



IronWare Software Release R04.2.00b for Brocade TurboIron 24X Series Switches Release Notes v1.0

November 22, 2010

Document History

Document Title	Summary of Changes	Publication Date
IronWare Software Release R04.2.00b for Brocade TurboIron 24X Series Switches Release Notes v1.0	Initial release	November 2010

Copyright © 2010 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, IronPoint, IronShield, IronView, IronWare, JetCore, NetIron, SecureIron, ServerIron, StorageX, and TurboIron are registered trademarks, and DCFM, Extraordinary Networks, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

Export of technical data contained in this document may require an export license from the United States Government.

Contents

Supported Devices for IronWare R04.2.00b	4
Summary of Enhancements in IronWare R04.2.00b.....	4
Summary of Enhancements in IronWare R04.2.00a	4
Summary of Enhancements in IronWare R04.2.00	5
Feature Support	8
Supported Management Features.....	8
Supported IPv6 Management Features	9
Supported Security Features	9
Supported System-Level Features	11
Supported Layer 2 Features	14
Supported Layer 3 Features	16
Image Files for IronWare R04.2.00b.....	17
Factory Pre-loaded Software	17
Upgrading software images.....	17
Upgrading the Boot Code	17
Upgrading the Flash Code	18
Technical Support.....	18
Additional Resources	19
Defects	20
Closed Defects in IronWare R04.2.00b	20
Closed Defects in IronWare R04.2.00a	20
Closed Defects in IronWare R04.2.00	20
Open Defects in IronWare R04.2.00	20

Supported Devices for IronWare R04.2.00b

This software release applies to the TurboIron 24X compact switch only.

Summary of Enhancements in IronWare R04.2.00b

BGP support has been added to the TurboIron 24X in Release 04.2.00b. BGP is documented in the chapter “Configuring BGP4” of the *FastIron and TurboIron 24X Configuration Guide*.

Note : In this release, there can be up to 12,000 BGP routes.

Summary of Enhancements in IronWare R04.2.00a

There are no enhancements in Release 04.2.00a of the TurboIron 24X.

Summary of Enhancements in IronWare R04.2.00

This section describes feature enhancements in the TurboIron 24X R04.2.00 software release.

Feature	Description	Described in the <i>FastIron and TurboIron Configuration Guide</i>
SAV	This enhancement improves SAV interoperability between Brocade devices and other vendors' devices that support the 802.1Q tag-types.	Chapter 13: Configuring Virtual LANs (VLANs) Section: "Support for 802.1Q-in-Q tagging"
Q-in-Q	802.1Q-inQ tagging provides finer granularity for configuring 802.1Q tagging and enables you to configure 802.1Q tag-types on a group of ports.	Chapter 13: Configuring Virtual LANs (VLANs) Section: "Configuring 802.1Q-inQ tagging"
MRP 1 and MRP 2	Brocade proprietary protocol that prevents Layer 2 loops and provides fast reconvergence in Layer 2 ring topologies.	Chapter 11: Configuring Metro Features Section: "Metro Ring Protocol (MRP)"
VSRP	Brocade propriety protocol that provides redundancy and sub-second failover in Layer 2 and Layer 3 mesh topologies.	Chapter 11: Configuring Metro Features Section: "Virtual Switch Redundancy Protocol (VSRP)"
Hardware-based private VLAN	A private VLAN is a standard Layer 2 port-based VLAN, which provides additional control over flooding packets on a VLAN. Private VLANs on the TurboIron device forward unknown-unicast, unregistered multicast, and broadcast in hardware.	Chapter 13: Configuring Virtual LANs (VLANs) Section: "Configuring private VLANs"
Topology and VLAN groups	VLAN group supports creating multiple port-based VLANs with identical port members.	Chapter 13: Configuring Virtual LANs (VLANs) Section: "Configuring VLAN groups and virtual routing interface groups"
Hardware-based DoS attack prevention	Supports DoS attack monitoring and detection performed in the hardware.	Chapter 46: Protecting Against Denial of Service Attacks Section: "Protection against ICMP attacks in TurboIron devices"
MAC authentication	Supports configuring MAC authentication and 802.1X authentication on the same port.	Chapter 44: Configuring Multi-Device Port Authentication Section: "Configuring multi-device port authentication"

Feature	Description	Described in the <i>FastIron and TurboIron Configuration Guide</i>
802.1x security	Supports IEEE 802.1X standard for authenticating devices attached to LAN ports.	Chapter 42: Configuring 802.1X Port Security Section: "Configuring 802.1X Port Security"
Port MAC security	Supports forwarding only packets that match secure addresses.	Chapter 43: Using the MAC Port Security Feature Section: "Using the MAC Port Security Feature"
Dynamic VLAN assignment	This feature supports placing a port in one or more VLANs based on the MAC address learned on that interface.	Chapter 44: Configuring Multi-Device Port Authentication Section: "Support for dynamic VLAN assignment"
MAC filter enhancements	Supports filtering packets based on the etype optional keyword.	Chapter 10: Configuring Basic Layer 2 Features Section: "Defining MAC address filters"
Virtual Ethernet Interface	Device can locally route IP, IPX, and PPLEtalk between VLANs defined within a single route.	Chapter 13: Configuring Virtual LANs (VLANs) Section: "Routing between VLANs"
VRRP and VRRPE	This release supports the standard route redundancy protocol described in RFC 233.	Chapter 37: Configuring VRRP and VRRPE Section: "Configuring VRRP and VRRPE"
Proxy ARP	Proxy ARP allows the TurboIron device to answer ARP requests from devices on one network on behalf of devices in another network.	Chapter 30: Configuring IP Section: "Enabling Proxy ARP"
IP Load Sharing	This release supports one route to many next hop relationships. It supports 2K ECMP table.	Chapter 30: Configuring IP Section: "Configuring IP load sharing"
RIP V1, V2	Dynamic routing protocol described in RFC 1058 and RFC 2453.	Chapter 33: Configuring RIP Section: "Configuring RIP"
OSPF V2	Dynamic routing protocol described in RFC 2328.	Chapter 35: Configuring OSPF Version 2 (IPv4) Section: "Configuring OSPF Version 2 (IPv4)"

Feature	Description	Described in the <i>FastIron and TurboIron Configuration Guide</i>
IGMP V1, V2, V3	This release introduces the support of IGMP version 3 on Layer 3 Switches.	Chapter 28: Configuring IP Multicast Protocols Section: "IGMP V3"
PIM-SM	Supports features described in RFC 2362.	Chapter 28: Configuring IP Multicast Protocols Section: "PIM Sparse"
PIM-DM	Supports features described in RFC 1075.	Chapter 28: Configuring IP Multicast Protocols Section: "PIM Dense"
MSDP	You must configure a fully meshed topology between MSDP peers. This is mandated for this release because of lack of any EGP that provides a peer RPF check for SA messages.	Chapter 28: Configuring IP Multicast Protocols Section: "Multicast Source Discovery Protocol (MSDP)"
Anycast RP	Anycast RP is a method of providing intra-domain redundancy and load-balancing between multiple Rendezvous Points (RP) in a Protocol Independent Multicast Sparse mode (PIM-SM) network.	Chapter 28: Configuring IP Multicast Protocols Section: "Anycast RP"
ACL for RP candidate	Limits the multicast groups that are covered by a static (RP). It controls the multicast groups for which candidate RPs send advertisement messages to bootstrap routers.	Chapter 28: Configuring IP Multicast Protocols Sections: "Using ACLs to limit static RP groups" & "Using ACLs to limit PIM RP candidate advertisement"
Auto-negotiation of 1G/10G	In this release, if the speed is set to Auto for a 1G port, the port auto-negotiates the flow control with the neighboring port.	Chapter 3: Configuring Basic Software Features Section: "Modifying port speed and duplex mode"
IPv6 Host Support	This release supports IPv6 host management.	Chapter 8: Configuring IPv6 Connectivity Section: "IPv6 management (IPv6 host support)"
L3 SNMP and MIB support	This release supports AES encryption. The SNMP group to which the user account is mapped should be configured before creating the user accounts; otherwise the group will be created without any views.	Chapter 48: Securing SNMP Access Section: "Defining an SNMP user account"

Feature Support

This section describes the feature highlights in this release. Features or options not listed in this section or documented in the *FastIron and TurboIron 24X Configuration Guide* are not supported.

Supported Management Features

This release supports the following management features.

Supported Management Features Category, Description, and Configuration Notes	Supported on TurboIron
802.1X accounting	No
AAA support for console commands	Yes
Access Control Lists (ACLs) for controlling management access	Yes
Alias Command	Yes
Combined DSCP and internal marking in one ACL rule	Yes
Configuring an interface as the source for all TFTP, Syslog, and SNTP packets	No
DHCP Client-Based Auto-Configuration	No
DHCP Server	No
Disabling TFTP Access	Yes
IronView Network Manager (optional standalone and HP OpenView GUI)	Yes
P-Bridge and Q-Bridge MIBs	Yes
Remote monitoring (RMON)	Yes
Retaining Syslog messages after a soft reboot	No
sFlow <ul style="list-style-type: none">For inbound traffic only802.1X username export support for encrypted and non-encrypted EAP types	Yes
sFlow support for IPv6 packets	No
sFlow Version 5	No
Serial and Telnet access to industry-standard Command Line Interface (CLI)	Yes
Show log on all terminals	Yes
SNMP v1, v2, v3	Yes
SNMP V3 traps	Yes
Specifying the maximum number of entries allowed in the RMON Control Table	Yes
Specifying which IP address will be included in a DHCP/BOOTP reply packet	No
Traffic counters for outbound traffic	Yes
Web-based GUI	No

Supported Management Features Category, Description, and Configuration Notes	Supported on TurboIron
Web-based management HTTPS/SSL	No

Supported IPv6 Management Features

This release supports the following IPv6 management features.

Supported IPv6 Management Features Category, Description, and Configuration Notes	Supported on TurboIron
Link-Local IPv6 Address	Yes
IPv6 Access List	No
IPv6 copy	Yes
IPv6 ncopy	Yes
IPv6 debug	Yes
IPv6 ping	Yes
IPv6 traceroute	Yes
DNS server name resolution	Yes
HTTP/HTTPS	No
Logging (syslog)	Yes
RADIUS	Yes
SCP	Yes
SSH	Yes
SNMP v1, v2, v3	Yes
SNTP	Yes
Syslog	Yes
TACACS/TACACS+	Yes
Telnet	Yes
TFTP	Yes
Traps	Yes

Supported Security Features

This release supports the following security features.

Supported Security Features Category, Description, and Configuration Notes	Supported on TurboIron
802.1X port security	Yes
802.1X authentication RADIUS timeout action	Yes
802.1X dynamic assignment for ACL, MAC filter, and VLAN	Yes
Access Control Lists (ACLs) for filtering transit traffic <ul style="list-style-type: none"> Support for inbound ACLs only. These devices do not support outbound ACLs. 	Yes
Address locking (for MAC addresses)	No
AES Encryption for SNMP v3	Yes
AES Encryption for SSH v2	Yes
Authentication, Authorization and Accounting (AAA) <ul style="list-style-type: none"> RADIUS, TACACS/TACACS+ 	Yes
Denial of Service (DoS) protection <ul style="list-style-type: none"> TCP SYN Attacks and ICMP Attacks 	Yes
DHCP Snooping	No
Dynamic ARP Inspection	No
EAP Pass-through Support	No
Enhancements to username and password	Yes
HTTPS	No
IP Source Guard	No
Local passwords	Yes
MAC filter override of 802.1X	Yes
MAC filtering <ul style="list-style-type: none"> Filtering on source and destination MAC addresses 	Yes
Ability to disable MAC Learning	Yes
Flow-based MAC learning	No
MAC port security	Yes
Multi-device port authentication	Yes
Multi-device port Authentication with dynamic ACLs	Yes
Multi-device port authentication with dynamic VLAN assignment	Yes
Multi-device port authentication password override	Yes

Supported Security Features Category, Description, and Configuration Notes	Supported on TurboIron
Multi-device port authentication RADIUS timeout action	Yes
Secure Copy (SCP)	Yes
Secure Shell (SSH) v2 Server	Yes
Packet filtering on TCP Flags	Yes
DHCP Relay Agent information (DHCP Option 82) for DHCP snooping	No
Web Authentication	No

Supported System-Level Features

This release supports the following system-level features.

Supported System –Level Features Category, Description, and Configuration Notes	Supported on TurboIron
10/100/1000 port speed	Yes
1 Gbps and 10 Gbps configurable port speed on fiber ports	Yes
32,000 MAC addresses per switch	Yes
ACL-Based Mirroring	Yes
ACL-Based Rate Limiting <ul style="list-style-type: none"> ACL-based fixed and adaptive rate limiting on inbound ports 	Yes
ACL filtering based on VLAN membership or VE port membership	Yes
ACL logging of denied packets <ul style="list-style-type: none"> ACL logging is supported for denied packets, which are sent to the CPU for logging ACL logging is not supported for permitted packets Packets that are denied by ACL filters are logged in the Syslog based on a sample time-period. 	Yes
ACL statistics	Yes
ACLs to filter ARP packets	No
Asymmetric flow control <ul style="list-style-type: none"> Responds to flow control packets, but does not generate them 	Yes
Auto MDI/MDIX	Yes
Auto-negotiation	Yes
Automatic removal of Dynamic VLAN for 802.1X ports	No

Supported System –Level Features Category, Description, and Configuration Notes	Supported on TurboIron
Automatic removal of Dynamic VLAN for MAC authenticated ports	No
Broadcast, multicast, and unknown-unicast rate limiting	Yes
Boot and reload after 5 minutes at or above shutdown temperature	Yes
Cut-through switching	Yes
DiffServ support	Yes
Digital Optical Monitoring	Yes
Displaying interface names in Syslog	Yes
Displaying TCP/UDP port numbers in Syslog messages	Yes
DSCP Mapping for values 1 through 8	Yes
Dynamic buffer allocation	Yes
Egress buffer thresholds	Yes
Fixed rate limiting <ul style="list-style-type: none"> • Port-based rate limiting on inbound ports. • Fixed rate limiting is supported on 1 Gbps and 10 Gbps Ethernet ports. • Fixed rate limiting is not supported on tagged ports in the full Layer 3 router image. 	Yes
Foundry Discovery Protocol (FDP) / Cisco Discovery Protocol (CDP)	Yes
Generic buffer profile	No
High Availability <ul style="list-style-type: none"> • Layer 2 hitless switchover • Layer 2 hitless Operating System (OS) upgrade 	No
LLDP	Yes
LLDP-MED	No
MAC filter-based mirroring	Yes
Multi-port static MAC address	Yes
Multiple Syslog server logging <ul style="list-style-type: none"> • Up to six Syslog servers 	Yes
Negative temperature setting	Yes
Outbound rate limiting	No
Outbound rate shaping	Yes
Path MTU Discovery support	No

Supported System –Level Features Category, Description, and Configuration Notes	Supported on TurboIron
Port flap dampening	Yes
Port mirroring and monitoring <ul style="list-style-type: none"> • Mirroring of both inbound and outbound traffic on individual ports is supported. 	Yes
Power over Ethernet	No
Priority mapping using ACLs	Yes
Protected link groups	No
Specifying a Simple Network Time Protocol (SNTP) Server	Yes
Specifying the minimum number of ports in a trunk group	Yes
Static MAC entries with option to set traffic priority	Yes
Virtual Cable Testing (VCT) technology <ul style="list-style-type: none"> • Uses Time Domain Reflectometry (TDR) technology to detect and report cable statistics such as; local and remote link pair, cable length, and link status. 	No

Supported Layer 2 Features

This release supports the following Layer 2 features.

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on TurboIron
802.1D Spanning Tree Support <ul style="list-style-type: none">Enhanced IronSpan support includes Fast Port Span and Single-instance SpanTurboIron switches support up to 510 spanning tree instances for VLANs.	Yes
802.1p Quality of Service (QoS) <ul style="list-style-type: none">Strict Priority (SP)Weighted Round Robin (WRR)Combined SP and WRR8 priority queues	Yes
802.1s Multiple Spanning Tree	Yes
802.1W Rapid Spanning Tree (RSTP) <ul style="list-style-type: none">802.1W RSTP support allows for sub-second convergence (both final standard and draft 3 supported)	Yes
802.3ad link aggregation (dynamic trunk groups) <ul style="list-style-type: none">Brocade ports enabled for link aggregation follow the same rules as ports configured for trunk groups.	Yes
ACL-based rate limiting QoS	Yes
BPDU Guard	Yes
Dynamic Host Configuration Protocol (DHCP) Assist	Yes
IGMP v1/v2 Snooping Global	Yes
IGMP v3 Snooping Global	Yes (* ,G and S,G)
IGMP v1/v2/v3 Snooping per VLAN	Yes
IGMP v2/v3 Fast Leave (membership tracking)	Yes
IGMP Filters	Yes
Interpacket Gap (IPG) adjustment	Yes
Jumbo frames <ul style="list-style-type: none">10/100/1000 and 10-Gigabit Ethernet portsUp to 9216 bytes	Yes
LACP <ul style="list-style-type: none">LACP trunk group ports follow the same configuration rules as for statically	Yes

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on TurboIron
configured trunk group ports. <ul style="list-style-type: none"> • Support for single link LACP 	
Link Fault Signaling (LFS) for 10-Gigabit Ethernet ports	Yes
MAC-Based VLANs Dynamic MAC-Based VLAN Activation	No
Metro Ring Protocol 1 (MRP 1)	Yes
Metro Ring Protocol 2 (MRP 2)	Yes
MLD Snooping V1/V2 <ul style="list-style-type: none"> • 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 	No
Multicast static group traffic filtering (for snooping scenarios)	No
PIM-SM V2 Snooping	Yes
PVST/PVST+ compatibility	Yes
PVRST+ compatibility	Yes
Remote Fault Notification (RFN) for 10-Gigabit Ethernet ports	No
Root Guard	Yes
Super Aggregated VLANs	Yes
Trunk groups <ul style="list-style-type: none"> • Trunk threshold for static trunk groups • Flexible trunk group membership 	Yes
Topology groups	Yes
Uni-directional Link Detection (UDLD) (Link keepalive)	Yes
Uplink Ports Within a Port-Based VLAN	Yes
VLAN Support on TurboIron Devices: <ul style="list-style-type: none"> • 4096 maximum VLANs • Dual-mode VLANs • 802.1Q with tagging • Port-based VLANs • VLAN groups • Private VLANs 	Yes

Supported Layer 2 Features Category, Description, and Configuration Notes	Supported on TurboIron
VLAN Q-in-Q Tagging (tag-type 8100 over 8100 encapsulation)	Yes
VLAN-based mirroring	No
VoIP Auto-configuration and CDP	No
Virtual Switch Redundancy Protocol (VSRP)	Yes
VSRP-Aware security features	Yes
VSRP and MRP signaling	Yes
VSRP Fast Start	Yes
VSRP timer scaling	Yes

Supported Layer 3 Features

This release supports the following Layer 3 features.

Supported Layer 3 Features Category, Description, and Configuration Notes	Supported on TurboIron
Anycast RP	Yes
IGMP V1, V2, and V3	Yes
IP helper	Yes
IP multicast routing protocols: PIM-SM and PIM-DM <ul style="list-style-type: none"> DVMRP is not supported 	Yes
ICMP Redirect messages	Yes
Multiprotocol Source Discovery Protocol (MSDP)	Yes
OSPF V2 (IPv4)	Yes
RIP V1 and V2 <ul style="list-style-type: none"> Static RIP support only. The Brocade device with the base Layer 3 does not learn RIP routes from other Layer 3 devices. However, the device does advertise directly connected routes. 	Yes
Route-only support <ul style="list-style-type: none"> Disabling Layer 2 Switching at the CLI Interface level as well as the Global CONFIG level. This feature is not supported on virtual interfaces. 	Yes
Routing for directly connected IP subnets	Yes
Static IP Routing	Yes
Virtual Interfaces	Yes

Supported Layer 3 Features Category, Description, and Configuration Notes	Supported on TurboIron
<ul style="list-style-type: none"> Up to 255 virtual interfaces 	
VRRP	Yes
VRRP-E	Yes

Note: Layer 3 features not listed under “Layer 3 Features” are not supported.

Image Files for IronWare R04.2.00b

The following Software Image Files are available for IronWare R04.2.00b.

Device	Boot Image	Flash Image
TurboIron 24X Series	GRZ04100.bin	TIS04200b.bin (Layer 2) TIR04200b.bin (Layer 3)

Factory Pre-loaded Software

This table lists the software that is factory-loaded into the primary and secondary flash areas on the device. All images are included on the CD-ROM shipped with the device.

Model	Software Images	
	Primary Flash	Secondary Flash
TurboIron 24X Series	Layer 2	Layer 2

Note: For Layer 3 image, go to myBrocade.com, click the Product Documentation tab, then click on the link to the Knowledge Portal (KP). Download the image from the KP and follow the steps below to upgrade the software image.

Upgrading software images

Upgrading the Boot Code

- Place the new boot code on a TFTP server to which the Brocade device has access.
- Enter the following command at the Privileged EXEC level of the CLI (example: FastIron Switch#) to copy the boot code from the TFTP server into flash memory:
copy tftp flash <ip-addr> <image-file-name> bootrom
- Use the **copy tftp flash** command to copy the boot code to the Brocade device only during a maintenance window. Attempting to do so during normal networking operations can cause disruption to the network.

4. Verify that the code has been successfully copied by entering the following command at any level of the CLI:

show flash

5. The output will display the compressed boot ROM code size and the boot code version.
6. Upgrade the flash code as instructed in the following section.

Upgrading the Flash Code

1. Place the new flash code on a TFTP server to which the Brocade device has access.
2. Enter the following command at the Privileged EXEC level of the CLI (example: `FastIron#`) to copy the flash code from the TFTP server into the flash memory:
`copy tftp flash <ip-addr> <image-file-name> primary | secondary`
3. Verify that the flash code has been successfully copied by entering the following command at any level of the CLI:

show flash

4. If the flash code version is correct, go to Step 5. Otherwise, go to Step 1.
5. Reload the software by entering the following command:

reload

(The **reload** command boots from the default boot source, which is the primary flash area by default)

Technical Support

Contact your switch supplier for 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
- Switch model
- Switch operating system 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 and the results

2. Switch Serial Number

Additional Resources

Below are some additional publications you can reference to find more information on the products supported in this software release.

Title	Contents
<i>FastIron and TurboIron 24X Configuration Guide</i>	Provides configuration procedures for system-level features, enterprise routing protocols, and security features.
<i>Brocade TurboIron 24X Series Hardware Installation</i>	Provides the following information: <ul style="list-style-type: none"><li data-bbox="690 531 950 562">• Product Overview<li data-bbox="690 573 1015 604">• Installation instructions<li data-bbox="690 615 1031 646">• Hardware Specifications

Defects

This section lists closed and opened defects in Multi-Service IronWare R04.2.00 releases for the TurboIron 24X.

Closed Defects in IronWare R04.2.00b

None.

Closed Defects in IronWare R04.2.00a

Defect ID: DEFECT000308117	Technical Severity: Medium
Summary: The TurboIron still learns MAC addresses even with mac-learn-disable configured.	
Feature: TI L2 Forwarding	Function: Transparent FW Mode
Reported In Release: FI TI 04.2.00	Service Request ID: 253798

Defect ID: DEFECT000309646	Technical Severity: Medium
Summary: The following error may be seen when applying multiple MAC filters “Error: Insufficient hardware resource for binding the MAC filters to interface”	
Symptom: MAC filters are not working.	
Feature: TI ACL	Function: L2 ACL
Reported In Release: FI TI 04.2.00	Service Request ID: 257030

Closed Defects in IronWare R04.2.00

This section lists defects closed with code in TurboIron R04.2.00.

Defect ID: DEFECT000297073	Technical Severity: Medium
Summary: If we use command dm pp-trunk-hash with invalid port number "o", then it will crash the switch.	
Risk of Fix: Low	Probability: Medium
Feature: TI LAG	Function: CLI
Reported In Release: FI TI 04.1.00	Service Request ID: 246229

Open Defects in IronWare R04.2.00

This section lists open defects in TurboIron R.04.2.00

Defect ID: DEFECT000287823	Technical Severity: High
Summary: When deleting a virtual link in an area, all virtual links get deleted.	
Symptom: When deleting a virtual link in an area, “show ip ospf virtual-neighbor” would show that there are no virtual-neighbor.	
Workaround: Re-add the ones you still need	
Feature: TI L3 Protocol	Function: OSPF
Reported In Release: FI TI 04.2.00	

Defect ID: DEFECT000283393	Technical Severity: Medium
Summary: Mac-authentication disable-aging command at global config level overrides the local Mac-authentication disable-aging command configured on the individual ports.	
Symptom: Mac-authentication disable-aging command configured on local individual ports will be lost on configuring the mac-authentication disable-aging command at global config level.	

Feature: Mac Authentication	Function: Security
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000285769	Technical Severity: Medium
Summary: If broadcast or multicast or unknown-unicast rate limit is configured on primary trunk port, it is not applied to secondary trunk ports	
Symptom: If broadcast/multicast/unknown-unicast rate limit is configured on the primary trunk port, it is not applied to secondary trunk ports	
Feature: TI QOS	Function: Port Based Ingress Rate Limiting
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000287692	Technical Severity: Medium
Summary: Mac filter applied using the 802.1x mac filter override command is not removed when the mac-filter is deleted from cli.	
Symptom: The running config does not contain the mac-filter, yet 802.1x has the mac-filter applied on the port.	
Workaround: Remove the 802.1x mac filter override when deleting the mac filter.	
Feature: TI Security	Function: Dot1x
Reported In Release: FI TI 04.2.00	Probability: Low

Defect ID: DEFECT000289081	Technical Severity: Medium
Summary: Rootguard enabled port changes state between "blocking" and "learning" periodically.	
Symptom: RootGuard enabled port keeps changing states between "blocking" and "learning"	
Workaround: Does not affects any functionality	
Feature: TI L2 Protocol	Function: Root Guard
Reported In Release: FI TI 04.2.00	Probability: High

Defect ID: DEFECT000290350	Technical Severity: Medium
Summary: CLI allows configuring a port with ACL to be tagged in a VLAN, which is not supported	
Symptom: CLI allows configuring a port with ACL to be tagged in a VLAN. This is not a supported configuration. Also, if one saves the config and reload the Router/Switch, an error will appear at boot-up and the configuration will be removed.	
Workaround: User should remove acl on a port before adding it as a tagged member to a VLAN.	
Feature: TI ACL	Function: IPv4
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000290572	Technical Severity: Medium
Summary: "no lldp adv mana ipv4 <ip-add> ports all" does not remove the management IP address from LLDP advertisements.	
Symptom: The management IP address is always advertised to peers in the LLDPDU even after entering this command.	
Workaround: Does not affects any other functionality	
Feature: TI System Protocols	Function: LLDP
Reported In Release: FI TI 04.2.00	Probability: High

Defect ID: DEFECT000290821	Technical Severity: Medium
Summary: The acl-logging command on multiple ports with the same ACL ID, will not work correctly	
Symptom: The acl-logging command on multiple ports with the same ACL ID, will not work correctly. You cannot enable acl-logging on some ports and disable acl-logging on other ports if they share the same ACL ID.	
Workaround: When using acl-logging, create a unique ACL for each port if you do not want to enable it on all the ports.	

Feature: TI ACL	Function: ACL Deny Logging
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000298123	Technical Severity: Medium
Summary: If a mac-filter is configured on a port and then 802.1x attaches another mac-filter on the same port, then 802.1x does not allow the original mac-filter to be removed.	
Symptom: Removal of mac-filters applied before 802.1x authentication is not smooth when 802.1x itself attaches a mac filter on that port.	
Workaround: Disable 802.1x on the port. Now you should be able to remove the mac filter from that port.	
Feature: TI Security	Function: Dot1x
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000298129	Technical Severity: Medium
Summary: 802.1x allows only 1 host to apply dynamic Mac filters on the port, and rejects all other hosts with a dynamic Mac filter	
Symptom: Multiple hosts with dynamic mac filters cannot be authenticated using 802.1x. Only the first one with dynamic mac filter is authenticated. Later hosts with dynamic mac filters are not authenticated.	
Workaround: 802.1x with Dynamic MAC Filters can only be used for 1 host per port.	
Feature: TI Security	Function: Dot1x
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000298899	Technical Severity: Medium
Summary: On Dual mode ports, even though a host is supposed to be authenticated only on tagged vlan, it gets authenticated for both tagged as well as untagged (dual-mode) vlans.	
Symptom: If the port receives untagged traffic, the host is authenticated on untagged vlan as well and this traffic is allowed by the port. This traffic should have been dropped.	
Workaround: Do not configure dual-mode on a port that has dynamic VLAN configured for mac authentication.	
Feature: TI Security	Function: Dot1x
Reported In Release: FI TI 04.2.00	Probability: Medium

Defect ID: DEFECT000287700	Technical Severity: Medium
Summary: Removing dual-mode configuration from a port may not remove ACL in dual-mode vlan permanently	
Symptom: Upon deletion and creation of 'dual-mode' configuration of a port, ACL configured previously (before deletion) re-appears automatically on the port.	
Workaround: Remove the per-vlan ACL on the port for the dual-mode port first, then remove the dual-mode configuration (OR) remove the unwanted per-vlan ACL after re-enabling the dual-mode on a port.	
Feature: TI ACL	Function: IPv4
Reported In Release: FI TI 04.2.00	Probability: Low