145 Rio Robles
San Jose, CA 95134
+1 877-801-7082

Customer Release Notes

7100-Series®

Firmware Version 8.31.01.0006
September 2014

INTRODUCTION:

This document provides specific information for version 8.31.01.0006 of firmware for the Enterasys 7100-Series products:

7100-Series Chassis			
71K11L4-48	71K11L4-24	71K91L4-48	71K91L4-24
71G21K2L2-48P	71G21K2L2-24P24	71G11K2L2-48	

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at: http://support.extremenetworks.com/

PRODUCT FIRMWARE SUPPORT:

Status	Firmware Version	Product Type	Release Date
Current Version	8.31.01.0006	Customer Release	September 2014
Previous Version	8.22.03.0006	Customer Release	July 2014
Previous Version	8.22.02.0012	Customer Release	June 2014
Previous Version	8.21.03.0001	Customer Release	January 2014
Previous Version	8.21.01.0002	Customer Release	December 2013
Previous Version	7.91.03.0007	Customer Release	July 2013
Previous Version	7.91.02.0006	Customer Release	March 2013
Previous Version	7.91.01.0001	Customer Release	December 2012

HIGH AVAILABILITY UPGRADE (HAU) FW COMPATIBILITY:

This version is not HAU compatible with previous versions.

HAU Key for this release: c7377aad29222273d825db43aecde796f1035b5a

The HAU key is reported using the CLI command “dir images”.

HARDWARE COMPATIBILITY:

This version of firmware is supported on all hardware revisions.

BOOT PROM COMPATIBILITY:

This version of firmware is compatible with all boot prom versions.

INSTALLATION INFORMATION:

System Minimum FW Version Required:

7100-Series Chassis			
Model	**Minimum FW Version**	**Model**	**Minimum FW Version**
71K11L4-48	07.91.01.0001	71G21K2L2-48P	08.21.01.0002
71K11L4-24		71G21K2L2-24P24	
71K91L4-48		71G11K2L2-48	08.22.02.0012
71K91L4-24			

It is recommended that the latest version of firmware be downloaded and the system be upgraded to the latest version of firmware prior to installation.

System Behavior

71G21K2L2-48P / 71G21K2L2-24P24 / 71G11K2L2-48 Supported Port Configurations

The 7100G-Series models (71G21K2L2-48P, 71G21K2L2-24P24, and 71G11K2L2-48) do not support all combinations of front panel 10/100Mb, Gigabit, 10 Gigabit, and 40 Gigabit port configurations. The dual QSFP+ ports must both be configured as 40Gb Ethernet / VSB interconnect ports or either both as 4 x 10Gb Ethernet ports. When the two QSFP+ ports are configured as 4 x 10Gb Ethernet ports, the two SFP+ ports are not available for use and will be reported as not present.

Supported port configurations are shown in the table below.

7100G-Series Model	RJ45 Triple Speed PoE+ Ports	SFP 100Mb/1Gb Ports	SFP+ 1/10Gb Ethernet Ports	QSFP+	
				10Gb Ethernet Ports (4x10Gb Mode)	40Gb Ethernet or VSB Ports
71G21K2L2-48P	48	-	2	-	2
	48	-	-	8	-
71G21K2L2-24P24	24	24	2	-	2
	24	24	-	8	-

71G11K2L2-48	-	48	2	-	2
	-	48	-	8	-

Half-Duplex Port Operation
The 7100-Series does not support half-duplex port configuration at any speed.

Supported 10GBASE-T Port Speeds
10GBASE-T ports on 71K91L4-24 and 71K91L4-48 support 100Mb/1Gb/10Gb speeds.

7100-Series Policy Capacities
Up to 63 policy profiles are supported by the 7100-Series.

Each 7100-Series chassis has an authenticated user capacity of 512 MAC or port addresses. A VSB stack of 8 7100s has an authenticated user capacity of 4096 (8x512) MAC or port addresses

7100-Series User Capacities:

Chassis Type	Maximum Authenticated MAC Address Capacity
71K11L4-48	512
71K11L4-24	512
71K91L4-48	512
71K91L4-24	512
71G21K2L2-48P	512
71G21K2L2-24P24	512
71G11K2L2-48	512

Policy Resource Allocation Profile - The user can configure the policy resource allocation limits by selecting a profile from a predefined profile list using the “set limits resource-profile” command. The predefined profiles are “default” and “router1”. The “router1” profile allows for ingress ACL/PBR support.

```
TOR(su)->set limits resource-profile ?
  default                  Default allocation profile
  router1                  Router1 allocation profile
```

Policy Rule Traffic Classification Group	Maximum Policy Rule Capacity per Group: Default profile	Maximum Policy Rule Capacity per Group: Router1 profile
macsource macdest	128	0
ipv6dest	128	0
ipsourcesocket ipdestsocket udpsourceportIP udpdestportIP tcpsourceportIP tcpdestportIP ipttl	249	249

Policy Rule Traffic Classification Group	Maximum Policy Rule Capacity per Group: Default profile	Maximum Policy Rule Capacity per Group: Router1 profile
iptos iptype		
ethertype vlantag tci port	175	175

7100-Series Virtual Switch Bonding (VSB) Implementation Guidelines

Up to 8 7100-Series systems can be bonded using VSB, in any mix of chassis types.

VSB Support on Port Types - Only 40 Gigabit ports can be used as VSB interconnect ports. 10 Gigabit and 1 Gb ports can only be used as LFR ports. LFR is supported for VSB virtual stacks up to 8 systems.

Any port configured for VSB or LFR should only have bonding related configuration applied.

A closed ring VSB interconnect is not required, but if you do not close the ring and an interconnect or a system failure occurs, the remaining systems could be divided, causing two systems to reside in your network with the same IP address. LFR is highly recommended if a closed ring VSB topology is not used.

When replacing a system in a VSB stack you can restore the port level configuration by appending the configuration with the configuration from a previously stored configuration file when the chassis was operational within the stack, using the **configure** *filename* **append** command**.**

Port Mirroring

The 7100-Series device supports traffic mirroring for a maximum of 2 destination ports for mirrors.
A mirror could be a:

- “One-to-one” port mirror
- “One-to-many” port mirror
- “Many-to-one” port mirror

This allows configurations like: (a) up to two one-to-one mirrors, (b) up to two many-to-one mirrors, or (c) a single one-to-two mirror.

For the “one-to-many” there can be up to 2 destination ports.
For the “many-to-one” there is no limit to the number of source ports.
For the port mirror case the source ports(s) can be a physical port or VLAN.
LAG ports can not be used as the source port for a mirror.
Mirror destinations can be physical ports or LAGs, including ones on other switches in the same stack. Mirror destinations can not be VLANs.
The port and VLAN mirror function does not mirror error frames.

Mirroring egress traffic results in the mirrored traffic always having an 802.1Q VLAN tag. The VLAN and priority values are the ones used for transmission of the original packet.

Note that the examples above are provided to illustrate the number and types of mirrors we support, as well as how they can be used concurrently. The mirror configurations are not limited to these examples.

Class of Service:

Class of Service (CoS) is supported with and without policy enabled. Policy provides access to classes 8-255. Without policy, classes 0-7 are available. They are not allowed to be changes as these are the default 802.1Q mappings for priority to queue.

Class of Service Support:

- Supports up to 256 Classes of Service
- ToS rewrite
- 802.1D/P Priority
- 9 Transmit Queues per port (8 customer and 1 internal reserved for control-plane traffic)
  - Queues support Strict, WFQ, ETS, and Hybrid Arbitration
  - All queues support rate-shaping
- 16 Inbound-Rate-Limiters per port
- Support for Flood-Limiting controls for Broadcast, Multicast, and Unknown Unicast per port.
- Management
  - Support for Enterasys CoS MIB

No support for Outbound-Rate-Limiters

Link Aggregation (LAG)

The 7100-Series chassis supports a total of 64 LAGs per chassis with up to 8 ports per LAG.

Multi-User 802.1X

Authentication of multiple 802.1X clients on a single port is supported. This feature will only operate correctly when the intermediate switch forwards EAP frames, regardless of destination MAC address (addressed to either unicast or reserve multicast MAC).

To be standards compliant, a switch is required to filter frames with the reserved multicast DA. To be fully multi-user 802.1X compatible, the intermediary switch must either violate the standard by default or offer a configuration option to enable the non-standard behavior. Some switches may require the Spanning Tree Protocol to be disabled to activate pass-through.

Use of a non-compatible intermediary switch will result in the 802.1X authenticator missing multicast destined users' logoff and login messages. Systems used by multiple consecutive users will remain authenticated as the original user until the re-authentication period has expired.

The multi-user 802.1X authenticator must respond to EAP frames with directed (unicast) responses. It must also challenge new user MAC addresses discovered by the multi-user authentication/policy implementation.

Compatible supplicants include Microsoft Window XP/2000/Vista, Symantec Sygate Security Agent, and Check Point Integrity Client. Other supplicants may be compatible.

The enterasys-8021x-extensions-mib and associated CLI will be required to display and manage multiple users (stations) on a single port.

This version of firmware does not support retrying MAC address authentication for failed stations, or renewing MAC address authentications for successful ones.

RMON Statistics:

Oversized packets are not counted on a port that is not enabled for jumbo frames.

If this oversized packet has an invalid CRC, it will be considered a jabber packet rather than an oversized packet.

SMON Guidelines:

The 7100-Series does not support port-VAN or LAG ports for SMON statistics collection.

Flash File System:

If for any reason the flash file system become seriously corrupted and nonfunctional the flash file system can be reformatted and the firmware image reloaded. Call Enterasys support.

Scale and Capacity Limits

Each release of 7100-Series firmware contains specific features and associated capacities or limits. The CLI command "show limits" provides a detailed description of the features and capacity limits available on your specific HW. Please use this command to get a complete list of capacities for this release.

	7100-Series	
ARP Entries (per router / per chassis)	4K	
Static ARP Entries	512	
IPv4: Route Table Entries	12000	
IPv6: Route Table Entries (/64)	6000	
IPv4: Router interfaces	256	
IPv6: Router interfaces	256	
OSPF Areas	8	
OSPF LSA(s)	12000	
OSPF Neighbors	60	
Static Routes	1024	
RIP Routes	2500	
Configured RIP Nets	300	
VRRP Interfaces	256	
ACLs	Resource Profile - **default**	Resource Profile - **router1**
IPv4 Ingress Access-Group Rules	0	128
IPv4 Egress Access-Group Rules	256	256
IPv6 Ingress Access-Group Rules	0	128
IPv6 Egress Access-Group Rules	256	256
Policy Based Routing (PBR) Entries (IPv4 only)	0	50
IPv4 Route-Map (Rules for all PBR entries)	0	128
ECMP Paths	8	
Static VRFs	128	
Dynamic VRFs	64	
Secondaries per Interface	128	
Total Primary + Secondary Interfaces per Router	512	
IP Helper addresses (per router/ per interface)	5120 / 20	
SPBv (constrained by 4094 VLANs)	Up to 100 VLANs mapped as base VIDs	Up to 100 SPBv nodes in SPB region

Multicast Capacities

IGMP/MLD Static Entries	64
IGMP/MLD *,G and S,G Groups	4K
IGMP/MLD Snooping Flow Capacity	4K

Multicast Routing (PIM/DVMRP flows)	2K
IGMP/MLD Clients[1]	64K

[1] A client is defined as a reporter subscribing to a *, G or S, G group, or sourcing a multicast flow.

DHCP Capacities

DHCP Server Leases	5000
DHCP Pools	100

Some of these limits may **not** be enforced by the firmware and may cause unknown results if exceeded.

Advanced Routing License Feature

The 7100-Series Advanced Routing License license adds routing features to the 7100-Series.

7100-Series Chassis	Advanced Routing License	Licensed Features
71K11L4-48	71A-EOS-ADVL3	OSPFv2/v3, PIM-SM, PIM-SMv6, PIM-DM, PIM-SSM, PIM-SSMv6, BGP, ISIS, Fabric Routing, VRF
71K11L4-24		
71K91L4-48		
71K91L4-24		
71G21K2L2-48P	71A-EOS-G-ADVL3	
71G21K2L2-24P24		
71G11K2L2-48		

An advanced routing license is required per chassis in a VSB stack.

Virtual Switch Bonding (VSB) License

No License is required for VSB support in the 7100-Series.

NETWORK MANAGEMENT SOFTWARE:

NMS	Version No.
NetSight Suite	5.1 or greater

NOTE: If you install this image, you may not have control of all the latest features of this product until the next version(s) of network management software. Please review the software release notes for your specific network.

PLUGGABLE PORTS SUPPORTED:

100Mb Optics: Supported on 7100G SFP ports only – 71G21K2L2-24P24 & 71G11K2L2-48

SFP Optics	Description
MGBIC-N-LC04	100 Mb, 100Base-FX, IEEE 802.3 MM, 1310 nm Long Wave Length, 2 Km, LC SFP
MGBIC-LC04	100 Mb, 100Base-FX, IEEE 802.3 MM, 1310 nm Long Wave Length, 2 Km, LC SFP
MGBIC-LC05	100 Mb, 100Base-LX10, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 Km, LC SFP

1Gb Optics:

MGBICs	Description
MGBIC-LC01	1 Gb, 1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550 M, LC SFP
MGBIC-LC03	1 Gb, 1000Base-SX-LX/LH, MM, 1310 nm Long Wave Length, 2 Km, LC SFP
MGBIC-LC07	1 Gb, 1000Base-EZX, IEEE 802.3 SM, 1550 nm Long Wave Length, 110 Km, LC SFP (Extended Long Reach)
MGBIC-LC09	1 Gb, 1000Base-LX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 Km, LC SFP
MGBIC-02	1 Gb, 1000Base-T, IEEE 802.3 Cat5, Copper Twisted Pair, 100 m, RJ 45 SFP
MGBIC-08	1 Gb, 1000Base-LX/LH, IEEE 802.3 SM, 1550 nm Long Wave Length, 80 km, LC SFP
MGBIC-BX10-U	1 Gb, 1000Base-BX10-U Single Fiber SM, Bidirectional 1310nm Tx / 1490nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-D)
MGBIC-BX10-D	1 Gb, 1000Base-BX10-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-U)

10Gb Optics:

SFP+ Optics	Description
10GB-SR-SFPP	10 Gb, 10GBASE-SR, IEEE 802.3 MM, 850 nm Short Wave Length, 33/82 m, LC SFP+
10GB-LR-SFPP	10 Gb, 10GBASE-LR, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 km, LC SFP+
10GB-ER-SFPP	10 Gb, 10GBASE-ER, IEEE 802.3 SM, 1550 nm Long Wave Length, 40 km, LC SFP+
10GB-LRM-SFPP	10 Gb, 10GBASE-LRM, IEEE 802.3 MM, 1310 nm Short Wave Length, 220 m, LC SFP+
10GB-ZR-SFPP	10 Gb, 10GBASE-ZR, SM, 1550 nm, 80 km, LC SFP+
10GB-USR-SFPP	10Gb, 10GBASE-USR MM 850nm, LC SFP+
10GB-BX10-D	10Gb, Single Fiber SM, Bidirectional, 1330nm Tx / 1270nm Rx, 10 km SFP+
10GB-BX10-U	10Gb, Single Fiber SM, Bidirectional, 1270nm Tx / 1330nm Rx, 10 km SFP+
10GB-BX40-D	10Gb, Single Fiber SM, Bidirectional, 1330nm Tx / 1270nm Rx, 40 km SFP+
10GB-BX40-U	10Gb, Single Fiber SM, Bidirectional, 1270nm Tx / 1330nm Rx, 40 km SFP+
10GB-LR271-SFPP	10G Gb, CWDM SM, 1271 nm, 10 km, LC SFP+
10GB-LR291-SFPP	10G Gb, CWDM SM, 1291 nm, 10 km, LC SFP+
10GB-LR311-SFPP	10G Gb, CWDM SM, 1311 nm, 10 km, LC SFP+
10GB-LR331-SFPP	10G Gb, CWDM SM, 1331 nm, 10 km, LC SFP+
SFP+ Direct Attach Copper Cables	**Description**
10GB-C01-SFPP	10Gb pluggable copper cable assembly with integrated SFP+ transceivers, 1 m
10GB-C03-SFPP	10Gb pluggable copper cable assembly with integrated SFP+ transceivers, 3 m
10GB-C10-SFPP	10Gb pluggable copper cable assembly with integrated SFP+ transceivers, 10 m
SFP+ Laserwire	**Description**
10GB-LW-SFPP	SFP+ Laserwire Transceiver Adapter

10GB-LW-03	Laserwire Cable 3 m
10GB-LW-05	Laserwire Cable 5 m
10GB-LW-10	Laserwire Cable 10 m
10GB-LW-20	Laserwire Cable 20 m
SFP+ Direct Attach Active Optical Cables	**Description**
10GB-F10-SFPP	10Gb Active optical direct attach cable with integrated SFP+ transceivers, 10m
10GB-F20-SFPP	10Gb Active optical direct attach cable with integrated SFP+ transceivers, 20m

40Gb Transceivers:

QSFP+ Optics	Description
40GB-SR4-QSFP	40Gb, 40GBASE-SR4, MM 100m OM3, MPO QSFP+ Transceiver
40GB-ESR4-QSFP	40Gb, Extended Reach SR4, MM, 300m OM3, MPO QSFP+
40GB-LR4-QSFP	40Gb, 40GBASE-LR4, SM 10km LC QSFP+ Transceiver
QSFP+ Direct Attach	**Description**
40GB-C0.5-QSFP	40Gb, Copper DAC with integrated QSFP+ transceivers, 0.5m
40GB-C01-QSFP	40Gb, Copper DAC with integrated QSFP+ transceivers, 1m
40GB-C03-QSFP	40Gb, Copper DAC with integrated QSFP+ transceivers, 3m
40GB-C07-QSFP	40Gb, Copper DAC with integrated QSFP+ transceivers, 7m
40GB-F10-QSFP	40Gb, Active Optical DAC with integrated QSFP+ transceivers, 10m
40GB-F20-QSFP	40Gb, Active Optical DAC with integrated QSFP+ transceivers, 20m
10GB-4-C03-QSFP	10Gb, Copper DAC Fan out, 4xSFP+ to QSFP+, 3m
10GB-4-F10-QSFP	10Gb, Active Optical DAC, 4xSFP+ to QSFP+, 10m
10GB-4-F20-QSFP	10Gb, Active Optical DAC, 4xSFP+ to QSFP+, 20m
QSFP+ Adapter	**Description**
QSFP-SFPP-ADPT	QSFP+ to SFP+ Adapter

See the Pluggable Transceivers data sheet for detailed specifications of supported transceivers.

Only Enterasys 40 Gigabit optical transceivers are supported. Use of any other transceiver types will result in an error.

Example Message for 40G cables that are unrecognized or unauthenticated

```
-   System[1]port fg.1.4 contains an unauthenticated pluggable
    module('manufacturer'/'part no.')
```

Example port hold-down message for unauthenticated 40G optical transceiver

```
-   System[1]port fg.1.4 will remain down because the pluggable
    module('manufacturer'/'part no.') is not supported
```

Auto Configuration of 4 x 10Gb Mode

The 7100-Series will recognize a 10GB-4-xxx-QSFP cable when inserted in a QSFP+ port and reconfigure a QSFP+ port to 4 x 10 Gigabit Ethernet. A system reset is required for the port speed change to take effect.

Example messages if the device installed in the QSFP+ port does not match the current configured mode:

```
-   System[1]port tg.1.49 contains a 40GB MAU but is currently in 4x10GB mode and
    will remain down until system is reset
```

```
-   System[1]port fg.1.1 contains a 4x10GB MAU but is currently in 40GB mode and
    will remain down until system is reset
```

QSFP-SFPP-ADPT transceiver support:

The QSFP-SFPP-ADPT allows the use of a single SFP or SFP+ transceiver in a QSFP+ port. The 10GB-LRM-SFPP transceiver is not supported when plugged into a QSFP+ port via a QSFP-SFPP-ADPT. If an attempt is made to operate the tranceiver the following error is logged:

```
port <port-name> will remain down because the pluggable module('<vendor>'/'<part-
number>') is not supported  and the port will remain operationally down.
```

Gigabit Support on QSFP+ ports:

When using the QSFP-SFPP-ADPT adapter on the 7100-Series, Gigabit port speed can be configured and a single Gigabit SFP can be used. When configured for Gigabit port speed, only the MGBIC-LC01 and MGBIC-LC09 Gigabit SFP transceivers are supported with the QSFP-SFPP-ADPT.

SFP and SFP+ Dual speed operation:

The SFP+ ports support the use of SFP+ transceivers and SFP transceivers. (10Gb/1Gb)
SFP ports on the 7100G-Series models support the use of SFP transceivers and 100Mb transceivers. (1Gb/100Mb)

NOTE: Installing third party or unknown pluggable ports may cause the device to malfunction and display MGBIC description, type, speed and duplex setting errors.

SUPPORTED FUNCTIONALITY:

Features		
Multiple Authentication Types Per Port - 802.1X, PWA+, MAC	Layer 2 through 4 VLAN Classification	Entity MIB
Multiple Authenticated Users Per Port - 802.1X, PWA+, MAC	Layer 2 through 4 Priority Classification	ICMP
SNTP	Dynamic VLAN/Port Egress Configuration	Auto MDI-X Media Dependent Interface Crossover Detect (Enhanced for non auto negotiating ports)
Web-based configuration (WebView)	Ingress VLAN Tag Re-write	DHCP Server
Multiple local user account management	VLAN-to-Policy Mapping	Jumbo Frame support
Denial of Service (DoS) Detection	RMON – Statistic, History, Alarms, Events,	Directed Broadcast
802.1X – Authentication	SMON – VLAN and Priority Statistics	Cisco CDP v1/2
802.1D – 1998	Distributed Chassis Management (Single IP Address)	CLI Management
802.1Q – Virtual Bridged Local Area Networking	SNMP v1/v2c/v3	RADIUS (Accounting, Snooping)
GARP VLAN Registration Protocol (GVRP)	IEEE 802.1ak MVRP (Multiple VLAN Registration Protocol)	Split RADIUS management and authentication
802.1p – Traffic Class Expediting	MAC locking (Static/Dynamic)	Port Mirroring
802.1w – Rapid Reconfiguration of Spanning Tree	Node/Alias table	Link Flap detection
802.1s – Multiple Spanning Trees	SSH v1/v2	Daylight Savings Time
802.1t – Path Cost Amendment to 802.1D	Audit trail logging	RFC 3580 with Policy support
802.3 – 2002	RADIUS Client	IPv6 Node Alias Support

Features		
802.1AX-2008 Link Aggregation (formerly 802.3ad)	FTP/TFTP Client	Virtual Switch Bonding (VSB) with Link Failure Response (LFR) links
802.3x – Flow Control	Telnet – Inbound/Outbound	Unidirectional Link Detection (ULD)
Broadcast Suppression	Configuration File Upload/Download	Configurable login banner
Ingress Rate Limiting	Text-based Configuration Files	High Availability FW Upgrades
Transmit queue shaping	Syslog	Type of Service (ToS) Re-write
Strict and Weighted Round Robin Queuing	Span Guard	802.3-2008 Clause 57 (Ethernet OAM – Link Layer OAM)
IGMP v1/v2/v3 and Querier support	Cabletron Discovery Protocol (CDP)	Path MTU Discovery
SMON Port and VLAN Redirect ?	LLDP and LLDP-MED	Secure Copy Protocol (SCP)
Spanning Tree Loop Protection	MLDv1/MLDv2	TACACS+
Data Center Bridging 802.1Qaz Enhanced Transmission Selection (ETS), Data Center Bridging Exchange Protocol (DCBx), Application Priority	Data Center Bridging 802.1Qbb Priority Flow Control (PFC)	Data Center Bridging 802.1Qau Congestion Notification (CN)
IP Routing	DVMRPv3	OSPF/OSPFv3
Static Routes	RIP ECMP, CIDR configuration	OSPF ECMP
Protocol Independent Multicast - Sparse Mode (PIM-SM) IPv4/v6	Virtual Router Redundancy Protocol (VRRP) v2/v3	OSPF Alternate ABR
RIP v2	Policy-Based Routing	Graceful OSPF Restart (RFC 3623)
Proxy ARP	DHCP Server	Passive OSPF support
Basic Access Control Lists	DHCP Relay w/option 82	OSPF NSSA, equal cost multi-path
Extended ACLs	Static Multicast Configuration	Bidirectional Forwarding Detection (BFD)
iBGP	BGP Route Reflector	eBGP
BGP Graceful Restart	BGP Route Refresh	BGP 4 byte AS number
IPv6 Policy Based Routing	IPv6 Static Routing	BGP Extended Communities
PIM-SSM IPv4/v6	PIM-DM IPv4/v6	IPv6 ACLs
Tracked Objects	IPv6 DHCP Relay	IP Source Guard
VLAN Provider Bridging (Q-in-Q	IPsec support for OSPFv3	RIPng
Anti-spoofing User Tracking and Control	ISIS	IPv6 Node Alias Support
IEEE 802.1Q-2011 Connectivity Fault Management (CFM)	Fabric routing	ISIS Graceful Restart
Dynamic Arp Inspection (DAI)	DHCP Snooping	IP Service Level Agreements (IPSLA)
Virtual Routing and Forwarding (VRF)	Remote Port Mirroring	RADIUS Server Load Balancing
IEEE 802.1aq SPBv Shortest Path Bridging	Transceiver extended digital diagnostics	Network load balanced servers (NLB)
		IEEE 802.3az Energy Efficient Ethernet (EEE)

FIRMWARE CHANGES AND ENHANCEMENTS:

Feature Enhancements in 8.31.01.0006

Feature Enhancements in 8.31.01.0006
SPBv - – IEEE 802.1aq Shortest Path Bridging (SPB) provides data traffic a shortest cost path between any pair of switches in the SPB network. SPB features dynamic route calculation in a loop-free Layer-2 network and fast convergence time using IS-IS. The 7100-Series supports Shortest Path Bridging VLAN (SPBV).

Feature Enhancements in 8.31.01.0006
VRF - & scale info - Support for multiple VRFs has been added to the 7100-Series with this release. VRF provides a method of partitioning your network into different routed domains. A VRF is a segregated domain for the routed forwarding of packets. An interface configured to a particular VRF is considered a member of that VRF. VRFs can either be static or dynamic. Static VRFs employ only static or policy based routing. Dynamic VRFs employ dynamic routing protocols such as: OSPF, BGP, RIP, PIM, DVMRP, VRRP The default VRF is known as the Global Router and only interfaces assigned to the Global Router may be used to manage the device. VRF Route Leaking - Static Routing has been modified to allow routes to leak from a VRF to the Global Router and vice-a-versa. VRF Aware Policy Based Routing - Policy Based Routing has been modified to allow inter-vrf routing based on Route-Maps. VRF-Aware DHCP Relay - DHCP Relay has been modified to allow DCHP requests to be relayed either within a VRF or between a VRF and the Global Router.
IS-IS Graceful Restart - Graceful Re-Start for the IS-IS protocol has been added. Graceful Re-Start provides for an IS-IS router to continue to forward existing traffic and remain on the forwarding path during a restart of the IS-IS software process.
Remote Port Mirroring - The mirror source port is the source of the mirrored packets found on the local router of interest. The mirror encapsulates the L2 traffic seen by the mirrored source port and delivers it to the tunnel destination address.
Extended Transceiver Information Display - Extended Information display for supported transceivers is provided. In addition to serial number and model details, digital diagnostic information is displayed such as Temperature, Voltage, Transmit Current, Receive Power, Alarm State as well as High/Low thresholds.
Network Load Balanced Servers - Network load balancer or similar proprietary server NIC load balancing technologies, comprised of multiple physical machines responding to a single “virtual” IP address, expect the switch to flood its traffic to all ports on the destination VLAN using a static unicast or multicast MAC address.
100BASE-T Support on 71K91L4-24 and 71K91L4-48 10GBASE-T Ports – 100Mb speed option is now supported on 10GBASE-T ports.

Problems Corrected in 8.31.01.0006

802.1d Filter Database Problems Corrected in 8.31.01.0006	Introduced in Version:
MAC addresses that should age out from filter database will fail to do so. The frequency of this will increase with lower mac age times.	7.91.01

ACL Problems Corrected in 8.31.01.0006	Introduced in Version:
When a packet with a protocol other than IPv4 or IPv6 matches an L2 ACL, the L2 source and destination addresses will be displayed in place of the IPv4 and IPv6 addresses and the ethertype will be displayed as a hex value.	8.11.01
When an L2 ACL is applied to an interface, removed from an interface, or when an L2 ACL currently in use is modified, connections may not be removed. This can cause traffic to flow as it did before the change was made. Toggling the interface down then up will clear all connections and allow the L2 ACL to be correctly applied to traffic.	8.11.01
IPv6 Neighbor discovery messages may be dropped if IPv6 Ingress ACL's are applied.	8.21.01

ACL Problems Corrected in 8.31.01.0006	Introduced in Version:
Configuring unsupported access-group types to interfaces results in a confusing error message.	8.21.01

ARP Problems Corrected in 8.31.01.0006	Introduced in Version:
The router configured on a service provider switch may respond to ARPs received on a customer VLAN when the VLAN ID matches a router's interface VLAN ID. Conversely, the router configured on a customer switch may respond to ARPs received on a service provider VLAN when the VLAN ID matches a router's interface VLAN ID.	7.91.01
Using the command "clear arp <ipAddress>" may not function properly when clearing an ARP or ND entry in the stale state. If the host is still up a new ARP or ND entry will be added immediately after it is deleted.	7.91.01

BGP Problems Corrected in 8.31.01.0006	Introduced in Version:
BGP does not provide a CLI command to allow the user to specify a per peer local AS number.	7.91.01
If a BGP Update message is received with no NLRI path attribute the peering session is torn down.	7.91.01

CFM Problems Corrected in 8.31.01.0006	Introduced in Version:
CFM PDUs that contain the SenderID TLV will be improperly discarded as invalid frames.	8.21.01
Remote MEP states may be incorrect on CFM MEPs that have no VLAN configuration ("Port MEPs").	8.21.01

Data Center Bridging Problems Corrected in 8.31.01.0006	Introduced in Version:
The "show dcb cn ?" output shows "<cr>" as a valid option.	7.91.01
CN does not properly update the automatic alternate priority when a new CNPV is created with a value one less than an existing CNPV. The existing CNPV will continue to remap priorities to the new CNPV on ingress.	7.91.01
CPs on the same port will generate CNMs with the same CPID when multiple CPs exists on the 7100G-series.	8.21.01
The "set dcb cn congestion-point" configuration does not persist when multiple CNPVs are created in a bonded system.	7.91.01
The CLI set or clear "dcb cn congestion-point" command with a port-string of "*.*.*" will fail with an error similar to "Error: Failed to clear congestion point 5 for port tg.1.25". In a stacked system, all subsequent ports will not be set or cleared by the command.	8.21.01
The CN domain defense mode that is automatically configured by LLDP is not cleared when the LLDP neighbor ages out.	7.91.01
The CPID in the cp-mapping table may differ from the CPID in the CNM generated by the CP if the qp-index parameter is modified on the 7100G-series.	8.21.01

Data Center Bridging Problems Corrected in 8.31.01.0006	Introduced in Version:
The ieee8021CnCpTransmittedFrames MIB object does not return the correct value for the number of frames transmitted on a CN queue. For congestion points corresponding to priorities 1, 2, or 3 the MIB object will return a value of 0. The ieee8021CnCpTransmittedFrames MIB object corresponds to the "Transmitted Frames" value in the "show dcb cn congestion-point" CLI.	8.20.02
The MIB supports setting the ieee8021CnCpQueueSizeSetPoint and ieee8021CnCpFeedbackWeight per ieee8021CnCpEntry, however the hardware does not support this parameter on a per CN queue basis. In the CLI, these objects are configured via the "set dcb cn congestion-point" command.	7.91.01
The min-sample setting for q-profile 0.1 does not persist.	7.91.01
The qp-index setting of the "set dcb cn congestion-point" CLI command does not appear in "show config" or "show config all".	7.91.01
Congestion point and queue profile settings do not display valid ranges for the min-sample and weight parameters in CLI help strings.	7.91.01

HostDos Problems Corrected in 8.31.01.0006	Introduced in Version:
Enabling the HostDoS portScan feature mistakenly filters inbound packets on port 22 when SSH is enabled. HostDoS should only filter these packets when SSH is disabled. This may render the switches SSH server inoperable, and the DoS attack detection logic may produce false positives. A workaround is to not enable HostDos portScan, or to enable it but with a relatively high portScan rate limit. Another workaround is to disable and then re-enable SSH (via a Telnet or console connection). However, the problem will return following a system reboot.	7.91.01

IGMP Problems Corrected in 8.31.01.0006	Introduced in Version:
IGMP may lose track of where a flow entered the system. It may cause flow Interruption due to bad internal hardware programming.	7.91.01
It is possible for IGMP to lose track of which port a flow comes in, and cause an IGMP verify failed, status:0x00020000 message.	7.91.01
When the command "set igmp flow-wait" has both oper-state and time set on the same line, only the oper-state is set.	8.11.01

IP Interface Manager Problems Corrected in 8.31.01.0006	Introduced in Version:
When removing a Layer-3 interface using the "no <interfaceName>" command you may receive a difficult to decipher error message if the interface does not exist.	7.91.01

IPSLA Problems Corrected in 8.31.01.0006	Introduced in Version:
The SLA scheduler sub-mode command 'reset' cannot be entered while the SLA entry is scheduled. In order to reset the attributes for the entry, the user must stop the SLA entry via the 'stop' command in the SLA scheduler sub-mode.	8.01.01

IPSLA Problems Corrected in 8.31.01.0006	Introduced in Version:
The user will see the following CLI error when attempting to configure an SLA entry that had been previously configured in another VRF: ' Error: Command failed - create IpSla Entry ' The user will either have to remove the SLA entry from VRF in which it is configured, or choose a different SLA entry to configure.	8.11.01

Host Services Problems Corrected in 8.31.01.0006	Introduced in Version:
ICMP echo requests to IP interface addresses exceeding 100 per second will not all be answered.	8.20.02
"Unexpected syslog messages may be displayed if an interface is removed after the underlying vlan is cleared. These syslog messages are benign. Example of syslog messages: rtrHwApi[2.tRtrHwApi]ERROR: failed to update iif at index 591. rtrHwApi[2.tRtrHwApi]bcm_vlan_control_vlan_get(0, 591,..) failed."	8.21.01
Message "masterTrapSem time out, dropping trap" may appear in message log indicating an SNMP trap being dropped.	
"Blade may reset with the following log message after a configuration change: <1>NonVol[5.tNVolCUp]cleanup:Remove() of first file on store=0, fileIndex=0 majorId=162 failed retval=3".	8.20.02
"Debug syslog message generated when an attempt to create a layer 3 interface is made with an out of range value. PiMgr[1.tConsole]generateIfIndex():retval=0;owner(0);mediaType(7);mediaPos(4096)".	7.91.01
Changing the owner string within an rmon command will result in a small memory leak.	7.91.01
"Failed to set -101" error is seen during logging configuration.	7.91.01
"show support" or "debug messageLog message" result in an exhaustion of memory and a "memPartAlloc: block too big" message stored in the log.	7.91.01
"show system utilization slot <slot>" allows invalid slot numbers such as 0.	7.91.01
"Module might reset with message similar to “<1>DistServ[4.tDsBrdOk]serverWatchDog.1(Config), client 63(PEME) in recv for 6007 tics (0x00d0f9e4 0x0067b420 0x006707ac 0x01683264 0x00000000)” while PoE Controller is being updated.”	7.91.01

Layer 1 Phy Problems Corrected in 8.31.01.0006	Introduced in Version:
Bonded 40G port with CR4 QSFP can potentially get into a link down condition when otherwise its link would be up. This can happen at bootup or any other link bounce condition.	7.91.01
Admin disabled 7100G-series tg ports do not bring link down with forcelinkdown enabled.	7.91.01
If nodealias is disabled on a given port and the maxentries value is set to default, after upgrading to firmware version 8.11.01 or newer will cause the maxentries value to be set to the previous default value.	8.11.01
POE may log a message similar to "bcPoE[4.tDSrecv5]bc_poeShutDown: Unable to get poeUpdateSemId" when a POE system is rebooted.	8.22.01

Layer 2 Problems Corrected in 8.31.01.0006	Introduced in Version:
CNM messages generated on a 7100G-series will be dropped if the reverse path is across a bond link.	8.22.02
Setting the mac age time to 10 seconds may cause the tNtpTmr task to use high amounts of CPU processing time.	8.21.01
"clear dcb cn priority <pri> lldp" will trigger a reset.	7.91.01
When GVRP adds a port to a VLAN that is not statically created, traffic will be dropped when not received on the same slot as the port added through GVRP.	7.91.01

L2 Multicast Problems Corrected in 8.31.01.0006	Introduced in Version:
It is possible for 7100-series modules to reset with the following message Machine Check exception Thread Name: tIgmpInp, at boot time, and may also get stuck in a constant reboot loop.	8.11.01
When setting IGMP setting for unknown input action to flood 7100-series does not flood the first packet.	7.91.01
IGMP may not properly send IGMP queries out interfaces on 7100 series product.	8.21.01

MVRP Problems Corrected in 8.31.01.0006	Introduced in Version:
Dynamic VLANs that were registered by MVRP may still show up in "show vlan" when there are no longer any egress ports. This can happen if the egress was registered on a module port that has since joined a lag.	7.91.01
Dynamic VLANs registered by MVRP fail resulting in no egress.	7.91.01
The ""show vlan"" command may show that egress on a port unexpectedly continues to be seen on a VLAN that once was dynamically registered by MVRP if the VLAN is configured statically on that port and then subsequently removed.	7.91.01

Spanning Tree Problems Corrected in 8.31.01.0006	Introduced in Version:
Output from the command ""show spantree blockedports"" shows a port state of ""Invalid"" instead of ""Disabled"". This error occurs when the port has the dot1dStpPortEnable value set to ""disabled"" and the port operstatus is up.	7.91.01
BPDUs are not processed when marked for discard by Policy. The port role and state will be designated forwarding. When the port is an inter-switch link and the attached port is designated forwarding, a loop will form if there is redundancy.	7.91.01
The "set spantree backuproot" command completes successfully but will not modify the value.	7.91.01

Layer 3 Problems Corrected in 8.31.01.0006	Introduced in Version:
The "age" column for the command "show ipv6 neighbors" displays the last time the ND entry was updated instead of the entry's age.	7.91.01
The description cli command is unavailable on a tunnel interface.	7.91.01

Layer 3 Problems Corrected in 8.31.01.0006	Introduced in Version:
The following syslog message can be seen on 7100 series switches after a system reset has been issued. ""rtrHwApi[1.tRtrHwApi]lock timeout warning. waited 10 seconds for the lock"". This message can be ignored as long as it occurs when the system is being reset.	8.21.01
When using VRRP fabric route mode, if a packet is sent to a host that is connected to the router that is in fabric-route mode (through the master router), the ARP response for that host will not make it back to the master router. This is because the ARP response will be consumed by the router in fabric route-mode.	7.91.01
Host routes for loopback interface addresses may not be didstributed to all blades on a system reset causing connectivity issues to those addresses.	7.91.01
Port Jumbo MTU settings allowed for values below 1519.	8.01.01
Host routes advertised from the host-mobility routers are installed in other host-mobility peers that direct frames to the core instead of the directly connected networks.	8.21.01

IPv6 Neighbor Discovery (ND) Problems Corrected in 8.31.01.0006	Introduced in Version:
ARP/ND entries may expire early if the host does not respond to periodic ARP/ND refresh attempts.	8.21.01
It is possible to configure a Static ND entry which uses the same IP address as an interface address or VRRP address if the static ND entry is created before the other address.	8.21.01
The configuration commands "arp" and "ipv6 neighbor" allow invalid VLAN interfaces such as vlan.0.4095.	8.21.01

OSPF Problems Corrected in 8.31.01.0006	Introduced in Version:
If a config file saved prior to version 7.60 contains an OSPF passive interface, it will cause the box to hang if a configure is executed on an upgrade. The config file can be edited to format vlan.0.# instead of vlan # to allow upgrade.	8.22.02
The "debug ip ospf packet" display for virtual interfaces reads "Interface not found for ifIndex 0".	8.21.01
When changing an OSPF network's area id then failing over, the original area ID is running seen in "show ip ospf interface", though the config reflects the new area ID.	8.21.01
With the removal of passive-interface default, the no passive-interface commands are removed, but they return on reboot of the router. They have no adverse effect.	8.21.01
If OSPF is configured to use a non-existent track object for cost, it does not calculate the cost based on the configured reference bandwidth but leaves it at default.	8.21.01

RIP and RIPng Problems Corrected in 8.31.01.0006	Introduced in Version:
If RIP is configured with passive interfaces and RIPng is configured, the passive-interfaces will function correctly but be displayed under RIPng.	8.21.01
When a RIPng interface is configured to be passive, the passive setting takes effect, but it is not displayed in show running.	8.21.01

VRRP Problems Corrected in 8.31.01.0006	Introduced in Version:
A VRRP router that owns the IP address may relinquish mastership if a packet is received from another VRRP router also claiming to the VRRP owner.	8.21.01

VRRP Problems Corrected in 8.31.01.0006	**Introduced in Version:**
When a VRRP VRID is the master the "show ip vrrp" command will show the default "Master Advertisement Interval" when the correct value should match "Advertisement Interval" of the VRID (since it is the master).	8.21.01
When creating more than the maximum number of allowed VRRP critical IP addresses the error returned indicates that the IP address is bad when it should indicate that the maximum number of critical IP addresses already exists.	8.21.01
When removing a VRRP VRID from configuration the VIP may not be available to use on subsequent VRIDs if the command for the VIP address is negated just before the VRID is disabled.	8.21.01

COS Problems Corrected in 8.31.01.0006	**Introduced in Version:**
Setting cos IRL reference to a value greater than 15 causes the device to continuously reset. If an invalid configuration is detected on upgrade the following syslog will display: SYSLOGX(kDbg_UPN,LOG_WARNING, ""CosTable unable to restore IRL "" ""reference %d mapping to resource %d "" ""for group %d.%d. Mapping is fixed for "" ""this product"",i,nvValue.ref[i],nvValue.group, nvValue.type); A change to the port configuration will prevent these messages from displaying after future reboots.	7.91.01

Policy Problems Corrected in 8.31.01.0006	**Introduced in Version:**
Policy mac address rules may not be immediately applied to flows on Tunneled Bridge Ports.	8.21.01

KNOWN RESTRICTIONS AND LIMITATION:

MGBIC-100BT transceiver doesn't support automatic detection of MDIX (Medium Dependent Interface Crossover).
The 7100-Series does not support half-duplex port configuration at any speed.
During an power down Machine Check and/or NonVol SysLog Messages may occur: These messages do not indicate a serious condition and may be ignored: Example Machine Check SysLog Message Message 52/128 Exception PPC750 Info 07.90.04.0000 02/23/2013 03:19:04 Exc Vector: Machine Check exception (0x00000200) Thread Name: tPhyIntr Exc Addr: 0x00c15588 Thread Stack: 0x073c9000..0x073c6000 Stack Pointer: 0x073c8e30 Traceback Stack: [0] 0x00c10fb8

[1] 0x00c11104 [2] 0x00f86b6c …. Example NonVol SysLog Message Message 67/143 Syslog Message 07.90.04.0000 02/23/2013 03:16:36 <0>NonVol[1.tusrAppInit]nonvol_init_dd: The persistent store for 0 is in complete. This data has been erased and the board will reset. (0x00b5a 874 0x0092f644 0x007c06b4 0x011f90ac 0x00000000)
L2 MAC address aging could take up to 2x the desired MAC age time.
For SPBv: When changing the ISIS areaID, spb should be disabled before the change, and re-enabled after the new areaID is configured.

Any problems other than those listed above should be reported to our Technical Support Staff.

RFC STANDARDS SUPPORT:

RFC No.	Title
RFC0147	Definition of a socket
RFC0768	UDP
RFC0781	Specification of (IP) timestamp option
RFC0783	TFTP
RFC0791	Internet Protocol
RFC0792	ICMP
RFC0793	TCP
RFC0826	ARP
RFC0854	Telnet
RFC0894	Transmission of IP over Ethernet Networks
RFC0919	Broadcasting Internet Datagrams
RFC0922	Broadcasting IP datagrams over subnets
RFC0925	Multi-LAN Address Resolution
RFC0950	Internet Standard Subnetting Procedure
RFC0959	File Transfer Protocol
RFC1027	Proxy ARP
RFC1027	Using ARP - transparent subnet gateways
RFC1034	Domain Names - Concepts and Facilities
RFC1035	Domain Names - Implementation and Specification
RFC1157	Simple Network Management Protocol
RFC1071	Computing the Internet checksum
RFC1112	Host extensions for IP multicasting
RFC1122	Requirements for IP Hosts - Comm Layers
RFC1123	Requirements for IP Hosts - Application and Support
RFC1191	Path MTU discovery
RFC1195	Use of OSI IS-IS for Routing in TCP/IP
RFC1213	MIB-II
RFC1245	OSPF Protocol Analysis
RFC1246	Experience with the OSPF Protocol
RFC1265	BGP Protocol Analysis
RFC1266	Experience with the BGP Protocol
RFC1323	TCP Extensions for High Performance
RFC1349	Type of Service in the Internet Protocol Suite

RFC No.	Title
RFC1350	TFTP
RFC1387	RIPv2 Protocol Analysis
RFC1388	RIPv2 Carrying Additional Information
RFC1389	RIPv2 MIB Extension
RFC1492	TACACS+
RFC1493	BRIDGE- MIB
RFC1517	Implementation of CIDR
RFC1518	CIDR Architecture
RFC1519	Classless Inter-Domain Routing (CIDR)
RFC1624	IP Checksum via Incremental Update
RFC1657	Managed Objects for BGP-4 using SMIv2
RFC1659	RS-232-MIB
RFC1721	RIPv2 Protocol Analysis
RFC1722	RIPv2 Protocol Applicability Statement
RFC1723	RIPv2 with Equal Cost Multipath Load Balancing
RFC1724	RIPv2 MIB Extension
RFC1771	A Border Gateway Protocol 4 (BGP-4)
RFC1772	Application of BGP in the Internet
RFC1773	Experience with the BGP-4 protocol
RFC1774	BGP-4 Protocol Analysis
RFC1812	General Routing
RFC1850	OSPFv2 MIB
RFC1853	IP in IP Tunneling
RFC1886	DNS Extensions to support IP version 6
RFC1924	A Compact Representation of IPv6 Addresses
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC1966	BGP Route Reflection
RFC1981	Path MTU Discovery for IPv6
RFC1997	BGP Communities Attribute
RFC1998	BGP Community Attribute in Multi-home Routing
RFC2001	TCP Slow Start
RFC2012	TCP-MIB
RFC2013	UDP-MIB
RFC2018	TCP Selective Acknowledgment Options
RFC2030	SNTP
RFC2080	RIPng (IPv6 extensions)
RFC2082	RIP-II MD5 Authentication
RFC2096	IP Forwarding Table MIB
RFC2104	HMAC
RFC2113	IP Router Alert Option
RFC2117	PIM -SM Protocol Specification
RFC2131	Dynamic Host Configuration Protocol
RFC2132	DHCP Options and BOOTP Vendor Extensions
RFC2138	RADIUS Authentication
RFC2233	The Interfaces Group MIB using SMIv2
RFC2236	Internet Group Management Protocol, Version 2
RFC2260	Support for Multi-homed Multi-prov
RFC2270	Dedicated AS for Sites Homed to one Provider
RFC2270	Dedicated AS for Sites Homed to one Provider
RFC2328	OSPFv2

RFC No.	Title
RFC2329	OSPF Standardization Report
RFC2338	VRRP
RFC2362	PIM-SM Protocol Specification
RFC2370	The OSPF Opaque LSA Option
RFC2373	RFC 2373 Address notation compression
RFC2374	IPv6 Aggregatable Global Unicast Address Format
RFC2375	IPv6 Multicast Address Assignments
RFC2385	BGP TCP MD5 Signature Option
RFC2401	Security Architecture for the Internet Protocol
RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC2409	The Internet Key Exchange (IKE)
RFC2428	FTP Extensions for IPv6 and NATs
RFC2450	Proposed TLA and NLA Assignment Rule
RFC2453	RIPv2
RFC2460	IPv6 Specification
RFC2461	Neighbor Discovery for IPv6
RFC2462	IPv6 Stateless Address Autoconfiguration
RFC2463	ICMPv6
RFC2464	Transmission of IPv6 over Ethernet
RFC2473	Generic Packet Tunneling in IPv6 Specification
RFC2474	Definition of DS Field in the IPv4/v6 Headers
RFC2475	An Architecture for Differentiated Service
RFC2519	A Framework for Inter-Domain Route Aggregation
RFC2545	BGP Multiprotocol Extensions for IPv6
RFC2553	BasiCSocket Interface Extensions for IPv6
RFC2577	FTP Security Considerations
RFC2578	SNMPv2-SMI
RFC2579	SNMPv2-TC
RFC2581	TCP Congestion Control
RFC2597	Assured Forwarding PHB Group
RFC2613	SMON-MIB
RFC2618	RADIUS Client MIB
RFC2620	RADIUS Accounting MIB
RFC2674	P/Q-BRIDGE- MIB
RFC2697	A Single Rate Three Color Marker
RFC2710	Multicast Listener Discovery (MLD) for IPv6
RFC2711	IPv6 Router Alert Option
RFC2715	Interop Rules for MCAST Routing Protocols
RFC2740	OSPF for IPv6
RFC2763	Dynamic Hostname Exchange Mechanism for IS-IS
RFC2787	VRRP MIB
RFC2796	BGP Route Reflection
RFC2819	RMON MIB
RFC2827	Network Ingress Filtering
RFC2858	Multiprotocol Extensions for BGP-4
RFC2863	IF-MIB
RFC2864	IF-INVERTED-STACK-MIB

RFC No.	Title
RFC2865	RADIUS Authentication
RFC2865	RADIUS Accounting
RFC2893	Transition Mechanisms for IPv6 Hosts and Routers
RFC2894	RFC 2894 Router Renumbering
RFC2918	Route Refresh Capability for BGP-4
RFC2922	PTOPO-MIB
RFC2934	PIM MIB for IPv4
RFC2966	Prefix Distribution with Two-Level IS-IS
RFC2973	IS-IS Mesh Groups
RFC2991	Multipath Issues in Ucast & Mcast Next-Hop
RFC3056	Connection of IPv6 Domains via IPv4 Clouds
RFC3065	Autonomous System Confederations for BGP
RFC3069	VLAN Aggregation for Efficient IP Address Allocation
RFC3101	The OSPF Not-So-Stubby Area (NSSA) Option
RFC3107	Carrying Label Information in BGP-4
RFC3137	OSPF Stub Router Advertisement
RFC3273	HC-RMON-MIB
RFC3291	INET-ADDRESS-MIB
RFC3315	DHCPv6
RFC3345	BGP Persistent Route Oscillation
RFC3359	TLV Codepoints in IS-IS
RFC3373	Three-Way Handshake for IS-IS
RFC3376	Internet Group Management Protocol, Version 3
RFC3392	Capabilities Advertisement with BGP-4
RFC3411	SNMP Architecture for Management Frameworks
RFC3412	Message Processing and Dispatching for SNMP
RFC3412	SNMP-MPD-MIB
RFC3413	SNMP Applications
RFC3413	SNMP-NOTIFICATIONS-MIB
RFC3413	SNMP-PROXY-MIB
RFC3413	SNMP-TARGET-MIB
RFC3414	SNMP-USER-BASED-SM-MIB
RFC3415	SNMP-VIEW-BASED-ACM-MIB
RFC3417	SNMPv2-TM
RFC3418	SNMPv2 MIB
RFC3446	Anycast RP mechanism using PIM and MSDP
RFC3484	Default Address Selection for IPv6
RFC3493	Basic Socket Interface Extensions for IPv6
RFC3509	Alternative Implementations of OSPF ABRs
RFC3513	RFC 3513 IPv6 Addressing Architecture
RFC3542	Advanced Sockets API for IPv6
RFC3562	Key Mgt Considerations for TCP MD5 Signature Opt
RFC3576	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
RFC3584	SNMP-COMMUNITY-MIB
RFC3587	IPv6 Global Unicast Address Format
RFC3590	RFC 3590 MLD Multicast Listener Discovery
RFC3595	Textual Conventions for IPv6 Flow Label
RFC3596	DNS Extensions to Support IP Version 6
RFC3621	POWER-ETHERNET-MIB
RFC3623	Graceful OSPF Restart

RFC No.	Title
RFC3635	ETHERLIKE-MIB
RFC3678	Socket Interface Ext for Mcast Source Filters
RFC3704	Network Ingress Filtering
RFC3769	Requirements for IPv6 Prefix Delegation
RFC3787	Recommendations for Interop IS-IS IP Networks
RFC3810	MLDv2 for IPv6
RFC3879	Deprecating Site Local Addresses
RFC3956	Embedding the RP Address in IPv6 MCAST Address
RFC3973	Protocol Independent Multicast - Dense Mode (PIM-DM)
RFC3986	URI Generic Syntax
RFC4007	IPv6 Scoped Address Architecture
RFC4022	MIB for the Transmission Control Protocol (TCP)
RFC4109	Algorithms for IKEv1
RFC4113	MIB for the User Datagram Protocol (UDP)
RFC4133	ENTITY MIB
RFC4167	Graceful OSPF Restart Implementation Report
RFC4188	Bridge MIB
RFC4193	Unique Local IPv6 Unicast Addresses
RFC4213	Basic Transition Mechanisms for IPv6
RFC4222	Prioritized Treatment of OSPFv2 Packets
RFC4264	BGP Wedgies
RFC4268	ENTITY-STATE-MIB
RFC4268	ENTITY-STATE-TC-MIB
RFC4271	A Border Gateway Protocol 4 (BGP-4)
RFC4272	BGP Security Vulnerabilities Analysis
RFC4273	Managed Objects for BGP-4 using SMIv2
RFC4274	BGP-4 Protocol Analysis
RFC4275	BGP-4 MIB Implementation Survey
RFC4276	BGP-4 Implementation Report
RFC4277	Experience with the BGP-4 protocol
RFC4291	IP Version 6 Addressing Architecture
RFC4292	IP Forwarding MIB
RFC4293	MIB for the Internet Protocol (IP)
RFC4294	IPv6 Node Requirements
RFC4301	Security Architecture for IP
RFC4302	IP Authentication Header
RFC4303	IP Encapsulating Security Payload (ESP)
RFC4305	Crypto Algorithm Requirements for ESP and AH
RFC4306	Internet Key Exchange (IKEv2) Protocol
RFC4307	Cryptographic Algorithms for Use in IKEv2
RFC4308	Cryptographic Suites for IPSec
RFC4360	BGP Extended Communities Attribute
RFC4384	BGP Communities for Data Collection
RFC4443	ICMPv6 for IPv6
RFC4444	MIB for IS-IS
RFC4451	BGP MULTI_EXIT_DISC (MED) Considerations
RFC4456	BGP Route Reflection
RFC4486	Subcodes for BGP Cease Notification Message
RFC4541	IGMP Snooping
RFC4541	MLD Snooping

RFC No.	Title
RFC4552	Authentication/Confidentiality for OSPFv3
RFC4560	DISMAN-PING-MIB
RFC4560	DISMAN-TRACEROUTE-MIB
RFC4560	DISMAN-NSLOOKUP-MIB
RFC4577	OSPF as PE/CE Protocol for BGP L3 VPNs
RFC4601	PIM-SM
RFC4602	PIM-SM IETF Proposed Std Req Analysis
RFC4604	IGMPv3 & MLDv2 & Source-Specific Multicast
RFC4607	Source-Specific Multicast for IP
RFC4608	PIM--SSM in 232/8
RFC4610	Anycast-RP Using PIM
RFC4632	Classless Inter-Domain Routing (CIDR)
RFC4668	RADIUS Client MIB
RFC4670	RADIUS Accounting MIB
RFC4724	Graceful Restart Mechanism for BGP
RFC4750	OSPFv2 MIB
RFC4760	Multiprotocol Extensions for BGP-4
RFC4835	Crypto Algorithm Requirements for ESP and AH
RFC4836	MAU-MIB
RFC4836	IANA-MAU-MIB
RFC4861	Neighbor Discovery for IPv6
RFC4862	IPv6 Stateless Address Auto-configuration
RFC4878	DOT3-OAM-MIB
RFC4884	RFC 4884 Extended ICMP Multi-Part Messages
RFC4893	BGP Support for Four-octet AS Number Space
RFC4940	IANA Considerations for OSPF
RFC4940	IANA Considerations for OSPF
RFC5059	Bootstrap Router (BSR) Mechanism for (PIM)
RFC5060	PIM MIB
RFC5065	Autonomous System Confederations for BGP
RFC5095	Deprecation of Type 0 Routing Headers in IPv6
RFC5132	IP Multicast MIB
RFC5132	IP Multicast MIB
RFC5186	IGMPv3/MLDv2/MCAST Routing Protocol Interaction
RFC5187	OSPFv3 Graceful Restart
RFC5240	PIM Bootstrap Router MIB
RFC5250	The OSPF Opaque LSA Option
RFC5291	Outbound Route Filtering Capability for BGP-4
RFC5292	Address-Prefix-Outbound Route Filter for BGP-4
RFC5294	Host Threats to PIM
RFC5301	Dynamic Hostname Exchange Mechanism for IS-IS
RFC5302	Domain-wide Prefix Distribution with IS-IS
RFC5303	3Way Handshake for IS-IS P2P Adjacencies
RFC5304	IS-IS Cryptographic Authentication
RFC5305	IS-IS extensions for Traffic Engineering
RFC5308	Routing IPv6 with IS-IS
RFC5309	P2P operation over LAN in link-state routing
RFC5310	IS-IS Generic Cryptographic Authentication
RFC5340	OSPF for IPv6
RFC5396	Textual Representation AS Numbers

RFC No.	Title
RFC5398	AS Number Reservation for Documentation Use
RFC5492	Capabilities Advertisement with BGP-4
RFC5519	MGMD-STD-MIB
RFC5643	OSPFv3 MIB
RFC5798	Virtual Router Redundancy Protocol (VRRP) V3
RFC6164	Using 127-Bit IPv6 Prefixes on Inter-Router Links
RFC6296	IPv6-to-IPv6 Network Prefix Translation
RFC6329	IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging
Drafts	draft-ietf-idr-bgp4-mibv2 (Partial Support)
Drafts	draft-ietf-idr-bgp-identifier
Drafts	draft-ietf-idr-as-pathlimit
Drafts	draft-ietf-idr-mrai-dep (Partial Support)
Drafts	draft-ietf-isis-experimental-tlv (Partial Support)
Drafts	draft-ietf-isis-ipv6-te (Partial Support)
Drafts	draft-ietf-ospf-ospfv3-mib
Drafts	draft-ietf-ospf-te-node-addr
Drafts	draft-ietf-idmr-dvmrp-v3-11
Drafts	draft-ietf-vrrp-unified-spec-03.txt

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT:

Title	Title	Title
CISCO-CDP-MIB	ENTERASYS-IF-MIB-EXT-MIB	ENTERASYS-SPANNING-TREE-DIAGNOSTIC-MIB
CISCO-TC	ENTERASYS-JUMBO-ETHERNET-FRAME-MIB	ENTERASYS-SYSLOG-CLIENT-MIB
CT-BROADCAST-MIB	ENTERASYS-LICENSE-KEY-MIB	ENTERASYS-TACACS-CLIENT-MIB
CTIF-EXT-MIB	ENTERASYS-LICENSE-KEY-OIDS-MIB	ENTERASYS-TRANSMIT-QUEUE-MONITOR-MIB
CTRON-ALIAS-MIB	ENTERASYS-LINK-FLAP-MIB	ENTERASYS-UPN-TC-MIB
CTRON-BRIDGE-MIB	ENTERASYS-MAC-AUTHENTICATION-MIB	ENTERASYS-VLAN-AUTHORIZATION-MIB
CTRON-CDP-MIB	ENTERASYS-MAC-LOCKING-MIB	ENTERASYS-VLAN-INTERFACE-MIB
CTRON-CHASSIS-MIB	ENTERASYS-MAU-MIB-EXT-MIB	IANA-ADDRESS-FAMILY-NUMBERS-MIB
CTRON-ENVIROMENTAL-MIB	ENTERASYS-MGMT-AUTH-NOTIFICATION-MIB	IEEE8021-CN-MIB
CTRON-MIB-NAMES	ENTERASYS-MGMT-MIB	IEEE8021-PAE-MIB
CTRON-OIDS	ENTERASYS-MIB-NAMES DEFINITIONS	IEEE8021-PFC-MIB
CTRON-Q-BRIDGE-MIB-EXT	ENTERASYS-MSTP-MIB	IEEE8023-LAG-MIB
ENTERASYS-AAA-POLICY-MIB	ENTERASYS-MULTI-AUTH-MIB	LLDP-EXT-DOT1-MIB
ENTERASYS-CLASS-OF-SERVICE-MIB	ENTERASYS-MULTI-USER-8021X-MIB	LLDP-EXT-DOT3-MIB
ENTERASYS-CONFIGURATION-MANAGEMENT-MIB	ENTERASYS-OIDS-MIB DEFINITIONS	LLDP-EXT-MED-MIB
ENTERASYS-CONVERGENCE-END-POINT-MIB	ENTERASYS-PFC-MIB-EXT-MIB	LLDP-MIB
ENTERASYS-CN-MIB-EXT-MIB	ENTERASYS-POLICY-PROFILE-MIB	RSTP-MIB
ENTERASYS-DIAGNOSTIC-MESSAGE-MIB	ENTERASYS-PWA-MIB	U-BRIDGE-MIB

Title	Title	Title
ENTERASYS-DNS-RESOLVER-MIB	ENTERASYS-RADIUS-ACCT-CLIENT-EXT-MIB	USM-TARGET-TAG-MIB
ENTERASYS-IEEE8023-LAG-MIB-EXT-MIB	ENTERASYS-RADIUS-AUTH-CLIENT-MIB	SNMP-RESEARCH-MIB
ENTERASYS-IETF-BRIDGE-MIB-EXT-MIB	ENTERASYS-RESOURCE-UTILIZATION-MIB	VSB-SHARED-SECRET-MIB
ENTERASYS-IETF-P-BRIDGE-MIB-EXT-MIB	ENTERASYS-SNTP-CLIENT-MIB	ENTERASYS-DOT3-LLDP-EXT-MIB
ENTERASYS-IEEE8021-CFM-EXT-MIB	ENTERASYS-IEEE8021-CFM-EXT-MIB	
ENTERASYS-OSPF-EXT-MIB	ENTERASYS-PIM-EXT-MIB	ENTERASYS-DVMRP-EXT-MIB
ENTERASYS-ETH-OAM-EXT-MIB	ENTERASYS-RIPv2-EXT-MIB	ENTERASYS-ENTITY-SENSOR-MIB-EXT-MIB

Extreme Networks Private Enterprise MIBs are available in ASN.1 format from the Extreme Networks web site at: www.extremenetworks.com/support/policies/mibs/. Indexed MIB documentation is also available.

SNMP TRAP SUPPORT:

RFC No.	Title
RFC 1493	New Root Topology Change
RFC 1907	Cold Start Warm Start Authentication Failure
RFC 4133	entConfigChange
RFC 2668	ifMauJabberTrap
RFC 2819	risingAlarm fallingAlarm
RFC 2863	linkDown linkup
RFC 2922	ptopoConfigChange
RFC 3621	pethPsePortOnOffNotification pethMainPowerUsageOnNotification pethMainPowerUsageOffNotification
RFC4268	entStateOperEnabled entStateOperDisabled
Enterasys-mac-locking-mib	etsysMACLockingMACViolation

RFC No.	Title
Cabletron-Traps.txt	boardOperational boardNonOperational wgPsInstalled wgPsRemoved wgPsNormal wgPsFail wgPsRedundant wgPsNotRedundant fanFail fanNormal boardInsertion boardRemoval
	etsysPseChassisPowerRedundant etsysPseChassisPowerNonRedundant etsysPsePowerSupplyModuleStatusChange
Enterasys-link-flap-mib	etsysLinkFlapViolation
Enterasys-ietf-bridge-mib-ext-mib	etsysIetfBridgeDot1qFdbNewAddrNotification etsysIetfBridgeDot1dSpanGuardPortBlocked etsysIetfBridgeDot1dBackupRootActivation etsysIetfBridgeDot1qFdbMovedAddrNotification etsysIetfBridgeDot1dCistLoopProtectEvent
Enterasys-notification-auth-mib	etsysMgmtAuthSuccessNotificiation etsysMgmtAuthFailNotificiation
Enterasys-multi-auth-mib	etsysMultiAuthSuccess etsysMultiAuthFailed etsysMultiAuthTerminated etsysMultiAuthMaxNumUsersReached etsysMultiAuthModuleMaxNumUsersReached etsysMultiAuthSystemMaxNumUsersReached
Enterasys-spanning-tree-diagnostic-mib	etsysMstpLoopProtectEvent etsysStpDiagCistDisputedBpduThresholdExceeded etsysStpDiagMstiDisputedBpduThresholdExceeded
Lldp-mib	lldpNotificationPrefix (IEEE Std 802.1AB-2004)
Lldp-ext-med-mib	lldpXMedTopologyChangeDetected (ANSI/TIA-1057)
Enterasys-class-of-service-mib	etsysCosIrlExceededNotification
Enterasys-policy-profile-mib	etsysPolicyRulePortHitNotification
Enterasys-mstp-mib	etsysMstpLoopProtectEvent
Ctron-environment-mib	chEnvAmbientTemp chEnvAmbientStatus

RADIUS ATTRIBUTE SUPPORT:

This section describes the support of RADIUS attributes on the 7100-Series. RADIUS attributes are defined in RFC 2865 and RFC 3580 (IEEE 802.1X specific).

RADIUS AUTHENTICATION AND AUTHORIZATION ATTRIBUTES:

Attribute	RFC Source
Called-Station-Id	RFC 2865, RFC 3580
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579
Filter-Id	RFC 2865, RFC 3580
Framed-MTU	RFC 2865, RFC 3580
Idle-Timeout	RFC 2865, RFC 3580
Message-Authenticator	RFC 3579
NAS-IP-Address	RFC 2865, RFC 3580
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-Type	RFC 2865, RFC 3580
NAS-Identifier	RFC 2865, RFC 3580
Service-Type	RFC 2865, RFC 3580
Session-Timeout	RFC 2865, RFC 3580
State	RFC 2865
Termination-Action	RFC 2865, RFC 3580
User-Name	RFC 2865, RFC 3580
User-Password	RFC 2865

RADIUS ACCOUNTING ATRRIBUTES:

Attribute	RFC Source
Acct-Authentic	RFC 2866
Acct-Delay-Time	RFC 2866
Acct-Interim-Interval	RFC 2866
Acct-Session-Id	RFC 2866
Acct-Session-Time	RFC 2866
Acct-Status-Type	RFC 2866
Acct-Terminate-Cause	RFC 2866
Calling-Station-ID	RFC 2865

GLOBAL SUPPORT:

By Phone:	**603-952-5000**
	1-800-872-8440 (toll-free in U.S. and Canada)
	For the Extreme Networks Support toll-free number in your country: **www.extremenetworks.com/support/contact/**
By Email:	**support@enterasys.com**
By Web:	**www.extremenetworks.com/support/**
By Mail:	**Extreme Networks, Inc.** **145 Rio Robles** **San Jose, CA 95134 (USA)**

For information regarding the latest software available, recent release notes revisions, or if you require additional assistance, please visit the Extreme Networks Support web site.