



Contact us for more information
U.S. & Canada:
+1.800.763.3423
Outside U.S. & Canada:
+1.937.291.5035

The FX Series Configuration Options Ease Satellite Link Management

February 2011

Today's satellite networks are becoming increasingly more complex. The ability to overcome bandwidth limitations, latency, and packet loss becomes critical in order to improve performance and control IT costs. The FX Series provides IT managers with the tools necessary to configure, monitor, and manage satellite links to support more traffic, while lowering overall costs.

This document describes the different ways the FX Series head-end appliances, FX Series Remote appliances and Client Acceleration technology can be configured to accelerate application traffic for satellite networks. The FX Series product family is based on a single platform that supports a wide range of satellite network environments as a single-sided Application Delivery Controller (ADC), or two-sided with Remote WAN Optimization Controller (RWOC).

The FX Series manages application interactions and applies coordinated acceleration and optimization techniques within satellite networks. The FX Series provides the following benefits:

- Improves response times for Web requests
- Optimizes bandwidth utilization
- Reduces the amount of unnecessary data sent over satellite networks
- Reduces the number of TCP and application turns (handshakes) required to complete a transaction
- Offloads computationally intensive tasks from clients and servers

Single-Sided Solution

All implementations start with a FX Series (ADC), which functions as a "head-end" application delivery controller. As a single-sided solution, the FX Series ADC is placed in the network operations center (NOC). The FX Series "single-sided" mode provides:

- Outbound JPEG image reduction
- Outbound GZIP compression
- Data caching
- Application firewalling and URL access control

Two-Sided Solution

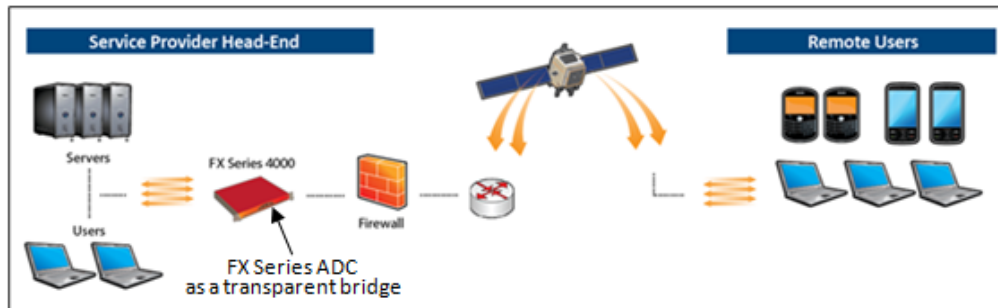
In a two-sided implementation, (RWOC), the FX Series ADC resides at the NOC, with the following remote options; FX Remote appliance or Acceleration On-Demand (AOD). The FX Series two-sided solution improves performance further through:

- Bi-directional data compression
- TCP turn reduction
- Cache differencing
- Cookie compression
- Multiplexing large compressed or encrypted data objects (TurboStreaming)
- Advanced Virtual Pipelining
- Content distribution / Pre-caching
- Persistent layer 5 virtual connections
- Protocol optimizations
- Traffic classification and prioritization
- Dynamic data suppression (DDS)

How the FX Series Fits into the Network Infrastructure

FX Series ADC in Transparent Bridge Mode

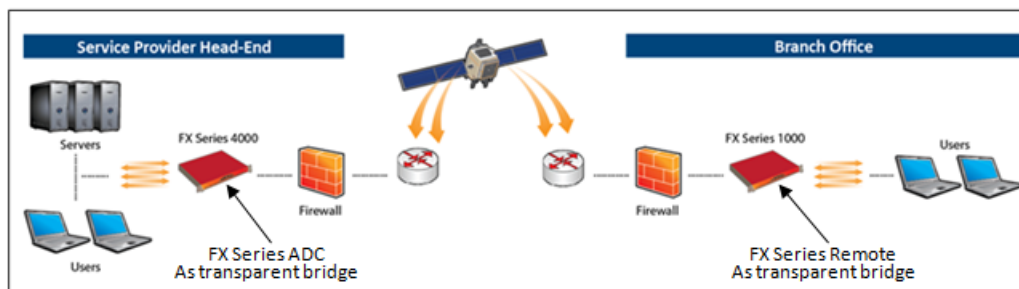
When operating in "transparent bridge" mode, the bridge networking ports are utilized such that all traffic flows through the FX Series ADC. In the event of a hardware or software fault, the specialized networking hardware "fails-to-wire" so that no loss of connectivity between clients and application servers can occur.



As a single-sided solution, the FX4000 Series located at the head-end, offers satellite connection management to fully utilize satellite link bandwidth.

FX Series Remote Transparent Acceleration

In the diagram below, an FX Series Remote appliance is deployed at a remote site. The specialized networking hardware allows the FX Series Remote to function as a transparent bridge and “fails-to-wire” if there is a software or hardware fault. The FX Series Remote examines all traffic and applies acceleration based on application policies defined at the FX Series ADC.



In a two-sided implementation, The FX4000 is located at the head-end, and FX1000 Series Remote appliance (or alternatively AOD) is located at the remote site.

Connection Management

Connection management removes the burden of establishing and terminating TCP connections from the web and application servers, allowing the servers to handle more traffic. The FX Series manages network connections in several ways to optimize the flow of data and reduce the impact on the network, 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 the 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. The FX Series eliminates this potential network-intrusive overhead.

Virtual Persistent Connections

The FX1000 remote appliance establishes a virtual / persistent session with the head-end FX Series appliance, maintaining session state information on both sides. Should the actual session between the FX Series remote and FX Series head-end appliance be interrupted for any reason (hard link failure, satellite loss, etc.), pertinent information is maintained, and the FX Series remote appliance will

reestablish communication when the session can reconnect. No data is lost, and the end-user may only experience a slight response time delay.

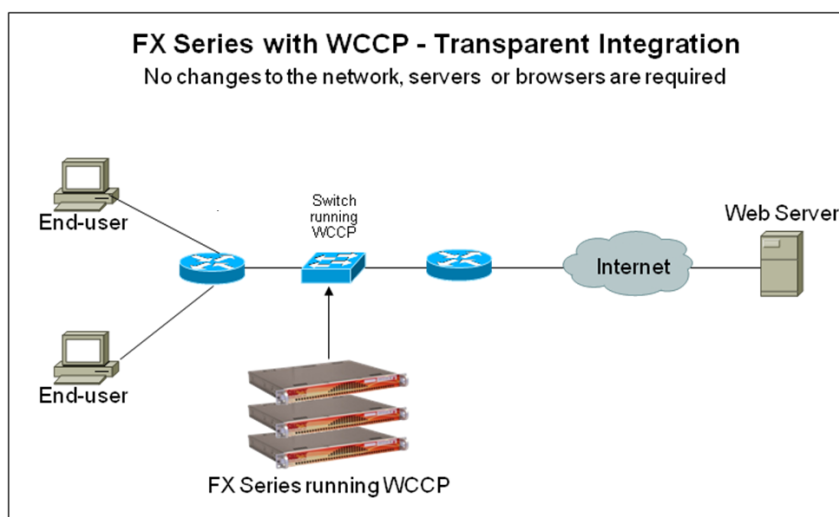
This feature is important for users of traditional client/server, or non-browser applications. If a session interruption occurs within these applications, all data could be lost, and typically the user must restart the session - wasting time and lowering productivity. The FX Series Virtual / Persistent connection feature mitigates this situation, and enables the end-user to continue without interruption.

FX Series Support for WCCP

The Web Cache Communications Protocol (WCCP) allows satellite Internet 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. 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 downtime, thus, ensuring fault-tolerance.

FX Series ADC with Transparent WCCP Redirection

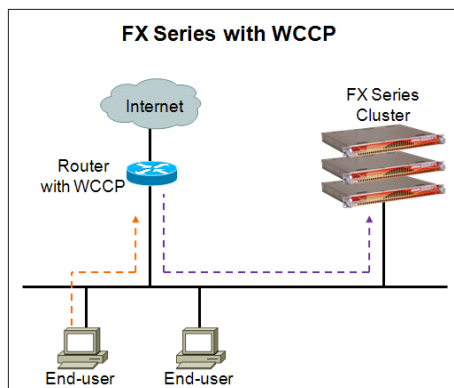
In this scenario, the Cisco router is configured such that requests from the client PCs are redirected to FX Series ADC. Based on the original source IP address, the Cisco router will direct the request to one of the FX Series ADCs in a pool.



Load balancing via WCCP intelligently distributes the TCP and HTTP workload across multiple FX Series appliances. For flexible scalability, satellite Internet 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.

WCCP enables Internet 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.

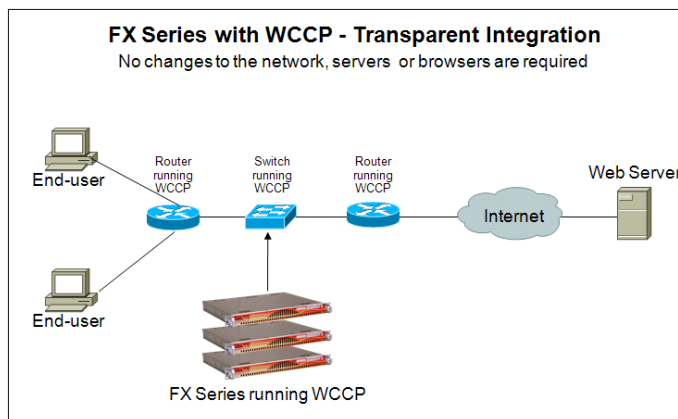
The FX Series (running WCCP) localizes content, and responds to content requests in order to reduce the amount of data going over the satellite link. This improves application delivery response times, and allows the link to support more traffic. Using WCCP, traffic is transparently redirected to the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



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.

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. 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.

With WCCP configured, the router redirects traffic to the FX Series to performance 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. See diagram below.



IP Source Preservation – IP Source 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 organizations Source IP address. The FX Series configuration method makes implementing IP Source Preservation easy within a WCCP environment. The FX Series is usually configured to use the IP address of the client when making requests to content servers, whereas, other acceleration devices 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 acceleration device is recorded in the Web server's logs. If the IP address of the acceleration device 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

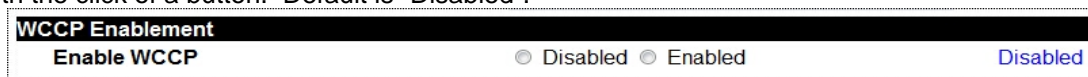
Series is able to avoid this problem. In addition to WCCP environments, source IP Preservation also works within transparent bridge mode.

Configuring the FX Series to Routers and Switches – The FX Series specifies the method in which the router or switch will direct packets. The configuration options are Generic Routing Encapsulation (GRE), or “Layer 2”, which means that the router will simply modify the MAC destination address to point to the FX Series appliance.

The FX Series Web GUI

The FX Series takes network deployments to a new level. The FX Series includes an easy-to-use Web GUI to allow network personnel to easily configure WCCP with the FX Series appliances. Below are examples showing how easy the FX Series is to use within WCCP deployments.

Enable web cache coordination protocol: This feature allows you to easily enable or disable WCCP support with the click of a button. Default is “Disabled”.



Protocol version: This feature specifies the version of WCCP that should be used. The default is 2.

Primary Router Settings

- **Router address:** This is the address of the primary router to which WCCP messages will be directed. This setting must be specified.
- **Source IP address:** This is the IP address (must have been already defined on the FX Series) that will be used when sending WCCP messages to the router.
- **Remote GRE tunnel address:** This is the address of the router that will send the redirected traffic to the FX Series in a GRE tunnel. If this field is not set, then the Remote GRE tunnel address is assumed to be the same as the router address. This field is not needed if L2 redirection is specified.
- **Local GRE tunnel address:** This is the IP address of the local end of the GRE tunnel.

WCCP v2 Settings

- **Redirect method:** This specifies the method in which the router or switch will direct packets to the FX Series appliance. 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 acceleration appliance. The default is “GRE”.
- **Return method:** Although the FX Series appliance 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 Series appliance to direct the packets. In general, this should be set to “Mask” for switches and “Hash” for routers. 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.
- **Use dynamic service groups:** If “Enabled”, then the FX Series appliance will attempt to join the service group depicted in the “Service group number” field, otherwise it will attempt to join service group 0 (web-cache). The default is “Disabled”.
- **Service group number:** This is the WCCP service group that the FX Series appliance should join to receive redirected client requests that otherwise would have been sent out from the router to the content server. Server groups are defined at the router. The default value is 99.
- **Ports:** Defines the TCP ports that the router should transparently redirect to the FX Series appliance. Up to 8 ports may be specified separated by a comma. Each port value must have a corresponding “Port Definition” defined in the “Configuration->Port Definitions” page. The default value is 80.

- **Use extra service group for IP spoofing:** This must be "Enabled" if you want the FX Series appliance to preserve the source IP address of the remote clients when making requests to content servers on behalf of those clients. If this is set you must also enable "Preserve client IP addresses" in the "Other" section on the "Configure->Settings->Networking" page. See more detailed description titled "WCCP IP Spoofing Configuration" below. The default value is "Disabled".
- **Server-facing service group:** This is the WCCP service group that the FX Series appliance should join to receive redirected responses from the content server that otherwise would have been sent out from the router to the users. The default value is 99.

Configure Independent WCCP Dialogs with 'N' Number of Cisco Routers

The GUI allows service providers to define the WCCP configuration on a flexible record oriented basis using FX Series WCCP policies. These policies allow the FX Series to communicate with "n" number of routers independently, and supports protocols other than HTTP. This enables the administrator to redirect traffic to the FX Series on other ports such as FTP, CIFS, MAPI, POP3, SMTP, etc. With the FX Series record configurations, service providers can configure it to communicate with multiple routers, each with independent WCCP dialogs.

WCCP Definitions

On the "Configuration->Settings->Networking" page of the FX Series, individual interfaces to a router or switch may be defined and edited from a list-box. For the most part, the fields are the same as described in the "Web Cache Coordination Protocol" section above with the following exceptions:

- The "Enablement" field allows an individual WCCP definition to be "Enabled" or "Disabled".
- A "Comment" field provides a place to store a description of the definition.

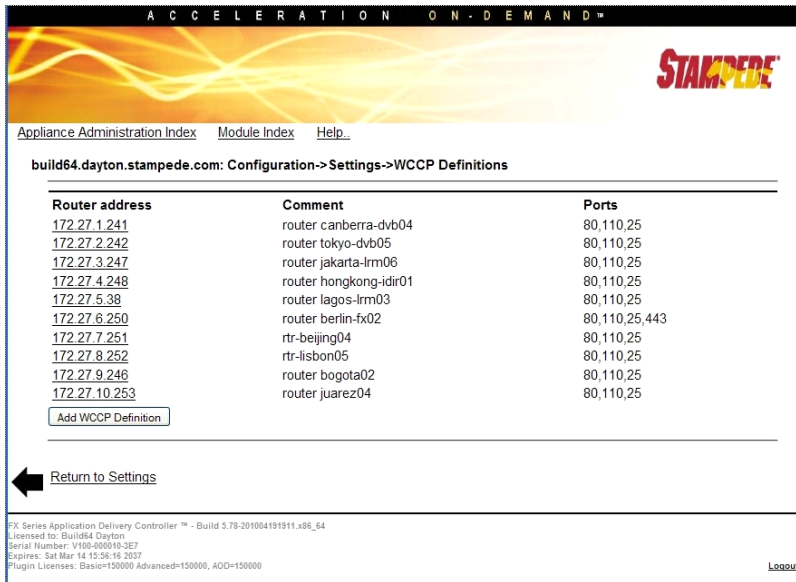
Deploying the FX Series with WCCP IP Spoofing Configuration for Routers

The FX Series appliance 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 group is referred to as the "Server-facing" service group, and it receives the redirected server responses. If two or more FX Series appliances have joined these service groups 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 Series appliance that originated the request on behalf of the remote user.

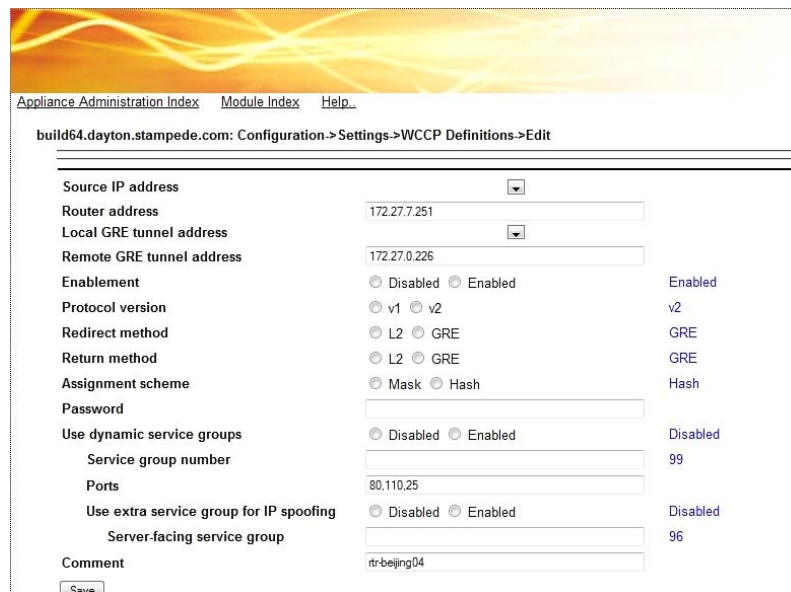
FX Series with WCCP IP Spoofing Configuration for Switches

Switches tend to have less CPU power than a router; 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 optimization appliance, use "L2" Redirection method
- On the optimization appliance, use "Mask" assignment scheme
- On the switch, use "redirect in" to direct packet flow to the appliance. (Never use "redirect-out")
- On the switch, do not use "redirect exclude in"



This screen is used for editing existing, or adding new WCCP definitions.



This screen is the form for WCCP definitions.

Summary

The FX Series provides a wide array of configuration techniques and acceleration technologies to help administrators control how their satellite links are utilized. A variety of tools are at your disposal to help you understand how applications are performing over satellite links.

- Managing connections between users and servers provides business agility, ensuring transactions are completed and users receive the best quality of service.
- Managing virtual, persistent connections, the FX Series mitigates against sessions that are interrupted, and enables the end-user to continue their session without loss of data or interruption.

- Supporting WCCP environments allows IT departments to easily scale network operations, provide fault tolerance, and enable service-assurance (failsafe) mechanisms. Load balancing via WCCP intelligently distributes the TCP and HTTP workload across multiple FX Series appliances.

Administrator-defined policies can be created to help you achieve the full potential that your satellite network can deliver, while supporting your business requirements. With its diverse set of configuration capabilities, the FX Series delivers industry-leading Total Cost of Ownership (TCO) for satellite link optimization.