IronWare Software Release R07.0.01b for Brocade FESX, FSX, SX, FCX, FGS, FGS-STK, FLS, FLS-STK, and FWS Switches

Release Notes v1.0

March 22, 2010

Document History

Document Title	Summary of Changes	Publication Date
IronWare Software Release 07.0.01b for Brocade FESX, FSX, SX, FCX, FGS, FGS-STK, FLS, FLS-STK, and FWS Switches Release Notes v1.0	New document	March 2010

Contents

Supported devices

This software release applies to the following Brocade FastIron switches:

- FastIron X Series:
  - FastIron Edge Switch X Series (FESX)
  - FastIron Edge Switch X Series Expanded (FESXE)
  - FastIron SuperX Switch (FSX)
  - FastIron SX 800, 1600, and 1600-ANR
- FastIron GS (FGS) and FastIron LS (FLS)
- FastIron GS-STK (FGS-STK) and FastIron LS-STK (FLS-STK)
- FastIron CX (FCX)
- FastIron WS (FWS)

Summary of enhancements in IronWare release R07.0.01b

This section lists the enhancements in software release 07.0.01b.

Summary of enhancements in FSX R07.0.01b

Table 1 lists the enhancements in software release 07.0.01b for FESX, FSX, and SX devices.

Table 1 Enhancements in FSX R07.0.01b

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
802.1p priority bit inspection in the ACL for adaptive rate limiting	Configures the Brocade device to rate limit traffic for a specified 802.1p priority value.	Inspecting the 802.1p bit in the ACL for adaptive rate limiting
Port priority override of incoming 802.1p bit	Configures a port to ignore an incoming packet's 802.1p priority for traffic classification.	802.1p priority override
Option to disable DHCP client learning on a port	You can disable the learning of DHCP clients on an individual port.	Disabling the learning of DHCP clients on a port

Summary of enhancements in FCX R07.0.01b

Table 2 lists the enhancements in software release 07.0.01b for FCX devices.

Table 2 Enhancements in FCX R07.0.01b

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
Option to disable DHCP client learning on a port	You can disable the learning of DHCP clients on an individual port.	Disabling the learning of DHCP clients on a port

Summary of enhancements in FGS R07.0.01b

Table 3 lists the enhancements in software release 07.0.01b for FGS, FGS-STK, FLS, FLS-STK, and FWS devices.

Table 3 Enhancements in FGS R07.0.01b

Feature	Description	See the *FastIron Configuration Guide*, section entitled...
Option to disable DHCP client learning on a port	You can disable the learning of DHCP clients on an individual port.	Disabling the learning of DHCP clients on a port

CLI differences in IronWare release R07.0.01b

The *FastIron Configuration Guide* and the section Configuration notes and feature limitations in these release notes describe the CLI differences in IronWare release 07.0.01b compared with earlier releases. No CLI commands have been deprecated for this release.

Configuration notes and feature limitations

This section contains configuration notes and describes some feature limitations in this release.

DHCP server support on FGS, FLS, and FWS devices

The CLI command **ip dhcp-server** is not present in software release 07.0.01b. Therefore, for FGS, FLS, and FWS devices running software release 04.3.03, if you upgrade to release 07.0.01b, the DHCP server feature will not be available and connected devices dependent on this feature for DHCP will no longer be offered an IP address. The DHCP server feature is targeted for a subsequent release.

ACL Statistics on FGS, FLS, and FWS devices

The FGS, FLS, and FWS do not support the use of traffic policies for ACL statistics only (CLI command **traffic-policy** <*TPD name*> **count**). However, these models do support the use of traffic policies for ACL statistics together with rate limiting traffic policies. For more information, refer to "Enabling ACL statistics with rate limiting traffic policies" in the *FastIron Configuration Guide*.

INM support on FGS, FLS, and FWS devices

IronView Network Manager (INM) release 03.2.00a is not able to discover ports on FGS, FLS, and FWS devices. INM support for these devices is targeted for a subsequent release.

VLAN-based mirroring on FWS devices

VLAN-based mirroring is not supported in software release 07.0.01b for FWS devices. If you upgrade from software release 04.3.03 to release 07.0.01b, VLAN-based mirroring will be removed from the configuration.

Dynamic buffer allocation for an IronStack

The CLI command **qd-descriptor** <*stack-unit*> <*x*> <*y*>, which is used to configure port descriptors for buffer allocation, is not supported in software release 07.0.01b. If you upgrade to release 07.0.01b, qd-descriptor will be removed from the configuration.

IGMP Snooping feature limitation on FESX, FSX, and SX devices

High CPU utilization will occur when IGMP Snooping and PIM/DVMRP routing are enabled simultaneously on a FESX, FSX, or SX router. With IGMP Snooping and PIM/DVMRP Routing enabled simultaneously on a given system, IP Multicast data packets received in the snooping VLAN(s) will be forwarded to client ports via the hardware; however, copies of these packets will also be received and dropped by the CPU.

Show interface brief command output

If a port name is longer than 5 characters, the port name will be truncated in the output of the **show interface brief** command.

ICMP redirect messages

In software release 07.0.01b, ICMP redirect messages are *disabled* by default, whereas in prior releases, ICMP redirect messages are *enabled* by default.

- IF ICMP redirect messages were enabled prior to upgrading to release 07.0.01b, you will need to re-enable this feature after upgrading to 07.0.01b. To do so, enter the **ip icmp redirect** command at the global CONFIG level of the CLI.
- If ICMP redirect messages were disabled prior to upgrading to release 07.0.01b, the configuration (**no ip icmp redirect)** will be removed from the configuration file after upgrading to 07.0.01b, since this feature is now disabled by default. In this case, ICMP redirect messages will not be sent and no further action is required.

Note regarding Telnet and Internet Explorer 7

The Telnet function in Web management does not work with Internet Explorer version 7.0.5730. The system goes to "telnet://10.43.43.145" page when the user clicks web/general system configuration/ (telnet) in Internet Explorer version 7.0.5730. This is a known issue for Internet Explorer. To work around this issue, you must download and install a patch for IE 7. To do so, go to http://www.lib.ttu.edu.tw/file/IE7_telnet.reg.

Feature support

These release notes include a list of supported features in IronWare software for the FastIron devices supported in this release. For more information about supported features, refer to the manuals listed in Additional resources.

Supported management features

Table 4 lists the supported management features. These features are supported in the Layer 2, base Layer 3, edge Layer 3, and full Layer 3 software images.

Table 4 Supported management features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
802.1X accounting	Yes	Yes	Yes	Yes	Yes
AAA support for console commands	Yes	No	No	No	Yes
Access Control Lists (ACLs) for controlling management access	Yes	Yes	Yes	Yes	Yes
Alias command	Yes	Yes	Yes	Yes	Yes
Combined DSCP and internal marking in one ACL rule	Yes	No	No	No	No
Single source address for the following packet types:	Yes	No	No	No	No

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
• Telnet • TFTP • Syslog • SNTP • TACACS/TACACS+ • RADIUS • SSH • SNMP					
DHCP client-based auto-configuration	No	Yes	Yes	Yes	Yes
Disabling TFTP access	Yes	No	No	No	Yes
IronView Network Manager (optional standalone and HP OpenView GUI)	Yes	Yes	Yes	Yes	Yes
Remote monitoring (RMON)	Yes	Yes	Yes	Yes	Yes
Retaining Syslog messages after a soft reboot	Yes	No	No	No	No
sFlow support for IPv6 packets	Yes	Yes	Yes	Yes	Yes
sFlow version 2	Yes	Yes	Yes	Yes	Yes
sFlow version 5 (default)	Yes	Yes	Yes	Yes	Yes
Industry-standard Command Line Interface (CLI), including support for: • Serial and Telnet access • Alias command • On-line help • Command completion • Scroll control • Line editing • Searching and filtering output • Special characters	Yes	Yes	Yes	Yes	Yes
Show log on all terminals	Yes	Yes	Yes	Yes	Yes
SNMP v1, v2, v3	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
SNMP V3 traps	Yes	Yes	Yes	Yes	Yes
Specifying the maximum number of entries allowed in the RMON Control Table	Yes	No	No	No	Yes
Specifying which IP address will be included in a DHCP/BOOTP reply packet	Yes	No	No	No	Yes
Traffic counters for outbound traffic	Yes	No	No	No	No
Web-based GUI	Yes	Yes	Yes	Yes	Yes
Web-based management HTTPS/SSL	Yes	Yes	Yes	Yes	Yes

Supported security features

Table 5 lists the supported security features. These features are supported in the Layer 2, base Layer 3, edge Layer 3, and full Layer 3 software images.

Table 5 Supported security features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
802.1X port security	Yes	Yes	Yes	Yes	Yes
802.1X authentication RADIUS timeout action	Yes	Yes	Yes	Yes	Yes
802.1X dynamic assignment for ACL, MAC filter, and VLAN	Yes	Yes	Yes	Yes	Yes
Access Control Lists (ACLs) for filtering transit traffic • Support for inbound ACLs only. Outbound ACLs are not supported.	Yes	Yes	Yes	Yes	Yes
Address locking (for MAC addresses)	Yes	Yes	Yes	Yes	Yes
AES Encryption for SNMP v3	Yes	Yes	Yes	Yes	Yes
AES Encryption for SSH v2	Yes	Yes	Yes	Yes	Yes
Authentication, Authorization and Accounting (AAA): • RADIUS • TACACS/TACACS+	Yes	Yes	Yes	Yes	Yes
Denial of Service (DoS) attack protection: • Smurf (ICMP) attacks • TCP SYN attacks	Yes	Yes	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes	Yes	Yes
Dynamic ARP Inspection	Yes	Yes	Yes	Yes	Yes
EAP Pass-through Support	Yes	Yes	Yes	Yes	Yes
HTTPS	Yes	Yes	Yes	Yes	Yes
IP Source Guard	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Local passwords	Yes	Yes	Yes	Yes	Yes
MAC address filter override of 802.1X	Yes	Yes	Yes	Yes	Yes
MAC address filtering (filtering on source and destination MAC addresses)	Yes	Yes	Yes	Yes	Yes
Ability to disable MAC learning	Yes	Yes	Yes	Yes	Yes
Flow-based MAC address learning	Yes	No	No	No	Yes
MAC port security	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication	Yes	Yes	Yes	Yes	Yes
Support for Multi-Device Port Authentication together with:					
• Dynamic VLAN assignment	Yes	Yes	Yes	Yes	Yes
• Dynamic ACLs	Yes	Yes	Yes	Yes	Yes
• 802.1X	Yes	Yes	Yes	Yes	Yes
• Dynamic ARP inspection with dynamic ACLs	Yes	No	No	No	No
• DHCP snooping with dynamic ACLs	Yes	No	No	No	No
• Denial of Service (DoS) attack protection	Yes	No	No	No	Yes
• Source guard protection	Yes	Yes	Yes	Yes	Yes
• ACL-per-port-per-VLAN	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication password override	Yes	Yes	Yes	Yes	Yes
Multi-device port authentication RADIUS timeout action	Yes	Yes	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes	Yes	Yes
Secure Shell (SSH) v2	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Packet filtering on TCP Flags	No	Yes	Yes	Yes	Yes
DHCP Relay Agent information (DHCP Option 82)	Yes	Yes	Yes	Yes	Yes
Web Authentication	Yes	Yes	Yes	Yes	Yes

Supported system-level features

Table 6 lists the supported system-level features. These features are supported in the Layer 2, base Layer 3, edge Layer 3, and full Layer 3 software images.

Table 6 Supported system-level features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
10/100/1000 port speed	Yes	Yes	Yes	Yes	Yes
16,000 MAC addresses per switch (FastIron devices)	Yes	Yes	Yes	Yes	Yes
32,000 MAC addresses per switch	Yes	No	No	No	Yes
ACL-based mirroring	Yes	Yes	Yes	Yes	Yes
ACL-based fixed rate limiting	Yes	Yes	Yes	Yes	Yes
ACL-based adaptive rate limiting	Yes	No	No	No	Yes
ACL filtering based on VLAN membership or VE port membership	Yes	Yes	Yes	Yes	Yes
ACL logging of denied packets (IPv4)	Yes	Yes	Yes	Yes	Yes
ACL statistics	Yes	Yes	Yes	Yes	Yes
ACLs to filter ARP packets	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Asymmetric flow control: • Responds to flow control packets, but does not generate them	Yes	Yes	Yes	Yes	No
Auto MDI/MDIX detection	Yes	Yes	Yes	Yes	Yes
Auto-negotiation	Yes	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for 802.1X ports	Yes	Yes	Yes	Yes	Yes
Automatic removal of Dynamic VLAN for MAC authenticated ports	Yes	No	No	No	No
Byte-based broadcast, multicast, and unknown-unicast rate limits	Yes	No	No	No	No
Packet-based broadcast, multicast, and unknown-unicast rate limits	Yes	Yes	Yes	Yes	Yes
DiffServ support	Yes	Yes	Yes	Yes	Yes
Digital Optical Monitoring	Yes	Yes	Yes	Yes	Yes
Displaying interface names in Syslog messages	Yes	Yes	Yes	Yes	Yes
Displaying TCP and UDP port numbers in Syslog messages	Yes	Yes	Yes	Yes	Yes
Dynamic buffer allocation for QoS priorities	Yes	Yes	Yes	Yes	Yes
Inbound rate limiting (port-based fixed rate limiting on inbound ports)	Yes	Yes	Yes	Yes	Yes
Foundry Discovery Protocol (FDP) / Cisco Discovery Protocol (CDP)	Yes	Yes	Yes	Yes	Yes
Generic buffer profile	No	Yes	Yes	Yes	Yes
High Availability (support for Layer 2 hitless switchover) For details, refer to the *Brocade FastIron X Series Chassis Hardware Installation Guide*	Yes FSX 800 and FSX 1600 only	No	No	No	No

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
LLDP	Yes	Yes	Yes	Yes	Yes
LLDP-MED	Yes	Yes	Yes	Yes	Yes
MAC address filter-based mirroring	No	Yes	Yes	Yes	Yes
Multi-port static MAC address	Yes	Yes	Yes	Yes	Yes
Multiple Syslog server logging (up to six Syslog servers)	Yes	Yes	Yes	Yes	Yes
Outbound rate limiting (port-based and port- and priority-based rate limiting on outbound ports)	No	Yes	Yes	Yes	No
Outbound rate shaping	Yes	No	No	No	Yes
Path MTU Discovery	Yes	No	No	No	Yes
Port flap dampening	Yes	Yes	Yes	Yes	Yes
Port mirroring and monitoring (mirroring of both inbound and outbound traffic on individual ports)	Yes	Yes	Yes	Yes	Yes
Power over Ethernet (POE)	Yes (POE-enabled Interface modules with POE power supply)	Yes (FGS-POE only)	Yes (FGS-POE-STK only)	Yes (FWS-POE and FWS-G-POE only)	Yes (FCX-S-HPOE only)
Priority mapping using ACLs	Yes	Yes	Yes	Yes	Yes
Protected link groups	Yes	Yes	Yes	Yes	Yes
System time using a Simple Network Time Protocol (SNTP) server or local system counter	Yes	Yes	Yes	Yes	Yes
Static MAC entries with option to set traffic priority	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Virtual Cable Testing (VCT) technology	Yes	Yes	Yes	Yes	Yes

Supported Layer 2 features

Layer 2 software images include all of the management, security, and system-level features listed in the previous tables, plus the features listed in Table 7.

Table 7 Supported Layer 2 features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
802.1D Spanning Tree Support: • Enhanced IronSpan support includes Fast Port Span, Fast Uplink Span, and Single-instance Span • Up to 254 spanning tree instances for VLANs	Yes	Yes	Yes	Yes	Yes
802.1p Quality of Service (QoS): • Strict Priority (SP) • Weighted Round Robin (WRR) • Combined SP and WRR • 8 priority queues	Yes	Yes	Yes	Yes	Yes
802.1s Multiple Spanning Tree	Yes	Yes	Yes	Yes	Yes
802.1W Rapid Spanning Tree (RSTP)	Yes	Yes	Yes	Yes	Yes
802.3ad link aggregation (dynamic trunk groups)	Yes	Yes	Yes	Yes	Yes
ACL-based rate limiting QoS	Yes	Yes	Yes	Yes	Yes
BPDU Guard	Yes	Yes	Yes	Yes	Yes
Dynamic Host Configuration Protocol (DHCP) Assist	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
IGMP v1/v2 Snooping Global	Yes	Yes	Yes	Yes	Yes
IGMP v3 Snooping Global	Yes (*,G)	Yes (S,G)	Yes (S,G)	Yes (S,G)	Yes (S,G)
IGMP v1/v2/v3 Snooping per VLAN	Yes	Yes	Yes	Yes	Yes
IGMP v2/v3 Fast Leave (membership tracking)	Yes	Yes	Yes	Yes	Yes
Interpacket Gap (IPG) adjustment	Yes	Yes	Yes	Yes	Yes
Jumbo frames: • Up to 10240 bytes, or • Up to 10232 bytes in an IronStack	Yes	Yes	Yes	Yes	Yes
Ling Aggregation Control Protocol (LACP)	Yes	Yes	Yes	Yes	Yes
Link Fault Signaling (LFS) for 10G	Yes	Yes	Yes	Yes	Yes
MAC-Based VLANs, including support for dynamic MAC-Based VLAN activation	No	Yes	Yes	Yes	Yes
Metro Ring Protocol 1 (MRP 1)	Yes	Yes	Yes	Yes	Yes
Metro Ring Protocol 2 (MRP 2)	Yes	Yes	No	Yes	Yes
Extended MRP ring IDs from 1 – 1023	Yes	No	No	No	Yes
MLD Snooping V1/V2: • MLD V1/V2 snooping (global and local) • MLD fast leave for V1 • MLD tracking and fast leave for V2 • Static MLD and IGMP groups with support for proxy	Yes	Yes	Yes	Yes	Yes
Multicast static group traffic filtering (for snooping scenarios)	No	Yes	Yes	Yes	Yes
PIM-SM V2 Snooping	Yes	No	No	No	Yes
PVST/PVST+ compatibility	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
PVRST+ compatibility	Yes	Yes	Yes	Yes	Yes
Remote Fault Notification (RFN) for 1 G fiber	Yes	Yes	Yes	Yes	Yes
Root Guard	Yes	Yes	Yes	Yes	Yes
Single link LACP	Yes	Yes	Yes	Yes	Yes
Super Aggregated VLANs	Yes	Yes	Yes	Yes	Yes
Trunk groups: • Trunk threshold for static trunk groups • Flexible trunk group membership • Option to include Layer 2 in trunk hash calculation (FGS, FLS, FWS only)	Yes	Yes	Yes	Yes	Yes
Topology groups	Yes	Yes	Yes	Yes	Yes
Uni-directional Link Detection (UDLD) (Link keepalive)	Yes	Yes	Yes	Yes	Yes
Uplink Ports within a Port-Based VLAN	Yes	Yes	Yes	Yes	Yes
VLAN-based mirroring	No	Yes	Yes	Yes	Yes
VLAN Support: • 4096 maximum VLANs • 802.1Q with tagging • 802.1Q-in-Q tagging • Dual-mode VLANs • GVRP • Port-based VLANs • Protocol VLANs (AppleTalk, IPv4, dynamic IPv6, and IPX • Layer 3 Subnet VLANs (Appletalk, IP subnet network, and IPX) • VLAN groups • Private VLANs	Yes	Yes	Yes	Yes	Yes
VLAN-based mirroring	No	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
VoIP Autoconfiguration and CDP	Yes	Yes	Yes	Yes	Yes
Virtual Switch Redundancy Protocol (VSRP)	Yes	Yes	Yes	Yes	Yes
VSRP-Aware security features	Yes	Yes	Yes	Yes	Yes
VSRP and MRP signaling	Yes	Yes	Yes	Yes	Yes
VSRP Fast Start	Yes	Yes	Yes	Yes	Yes
VSRP timer scaling	Yes	Yes	Yes	Yes	Yes

Supported base Layer 3 features

Base Layer 3 software images include all of the management, security, system, and Layer 2 features listed in the previous tables, plus the features listed in Table 8.

NOTE: FCX devices will not contain a base Layer 3 image. The features in this table will be supported on the full Layer 3 image for these devices.

Table 8 Supported base Layer 3 features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
BootP/DHCP Relay	Yes	Yes	Yes	Yes	Yes
Equal Cost Multi Path (ECMP) load sharing	Yes	Yes	Yes	Yes	Yes
IP helper	Yes	Yes	Yes	Yes	Yes
IPv4 point-to-point GRE IP tunnels	Yes (IPv6 devices only)	No	No	No	No
RIP V1 and V2 (advertising only)	Yes	Yes	Yes	Yes	Yes
Routing for directly connected IP subnets	Yes	Yes	Yes	Yes	Yes

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Static IP routing	Yes	Yes	Yes	Yes	Yes
Virtual Interfaces (up to 255)	Yes	Yes	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP)	Yes	Yes	Yes	Yes	Yes
VRRP timer scaling	Yes	Yes	Yes	Yes	Yes

Supported edge Layer 3 features

Edge Layer 3 software images include all of the management, security, system, Layer 2, and base Layer 3 features listed in the previous tables, plus the features shown in Table 9.

NOTE: Edge Layer 3 images are supported in the FastIron devices listed in Table 9.

Table 9 Supported edge Layer 3 features

Category and description	FGS-EPREM FLS-EPREM FWS-EPREM FWSG-EPREM
OSPF V2 (IPv4)	Yes
Full RIP V1 and V2	Yes
Route-only support (Global configuration level only)	Yes
Route redistribution	Yes
1020 routes in hardware maximum	Yes
VRRP-E	Yes

Supported full Layer 3 features

Full Layer 3 software images include all of the management, security, system, Layer 2, base Layer 3 and edge Layer 3 features listed in the previous tables, plus the features listed in Table 10 .

NOTE: Full Layer 3 features are supported on FastIron X Series –PREM devices and on FastIron CX Series devices.

Table 10 Supported full Layer 3 features

Category and description	FESX-PREM FSX-PREM FSX 800-PREM FSX 1600-PREM	FCX
Active host routes	Yes (6,000)	Yes (16,000)
Anycast RP	Yes	No
BGP4	Yes	Yes (ADV models)
Distance Vector Multicast Routing Protocol (DVMRP) V2 (RFC 1075)	Yes	No
Internet Group Management Protocol (IGMP) V1, V2, and V3 (for multicast routing scenarios)	Yes	Yes
ICMP Redirect messages	Yes	Yes
IGMP V3 fast leave (for routing)	Yes	Yes
IPv6 Layer 3 forwarding[1]	Yes	No
IPv6 over IPv4 tunnels in hardware[1]	Yes	No
IPv6 Redistribution[1]	Yes	No
IPv6 Static Routes[1]	Yes	No
Multiprotocol Source Discovery Protocol (MSDP)	Yes	No
OSPF V3 (IPv6)[1]	Yes	No

[1] This feature is enabled by the IPv6 PROM (IPv6 full layer 3 image) and requires IPv6-series hardware.

Category and description	FESX-PREM FSX-PREM FSX 800-PREM FSX 1600-PREM	FCX
Protocol Independent Multicast Dense mode (PIM-DM) V1 (draft-ietf-pim-dm-05) and V2 (draft-ietf-pim-v2-dm-03)	Yes	Yes
Protocol Independent Multicast Sparse mode (PIM-SM) V2 (RFC 2362)	Yes	Yes
PIM passive	Yes	Yes
Policy-Based Routing (PBR)	Yes	Yes
RIPng (IPv6)[1]	Yes	No
Route-only support (Global CONFIG level and Interface level)	Yes	Yes
Route redistribution (including BGP4)	Yes	Yes (BGP4 supported on ADV models only)
Routes in hardware maximum: • FESX4 – up to 128K routes • FESX6 – up to 256K routes • FESX6-E – up to 512K routes • FSX – up to 256K routes • FCX – up to 16K routes	Yes	Yes
Static ARP entries	Yes (up to 6,000)	Yes (up to 1,000)
VRRP-E	Yes	Yes
VRRP-E slow start timer	Yes	Yes
VRRP-E timer scale	Yes	Yes

Supported IPv6 management features

Table 11 shows the IPV6 management features that are supported in Brocade devices that can be configured as an IPv6 host in an IPv6 network, and in devices that support IPv6 routing.

Table 11 Supported IPv6 management features

Category and description	FESX FSX FSX 800 FSX 1600	FGS FLS	FGS-STK FLS-STK	FWS	FCX
Link-Local IPv6 Address	Yes	Yes	Yes	Yes	Yes
IPv6 Access List (management ACLs)	Yes	Yes	Yes	Yes	Yes
IPv6 copy	Yes	Yes	Yes	Yes	Yes
IPv6 ncopy	Yes	Yes	Yes	Yes	Yes
IPv6 debug	Yes	Yes	Yes	Yes	Yes
IPv6 ping	Yes	Yes	Yes	Yes	Yes
IPv6 traceroute	Yes	Yes	Yes	Yes	Yes
DNS server name resolution	Yes	Yes	Yes	Yes	Yes
HTTP/HTTPS	Yes	Yes	Yes	Yes	Yes
Logging (Syslog)	Yes	Yes	Yes	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes	Yes
SCP	Yes	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes	Yes
SNMP	Yes	Yes	Yes	Yes	Yes
SNMP traps	Yes	Yes	Yes	Yes	Yes
SNTP	Yes	Yes	Yes	Yes	Yes
TACACS/TACACS+	Yes	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes
TFTP	Yes	Yes	Yes	Yes	Yes

Unsupported features

Table 12 lists the features that are not supported on the FastIron devices. If required, these features are available on other Brocade devices.

Table 12 Unsupported features

System-level features not supported
• ACL logging of permitted packets.
• Broadcast and multicast MAC filters
• Outbound ACLs
Layer 2 features not supported
• SuperSpan
• VLAN-based priority
Layer 3 features not supported
• AppleTalk routing
• BGP4+
• Foundry Standby Router Protocol (FSRP)
• IPv6 Multicast Routing
• IPX routing
• IS-IS
• Multiprotocol Border Gateway Protocol (MBGP)
• Multiprotocol Label Switching (MPLS)
• Network Address Translation (NAT)

Software image files for IronWare release R07.0.01b

Table 13 lists the software image files that are available for IronWare Release 07.0.01b.

Table 13 Software image files

Device	Boot Image	Flash Image
FESX FSX FSX 800 FSX 1600	SXZ05000.bin	SXS07001b.bin (Layer 2) or SXL07001b.bin (base Layer 3) or SXR07001b.bin (full Layer 3)
FGS FLS FWS	FGZ05000.bin	FGS07001b.bin (Layer 2) or FGSL07001b.bin (base Layer 3) or FGSR07001b.bin (edge Layer 3)
FGS-STK FLS-STK	FGZ05000.bin	FGS07001b.bin (Layer 2) or FGSL07001b.bin (base Layer 3)
FCX	GRZ07001.bin	FCXS07001b.bin (Layer 2) or FCXR07001b.bin (Layer 3)

Factory pre-loaded software

Table 14 lists the software that is factory-loaded into the primary and secondary flash areas on the device.

Table 14 Factory pre-loaded software

Model	Software Images	
	Primary Flash	Secondary Flash
FESX FSX FSX 800 FSX 1600	Layer 2	Base Layer 3
FESX PREM FSX PREM FSX 800 PREM FSX 1600 PREM	Full Layer 3	Layer 2

Model	Software Images	
	Primary Flash	Secondary Flash
FGS FGS-STK FLS FLS-STK FWS	Layer 2	Base Layer 3
FGS EPREM FLS EPREM FWS EPREM	Edge Layer 3	Layer 2
FCX	Layer 2	Layer 3

Upgrading the software

Use the procedures in this section to upgrade the software.

Important notes about upgrading or downgrading the software

NOTE: For other important notes that may apply when upgrading or downgrading the software, refer to Configuration notes and feature limitations on page 7.

Note the following when upgrading to software release 07.0.01b:

- To upgrade an FWS device running software version 04.3.00 to version 07.0.01b, you must first upgrade to release 04.3.02 before upgrading to 07.0.01b. For instructions on how to upgrade to release 04.3.02, see the 04.3.02 release notes.
- If FGS-STK or FLS-STK devices are upgraded from software release 04.3.00 non-stacking mode to release 07.0.01b stacking mode, these devices may lose some port-related functions. If you are upgrading from a pre-stacking release to a stacking release, refer to "Converting from a pre-stacking image to a stacking image" in the *FastIron Configuration Guide*.

Note the following when downgrading from software release 07.0.01b:

- FCX-F devices require software release 06.1.00 or later.
- If FCX units In an IronStack are downgraded from software release 07.0.01b to release 06.0.00, in some instances, the units may not be able to form a stack. This will occur if there is a mismatch of BGP capability within the stack (i.e., some units support it and others do not). If you encounter this problem, contact Brocade Technical Support for assistance.
- If FGS-STK or FLS-STK units in an IronStack are downgraded from software release 07.0.01b to release 04.3.00, these units may lose some port-related functions since 04.3.00 does not support stacking. The same issue applies when FGS or FLS (standalone) devices that use stack-unit ID 2 or

greater are downgraded from release 07.0.01b to 04.3.00. This will occur because the default non-stacked port numbering scheme in release 4.3.00 and earlier is **0**/*x*/*x*, versus the new non-stacked port numbering scheme in 7.0 which is **1**/*x*/*x*. After downgrading from release 7.0.01b to 4.3.00 or earlier, all configuration items relating to port numbers will be invalid and will need to be reprogrammed in the switch.

Upgrading the software to the new release

This section describes how to upgrade the software to run release 07.0.01b.

Upgrading the boot code

To upgrade the boot code, perform the following steps.

1. Place the new boot code on a TFTP server to which the Brocade device has access.
2. Copy the boot code from the TFTP server into flash memory. To do so, enter a command such as the following at the Privileged EXEC level of the CLI.

   ```
   FastIron# copy tftp flash 10.100.105.1 GRZ07001.bin bootrom
   ```

   You should see output similar to the following.

   ```
   FastIron# Flash Memory Write (8192 bytes per
   dot).........................
   (Boot Flash Update)Erase.........Write.............
   TFTP to Flash Done
   ```

   Syntax: copy tftp flash <ip-addr> <image-file-name> **bootrom**

   NOTE: Brocade recommends that you use the **copy tftp flash** command to copy the boot code to the device during a maintenance window. Attempting to do so during normal networking operations may cause disruption to the network.

3. Verify that the code has been successfully copied by entering the **show flash** command at any level of the CLI.

   ```
   FastIron# show flash
   Compressed Pri Code size = 3096603, Version 06.0.00 (FCXS06000.bin)
   Compressed Sec Code size = 2873963, Version 06.0.00 (FCXR06000.bin)
   Compressed BootROM Code size = 416315, Version 07.0.01T7e5
   Code Flash Free Space = 196608
   ```

4. Upgrade the flash code as instructed in the following section.

Upgrading the flash code

To upgrade the flash code, perform the following steps.

1. Place the new flash code on a TFTP server to which the Brocade device has access.
2. Copy the flash code from the TFTP server into flash memory. To do so, enter a command such as the following at the Privileged EXEC level of the CLI.

```
FastIron# copy tftp flash 10.100.105.1 FCXS07001b.bin primary
```

You should see output similar to the following.

```
FastIron# Flash Memory Write (8192 bytes per dot)
.......................
.....................................................................
.....................................................................
.....
TFTP to Flash Done
```

Syntax: copy tftp flash <*ip-addr*> <*image-file-name*> **primary | secondary**

3. Verify that the flash code has been successfully copied by entering the show flash command at any level of the CLI.

```
FastIron# show flash
Compressed Pri Code size = 3096603, Version 07.0.01b (FCXS07001b.bin)
Compressed Sec Code size = 2873963, Version 06.0.00 (FCXR06000.bin)
Compressed BootROM Code size = 416315, Version 07.0.01T7e5
Code Flash Free Space = 196608
```

If the flash code version is correct, go to step 4, otherwise, go back to step 1.

4. Once you have completed the upgrade, you must reboot the device to complete the upgrade process. Use one of the following commands:

- **reload** (this command boots from the default boot source, which is the primary flash area by default)
- **boot system flash primary** | **secondary**

A confirmation step may occur after a boot system flash primary/secondary command is entered and gives an administrator the opportunity to make last minute changes or corrections before performing a reload. The example below shows the confirmation step.

```
FastIron# boot system flash primary
Are you sure? (enter 'Y' or 'N'): y
```

5. For FGS-STK and FLS-STK devices equipped with upgraded memory DIMMs, EEPROM, or both, if you encounter a problem after reloading the software, make sure the device has the correct boot code version and the following (if applicable) are installed correctly:

- EEPROM
- Memory DIMM

NOTE: If the stacking EEPROM is missing or is not installed correctly, or if you have installed the wrong EEPROM, you will see an error message on the console. For details, see the *FastIron Configuration Guide.*

6. For devices in an IronStack, make sure all devices are running the same software image. See Confirming software versions (IronStack devices) in the next section.

Confirming software versions (IronStack devices)

All units in an IronStack must be running the same software image. To confirm this, check the software version on all devices that you want to add to your IronStack. Upgrade any units that are running older versions of the software before you build your stack.

1. Telnet, SSH, or connect to any of the console ports in the stack.
2. Enter the **show version** command. Output similar to the following is displayed.

```
FastIron# show version
Copyright (c) 1996-2010 Brocade Communications Systems, Inc.
   UNIT 1: compiled on Jan 26 2010 at 22:16:08 labeled as FGS07001b
               (2441570 bytes) from Primary fgs07001b.bin
       SW: Version 07.0.01b51T7e1
   UNIT 2: compiled on Jan 26 2010 at 22:16:08 labeled as FGS07001b
               (2441570 bytes) from Primary fgs07001b.bin
       SW: Version 07.0.01b51T7e1
   UNIT 3: compiled on Jan 26 2010 at 22:16:08 labeled as FGS07001b
               (2441570 bytes) from Primary fgs07001b.bin
       SW: Version 07.0.01b51T7e1
   UNIT 4: compiled on Jan 26 2010 at 22:16:08 labeled as FGS07001b
               (2441570 bytes) from Primary fgs07001b.bin
       SW: Version 07.0.01b51T7e1
```

NOTE: If any unit in the IronStack is running an incorrect version of the software, it will appear as non-operational. You must install the correct software version on that unit for it to operate properly in the stack. For more information, refer to "Copying the flash image to a stack unit from the Active Controller" in the *FastIron Configuration Guide*.

Technical support

Contact your switch supplier for the hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

1. General Information
   - Technical Support contract number, if applicable
   - Device model
   - Software release version
   - Error numbers and messages received
   - Detailed description of the problem, including the switch or network behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed, with the results
2. Switch Serial Number

Getting help or reporting errors

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance, or find errors in the manuals, contact Brocade using one of the following options.

Web access

Go to myBrocade.com, click the Product Documentation tab, then click on the link to the Knowledge Portal (KP) to obtain more information about a product, or to report documentation errors. To report errors, click on **Cases > Create a New Ticket**. Make sure you specify the document title in the ticket description.

Email access

Send an e-mail to IPsupport@brocade.com

Telephone access

United States: 800-752-8061 United States

International: +800-ATFIBREE (+800 28 34 27 33)

Refer to the Services & Support page on www.brocade.com for additional toll-free numbers that may be available within your country.

Areas unable to access 800 numbers: +1-408-333-6061

Additional resources

For more information about the products supported in this software release, refer to the following publications.

Document Title	Contents
FastIron Configuration Guide	Provides configuration procedures for system-level features, enterprise routing protocols, and security features.
Brocade FastIron GS and GS-STK Compact Switch Hardware Installation Guide *Brocade FastIron LS and LS-STK Compact Switch Hardware Installation Guide* *Brocade FastIron WS Hardware Installation Guide* *Brocade FastIron CX Hardware Installation Guide* *Brocade FastIron X Series Chassis Hardware Installation Guide* *Brocade FastIron Compact Switch Hardware Installation Guide (for FESX switches)*	Describes the hardware as shipped. Provides installation instructions, hardware maintenance procedures, hardware specifications, and compliance information.
IronWare MIB Reference	Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects.

Document Title	Contents
FastIron CX Web Management Interface User Guide	Describes the Graphical User Interface (GUI) and procedures for monitoring and configuring various features of the FastIron CX series switches using the GUI.

Documentation updates

The information in this section supplements the individual guides listed. This information will be incorporated in the next major release of the guides.

The following updates apply to the ***FCX Installation Guide***

- Table entitled *Table 10 Switch status for two installed power supply units*

  When two 620W power supplies are installed in a POE system that has no load or light load on the POE function, one of two power supplies may have its "DC OK" LED light red. There is no fault in the power supply or the system and the switch is functioning normally. The LED will turn to green automatically once the load is increased over the minimum load requirement. In configurations with a single power supply installed the "DC OK" LED will light green in a no-load or light-load condition.

- Section entitled *Package contents*

  In addition to the items listed in this section, FCX-S devices ship with a .5M CX-4 Stacking Cable.

The following updates apply to the ***FastIron Configuration Guide***

- Section entitled *Disabling support for POE legacy power consuming devices*

  The CLI command **no legacy-inline-power** does not require a software reload if it is entered prior to connecting the PDs. If the command is entered after the PDs are connected, the configuration must be saved (**write mem**) and the software rebooted before the change is placed into effect.

- Section entitled *Disabling password encryption*

  The CLI command **no service password-encryption** does not work if **service password-encryption** was configured earlier by default. To use this command, enter **no service password-encryption** then create a username and password.

Defects

This section lists the closed and opened defects in this release.

Customer reported defects Closed with Code

The following table lists the customer defects fixed in this release.

Defect ID: DEFECT000285199	**Technical Severity:** Medium
Summary: Display issue on FCX with "show version"	
Symptom: The "show version" output does not display the name correctly. For router code it should display FCX624SF-PREM but it is showing as FCX624SF.	
Risk of Fix: Medium	**Feature:** FCX Management Functionality
Probability: Medium	**Function:** CLI and parser
Reported In Release: FI 07.0.01	

Defect ID: DEFECT000285393	**Technical Severity:** Medium
Summary: The "show inline power" output returns the following error: "internal h/w fault".	
Symptom: Customer performed upgrade from 4302b to 7001 and started seeing this issue.	
Workaround: Use the old code 4302b (fgs04302b.bin)	
Feature: FCX Layer1 features	
Probability: High	**Function:** PoE/PoE+
Reported In Release: FI 07.0.01	**Service Request ID:** 244072

Defect ID: DEFECT000286017	**Technical Severity:** Medium
Summary: POE Ports show "underload" state on FGS648.	
Symptom: Customer connected a POE device (say class 4/anything that needs 22 watt) on POE ports on FGS. Then they disconnected that device and connected another device of lower power rating (class 3). They did it a few times and the port showed "Underload state" and the POE device did not get power.	
Workaround: Reload the box.	
Feature: FCX Layer1 features	
Probability: High	**Function:** PoE/PoE+
Reported In Release: FI 07.0.01	**Service Request ID:** 244447

Defect ID: DEFECT000287855	**Technical Severity:** High
Summary: "link-keepalive" command didn't get parsed after upgrading to 7.0.01 release.	
Symptom: The customer is reporting that the FGS's lost connectivity to the network due to link-keepalive command line change in 7.0.01. The syntax for link-keepalive has been changed from 4302 when multiple ports are enabled.	
Feature: FCX L2 Control	
Probability: High	**Function:** UDLD
Reported In Release: FI 07.0.01	**Service Request ID:** 245283

Defect ID: DEFECT000288131	**Technical Severity:** Medium
Summary: Enable password disappears upon upgrade from 4.x to 7.x code.	
Symptom: Enable password disappears upon upgrade from 4.x to 7.x code.	
Feature: SX Management Functionality	
Probability: Medium	**Function:** CLI and parser
Reported In Release: FI 07.0.01	**Service Request ID:** 244849

Defect ID: DEFECT000288256	**Technical Severity:** Medium
Summary: Password seen as clear text when exporting configuration file to TFTP server.	
Symptom: Customer exported his configuration file to the TFTP server. The exported file shows the password as clear text.	
Feature: SX Management Functionality	
Probability: Medium	**Function:** CLI and parser
Reported In Release: FI 07.0.01	**Service Request ID:** 245398

Defect ID: DEFECT000288264	**Technical Severity:** Medium
Summary: No password encryption in 7001.	
Symptom: There is no way to encrypt the "enable" password in 7001. The customer tried "service password-encryption" (which is by default) but still the password appears as clear text in the running configuration.	
Feature: SX Management Functionality	
Probability: Medium	**Function:** CLI and parser
Reported In Release: FI 07.0.01	**Service Request ID:** 245226

Defect ID: DEFECT000288276	**Technical Severity:** Medium
Summary: "no web-management hp-top-tools" commands disappear after upgrade from 5.x to 7001.	
Symptom: "no web-management hp-top-tools" commands disappear after upgrade from 5.x to 7001.	
Feature: FCX Network Management	
Probability: Medium	**Function:** Web Management
Reported In Release: FI 07.0.01	**Service Request ID:** 245197

Defect ID: DEFECT000288333	**Technical Severity:** High
Summary: POE ports gets admin disabled when upgraded from 4303 to 7001 on FGS.	
Symptom: Customer performed upgrade from 4303 to 7001 and saw that the ports which had "inline power power-limit 7500" under interface went down. Also the command disappeared in the configuration after the upgrade.	
Feature: FCX Platform Specific features	
Probability: High	**Function:** PoE/PoE+
Reported In Release: FI 07.0.01	**Service Request ID:** 245634

Defect ID: DEFECT000288848	**Technical Severity:** Critical
Summary: DHCP discover packet won't flood in VLAN when there is an IP helper address under VE.	
Symptom: When VE under VLAN has an IP helper address configured, the DHCP discover packet from one of the VLAN ports, will not flood in the VLAN member port.	
Feature: SX L2 Forwarding	
Probability: High	**Function:** DHCP assist
Reported In Release: FI 07.0.01	**Service Request ID:** 245638

Defect ID: DEFECT000289620	**Technical Severity:** High
Summary: Fan speed configuration ("fan-speed" command) is lost on upgrading to 7.0.01.	
Symptom: Fan speed configuration ("fan-speed" command) is lost on upgrading to 7.0.01.	
Risk of Fix: Medium	**Feature:** FCX Platform Specific features
Probability: High	**Function:** Chassis/fan/power supplies/temperature sensors
Reported In Release: FI 07.0.01	

Defect ID: DEFECT000290153	**Technical Severity:** High
Summary: If two VLANs have the same name, after upgrading to 7.0.01 code, only one of the VLANs is created.	
Symptom: Reloading to 7.0.01 will fail when parsing a configuration with two VLANs that have the same name and as a result that second VLAN will not get created.	
Workaround: Rename the VLAN prior to upgrade and reload.	
Feature: FCX L2 Forwarding	
Probability: Medium	**Function:** VLAN Manager
Reported In Release: FI 07.0.01	**Service Request ID:**

Defect ID: DEFECT000266691	**Technical Severity:** Medium
Summary: The "ip multicast-boundary" command does not take affect after a reload.	
Symptom: The "ip multicast-boundary" command does not take affect after a reload.	
Risk of Fix: Medium	**Probability:** Medium
Feature: SX L2/L3 Multicast Features	**Function:** PIM Dense
Reported In Release: FI 05.0.00	**Service Request ID:** 222852

Defect ID: DEFECT000266995	**Technical Severity:** Medium
Summary: With sFlow enabled, higher CPU utilization is seen in 5.1.00 code.	
Symptom: Higher CPU utilization occurs when sFlow is enabled.	
Risk of Fix: Medium	**Probability:** Medium
Feature: SX Network Management	**Function:** sFlow
Reported In Release: FI 05.1.00	**Service Request ID:** 225277

Defect ID: DEFECT000267179	**Technical Severity:** Medium
Summary: SysUptime changes at the rate of 1 or 2 seconds a day despite the presence of an SNTP server	
Symptom: When the customer checked “show version” once a day, they found that the time given for “System started at” changed by 1 or 2 seconds a day.	
Workaround: Incorrect system up time.	
Risk of Fix: Medium	**Probability:** High
Feature: SX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 05.0.00	**Service Request ID:** 231663

Defect ID: DEFECT000271032	**Technical Severity:** Medium
Summary: When there are a large number of VSRP instances, a VSRP switchover between master and standby causes a software reload.	
Symptom: Software reloads after a VSRP failover.	
Workaround: Configure a fewer number of VSRP instances.	
Risk of Fix: High	**Probability:** Medium
Feature: SX Layer 2 Control	**Function:** VSRP
Reported In Release: FI 05.1.00	**Service Request ID:** 00236191

Defect ID: DEFECT000272234	**Technical Severity:** Medium
Summary: Configured speed and duplex settings revert back to the default configuration after a reload.	
Symptom: If port speed is configured using the command "link-config gig copper autoneg-control 10/100m-auto ethe <port number>", the configuration will not take effect when the device is reloaded. This error occurs on an FWS device running release FGS04302.	
Workaround: 1. Remove the configuration line: no link-config gig copper autoneg-control 10m-auto ethe 0/1/23 2. Reapply the configuration: link-config gig copper autoneg-control 10m-auto ethe 0/1/23	
Risk of Fix: Low	**Probability:** High
Feature: SX L1 Features	**Function:** Auto-negotiation
Reported In Release: FI 04.3.00	**Service Request ID:** 237328

Defect ID: DEFECT000272761	**Technical Severity:** Medium
Summary: Entering the 'show optic' command for a module that does not exist may cause a software reload.	
Symptom: Entering the 'show optic' command for a module that does not exist may cause a software reload.	
Workaround: Not found yet	
Risk of Fix: Low	**Probability:** Medium
Feature: FCX Management Functionality	**Function:** CLI and parser

Reported In Release: FI 04.3.00	**Service Request ID:** 237736

Defect ID: DEFECT000274041	**Technical Severity:** Medium
Summary: "Invalid Port Id - 128" message seen on the console.	
Symptom: "Invalid Port Id - 128" appears when the CLI command "show run", "show tech", "conf t" or "end" is entered when a 10-G module is configured on slot 2.	
Risk of Fix: Low	**Probability:** High
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 04.3.00	**Service Request ID:** 232142

Defect ID: DEFECT000274954	**Technical Severity:** High
Summary: If an ARP entry is pointing to an invalid port, a software reload may occur when the ARP entry is cleared.	
Symptom: If an ARP entry is pointing to an invalid port, a software reload may occur when the ARP entry is cleared.	
Risk of Fix: Low	**Probability:** Medium
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 04.2.00	**Service Request ID:** 239109

Defect ID: DEFECT000274991	**Technical Severity:** Medium
Summary: DHCP snooping is not working when the interface has a permit ACL configured.	
Symptom: DHCP Snooping is not working.	
Risk of Fix: High	**Probability:** Medium
Feature: SX ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 05.1.00	**Service Request ID:** 235477

Defect ID: DEFECT000275381	**Technical Severity:** Medium
Summary: While polling 1.3.6.1.4.1.1991.1.1.1.1.2 OID we receive the serial number of the management module instead of the chassis serial number.	
Symptom: When customer polls 1.3.6.1.4.1.1991.1.1.1.1.2 OID he receives the serial number of the management module instead of the chassis serial number.	
Risk of Fix: Medium	**Probability:** High
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 05.1.00	**Service Request ID:** 00234936

Defect ID: DEFECT000275782	**Technical Severity:** Critical
Summary: A software reload may occur when VLAN configuration changes are made.	
Symptom: A software reload may occur when VLAN configuration changes are made.	
Risk of Fix: Low	**Probability:** Low
Feature: SX L2/L3 Multicast Features	**Function:** IGMP/MLD
Reported In Release: FI 05.0.00	**Service Request ID:** 238401

Defect ID: DEFECT000278036	**Technical Severity:** Medium
Summary: ECMP routing entries do not get removed when a port is down.	
Symptom: ECMP routing entries remain in the routing table even when one of the interfaces is down.	
Risk of Fix: Medium	**Probability:** High
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** ECMP
Reported In Release: FI 06.0.00	**Service Request ID:** 239486

Defect ID: DEFECT000278166	**Technical Severity:** Medium
Summary: With ECMP configured, the router may reload when an Ethernet port that learns the candidate route goes down.	
Symptom: With ECMP configured, the router may reload when an Ethernet port that learns the candidate route goes down.	
Risk of Fix: Low	**Probability:** Medium
Feature: FCX Layer3 Control Protocols	**Function:** RIP(v1-v2) - IPV4
Reported In Release: FI 06.0.00	**Service Request ID:** 238259

Defect ID: DEFECT000279505	**Technical Severity:** Critical
Summary: During an OSPF default route failover from the primary default route to the secondary default route, traffic going to the new default route gets dropped.	
Risk of Fix: Medium	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.0.00	

Defect ID: DEFECT000280058	**Technical Severity:** Medium
Summary: FGS cannot ping the DHCP server connected to the FESX after getting the IP address from the same DHCP server.	
Symptom: FGS is NOT able to download the configuration file from a TFTP server although FGS obtains IP address from DHCP server via DHCP snooping/relay FESX.	
Risk of Fix: Low	**Probability:** Medium
Feature: SX ACL	**Function:** DHCP Snooping functionality
Reported In Release: FI 05.1.00	**Service Request ID:** 239086

Defect ID: DEFECT000281011	**Technical Severity:** Medium
Summary: A software reload may occur when applying a MAC filter to a port.	
Symptom: A software reload may occur when applying a MAC filter to a port.	
Risk of Fix: High	**Probability:** Low
Feature: SX ACL	**Function:** MAC filters
Reported In Release: FI 05.1.00	**Service Request ID:** 231003

Defect ID: DEFECT000281013	**Technical Severity:** Medium
Summary: When using web authentication and HTTP desktop widgets, the "original location" link can become a URL requested by a widget.	
Symptom: When using web authentication and HTTP desktop widgets, the "original location" link can become a URL requested by a widget.	
Risk of Fix: High	**Probability:** Medium
Feature: SX Network Management	**Function:** Web Management
Reported In Release: FI 05.0.00	**Service Request ID:** 222178

Defect ID: DEFECT000281015	**Technical Severity:** Medium
Summary: The “show media” command does not display Foundry Networks in the vendor field.	
Symptom: Incomplete “show media” output	
Risk of Fix: High	**Probability:** High
Feature: SX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 05.1.00	**Service Request ID:** 239371

Defect ID: DEFECT000281017	**Technical Severity:** Medium
Summary: A software reload may occur when a packet is received with an invalid IPV4 packet header length.	
Symptom: A software reload may occur when a packet is received with an invalid IPV4 packet header length.	
Risk of Fix: Medium	**Probability:** Low
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 05.1.00	**Service Request ID:** 229830

Defect ID: DEFECT000281021	**Technical Severity:** Medium
Summary: Multicast limit command does not work on trunk ports.	
Symptom: Multicast limit command does not work on trunk ports.	
Risk of Fix: High	**Probability:** High
Feature: SX ACL	**Function:** broadcast/multicast unknown unicast Rate Limiting
Reported In Release: FI 05.1.00	**Service Request ID:** 231265

Customer reported defects Closed without Code

The following table lists the customer defects fixed in this release.

Defect ID: DEFECT000267175	**Technical Severity:** High
Summary: The "dm diag" command may miss a failure on a packet processor.	
Symptom:: The "dm diag" command may miss a failure on a packet processor.	
Reason Code: Already Fixed in Release	**Probability:** Medium
Feature: SX_SYSTEM	**Function:** SX System
Reported In Release: FI 05.0.00	**Service Request ID:** 225837

Defect ID: DEFECT000268577	**Technical Severity:** High
Summary: RSTP enters a "BROKEN" state in some VLAN after 255 RSPT instances are created.	
Symptom: RSTP enters a "BROKEN" state in some VLAN after 255 RSPT instances are created.	
Reason Code: Already Fixed in Release	**Probability:** Medium
Feature: SX L2 Control	**Function:** 802.1W
Reported In Release: FI 06.0.00	**Service Request ID:** 228917

Open defects

The following table lists the customer defects that are open in this release.

Defect ID: DEFECT000282621	**Technical Severity:** High
Summary: SuperX reloaded after applying an ACL to the lead port of a trunk, with vlan-group configuration of more than 100 VLANs.	
Symptom: SuperX reloaded after applying an ACL to the lead port of a trunk, with vlan-group configuration of more than 100 VLANs.	
Feature: SX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000266633	**Technical Severity:** High
Summary: OSPFv3 - Learned routes are not present after configuring 'redist static'	
Symptom: Customer may not see the learned routes after issuing 'redist static'. Need to wait few more seconds to see the routes.	
Workaround: Wait few more seconds to see all the routes.	
Feature: SX Layer3 Control Protocols	**Function:** OSPFV3 - IPV6
Reported In Release: FI 05.0.00	**Probability:** Low

Defect ID: DEFECT000266969	**Technical Severity:** High
Summary: GRE forwards multicast stream through PIM-SM disabled tunnel if there is a cloud between the tunnel endpoint routers	
Symptom: 1. In a 3 or more router topology with a cloud between GRE tunnel endpoints, GRE forwards multicast streams through a PIM-SM disabled tunnel, if the multicast Group destination is on the same side of the cloud as the PIM-SM RP. 2. Since PIM is disabled, TTL is not decremented. Since the destination is 3 or more multicast hops from the source, a loop may occur.	
Workaround: 1. Use PIM-DM for GRE tunnel topologies where there are one or more clouds between the tunnel endpoints, and at least one multicast data path is not through the GRE tunnel. 2. Only configure PIM-SM over a GRE tunnel with one or more clouds, if PIM-SM is enabled all router endpoints of a GRE tunnel. 3. If PIM-SM cannot be enabled on all tunnel endpoint routers, if possible maintain PIM-SM RP on the multicast source side of a tunnel, not the multicast destination side of the tunnel. 3a. After disabling PIM-SM on a GRE tunnel router, save running configuration and reboot all cloud and tunnel routers. 3b. If PIM-SM is not enabled on both tunnel router endpoints, reboot cloud routers whenever rebooting tunnel routers.	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** GRE Tunnels

Reported In Release: FI 05.1.00	**Probability:** Medium

Defect ID: DEFECT000267124	**Technical Severity:** High
Summary: "buffer-sharing-full" is not removing existing QD commands	
Symptom: "buffer-sharing-full" is not removing existing QD commands	
Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000267159	**Technical Severity:** High
Summary: ACL - Some permitted IP traffic with precedence 7 is not forwarded.	
Symptom: When IP traffic with different IP precedence is transmitted, intermittently some of the precedence 7 traffic is not forwarded.	
Feature: SX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000268863	**Technical Severity:** High
Summary: Neither implicit nor explicit deny clauses after permit clauses will work in OSPF redistributing static.	
Symptom: User expects those routes which are not specified in the permit clauses would be denied, but they will not be denied.	
Workaround: To use specific deny clauses first, then ends up with a permit 0.0.0.0/0 clause.	
Feature: SX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000269860	**Technical Severity:** High
Summary: sFlow extended type Router next hop value is 0.0.0.0 for directly connected subnets instead of the gateway IP	
Symptom: sFlow router next hop values for direct routes (directly connected subnets) display as 0.0.0.0 instead of the gateway IP.	
Workaround: None. A gateway IP of 0.0.0.0 is considered a default route per the IP forwarding table MIB for CIDR (RFC 2096), which deprecates the RFC 1213 IP routing table.	
Feature: SX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.00	**Probability:** High

Defect ID: DEFECT000279513	**Technical Severity:** High
Summary: sFlow stops sampling after changing configuration from a very large sampling rate to a very	

small sampling rate.	
Symptom: sFlow stops sampling after changing configuration from a very large sampling rate to a very small sampling rate.	
Workaround: Perform "no sflow enable" and "sflow enable", then sflow starts to work again.	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000279708	**Technical Severity:** High
Summary: Change OSPF cost on link port in ECMP mode will remove both default route entries for as long as 30 seconds.	
Symptom: If it happens, the data flow based on OSPF default routes will be disrupted for 30 seconds, which means a big data loss. However, it is an unknown condition which is very rarely seen.	
Workaround: Disable ECMP.	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000280440	**Technical Severity:** High
Summary: Default buffer allocations only using 2/3 the buffers.	
Symptom: Default buffer allocations only using 2/3 the buffers.	
Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000280923	**Technical Severity:** High
Summary: If a global policy is installed prior to the router's rebooting, "Sanity check failed" occurs after removing the global policy and then hot-swap module.	
Symptom: (1) Customer will not see it if only interface-policy is configured before rebooting the box, even a global policy is added after rebooting, and then gets removed. (2 Customer will see it only if a global policy and few interface-policies are configured before rebooting. Then after rebooting, remove the global policy, and start hot-swap module.	
Workaround: None.	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** PBR
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000282304	**Technical Severity:** High
Summary: [chassis-temp-fan] FCX-I/FCX-E does not send any traps or syslog messages when the fan is down.	
Symptom: Customer will not see Syslog messages or traps when there is a fan failure.	
Feature: FCX Platform Specific features	**Function:** Chassis/fan/power

	supplies/temperature sensors
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000282504	**Technical Severity:** High
Summary: CPU high on stack with 2 port trunk between stack and standalone unit	
Symptom: Using the CLI command "show cpu" after creating a trunk between a stack and a stand-alone switch will show a CPU rate of 12% for initial traffic over the trunk.	
Workaround: Wait a few minutes before entering the 'show cpu' command.	
Feature: FCX L2 Control	**Function:** Link Aggregation - LACP/Dynamic
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000281981	**Technical Severity:** Medium
Summary: An error message "sh ip rsw_gi_set_application_vlan_port_mask: ERROR! vidx 4128 is not in use!" is seen on the console when a dynamic configuration change is performed.	
Symptom: This message is seen when a multi-netted VE has one of its IP addresses removed from the configuration. Also, this is not seen after a reboot.	
Feature: SX L2/L3 Multicast Features	**Function:** PIM Dense
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000267007	**Technical Severity:** Medium
Summary: When using GVRP with 1000 VLANs, it will cause 99% CPU on stack.	
Symptom: High CPU will be seen when GVRP is used on 1000 VLANs.	
Workaround: None or reduce number of VLANs to 100 VLANs.	
Feature: FCX L2 Control	**Function:** GVRP
Reported In Release: FI 06.0.00	**Probability:** Medium

Defect ID: DEFECT000267214	**Technical Severity:** Medium
Summary: In PBR routing, the egress interface MTU is ignored, leading to failure of forwarding from jumbo-mode to non-jumbo mode.	
Symptom: In PBR routing, the egress interface MTU is ignored, leading to failure of forwarding from jumbo-mode to non-jumbo mode.	
Feature: SX Layer 3 Forwarding - IPV4 and IPV6	**Function:** PBR
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000267312	**Technical Severity:** Medium

Summary: ACL logging doesn't work with mac-auth dynamic ACL	
Symptom: ACL logging doesn't work on an ACL rule if the ACL is dynamically assigned to the interface by mac-authentication.	
Feature: SX ACL	**Function:** Mac Authentication and user based policies
Reported In Release: FI 07.0.00	**Probability:** Low

Defect ID: DEFECT000268681	**Technical Severity:** Medium
Summary: OSPF v3: "clear ipv6 ospf counts neighbor int ve xxx" returns "Error - ve xxx was not configured".	
Symptom: Customer sees an unexpected error message which actually is a false alarm.	
Feature: SX Layer3 Control Protocols	**Function:** OSPFV3 - IPV6
Reported In Release: FI 07.0.00	**Probability:** High

Defect ID: DEFECT000269117	**Technical Severity:** Medium
Summary: lldpLocManAddrTable and lldpRemManAddrTable do not display correct IPv4 and IPv6 address.	
Symptom: lldpLocManAddrTable and lldpRemManAddrTable do not display correct IPv4 and IPv6 address.	
Feature: FCX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000270250	**Technical Severity:** Medium
Summary: Multiple spanning tree (mstp disable command) gets removed from the configuration.	
Symptom: If a port is configured as disabled with "no span" and if "mstp disable" command is configured for that port (and the configuration is saved). Then after a reboot the command mstp disable gets removed from the configuration.	
Feature: SX L2 Control	**Function:** Spanning Tree Protocols
Service Request ID: 235805	
Reported In Release: FI 05.1.00	**Probability:** Medium

Defect ID: DEFECT000272698	**Technical Severity:** Medium
Summary: After one next-hop goes down, the other entry in ECMP routing is flapped, on an OSPF internal router with VL.	
Symptom: Short time connectivity disruption. However, experiences show that it is a condition built intermittently, not "always" the case.	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000273440	**Technical Severity:** Medium
Summary: "snmpset" fails to delete existing fdryTrapReceiverEntry	
Symptom: "snmpset" fails on fdryTrapReceiverEntry table.	
Workaround: Use CLI to configure trap receiver.	
Feature: SX Network Management	**Function:** SNMP V4/V6
Reported In Release: FI 07.0.00	**Probability:** Low

Defect ID: DEFECT000275023	**Technical Severity:** Medium
Summary: IPv6 Neighbor discovery commands do exist on the FCX/FGS/FWS.	
Symptom: IPv6 Neighbor discovery commands do exist on the FCX/FGS/FWS.	
Feature: FCX Layer3 Control Protocols	**Function:** Neighbor Discovery
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000275133	**Technical Severity:** Medium
Summary: Incorrect CLI parser options after enabling password-masking	
Symptom: ASCII string option should not be an option presented by the "?" after enabling password-masking. Entering an ASCII string results in an invalid command error message.	
Feature: FCX Network Management	**Function:** AAA RADIUS/TACACS+ V4/V6
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000275395	**Technical Severity:** Medium
Summary: After continuous "clear ip routes" then "show mem", the Used Mem can increase by 1%.	
Symptom: Continuous "clear ip route" is not practical and not allowed in an official network operation. Customer may see this in LAB testing if their LAB network injects a decent amount of ip routes.	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000275416	**Technical Severity:** Medium
Summary: Web Management does not make stack priority become affected right after first reload. Only works after second reload.	
Symptom: Web Management does not make stack priority become affected right after first reload. Only works after second reload.	
Feature: FCX Network Management	**Function:** Web Management
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000275558	**Technical Severity:** Medium
Summary: On FCX and FGS related platforms, disabling spanning tree and enabling spanning tree on the global config mode will not enable the spanning tree on the Member VLANs in a topology group and will only enable spanning tree on the master VLANs	
Symptom: On FCX and FGS related platforms, disabling spanning tree and enabling spanning tree on the global config mode will not enable the spanning tree on the Member VLANs in a topology group and will only enable spanning tree on the master VLANs.	
Workaround: Disabling and enabling spanning tree on master VLAN all member VLANs will share spanning tree.	
Feature: FCX L2 Control	**Function:** Spanning Tree Protocols
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000275601	**Technical Severity:** Medium
Summary: 30W are allocated for Legacy PD's on FCX PoE. Legacy should be 15.4	
Symptom: In a large scale PoE network, some device may not get the power needed.	
Workaround: Set the power class to 1, 2 or 3 depending on the need. Or manually define the needed power.	
Feature: FCX Layer1 features	**Function:** PoE/PoE+
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000275786	**Technical Severity:** Medium
Summary: Slot numbers are not mentioned in front panel display	
Symptom: On front panel display, slot numbers are not mentioned for all these platforms SuperX, FCX, FGS, FLS 648, FWS and FGS. For FLS 624, slot numbering is wrong, it says slot 4 instead of slot 1.	
Workaround: For FLS 624, slot numbering is wrong, it says slot 4 instead of slot 1. For SuperX, FCX, FGS, FLS 648, FWS and FGS, slot numbering can be seen on console or for some on hardware unit also.	
Feature: FCX Network Management	**Function:** Web Management
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000275917	**Technical Severity:** Medium
Summary: "super-user-password" not masked after enabling "enable user password-masking"	
Symptom: ASCII string input for "enable super-user-password" configuration command is not masked after issuing "enable user password-masking" configuration command.	
Feature: FCX Management Functionality	**Function:** CLI and parser
Reported In Release: FI 07.0.00	**Probability:** Medium

Defect ID: DEFECT000278377	**Technical Severity:** Medium
Summary: VLAN membership mis-match with expected VLAN (10) after logoff stays at VLAN 20.	
Symptom: If login and logoff, you may see the problem. But once the correct login happens, the port will be assigned to correct VLAN. So the actual client on the port may not notice the problem because the client is logged off.	
Workaround: Either login again, or clear dot1x/mac-auth.	
Feature: FCX ACL	**Function:** Mac-Authentication with 802.1X
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000278385	**Technical Severity:** Medium
Summary: All traffic passing the permit-at-low-pri TPD is sent through 0-priority queue (802.1p)	
Symptom: When permit-at-low-pri is configured in a traffic-policy, even the green packets with original 802.1p priority (as 3) are sent through 0-priority queue. When drop is configured for the traffic-policy, it works fine, and packets are sent via 3-pri (original configured priority) queue.	
Feature: SX ACL	**Function:** ACL based rate limiting
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000278499	**Technical Severity:** Medium
Summary: An SCP AES copy of the running or start configuration from the Brocade device to Linux WS 4 or 5 will fail when the configuration size is small(<700 bytes).	
Symptom: An SCP AES copy of the running or start configuration from the Brocade device to Linux WS 4 or 5 will fail when the configuration size is small(<700 bytes).	
Workaround: Use putty to perform the SCP.	
Feature: FCX Network Management	**Function:** SSHv2/SCP V4/V6
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000278934	**Technical Severity:** Medium
Summary: TDR is not functional on FCX-F	
Symptom: Customer cannot perform virtual cable testing when FCX-F is in stacking.	
Workaround: Remove the cable on which TDR should be performed, then connect to the active controller and perform TDR.	
Feature: FCX Layer1 features	**Function:** Virtual cable testing technology (VCT)
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000278971	**Technical Severity:** Medium

Summary: After the ASBR creates a summary LSA, the more specific LSAs are not flushed from neighbor routers.	
Symptom: Customer creates summary for external routes to conserve system resource, but they will not achieve the goal until the LSAs are aged out on neighbor routers, and the maximum waiting time could be 1800 seconds. Since the ASBR which originates these LSA will not flush them with an age of 3600, a reload may be necessary.	
Workaround: None.	
Feature: FCX Layer3 Control Protocols	**Function:** OSPFV2 - IPV4
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000279567	**Technical Severity:** Medium
Summary: The hello, dead and hold interval do not resume default values after reload without saving config	
Symptom: The Hello-interval, dead-interval and hold-interval might not resume default values if before a reload, their values were changed and then reloaded without saving the configuration.	
Workaround: Before reload, save config by "write memory" with desired values of Hello-interval, dead-interval and hold-interval.	
Feature: FCX L2 Control	**Function:** VSRP(master and aware)
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279583	**Technical Severity:** Medium
Summary: TDR is not functional on FCX stand-by and members.	
Symptom: Customer cannot see TDR from stand by and member units.	
Workaround: None. Connect the cable to active and perform TDR	
Feature: FCX Layer1 features	**Function:** Virtual cable testing technology (VCT)
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000279589	**Technical Severity:** Medium
Summary: TDR shows the cable length as below 50 meters even it is greater than 50 mts (150 mts)	
Symptom: The customer will not get wrong information from TDR even though the cable length is above 50 mts.	
Feature: FCX Layer1 features	**Function:** Virtual cable testing technology (VCT)
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279613	**Technical Severity:** Medium
Summary: DOM: FCX-S 10G-XFP-LR Avago optic does not show in Show Media. Error Optic is not Brocade qualified (port 1/3/2).	
Symptom: LR Optic (Avago p/n ending in FD2) does not show in show media.	

Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279623	**Technical Severity:** Medium
Summary: ACL logging should be disabled for permit ACL traffic	
Symptom: On enabling ACL logging feature with permit ACL, Syslog events are generated for permit traffic. This should be disabled. ACL logging feature is for deny ACL.	
Feature: SX ACL	**Function:** ACL Logging
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000279721	**Technical Severity:** Medium
Summary: In Fan- threshold "speed-1 cannot be changed below 56" and "speed-3 cannot be changed above 67"	
Symptom: Customer can not set the fan-threshold values below 56 on speed-1 and above 67 on speed-3.	
Workaround: NONE	
Feature: FCX Platform Specific features	**Function:** Chassis/fan/power supplies/temperature sensors
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000279775	**Technical Severity:** Medium
Summary: LLDP does not show syslog message under 'show log' command.	
Symptom: LLDP syslog message is not seen under system log file.	
Feature: FCX L2 Control	**Function:** LLDP
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279824	**Technical Severity:** Medium
Summary: Root port does not update for shortest path in MSTP, it requires restarting MSTP to update it correctly	
Symptom: If force-version is changed from 3 to 0 and back to 3, then it will not update root port for shortest path.	
Workaround: Need to restart MSTP by issuing commands "no mstp start" followed by "mstp start".	
Feature: FCX L2 Control	**Function:** 802.1s
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279825	**Technical Severity:** Medium

Summary: Changing mstp force-version 3 to 0 and then back to 3 does not update regional root bridge, root port and path cost	
Symptom: If force-version is changed from 3 to 0 and back to 3, then it will not update mstp information (regional root bridge, root port and path cost). It will show two root bridges in mstp after these changes.	
Workaround: Need to restart MSTP by issuing commands "no mstp start" followed by "mstp start".	
Feature: SX L2 Control	**Function:** 802.1s
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279836	**Technical Severity:** Medium
Summary: Show Media S/S/P on non active currently only displays media type and leaves other fields blank	
Symptom: Show Media Ethernet S/S/P on a non master unit only displays the optic type. Other information fields are returned as blank.	
Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279875	**Technical Severity:** Medium
Summary: [MSTP] On doing "no force-version 0" the root port principle is violated(lowest numbered port should be root port if there are redundant links to root from same switch)	
Symptom: MSTP root port changes which changes operation of MSTP	
Workaround: Stop MSTP and restart MSTP	
Feature: FCX L2 Control	**Function:** Spanning Tree Protocols
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000279919	**Technical Severity:** Medium
Summary: FCX-F: BXD-OM optic does not remove from Show Media on NON active units when optic removed	
Symptom: Show media still displays E1MG-BXD-OM optic after it has been removed.	
Workaround: Reboot.	
Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279922	**Technical Severity:** Medium
Summary: FCX-F: BXU-OM optic does not remove from Show Media on NON active units when optic removed	
Symptom: When you remove an E1MG-BXD-OM optic, it still shows in Show Media.	
Workaround: Reboot	

Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000279966	**Technical Severity:** Medium
Summary: [RSTP] Port should not be both Admin-edge-port and Admin-p2p-port .	
Symptom: Same port can be configured as edge port and point to point.	
Workaround: Remove the point to point or edge configuration.	
Feature: FCX L2 Control	**Function:** Spanning Tree Protocols
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000279980	**Technical Severity:** Medium
Summary: DOM: FCX-F: DOM features not reporting on 100MB optics in Standby and Member roles	
Symptom: Show Optic/ Show Optic Threshold commands are not returning values. (blank)	
Feature: FCX Layer1 features	**Function:** Digital Optical Monitoring
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000280053	**Technical Severity:** Medium
Summary: Error message "Sanity check failed" is seen when adding/removing ports from a VLAN.	
Symptom: Error message "Sanity check failed" is seen when adding/removing ports from a VLAN.	
Workaround: remove the ip access group from VE1	
Feature: SX ACL	**Function:** ACL(all aspects of ACLs - IPV4)
Service Request ID: 240866	
Reported In Release: FI 05.1.00	**Probability:** High

Defect ID: DEFECT000280090	**Technical Severity:** Medium
Summary: Mac-based VLAN: After configuring a port on a VLAN using "mac-vlan-permit", if you later do "no vlan <num>" and then "vlan <num>", you will no longer be able to remove the mac-vlan-permit configuration from the running config	
Symptom: Mac-based VLAN: After configuring a port on a VLAN using "mac-vlan-permit", if you later do "no vlan <num>" and then "vlan <num>", you will no longer be able to remove the mac-vlan-permit configuration from the running config. This means that you cannot change that port to be tagged or untagged on that VLAN.	
Workaround: If you re-configure the "mac-vlan-permit eth <port>" in the VLAN, then you will be able to successfully remove it. Do not do "no vlan <num>" if you have any mac-vlan-permit entry configured in that VLAN.	
Feature: FCX L2 Forwarding	**Function:** MAC- BASED VLAN
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000280253	**Technical Severity:** Medium
Summary: Mac-Auth fails to authenticate after removing it and adding it back. Configuration has both mac-auth and dot1x with dynamic VLAN.	
Symptom: mac-auth will fail to authenticate	
Workaround: Reload or remove both mac-auth and dot1x and reconfigure it.	
Feature: FCX ACL	**Function:** Mac-Authentication with 802.1X
Reported In Release: FI 07.0.01	

Defect ID: DEFECT000280327	**Technical Severity:** Medium
Summary: When enable SFLOW or reboot with SFLOW, seeing "UNIT3:rated 1: UNIT3:ERROR:: non-existing device in sw_cheetah_is_user_port, dev" message.	
Symptom: When enable SFLOW or reboot with SFLOW, seeing "UNIT3:rated 1: UNIT3:ERROR:: non-existing device in sw_cheetah_is_user_port, dev" message.	
Workaround: This error message does not impact sFlow functionality.	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000280333	**Technical Severity:** Medium
Summary: System priority value for a LACP does not display configured value in the "show link-ag"	
Symptom: The system Priority configured for an LACP link is not reflected in the "show link-a"	
Feature: FCX L2 Control	**Function:** Link Aggregation - LACP/Dynamic
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000280342	**Technical Severity:** Medium
Summary: VSRP instability during transition when protocol VLAN is configured.	
Symptom: VSRP instability during transition when protocol VLAN is configured.	
Feature: FCX L2 Control	**Function:** VSRP(master and aware)
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000280428	**Technical Severity:** Medium
Summary: Weighted priority QOS profile setting 0 and 7 not working intermittently on FCX624.	
Symptom: Weighted priority QOS profile setting 0 and 7 not working intermittently on FCX624. QOS priorities are swapped back and forth several times to see the problem.	
Feature: SX Quality Of Service	**Function:** Layer3 QoS Test cases
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000280444	**Technical Severity:** Medium
Summary: Router: DoS attack protection on routed traffic only allows half of the burst-normal that is configured and also exceeds burst-max before actually exceeding for low values	
Symptom: Router: DoS attack protection on routed traffic only allows half of the burst-normal that is configured and also exceeds burst-max before actually exceeding. This occurs when the burst configuration is set to low values.	
Workaround: Tell user to configure the burst-normal and burst-max to be 100 or greater.	
Feature: SX ACL	**Function:** DoS Protection
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000280467	**Technical Severity:** Medium
Summary: Dynamically modifying dual-mode configuration on port creates duplicate mac-auth session.	
Symptom: Duplicate mac-auth entries are shown under authorized mac table.	
Workaround: Disable port first before changing dual-mode configuration.	
Feature: FCX ACL	**Function:** Mac-Authentication with 802.1X
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000280579	**Technical Severity:** Medium
Summary: Mac-based VLAN does not reject host when radius attribute contains a dynamic ACL, this also causes all packets from the host to go to CPU	
Symptom: Mac-based VLAN does not reject the host when radius attribute contains a dynamic ACL. This can cause all packets from that host to go to CPU.	
Workaround: Tell user to make sure that the radius attribute for MAC-based VLAN hosts does not have dynamic ACL configured.	
Feature: FCX L2 Forwarding	**Function:** MAC- BASED VLAN
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000280595	**Technical Severity:** Medium
Summary: sFlow doesn't display correct source and destination subnet mask value.	
Symptom: sFlow doesn't display correct source and destination subnet mask value.	
Feature: FCX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000280626	**Technical Severity:** Medium
Summary: "buffer-profile" commands for VOIP do not set buffers if Jumbo is enabled.	
Symptom: "buffer-profile" commands for VOIP do not set buffers if Jumbo is enabled.	

Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000281016	**Technical Severity:** Medium
Summary: The system allows you to configure the “Backup Priority to 0” however the valid range is 3 to 254.	
Symptom: The system allows you to configure the “Backup Priority to 0” however the valid range is 3 to 254.	
Feature: SX Layer3 Control Protocols	**Function:** VRRP/VRRP-E and slow-start timer-VRRP-E timer scale
Service Request ID: 229339	
Reported In Release: FI 05.1.00	**Probability:** High

Defect ID: DEFECT000281399	**Technical Severity:** Medium
Summary: Optical monitor disabled on stacking ports conflict seen between active and standby unit.	
Symptom: If optical monitor is enable on a unit before running secure setup, then the stack running config will show 'no optical-monitor' under stacking ports. However, after removing active unit and the standby became the active unit, the 'no optical-monitor' configuration on some stacking ports were not allowed.	
Feature: FCX Stacking	**Function:** stack-ports
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000281400	**Technical Severity:** Medium
Summary: FCX/FGS/FLS - repeatedly sends traps and syslog messages when the warning temperature is exceeded.	
Symptom: FCX and FGS/FLS stacking devices will repeatedly send out traps and syslog messages when a temperature warning has occurred. No trap or syllogism message is sent when the device returns to normal operating temperature. The customer will not be certain if the device has returned to normal temperature and then exceeded the warning level again.	
Workaround: Check the device actual temperature by issuing the following CLI command 'show chassis' and verify the actual device temperature.	
Feature: FCX Network Management	**Function:** SNMP Traps
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000281648	**Technical Severity:** Medium
Summary: "buffer-sharing full" is not setting 10G ports to maximum buffers.	
Symptom: "buffer-sharing full" is not setting 10G ports to maximum buffers.	
Workaround: Use QD command	

Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000281703	**Technical Severity:** Medium
Summary: ACL with "permit ip any any dscp-marking" doesn't remark DSCP in egress packet.	
Symptom: ACL with "permit ip any any dscp-marking" doesn't remark DSCP in egress packet.	
Workaround: Use dscp-marking with dscp-matching and 802.1p-priority-matching.	
Feature: FCX ACL	**Function:** ACL ToS/QoS - IPv4
Reported In Release: FI 07.0.01	

Defect ID: DEFECT000281827	**Technical Severity:** Medium
Summary: sFlow displays CPU percentage value with incorrect digit number.	
Symptom: sFlow CPU percentage value displays with incorrect digit number. e.g. 1% ==> display as 0.1	
Feature: SX Network Management	**Function:** sFlow
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000281946	**Technical Severity:** Medium
Summary: "tag-profile" is using default 8100 instead of what was configured.	
Symptom: When users use tag-type or tag-profile to configure the core switch and add additional tag other than 8100, it will use 8100.	
Workaround: There is no impact to traffic.	
Feature: FCX L2 Forwarding	**Function:** Q-in-Q
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000281968	**Technical Severity:** Medium
Summary: ACL-per-vlan - traffic not blocked after removing a trunk and re-configure it for applied acl on per-vlan.	
Symptom: Traffic not blocked by deny ACL after removing a trunk and re-configure it for applied acl on per-vlan.	
Workaround: Remove the ACL and re-apply it again.	
Feature: SX ACL	**Function:** ACL per port per VLAN
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000282346	**Technical Severity:** Medium
Summary: IPv6 ping fails intermittently on FCX-F when the port is configured for untagged VLAN xyz	
Symptom: May fail IPv6 telnet, SSH, and other IPv6 data connections.	

Workaround: Keep the ports in default VLAN	
Feature: FCX Layer 3 Forwarding - IPV4 and IPV6	**Function:** Data Forwarding
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000282498	**Technical Severity:** Medium
Summary: QD commands pre-configured to 8192 are being changed to 8096 with no indications.	
Symptom: QD commands pre-configured to 8192 are being changed to 8096 with no indications.	
Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000282539	**Technical Severity:** Medium
Summary: sFlow FCX stack reports hardware FLOWSAMPLES ingressing standby slave as discarded packets instead of L2 forwarded or L3 routed.	
Symptom: sFlow FCX stack reports hardware FLOWSAMPLES ingressing standby slave as discarded packets instead of L2 forwarded or L3 routed.	
Feature: FCX Stacking	**Function:** stack-ports
Reported In Release: FI 07.0.01	**Probability:** High

Defect ID: DEFECT000282594	**Technical Severity:** Medium
Summary: Setting qd buffer and descriptor to max 8096, but only getting 8059 packets out.	
Symptom: Setting qd buffer and descriptor to max 8096, but only getting 8059 packets out.	
Feature: FCX Layer1 features	**Function:** Dynamic buffer allocation
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000282618	**Technical Severity:** Medium
Summary: max-acl-log-num command is not configuring maximum ACL related log entries.	
Symptom: When maximum number of ACL-related log entries using max-acl-log-num command is set, it is not coming into effect. Even after configuring a certain number as max-acl-log-num, the show log command is showing more than configured log entries for ACL.	
Feature: SX ACL	**Function:** ACL Logging
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000282752	**Technical Severity:** Medium
Summary: "system-max hw-traffic-conditioner" command is not configuring maximum limit on traffic-policy counts	
Symptom: When maximum number of traffic-policy is configured using "system-max hw-traffic-conditioner" command, configured number is not honored. After configuring a certain number as system-max for hw-traffic-conditioner, it allows to configure more than 10 traffic policy and bind it along with ACL to interface.	
Feature: SX ACL	**Function:** ACL based rate limiting
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000282838	**Technical Severity:** Medium
Summary: L3M: "Error - Port Total Bandwidth = 0!" while switchover on SuperX.	
Symptom: Sometimes during switchover "Error - Port Total Bandwidth = 0!" message displayed on console.	
Workaround: Interfaces are forwarding traffic after switchover is complete. It might not affect traffic forwarding through the ports.	
Feature: SX Platform Specific features	**Function:** Hot Swap
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000282956	**Technical Severity:** Medium
Summary: PSU 'DC ok' LED stays red after the power source is unplugged then plugged back in.	
Symptom: In FCX648s-HPOE and FCX624s-HPOE with two power supply units (PSUs) in the switch, when powered up together, sometimes one of the PSU DC LEDs will stay red. Or, when both PSUs are powered up and one of the power cords is unplugged then plugged back in, the DC LED will stay red. Also the front panel PSU LED will be amber. If the switch has some POE devices connected, it will not run into this condition.	
Feature: FCX Platform Specific features	**Function:** Chassis/fan/power supplies/temperature sensors
Reported In Release: FI 06.0.00	**Probability:** High

Defect ID: DEFECT000282977	**Technical Severity:** Medium
Summary: SSH session terminates after "Bad packet length" message.	
Symptom: SSH session terminates with "Bad packet length" message when attempting to paste configuration commands.	
Feature: SX Management Functionality	**Function:** IPv4/V6 SSH Service
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000283012	**Technical** Medium

	Severity:
Summary: L3M: "Duplicating the IPV4 (*,G) MC Route Entry (route to CPU) for the group address 225.108.1.55 failed, error code: 11." are coming on switchover	
Symptom: After issuing switchover on active module, these error messages for duplicating MC entry for groups will be displayed on console of this module.	
Feature: SX L2/L3 Multicast Features	**Function:** L2 multicast Hitless support
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000283617	**Technical Severity:** Medium
Summary: L3M: 'sysInfo_client_sendInfo: error' and 'sxr_sync_port_link_speed_state : ERROR' error messages during hotswap	
Symptom: Sometimes 'sysInfo_client_sendInfo: error' and 'sxr_sync_port_link_speed_state : ERROR' messages coming on console during hotswap.	
Workaround: It doesn't affect the functionality as such and all ports are up and running as before.	
Feature: SX Platform Specific features	**Function:** Hot Swap
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000289349	**Technical Severity:** Medium
Summary: "no legacy-inline-power" does not work on FGS and FGS-STK devices.	
Symptom: If support for POE legacy powered devices is disabled by the CLI command **no legacy-inline-power** and a legacy phone is plugged into a POE port, or unplugged then plugged into the same POE port, or if the device is rebooted, the Brocade device will incorrectly recognize the phone as 802.3af-compliant and will allocate power to it.	
Feature: FCX Layer 1 features	**Function:** POE/POE+
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000289451	**Technical Severity:** Medium
Summary: A port does not release power after configuring “inline power power-limit” when no PD is connected to it. This occurs on FWS, FGS, and FGS-STK devices.	
Symptom: If a powered device (PD) is unplugged from a POE port, the Brocade device will continue to provide power to the port even when the PD is no longer connected. The “show inline power” command output will not be updated in this case. However, the “show interface brief” command output will give the correct status of the POE port. There is a chance if Inline power is configured for new ports, or there are ports waiting to get power, they might not get power because some ports where a PD was removed did not release power. These new PD ports will be waiting for power and will come to an operational state of ‘ON’. In that	

case, reloading the unit might recover the unit's normal state.	
Feature: FCX Layer 1 features	**Function:** POE/POE+
Reported In Release: FI 07.0.01	**Probability:** Low

Defect ID: DEFECT000289753	**Technical Severity:** Medium
Summary: DHCP Client fails to TFTP download configuration files on 48 port FGS unit	
Symptom: DHCP client may fail to download some configuration files from the TFTP server to the FGS648. This problem occurs when all of the following conditions are true: 1. The unit is an FGS648 standalone (non-stacking) device and is being upgraded from pre-release 7.0.01 (non-stacking releases only) to release 7.0.01 or later. 2. There is no configuration saved in the flash memory of the FGS648. 3. The TFTP-downloaded configuration file is downloaded with "unit prompt name and base MAC address concatenated file name". For example, the file name is "FGS648P-Switch0024.3801.8b00-config.cfg" or "FGS648P-Switch0024.3801.8b00.cfg". In the scenario above, TFTP requests will be sent out in the following sequence and TFTP requests 1 and 2 will fail: 1. FGS648P-Switch0024.3801.8b04-config.cfg 2. FGS648P-Switch0024.3801.8b04.cfg 3. foundry.cfg 4. brocade.cfg 5. fgs-Switch.cfg	
Workaround: Do one of the following: • Before upgrading the software to release 07.0.01b, save the configuration to flash memory by issuing the write memory CLI command on the FGS648. • On the TFTP server, change the configuration file names. For example, if the file name is "FGS648P-Switch0024.3801.8b00.cfg", change it to "FGS648P-Switch0000.0801.8b00.cfg". The first 2 and a half bytes are changed.	
Feature: FCX DHCP	**Function:** Client
Reported In Release: FI 07.0.01	**Probability:** Medium

Defect ID: DEFECT000289798	**Technical Severity:** Medium

Summary: Inline power configuration on some ports affecting port 35 and 36 of that particular unit...	
Symptom: When inline power is enabled or disabled on some ports, it will withdraw power and re-allocate back to ports 35 and 36 of that particular unit (with inline power already configured on 35 and 36).	
Feature: FCX Layer 1 features	**Function:** POE/POE+
Reported In Release: FI 07.0.01	**Probability:** Low