Series intelligently monitors the data stream and is able to distinguish protocol headers which change frequently from payload data which is often static. The FX Series extracts this payload data and segments it into blocks, storing each block into persistent memory known as a "byte cache". Blocks of data are replaced with a signature for that data. This generates significant data reduction.

### 1.4.6 Header Compression/Packet Aggregation

As real time traffic moves to IP, there is a proliferation of traffic with small payloads. In this case, the header bytes can be 2 to 4 times the number of payload bytes. For small voice packets, compression can result in reducing the required data rate to 30 – 50% of the original. The FX aggregates packets into an Ethernet frame and sends it to a peer, where the packets are restored. Header compression is integrated into the traffic shaping, and maximum latency per queue can be set.

## 1.4.7 Multicator

### Theory of Operation

A powerful new content distribution system can now be set up with the “Multicator” feature. This feature allows a user to upload a file to an FX Series device via ftp, the file is then reliably multicast to a group of receivers. The receivers then upload the content to a local ftp server. The Multicator employs the “Content Distribution Control Protocol” (CDCP) to ensure that only one multicast transmission is in progress.

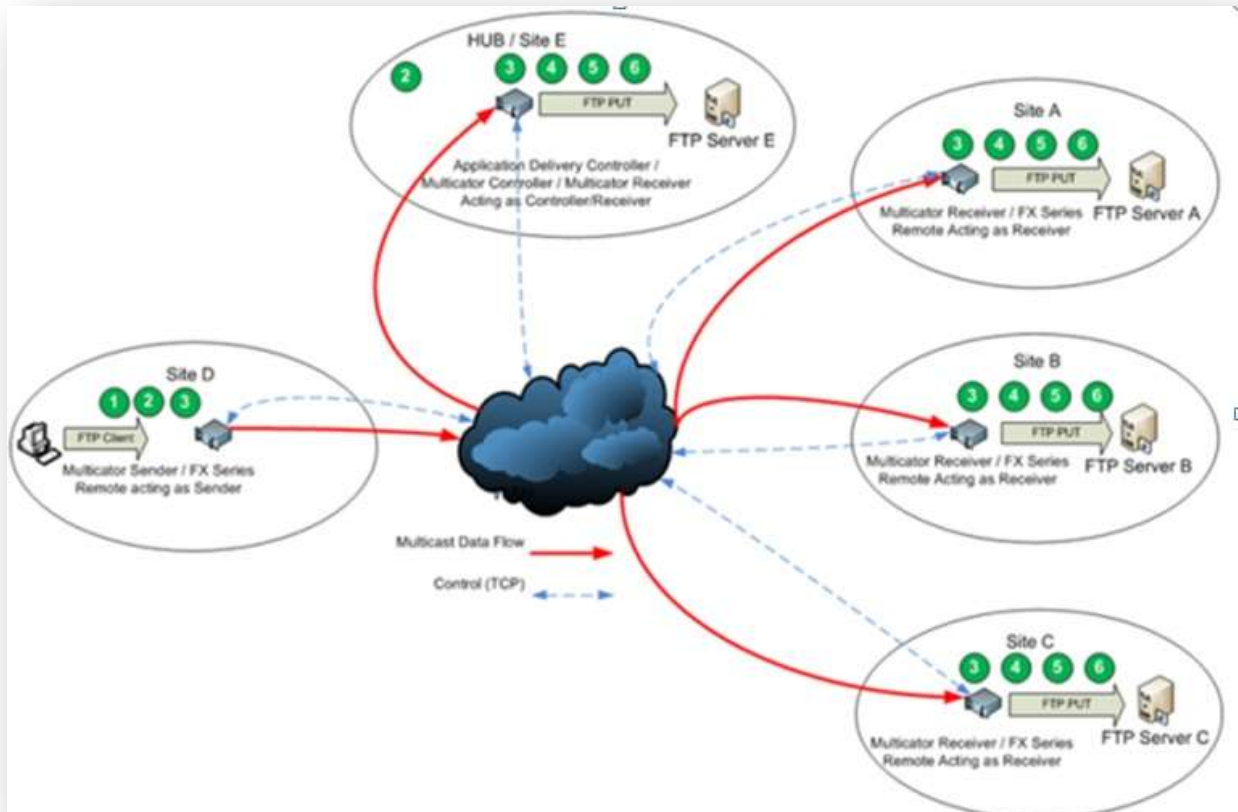


Figure 1-1 FX Series Multicator Theory of Operation

### Sequence of Events

- 1 Files are deposited on the Remote Sender (Site D) using a standard FTP client
- 2 The Sender then notifies the Controller that it has data to send and is granted permission to reliably multicast the data across the WAN
- 3 Under control of the Multicator Controller, the Sender establishes a reliable multicast connection to the Receivers.
- 4 The Sender sends the file to each of the Receivers (Sites A, B, C, and E)
- 5 Each Receiver verifies receipt to the Controller
- 6 Each receiver FTPs the file to the respective server.

## 1.5 FX Series ADC Appliance

### 1.5.1 Theory of Operation

The FX Series ADC software can run on the FX-4010, the FX-4000, the FX-1005 or the FX-1000. The FX Series ADC applies deflate compression, image transformation, static and dynamic content caching. To the client, the FX Series ADC appears to be the back-end server.

The FX Series Application Delivery Controller (ADC) devices accelerate application delivery and reduce the amount of traffic over satellite links. ADCs are single-sided (asymmetric), requiring an appliance only in the head-end. The FX Series ADC serves as a proxy for TCP management, acceleration and offloading server and network resources for out-bound traffic. TCP acceleration removes the time, quantity and complexity associated with multiple short-lived connections that slow network performance and add overhead to Web server CPU resources. An ADC terminates the client-side TCP session requests, and multiplexes many short-lived sessions into a single longer-lived session between the FX Series ADC and the Web servers.

In addition to a one-sided configuration, the FX Series ADC can reside at the service provider head-end, and work together with FX Series Remote appliances located at each remote site. These products provide two-sided WAN optimization and application acceleration to alleviate the adverse effects that latency and performance errors have upon satellite network performance. They are referred to as WAN Optimization Controllers (WOCs).

In two-sided optimization, if a connection to the FX Series ADC is not able to be achieved by a remote appliance, then the remote appliance will go into a “pass-through” mode where the requests will be directed to the target content server.

### 1.5.2 Reporting

Important FX Series ADC appliance events are recorded so that the following reports can be viewed:

#### Acceleration Statistics

- Aggregate Statistics
- By L7 HTTP Policy
- By L5 Application Policy
- Current Connections

#### Throughput Statistics

- Aggregate Throughput

#### Port Statistics

- By Port Definition

#### Load Balancing Statistics

- By Server Pool Definition

#### WCCP Status

- By WCCP Definition

#### ACM QoS

- By VSAT Modem

#### Routes

- By Table

#### Network Status

- By Interface

#### HTTP Log Analysis

- By Month

#### Multicator Status

- By Function

### 1.5.3 Deployment Options

The FX Series ADC can run in bridged mode, in routed mode or in WCCP mode. The installation instructions for these are in the FX Series Installation Patterns Section.



## 1.6 FX Series Remote Appliance

### 1.6.1 Theory of Operation

The FX Series Remote software can run on the FX4010, the FX-4000, the FX-1005, the FX-1010 and the FX-1000. The FX Series Remote accelerates traffic by intercepting user requests and forwarding them to the FX Series ADC. The FX Series ADC applies deflate compression, image transformation, static and dynamic content caching. The FX Series Remote applies static content caching, dynamic content caching, deflate compression, Dynamic Data De-duplication, persistent connections, connection multiplexing, client side connection termination, and TurboStreaming. To the client, the FX Series Remote appears to be the back-end server. When in a two-way configuration the FX Series Remote will communicate with the FX Series ADC via the port that the client is connecting by default. . If the FX Series Remote is configured to connect to a specific FX Series ADC then port 4922 will be used. If a connection to the FX Series ADC is not able to be achieved then the remote appliance will go into a “pass-through” mode where the requests will be directed to the target content server.

Most FX Series Remote configuration is accomplished with an easy-to-use browser-based tool to set policies on the FX Series ADC appliance. The configuration policies are designed to provide full inheritance properties, meaning that most configuration settings are shared between all FX Series Remote appliances, but individual over-rides can be set for specific FX Series Remote appliances. Examples of policy-based settings include:

- Bandwidth reservation and prioritization
- HTTP application optimization
- Compression and caching settings for HTTP, CIFS, POP3, SMTP, and FTP

### 1.6.2 TCP Optimization and Data Compression

All TCP traffic between the FX Series Remote is compressed using intelligent data dictionaries to ensure that repeated patterns are eliminated from subsequent accesses. Several techniques are utilized to guarantee that the TCP communications between the FX Series Remote and the FX Series head-end appliance are fully optimized, including:

#### **RFC3649**

"High-speed TCP for Large Congestion Windows"

#### **TurboStreaming**

Moves data streams over multiple concurrent TCP connections between FX Series Remote appliances and FX Series head-end appliance. This insulates the FX Series from intermittent packet loss, as data is almost always going at full speed over at least one of the connections.

#### **HTTP Optimization**

The optimization techniques of the FX Series client acceleration are built into the FX Series Remote appliance, resulting in highly optimized delivery of HTTP applications to remote site users without having to deploy software on individual computers. Some of the optimizations that FX Series Remote appliance can apply to HTTP applications include:

- Caching of static objects
- Cache differencing of dynamic content
- Cookie Compression

### 1.6.3 Reporting

Important FX Series Remote appliance events are consolidated at the FX Series ADC appliance. These events are recorded so that the following consolidated reports can be viewed on the Remote Appliance:

- Acceleration Statistics
  - Aggregate Statistics
  - Current Connections
- Throughput Statistics
  - Aggregate Throughput

### 1.6.4 Deployment Options

The FX Series Remote can run in bridged mode, in routed mode or in WCCP mode.

The installation instructions for these are in the FX Series Installation Patterns Section.

## 1.7 Mesh Networking with the FX Series

### 1.7.1 Theory of Operation

In addition to the single sided and the two sided client/server or Hub/Remote star network, we've now introduced a full mesh network. We accelerate traffic from the FX Series Remote to the FX Series ADC, with both appliances at each site.



NOTE: The FX Series Mesh can utilize the FX1005 appliances in a dual rack installation.

The FX Series Remote accelerates traffic by intercepting user requests and forwarding them to the FX Series ADC. The FX Series ADC applies deflate compression, image transformation, static and dynamic content caching.

The FX Series Remote applies static content caching, dynamic content caching, deflate compression, Dynamic Data De-duplication, persistent connections, connection multiplexing, client side connection termination, and TurboStreaming. To the client, the FX Series Remote appears to be the back-end server.

### 1.7.2 Mesh Capability with two FX Series appliances at each node

- All optimizations are handled – Remote to ADC
- Traffic shaping, is done with the FX Remote, not the FX ADC
- The first ADC picks up the traffic and will accelerate/optimize it.

The configurations for each appliance are done separately and have a cable connected between the Remote LAN port and the ADC WAN port as shown below.

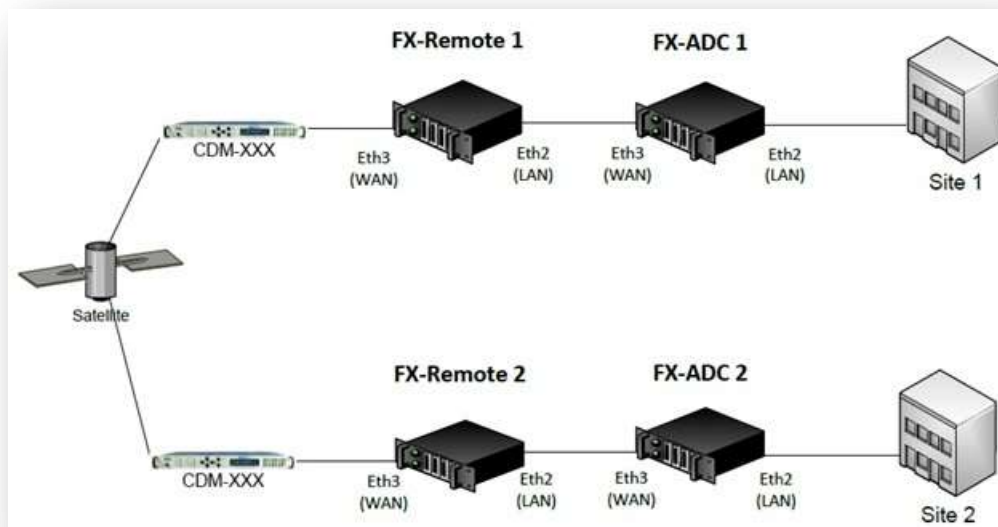


Figure 1-2 FX Series Basic Mesh Connectivity Diagram

- Hub/Spoke with meshing between FX Remotes, with the FX ADC hub available for web browsing and other applications.

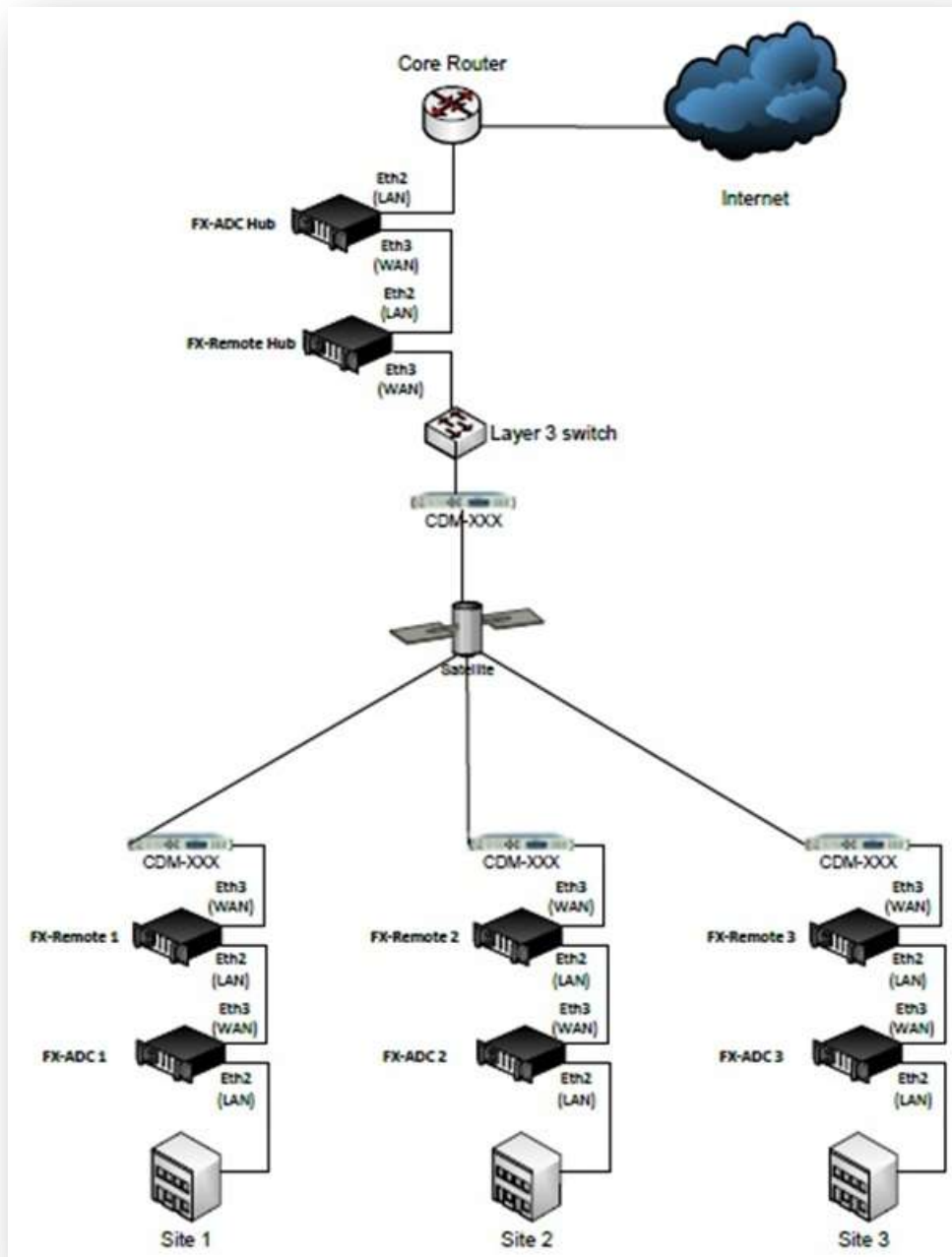


Figure 1-3 FX Series Hub Spoke Mesh Connectivity Diagram

- Mesh configuration with Redundancy

The Redundancy configuration could be set up at each site to provide total redundancy

The fail to wire capability is structured between the two like devices and between the Remotes and the ADC as shown below.

The appliances are connected in series as shown below.

See the mesh deployment installation pattern for details.

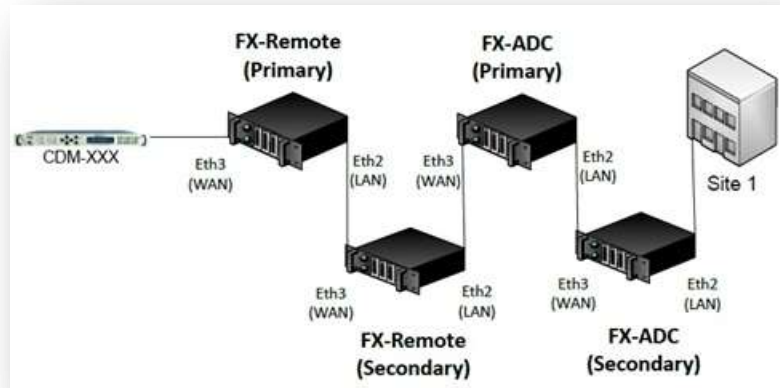


Figure 1-4 FX Series Mesh with Redundancy Connectivity Diagram

## 1.8 FX Series Appliances Data Sheet

Deploy the Stampede FX Series (ADC) as a single-sided solution to optimize traffic from your outbound channel. For a two-sided solution, add the FX Series Remote (REM) appliance and achieve the ultimate in application acceleration and WAN optimization.

### 1.8.1 Single Sided with the Application Delivery Controller (ADC)

	FX-1005 ADC	FX-4010-ADC
<b>Max Accelerated Sessions</b>	3,000	30,000
<b>Data Rate Options Mbps</b>	1, 2, 4, 6, 10, 15	10, 15, 25, 45, 70, 155, 310
<b>Load Balancing via WCCP</b>	✓	✓
<b>Connection Management</b>	✓	✓
<b>Advanced Traffic Shaping with ACM (d)</b>	✓	✓
<b>Source IP Preservation</b>	✓	✓
<b>Optimize VLAN Tagged Data</b>	✓	✓
GZIP Compression (b)	✓	✓
Image Reduction (c)	✓	✓
<b>Content Caching</b>		
Static Caching	✓	✓
<b>Redundancy - In-Path and Routed Modes</b>	✓	✓

### 1.8.2 Two Sided with the ADC and the Remote

	FX-1005 REM/ADC	FX-1010 REM	FX-4010 REM/ADC
<b>Max Accelerated Sessions (a)</b>	6,000 (a)	6,000	30,000 (a)
<b>Data Rate Options Mbps</b>	1, 2, 4, 6, 10, 15	2, 4, 6, 10, 15, 25	10, 15, 25, 45, 70, 155, 310, 700 (f)
<b>Header Compression Rate (PPS) (e)</b>	35,000		700,000
<b>Load Balancing via WCCP</b>			
<b>Connection Management</b>	✓	✓	✓
<b>Traffic Shaping with ACM (d)</b>	✓	✓	✓
<b>IP Source Preservation</b>	✓	✓	✓
<b>Optimize VLAN Tagged Data</b>	✓	✓	✓
<b>Multicator</b>	✓	✓	✓
<b>Content Reduction</b>			
Bi-directional Compression	✓	✓	✓
Image Reduction (c)	✓	✓	✓
Dynamic Data De-duplication	✓	✓	✓
<b>Content Caching</b>			
Static Caching	✓	✓	✓
Cache Differencing	✓	✓	✓
<b>TCP Optimization</b>	✓	✓	✓
<b>Multiplexing Data Streams</b>	✓	✓	✓
<b>Auto Updates to the Remotes</b>	✓	✓	✓

Figure 1-5 FX Series Appliances Data Sheet

NOTES: (a) (b) (c) (d) (e) (f) See DATA SHEET Notes on next page

## Data Sheet Notes:

- (a) When used as an ADC, the FX-1005 will handle 3000 concurrent sessions.
- (b) Maximum accelerated WAN rates are a function of compressibility. If all content is being GZIP compressed with a ratio of greater than 4:1, the maximum WAN rate may not be accelerated.
- (c) The number of images handled per second is a function of image size.

	FX-4010-ADC	FX-1005-ADC
IMAGE SIZE	IMAGES PER SECOND	IMAGES PER SECOND
10 KB	1800	80
50KB	1000	35
500KB	100	35

- (d) Available as either a stand-alone feature or part of the WAN optimization product. As a stand-alone feature, the maximum data rate is 700 Mbps, when purchased with the WAN optimization; the data rate is limited to the WAN optimization rate.
- (e) Packets per second (PPS) is 50% outbound and 50% inbound. Header compression is currently only available in point-to-point configurations and is not currently supported in the FX-1010. Header Compression is currently available as either a standalone feature added to the base configuration or part of the WAN Optimization product. When purchased without the WAN Optimization feature the maximum rate is 700KBps. When included with WAN Optimization, the data rate is limited to the WAN Optimization rate.
- (f) Header Compression only.

## Configuration Models

Base Configuration with QOS only as an option with no WAN Optimization.

Option 1 Add Header Compression (rates up to 700KBps) with no WAN Optimization.

Option 2 Wan Optimization including Header Compression with rates as shown in the tables.

## 1.8.3 FX Series Hardware Specification



	FX Series 1005	FX Series 1010	FX Series 4010
<b>Model</b>	<b>FX-1005</b>	<b>FX-1010</b>	<b>FX-4010</b>
<b>Form Factor</b>	1RU	1RU	1RU
<b>Weight</b>	2.6 lbs (1.2kg)	13.3 lbs (6.0 kg)	15 lbs (6.8 kg)
<b>Dimensions (h x w x d)</b>	1.7" x 8.5" x 7.4" (43 x 215 x 188 mm)	1.7" x 17.0" x 15.6" (44 x 431 x 395 mm)	1.7" x 16.8" x 14.0" (43 x 427 x 356 mm)
<b>Memory</b>	4 GB	4 GB	16 GB
<b>Storage</b>	(1) 160 GB SATA	(1) 160 GB SATA	(1) 1 TB SATA III
<b>Network Interface (GE) Ports/Fail-to-Wire Pairs</b>	4/1	11/0	4/1
<b>Serial Ports</b>	1	1	1
<b>USB Interface Ports</b>	2	2	2
<b>Rack Mount Kits</b>	1 or 2 units in 1RU		
<b>Power Supply – UL Approved, FCC Compliant</b>	Requires a 60 W/12V power adapter with lock	200 W ATX power supply unit with input range of 90~264V@ 47-63 Hz	Single Power (200 W) Auto (100V-240V)
<b>Environment</b>	Operating temp 0 - 40°C, Storage temp -20 - 60°C, Humidity 5 - 90%	Operating temp 0 - 40°C, Storage temp -20 - 60°C, Humidity 5 - 90%	Operating temp 10 - 35°C, Storage temp -40 - 70°C, Humidity 8 - 90%

Figure 1-6 FX Series Hardware Specifications

## 1.8.4 FX-4010 Physical Description

### Back Panels

Using suitable RJ-45 cable, you can connect FX Series FX-4010 System to a computer, or to any other piece of equipment that has an Ethernet connection; for example, a hub or a switch. Moreover, LAN3-LAN4 is configured as LAN Bypass when failure events occur.

- 1) (MGT) Management
- 2) (AUX) Auxiliary
- 3) (LAN)
- 4) (WAN)



**Figure 1-7 FX Series FX-4010 Back Panel**

From left to right

1. Power-In Socket
2. Inputs for mouse and keyboard
3. (2) USB 2.0 Ports
4. Serial Port
5. VGA Port
6. MGT Port Eth(0)
7. AUX Port Eth(1)
8. LAN Eth(2)
9. WAN Eth(3)



## 1.8.5 FX-1005 Physical Description

### Front Panel



Figure 1-8 FX Series FX-1005 Front Panel

#### Power/Status/HDD LED (left vertical icons)

**Power** (Green): If the LED is on it indicates the system is powered on. If it is off, it indicates the system is powered off.

**Status** (Green/Amber): If the LED is Green, it indicates that the system's operational state is normal.

If it is Amber, it indicates that the system is malfunctioning.

**HDD** (Yellow): If the LED blinks, it indicates data access activities; otherwise, it remains off.

#### LED indicators for Network Ports:

**1 Management Port      2 Auxiliary Port      3 LAN Port      4 WAN Port**

LED Indicator	Interpretation
	<b><u>SPEED</u></b>
<b>Amber</b>	The connection speed is 1000Mbps
<b>Green</b>	The connection speed is 100Mbps
<b>Off</b>	The connection speed is 10Mbps.
	<b><u>LINK/ACT</u></b>
<b>On/Flashing (Yellow)</b>	The port is linking.
<b>Off</b>	The port is not linking.

## Rear Panel



Figure 1-9 FX Series FX-1005 Rear Panel

### Reset Switch

Use a pointed object to press the reset button to reboot the system without turning off the power.

### Console Port

By using suitable rollover cable (also known as Cisco console cable), you can connect to a computer terminal for diagnostic or configuration purpose

### Two USB 2.0 Ports

It connects to any USB devices, for example, a flash drive

### 4 Gigabit LAN ports

Using suitable RJ-45 cable, you can connect FX Series 1005 System to a computer, or to any other piece of equipment that has an Ethernet connection; for example, a hub or a switch. Moreover, LAN3-LAN4 are configured as LAN Bypass when failure events occur.

- 1) (MGT) Management
- 2) (AUX) Auxiliary
- 3) (LAN)
- 4) (WAN)

### DC-in 12V Jack

The system requires a 60W/12V power adapter with lock.

### Power-on Switch

It is a switch to turn on or off the power.

## Summary of Specifications

Network Interface /Fail to Wire

Power Supply – UL Approved

(4) GbE ports, (1) pair bypass

200 W (Auto 100V – 200V)

System Subscription 1 Year of hardware/software support, maintenance and updates

## 1.8.6 FX-1010 Physical Description

### Front Panel



Figure 1-10 FX Series FX-1010 Front Panel

#### F1 Power/Status/HDD LED

##### Power:

If the LED is on it indicates that the system is powered on. If it is off, it indicates that the system is powered off.

##### Status:

If the LED is green, it indicates that the system's operational state is normal. If it is red, it indicates that the system is malfunctioning.

##### HDD:

If the LED is on, it indicates that the system's storage is functional. If the LED blinks, it indicates data access activities. If it is off, it indicates that there is no hard disk present or functional.

#### F2 System Panel: LCD System Panel

The LCD System Panel is programmed to display WOC on the first line and "Active" on the second.

#### F3 Reset Switch:

The reset switch can be used to reboot the system without turning off the power.

#### F4 Console Port:

By using suitable rollover cable or RJ-45 to DB-9 Female (Cisco console cable), you can connect to a computer terminal for diagnostic or configuration purpose. Default terminal Configuration Parameters: 115200 baud, 8 data bits, no parity, 1 stop bit, no flow control.

#### F5 Two USB 2.0 Ports:

It connects to any USB devices, for example, a flash drive.

#### F6 Management Port and Auxiliary Ports:

The Management Port is a Fast Ethernet port that can be connected for configuration or troubleshooting purpose. It conforms to the IPMI (Intelligent Platform Management Interface) and can be implemented on this port through the Open Platform Management Architecture (OPMA) interface.

#### F7 5 Gigabit LAN ports (Ports 1-5)

##### Right LED:

If the LED is orange, it indicates that the connection speed is 1000Mbps. If the LED is green, it indicates that the connection speed is 100Mbps. And if it is off, it indicates that the speed is 10Mbps.

**Left LED:**

If the LED is on, it indicates that the port is linked. If it blinks, it indicates there is traffic.

Using suitable RJ-45 cable, you can connect FX-1010 system to a computer, or to any other piece of equipment that has an Ethernet connection; for example, a hub or a switch.

**F8 4 Gigabit LAN ports (Ports 6, 7, 8, WAN) Expansion Module**

This expansion of the LAN switch adds an additional 4 Ethernet ports.

**Rear Panel**



**Figure 1-11 FX Series FX-1010 Rear Panel**

**4 System CPU Fans**

**Power-on Switch**

**AC Power-in socket -**

200W ATX power supply unit with input range of 90~264V@47-63Hz.

**Power Supply Fan**

**Summary of Specifications**

Network Interface /Fail to Wire (4) 10/100/1000, (1) 10/100/1000 bypass pair

Power Supply – UL Approved 200 W (Auto 100V – 200V)

System Subscription - 1 Year of hardware/software support, maintenance and updates

**Rack Mounting**

Rack mounting hardware is included with FX-1010 appliance

## 1.8.7 Hardware Mounting Options for FX Series FX-1005

### Tabletop Mounting (Standard)

To mount the FX-1005 on the table, use the rubber feet in the tabletop mounting pack. Follow the following procedures as a guideline: (may be pre-attached)

1. Place the rubber feet on the mounting spots at the bottom of the FX-1005 .
2. Place the FX-1005 on the table using the rubber feet.

### Double Unit Rack Mount (Optional Accessory)

To mount two FX-1005 systems onto the rack, use the mounting kit with the screw pack. Follow the following procedures as a guideline:

1. Attaching two screws having a washer under the head to the inner side of the system's chassis.
2. Align the screws of one system with the mounting slots of the other system and mount the two systems side by side by clipping them together
3. Make sure that the attachment between the two systems is secure and the mounting screws are locked in place.
4. Use the screws provided to fix the short ear-bracket to the left and right sides of the system as shown in the picture.
5. Use the mounting hardware included to attach and secure the bracket to the rack.



Installing the ear-bracket to the rear side as an alternative rack mounting

**NOTE:** The short-ear bracket could also be mounted at the rear side of the system. Thus, the rear panel of the system could be mounted in the front of the rack mounting equipment.

### Single Unit Rack Mount (Optional Accessory)

**NOTE:** Place the power adaptor in the bracket first before installing the adaptor holder.

To mount the FX-1005 onto the rack, use the mounting kit with the screw pack.

Follow these procedures as a guideline:

1. Attach the adaptor mounting bracket to the system by fastening 5 screws
2. Place the adaptor in the adaptor mounting bracket.
3. Make sure that the power adaptor's AC socket is not blocked. Align the AC socket with the holes on the mounting bracket.
4. You could use the adaptor holder to hold your adaptor to prevent it from sliding back and forth.
5. Use 3 screws provided to fix the bracket to the left and right side of the system.
6. Use the mounting hardware included to attach and secure the bracket to the rack.



## 2 Pre-Installation Information

### 2.1.1 Unpacking

Inspect shipping containers for damage. If shipping containers are damaged, keep them until the contents of the shipment have been carefully inspected and checked for normal operation.

The FX Series appliance is packaged in pre-formed, reusable, cardboard cartons containing foam spacing for maximum shipping protection.

Unpack the appliance as follows:

#### Step Procedure

- 1 Remove the appliance, and the power cord and cables from the carton.
- 2 Save the packing material for storage or reshipment purposes.
- 3 Inspect the appliance for any possible damage incurred during shipment.
- 4 Check the equipment and accessories against the packing list to ensure the shipment is correct.

#### Parts List

Acceleration Appliance

Quick Start Guide

1 - Power Cord

2 - Cat5e 7ft UTP Snagless Cable

1 - Cat5e Crossover Red 7ft UTP Snagless Cable

1 – Null Modem 6ft Cable

### 2.1.2 User Interfaces

The FX Series supports a basic menu-driven interface, which is accessible using the console port (eth0) or a web-based graphical user interface (GUI). Initial network configurations are managed thru the console connection, and the optimization and general operations functions are managed via the GUI. There are three alternate methods to connect to the FX Series Appliance

1. Attach a Monitor, keyboard and mouse to device.
2. Connect the supplied serial cable with a setting of (19200,N,8,1)
3. Attach a cross-over cable to the eth1 interface which has a static IP address of 169.254.55.55

(See [FX Series Console Management Functions in Appendix](#))

To connect to the Web GUI using a PC with a Browser access:

<http://yourFxHostname:10000> or

<http://IP:10000>

The default USERID and PASSWORD are “comtech” and “comtech” for both the console and the GUI.



### 2.1.3 Documentation

Before you try to install the FX Series appliance on your network, please review the documentation in the [\*Installation Patterns Guide\*](#).

Current Documentation for this appliance can be found on these locations.

**On the Comtech EF Data web site:**

<http://www.comtechefdata.com/stampedeDocs.asp>

Or

[www.comtechefdata.com](http://www.comtechefdata.com)

Under Support Information, Click on Manuals

Under [\*RAN & WAN Optimization\*](#), click on [Stampede FX Series](#)

**On the Appliance:**

To connect to the GUI, use any PC with a Web Browser to access:

- Attach a cross-over cable to the eth1 interface and connect to the browser interface at <http://169.254.55.55:10000>
- Login using the USERID and password of “comtech” and “comtech”
  - Using the web GUI
  - Click on the FX Series Appliance Administration link for the Main Index
  - Click on “Documentation” from the Main Index

To view a document, click on the link in the left column of each row of the table. You can right click on the link and choose “Save target as” to save a copy of the “.pdf” file to your desktop.

---

## 2.2 Configure Appliance Management Address – All Installation Patterns

*Log into the appliance via console or SSH session using the username: comtech and password: comtech*

- 1 Select option 1 “Configure appliance”
- 2 Select option 1 “Configure network settings”
- 3 Select option 4 “Configure TCP/IP for eth0 Ethernet Port”
- 4 Select option 1 “Configure DHCP”
  - a. Enter no and press Enter key (disable DHCP for this interface)
- 5 Select option 2 “Configure IP Address”
  - a. Enter the IP address of the appliance and press enter
- 6 Select option 3 “Configure Netmask”
  - a. Enter the subnet mask and press the Enter key
- 7 Select option 0 “Return to previous menu”
- 8 Select option 3 “Configure Default Gateway”
  - a. Enter the default gateway IP address and press the Enter key

*Verify network connectivity by doing a ping of the appliance address from an external device.*

Depending on the environment, there are several network installation patterns that can be used.

- Bridged (“In-Path”)
- Routed
- WCCP
- Mesh

These are documented in the FX Series Network Installation Patterns section of the Administration Guide.

## 3 FX Series Network Installation Patterns

### 3.1 FX Series Installation Pattern (In-Path Bridged)

#### 3.1.1 Cable the Appliance

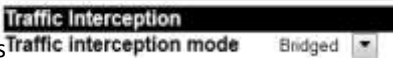
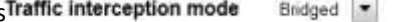
The eth2 (LAN) and eth3 (WAN) ports both need to be connected to a switch or router in which:

1. The eth2 (LAN) port is on the link closest to the:
  - a. Backend servers if the appliance is an FX-ADC.
  - b. Clients if the appliance is a FX-Remote.
2. The eth3 (WAN) port is on the link closest to the satellite modem.

#### 3.1.2 Configure the Appliance

Login to the appliance through the browser interface at:

[http://{IP\\_address\\_of\\_the\\_appliance}:10000](http://{IP_address_of_the_appliance}:10000)

1. Enter the default user name “comtech” and the default password “comtech”.
  - a. Click Login.
2. Click Configuration -> General Settings
  - a. Change “Traffic interception mode” to “Bridged”.
    - b. Click Save. 
3. Click In-Path Interfaces 
  - a. Click the Add button to add a new in-path interface.
    - Enter the VLAN ID of 0. If no VLAN tagging is to be used. Use the VLAN ID of the VLAN if traffic is to be VLAN tagged
    - Enter the IP Address.
    - Enter the Netmask.
    - Enter the Gateway.
    - Enter any static routes needed in the “Routes” field.
  - b. Click “Add In-Path Interface”.
  - c. Click the “Return to Configuration” link.
4. Click on LAN Interfaces.
  - a. Click on the “Add” button to add a new LAN interface.
    - Select “eth2” in the “Physical interface” selection box.
    - In the “In-Path Interface(s)” selection box, click the IP address of the in-path interface \*from above\*.
    - In the “Untagged in-path interface” selection box, select the IP address of the in-path interface \*from above\*. Select “None” if the VLAN tag is to be propagated across the WAN.
  - b. Click “Add LAN Interface”.
  - c. Click the “FX Series Administration Index” link at the top of the page.
5. Click “Status”, then click “Real-Time Monitor”, then click “Restart Service”.






## 3.2 FX Series Installation Pattern (Routed)

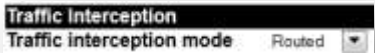
### 3.2.1 Cable the Appliance

Connect the eth3 (WAN) port to a switch or a router.

### 3.2.2 Configure the Appliance

Login to the appliance through the browser interface at:

[http://{IP\\_address\\_of\\_the\\_appliance}:10000](http://{IP_address_of_the_appliance}:10000)

1. Enter the default user name "comtech" and the default password "comtech".
  - a. Click Login.
2. Click Configuration -> General Settings
  - a. Change "Traffic interception mode" to "Routed"
 
  - b. Click Save
3. Click In-Path Interfaces
  - a. Click the Add button to add a new in-path interface.
    - Enter the VLAN ID of 0, if no VLAN is to be tagged. Use the VLAN ID of the VLAN if traffic is to be VLAN tagged.
    - Enter the IP Address.
    - Enter the Netmask
    - Enter the Gateway
    - Enter any static routes needed in the "Routes" field.
  - b. Click "Add In-Path Interface"
  - c. Click the "Return to Configuration" link
4. Click on LAN Interfaces.
  - a. Click on the "Add" button to add a new LAN interface.
    - Select "eth3" in the "Physical interface" selection box.
    - In the "In-Path Interface(s)" selection box, click the IP address of the in-path interface \*see above\*.
    - In the "Untagged in-path interface" selection box, select the IP address of the in-path interface \*see above\*. Select "none" if the VLAN tag is to be propagated across the WAN.
  - b. Click "Add LAN Interface".
  - c. Click the "FX Series Administration Index" link at the top of the page.




5. Click "Status", then click "Real-Time Monitor", then click "Restart Service".

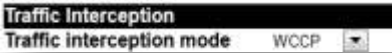
### 3.3 FX Series Installation Pattern (WCCP)

#### 3.3.1 Cable the Appliance

Connect the eth2 (LAN) port to a switch or a router.

#### 3.3.2 Configure the Appliance

Login to the appliance through the browser interface at: [http://{IP\\_address\\_of\\_the\\_appliance}:10000](http://{IP_address_of_the_appliance}:10000)

6. Enter the default user name “comtech” and the default password “comtech”.
  - a. Click Login.
7. Click Configuration -> General Settings
  - c. Change “Traffic interception mode” to “WCCP”
  - d. Click Save 
8. Click In-Path Interfaces
  - a. Click the Add button to add a new in-path interface.
    - Enter the VLAN ID of 0.
    - Enter the IP Address.
    - Enter the Netmask
    - Enter the Gateway
    - Enter any static routes needed in the “Routes” field.
  - b. Click “Add In-Path Interface”
  - c. Click the “Return to Configuration” link



FX Series Administration Index Help

Configuration->In-Path Interface->Edit

**In-Path Interface Definition**

VLAN ID

Status  Disabled  Enabled

Address

Netmask

Gateway

Routes

Router polling  Disabled  Enabled

Poll address

SNMP version  2c  3

Poll community

Poll interval (seconds)

In-band management  Disabled  Enabled  
Change requires restart

Comment

Add In-Path Interface

Return to In-Path Interface

9. Click on LAN Interfaces.
  - a. Click on the “Add” button to add a new LAN interface.
    - Select “eth3” in the “Physical interface” selection box.
    - In the “In-Path Interface(s)” selection box, click the IP address of the in-path interface \*see above\*.
    - In the “Untagged in-path interface” selection box, select the IP address of the in-path interface \*see above\*.
  - b. Click “Add LAN Interface”.
  - c. Click the “FX Series Administration Index” link at the top of the page.
  - d. Click “Status”, then click “Real-Time Monitor”, then click “Restart Service”.
  - e. Click the “FX Series Administration Index” link at the top of the page.
  - f. Click “Configuration”

10. Click “WCCP”



FX Series Administration Index Help

Configuration->LAN Interfaces->Edit

**LAN Interface Definition**

Active  No  Yes

Physical interface eth2

Comment

Speed

MTU 1500

In-Path interface(s)

192.168.4.40 VLAN 400

192.168.3.30 VLAN 300

192.168.2.20 VLAN 200

192.168.1.10 VLAN 500

Untagged in-path interface None

Untagged choice must be a selected in-Path interface

Add LAN Interface

Return to LAN Interfaces

- a. Click “Add WCCP Definition”
  - b. Select the IP address of the interface that will send the WCCP messages to the router in the “Source IP address” selection box.
  - c. Enter the routers IP address in the “Router address” field.
  - d. Select the local interface that will receive the GRE traffic if using GRE redirection. If using L2 redirection leave blank.
  - e. If using GRE redirection enter the router identifier of the router in the “Remote GRE tunnel address” field. If using L2 redirection leave blank.
  - f. Use default value for “Enablement”.
  - g. Use default value for “Critical”.
  - h. Select Redirection method.
  - i. Select the same value used for Redirection method.
  - j. For L2 use Mask Assignment scheme. For GRE use Hash Assignment scheme. \* This may differ on highest end Cisco equipment.
  - k. Leave the password field blank, unless one was configured for WCCP on the Cisco device.
  - l. If using “web-cache” WCCP redirection (no source IP address preservation) enter 0 in the “Service group number” field. If using source IP address preservation use the default value.
- 
- NOTE:** See Section 4.9 below for details and difference.
- m. Use the default values for “Redirect based on”, “Accept traffic for”, and “Ports”.
  - n. If using source IP address preservation select “Enabled” for “Use additional service group”. If using “web-cache” default this value.
  - o. Click “Add WCCP Definition”
11. Click “Status”, then click “Real-Time Monitor”, then click “Restart Service”.

### 3.4 Installation of Two FX Series Appliances in a Mesh Configuration

This configuration consists of two FX Series appliances, one configured as a FX Series ADC and the second appliance configured as a FX Remote.

NOTE: Two FX1005 appliances can be installed in a rack using the Double Unit Rack Mount (See 1.8.7 above)

A short cable is provided for the connection from the Remote's LAN port to the ADC's WAN port (the yellow connection in the figure below:

(See picture of rear panel in section 1.8.5 above)

1. Connect the Eth3 (WAN) port of FX Remote to the satellite connection. [Blue]
2. Connect the Eth2 (LAN) port of the FX-Remote to the Eth3 (WAN) port of the FX-ADC. [Yellow]
3. Connect the Eth2 (LAN) port of the FX-ADC to the user network. [Green]

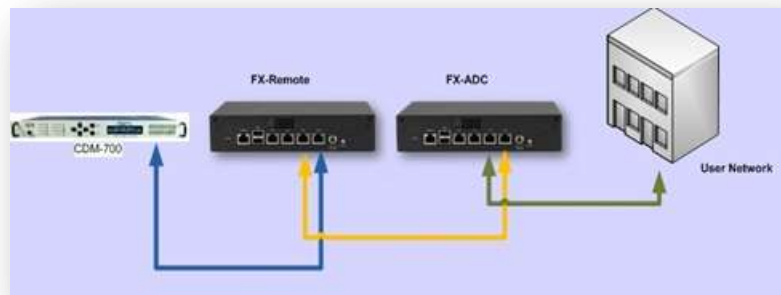


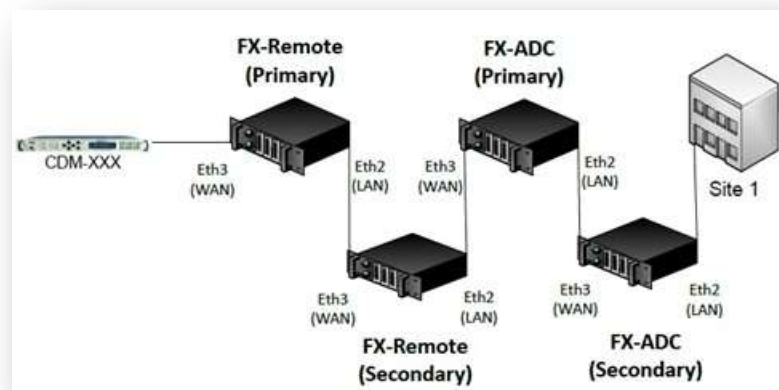
Figure 3-1 FX Series Mesh Connection Diagram

#### 3.4.1 Configure the appliances

Configure as noted in Sections 2.2 and 3 above

#### 3.4.2 Mesh installation with Redundancy capability

This scenario consists of two sets of appliances at the site. The configuration for each appliance is done separately to backup FX Series Appliances with fail to wire configuration. The configuration setups are similar as described in Section 4.8 below and is shown diagramed here.



## 4 FX Series Network Settings



Figure 4-1 FX Series Standard Configuration Screen

### 4.1 Standard Network Configuration Overview

The following network screens provide common interfaces for the FX Series appliances.

#### Application Policies

Customize the optimization techniques that will apply to your enterprise applications.

(See the Optimization Acceleration Settings in Section 8 below).

#### FX Series Basic Network Interfaces

Define network settings for management and auxiliary interfaces.

#### FX Series General Settings

The General Settings control the method of traffic interception and WCCP. In addition, this section includes settings to configure basic HTTP settings, system time and software updates of FX-Remotes. See Specific Sections below.

[FX Series ADC Specific Settings Section](#)

[FX Series Remote Specific Settings Section](#)

#### FX Series Redundancy

Configure a Redundancy cluster that can share a common configuration.

#### FX Series Host Settings

Configure the host name and DNS settings to facilitate management and time synchronization.

#### FX Series In-Path Interfaces

For FX Series ADC see: Configure network settings for the interfaces for user data.

For FX Series Remote In-Path Interfaces see: [FX Series Remote Specific Settings Section](#).

#### FX Series LAN Interfaces

Set speed, MTU and VLAN options of the physical LAN interfaces. .

#### FX Series Multicator Settings

Configure reliable multicast fan-out settings.

### Port Definitions

Configure a list of port definitions see: [FX Series ADC Specific Settings Section](#).

### FX Series Quality of Service Settings

Define ACM settings and configure QoS.

### WCCP Settings

The Web Cache Communication Protocol (WCCP) is a Cisco-developed content-routing technology which allows you to integrate cache engines into your network infrastructure.



**NOTE:** The screens that have specific functionality for the FX Series ADCs or the FX Series Remotes can be found in these sections: [FX Series ADC Specific Settings Section](#) or the [FX Series Remote Specific Settings Section](#).

## 4.2 Basic Network Interfaces

The FX Series reserves two ports, management and auxiliary, for management traffic. This traffic is isolated from the ports in which accelerated traffic flows. These interfaces are tied to a management routing table which is not used for accelerated traffic.

The screenshot shows the 'FX Series Administration Index' with a 'Help' link. The main heading is 'Configuration->Basic Interfaces'. There are two main sections: 'Management Interface' and 'Auxiliary Interface'. Each section has a dropdown menu for 'Automatically obtain IPv4 address' (currently set to 'Disabled'). Below each dropdown are input fields for 'IPv4 address', 'Subnet mask', and 'Default gateway'. There is also a 'Speed' dropdown (set to 'Auto') and a 'Max transmit unit' input field (set to '1500'). Below these sections is a section titled 'Management and Auxiliary Static Routes' with a 'Routes' table and a 'Save' button. At the bottom left, there is a 'Return to Configuration' button with a left-pointing arrow.

Figure 4-2 FX Series Basic Network Interfaces Screen

### 4.2.1 Management Interface

The management interface corresponds to the “eth0” Ethernet port. Typically the management interface is connected to a private network where system management tools such as ssh, the management web GUI, and SNMP are utilized.

#### Automatically obtain IPv4 address:

If set then the FX appliance will use DHCP to obtain an IP address, subnet mask, and default gateway. The factory default for the management interface is to use DHCP.

#### IPv4 Address:

This is the IP address of the management interface.

#### Subnet Mask:

This specifies the network that the management interface is on. The default value is 255.255.255.0.

**Default Gateway:**

This is the IP address of the gateway for which packets that are outside the bounds of the management subnet will be directed. A default gateway address which is on the same subnet as depicted by the “IPv4 address” and “Subnet mask” must be specified even if the gateway does not exist.

**Speed:**

This presents a pull-down selector of speed/duplex combinations that will be set for this interface. The default value is to automatically negotiate the speed and duplex.

**Max Transmit Unit (MTU):**

Specifies the max transmit unit. The default value is 1500. The range is 576 to 9000.

#### 4.2.2 Auxiliary Interface

**Automatically obtain IPv4 address:**

If set, then the FX appliance will use DHCP to get an IP address, subnet mask, default gateway.

**IPv4 address:**

This is the IP address of the auxiliary interface. The factory default is 169.254.55.55.

**Subnet mask:**

This specifies the network that the auxiliary interface is on. The default value is 255.255.0.0.

**Speed:**

This presents a pull-down selector of speed/duplex combinations that will be set for this interface. The default value is to automatically negotiate the speed and duplex.

**Max Transmit Unit (MTU):**

Specifies the max transmit unit. The default value is 1500. The range is 576 to 9000.

#### 4.2.3 Management Static Routes

**Routes:**

Enter into the text area static routes which are used by the management interface. Each static route must be entered on a separate line and must have exactly the following format:

Subnet “SubnetMask” “Gateway”

For example, to define a static route such that subnet 172.88.0.0/16 should be routed by gateway 172.27.101.99 you would enter the following:

172.88.0.0 255.255.0.0 172.27.101.99



## 4.3 Host Settings

In most environments, configuring host names and DNS is not required for the FX to operate because for most accelerated traffic, the IP address of the content server is resolved by the originating client before it is processed by the FX. The host settings should be set to facilitate management and time synchronization.

**Configuration->Host/DNS Settings->Edit**

**Host Networking Settings**

Host name

Domain

DNS servers

**Host File Entries**

Hosts

[Return to Configuration](#)

Figure 4-3 FX Series Host/DNS Settings Screen

### 4.3.1 Host Networking Settings

**Host name:**

This is the host name of the appliance. This must be a “short” name and must not contain any periods. A fully qualified name is formulated by appending a ‘.’ followed by whatever is entered into the “Domain” field.

**Domain:**

This is the DNS domain of the appliance.

**DNS Servers:**

Enter one or more IP addresses separated by commas.

### 4.3.2 Host File Entries

#### Hosts:

If no DNS is available, this field allows you to map specific host names to an IP address. This may be needed for active-passive redundant configurations. Each entry should be on a separate line. The format of each line is:

`"nn.nn.nn.nn FullyQualifiedHostName OptionalShortHostName"`

Where nn.nn.nn.nn is the IPv4 address that you want to assign to FullyQualifiedHostName".

#### DNS Server Configuration Guidelines:

In order for the fully qualified host name to be accurate within a domain, it is a best practice to set your local DNS server to match the IP address of the FX appliance with the name "Host name" and "Domain" fields on this page. Or you can set a "Host File Entry" with the IP address of the FX appliance with the fully qualified name and the short name.

## 4.4 In-Path Interface

These settings allow you to maintain in-path interfaces. A list of previously defined in-path interfaces are displayed in the order in which they were defined. An existing entry may be chosen by clicking on the IP Address. The user adds interfaces by clicking the “Add” button. Interfaces can be “enabled” or “disabled” by checking box to the left of the IP address and clicking on the enable or disable button. Clicking on the Interface “Name” will allow you to modify that Interface. Each of those actions will then lead to an In-Path Interface screen.

Figure 4-4 FX Series In-Path Interfaces Definition Screen

### 4.4.1 In-Path Interface Definition

#### VLAN ID:

If this interface carries tagged VLAN traffic, then enter the VLAN ID number which is a value between 2 and 4094. Untagged traffic should have a value of 0. The default is 0.

#### Address:

This is the IPv4 address of this interface.

#### Netmask:

This defines the subnet boundaries of this interface.

**Gateway:**

This is the default gateway for this interface.

**Routes:**

Enter into the text area static routes which are used by this in-path interface. Each static route must be entered on a separate line and must have exactly the following format:

Subnet "SubnetMask" "Gateway"

For example, to define a static route such that subnet 172.88.0.0/16 should be routed by gateway 172.27.101.99 you would enter either of the following supported formats:

172.88.0.0 255.255.0.0 172.27.101.99

Or

172.88.0.0 /16 172.27.101.99

**Router Polling:**

If enabled, then SNMP router polling will be used (over the management interface) to ascertain the routes that should be added to the route table that is associated with this interface. The default value is disabled. Router polling is only supported for VLAN 0.

**Poll address:**

This is the IPv4 address of the router which will respond to the SNMP router poll requests.

**SNMP Version:**

This is the version of SNMP that will be employed when making the router poll requests. The default value is 2c.

**Poll Community:**

This is the SNMP community that is associated with the router poll request. The default value is "public".

**Poll Interval (seconds):**

This is the frequency in seconds that the router tables will be updated based upon the SNMP router polling response.

**In-Band Management:**

Normally out-of-band management of the FX is accomplished through the management interface, however in some scenarios, out-of-band management is not feasible and management of the device must be performed over an in-path interface. If this is the case, only one in-path interface may be used for in-band management. The default value is disabled.

**Comment:** This field provides a means to store useful information about the configuration



**NOTE:** Changing this setting requires a restart of the acceleration service on the "Status->Real-time Monitor" page.

## 4.5 LAN Interfaces

These settings allow you to maintain LAN interfaces.

The user adds interfaces by clicking the “Add” button. Interfaces can be “enabled” or “disabled” by checking box to the left of the IP address and clicking on the enable or disable button. Clicking on the Interface “Name” will allow you to modify that Interface. Each of those actions will then lead to a LAN Interface Configuration Screen.

### Working with LAN Interfaces without WAN Optimization

If you are utilizing the FX strictly for ACM QoS or packet compression, in order to configure a non-default MTU of the network interfaces, you must define a LAN interface for all network interfaces for which the traffic to be processed by the FX will flow through, typically these will correspond to “eth2” (LAN) and “eth3” (WAN) physical interfaces. In this case, it is recommended to have the MTU on both LAN interfaces to be the same.



**NOTE:** You must only do it if you want to have a non-default MTU

Figure 4-5 FX Series LAN Interfaces Screen

### 4.5.1 LAN Interface Definition

**Active:**

If adding a new LAN interface, this field allows you to set the initial status.

**Physical interface:**

Select the physical interface from the pull-down.

**Comment:**

This provides a place to store any user defined comment to describe the rationale for this VLAN definition.

**Speed:**

Select speed and duplex from the pull-down

**MTU:**

Specify a value between 576 and 9000. Note that when operating in “In-Line” mode, the MTU of the WAN interface will automatically be set to match the setting of the LAN interface.

**In-Path Interface(s):**

Select the in-path interfaces that can be connected to the physical interface. In a trunked environment, there may be multiple in-path interfaces connected to the physical interface.

VLAN tags will be preserved.

**Untagged in-path interface:**

You can specify one and only one of the selections from the “In-Path interfaces(s)” field or “None” If an in-path interface is selected then the VLAN tag associated with that in-path interface will be applied to the traffic received before forwarding it to the WAN interface and removed when forwarding traffic from the WAN interface. If “None” then no tags are added or removed. The “None” value will only be used when connecting to a “Trunked” interface.

**MAC Address:**

This field specifies the Ethernet address of the interface. This should only be set in redundant configurations where the traffic interception mode is ‘in-line’. In this case, this field should be set to the permanent MAC address of the primary. The permanent MAC address of this FX is shown in blue. If the field is left blank, then the permanent address of the FX is used.

## 4.5.2 Configure SNMP Settings

The system SNMP settings can be set using the “FX-Series Appliance Manager” using the console to access the management menus. MIB-II queries from SNMP monitoring tools such as HP OpenView can then be made.

**SNMP MIB Designation**

The optimization server’s SNMP designation for its MIB is 19418. The MIB files can be downloaded from the “Documentation” page and then compiled into an SNMP network management tool such as HP OpenView. All of the tallies that are shown via the “Detailed Statistics” button on the “Status->Real-Time Monitor” page may be queried. In addition, summary statistics for each application policy may also be queried as a table, which allows tracking of throughput statistics on a “per customer” basis, if application policies, tied to authorization realms that describe each customer, have been defined.

The MIB allows full management of the FX. The same MIB is used for both FX-Remote and ADC

**sysLocation:** This is used to indicate the physical location of this node (e.g. “telephone closet, 3rd floor”). If the location is unknown, the value is the zero-length string.

**sysName:** This is the name used to identify this appliance.

**sysContact:** This is the email address of the administrator that should be contacted regarding this appliance.

**Read-Only community:** This specifies the group of SNMP monitors that have read-only access to the MIB-II variables. The default value is ‘public’.

(See [FX Series Console Management Functions in Appendix](#))

To enter information, log into the appliance username: comtech password: comtech

Select Option "1 Configure Appliance"

Select Option "5 Configure SNMP"

The wrap SNMP configuration wizard Option 6 now prompts for destination 'trap' community and 'read/write' community. (Previous MIB was not read/write and did not emit traps (traps are an SNMP term for alerts))



Figure 4-6 FX Series SNMB Configuration Screen

## 4.6 Configuring Quality of Service with ACM

### 4.6.1 Overview

The Quality of Service Function with ACM option is intended to work with EF Data modems that support ACM. The FX Series ADC and Remote have the ability to read the current data rate from the modem, and will adjust the output data rate to match the modem data rate. The FX Series data rate is calculated based on the Ethernet frame header. The FX is also designed to work with the modem in a 1:1 Redundant with Fail Over mode and work with the modems when they are in a 1:1 redundant configuration.

#### Output Data Rate

All data rates are Ethernet frame rates. The total data rate is a parameter that can be set, or under the optional ACM mode, can be updated dynamically and continuously by polling the modem in the link.

#### Traffic Classification

Traffic can be classified on combinations of Protocol, VLAN, Source/Destination IP Port number, Source/Destination subnet, and DSCP bits. Classified traffic is directed into specified Queues. Queues are assigned priority.

#### Traffic shaping

Traffic is shaped using drain algorithms on the specified queues. Queues of equal priority are treated in a fair-weighted manner. Connections within a specified Queue are also treated in a fair-weighted manner.

The drain algorithms are strict priority or Min-Max. In Strict Priority, available bandwidth is allocated on the basis of priority. Min-Max gives more control. Bandwidth is allocated up to a committed information rate based upon priority. Once the committed information rate is reached for all classes, excess bandwidth is allocated based on the same priority, up to a defined maximum for each Queue.

### Quality of Service Configuration Menu



Figure 4-7 FX Series Quality of Service Menu

#### Dynamic ACM:

Set parameters for learning the data rate from the CEFD satellite modem and dynamically adjusting QoS settings based on this rate.

#### Filters:

Define rules to classify traffic and direct it to a queue based upon protocol, DSCP, VLANs, source / destination subnets, and ports.

#### Queues:

Defines the order and rate in which outbound traffic is sent.



## 4.6.2 Configure Dynamic ACM Parameters

### Dynamic ACM Parameters

Figure 4-8 FX Series Dynamic ACM Configuration Screen

#### Poll Satellite Modem:

This setting allows you to enable or Disable polling of the satellite modem. The default value is “Disabled”.

#### Modem IP Address:

This is the IP address of the CEFD satellite modem. (This field must be entered if Polling is enabled). A second IP address may be added separated by a comma. This second IP address can be used for 1:1 redundancy in which case the primary modem rate will be used. If the secondary modem responds, then its rate will be used. If a second modem is specified, then the FX assumes that both have the same SNMP community.

#### Modem type:

This allows you to set the CEFD satellite modem type. (Default: CDM-750).

#### Modem SNMP community:

This is the read-only community of the satellite modem.

#### Polling frequency (msecs):

This is the period in milliseconds that the FX will wait between polls to ascertain the data rate from the modem. (Default: 250)

**Reserve bandwidth (Kbps):**

The data rate that the FX delivers data is the Ethernet frame rate. This parameter sets the amount of bandwidth that will be held in reserve. The FX will deliver data at the rate read from the modem minus this rate. This will allow for any mismatch between the Ethernet frame rate, and the rate that the modem reports.

**Clear sky data rate (kbps):**

This is the output data rate that will be used if the FX is unable to read a rate from the modem. The default is the FX licensed rate.

**Traffic Control Properties****Queue drain algorithm:**

This parameter specifies the drain method for scheduling outbound packets for all Queue definitions.

**Strict Priority:**

In the Strict Priority Drain algorithm, higher priority queues are depleted before lower priority queues pass traffic. Traffic is capped at the link rate.

**Min-Max:**

The drain algorithm is priority based. If there is enough data rate available, each queue will receive their respective CIR. If there is not sufficient data rate to satisfy all of the requested CIRs, then traffic will be dropped starting with the lowest priority queue and progressing through the queues in ascending priority until the requested CIR is met.

When traffic is dropped from queues with the same priority, then each of the equally ranked queues will have traffic dropped proportionally.

Once all requested CIRs are met, if there is additional data rate that can be filled, it will be allocated to the queues in order of priority starting with the highest. Each queue is given additional data rate up to the requested rate, or MIR, whichever is lowest. If there are queues at the same priority, they are granted additional data rate proportionally.

**Packet Compression Settings****Compression method:**

Globally specifies the basic method of packet compression and aggregation. If 'disabled' then the feature is disabled. If 'L2 Point-to-Point' then compressed aggregated packets are encapsulated in Ethernet frames and sent directly to the MAC address specified in the 'MAC address of L2 peer' field. If this field is set up then you can enable/disable packet compression on a per QoS queue basis.

**MAC address of L2 peer:**

This setting specifies the MAC address of WAN Interface of the FX which will receive the encapsulated compressed and aggregated packets. The MAC address must be specified in format xx:xx:xx:xx:xx:xx where each 'xx' is a hex digit.



**NOTE:** In a redundant configuration, it is important to configure the MAC address field of the LAN interface associated with eth3 such that the primary and secondary FX devices utilize the same MAC address).

**MAC address of this device:**

This is a 'display-only' field that shows the MAC address of the WAN interface of this device which can be copied and pasted when configuring the L2 Peer.

## Redundancy/Fail Over

When two modems are specified in the Modem IP Address, the first modem identified is the primary modem; the other is the secondary. As long as the primary modem responds, it will be assumed to be the active modem. Once the primary modem fails to respond, as described below, the FX will switch over to the secondary modem. When the secondary modem is being used, if the primary modem begins to respond, then the FX will switch back to the primary modem.

The process that the FX uses to determine that a modem is non-responsive and should be assumed to be off line will be if any of the following three cases are satisfied:

- CASE 1: After the second unsuccessful attempt to set up a session to the modem, the modem will be assumed to be off line. The FX waits 10 seconds between attempts.
- CASE 2: If a session with the modem is dropped, after the first unsuccessful attempt to re-establish the session, the modem will be assumed to be offline.
- CASE 3: Once a session is set up, after 20 consecutive failures to get a successful poll to the modem, it will be assumed to be off line. If the modem fails to respond in 200 milliseconds, it is an unsuccessful poll. Note, that after waiting 200 milliseconds, the modem also waits the set period before attempting another poll.

The FX will attempt to establish a link with the modems over the management interface. If a link fails to get set up, then after waiting 10 seconds, another attempt is made. Once a link is set up, the modem will be polled as specified above. If the primary modem is assumed to be off-line, then the secondary modem will be used.



**NOTE:** IF BOTH MODEMS ARE ASSUMED TO BE OFF-LINE, THEN THE OUTPUT QOS RATE WILL BECOME THE CLEAR SKY DATA RATE OF THE FX APPLIANCE.

At all times, the modems will be polled, and once they respond, will be assumed to be on-line.

## Verifying ACM QoS Connectivity

To verify that the FX is correctly ascertaining the data rate from the VSAT modem, click on “Status->View Current Status” and select the “ACM QoS Status” button. This will cause the current data rate from all VSAT modems which were defined to be displayed, as well as tallies of successful and unsuccessful poll operations. This is an example of output for modem XXX.XXX.XXX.XXX and YYY.YYY.YYY.YYY.

```

Mon May 19 12:19:47 GMT 2013
Current data rate of satellite modem(s) at XXXXXX.XXX.XXX YYY.YYY.YYY.YYY is 28,748,848 bits per sec.
J High 3213 id receive
Modem: XXXXXX.XXX.XXX Current data rate is 28,748,848 bps RedundancyStatus=Primary
Successful polls=188, Rejected=0, PeakConsecutiveRejections=0
LastSession=0 FailedAttempts=0 GoodRedundancyPolls=0 RejectedRedundancyPolls=0
Modem: YYY.YYY.YYY.YYY RedundancyStatus=Backup
Successful polls=0, Rejected=0, PeakConsecutiveRejections=0
LastSession=0 FailedAttempts=0 GoodRedundancyPolls=0 RejectedRedundancyPolls=0

# QoS Queue
#
There are 6 qoses, of which 4 have packet compression enabled
-----
Name          Prio  Max Rate (bps)  Cur Rate (bps)  Drops      Flts on Q  ExposedBytes  ExposedPkts
-----
-Internal Signalling-  1    28,747,000      271,848         0           0           18,758,708    12,328
VIDEO 1          1    28,747,000      271,848         0           0           18,758,708    12,328
VIDEO 2          2    28,747,000     10,076,280      0           0           15,878,250    11,325
VIDEO 3          3    28,747,000      9,874,132       0           0           17,876,584    12,849
VIDEO 4          4    28,747,000      9,874,132       0           0           17,876,584    12,849
-Default-       5    28,747,000      228,128         0           0           28,721,184    18,482

# Filters
#
There are 6 filters
-----
Name          Prio.  Releas  Criteria
-----
-Internal Signalling-  Any    21,848
VIDEO 1          COP    237,884  DestPort=4000
VIDEO 2          COP    258,874  DestPort=3004
VIDEO 3          COP    299,800  DestPort=5000
VIDEO 4          COP    258,128  DestPort=5006
-Default-       Any    18,390

```

Figure 4-9 FX Series ACM QoS Status by VSAT Modem Screen

### 4.6.3 QoS Filter Definitions

If the user checks a box and clicks “Add” the rank will be set based upon the rank of the selected item. Each of those actions lead to a Filter Definition screen. The rules in the pick-list will be sorted based upon Rank. “Up” and “Down” buttons will appear at the bottom of the pick list to move rules up or down in priority. An existing entry may be chosen by clicking on the queue name.

The Default filter is a wild card filter that will always be the last filter evaluated. The Default filter maps data to the Default Queue. This can be reconfigured in the Filter Edit screen.



**NOTE:** If the FX appliance is positioned between clients and a network device requiring ARP resolution, such as a router or default gateway, a high priority QoS filter for ARPs should be defined.

#### Add QoS Filters

The fields on this screen dictate how traffic will be directed to a queue

Figure 4-10 FX Series QoS Filters Configuration Screen

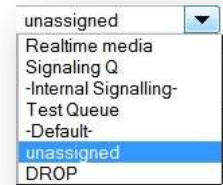
#### QoS Filter Definitions

##### Name:

This summarizes the customer/function of the filter. This field must be entered and must be unique.

**Queue:**

Selects which queue that traffic that matches the criteria specified in this filter definition should be directed. This field may be left blank during definition, but must be eventually be assigned. If the “Drop” option is selected, all traffic selected by this filter will be dropped. The Default filter will target the Default Queue, but can be redefined in this screen.

**Protocol:**

Select between \* / ARP / TCP / FTP / UDP / IP / ICMP / MPLS / SCTP / PTPv1 / PTPv2



**NOTES:** (only one choice may be selected). The default is \* (all protocols)

**FTP:** If FTP is selected, the FX automatically tracks the data ports associated with FTP transfers by monitoring the activity on the FTP control port, which is defaulted to port 21 upon initial selection. To maintain Multicator transmitter functionality when performing QOS on non standard FTP ports, an additional QOS filter must be created for FTP that utilizes port 21. The FTP control port may be changed. “For active FTP”, the source port field should be configured to “20, 21”

**MPLS:** If MPLS is selected, then the “MPLS Label”, and “MPLS experimental bits” fields will be enabled as filter criteria, otherwise these fields are disabled. If MPLS is selected, then additionally the VLAN filter criterion is enabled but all other filter criteria fields are disabled.

If **ARP, PTPv1, PTPv2 or FTP** is selected, then this filter can’t be assigned to a queue for which packet compression is enabled.

**PTPv1 or PTPv2 :** If PTPv1 or PTPv2 is selected, only DSCP, VLAN, VLAN Priority, Destination subnets, and Source subnets may be selected. If PTPv2 is selected, in addition to PTPv2 running over UDP, the filter will also check for packets on ethertype 88f7, in which case IP specific options do not apply.

**SCTP:** If SCTP is selected, only DSCP, VLAN priority, Destination subnets, and Source subnets may be selected.

**DSCP:**

Select one of the choices from the pull-down menu of DCSP choices. Only one choice may be selected). The default is \* (any)

**VLAN:**

Enter either 0 or a VLAN ID between 2 and 4094. Only one may be selected. 0 indicates untagged traffic as the selection criteria. The default is \* (any VLAN)

**VLAN Priority:**

Choose between ‘any’ or a priority value between 0 and 7. Only one choice may be selected. The default is \* (any VLAN priority)

**MPLS Label:**

If MPLS was selected as the protocol then a decimal value between 0 and 1048575 may be entered. If no value is entered then all MPLS labels will match the filter criteria. If there are multiple MPLS labels, the filter will only match the first label encountered in the packet.

**MPLS experimental bits:**

If MPLS was selected as the protocol then you can choose a value between 0 and 7 as match criteria. If ‘\*’ is chosen then the filter does not use the experimental bits in the match criteria, otherwise all bits must match exactly.

**Destination Subnets:**

This is specified in CIDR format. Multiple subnets may be separated by a comma. The default is '\*' (any subnet). Acceleration tunnels utilized by FX WAN Optimization may not maintain the original application destination address, therefore this field should not be used when classifying FX Wanop traffic unless an application policy is defined to prevent tunnel sharing between different destination subnets.

**Destination Ports:**

Port ranges can be specified by either entering the lowest port followed by '-', followed by highest port; or multiple ports may be entered separated by comma. The destination port is relative to the FX.

**Source Subnets:**

This is specified in CIDR format. Multiple subnets may be separated by a comma. The default is '\*' (any subnet)

**Source Ports:**

Port ranges can be specified by either entering the lowest port followed by '-', followed by highest port; or multiple ports may be entered separated by comma. The source port is relative to the FX. Acceleration tunnels utilized by FX WAN Optimization do not maintain the original application source port; therefore this field should not be used when classifying FX Wanop traffic.



When specifying multiple fields as selection criteria the choices are logically "ANDed" when formulating a match. Multiple selections within a field are logically "ORed" when formulating a match.

#### 4.6.4 QOS Queue Definitions

These settings allow you to manage QoS Queue Definitions. A list of previously defined queues will be displayed in order of priority. From this screen the following parameters can be updated: Status, Priority, Compression CIR, and MIR. Using the pull down options or entering new values in the numeric fields and clicking the "update" button will update the definition for that specific queue.

Name	Status	Priority	CIR	MIR	update	delete
Signaling_Q	Enabled	1	0	20	update	delete
Realtime media	Enabled	2	1000	2000	update	delete
Test Queue	Enabled	2	0	20000	update	delete
-Default-	Enabled	8	0	155000	update	delete

**Figure 4-11 FX Series Quality of Service Queues**

An existing entry may be chosen by clicking on the queue name which leads to the Queues Add/Edit Screen. The user adds queues by clicking the "Add Queue" button.



**NOTE:** The Default Queue is always defined. It is initial priority is 8, the lowest priority and is associated with the Default Filter.

## View Statistics by QoS Queue

The QoS Status Monitor provides a real time view of vital QoS statistics, including current, average and elapsed stats. All elapsed and average stats begin with the last Reset of the screen. See Status Monitor in the Status Section 7.2 below.

## Add QoS Queue

FX Series Administration Index Help

Configuration->Quality of Service->Queues->Edit

Name	VIDEO 1
CIR (kbps)	0
MIR (kbps)	255000
Priority	1
Scheduling discipline	Stochastic Fair Weighted
<small>Strictly ordered is recommended for signaling traffic.</small>	
Packet compression	Header
Aggregation interval (msecs)	5
Threshold to trigger payload compression	
Filters assigned to this queue	VIDEO 1

Save

Return to Queues

Figure 4-12 FX Series QoS Queues Configuration Screen

### Name:

This field is a logical name that is used as a reference when Filters are defined. This field must be entered.

### CIR (kbps):

This specifies the “Committed Information Rate” in kbps (1000 bits per second). The range is 0 up to the licensed rate. If the FX WAN optimization feature is not licensed, then up to 700000 kbps can be specified. The default is 0. This field is disabled if “Strict Priority” was configured as the drain algorithm.

### MIR (kbps):

This specifies the “Maximum Information Rate” in kbps (1000 bits per second). The range is 0 up to the licensed rate. If the FX WAN optimization feature is not licensed then up to 500000 can be specified. If 0 is specified, some packets may still be sent at a very low rate, to inhibit all traffic then a “DROP” filter should be defined. The default is the max licensed rate. This field is disabled if “Strict Priority” was configured as the drain algorithm.

### Priority:

This is the drain priority for the queues. Classes of equal priorities will be treated the same, with rates split proportionally between them. The minimum value is 1 the max is 8. 1 is the highest priority. The default value is 8.

### Scheduling Discipline:

This specifies the order in which packets in this queue are scheduled for transmission. The default is Stochastic Fair Weighted.

The choices are:

**Stochastic Fair Weighted**

The scheduler will attempt to evenly distribute outbound traffic based on hashing the source and destination addresses.

This is the default choice and prevents one traffic flow from consuming all bandwidth assigned to this queue at the expense of other flows assigned to this queue. When there is high link congestion this method may introduce miniscule delays.

**Strictly ordered**

Packets are sent in the order that they are received. This may be a good choice for signaling traffic where there can be absolutely no disruption in packet transmission.

**Packet compression:**

Enables/disables packet compression and aggregation for this queue. For packet compression to occur, you must also globally configure packet compression on the 'Configuration->QoS->Dynamic ACM' page. If packet compression is enabled then WAN optimization features such as caching can't be performed on traffic associated with this queue. When configuring packet compression, you can choose to perform header compression or both header and payload compression.

**Aggregation interval (msecs):**

Specifies the packet aggregation flush interval in milliseconds if packet compression is enabled. The minimum and default value is 10 msecs. The maximum is 1000 msecs.

**Threshold to trigger payload compression:**

If 'header and payload' compression is selected, this value specifies the minimum payload size to trigger payload compression. The default is 300 bytes.

**Filters:**

This is a read-only list of filters that are currently assigned to this queue.



## 4.7 FX Series Multicator Overview

The Multicator is a set of three components of the FX Series which allow controlled reliable content distribution via multicast. These components are as follows:

### Multicator Controller (MC)

Within a Multicator deployment, there is one, and only one, FX SERIES ADC appliance which must be designated as an MC.

An MC is the central point where Multicator configuration parameters are stored. The MC ensures that only one multicast transmission is occurring at a time. The MC ensures that if there is a network outage, a multicast which was in progress will resume from the point where the outage occurred. The MC maintains a central log of all Multicator events.

### Multicator Transmitter (MT)

This component actually performs the multicast of the content after checking with the MC. Any FX Series ADC or FX Series Remote can function as a Multicator Transmitter (MT) if the license is enabled. The MT employs world renowned open source technology to reliably deliver content via multicast.



**NOTE:** Any FTP program can be used to upload content to the MT.

### Multicator Receiver (MR)

This component receives the content which is transmitted by the MT. Upon completion of a successful reception of new content, the MR uploads this content to a local FTP server.



**NOTE:** Any combination of MC, MT, and MR may be configured on the same appliance as long as there exists one, and only one MC in the Multicator deployment.

### 4.7.1 Theory of Operation

A powerful new content distribution system can now be set up with the separately licensed “Multicator” feature. This feature allows a user to upload a file to an FX Series device via FTP. The file is then reliably multicast to a group of receivers. The receivers then upload the content to a local FTP server. The Multicator employs the “Content Distribution Control Protocol” (CDCP) to ensure that only one multicast transmission is in progress.

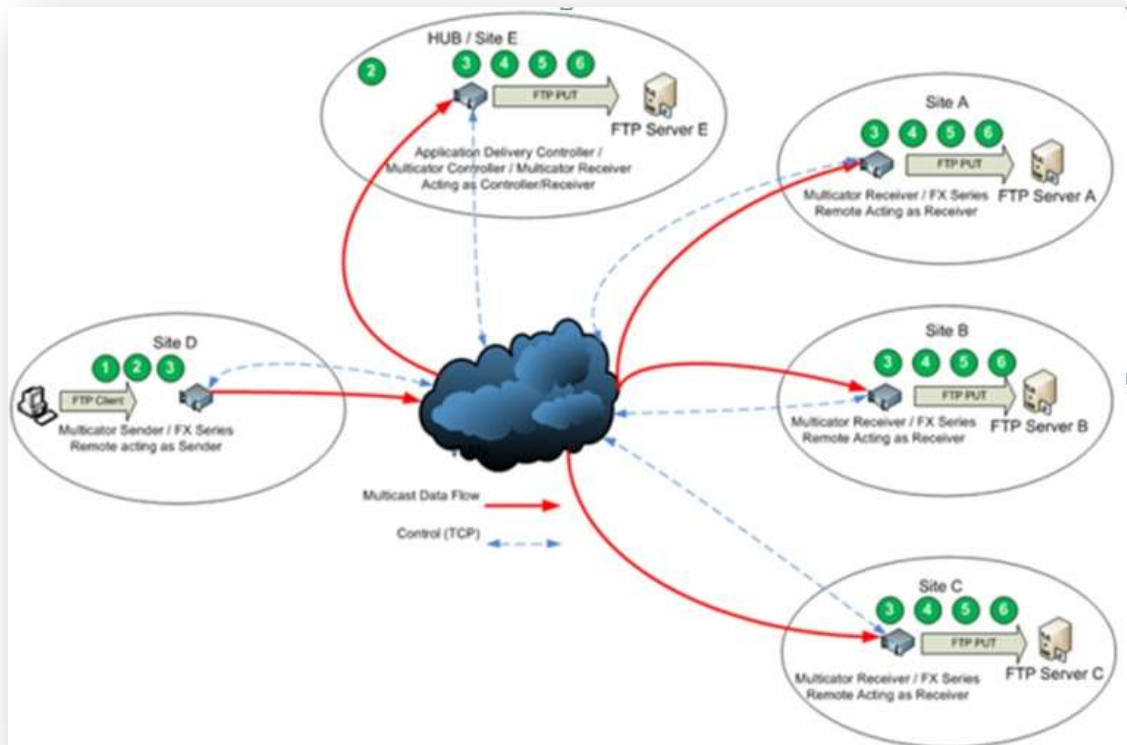


Figure 4-13 FX Series Multicator Theory of Operation

#### Sequence of Events

1. Files are deposited on the Transmitter (Sender) using a standard FTP client (Site D).
2. The Transmitter then notifies the Controller that it has data to send and is granted permission to reliably multicast the data across the WAN.
3. Under the direction of the Controller, the Transmitter establishes a reliable multicast connection to the Receivers.
4. The Transmitter sends the files to each of the Receivers (Sites A, B, C, and E).
5. Each Receiver sends an acknowledgment of receipt to the Controller.
6. Each receiver uses FTP to send the files to the respective server.

## 4.7.2 Multicator Settings



FX Series Administration Index Help

Configuration->Multicator

**General Settings**

Source Interface 172.27.120.66

Controller Address 5.6.7.8

Controller Port 1

**Multicator Controller**

Enable Multicast Controller  Disabled  Enabled

Multicast Address 5.6.7.8

Multicast Port 1

Transaction Rate (Mbps) 2

Figure 4-14 FX Series Multicator Configuration Screen (Controller Settings)

### Source Interface:

For transmitters and receivers, this is the interface used when communicating with the controller. For the controller, this is the interface used when transmitters and receivers communicate



**Note:** In routed mode this should always be the interface designated as the WAN interface

### Controller Address:

This is the address of the controller that the transmitter/receiver will communicate with. If this device is a controller and a transmitter or receiver this address should match the "Source Interface" field.

### Controller Port:

The port that the controller will use to communicate with transmitters and receivers, if this appliance is a transmitter or receiver it is the port used to communicate with the controller

### Multicator Controller Settings

#### Enable Multicast Controller:

This setting enables the multicast controller on this appliance. Only one controller should be enabled on a network. The default is "Disabled".

#### Multicast Address:

This is the multicast IPv4 address that will be used to transfer files via reliable multicast. This address is communicated to the transmitters and receivers. The default value is 224.0.55.55.

#### Multicast Port:

This is the multicast port that will be used to transfer files via reliable multicast. This port is communicated to the transmitters and receivers. The default value is 4929.

**Transaction Rate:**

This is the max speed that a multicast transmitter will transmit a file. The default value is based off the license.

The screenshot shows a configuration page for Multicator Transmitter and Receiver. The 'Multicator Transmitter' section is at the top, with 'Enable Multicast Transmitter' set to 'Enabled'. Below it are fields for 'Incoming FTP User' (iftpu) and 'Incoming FTP password' (masked with dots). The 'Multicator Receiver' section follows, with 'Enable Multicast Receiver' set to 'Enabled'. Below this are fields for 'FTP Server' (10.9.8.7), 'FTP User' (ftpu1), 'FTP Password' (masked with dots), 'FTP Directory' (some directory), 'FTP Retries' (20), 'FTP seconds between retries' (60), and 'Action on FTP failure' (delete). At the bottom are buttons for 'Retry Failed FTP', 'Purge Failed FTP', and 'Save'.

Figure 4-15 FX Series Multicator Transmitter/Receiver Configuration Settings

**Multicator Transmitter Settings****Enable Multicast Transmitter:**

This setting enables the multicast transmitter on this appliance.

**Incoming FTP User:**

This is the user name that must be used when content is uploaded to the FX appliance. The default is "mc".

**Incoming FTP Password:**

This is the password that must be used when content is uploaded to the FX appliance. The default password is "comtech".

**Multicator Receiver Settings****Enable Multicast Receiver:**

This setting enables the multicast receiver on this appliance.

**FTP Server:**

This is the IP address of the FTP server into which newly received content will be fanned-out.

**FTP User:** This is the user name used when transferring new content to the FTP server.

**FTP Password:**

This is the password which will be used when transferring new content to the FTP server.

**FTP Directory:**

This optional parameter is the directory where new content will be transferred. If this directory does not already exist, it will be created before the file is transferred. The default is none.

**FTP Retries:**

This is the number of times to attempt to send the file to the FTP server before both deleting it and moving on to the next or keeping it and moving on to the next. The receiver will attempt to resend all failed files when the acceleration service is restarted or the "Retry Failed FTP" button is pressed.

**FTP seconds between retries:**

This pull-down allows you to select number of seconds which will elapse between each attempt to send the file to the FTP server.

**Action on FTP failure:**

This specifies the action to take if the FTP retry limit is exceeded. If delete is selected the file will be delete, otherwise the file will be stored until the "Retry Failed FTP" button is clicked or the acceleration service is restarted.

**Retry Failed FTP:**

This button will cause any files that failed FTP transfer to be re-sent to the FTP server. This action is only valid if "Action on FTP Failure" is set to "keep"

**Purge Failed FTP:**

This button will delete any files which are pending to be re-sent to the FTP server. This action is only valid if "Action on FTP Failure" is set to "keep".



**Note:** If disk utilization reaches 80%, a purge of all files that failed FTP transfer will automatically occur.

### 4.7.3 Multicator General Setup (required for all roles)

1. Log into the browser interface of the appliance.
2. Click the Configuration link; Click the Multicator link.
3. Select the appropriate interface in the "Source Interface" field in the "General Settings" section. In routed mode this should always be the WAN facing interface.
4. Enter the IP address of the controller for the transmitter and receiver in the "Controller Address" field. If this is the controller enter the IP address in the "Source Interface" field.
5. Enter the port the transmitter/receiver will communicate with the controller on. If this appliance is also a controller, this is the port it will listen on.

#### 4.7.4 Multicator Controller Configuration Setup

1. Log into the browser interface of the appliance.
2. Click the Configuration link; Click the Multicator link.
3. Click the enable radio button in the "Enable Multicast Controller" field in the "Multicator Controller Section"
4. Enter the multicast IP address you wish to use in the "Multicast Address" field. Default: 224.0.55.55
5. Enter the port you wish to use for multicast in the "Multicast Port" field. Default: 4929
6. Enter the rate at which data should be transmitted via multicast in the "Transaction Rate" field. Default: The licensed rate of the appliance.

#### 4.7.5 Multicator Receiver Configuration Setup

1. Log into the browser interface of the appliance.
2. Click the Configuration link; Click the Multicator link.
3. Click the enable radio button in the "Enable Multicast Receiver" field in the "Multicator Receiver" section.
4. Enter the controller port of the Multicator controller. Default: 4929
5. In the "FTP Server" field, enter the IP address of the FTP server that will receive the file delivered to the receiver via multicast.
6. In the "FTP User" field, enter the user name for the FTP server that will receive the file delivered to the receiver via multicast.
7. Default: anonymous
8. In the "FTP Password" field, enter the password for the FTP server where the file received via multicast will be placed.
  9. Default: no directory, file deposited in FTP root
10. In the "FTP Directory" field, enter the directory on the FTP server where the file received via multicast will be placed.
11. In the "FTP Retries" field select the number of times the receiver should attempt to deliver a file to the FTP server before abandoning the file transfer. Default: 5
12. In the "FTP seconds between retries" field select the number of second between FTP retry attempts. Default: 10
13. In the "Action on FTP failure" field select the action to be taken on the file if the FTP transfer fails and all retry attempts have been exhausted. Default: keep

#### 4.7.6 Multicator Transmitter Configuration Setup

1. Log into the browser interface of the appliance.
2. Click the Configuration link; Click the Multicator link.
3. Click the enable radio button in the "Enable Multicast Transmitter" field in the "Multicator Transmitter" section.
4. Enter the username used in FTP file submissions to the transmitter in the "Incoming FTP user" field. Default: mc
5. Enter the password used in FTP file submissions to the transmitter in the "Incoming FTP Password" field. Default: comtech

## 4.8 Redundancy

This section allows you to configure 1:1 redundancy with fail over in which a secondary FX, with the same configuration as the primary FX, polls for the existence of the primary FX, and takes over its non-management IP addresses when the primary does not respond to the poll. When the primary FX comes back up, the secondary FX will relinquish the IP addresses. This section also allows you to configure shared configurations between members of an appliance pool. This is useful to synchronize configurations in a WCCP cluster.

Figure 4-16 FX Series Redundancy Screen

### 4.8.1 Redundancy Configuration Settings

#### Redundancy

This must be enabled if either the 1:1 Redundancy with fail over or “Automatically synchronize configurations” feature is required.

#### Primary Appliance:

This is the host name of the primary (master) FX.

#### Secondary Appliance:

Enter the ‘short’ host name or IP address of the secondary FX that will engage if the primary FX becomes inoperable. The secondary appliance continually polls the primary appliance and if the primary appliance does not respond then the secondary appliance asserts control over the realm of IP addresses that external clients connect to. When the primary appliance becomes operational again, the secondary will relinquish control of these IP addresses. This parameter is not required if only synchronizing configuration changes to member pool appliances is being configured.

#### Authentication Key:

By default, this key is generated automatically. For 1:1 Redundancy with fail over, the secondary appliance's key must match the primary appliance's key. This requires manually copying the primary appliance's key and pasting it into this field on the secondary appliance (after deleting the secondary appliance's generated key).

**Automatically Synchronize Configuration Changes:**

This field must be enabled for configuration synchronization. Any time a configuration change is applied using the browser administration interface; the change is immediately synchronized with the Secondary Appliance and/or members of the "Member Appliance Pool". The 'Configuring Key-Exchange' procedure below must be performed.

**Member Appliance Pool:**

If the "Automatically Synchronize Configuration Changes" is enabled, then this field defines the list of host names or IP addresses, separated by commas, of the appliances that will share the same configuration files as the primary appliance. The devices defined in the "Member Appliance Pool" share their configurations and require a valid SSH key to be exchanged with the "primary" appliance.

(See section titled "Configuring Key-Exchange" below).

**Save Button:**

Clicking on 'Save' will commit the fields on this form to disk. If this is the Initial configuration of high-availability the appliance must be rebooted after the 'Save' completes.

## 4.8.2 Configuring Key-Exchange

In order for the FXs to securely communicate with each other in an automated fashion it is necessary to use the "FX-Series Appliance Manager" via SSH to configure common cluster authentication keys.

To configure the key exchange between the primary and secondary, log into the FX with "ssh" to access the "FX-Series Appliance Manager" and perform the following sequence on the primary FX:

1. Choose "1 Configure Appliance"
2. Then choose "2 Configure Passwords"
3. Then choose "2 Configure Redundancy Cluster Key"
4. Enter the IP Address or host name of the peer appliance
5. On prompt: Are you sure you want to continue connecting (yes/no) enter 'yes'
6. On the password prompt enter "comtech"

Repeat this for the secondary and/or each entry in the Member Appliance Pool.



**NOTE:** For 1:1 Redundancy with failover configurations, the primary appliance and secondary appliance entries must be associated with the auxiliary port. A 'short' host name is required. These may be specified via the DNS server or by configuring the local host table. (See Configuration->Host Settings)

**ARP Considerations:**

When the FX performs the IP take over it will send out a gratuitous ARP so that other routers are notified of the take-over.



### 4.8.3 Example 1:1 redundancy with fail over setup scenario

- Given an FX-4000/FX4010 ADC named '**PrimAdc**' installed and operating in "in-line mode" eth2/eth3) using eth0 as a management port.
  - Add a new FX-4000/FX4010 ADC appliance named '**Adc2nd**' for 1:1 redundancy with fail over.
1. Cable the ADC appliances:
    - a) Connect **PrimAdc/Adc2nd** auxiliary (eth1) ports with cross-over cable
    - b) Remove **PrimAdc** eth3 port connection (Wan) and plug it into **Adc2nd** eth3 (Wan) port
    - c) Use cross-over cable and connect **PrimAdc**'s eth3 to **Adc2nd** eth2 (Lan) port.
  2. Browse to **Adc2nd: Configuration->Host Settings**:
    - a) Set 'Host name' to Adc2nd
    - b) In 'Host File Entries' add the following lines:
 

```
10.1.1.10 PrimAdc.com PrimAdc
10.1.1.11 Adc2nd.com Adc2nd
```

 Click 'Save'
  3. Browse to **Adc2nd: Configuration->Basic Network interfaces**
 Set Auxiliary Interface  
 'Ip v4Address' = 10.1.1.11 'Subnet mask' = 255.255.255.0  
 Click 'Save'
  4. Browse to **PrimAdc: Configuration->Basic Network interfaces**
 Set Auxiliary Interface  
 'Ip v4Address' = 10.1.1.10 'netmask' = 255.255.255.0  
 Click 'Save'
  5. Browse to **PrimAdc: Configuration->Host Settings**
 In 'Host File entries' add the following line
 

```
10.1.1.11 Adc2nd.com Adc2nd
10.1.1.10 PrimAdc.com
```

 Click 'Save'
  6. On **PrimAdc** browse to: **FX Series Application Delivery Controller-> Configuration->Redundancy**
    - a) Enable 'Redundancy'
    - b) Set 'Primary Appliance' to **PrimAdc**
    - c) Set 'Secondary Appliance' to **Adc2nd**
    - d) Set "Automatically Synchronize Configuration Changes" to "Enabled"

Click 'Save' and refresh the browser screen.

Should see "Authentication Key" similar to:

```
auth 1
1 sha1 0509160a630240f400ec5e389c942422
```

The 'Save' action will synchronize **PrimAdc**'s configuration with **Adc2nd**.

7. On **Adc2nd** browse to:
  - a) **FX Series Application Delivery Controller-> Configuration->Redundancy**  
Verify that 'Authentication Key' matches that shown on the **PrimAdc**.

**Note:** If the Keys do not match, copy and paste the Authentication Key from **PrimAdc** to **Adc2nd** then click 'Save' on **Adc2nd**.

It is necessary to reboot both appliances for Redundancy service to run

#### 4.8.4 Synchronizing Configurations in a WCCP Cluster

When multiple FX devices are functioning in a WCCP cluster, each device has unique network settings, therefore only selected configuration settings are synchronized between the members of the cluster. The settings which are synchronized include only the following:

- HTTP Application Policies
- L5 Application Policies
- Authorization Realms
- QoS Queue Definitions
- QoS Filters

Of the above, HTTP application policy synchronizations take effect immediately, throughout the cluster, unless the HTTP policy references a newly defined authorization realm. If an HTTP application policy references a modified realm then a restart of the acceleration service may be required for the intended change to take effect. The other settings require a restart of the acceleration service to take effect.

## 4.9 WCCP

The Web Cache Communication Protocol (WCCP) is a Cisco-developed content-routing technology which allows you to integrate cache engines into your network infrastructure.

This screen allows you to maintain WCCP definitions. A list of previously defined WCCP definitions is displayed in the order in which they were defined. An existing entry may be chosen by clicking on the router address. Other buttons at the bottom of the screen are as follows:

**Add** – Create a new WCCP definition:

Clicking on this button will bring up the following screen.

FX Series Administration Index [Help..](#)

**Configuration->WCCP Definitions->Edit**

<b>Source IP address</b>	192.168.4.40 VLAN 400	
<b>Router address</b>		
<b>Local GRE tunnel address</b>		
<b>Remote GRE tunnel address</b>		
<b>Enablement</b>	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	Enabled
<b>Critical</b>	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	Disabled
<b>Redirect method</b>	<input type="radio"/> L2 <input checked="" type="radio"/> GRE	GRE
<b>Return method</b>	<input type="radio"/> L2 <input checked="" type="radio"/> GRE	GRE
<b>Assignment scheme</b>	<input type="radio"/> Mask <input checked="" type="radio"/> Hash	Hash
<b>Password</b>		
<b>Service group number</b>		96
<b>Redirect based on</b>	<input type="radio"/> Source IP <input checked="" type="radio"/> Dest IP	Dest IP
<b>Accept traffic for:</b>	<input type="radio"/> Specific ports <input checked="" type="radio"/> All ports	Specific ports
<b>Ports</b>		80
<b>Ports refer to</b>	<input type="radio"/> Dest <input checked="" type="radio"/> Source	Source
<b>Use additional service group</b>	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	Disabled
<b>User-facing service group number</b>		99
<b>Redirect based on</b>	<input type="radio"/> Source IP <input checked="" type="radio"/> Dest IP	Source IP
<b>Comment</b>		

[Return to Configuration](#)

Figure 4-17 FX Series ADC WCCP Definitions Screen

### 4.9.1 WCCP Configuration Considerations

There are two basic configurations that will be used when installing an appliance.

#### 1) Web-cache or transparent proxy interception.

In this mode of interception the FX will have the same characteristics as a standard proxy. The Cisco device will redirect traffic to the appliance, which will then make request on behalf of the user using the appliance's IP address as the source.



**NOTE:** Only one service group is required, service group zero. On the Cisco device this will be configured as "web-cache".

#### 2) Dynamic service groups or source IP address preservation

In this mode of interception the FX will have the same characteristics as an in-line device. The Cisco device will redirect traffic to the appliance, which will then make request on behalf of the user using the user's address as the source (spoofing).



**NOTE:** This configuration requires two service groups, inbound and outbound.

### 4.9.2 WCCP Cisco Device configuration

We will use either eth0 or eth1 when installing in a WCCP pattern. Log into the Cisco device and identify the inbound and outbound interfaces. These must correspond to in-path interfaces.

In the global configuration enable WCCP with the appropriate commands.

If configuring as a web-cache we will enter the following:

```
"ip wccp web-cache"
```

For a WCCP with source IP address preservation setup. We will enter the following commands:

```
"ip wccp 99", "ip wccp 96"
```

By default our appliances use service groups 99 for outbound traffic and 96 for inbound traffic.

At the interface level if we are configuring a web-cache setup. We will enter the following command:

```
For all inbound interfaces: "ip wccp web-cache redirect in"
```

At the interface level if we are configuring a source IP address preservation setup. We will enter the following commands:

```
For all inbound interfaces: "ip wccp 99 redirect in"
```

```
For all outbound interfaces: "ip wccp 96 redirect in"
```

It is possible to control which traffic is redirected by subnet using the redirect-list option

### 4.9.3 Web Cache Communication Protocol Parameters

#### Configuration->WCCP Definitions:

This page allows you to configure the settings for support of the Cisco "Web Cache Communication Protocol" (WCCP).

#### Source IP address:

This is the IP address, which has already been defined on the FX Series ADC that will be used when sending WCCP, messages to the router. The IP address must be selected from the list of in-path interfaces.

**Router address:**

This is the address of the router to which WCCP packets will be directed.

**Local GRE tunnel address:**

This is the IP address of the local end of the GRE tunnel. If this field is not specified then the “Source IP address” will be used for the local endpoint. This field is not needed if L2 redirection is specified.

**Remote GRE tunnel address:**

This is the address of the router which will send the redirected traffic to the FX Series ADC in a GRE tunnel. If this field is not set then the FX will attempt to dynamically learn the address by examining the WCCP packets from the router. This field is not needed if L2 redirection is specified.

**Enablement:**

This specifies if this WCCP definition should be processed. The default value is enabled

**Critical:**

If set, and “Use additional service group” is disabled, then this service group is considered critical. Non-critical service groups will not attempt to negotiate WCCP with the router unless all critical members have seen their IP address in the assignment map or hash allotment and are in a usable state.

**Redirect method:**

This specifies the method in which the router or switch will direct packets to the FX. The choices are “GRE” (Generic Routing Encapsulation) or “L2” which means that the router will simply modify the MAC destination address to point to the FX. The default is “GRE”.

**Return method:**

Although the FX never returns redirected packets to the router, it may be necessary to set this to “GRE” even though “L2” was specified as the redirect method in order to successfully negotiate WCCP.

**Assignment scheme:**

This specifies how the router or switch will decide which FX to direct the packets. In general, this should be set to “Mask” for switches and “Hash” for router. The default setting is “Hash”

**Password:**

If WCCP packet signing is required then this password must match the setting of the WCCP router. The default is no password.

**Service group number:**

This is the WCCP service group that the FX should join. The default value is 96.

**Redirect based on:**

If “source” then the router will redirect responses from the content server to this member, otherwise the router will redirect client requests that otherwise would have been directed to the content server. Service groups are defined at the router. The default is the “Destination”.

**Accept traffic for:**

This radio button allows you to control if only specific ports or all ports should be redirected to the FX Series FX. If “Specific Ports” selected then these are specified in the “Ports” field. If “All ports” is selected then the WCCP router will direct all TCP and UDP traffic to the FX. The default value is “Specific Ports”.

**Ports:**

This defines the TCP and UDP ports that the router should transparently redirect to the FX. Up to 8 ports may be specified separated by a comma. The default value is 80.

**Ports refer to:**

This indicates if the ports field pertains to the source port (for responses from content server) or destination port (for requests from clients). The default value is "Source".

**Use additional service group:**

You can define two service groups within the same WCCP definition. This is normally used if you want the FX to preserve the source IP address of the remote clients when making requests to content servers on behalf of those clients. However, if using the "extra" group then the definition is not deemed as non-critical and will not verify that "critical" service groups are in a usable state. If this is set you must also enable "Preserve client IP addresses" in the "Other" section on the "Configure->General" page. See more detailed description titled "WCCP IP Spoofing Configuration" below. The default value is "Disabled".

**User-facing service group:**

This is the WCCP service group that the FX should join to receive redirected client. The FX will not attempt to join this group unless it successfully enrolls in the main service group. This prevents the situation where client requests are redirected to the FX when it is not able to receive server responses. The default value is 99.

**Comment:**

A comment of up 80 characters can be entered into this field.

#### 4.9.4 WCCP Router Configuration and Status Monitoring

**Configuration:**

The following is an example of some common WCCP Router "cli" commands.

```
conf t
ip wccp enable
ip wccp version 2
interface (specify interface carrying traffic)
ip web-cache redirect
CTRL-Z
```

**Status Monitoring:**

The following WCCP Router "cli" commands can show status:

```
show ip wccp
show ip wccp 99 view
show ip wccp 96 detail
term mon
debug ip wccp packets
debug ip wccp events
clear ip wccp
```

#### 4.9.5 WCCP IP Spoofing Configuration for Routers

The FX can preserve the source IP address of the remote client when making requests on their behalf by joining two service groups. The first service group receives the redirected client requests and is also known as the “User-facing” service group. The second is referred to as the “Server-facing” service group and it receives the redirected server responses. If two or more FXs have joined these service groups, then the router will be instructed to split the load of the user-facing service group based on source IP address, and the responses of the server-facing service group will be split based on destination IP address. This technique ensures that the response will be directed to the same FX that originated the request on behalf of the remote user.

The recommended router configuration is to use three interfaces, each corresponding to a different subnet. To illustrate the setup, we provide an example configuration along with a “show running-config” that is compatible with the default WCCP settings of the FX.

##### Example:

###### Interface A: (Ethernet0/0)

This is the user-facing subnet that receives redirected requests from clients.

###### Interface B: (Ethernet0/1)

This is the server-facing subnet that receives redirected responses from the content server.

###### Interface C: (Ethernet1/0)

FX subnet

###### Service group 99

This should be defined to handle redirected outbound requests from the users destined for the subnets on Interface B. “Interface C” must be excluded from this to avoid loop-backs that would otherwise occur when FXs spoof the user IP addresses.

###### Service group 96

Should be defined to handle redirected responses from content servers that would have otherwise been sent out on “Interface-A”.

###### The subnets:

A: User (192.168.103.xxx subnet)

B: Content servers - all other subnets via gateway at 192.168.101.158

C: FXs (192.168.106.xxx)

##### #show running-config

Building configuration...

```
Current configuration: 948 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2600-lab
```

```
!  
enable password xxxx  
!  
memory-size iomem 10  
ip subnet-zero  
ip wccp 96  
ip wccp 99  
!  
!  
no ip domain-lookup  
ip domain-name example.enterprise.com  
ip name-server 192.168.101.202  
!  
!  
interface Ethernet0/0  
ip address 192.168.103.224 255.255.255.0  
ip wccp 96 redirect out  
half-duplex  
!  
interface Ethernet0/1  
ip address 192.168.101.224 255.255.255.0  
ip wccp 99 redirect out  
half-duplex  
!  
interface Ethernet1/0  
ip address 192.168.106.224 255.255.255.0  
ip wccp redirect exclude in  
half-duplex  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 192.168.101.158  
ip http server  
ip pim bidir-enable
```



#### 4.9.6 WCCP IP Spoofing Configuration for Switches

Switches tend to have less CPU power than a router but on the other hand they have the ability to handle traffic flow decisions in hardware. In order to leverage the hardware switching capabilities the following configuration settings are recommended:

- On the FX, use “L2” Redirection method
- On the FX, use “Mask” assignment scheme
- On the FX, do not define separate service group definition records, instead set the “Use additional service group field”, this is because the Cisco L2 expects the same WCCP source port to be used to conduct WCCP negotiations.
- On the switch, use “redirect in” to direct packet flow to the appliance.



- On the switch, never use “redirect-out”
- On the switch, do not use “redirect exclude in”

In the same subnet scenario described above, the following is an example of a configuration for an intelligent switch:

##### #show running-config

```
.
.
.
!
ip routing
ip wccp 96
ip wccp 99
!
interface Vlan1
ip address 192.168.101.225 255.255.255.0
ip wccp 96 redirect in
!
interface Vlan3
ip address 192.168.103.225 255.255.255.0
ip wccp 99 redirect in
!
interface Vlan5
ip address 192.168.105.225 255.255.255.0
!
interface Vlan6
description for 106 subnet
ip address 192.168.106.225 255.255.255.0
!
```

##### Using “redirect-list” to select specific redirection

For testing purposes, or to gradually stage traffic redirection to the FX Series ADC, a Cisco router will support redirection by either access control lists or group lists. For example:

```
ip wccp 99 redirect-list access-list
```

#### 4.9.7 LAN and In-Path Interface Requirements for WCCP

The FX Series uses the eth2 physical interface to conduct the WCCP protocol with the router or switch and also to receive redirected requests and responses. Therefore in order to configure WCCP, you must define an in-path interface with an IP address that is on the same subnet as the Cisco router or switch. The gateway for this in-path interface must be that of the Cisco router or switch interface the appliance is connected to. The VLAN ID must be 0. Following this, a LAN interface must be defined for eth3 and assigned to the aforementioned In-Path interface.

#### 4.9.8 Configuring WCCP on earlier models

On FX-1000 and some earlier models of FX-4000, the specialized fail-to-wire network interface card requires that an eth3 LAN interface be defined in order to run WCCP over eth2, even though it's not actually used. Therefore, on an FX-1000, an in-path interface with a non-existent VLAN must be defined. This in-path interface must subsequently be assigned to a LAN interface for eth3. It is not required that the eth3 physical interface be cabled to anything.

## 5 FX Series ADC Specific Settings

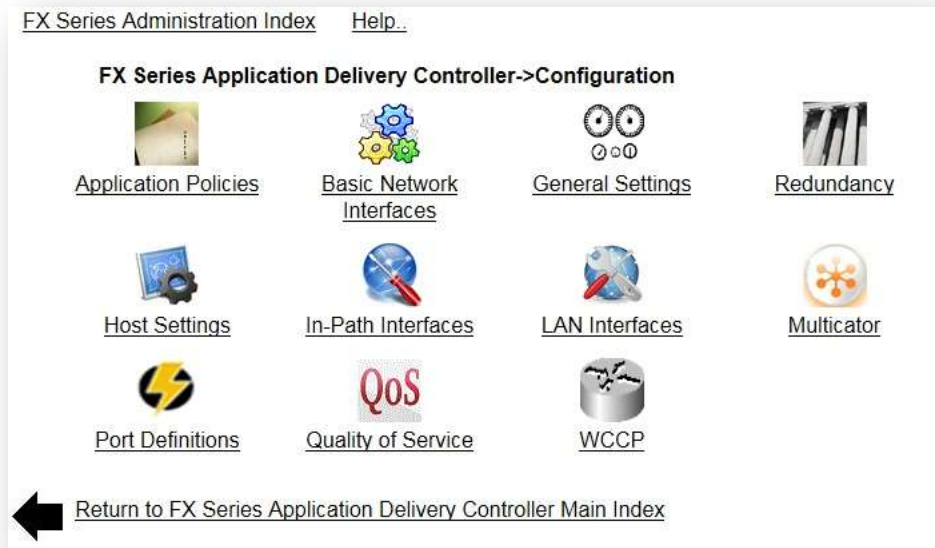


Figure 5-1 FX Series ADC Configuration Menu

### 5.1 Overview

This chapter discusses in much greater detail, General Settings and Port Definitions of the FX Series ADC appliances. The key elements are listed below.

The following items are listed in [Section 4 FX Series Basic Network Settings](#).

- Basic Network Interfaces
- Redundancy
- Host Settings
- LAN Interfaces
- Multicator
- In-Path Interfaces
- Quality of Service
- WCCP

#### FX Series ADC General

Control enablement of DDS, and the traffic interception method. Configure basic HTTP settings and system time.

#### FX Series ADC Port Definitions

Define the IP addresses and ports that the FX will listen on for the purpose of optimizing data flow to a web or application server. FX Series ADC General Configuration Settings

These settings allow you to configure advanced parameters that apply to many aspects of the FX Series application delivery controller (FX Series ADC).

### 5.1.1 General Settings

**Configuration->General**

---

**General Settings**

ADC is in 'Configuration-Only' mode     Disabled     Enabled    Disabled

Enable dynamic data suppression     Disabled     Enabled

HTTP session inactive timeout (seconds)

HTTP server connect timeout (seconds)

Generate HTML error pages     Disabled     Enabled

Preserve client IP addresses     Disabled     Enabled

---

**Object Retrieval Logging**

Log HTTP requests     Off     On

    Maximum size in KB   

---

**Traffic Interception**

Traffic interception mode    In-Line

VLAN mode     Trunk     Access    Trunk

Fail-to-wire mode     Disabled     Enabled    Enabled

---

**System Time**

Network time server   

Time zone    (UTC-00) Greenwich Mean Time (GMT)

---

**Software Updates**

Automatically distribute remote updates     Disabled     Enabled

---

**Administration**

Use SSL for the administrative Web GUI     Disabled     Enabled

---

**Other**

Use spanning tree protocol     Disabled     Enabled

**Figure 5-2 FX Series ADC General Settings Screen**

#### **FX Series ADC in “config-only” Mode:**

This setting is useful if you are in the process of configuring your FX Series ADC while the unit is networked in-line. In “Configuration-Only” mode the in-line networking card is put into “bypass” mode so that traffic is simply passed through. When you are satisfied that the FX Series ADC is properly configured you can disable this setting. The default setting is “Disabled”.

#### **Enable Dynamic Data Suppression:**

This is a global switch that applies to all traffic processed by this FX Series ADC. If “Enabled” then a cache of data and signatures and byte patterns will be maintained and when possible a signature will be sent instead of a redundant byte pattern. The default value is “Enabled”.

**HTTP Session Inactive Timeout (seconds):**

This setting controls the maximum time that inactive browser sessions are kept open before closing them in order to minimize thread and TCP session resources. The default interval value is 60 seconds.

**HTTP Server Connect Timeout (seconds):**

This controls the maximum number of seconds that the FX Series ADC will wait for a TCP connection to complete to an HTTP content server before timing-out. After the timeout, a 503 HTTP error code will be returned to the browser that initiated the request. The default value is 20 seconds.

**Generate HTML error pages:**

This controls whether the FX Series ADC should generate an HTML page describing the problem and identifying the FX Series ADC when it encounters a problem connecting and/or receiving content from a back-end server. The default value is "Enabled".

**Preserve Client IP Addresses:**

If enabled, then the FX Series ADC will send the requests to the back-end servers with a source IP address that is the same as the client that the request is on behalf of. Enabling this setting may require a Transparent Bridging configuration. This setting only applies to single-sided optimization. IP source preservation with FX Remotes is specified in the L5 application policies. The default value is "Enabled".

**5.1.2 Object Retrieval Logging****Log HTTP Requests:**

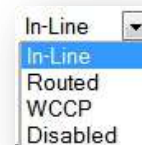
Enables logging of URLs for all HTTP web object retrievals in "common log format". The default setting is "On".

**Maximum Size in KB**

This sets the maximum size of the object retrieval log file in kilobytes. When this size is reached a backup is made and the file is reset. The default setting is 1000000 (1 GB).

**5.1.3 Traffic Interception****Traffic interception mode:**

This is the means by which the FX-ADC will transparently intercept packets. Choose either "In-Line", "Routed", "WCCP" or "Disabled". The default is "In-Line".



- In-Line mode, the LAN port is eth2 and the WAN port is eth3. Traffic is intercepted as a transparent bridge. If there is a service disruption then the units will "fail-to-wire". In bridged mode, you must assign an IP address to the in-path interface which bridges the LAN and WAN interfaces. In FX nomenclature, the "WAN" interface is considered to be the interface which is connected to the satellite modems and the LAN interface is connected to the internet or to enterprise servers.
- In routed mode, traffic must be directed to these interfaces by a router. You must assign an IP address to the in-path interface which will receive traffic from the router. There is no "fail-to-wire" capability if there is a service disruption.
- In WCCP mode, traffic is redirected to the FX by a Cisco router via WCCP.
- If "Disabled" then traffic redirection is effectively shut off.

**VLAN mode:**

This controls how the FX will process VLAN tags. In 'Trunk' mode, the VLAN tags are already embedded in the packets when they are intercepted by the FX. In 'Access' mode, the FX will add tags to untagged traffic. The default setting is 'Trunk'.



**Note:** Changing either the 'Traffic interception mode' or 'VLAN mode' settings will automatically trigger a restart of the acceleration service.

**Fail-to-wire mode:**

If enabled, the FX will go into bypass mode it is not accelerating traffic or if it is powered off. If disabled, it will not go into bypass mode which will prevent packets from being forwarded through the FX. If the FX is adding the VLAN tags to the traffic, it may be desirable to disable 'Fail-to-wire' mode to prevent untagged traffic from entering a network. The default setting is "Enabled".



**Note:** The FX-1010 does not support fail-to-wire mode

#### 5.1.4 System Time

**Network Time Server**

This setting will specify the host address for which the FX Series ADC will attempt to synchronize its time via the "Network Time Protocol". The FX Series ADC performs this synchronization one minute following a restart and once per week thereafter.

**Time Zone**

This selector allows you to specify a time zone in which the FX Series ADC resides. In most cases, the default value of UTC-0 (GMT) is desirable because this will facilitate correlating system events with troubleshooting and other logs.

#### 5.1.5 Software Updates

**Automatically Distribute FX Series Remote Updates:**

If "enabled", then the FX-Remote devices will periodically check to see if a newer version of firmware is available. If so, the FX-Remote devices will automatically download and apply the firmware update. The default value is "Disabled". It is a recommended practice that this setting be enabled only when you wish to deploy updated FX firmware during off-peak hours.

#### 5.1.6 Administration

**Use SSL for the administrative Web GUI:**

If "enabled" then HTTP/S must be used when managing the FX from the Web graphical user interface. This is a recommended practice to prevent passwords from being transmitted unencrypted. The default value is "Enabled".

#### 5.1.7 Other

**Use Spanning-Tree Protocol:**

If enabled, then spanning-tree protocol (STP) will be used when operating in "in-line" mode. Otherwise STP packets will be discarded. The default value is "Enabled".



**NOTE:** If this setting is changed, then it is necessary to restart the acceleration software on the "Status->Real-time Monitor" screen.

## 5.2 Port Definitions

Port definitions allow you to define which IP address and port combinations that the FX Series ADC will listen on and what protocols should be accepted over these combinations. A port definition is required for every IP address and port combination on which the FX Series ADC will accept connections in a proxy mode. For each port definition you must specify the protocol that will be used. Port definitions are only needed if you will be directing traffic to the FX Series ADC as a proxy, or from a remote software client that is running acceleration plug-in.

This screen allows you to maintain Port definitions. A list of previously defined Port definitions is displayed in the order in which they were defined. An existing entry may be chosen by clicking on the port. You can “Enable”, “Disable”, or “Delete” one or more Port definitions by selecting the checkbox to the left of the port column and clicking on the desired button. By clicking on “Add” you can add a new port definition which will bring up the port definition screen.

Figure 5-3 FX Series ADC Port Definitions Screen

### 5.2.1 In-Path Interface:

Specify the IP address that is associated with this port definition.

#### Port:

This field will be filled in automatically as you set the “Protocol” field. After setting these fields, you can then override the port field to create a unique IP Address / Port combination.

#### Protocol:

This specifies the protocol that will run over this port. There are the following choices:

##### HTTP:

This choice specifies that you want the ADC to function as either a forward or reverse proxy on this port.

**Accelerated HTTP/L5:**

This choice specifies that you want the ADC to use this port to service the HTTP Acceleration Protocol (HAP) that has been extended to also accelerate non-HTTP TCP/IP based protocols at layer 5. Accelerated HTTP/L5 is only available if you have deployed the acceleration plug-in to your remote users.

**Autosense:**

This setting supports the AOD injection where both HTTP traffic and accelerated HTTP can flow over the same port.

**Comment:**

This provides a place to store any user defined comment to describe the rationale for this port definition.

**Status:**

This allows you to control whether this port definition is enabled or disabled.

## 5.2.2 Example Port Definitions

By default, port definitions are not required to function as a one-sided FX Series ADC or as a head-end serving FX Series Remote appliances.

The table below shows port definition setting examples:

IP	Port	Protocol - SLL	Typical Use
any	80	HTTP / Acc. HTTP - Autosense	Transparent redirection with capability to inject AOD.
any	8080	HTTP	Forward proxy of HTTP traffic from standard browsers
any	4917	Acc. HTTP/L5	Accelerated traffic between standard and advanced clients and FX Series ADC

## 5.2.3 Setting up an HTTP Forward Proxy

A forward proxy requires that an end user specifically set their browser proxy settings such that port 80 traffic is specifically directed to the IP address of an in-path interface of the ADC on a specific port (usually 8080). In order to get this to work some additional steps are required:

1. An L5 Policy must be defined for port 8080 traffic.
2. This L5 policy must have the "certified application" set as "HTTP Traffic".
3. This L5 policy must have "Protocol" defined as "Generic TCP".

The "Protocol" on the "Port Definition" must be defined as "HTTP".



## 6 FX Series Remote Specific Settings

### 6.1 FX Remote Settings Overview

The FX Series Remote appliance works in conjunction with a head-end FX Series ADC appliance. The FX Series (ADC) appliance resides at the data center and supports connections with multiple remote sites where FX Series Remote appliances are installed. Most FX Series Remote configurations are accomplished with an easy-to-use browser-based tool to set policies on the appliance. The configuration policies are designed to provide full inheritance properties, meaning that most configuration settings are shared between all FX Series Remote appliances, but individual over-rides can be set for specific FX Series Remote appliances.



Figure 6-1 FX Series Remote Main Index Screen

This is the main menu for performing administration on the FX Series Remote (REM) that features the best enterprise application data communication optimization technology in the industry.

#### **Configuration:**

Customize the configuration for your environment by editing networking settings, and Traffic Classes.

#### **Status:**

This provides a real-time status monitor and allows you to easily restart the acceleration service. View activity logs. (See [FX Series Status](#))

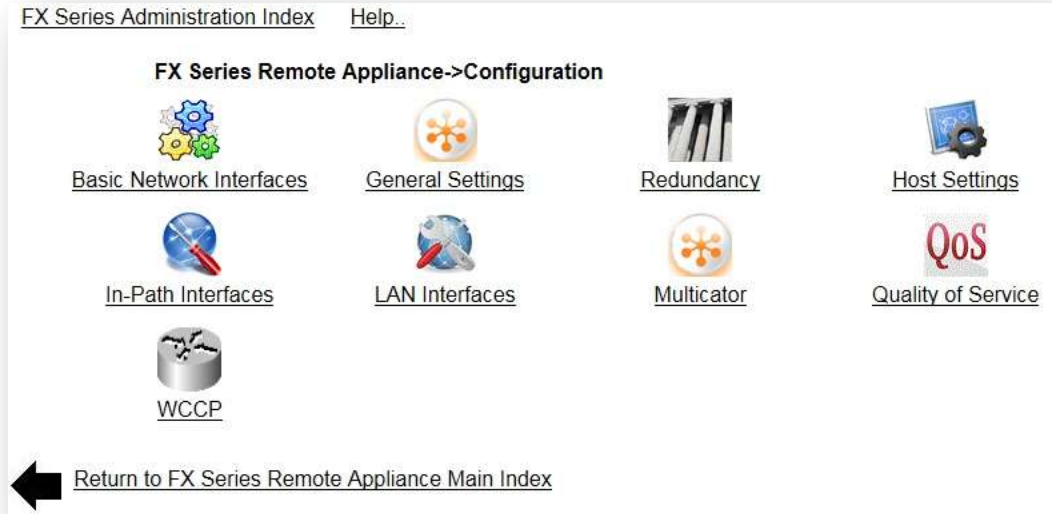
#### **Operations:**

The following actions are included: Shutdown/Restart the appliance. Backup/Restore configuration files. Obtain packet capture. Manage license files. (See [FX Series Operations Functions](#))

#### **Documentation:**

Access the documentation in PDF format. (See [FX Series Documentation](#))

## 6.2 FX Series Remote Configuration Settings



**Figure 6-2 FX Series Remote Configuration Screen**

These settings allow you to customize the configuration for your environment.

Note the following are common for both the FX Series ADC and the FX Series Remote. The details can be reviewed in [FX Series Basic Networking Settings Section](#).

- Basic Network Interfaces
- Redundancy
- Host Settings
- LAN Interfaces
- Multicator
- Quality of Service
- WCCP

The following configuration settings are included in this section

### General Settings

Control method of traffic interception. Configure basic HTTP settings, system time and other options.

### In-Path Interfaces

Configure network settings for the interfaces which will carry accelerated traffic.

## 6.2.1 FX Series Remote General Settings

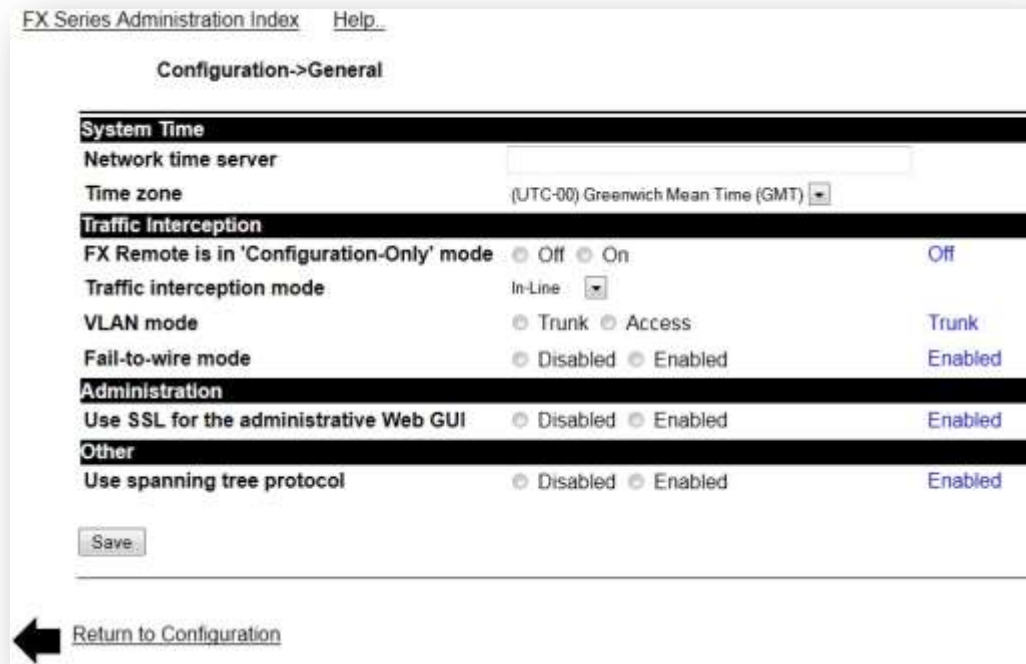


Figure 6-3 FX Series Remote General Settings Screen

### 6.2.2 System Time

#### Network Time Server:

Specify the host address for which the FX Series Remote will attempt to synchronize its time via the “Network Time Protocol”. The FX Series Remote performs this synchronization one minute following a restart and once per week thereafter.

#### Time Zone:

This selector allows you to specify a time zone in which the FX Series Remote resides. In most cases, the default value of UTC-0 (GMT) is desirable because this will facilitate correlating system events with troubleshooting and other logs.

### 6.2.3 Traffic Interception

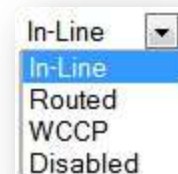
#### FX Remote is in “Configuration-Only” mode:

This setting is useful if you are in the process of configuring your FX Remote while the unit is networked as a bridge. In “Configuration-Only” mode the bridge networking card is put into “bypass” mode so that traffic is simply passed through. When you are satisfied that the FX Remote is properly configured you can disable this setting. The default setting is “Off”.

#### Traffic Interception Mode:

This is the means by which the FX Series Remote will transparently intercept packets.

Choose either “In-Line”, “Routed”, WCCP” or “Disabled”. The default is “In-Line”.



**In-Line Mode:**

In In-lined mode, the LAN port is eth2 and the WAN port is eth3. Traffic is intercepted as a transparently. If there is a service disruption then the units will “fail-to-wire”. For in-line mode, you must assign an IP address to the in-path interface which bridges the LAN and WAN interfaces. In FX nomenclature, the “WAN” interface is considered to be the interface which is connected to the satellite modems and the LAN interface is connected to the internet or to enterprise servers or clients.

**Routed Mode:**

In routed mode, traffic must be directed to these interfaces by a router. You must assign an IP address to the in-path interface which will receive traffic from the router. There is no “fail-to-wire” capability if there is a service disruption.

**WCCP Mode:**

In WCCP mode, traffic is redirected to the FX by a Cisco router via WCCP.

**Disabled Mode:**

If “Disabled” then traffic redirection is effectively shut off.

**VLAN mode:**

Controls how the FX will process VLAN tags. In 'Trunk' mode, the VLAN tags are already embedded in the packets when they are intercepted by the FX. In 'Access' mode, the FX will add tags to untagged traffic. The default setting is 'Trunk'.



**Note:** Changing either the 'Traffic interception mode' or 'VLAN mode' settings will automatically trigger a restart of the acceleration service.

**Fail-to-wire mode:**

If enabled, the FX will go into bypass mode it is not accelerating traffic or if it is powered off. If disabled, it will not go into bypass mode which will prevent packets from being forwarded through the FX. If the FX is adding the VLAN tags to the traffic, it may be desirable to disable 'Fail-to-wire' mode to prevent untagged traffic from entering a network. The default setting is “Enabled”.



**NOTE:** The FX-1010 does not support fail-to-wire mode.

## 6.2.4 Administration

**Use SSL for the administrative Web GUI:**

If “enabled” then HTTP/S must be used when managing the FX from the Web graphical user interface. This is a recommended practice to prevent passwords from being transmitted unencrypted. The default value is “Enabled”.

## 6.2.5 Other

**Use Spanning-Tree Protocol:**

If enabled, then spanning-tree protocol (STP) will be used when operating in “bridged” mode. Otherwise STP packets will be discarded. The default value is “Enabled”.



**NOTE:** If this setting is changed, it is necessary to restart the acceleration software on the “Status->Real-time Monitor” screen or disable and then re-enable each in-path interface.

## 6.2.6 Configuration Notes

### Configuring Routed Mode for Two Interfaces

In routed mode, an IP address must be assigned to all in-path interfaces.

This is a two-step process.

- 1.) You must define two in-path interfaces each with a different IP address and gateway. Normally both of these interfaces will use VLAN 0. It is a recommended practice to define a comment for the in-path interfaces that describes both physical and routing aspects of the interface.
- 2.) You must define two LAN interfaces and then assign them to the in-path interfaces. On the "LAN Interface Definition" screen you would normally leave the "Untagged in-path interface" field at the default setting of "None".

## 6.3 FX Series Remote In-Path Interfaces

This screen allows you to maintain In-Path interface definitions.

A list of previously defined in-path interfaces are displayed in the order in which they were defined. An existing entry may be chosen by clicking on the IP Address. You can “Enable”, “Disable”, or “Delete” one or more In-Path interfaces by selecting the checkbox to the left of the port column and clicking on the desired button. By clicking on “Add” you can add a new In-Path interface which will bring up the In-Path interface definition screen.

The screenshot shows the 'Configuration->In-Path Interface->Edit' screen. It features several sections:
 

- In-Path Interface**: A header bar.
- VLAN ID**: A text input field containing '0'.
- Comment**: A text input field.
- Status**: Radio buttons for 'Disabled' and 'Enabled', with 'Enabled' selected. A 'Enabled' label is on the right.
- Address**: A text input field.
- Netmask**: A text input field.
- Gateway**: A text input field.
- Routes**: A large text area for entering routes.
- Router polling**: Radio buttons for 'Disabled' and 'Enabled', with 'Disabled' selected. A 'Disabled' label is on the right.
- Poll address**: A text input field.
- SNMP version**: Radio buttons for '2c' and '3', with '2c' selected. A '2c' label is on the right.
- Poll community**: A text input field containing 'public'.
- Poll interval (seconds)**: A text input field containing '300'.
- ADC auto-discover**: Radio buttons for 'Disabled' and 'Enabled', with 'Enabled' selected. An 'Enabled' label is on the right.
- ADC list**: A text input field.
- Inbound bandwidth (Kbps)**: A text input field containing '15000'.
- Outbound bandwidth (Kbps)**: A text input field containing '15000'.
- In-band management**: Radio buttons for 'Disabled' and 'Enabled', with 'Disabled' selected. A 'Disabled' label is on the right. Below it is the text 'Change requires restart'.
- Buttons**: An 'Add In-Path Interface' button at the bottom left and a 'Return to In-Path Interface' button with a left-pointing arrow at the bottom left.

Figure 6-4 FX Series Remote In-Path Interfaces Screen

### 6.3.1 Best Practices for Routed Mode Configurations

If using two in-path interfaces in routed mode and both interfaces are on the same VLAN, which is normally the case, then only one in-path interface can have a default gateway. The in-path interface with no default gateway defined must have a routing configuration that is comprised entirely of static routes.

### 6.3.2 Add In-Path Interfaces

#### VLAN ID:

If this interface carries tagged VLAN traffic, then enter the VLAN ID number which is a value between 2 and 4094. Untagged traffic should have a value of 0.

The default is 0.

#### Comment:

Provides a place to store any user defined comment to describe the rationale for this In-Path interface definition.

**Address:**

This is the IPv4 address of this interface.

**Netmask:**

This defines the subnet boundaries of this interface.

**Gateway:**

This is the default gateway for this interface.

**Routes:**

Enter into the text area static routes which are used by the management and auxiliary interfaces. Each static route must be entered on a separate line and must have exactly the following format:

Subnet "SubnetMask" "Gateway"

For example, to define a static route such that subnet 172.88.0.0/16 should be routed by gateway 172.27.101.99 you would enter one of the following:

NOTE: both are supported.

172.88.0.0 255.255.0.0 172.27.101.99

Or

172.88.0.0/16 172.27.101.99

**Router polling:**

If enabled, then SNMP router polling will be used (over this in-path interface) to ascertain the routes that should be added to the route table that is associated with this interface. The default value is disabled.

**Poll address:**

This is the IPv4 address of the router which will respond to the SNMP router poll requests.

**SNMP Version:**

This is the version of SNMP that will be employed when making the router poll requests. The default value is 2c.

**Poll Community:**

This is the SNMP community that is associated with the router poll request. The default value is "public".

**Poll Interval:**

This is the frequency in seconds that the router tables will be updated based upon the SNMP router polling response.

**ADC Auto-discover:**

If enabled, the FX Remote will auto discover the FX Series ADCs by embedding probes in the TCP options. If disabled, then the FX Remote will perform acceleration with a static list of ADCs. The default value is "Enabled".

**ADC List:**

This field allows specification of IPv4 addresses of FX Series ADCs that the FX Remote will perform acceleration with.



**NOTE:** IPv4 addresses entered into this field while "ADC auto-discover" is enabled will not be accepted. Host names that require DNS resolution generally will not work because DNS requests only flow over the management interface.

**Inbound Bandwidth (Kbps):**

This specifies the amount of inbound bandwidth that will be directed to this interface.

**Outbound Bandwidth (Kbps):**

This field sets the total max outbound rate for all traffic classes of this interface.

**In-band Management:**

Normally out-of-band management of the FX is accomplished through the management interface, however in some scenarios, out-of-band management is not feasible and management of the device must be performed over an in-path interface. If this is the case, only one in-path interface may be used for in-band management. The default value is disabled.



**NOTE:** Changing this setting requires a restart of the acceleration service on the “Status->Real-time Monitor” page.



## 7 FX Series Status

### 7.1 FX Series ADC Status

This section provides the reporting options and statistics on a current and aggregate basis of many parameters which are monitored on the FX Series.



Figure 7-1 FX Series Status Menu

#### Real-Time Monitor

Perform real-time monitoring of the acceleration activity via our JavaScript status monitor applet. In order to run this applet, JavaScript must be enabled in your browser settings.

#### View Current Status

View XML formatted reports of current acceleration statistics, traffic control, network interfaces, routes, current connection, and current throughput.

#### 7.1.1 FX Series ADC Real-Time Monitor

Perform real-time monitoring of the acceleration activity via our Java JavaScript status monitor applet.



Figure 7-2 FX Series ADC Real-Time Monitor Screen

## Real-Time Statistics

### **CPU (%):**

This represents the CPU utilization of the FX Series ADC for all system tasks.

### **Memory usage (%):**

The percent of RAM being consumed by the ADC including both the WAN optimization service and the operating system. When this value approaches 90%, the ADC will automatically reduce its memory resource consumption to prevent service disruption.

### **HTTP objects retrieved:**

This shows the number of objects that the FX Series ADC retrieved from the target HTTP web servers.

### **HTTP server hits saved:**

The number of times that the back-end HTTP server did not need to service an HTTP request because it was handled out of the FX Series ADC cache. This tally also includes savings generated by the advanced caching of the client acceleration software.

### **HTTP hit savings (%):**

The percentage of "HTTP server hits saved" versus the total number of requests that would have been made to the back-end HTTP servers had it not been for the FX Series ADC.

### **HTTP request throughput:**

The number of HTTP requests per second that were processed by the ADC over the last refresh interval.

### **WAN bytes processed:**

Total number of bytes processed, both sent and received, by the FX Series ADC for traffic between clients and the FX Series ADC.

### **WAN bytes saved:**

This represents the reduction in traffic between clients and the FX Series due to various acceleration techniques such as data compression, cache differencing, JPEG reduction etc.

### **Remote cache savings:**

The number of bytes saved due to caching at the FX Remote.

### **WAN savings (%)**

The "WAN bytes saved" divided by the "WAN bytes processed".

### **Effective throughput:**

Shows the WAN bytes processed throughput based on the refresh interval.

### **Link throughput:**

This shows the number of bits per second received over the WAN port based on the refresh interval.

### **Capacity improvement:**

This is the bits per second improvement in the WAN link capacity due to the optimization provided by the FX ADC and Remote over the "refresh interval"

### **Capacity improvement %:**

This is the percentage improvement of the WAN link capacity provided by the FX ADC and Remote over the last refresh interval.

**Users:**

This is the total number of unique IP addresses that currently have one or more TCP connections from the remote users to the FX Series ADC.

**LAN Connections**

This is the number of TCP connections from the FX Series ADC to backend content servers such as web servers or file servers.

**WAN Connections**

This is the number of TCP connections between the remote users (including FX Series Remotes) and the FX Series ADC.

**Status**

This shows the current state of the acceleration service. Possible values are "Active", or "Stopped".

**Server running since**

This is the date and time that the FX Series ADC was last started.

**Refresh interval (sec)**

This is how often real-time monitor will refresh the statistics. Changes take effect immediately and are stored as a browser cookie and remembered in subsequent accesses to the real-time monitor.

**Action Buttons**

**Restart Service:**

This button provides a means to restart the acceleration service.

**Detailed stats:**

This displays all aggregate tallies accumulated since the ADC service was last started or since they were last reset.

**Connections:**

This displays a list of each connection-group. If the ADC is accelerating traffic for FX-Remotes then a connection group may be comprised of multiple TCP connections that form a TurboStream. If the ADC is servicing HTTP clients in a one-sided mode then each connection group will be comprised of a single TCP connection. When the list is displayed you can drill down on an individual connection-group to examine detailed tallies.

**Reset Stats:**

This button clears the acceleration server tallies and other stats including the stats displayed in the status monitor.

**Clear cache:**

This clears all objects out of all caches and then restarts the acceleration service.

## 7.2 QOS Status Monitor

The QOS Status Monitor provides a real time view of vital QoS statistics, including current, average and elapsed stats. All elapsed and average stats begin with the last Reset of the screen.

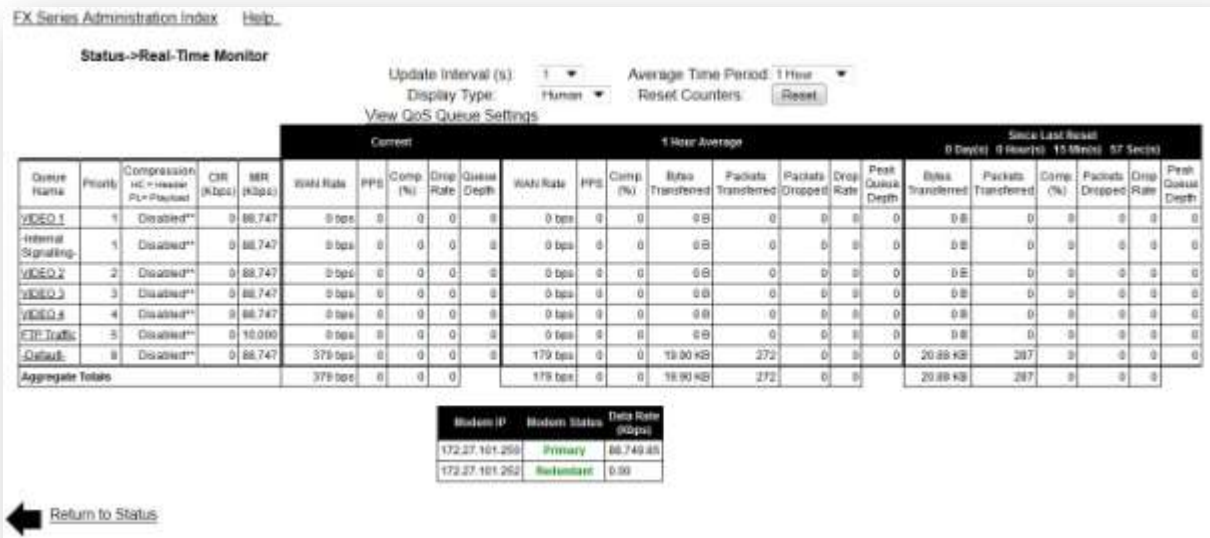


Figure 7-3 FX Series QOS Status Monitor Screen

### 7.2.1 QOS Status Monitor Options

#### Pull Downs:

##### Current Update Interval:

This determines the rate at which the screen is updated. There are selectable rates from 1 to 60 seconds.

##### Average Time Period:

This selects the time for which stats are averaged in the associated field. Options are 1, 24 and 72 hours.

##### Display Type:

Raw is the just that, the raw number. Human readable uses metric conventions. All data rate numbers will be given as powers of 10. In this case, k = 10<sup>3</sup>, M = 10<sup>6</sup>, G = 10<sup>9</sup>, and T = 10<sup>12</sup>. This refers to both data rate and total number of packets sent.

When referring to the number of bytes sent, the convention is powers of 2. In this case, k = 2<sup>10</sup>, M = 2<sup>20</sup>, G = 2<sup>30</sup> and T = 2<sup>40</sup>.

##### Reset Button:

This resets the inception time to the current time.

## 7.2.2 QOS Status Matrix

### By Queues

All defined queues are represented in the list. Queues are referenced by name

#### Priority:

This is the assigned priority.

#### Compression:

Indicates if packet header and payload compression is enabled. Choices are Header (HC) only, both or disabled.

#### CIR: (Kbps):

This is the assigned CIR.

#### MIR: (Kbps):

This is the assigned MIR

### Current QOS Stats

#### Data Rate (Kbps):

Data rate averaged over the previous 5 seconds.

#### PPS:

Packet rate averaged over the previous 5 seconds.

#### Compression (%)

This indicates the percentage bandwidth reduction due to header and payload compression.

#### Drop Rate:

Drop rate averaged over the previous 5 seconds.

#### Queue Depth:

Max queue depth over the previous 5 seconds.

### Average Rate:

This average is set with the average time period pull down menu shown above. Average time can be 1, 24 or 72 hours.

The fields in Average Section update at intervals that are a function of the Average Time Period. When the Average Time Period is set at 1 Hour, the fields update every minute on the minute as given by the "Since Last Reset" timer. If the total time is less than an hour, then the fields represent the data since the last reset. For example, if it's been 37 minutes, 14 seconds since the reset, then the data represents the first 37 minutes of traffic.

When the Average Time Period is set to either 24 or 72 hours, the fields update every hour on the hour as given by the "since Last Reset" timer. If the total time is less than the number of hours set by the Average Time Period, then the fields represent the data since the last reset. For example, if the Average Time Period is set to 72 hours, and it's been 54 hours, 38 minutes and 18 seconds since the last reset, then the fields represent the first 54 hours of traffic.

The rates are updated every minute and represent the data over the respective interval terminating at that time.

**Data Rate (Kbps):**

Average data rate over the interval.

**PPS:**

Average packet rate over the interval.

**Compression (%)**

Indicates the percentage bandwidth reduction due to header and payload compression.

**Bytes Transferred:**

Total bytes transferred during the interval.

**Packets Transferred:**

Total packets transferred during the interval.

**Packets Dropped:**

Total packets dropped during the interval.

**Drop Rates:**

Rate at which packets are dropped during the interval.

**Peak Queue Depth:**

Maximum number of packets on the queue during the interval.

**Since Inception: (elapsed since last reset)**

Stats for the queues are also kept since the last reset. These stats are updated every second.

**Bytes Transferred:**

Total bytes transferred.

**Packets Transferred:**

Total packets transferred.

**Compression (%)**

Indicates the percentage bandwidth reduction due to header and payload compression.

**Packets Dropped:**

Total packets dropped

**Drop Rates:**

Percentage of the packets dropped.

**Peak Queue Depth:**

The maximum Queue depth

**Aggregate Totals**

This line gives the totals over all the queues.

### 7.2.3 Modem Status:

This block is visible if polling the satellite modem is enabled on the Dynamic ACM screen. In this block, the modems are identified by IP address, the status as Primary or redundant is identified and the data rate is identified.

The modem that is active will have a non-zero data rate in the “Data Rate” field. This rate will be that which is currently being read from the modem. The non active modem rate will be zero.

### 7.2.4 Output Data Rate:

If polling is not enabled for a satellite modem, then this block will appear. This block will identify the clear sky data rate configured for the output port.

## 7.2.5 FX Series ADC Current Statistics

This screen allows you to view various reports generated by the ADC. On most of the reports, you can hit the "F5" key and your browser will update the report. Note that the FX Series Remote has only a subset of the reports of the FX Series ADC.

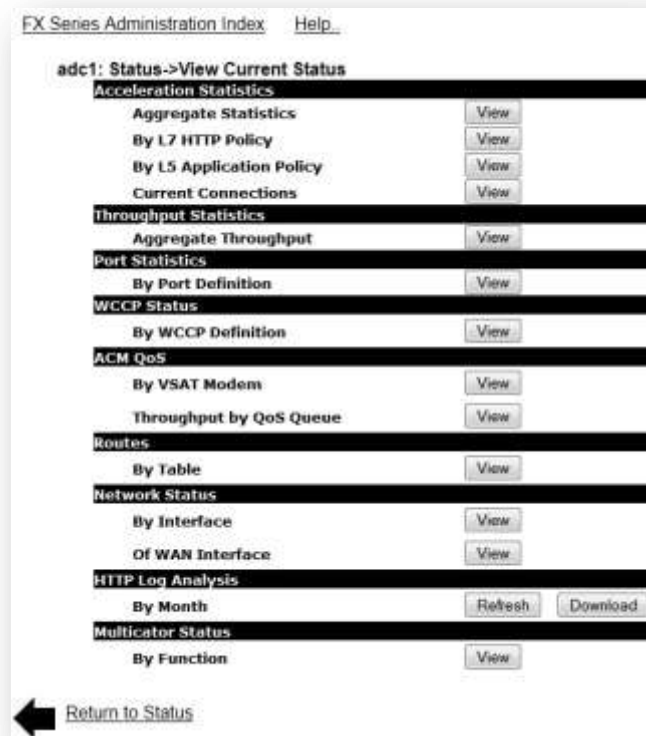


Figure 7-4 FX Series ADC Current Status Screen

### View

This button causes the associated log to be opened which will launch the program (on the viewer's computer) that is associated with file type ".log" or ".xml" in "Folder Options" of your Windows control panel, depending on the log file being accessed.

### Acceleration Statistics

This is a recording of the acceleration tallies that have accumulated since the last time that they were cleared or since the FX Series software was last restarted.

#### Aggregate Statistics:

This shows tallies of many acceleration techniques.

#### By L7 HTTP Policy:

This shows counters on a per L7 HTTP policy basis

#### By L5 Application Policy:

This shows counters on a per L5 Application policy basis

#### Current Connections:

This shows a report of remote clients currently connected.



## Throughput Statistics

This is a recording of FX Series ADC throughput statistics based on current statistics since either the last time that the statistics were cleared or the configured “throughput statistics interval” has elapsed. The “delta” value in the upper-left corner of the report indicates the number of seconds that elapsed in the throughput interval. A snapshot of the current statistics was taken “delta” seconds ago; each counter in this snapshot is then subtracted from corresponding counter in the “current statistics”. The remainders are then divided by the “delta” value to yield throughput values on a “per second” basis. It is possible that some of the values in the report are negative, meaning that a counter declined at a certain rate (for example CPU utilization may go down) over the throughput interval. The size of the throughput log file is relatively constant.

## Port Statistics:

This provides summary traffic counters for each port definition

## WCCP Status:

This provides a summary status of all of the service groups that the ADC is a member of. This report includes redirection maps and other important counters.

## ACM QoS:

### By VSAT Modem:

This report provides a summary status of the satellite modems if modem polling is enabled. Also provides a summary of filter matches.

### Throughput by QoS Queue:

This report provides a real time view of vital QoS statistics, including current, average and elapsed stats.

```
Tue Oct 1 16:06:07 GMT 2013
Dynamic ACM is DISABLED!
Current data rate is 255,000 kbps
#
# QoS Queues
#
There are 5 qosqs, of which 0 have packet compression enabled
-----
Name      Pri      Max Rate (bps)  Cur Rate (bps)  Drops      Pkts on Q      IngressBytes      IngressPkts
-----
  Signaling Q      1           20,000           472           0           0           0           0
-Internal Signalling-  1      255,000,000           0           0           0           0           0
  Realtime media   2           2,000,000           0           0           0           0           0
  Test Queue       2           20,000,000           0           0           0           0           0
  -Default-        8           255,000,000       20,600           0           0           0           0
#
# Filters
#
There are 6 filters
-----
Filter Name      AssignedToQueue      Prot.      Matches      Criteria
-----
-Internal Signalling-  -Internal Signalling-  Any           0
  Test Filter         -Default-             TCP           0           VLAN 300 DestPorts=80
    arps              Signaling Q           ARP           796
  RealTime media      Realtime media        TCP           0
SrcPorts=554,5505,5000-5010,64064,1935,1111,8134
  -Default-          -Default-             Any           37,677
  Test Filter 2      Test Queue            UDP           0
```

## Routes:

This report shows a detailed list of all the routes that are currently in use on this ADC on all route tables.

**Network Status:****By Interface:**

This report shows detailed statistical information about each active network interface on this ADC.

**Of WAN Interface:**

This report shows detailed stats about the WAN interface, in particular the MAC address needed to configure layer 2 packet compression is shown below:

```
Wed May 15 00:12:25 GMT 2013
eth3      Link encap:Ethernet  HWaddr 00:90:0B:26:5E:aa
          inet6 addr: fe80::290:bff:fe26:5e07/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:1037785 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59175394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:94519261 (90.1 Mb)  TX bytes:80227185974 (76510.6 Mb)
          Interrupt:19 Memory:febe0000-fec00000
```

**HTTP Log Analysis:**

- This chart shows graphically the statistics on the HTTP objects which have been requested by clients accelerated by this ADC.
- The “View” button shows the last report that was generated by clicking the “Refresh” button.
- If the “Refresh” button was never pressed then no report will be displayed.
- The “Download” button allows download of a zipped copy of the HTTP log file in its current state.
- The HTTP Log Format is described in the information below.

**Multicator Status:**

This report shows summary counters of reliable multicast events.

```
General.Miscellaneous.HostName = adc1
General.Miscellaneous.Version = 6.1
General.Miscellaneous.Status = Active
General.Miscellaneous.Up Since = Tue May 14 22:31:12 2013
General.Miscellaneous.HDD used = 5,167,394,816
General.Miscellaneous.HDD Capacity = 30,546,030,592
General.Miscellaneous.Real memory used = 1,952
General.Miscellaneous.Virtual memory used = 63,736
Controller.Config.Controller is enabled = 0
Controller.Current.Current receivers = 0
Transmitter.Config.Transmitter is enabled = 0
Transmitter.Current.Current size = 0
Transmitter.Cumulative.Files sent = 0
Transmitter.Cumulative.Bytes sent = 0
Receiver.Config.Receiver is enabled = 0
Receiver.Current.Filename = (null)
Receiver.Current.Expected Size = 0
Receiver.Current.Bytes Rcvd = 0
Receiver.Cumulative.Files Rcvd = 0
Receiver.Cumulative.Bytes Rcvd = 0
```

## **HTTP Log Format**

Each line of the FX HTTP log represents a separate HTTP request. Each line has the following format:

```
OriginatorsIP streamInfo AccelerationTechnique - [TimeStamp] "HTTPRequest"  
HTTPStatus Bytes
```

OriginatorsIP is the IP address of the client that made the request

streamInfo is seven strings separated by commas. The first three strings are hex digits that represent flow identifiers.

The next 4 strings are:

fbr=nnn where nnn is number of milliseconds since the client request came in until the first byte was received from web server

lbr=nnn where nnn is number of milliseconds since the client request came in until the last byte was received from the web server

fbs=nnn where nnn is number of milliseconds since the client request came in until the first byte was sent back to the client

lbs=nnn where nnn is number of milliseconds since the client request came in until the last byte was sent back to the client

AccelerationTechnique is one of:

"IMS-HIT" - The client issued an If-Modified-Since request for an object which was in the cache and fresh.

"INM-HIT" - The client issued an If-None-Match request for an object which was in the cache and fresh.

"HIT" - The object was returned from cache

"CV-HIT" - The object was returned "Not Modified" from the content validation cache

"DIFF\_HHIT" – Cache difference of just the response HTTP header

"DIFF\_HIT" – Cache difference of the object

"REFRESH-UNMODIFIED" – The requested object was cached but STALE. The IMS query for the object resulted in "304 not modified"

"REFRESH-MODIFIED" – The requested object was cached but STALE. The IMS query returned the new content.

"404-HIT" - The object was returned a 404 Not Found based on the freshness of the 404 cache object

## 7.3 FX Series Remote Status

### 7.3.1 FX Series Remote Real-Time Monitor

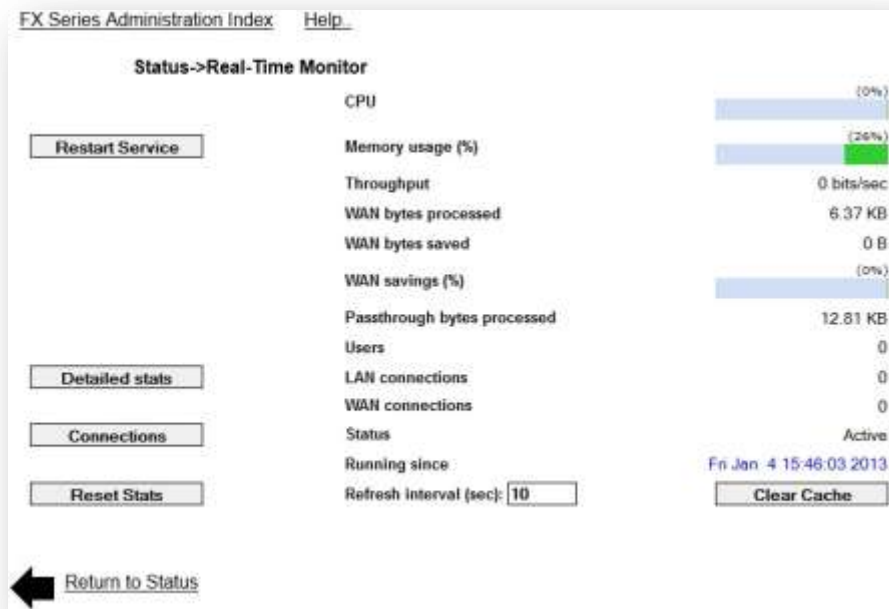


Figure 7-5 FX Series Remote Real-Time Monitor Screen

Perform real-time monitoring of the acceleration activity via our Java status monitor applet.

#### Real-Time Statistics

##### CPU (%):

This represents the CPU utilization of the FX for all system tasks.

##### Memory usage (%):

This shows the percent of RAM being consumed by the FX Series Remote including both the WAN optimization service and the operating system. When this value approaches 90%, the appliance will automatically reduce its memory resource consumption to prevent service disruption.

##### WAN bytes processed:

Total number of bytes processed, both sent and received, by the acceleration server for traffic between clients and the acceleration server.

##### WAN bytes saved:

This represents the reduction in traffic due between clients and the acceleration server due to various acceleration techniques such as data compression, cache differencing, JPEG reduction, Dynamic Data Suppression etc.

##### WAN savings (%):

The "WAN bytes saved" divided by the "WAN bytes processed".

**Throughput:**

This is the throughput, in bits per second, since the last refresh interval.

**Pass through bytes processed:**

This is the total quantity of bytes that have flowed through the acceleration server but no optimization operations were attempted.

**Users:**

This is the total quantity of unique IP addresses that have TCP connections flowing through the FX Remote.

**LAN Connections:**

This shows the quantity of TCP connections between clients and the FX Remote.

**WAN Connections:**

This shows the quantity of TCP connections between the FX Remote and FX SERIES ADCs.

**Status:**

This shows the current state of the acceleration service. Values are "Active", or "Stopped".

**Server running since:**

This is the date and time when the acceleration server was last started.

**Refresh interval (sec):**

This is how often real-time monitor will refresh the statistics. Changes take effect immediately and are remembered in subsequent accesses to the real-time monitor.

**Action Buttons**

**Restart Service:**

This provides a means to restart the acceleration service.

**Detailed stats:**

This displays tallies and other stats.

**Connections:**

This displays the active user connections to the acceleration server.

**Reset Stats:**

This clears the acceleration server tallies and other stats including the stats displayed in the status monitor.

**Clear cache:**

This clears all objects out of all caches, and then restarts the acceleration service.

### 7.3.2 FX Series Remote Current Status Reports

This page allows you to view various reports generated by the FX Series Remote. On most of the reports, you can press the “F5” key and your browser will update the report.

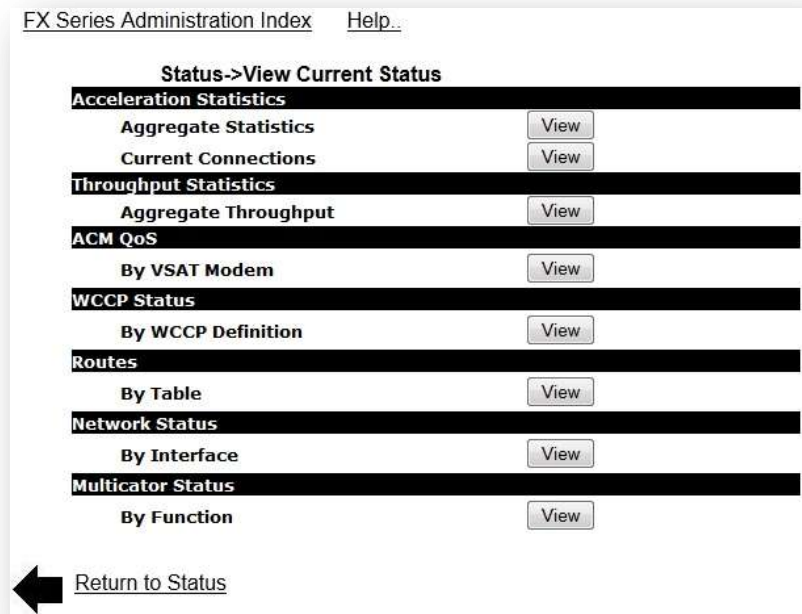


Figure 7-6 FX Series Remote Current Status Screen

#### Acceleration Statistics

##### Aggregate Statistics:

This is a recording of the acceleration tallies that have accumulated since the last time that they were cleared or since the acceleration server software was last restarted.

##### Current Connections:

This report shows the user names, connection type, and other data of each currently active connection to the acceleration server.

##### Aggregate Throughput:

This is a recording of acceleration server throughput statistics based on current statistics since either the last time that the statistics were cleared or the configured “throughput statistics interval” has elapsed. The “delta” value in the upper-left corner of the report indicates the number of seconds that elapsed in the throughput interval.

##### Aggregate Throughput Calculation:

A snapshot of the current statistics was taken “delta” seconds ago; each counter in this snapshot is then subtracted from corresponding counter in the “current statistics”. The remainders are then divided by the “delta” value to yield throughput values on a “per second” basis.



**NOTE:** It is possible that some of the values in the report are negative, meaning that a counter declined at a certain rate (for example CPU utilization may go down) over the throughput interval. The size of the throughput log file is relatively constant.

## **Other Status Reports**

### **ACM QoS:**

This provides a summary status of the satellite modems if modem polling is enabled.

### **WCCP Status:**

This provides a summary status of all of the service groups that the FX Series Remote is a member. This report includes redirection maps and other important counters.

### **Routes:**

This report shows a detailed list of all the routes that are currently in use on this FX Series Remote on all route tables.

### **Network Status:**

This report shows detailed statistical and status information about each active network interface on this FX Series Remote.

### **Multicator Status:**

This report shows summary counters of reliable multicast events.

## 8 FX Series Optimization Settings

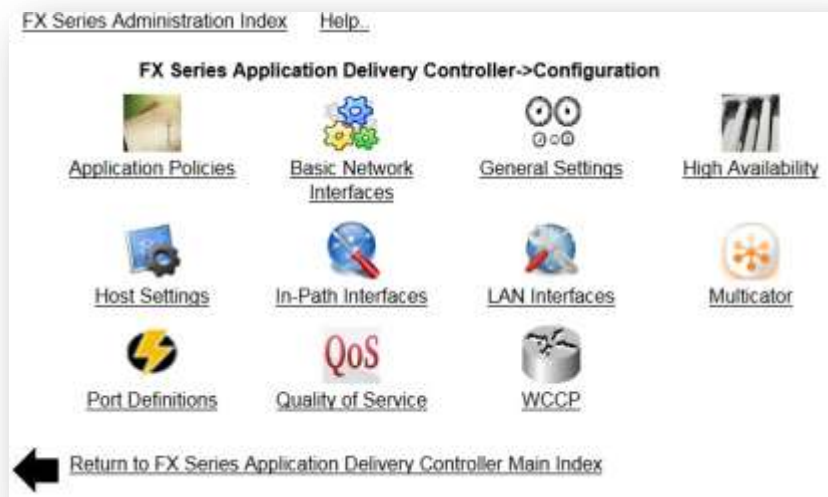


Figure 8-1 FX Series ADC Features Menu

### 8.1 Configure Application Policies

Customize the optimization techniques settings on the FX Series ADC by central policy management that will apply to your enterprise applications.



Figure 8-2 FX Series ADC Application Policy Menu

#### Authorization Realms

Define objects based on source IP, browser type, and other criteria to be used as a basis for policies.

#### Web Application Policies

Choose this if you wish to configure the optimization properties of the HTTP-based Web applications that the FX Series ADC will accelerate.

#### Layer 5 Application Policies

Choose this if you wish to configure the optimization properties of the non-HTTP-based TCP/IP applications that FX Series ADC will accelerate.



### 8.1.1 FX Series Optimization Summary

- The FX Series is built upon a flexible and secure base of operating system and acceleration software. Utilizing an architecture that is modularized, The FX Series accelerates the movement of data, accelerates the processing of that data and ensures a safe and reliable system.
- The FX Series can be configured and implemented in several ways to accelerate enterprise application traffic. All implementations start with an appliance, which functions as a "front-end" processor to web servers. In this initial "one-sided" mode, the appliance processes traffic between HTTP clients (browsers) and web servers. The FX Series can also be implemented with optional client-side hardware, FX Series Remote appliance. The client-side appliance provides many additional optimization features in a "two-sided" mode.
- With flexible options for in-line or Cisco's Web Cache Communication Protocol (WCCP) the FX Series devices deliver unprecedented transparent optimization. End to End assurance is maintained for all applications providing complete transparency and the ability for existing Quality of Service (QOS) and network visibility management programs to continue monitoring the health of your network.
- Business critical applications requiring 24/7 availability will always perform optimally no matter how fast your business grows. The Stampede FX Series platforms support deployments in either N+N or N+ 1 configuration. Simply add additional FX Series devices as needed for increased scalability or failover protection.
- Stampede's FX Series platforms provide a comprehensive range of flexible options for total transparent 24/7 operation within your existing or growing network infrastructure. No matter what your application acceleration or WAN optimization requirements are today or in the future, Stampede's FX Series platform solutions will handle all your business critical applications with ease

### 8.1.2 Single-Sided Optimizations:

#### **GZIP:**

Industry standard compression is applied to both static and dynamic HTML and XML content including attachments.

#### **Image Optimization Transformation:**

This reduces image size, while optimizing image quality.

#### **Static Caching:**

This returns un-expired static objects and pages directly from cache.

### 8.1.3 Two-sided Optimizations

#### **TurboStreaming:**

Optimization techniques are utilized to overcome inherent TCP inefficiencies. This removes congestion from WAN links and significantly improves response time for downloading large attachments, even those considered to be non-compressible.

#### **Content Aware Compression**

##### **Dynamic Cache Differencing:**

The FX Series ADC appliance and the Remote appliance maintain a copy of browser cache and send only the difference back to the browser when content is changed.

**Persistent Connection:**

The FX Series maintains a persistent TCP connection with clients with a configurable timeout based on application policy.

**Content Aware Caching:**

The FX Series accelerates client accesses by eliminating round-trips to servers to validate data. This is intelligently performed to avoid unnecessary network consumption and reduces server transaction processing.

#### 8.1.4 Authorization Realms

Authorization realms provide a means for grouping users so that different policy application attributes can be assigned. For example, perhaps you want a set of users to have unrestricted Internet access and others you wish to be routed to another appliance that performs filtering, then you can define authorization realms to delineate these user groups by assigning different application policies based on authorization realm.



**NOTE:** Examples for using Authorization Realms is shown in Section 8.3.2

**Realm Name:**

This specifies the logical name to assign to this realm. This name is used to reference the definition in the application policies and client policies.

**Comment:** This is a description in which the administrator can enter up to 64 characters of text.

**Origin IP Address Ranges:**

Specified using “CIDR” notation where a base IP address is followed by a ‘/’ character which is followed by a value between 1 and 32 that denotes the number of bits used to describe the network and the remaining bits (32 – the value) are used to specify the nodes on that network. For example a setting of 192.110.1.0/24 would be equivalent to specifying a network of 192.110.1.0 with a net mask of 255.255.255.0. Separating each CIDR entry with a comma can specify multiple destinations. You may also enter one or more single IP addresses or hyphenated IP address ranges, separated by commas in the same manner. i.e. 10.2.2.5 or 10.2.2.50-10.2.2.59. In a two-sided environment with FX-Remotes, the IP address must be that of an in-path interface of the FX-Remote. The default setting is any network.

**VLAN ID:**

Specifies the VLAN ID for which the realm should apply. If “None” is selected then the VLAN ID is not part of the match criteria when realms are evaluated. The selector only shows VLAN IDs for which an in-path interface has been defined.

### Client Type:

This field allows you to specify that client types that are associated with this authorization realm.

The valid choices are:

Native – HTTP traffic which is not accelerated by a Plug-In

FX-Remote – Traffic which is accelerated by the FX Series Remote Appliance



**NOTE:** Press and hold the control key for multiple selections. The default is any client type.

### In-Path Interface:

Allows you to designate the authorization realm to only apply to traffic that flows on a particular VLAN.



**NOTE:** When assessing authorization realm membership, if the appliance determines that if all of the above field criteria are met, then the user is deemed to be a member of the authorization realm.

### Using Authorization Realms for Testing:

Authorization realms can be useful for testing because they provide a convenient means to stage deployment of new application policy.

- You can define an authorization realm with just one IP address – that of a test machine.
- Then you can enable an application policy and limit the deployment to that authorization realm.
- When you are satisfied that further deployment is warranted you can broaden the scope of the authorization realm for further staging or you may choose to delete the authorization realm altogether from the policy.

### 8.1.5 Web Application Policies

#### Purpose

The Web application policies control how the FX Series interacts with various web sites. This will allow users to enable, disable, and tune acceleration techniques for specific URLs. A Web application policy is defined by two parts: a Target web server (HOST) and an Application (the trailing text of the URL following the host portion).

#### Example:

In this example the user has requested the web site “**www.dailygalaxy.com**” which is the target web server or host. The page or application is “my\_weblog/2011/09/image-of-the-day-firey-icy-beauty-of-an-infrared-neptune.html”. We could enable or disable features for this web site by entering “**www.dailygalaxy.com**” as the Target Web Server in the web application policy and entering and star / asterisk “\*” as the application wildcarding all request to the defined web server. We can also gain greater granularity by adding portions of the application to the application field.



**NOTE:** How to set up Web Application Policies is shown in Section 8.3

A list of previously defined Application Policies is displayed in the order in which they were defined. An existing entry may be chosen by clicking on the Policy.

You can “Enable”, “Disable”, or “Delete” one or more Policies definitions by selecting the checkbox to the left of the Title column and clicking on the desired button. By clicking on “Add” you can add a new Application Policy which will bring up the Application Policy definition screen.



**NOTE:** Policy Deletions are allowed 10 minutes after all active client connections using the policy have terminated.

#### Target Web Server

The case-insensitive name of the web server for this policy can also be a virtual server name that corresponds to a pool defined in the “Load Balancing” configuration section. The name can be a fully qualified domain name or it can be a short name (no dots in the name). This name is relative to the browser and is often not the same name that the FX Series ADC uses to access the content when it is functioning as a forward or reverse proxy. It is possible to configure both the short name and a fully qualified name with different policies. In this case, the policy in effect will depend on whether the URL has just a short name or a fully qualified domain name.



**NOTE:** If a non-standard port (80 or 443) is used to access the application, the port must be specified as part of the name. An IP address may also be specified in lieu of a host name.

The server name can be configured with a leading “\*”. This allows an administrator to configure all servers within a domain. An example of this is “\*.acme.com” which means all servers in the acme.com domain. If “\*” or empty then the policy applies to all servers running the specified application. Do not enter the “http://” or “https://” prefix when specifying this field. The administrator can configure a default server by having a policy that is either “\*” or empty. If the FX Series does not find a match for the server then it will look for this default server.

## Application

The case-insensitive application name for this policy can be a partial name. For example, if “abc” is specified, then this policy will apply to a URL containing “abc/def”. When the FX Series ADC matches a URL against its application policies it will apply the most specific match that it encounters. If “abc/def” is specified in addition to “abc”, then this policy will be used for a URL containing “abc/def/ghi”.



**NOTE:** Additionally, the application name of the policy can be “\*” or empty. This is the default application policy for this server. If no other match is found then this policy will be used. It is possible to configure both a default server and a default application. This becomes the default policy that is used when no server and application names match.

### 8.1.6 Authorization realm

This is a pull-down selector that enables you to limit the scope of this policy to a specific previously defined authorization realm. Authorization realms (see Section 8.1.4 above) allow users to be grouped based on source IP address or in-path interface.

**Comment:** Up to 80 characters of text can be entered to help document your configuration.

### 8.1.7 Enable Acceleration

Acceleration can be turned on or off.

- When Enable Acceleration is “Yes”, the FX Series ADC will perform the acceleration techniques that are enabled in this policy.
- When Enable Acceleration is “No”, then, no acceleration techniques will be applied for applications specified by this policy.
- When a FX Series Remote or Plug-In is used and “Enable Acceleration is set to “No”, then the FX Series Remote or Plug-In will pass the HTTP requests directly to the application server and bypass the FX Series ADC. The default value is “No”.

### 8.1.8 Caching

#### Cache Data at ADC

This setting specifies if requested HTTP objects should be cached on the FX Series ADC. The “Guaranteed object freshness time” also applies to these cached objects. The default is to cache the HTTP objects (“Yes”).

#### Cache Data at Remote

This setting specifies if requested HTTP objects should be cached on the FX Series Remotes (REM). The default is to cache the HTTP objects (“Yes”).

#### Enable Cache Differencing:

The FX Series ADC will cache dynamic content sent to a FX Series Remote or Plug-In enhanced browser. On subsequent accesses to the same content, the FX Series ADC will send the changes rather than the entire updated content and the FX Series Remote will edit the changes into its cache. The default is to enable cache differencing (“Yes”).

### 8.1.9 Content Validation

#### Guaranteed Object Freshness Time (seconds)

This setting determines the number of seconds that will elapse after storing an object in the client browser cache before the object must be verified for freshness. If the value is set to 0 then objects are verified every time the object is accessed. The default value is 10800 seconds (3 hours).

**For Static Content:**

The FX Series ADC optimizes data flow by keeping track of object expiration times. For native browsers, if the object has not changed then a HTTP 304 Not Modified response is sent from the FX Series ADC without requiring a round-trip between the FX Series ADC and the target web server. If the client browser is engaged with the FX Series Remote or Plug-In enhanced browser, then this operation is performed at the client eliminating round-trips between the browser and the FX Series ADC.

**Override Expirations**

This specifies whether the FX Series ADC should intelligently override the expiration date of an object based on its heuristics. This feature reduces round trips by eliminating many unnecessary content validation requests from the browser. Enabling this option for caching in some instances could produce undesirable results. The default value is "Yes".

The object must be one of the content types specified in the "For the following content types:" field. A comma separates each content type. The default value for this field is: "image/\*, text/css, application/x-javascript, application/x-shockwave-flash, and text/javascript"

### 8.1.10 Image Optimization

**JPEG Transformation**

This function can lower the resolution of a JPEG in order to reduce communication bandwidth requirements. The goal of the JPEG quality and smoothing values is to reduce the amount of data while maintaining a usable image. The default settings (Quality=50, Smoothing=20) are reasonable settings for most images and give a dramatic savings on the size of the jpeg images. The image is still very usable but is not as crisp as the original. Depending on the jpeg, the compression is often in the range 9:1. If image quality is paramount, setting Quality to 75 and Smoothing to 0, will still give some image size savings with little if any loss of image integrity. There is a tradeoff between quality image compressions while still yielding some savings of image sizes. The optimal setting is application dependent.

**JPEG Quality**

A number between 1 and 100 that specifies the tradeoff between size of the jpeg data and quality of the original image. A higher number will retain a higher quality but will not conserve as much bandwidth. The default value is 50.

The JPEG quality setting allows you to trade off compression against the quality of the reconstructed image: the higher the quality setting, the larger the JPEG bandwidth requirements, and the closer the output image will be to the original input.

**JPEG Smoothing**

A number between 1 and 100 that specifies the amount of dithering that will be used when generating the image. A higher value indicates more dithering and somewhat less desirable image. The default value is 20.

**Minimum size threshold in K**

This setting sets a minimum size of the JPEG file that is required for the JPEG optimization processing to engage. The default size is 5K.

### 8.1.11 Back-End Server Interface Options

These options govern how the FX Series ADC will communicate with the back-end Web application server.

#### **Request GZIP content:**

If set to “Yes” then the FX Series ADC will request that the backend servers deliver the content to the FX Series ADC in GZIP format. This saves bandwidth over the backhaul connection and is suitable for most ISP environments. If set to “No”, then the back-end server will deliver the content to the FX Series ADC in non-compressed form. “No” may be a good setting for an enterprise server environment where the FX Series ADC is offloading the GZIP task. The default setting is “Yes”

#### **Web server timeout (seconds)**

This sets the number of seconds that the FX Series ADC will wait for a request to be fulfilled from the enterprise web server. After the timeout a 502 HTTP error code will be returned to the browser that initiated the request. The default value is 40 seconds.

#### **Use reduced window scaling:**

If set to “Yes” then the ADC will use a smaller window scaling factor when connecting to back-end servers. The default value is “No”.

### 8.1.12 When Application Policies Take Effect:

Application policy changes take effect on an FX Series ADCs immediately after changes are made. Once this occurs, the FX Series Remote will be notified of the policy change at the next object retrieval request. At that time, the FX Series Remote will read all of the current policies from the FX Series ADC, and it will adhere to those policies for the applications for which that FX Series ADC is being used for optimization. The new policies will not affect the FX Series Remote interaction with other FX Series ADCs (if it is interacting with multiple FX Series ADCs concurrently).

---

## 8.2 Web Application Firewall Features

The FX Series ADC offers Web Application Firewall capabilities to an enterprise infrastructure. Below is a discussion of these features and how to configure them in an FX Series ADC:

### 8.2.1 Buffer Overflow Prevention:

Detection and blockage of overflow attacks which otherwise could lead to malicious code being run on a server or other unauthorized access. This is an inherent feature of the FX Series ADC - no special configuration is required. Any buffer overflow detected in an HTTP message will cause an event to be recorded in the exception log.



## 8.3 Setting up Basic Web Application Policies

This section is designed to delineate how to set up application policies. All of the detail descriptions for each item are provided in Section 8.1.5 above. Application policy changes take effect on an FX Series ADC immediately after changes are made.

### 8.3.1 How to Set the Policy Header

Applicability	Inherited Setting
Target web server	*
Application	*
Authorization Realm	
Enable Acceleration	Yes
Comment	

Figure 8-3 FX Series Application Policy Applicability

#### Set the case-insensitive name of the Web server for this policy.

The server name can be configured with a leading “\*”. This allows an administrator to configure all servers within a domain.

#### Set the case-insensitive application name for this policy.

This can be a partial name. Additionally, the application name of the policy can be “\*” or empty. This is the default application policy for this server. If no other match is found then this policy will be used.

#### Set the authorization realm to define the users who will use this policy

If the default authorization realm is used, then the policy will apply to all users. Setting up authorization realms will be described in the next section.

**Comment:** This field is used to briefly describe the purpose of the policy.

#### Enable or disable acceleration for this policy

Acceleration can be turned off or on. When Enable Acceleration is “Yes”, the FX Series ADC will perform the acceleration techniques that are enabled in this policy. When Enable Acceleration is “No”, no acceleration techniques will be applied for applications specified by this policy. The default is enabled.

#### When complete click on “Add Application Policy”



**Note:** A “default policy” is a policy which allows access to all servers, all applications for all users. It is created with a “\*” in these fields: Target Web Server, Application Policy. In addition it uses the default user authorization realm, which is set to all users. Acceleration can be enabled or disabled for this policy. If disabled, then you would want to set other policies to allow users access to specific site(s).

### 8.3.2 Set Specific Users Access

This section allows you to restrict the application policy to a specific set of users/IP addresses. All of the detail descriptions for each item are provided in Section 8.1.4 above. The standard setting preconfigured in the default settings is: *all sites available and accelerated for all users with all client types on any port*. NOTE: Authorization realms can be useful for testing because they provide a convenient means to stage deployment of new application policy by limiting the users who can access the new application policy.

FX Series Administration Index Help

Configuration->Application Policies->Authorization Realms->Edit

**Authorization Realm**

Name

Comment

**Attributes**

Origin IP address ranges

Client Type  Native Browsers  Fx Remote

In-Path Interface

[Return to Authorization Realms](#)

Figure 8-4 FX Series Authorization Realm Screen

#### Setting the authorization realm name

This specifies the logical name to assign to this realm. This name is used to reference the definition in the application policies and client policies and can be up to 64 characters of text.

**Comment:** This field is used to briefly describe the users that this realm applies.

#### Set the origin IP address ranges for the users that this realm applies.

You may enter one or more single IP addresses or hyphenated IP address ranges, separated by commas in the same manner. i.e. 10.2.2.5 or 10.2.2.50-10.2.2.59. The default setting is any network.

#### Set the client type that this realm applies.

This field allows you to specify that client types that are associated with this authorization realm. Pressing the control key allows you to choose multiple selections. The default is any client type.

#### In-Path Interface:

Allows you to designate the authorization realm to only apply to traffic that flows on a particular VLAN.

When complete click on **"Add Authorization Realm"**

### 8.3.3 Restrict acceleration for specific sites, or users

- To restrict acceleration for *specific sites*; set up application policy for each specific site with acceleration disabled in the policy
- To restrict acceleration for *specific users*; set an application policy for specific authorization realm with acceleration disabled in the policy
- To restrict all acceleration except for specific sites for *certain user groups*
  - Set a \* application policy with acceleration disabled in the policy for the default authorization realm.
  - Set an application policies for the specific sites with acceleration enabled in the policy for a specific authorization realms

### 8.3.4 Set Specific Optimization Techniques

Each of these options can be enabled or disabled by clicking on the preferred choice. The inherited default for all acceleration options is “Yes” for enabled except the reduced window scaling option. All of the detail descriptions for each item are provided in Section 8.1

Caching		
Cache data at ADC	<input type="radio"/> Yes <input checked="" type="radio"/> No	Yes
Cache data at RWOC	<input type="radio"/> Yes <input checked="" type="radio"/> No	Yes
Enable cache differencing	<input type="radio"/> Yes <input checked="" type="radio"/> No	Yes
Content Validation		
Guaranteed object freshness time (seconds)	<input type="text" value=""/>	10800
Override expirations	<input type="radio"/> Yes <input checked="" type="radio"/> No	Yes
For the following content types:	<input type="text" value="image/*,text/css,text/javascript,application/x-javascript,application/x-shockwave-flash"/>	
Image Optimization		
JPEG transformation	<input type="radio"/> Yes <input checked="" type="radio"/> No	Yes
JPEG quality	<input type="text" value="50"/>	50
JPEG smoothing	<input type="text" value="20"/>	20
Minimum size threshold in K	<input type="text" value="5"/>	5
Backend server interface options		
Request GZIP content	<input type="radio"/> Yes <input checked="" type="radio"/> No	Yes
Web server timeout (seconds)	<input type="text" value="60"/>	60
Use reduced window scaling	<input type="radio"/> Yes <input checked="" type="radio"/> No	No

[Add Application Policy](#)

[Return to Web Application Policies](#)

Figure 8-5 FX Series Specific Optimization Techniques Configurations

#### For the following content types

The default value for this field is “image/\*, text/css, application/x-javascript, application/x-shockwave-flash, text/javascript”. Additional items can be added to this line and placing all items in the field.

#### JPEG Quality

The default is 50. The range of the field is 1 – 100. A higher number will retain a higher quality but will not conserve as much bandwidth.

#### JPEG Smoothing

The default is 20. The range of the field is 1 – 100. A higher value produces a less desirable image.

## 8.4 Layer 5 Application Policies

“Layer 5” acceleration provides optimization of communication protocols when a FX Series Remote is installed at a branch in “in-line” mode. The FX Series Remote can then intercept and optimize the traffic with additional capabilities such as dynamic data suppression and traffic classification/prioritization.

Layer 5 application policies are defined at the ADC and then read by the FX Remote to determine how it should process the traffic that it intercepts as an in-line bridge.

A list of previously defined Application Policies is displayed in the order in which they were defined. An existing entry may be chosen by clicking on the Policy.

You can “Enable”, “Disable”, or “Delete” one or more Policies definitions by selecting the checkbox to the left of the Title column and clicking on the desired button. By clicking on “Add” you can add a new Application Policy which will bring up the Application Policy definition screen.



**NOTE:** Policy Deletions are allowed 10 minutes after all active client connections using the policy have terminated.

### 8.4.1 Certified Applications

This is a pull-down of pre-defined communication protocols that have been certified as compatible with FX Series application acceleration. These include HTTP, CIFS, MAPI, NFS, FTP, SMTP, and POP3. If you select one of the pre-defined choices then the fields of the policy will be populated.

### 8.4.2 Configuring Other Applications

If the traffic that you wish to accelerate is not listed then select “Other” and you can set the policy field based on the characteristics of the protocol.

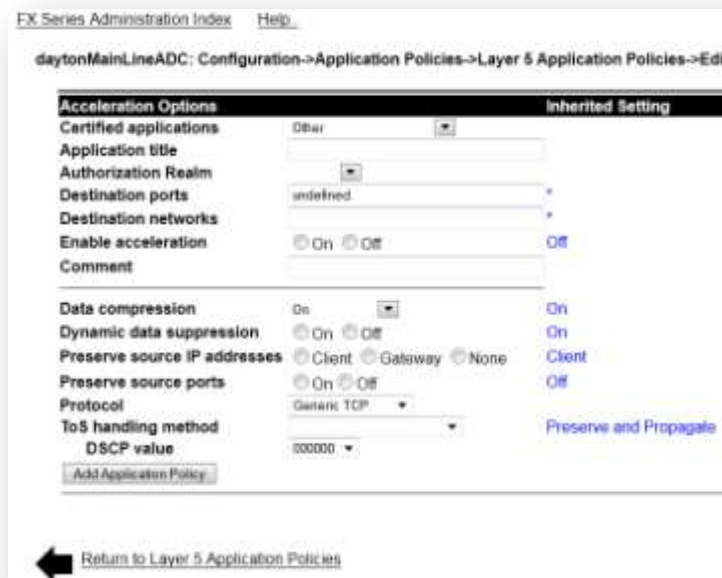
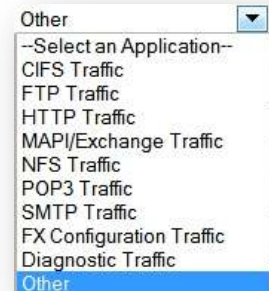


Figure 8-6 FX Series Layer 5 Policy Configuration Screen

**Application title:**

This field applies a name to the traffic being accelerated.

**Authorization Realm:**

This is a pull-down selector that enables you to limit the scope of this policy to a specific previously defined authorization realm. Authorization realms allow users to be grouped based on organization source IP address.

**Destination ports:**

This mandatory setting allows you to specify the TCP port(s) that apply to this policy. Multiple ports may be specified separated by commas or a port range may be specified with a dash. Multiple port ranges may be separated by commas. The minimum port value is 1 and the maximum value is 65535. There is no default setting.



**NOTE:** A "\*" policy for L5 can be defined. A "\*" policy is a port range of 1-65525.

**Destination networks:**

This setting allows you to limit the Layer 5 acceleration only to traffic that is destined for certain networks. The destination network is specified using "CIDR" notation where a base IP address is followed by a '/' character which is followed by a value between 1 and 32 that denotes the number of bits used to describe the network and the remaining bits (32 – the value) are used to specify the nodes on that network. For example a setting of 192.110.1.0/24 would be equivalent to specifying a network of 192.110.1.0 with a net mask of 255.255.255.0. Separating each CIDR entry with a comma can specify multiple destinations. The default setting is all networks.

**Enable Acceleration:**

If enabled then the FX-Remote will apply the acceleration techniques based upon the specifications of this policy, otherwise it will not intercept the traffic specified in this policy. This setting is useful for defining exceptions to a broad port range defined in other policies. The default setting is 'Enabled'.

**Comment:**

Up to 80 characters of text can be entered to help document your configuration.

### 8.4.3 Configuring Layer 5 Optimizations

**Data compression:**

If "On", and the remote machine is enhanced with the Layer 5 software, then bi-directional compression of all traffic is performed. If "Off" is specified, then no compression will be performed. If "Only-to-client" is set, then data compression will only be performed on traffic that flows from the server to the client. If "Only-to-server" is set, then data compression will only be performed on traffic that flows from the client to the server. The default is on.

**Dynamic data suppression:**

If "On", the FX Series will maintain a byte cache of network traffic and replace repeated patterns with signatures when they are detected in the data stream. The default value is on.

**Preserve source IP address:**

This specifies which source IP address should be presented to the back-end server when the ADC makes requests on behalf of a remote client. If "Client" is specified then the client's IP address will be used. If "Gateway" is specified, then the IP address of the gateway will be used, this is sometimes useful when Network Address Translation makes it unfeasible to use the client's IP address. If "None" is specified, then the ADC's IP address is used. The default setting is "Client".

**Preserve source ports:**

This specifies if the ADC should use the same source port as the client. If “On” then “Preserve source IP address must be set to “Client”. If this is set to “Off”, then an arbitrary port will be used. Some applications such as “NFS” require this to be set to “On”. The default setting is “Off”.

#### 8.4.4 Layer 5 Protocols

This setting allows a protocol-specific optimization module to process the traffic. The choices are as follows:

**Generic TCP:**

Perform “Dynamic data suppression” (DDS), QOS traffic prioritization, compression, TurboStreaming on the traffic.

**HTTP/HTTPS:**

In addition to the Generic TCP optimization, perform intelligent object caching, cache differencing, turn reduction and other techniques as specified in L7 application policies on the traffic.

**CIFS:**

In addition to the Generic TCP optimization, perform optimizations to overcome unneeded latencies in the CIFS application protocol.

**MAPI:**

In addition to the Generic TCP optimization, performs optimizations to overcome unneeded latencies in the MAPI application protocol that is used in Outlook/Exchange server communications.

**SMTP/POP3:**

This optimizes standard internet email traffic.

**FTP:**

In addition to the Generic TCP optimization, this performs optimizations to allow better DDS when communicating with an FX Series Remote.

**Diagnostic:**

This specifies parameters when running diagnostic tests between FX Series Remote and FX Series ADC.

**FX Configuration:**

This protocol entry is utilized by FX-Remotes for ADC location services. FX Remote appliances will use this entry to locate configuration information when Auto-discovery is not enabled. The default is for Auto-discovery to be enabled so normally this entry is not used. This entry is auto-generated when new in-path interfaces are created and should not be deleted. If this entry is deleted it can be easily added back by simply selecting it from the list and selecting “Add Application Policy”.

#### 8.4.5 ToS handling method

Specifies how you want the FX to handle “Type of Service” (ToS) bits in the IP header for accelerated traffic. The default method is to “Preserve and Propagate” which means that ToS bits for request packets will be preserved through the acceleration tunnels and propagated in the responses. “Preserve” means that the ToS bits will be preserved for request traffic but not propagated in the responses. “Set” means that the FX will apply the ToS bits as specified in the “DSCP value” field in both the request and response traffic.

**The DSCP value:** Specifies the ToS bits based on the binary value in the “DSCP value” field. DSCP is an abbreviation for “Differentiated Services Code Points” and is described in more detail in the [RFC-2724](#) specification.

### 8.4.6 Layer 5 Acceleration - Theory of Operation

“Layer 5” acceleration provides optimization of communication protocols when a FX Remote is installed at a branch in “in-line” mode. The FX Remote can then intercept and optimize the traffic with additional capabilities such as dynamic data suppression and traffic classification/prioritization. Most TCP based protocols can be accelerated with this solution, however there are some exceptions:

- FTP can only be accelerated when it is operating in “passive” mode. By default the ftp function of the Internet Explorer operates in “active” mode and you must adjust an advanced browser setting in order for Layer 5 to operate. Also the standard Windows command line “ftp.exe” program only operates in “active” mode and therefore can’t be accelerated by Layer 5.
- Due to the nature of some TCP/IP based protocols; The Layer 5 acceleration techniques can function however they do not provide significant benefit. For example:
  - The latest version of MS-Outlook/Exchange protocol is already highly compressed and also there is an application level acknowledgement that takes place after every 17K bytes which defeats the value of TurboStreaming. (MS-Outlook using the POP3/SMTP protocols can derive great benefit from Layer 5 acceleration.)
  - Protocols that are encrypted (or already compressed) will not benefit from the product’s Layer 5 compression but may benefit from the TurboStreaming.

The following table depicts a list of TCP and UDP ports used by well-known applications.

Application	TCP / UDP	Ports
CIFS	TCP	139,445
Citrix ICA	TCP/UDP	2598,1494
CVS	TCP	2401
DNS	UDP	53
FTP	TCP	20,21
Lotus Notes/Domino	TCP	1352
Lotus Sametime	TCP	1533
MS Remote Desktop Connection	TCP	3389
NFS	UDP	2049
Novel GroupWise	TCP	1677
NTP (Network Time Protocol)	UDP	123
POP3	TCP	110
SIP (Session Initiation Protocol)	TCP/UDP	5060,5061
SMTP	TCP	25
Telnet	TCP	23
TFTP	UDP	69
TurboGold Enterprise Edition	TCP	4916
VNC	TCP	5900
Windows Live Messenger (Voice)	TCP/UCP	6901

**Figure 8-7 FX Series TCP/UDP Ports Table**

## 9 FX Series Operations Features



Figure 9-1 FX Series Operations Menu

### Backup/Restore Configuration

This facility allows you to backup or restore your FX's configuration files.

### Change Passwords

This function allows you to change the administrative interfaces to the FX.

### Manage Licenses

This function allows you to view and replace license files or Fast codes. These are used to license the specific appliance, turn on the Multicator functionality and set the Max Data Rate.

### Shutdown/Restart Appliance

This facility allows you to shut down and restart the appliance.

### Packet Capture

This function allows you to collect WireShark compatible packet captures on up to two interfaces concurrently.

### Update Software

This facility allows you to upload and install the latest acceleration server images



## 9.1 Basic Operations Functions

### 9.1.1 Backup/Restore Configuration Files

This screen allows you to back up the acceleration server configuration files so that you can quickly restore your FX as part of a disaster recovery procedure.



Figure 9-2 FX Series Backup and Restore Screen

The files include hostname, time-zone, and IP addresses for the management and in-path interfaces, DNS server, settings, application policies, and SSL security certificates. The files are backed up to a single “.zip” file which is then downloaded to your desktop workstation.

#### Backup Acceleration Appliance:

This button causes the acceleration server configuration files to be stored into a zip file with the name “wrbackup\_hostname\_year-month-day.zip”. Following this, a dialog will appear so that you can save this file to your desktop.

#### Restore Acceleration Appliance:

This button should only be clicked after selecting a backup zip file using the "Choose File" button. Following this, clicking the "Restore Acceleration Appliance" button will restore the appliance from the specified zip file. The specified zip file should have been previously created using the "Backup Acceleration Appliance" button. The FX must be restarted for the restoration to take effect.

### 9.1.2 Disaster Recovery Procedure

In the event that you need to restore your FX from a USB flash drive, please complete the following steps:

- 1) Reinstall the installation image from USB Flash drive.
- 2) Using the “FX Series Appliance Manager”, set your passwords for the acceleration server administrator by selection "Configure Appliance", and then "Configure Passwords".
- 3) Using a browser, go to the FX’s “Operations” page and select
- 4) "Backup/Restore Configuration". Then, restore the configuration from the backup zip file.
- 5) From the “Operations” page, select "Shutdown/Restart Appliance", then click
- 6) "Restart Appliance Hardware" to restart the FX.
- 7) Using the “Appliance Management Program”, re-establish the high-availability keys for the cluster-mates that share a common acceleration server configuration.
- 8) Re-apply any patches that you may have applied subsequent to your installation via the Web Administrative GUI.

### 9.1.3 Change Password

This function allows you to change the FX Administrator password used by the FX Series appliance. If you do not remember this password you will have to re-initialize the FX Series appliance. To change the password you must enter it twice and then press the corresponding “Change” button.



Figure 9-3 FX Series Change Passwords Screen

### 9.1.4 Manage Licenses / Fast Codes

This function allows you to install and update the license file or fast codes for the FX Series appliance. For all new installations, Fast Codes will be used for upgrading functionality and Max Data Rates



Figure 9-4 FX Series Upgrade Fast Codes Screen

#### Fast Codes

The Fast Code is a 14 digit key that will enable the WAN Optimization and the max data rate.

**Upgrading Fast Code:** Enter the character sequence provided by Comtech, and then click the ‘Upload Upgrade Code and Restart’ button. If successful, this action will immediately restart the acceleration service and the new upgrade license information will be displayed.



**NOTE 1:** There are 'trial license' fast codes for 30/60/90 days for Packet Compression and WANOP. The remaining time trial license period will be noted in the license display at the left bottom of the Web GUI screens with the firmware version and the serial number.



**NOTE 2:** For existing installations, where a license file is currently being used, an upgrade is available to move to Version 6.0.3 for the new features, including Multicator. License files will continue to be used for these appliances.

## 9.1.5 Shutdown/Restart Appliance

This function allows you to power down or reboot your FX Series appliance in an orderly fashion. If you wish to just restart the acceleration software service then go to the “Status->Real-Time Monitor” page.



**Figure 9-5 FX Series Shutdown/Restart Appliance Screen**

### Shutdown Appliance Hardware

This button will issue a command to the native operating system to shut down the software in an orderly fashion and then power down the appliance.

### Restart Appliance Hardware

This button will issue a command to the native operating system to shut down the software in an orderly fashion and then reboot the appliance.

### Start Acceleration Service

This button will issue a command to the native operating system to start the acceleration service. This button will not be displayed if the service is already started.

### Restart Acceleration Service and Reset Cache

New restart acceleration service and reset cache function. This button will stop the acceleration service, clear the cache, and restart the acceleration software.



This is now the only way to completely reset the cache files. (real-time monitor now does a 'quick' reset that does not require reboot.)

### Stop Acceleration Service

This button will stop the acceleration service but still allow access to the appliance via the management interfaces. If the appliance is configured for “in-band” management then this button will not be displayed.

## 9.2 Packet Capture

This function allows you obtain packet captures to facilitate troubleshooting of network connectivity problems.

Figure 9-6 FX Series Packet Capture Screen

### Capture Parameters

#### Max packet size (bytes):

Specifies how much of each packet to store in the capture file. The max size is whatever your MTU is set to for the interface (up to 9000 for jumbo frames) and the default size is 1500.

#### Max capture size (MB):

This specifies the maximum size of the capture file before rotating to a second file. The default size is 10 megabytes.

#### Capture filter:

This specifies a filter that will reduce the size of the capture file by recording only the traffic which matches the filter.

#### 1<sup>st</sup> Capture interface:

Select the Ethernet interface that actions (e.g. “start” “stop”) of the first capture will be associated with.

#### 2<sup>nd</sup> Capture interface:

Use the pull down and select the Ethernet interface that actions of the second capture will be associated with. In this case it is eth5.



#### Save Button:

This button must be clicked in order to apply them prior to performing the capture actions.

### **Capture Actions**

After the common parameters have been “Saved”, you can click the “start” or “stop” buttons associated with the capture interfaces that have been defined.

### **Download Traces**

After stopping the packet captures, click the “Download Traces” button to invoke a log collection process that will zip up the packet captures and also an assortment of event tracing logs. The captures in the “.zip” file will have names that end in either “.pcap0” or “.pcap1”.

### **Sample Capture Filters**

host 10.1.1.1

Records only traffic for which either source or destination is 10.1.1.1

tcp port 443

Records only traffic for which either source or destination is port 443

tcp port 443 and host 10.1.1.1

Records only traffic that has source/dest port 443 AND also has source/dest of 10.1.1.1

## 9.3 Update Software

This selection allows you to apply available acceleration server software updates to your systems.



**Figure 9-7 FX Series Update Software Screen**

If you are running both FX Series ADCs and Remotes, then you would want to update the FX ADCs and then apply the Remote updates using the recommended process outlined.

### 9.3.1 Upload and Apply Server Installation Image Version 6.02+:

This button can only be clicked after selecting a file relative to your desktop workstation using the “Choose File” button. After picking the updated Acceleration Server software from the location that you saved it, click on the “Upload and Apply Server Installation Image” button to upload the software and install it on the system.

### 9.3.2 Download and Apply Image from ADC (FX Remote Only):

This button downloads the RCO firmware image that is included with the ADC and applies it to the FX Remote.

### 9.3.3 Software Update Discussion

The acceleration service has to be started to update the appliance. If the acceleration service is not started, the button to update the appliance will be disabled.

An FX Remote polls the FX ADC every 45 minutes to determine if a software update is available. If a newer version is available and the FX ADC is configured to “Automatically distribute remote updates” then the FX remote will automatically download the update and apply it.

Applying the firmware update, regardless of the method used to acquire the image, results in about a 30 second service disruption.

### 9.3.4 Recommended Process for Software Upgrades

A recommended practice for deploying new FX image updates is as follows:

- On FX ADC, navigate to "Configuration->General Settings". Turn off "Automatically Distribute Remote Updates".
- On FX ADC, navigate to "Operations->Update Software". Use the "Upload and Apply Server Installation Image" to update the firmware on the FX ADC.
- After the firmware update is applied to the FX ADC, plan a time window when you would like firmware updates to be distributed to the FX Remotes. This time window could be an hour or two and is usually done when traffic is low.
- At the time that you wish to distribute updates to the FX Remotes, on the FX ADC, navigate to "Configuration->General Settings". Turn on "Automatically Distribute Remote Updates".
- Since each FX Remote checks every 45 minutes for an update, within an hour all FX Remotes should have downloaded and applied the firmware update.
- After all FX Remotes have been updated, navigate to "Configuration->General Settings". Turn off "Automatically Distribute Remote Updates".

To verify that the FX Remote devices have been updated, you can use SNMP to query the version number of FX Remote firmware.

- The OID of the version string is 1.3.6.1.4.1.19418.1.2.1.1.
- The following Windows console script would show the version numbers currently running at two FX Remotes using the net-snmp tools:

```
set netsnmp=c:\netsnmp
set SNMPCONFPATH=c:/netsnmp/etc/snmp;c:/netsnmp/snmp/persist
set SNMPSHAREPATH=c:/netsnmp/share/snmp
bin\snmpwalk -m all -v 2c -c public 172.27.101.206 1.3.6.1.4.1.19418.1.2.1.1
bin\snmpwalk -m all -v 2c -c public 172.27.101.244 1.3.6.1.4.1.19418.1.2.1.1
```

- Execution of the above script would yield the following output:

```
C:\netsnmp 14:46:13.25>bin\snmpwalk -m all -v 2c -c public 172.27.101.206
1.3.6.1.4.1.19418.1.2.1.1
SAAS-RCO-MIB::wanopVersion.0 = STRING: "6.0.0a-201206081729N4.x86_64"
C:\netsnmp 14:46:13.57>bin\snmpwalk -m all -v 2c -c public 172.27.101.244
1.3.6.1.4.1.19418.1.2.1.1
SAAS-RCO-MIB::wanopVersion.0 = STRING: "6.0.0a-201206081729N4.x86_64"
```

---

## 9.4 Updating FX Series Appliance Software at 5.78.0 or earlier

This is a two-step process.

1. Upgrade the Base Platform Image and install version 5.78.0
2. Upgrade the application software to version 6.1 or later.

### 9.4.1 Base Platform Image (BPI) Upgrade Process

The Comtech FX Series version 6.1 or higher includes features that were not included in the previous Comtech FX Series releases. These will require a Base Platform system software upgrade.

This Upgrade kit enables upgrading from 5.78 or earlier releases to a platform capable of supporting the new FX 6.1 and higher functionality. Note that all FX 5.78 or earlier versions are compatible with this BPI upgrade. The completion of the BPI upgrade process will install version 5.78.0. The process to upgrade the appliance to Version 6.1 will follow the standard upgrade process as discussed in section 9.5 below. In addition,

### 9.4.2 Upgrade Kit and Prep

The upgrade kit consists of the following:

- This Guide
- A bootable USB drive that will automatically install the new FX Series BPI including FX Series 5.78.0 system software.

### 9.4.3 The Upgrade Process

- 1) You will need to save the current configuration file to your PC desktop.
- 2) The USB drive will upgrade the FX Series BPI to accommodate FX Series version 6.0.3.
- 3) It will ask for which appliance you are upgrading:
  - a. FX Series ADC or FX Series Remote
- 4) Once you choose, it will install the appropriate Version 5.78 FX Series Software
- 5) You will then manually restore the saved configuration file.
- 6) You can then remove the USB drive and reboot the server.

#### Save Current Configuration File

Connect to the appliance using the Web GUI as described above.

- 1) Login in using "comtech" and your current password
- 2) Go to the "Operations Screen".
- 3) Chose "Backup/Restore Configuration"
- 4) Click on "Backup Configuration"
- 5) Save configuration file. -
- 6) This file must be used after the BPI upgrade and before the upgrade to Version 6.0.3.

#### Configure "Boot Options" for USB Drive

- 1) With the appliance powered off, insert USB drive
- 2) Reboot the appliance, clicking on "delete key"
- 3) Select "Boot Options" tab and set USB flash drive as the first boot drive Set HDD as the 2nd boot drive
- 4) Choose "(F10) Exit" and save changes - system will reboot.



## Running the upgrade process

After the system reboots, enter “Y” or “N” at the “let me ask again. Are you sure you want to *continue*” prompt.



**NOTE:** Entering “Y” will proceed to re-image the local hard drive.

1. The appliance will power down automatically when the imaging has completed.
  - 1) Remove the Comtech USB drive.
  - 2) Reboot the system and use the basic menu-driven interface as described above
  - 3) You will be presented with “FX Series Appliance Manager” screen that includes which FX Series software (FX SERIES ADC or FX Remote) to install.
  - 4) Select the appropriate choice to install.

## Restore Current Configuration File

- 1) Log into the Web GUI and go to the “Operations Screen” as you did earlier
- 2) Chose “Backup/Restore Configuration”
- 3) Click on “Restore Configuration”
- 4) Browse to the configuration file that you saved earlier
- 5) Click on “Restore Configuration Files”

**The FX Series BPI update is now completed and your system is on Version 5.78.0. You are ready to now upgrade to FX Series Version 6.1. See Section 9.5 for upgrade procedure.**

## 9.5 Updating FX Series Appliance Software to Version 6.1

This function allows you to apply available acceleration software updates to your FX appliance.



**NOTE:** You must have run the Base Platform Image upgrade (BPI3) and currently be at Version 5.78.0 or higher before you can upgrade to Version 6.1 or higher.

The Comtech FX Series version 6.1 includes packet compression features that will require a Base Platform Image (BPI) service pack upgrade to enable the functionality. It is recommended that it is installed for all WANOP enabled appliances. Note that **only** the FX 6.1 and above versions are compatible with the service pack.

### 9.5.1 User Interfaces

The FX Series supports a basic menu-driven interface, which is accessible using the console port (eth0), and SSH or a web-based graphical user interface (GUI). The operations functions are accessed through the Web GUI.

To connect to the GUI, use any PC with a Web Browser to access:

`http://yourFxSeriesHostname:10000` or IP address. The default USERID and PASSWORD are "comtech" and "comtech or your current password" for both console and Web GUI.

### 9.5.2 Determine the Current Software Version

Telnet, SSH <IP address> or login with console

Go to: Option 2 "Show Status" >> Option 1 "Show Version Information"

### 9.5.3 Screen print version information for reference

Check your current machine's [FX-Series Acceleration System Software Package](#). In the example below, the version is shown as 5.78.0 and has been upgraded to BPI3 (-FX9)



**NOTE:** If you have upgraded the Base Platform Image to BPI3 to prepare for the Version 6.1+ upgrade, you should be at 5.78.0

Check your software

```
Version Information:
  FX Series Appliance Manager - Version: 5.78.0
  Operating System: Linux linux-3z1j 2.6.38.8-FX9 #1 SMP PREEMPT Wed Dec 7 16:48
:51 EST 2011 x86_64
  openSUSE 11.4 (x86_64)
  VERSION = 11.4
  CODENAME = Celadon
  Fx-Series Acceleration System Software Package: 5.78.0-201111301824N4.x86_64
  WebMin Package Version: webmin-1.550-1.noarch
```

**Figure 9-8 FX Series Software Version Display Screen**

If there is a more recent software package with a version for your OS, you can upgrade.



**NOTE:** To utilize the newest functionality you should upgrade to Version 6. 1+.

If you have not updated the BPI to v3, see the process for updating to Version 5.78.1+ with the new Base Platform Image (BPI) on page 142.

#### 9.5.4 Determine the Available Upgrade Versions

Access the Comtechefdata.com web site

<http://www.comtechefdata.com/support/software/flashupgrades/ran-wan-optimization/stampede-fx-series>

Or Home » Support » Software Downloads » Flash & Software Update Files » Stampede FX Series Software Downloads

1. Download the 6.1 version of software
2. Download the 'FX Platform Image Update' ("spker-3.7.9-FX27.bin")

If there is a more recent software package with your version, you can upgrade.

To utilize the newest functionality you should upgrade to Version 6. 1+.



See the process for updating to Version 5.78.1+ with the new base platform image (BPI) on page 142, if you have not updated the BPI to v3.

#### 9.5.5 Download the files to your desktop or other convenient location.

Download the 6.1 software and the service pack on the PC that you will be using to access the appliance by the web based admin module.

#### 9.5.6 Check for new software:

If it is currently at BPI version 3 and version 6.0.2 or below, then the 6.1 version must be downloaded and that upgrade completed before the service pack is applied.

Download the current 6.1+ version file to your desktop or other convenient location.

Download the Service Pack file ("spker-3.7.9-FX27.bin") to the same location.



**NOTE:** You need to place the updated software and patch on the PC that you will be using to access the appliance by the web based admin module.

#### 9.5.7 Installing the Latest Software Version

This function allows you to easily update the FX Series software to the latest version.

##### Upload and Apply Server Installation Image:

Browse to the location that you saved the updated software and select the software

##### Install the software

Click on the "Upload and Apply Server Installation Image" button install it on the system. The system will automatically upload the software, install it and reboot the appliance.



**NOTE:** The new software version should show in the licensing information at the bottom left of the Web GUI Admin Screens.

#### 9.5.8 Install the FX Platform Image Update

Browse to the location that you saved the updated software and select the software

Select the service pack: "spker-3.7.9-FX27.bin"

#### 9.5.9 Upload and Apply FX Platform Image Update:

Click on the "Upload and Apply Server Installation Image" button install it on the system. The system will automatically upload the software, install it and reboot the appliance.



**NOTE:** The FX Series software should be now updated to the current software level with the latest service pack.

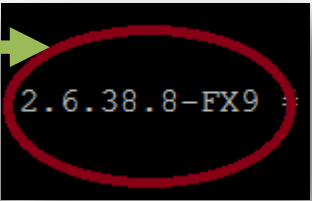
### 9.5.10 Verify Update Success

Telnet, SSH <IP address> or login with console

Go to: Option 2 "Show Status" >> Option 1 "Show Version Information"

```
Version Information:
  FX Series Appliance Manager - Version: 6.0.0aD
  Base Platform Image Version:
6.0.-201202081500.x86_64
  Extended Platform Version:  Operating System: Linux adc-61faf8 2.6.38.8-FX9
1 SMP PREEMPT Wed Dec 7 16:48:51 EST 2011 x86_64
openSUSE 11.4 (x86_64)
VERSION = 11.4
CODENAME = Celadon
  FX-Series Acceleration System Software Package: 6.0.0aD-201205081959N4.x86_64

FX Series Appliance Manager - Status Menu
  0  Return to previous menu
  1  Show Version Information
```



**-FX9**  
Indicates  
that the BPI  
is now at  
BPI3.



NOTE: The Service Pack will appear on the Web GUI Admin Screens.

```
FX Series Application Delivery Controller™ - Build 6.1.0-201307091658N4-3.7.9-FX27
WAN Optimization is enabled
Max Throughput: 155 Mbps
```

It will end with "-3.7.9-FX27"

Screen Print both the version and service pack information for future reference.

## 9.6 FX Series Documentation

Current Documentation for this appliance can be found on these locations.

### 9.6.1 On the Comtech EF Data web site:

<http://www.comtechedata.com/stampedeDocs.asp>

Or

[www.comtechedata.com](http://www.comtechedata.com)

Under Support Information, Click on Manuals

Under *RAN & WAN Optimization*,

Click on [Stampede FX Series](#)

### 9.6.2 On the appliance:

To connect to the GUI, use any PC with a Web Browser to access:

Attach a cross-over cable to the eth1 interface and connect to the browser interface at [http:// 169.254.55.55:10000](http://169.254.55.55:10000)

Login using the USERID and password of “comtech” and “comtech”

Click on “*Documentation*” from the Main Index

#### To view a document:

You can open the document by clicking on the link in the left column of each row of the table. You can right-mouse on the links and “Save target as” to save a copy of the “.pdf” file to your desktop.

An overview of each document along with its estimated size is listed in the table.



**Note:** Visit <http://www.adobe.com> in order download a reader for these files.

# 10 Appendix

## 10.1 FX Series Console Management Functions

Here are some of the key screens for configuring many parameters on the FX Series Appliances.

The FX Series supports a basic menu-driven interface, which is accessible using the console port (eth0). It can also be accessed via SSH software once basic network connectivity is established.

### 10.1.1 Main Menu

```
FX Series Appliance Manager - Main Menu

 1   Configure Appliance
 2   Show Status
 3   Diagnose Network Connectivity

Enter Option: █
```

### 10.1.2 Configure Appliance

```
FX Series Appliance Manager - Configure Appliance Menu

 0   Return to previous menu
 1   Configure Network Settings
 2   Configure Passwords
 3   Configure Time
 4   Configure Web Management Interface
 5   Configure SNMP
 6   Restart this Optimization Appliance
 7   Configure FAST Codes

Enter Option: █
```

#### 10.1.2.1 Configure Network Settings

Select "1 Configure Network Settings"

```
FX Series Appliance Manager - Network Settings Configuration Menu

 0   Return to previous menu
 1   Configure Host Name
 2   Configure DNS
 3   Configure Default Gateway
 4   Configure TCP/IP for eth0 Ethernet Port
 5   Configure TCP/IP for eth1 Ethernet Port
 6   Configure TCP/IP for br0 Bridge Interface
 7   Configure TCP/IP for eth2 Ethernet Port
 8   Configure TCP/IP for eth3 Ethernet Port
 9   Set bridged or routed mode

Enter Option: █
```

### 10.1.2.2 Configure SNMP Settings

Select "5 Configure SNMP"

```
FX Series Appliance Manager - SNMP Configuration Menu

0   Return to previous menu
1   Enable/Disable SNMP
2   Configure 'SysLocation'
3   Configure 'SysName'
4   Configure 'SysContact'
5   Configure SNMP Trap Destination
6   Launch SNMP configuration wizard
7   Show SNMP Settings

Enter Option: █
```

### 10.1.2.3 Configure FAST Codes

Select "7 Configure FAST Codes"

```
FX Series Appliance Manager - FAST Code

0   Return to previous menu
1   Enter initial serial number
2   Enter upgrade code

Enter Option: █
```

### 10.1.3 Show Status

```
FX Series Appliance Manager - Status Menu

0   Return to previous menu
1   Show Version Information
2   Show System Up Time
3   Show Memory Status
4   Show Disk Space
5   Show Network Traffic Stats
6   Show CPU Utilization and Top Running Processes

Enter Option: █
```

### 10.1.4 Diagnose Network Connectivity

```
FX Series Appliance Manager - Diagnostics Menu

0   Return to previous menu
1   Ping
2   Determine MTU
3   Trace Route
4   Fetch a URL
5   DNS Lookup
6   Show the route table
7   Measure link speed between FX-Remote and ADC

Enter Option: █
```