BLACK BOX®
NETWORK SERVICES

24-Port Web Smart Gigabit Ethernet Switch

This Web smart switch provides 24 10-/100-/1000-Mbps ports.

Supports Gigabit speed on all ports.

FEDERAL COMMUNICATIONS COMMISSION and
INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult an experienced radio/TV technician for help.

CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Normas Oficiales Mexicanas (NOM)
Electrical Safety Statement
INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.

3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objetos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

Trademarks Used in this Manual

Black Box and the Double Diamond logo are registered trademarks of BB Technologies, Inc.

Internet Explorer is a registered trademark of Microsoft Corporation.

UL is a registered trademark of Underwriters' Laboratories.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Table of Contents

1. Specifications

Buffer Memory — 500 KB

Compliance — FCC Class B; power supply is UL® Listed

Filtering/Forwarding Rate — 1000-Mbps port: 1,488,000 pps;
   100-Mbps port: 148,800 pps;
   10-Mbps port: 14,880 pps

Jumbo Frames — 9.6 KB

MAC Address — 8K

Standards — IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX,
   IEEE 802.3ab 1000BASE-T, IEEE 802.3x flow control

Transmission Media — 10BASE-T CAT3, 4, 5 UTP/STP;
   100BASE-TX CAT5 UTP/STP;
   1000BASE-T CAT5e UTP/STP

Connectors — (24) RJ-45, (1) power connector

Indicators — (49) LEDs: Per port: (1) LINK/ACT, (1) 1000M;
   Per unit: (1) Power

Power — Internal power supply: Input Voltage: 90–260 VAC, 50–60 Hz;
   Input Power/Watts: 20 watts (max.)

Temperature Tolerance — Operating: +32 to +131° F (0 to +55° C);
   Storage: -4 to +194° F (-20 to +90° C)

Operating Humidity — 10 to 90% relative humidity (non-condensing)

Size — 1.73"H x 17.32"W x 8.66"D (4.4 x 45 x 22 cm)

Weight — 6.39 lb. (2.9 kg) unit;
   6.61 lb. (3 kg) shipping

2. Overview

2.1 Introduction

The 24-Port Web Smart Gigabit Ethernet Switch provides 24 10-/100-/1000-Mbps ports. It is designed for easy installation and enables high performance in an environment where traffic on the network and the number of users increases continuously. With the newest Gigabit chipset, this 19" Gigabit Ethernet switch fully supports the highest speed without any problems, even when running full-duplex fully loaded.

The switch also provides automatic crossover detection on each port, making it easy to uplink to another switch without using a crossover cable.

This rackmount switch is specifically designed for medium to large workgroups. It provides smooth network migration and makes it easy to increase network capacity.

2.2 Features

• Supports real-time status (link, speed, duplex) of each port.

• Supports port setting for enable or disable operation (the first port can't be disabled).

• Includes port setting for N-Way or force mode operation.

• Features broadcast storm protection.

• Enables port-based VLAN.

• Supports priority queues for QoS.

• Complies with IEEE 802.3 Ethernet, IEEE 802.3u Fast Ethernet, and IEEE 802.3ab Gigabit Ethernet standards.

• 24 ports autonegotiate speeds of 10, 100, and 1000 Mbps.

• 19" rackmountable.

• Provides non-blocking and non-head of line blocking full wire-speed forwarding.

• Store-and-forward operation support.

• Supports 9.6 KB jumbo frames.

• Provides 8K MAC addresses.

• Supports broadcast storm filitering.

• All ports provide autonegotiation and Auto MDI/MDI-X functions.

• Supports flow control: backpressure for half-duplex and IEEE 802.3x for full-duplex mode.

• Smart plug and play.

2.3 What's Included

Your package should contain the following items. If anything is missing or damaged, contact Black Box Technical Support at 724-746-5500 or info@blackbox.com.

• (1) 24-Port Web Smart Gigabit Ethernet Switch

• (1) U.S. power cord

• This user's manual in PDF format on CD-ROM

• (1) rackmount kit: (2) brackets, (8) screws

2.4 Hardware Description

Figures 2-1 and 2-2 show the front and back panels of the 24-Port Web Smart Gigabit Ethernet Switch. Table 2-1 describes its components.
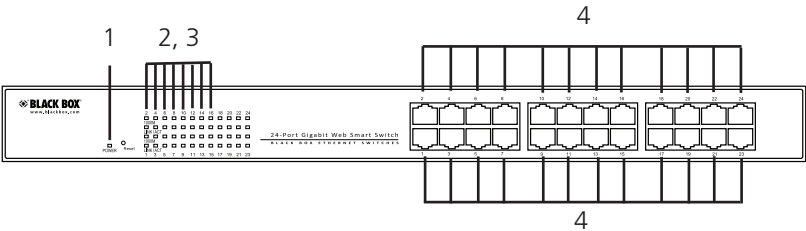
Figure 2-1. Front panel.
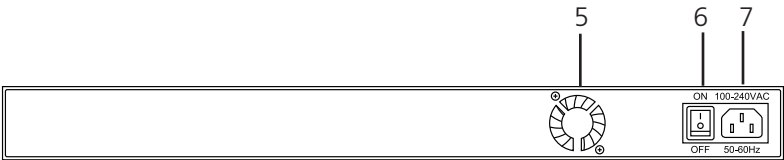
Figure 2-2. Back panel.

Table 2-1. 24-Port Web Smart Gigabit Ethernet Switch components.

Number	Component	Description
1	(1) Power LED	Lights when power to the unit is on.
2	(24) 1000M LEDs	Light when a port is operating at 1000 Mbps.
3	(24) LINK/ACT LEDs	Light solid when link is up, blink when data is present, and are off when there is no link.
4	(24) RJ-45 connectors	Connect to 10/100/1000 devices.
5	Air vents	Maintain proper airflow.
6	Power on/off switch	Switches the power to the unit on or off.
7	Power receptacle	Links 90–260-VAC, 50-60-Hz, 20-W internal power supply to power outlet

3. Software Description

This section explains how to set up and manage the switch through the Web user interface.

3.1 Login

First, open the Web browser, and go to 192.168.2.1. The login screen will appear. Type in the password (default password: "admin") to pass the authentication, and click on the "Apply" button. The following message will appear:

"Password successfully entered."

Please enter password to login

Password:	

Apply

Figure 3-1.

3.2 Configuration

3.2.1 System

This page shows system configuration information, as illustrated in Figure 3-3.

System Configuration

MAC Address	12-0e-c0-ee-30-e2
S/W Version	Luton 2.34d 2m
H/W Version	1.0
Active IP Address	192.168.2.1
Active Subnet Mask	255.255.255.0
Active Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	☐
Fallback IP Address	192.168.2.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	0.0.0.0
Management VLAN	1
Name	
Password	
Inactivity Timeout (secs)	0
SNMP enabled	☑
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public

Apply   Refresh

Figure 3-2. System Configuration screen.

• MAC Address: Displays the unique hardware address assigned by manufacturer (default).

• S/W Version: Displays the switch's firmware version.

• H/W Version: Displays the switch's hardware version.

• DHCP Enabled: Click the box to enable DHCP.

• Fallback IP address: Manually assign the IP address that the network is using. The default IP is 192.168.2.1.

• Fallback Subnet Mask: Assign the subnet mask to the IP address.

• Fallback Gateway: Assign the network gateway for industrial switch. The default gateway is 0.0.0.0.

• Management VLAN: ID of a configured VLAN (1–4096) through which you can manage the switch. By default, all ports on the switch are members of VLAN 1. However, you change the management VLAN, the management station must be attached to a port belonging to this VLAN.

• Name: Type in a unique name to identify the switch.

• Password: Type in the new password (the default value is "admin").

• SNMP Enabled: Enables or disables SNMP on the switch. Supports SNMP version 1 and 2c management clients.

• SNMP Trap Destination: IP address of the trap manager to receive notification messages from this switch. Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station.

• SNMP Read Community: A community string that acts like a password and permits access to the SNMP database on this switch. Authorized management stations are only able to retrieve MIB objects.

• SNMP Trap Community: Community string sent with the notification operation.

3.2.2 Ports
Port Security ensures access to a switch port based on MAC address, limits the total number of devices from using a switch port, and protects against MAC flooding attacks.

3.2.2.1 Port Configuration
In Port Configuration, you can set and view the operation mode for each port.

• Enable Jumbo Frames: This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports up to 9.6 KB. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

• Power Saving Mode: Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements.

• Mode: Manually set the port speed such as auto, 10 half, 10 full, 100 half, 100 full, 1000 full. or disabled. Click on the "Apply" button to complete the configuration.

Flow Control

Click the check box (x) to enable flow control. If flow control is set to enable, both parties can send PAUSE frames to the transmitting device(s) if the receiving port is too busy to handle the amount of data being sent. When it is set to disable, there will be no flow control on that port. The port will drop packets if the amount of data becomes too much for the port to handle.

Port Configuration

Enable Jumbo Frames ☐

PERFECT_REACH/Power Saving Mode:	Full ▾

Full
Link-up
Link-down
Disable

Port	Link	Mode	Flow Control
1	Down	Auto Speed ▾	☐
2	100FDX	Auto Speed ▾	☐
3	Down	Auto Speed ▾	☐
4	100FDX	Auto Speed ▾	☐
5	Down	Auto Speed ▾	☐
6	Down	Auto Speed ▾	☐
7	Down	Auto Speed ▾	☐
8	Down	Auto Speed ▾	☐

Figure 3-3.

Port	Link	Mode	Flow Control
1	Down	Auto Speed ▾	☐
2	100FDX	Auto Speed	☐
3	Down	10 Half	☐
4	100FDX	10 Full	☐
5	Down	100 Half	☐
6	Down	100 Full	☐
7	Down	1000 Full	☐
8	Down	Disabled	☐

Drop frames after excessive collisions	☐

Apply   Refresh

Figure 3-4.

3.2.3 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from the members of the same VLAN.

Basically, creating a VLAN from a switch is logically equivalent to reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

3.2.3.1 Port Segmentation (VLAN) Configuration

• VLAN ID: ID of the configured VLAN (1–4096, no leading zeroes).

• VLAN Configuration List: Lists all the current VLAN groups created for this system. Up to 16 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

Port	Link	Mode	Flow Control
1	Down	Auto Speed ▾	☐
2	100FDX	Auto Speed / 10 Half / 10 Full / **100 Half** / 100 Full / 1000 Full / Disabled	☐
3	Down		☐
4	100FDX		☐
5	Down		☐
6	Down	Auto Speed ▾	☐
7	Down	Auto Speed ▾	☐
8	Down	Auto Speed ▾	☐

Drop frames after excessive collisions	☐

Figure 3-5.

3.2.3.2 VLAN Setup

The switch supports up to 16 VLANs based on 802.1Q standard. From the VLAN Membership page you can create and delete VLANs, and change the VLAN port membership.

VLAN Setup

VLAN ID: 12			
Port	Member	Port	Member
Port 1	☑	Port 5	☐
Port 2	☑	Port 6	☐
Port 3	☐	Port 7	☑
Port 4	☐	Port 8	☑

Apply   Refresh

Figure 3-6.

3.2.3.3 VLAN Per Port Configuration

The 802.1Q Per Port Configuration page allows you to change the VLAN parameters for individual ports or trunks. You can configure VLAN behavior for specific interfaces, including the accepted frame types and default VLAN identifier (PVID). Each row of the table corresponds to one port or trunk; trunked ports cannot be configured individually; configure the trunk instead.

VLAN Per Port Configuration

Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid
Port 1	☑	☐	⦿ All ○ Tagged Only	12 ▼
Port 2	☑	☐	⦿ All ○ Tagged Only	None / 12
Port 3	☐	☐	⦿ All ○ Tagged Only	None ▼
Port 4	☐	☐	⦿ All ○ Tagged Only	None ▼
Port 5	☐	☐	⦿ All ○ Tagged Only	None ▼
Port 6	☐	☐	⦿ All ○ Tagged Only	None ▼
Port 7	☐	☐	⦿ All ○ Tagged Only	None ▼
Port 8	☐	☐	⦿ All ○ Tagged Only	None ▼

Figure 3-7. VLAN per port configuration.

• Port/Trunk: The port number of the port or the ID of a trunk.

• VLAN Aware Enabled: VLAN aware ports are able to use VLAN tagged frames to determine the destination VLAN of a frame. (Default: Enabled)

• VLAN aware ports will strip the VLAN tag from received frames and insert the tag in transmitted frames (except for the PVID). VLAN unaware ports will not strip the tag from received frames or insert the tag in transmitted frames.

• Ingress Filtering Enabled: If enabled, incoming frames for VLANs that do not include this ingress port in their member set will be discarded. (Default: Disabled)

• Packet Type: Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. (Default: All) If the Packet Type is set to "All," the port can accept incoming tagged and untagged packets. Any received packets that are untagged are assigned to the default VLAN. Any tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. If the Packet Type is set to "Tagged Only," the port will drop untagged packets and will only receive tagged packets. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. Switches should be connected to each other with the Packet Type set to "Tagged Only."

• PVID: The PVID (Port VLAN ID) is associated with untagged, ingress packets. It is assigned to untagged frames received on the specified interface. The PVID has no effect on ports that have Packet Type set to "Tagged Only." (Default PVID: 1) It is not possible to remove a port from VLAN 1 unless its PVID has been changed to something other than 1. Outgoing packets are tagged unless the packet's VLAN ID is the same as the PVID. When the PVID is set to "None," all outgoing packets are tagged.

NOTE: If you select "Tagged Only" mode for a port, we recommend setting the PVID to "None" as the standard configuration.

3.2.4 Aggregation

Port trunk allows multiple links to be bundled together and act as a single physical link for increased throughput. It provides load balancing, and redundancy of links in a switched inter-network. Actually, the link does not have an inherent total bandwidth equal to the sum of its component physical links. Traffic in a trunk is distributed across an individual link within the trunk in a deterministic method that called a hash algorithm. The hash algorithm automatically applies load balancing to the ports in the trunk. A port failure within the trunk group causes the network traffic to be directed to the remaining ports. Load balancing is maintained whenever a link in a trunk is lost or returned to service.

3.2.4.1 Aggregation / Trunking Configuration

To assign a port to a trunk, click the required trunk number, and then click "Apply."

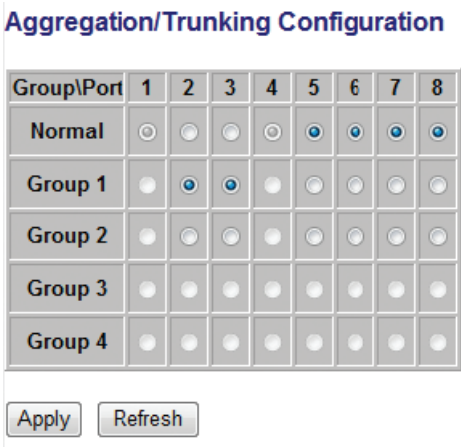Figure 3-8. Aggregation/trunking configuration screen.

3.2.5 LACP

IEEE 802.3ad Link Aggregation Control Protocol (LACP) increases bandwidth by automatically aggregating several physical links together as a logical trunk and providing load balancing and fault tolerance for uplink connections.

3.2.5.1 LACP Port Configuration

• Port: The port number.

• Enabled: Enables LACP on the associated port.

• Key Value: Configures a port's LACP administration key. The port administrative key must be set to the same value for ports that belong to the same link aggregation group (LAG). If this administrative key is not set when an LAG is formed (i.e., it has the null value of 0), this key will automatically be set to the same value as that used by the LAG.

LACP Port Configuration

Port	Protocol Enabled	Key Value
1	☐	auto
2	☐	auto
3	☐	auto
4	☐	auto
5	☐	auto
6	☐	auto
7	☐	auto
8	☐	auto

Apply Refresh

Figure 3-9. LACP port configuration screen.

3.2.6 RSTP

IEEE 802.1w Rapid Spanning tree protocol (LACP) provides a loop-free network and redundant links to the core network with rapid convergence to ensure faster recovery from failed links, enhancing overall network stability and reliability.

3.2.6.1 RSTP System Configuration

• System Priority: This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

• Hello Time: Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1–10 (default is 2).

• Max Age: The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. This also means the maximum life time for a BPDU frame. Number between 6–40 (default is 20).

• Forward Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4–30 (default is 15).

• Force Version: Set and show the RSTP protocol to use. Normal - use RSTP, Compatible—compatible with STP.

Figure 3-10. RSTP system configuration.

3.2.6.2 RSTP Port Configuration

• Port: The port ID. It cannot be changed. Aggregations mean any configured trunk group.

• Enabled: Click on the tick-box to enable/disable the RSTP protocol for the port.

• Edge: Expect the port to be an edge port (linking to an end station) or a link to another STP device.

• Path Cost: This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP pathcost on the port. Number between 0–200000000. 0 means auto generated pathcost.

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	☐		
1	☐	☑	auto
2	☐	☑	auto
3	☐	☑	auto
4	☐	☑	auto
5	☐	☑	auto
6	☐	☑	auto
7	☐	☑	auto
8	☐	☑	auto

Apply   Refresh

Figure 3-11. RSTP port configuration screen.

RSTP System Configuration

System Priority	32768 ▼
Hello Time	
Max Age	
Forward Delay	
Force version	▼

```
0
4096
8192
12288
16384
20480
24576
28672
32768
36864
40960
45056
49152
53248
57344
61440
```

RSTP Port Co   tion

Port	F nabled	Edge	Path Cost
Aggregations			

Figure 3-12. RSTP system configuration screen.

Figure 3-13. RSTP system configuration screen.

3.2.7 IGMP Snooping

IGMP Snooping is the process of listening to IGMP network traffic. IGMP Snooping, as implied by the name, is a feature that allows a layer 2 switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network.

When IGMP Snooping is enabled in a switch, it analyzes all IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

Prevents flooding of IP multicast traffic, and limits bandwidth intensive video traffic to only the subscribers.

3.2.7.1 IGMP Configuration

• IGMP Enabled: When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

• Router Ports: Set if ports are connecting to the IGMP administrative routers.

• Unregistered IPMC Flooding enabled: Set the forwarding mode for unregistered (not joined) IP multicast traffic. The traffic will flood when enabled, and forward to router-ports only when disabled.

• IGMP Snooping Enabled: When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.

• IGMP Querying Enabled: When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.

IGMP Configuration

IGMP Enabled	☑
Router Ports	1☑ 2☑ 3☑ 4☑ 5☑ 6☑ 7☑ 8☑
Unregistered IPMC Flooding enabled	☐

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	☑

[Apply] [Refresh]

Figure 3-14.

3.2.8 Mirroring

Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection on another switch port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system.

3.2.8.1 Mirroring Configuration

• Port to Mirror to: The port that will "duplicate" or "mirror" the traffic on the source port. Only incoming packets can be mirrored. Packets will be dropped when the available egress bandwidth is less than ingress bandwidth.

• Ports to Mirror: Select the ports that you want to mirror from this section of the page. A port will be mirrored when the "Mirroring Enabled" check-box is checked.

Mirroring Configuration

Port	Mirror Source
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐

Mirror Port	1 ▾

[Apply] [Refresh]

Figure 3-15. Mirroring configuration screen.

Mirroring Configuration

Port	Mirror Source
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐

Mirror Port	4 ▾

| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 6 |
| 7 |
| 8 |

[Apply] [Refresh]

Figure 3-16. Mirroring configuration screen.

3.2.9 Quality of Service (QoS)

In QoS Mode, select QoS Disabled, 802.1p, or DSCP to configure the related parameters.

3.2.9.1 QoS Configuration

• Strict: Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

• WRR: Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights with default values of 1, 2, 4, 8 for queues 0 through 7, respectively. (This is the default selection.)

NOTE: WRR can only be selected if Jumbo Frame mode is disabled on the Port Configuration page.
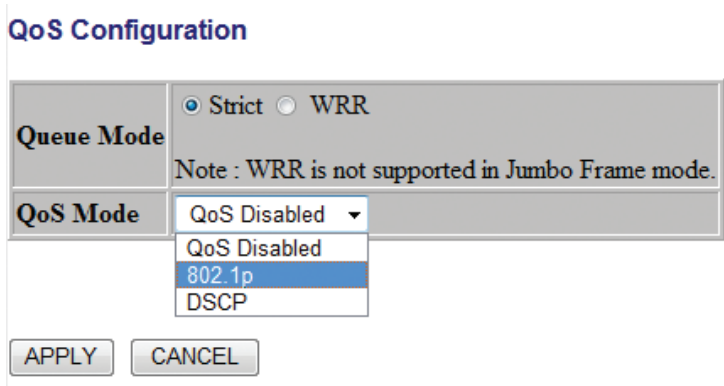
Figure 3-17. QoS configuration screen.

3.2.9.2 QoS Mode: QoS Disabled

When the QoS Mode is set to QoS Disabled, the following table is displayed.
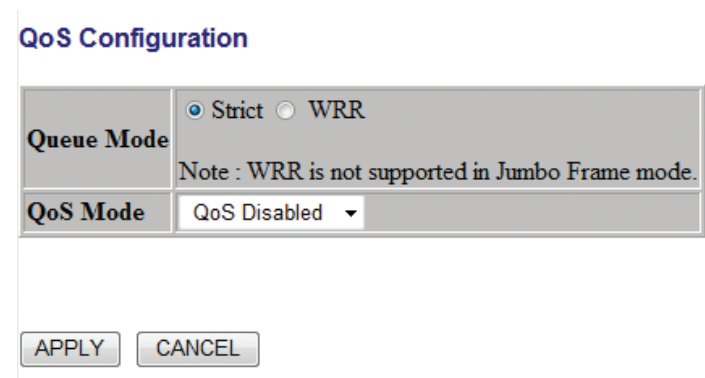
Figure 3-18. QoS disabled screen.

3.2.9.3 QoS Mode: 802.1p

Packets are prioritized using the 802.1p field in the VLAN tag. This field is three bits long, representing the values 0–7. When the QoS Mode is set to 802.1p, the 802.1p Configuration table appears, allowing you to map each of the eight 802.1p values to a local priority queue (low, normal, medium or high). The default settings are shown below.

When the QoS Mode is set to 802.1p, the 802.1p Configuration table is displayed as shown next.

QoS Configuration

Queue Mode	⊙ Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	802.1p
Prioritize Traffic	Custom

Custom
All Low Priority
All Normal Priority
All Medium Priority
All High Priority

802.1p Configu

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal	1	low	2	low	3	normal
4	medium	5	medium	6	high	7	high

APPLY   CANCEL

Figure 3-19. QoS configuration custom selected.

QoS Configuration

Queue Mode	⊙ Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	802.1p
Prioritize Traffic	Custom

802.1p Configuration

802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	medium	1	low	2	low	3	normal
4	medium	5		6	high	7	high

low
normal
medium
high

APPLY   CANCEL

Figure 3-20.

3.2.9.4 QoS Mode: DSCP

DSCP: Packets are prioritized using the DSCP (Differentiated Services Code Point) value. The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0–63. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, allowing you to map each of the DSCP values to a hardware output queue (low, normal, medium or high). The default settings map all DSCP values to the high priority egress queue. Users can use the Prioritize Traffic drop-down list to quickly set the values in the DSCP Configuration table to a common priority queue. Use Custom if you want to set each value individually.

When the QoS Mode is set to DSCP, the DSCP Configuration table is displayed as shown below.

Figure 3-21.

Figure 3-22.

3.2.10 PoE (Power over Ethernet) Configuration

Power over Ethernet (PoE) is an advanced technology providing a whole new application aspect for networking products. PoE products provide power for wide range of devices over an installed CAT5 cable, and is especially useful for VoIP phones, wireless LAN access points and IP cameras.

It is deployed in applications where AC power would be inconvenient, expensive, or not feasible to supply. Web Smart features are able to remote control and centralize the power management.

3.2.10.1 PoE Configuration

Remote access and monitor the attached PD (Powered Device) status by using Enable/Disable function.

• PoE Enabled: POE of the port is able to supply power to the attached PD (Powered Device).

• PD Class: Detect the class of PD.

• Delivering Power (W): Output power.

• Current (mA): The status of the port current.

• Power output voltage per port.

• Power budget percentage of PoE power that has been used.

PoE (Power over Ethernet) Configuration

Port	PoE Enabled	PD Class	Delivering Power [W]	Current [mA]	Voltage [V]	Power Budget [%] (total power = 65W)
1	✓	--	0	0	0	
2	✓	--	0	0	0	
3	✓	--	0	0	0	
4	✓	0	3.903	75.884	51.436	14
5	✓	--	0	0	0	
6	✓	--	0	0	0	
7	✓	--	0	0	0	
8	✓	3	5.208	101.992	51.062	

Apply   Refresh

Figure 3-23.

3.2.11 Storm Control

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

3.2.11.1 Storm Control Configuration

There are three type of traffic that can be rate limited, including broadcast multicast frame and Flooded Uncast Rate.

Storm Control Configuration

Storm Control Number of frames per second	
Broadcast Rate	No Limit ▾
Multicast Rate	No Limit ▾
Flooded unicast Rate	No Limit ▾

Figure 3-24.

• Enable Rate Limit: Click the check box to enable storm control.

• Rate (number of frames per second): The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings.

• Web: Click PORTS, Storm Control. This page enables you to set the broadcast storm control parameters for every port on the switch.

3.3 Monitoring

3.3.1 Statistic Overview

Statistic Overview for all ports

User can mirror traffic from any source port to a target port for real-time analysis the following figures shows clearly the statistics overview.

Clear | Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	2092	17	63016	251	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	45001	197	3355	26	0	0
8	0	0	0	0	0	0

Figure 3-25.

3.3.2 Detailed Statics

| Clear | Refresh | | Port 1 | Port 2 | Port 3 | Port 4 | Port 5 | Port 6 | Port 7 | Port 8 |

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	0	Tx Broad- and Multicast	0
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Aligment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	-	Tx Overflow	-
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Figure 3-26.

3.3.3 LACP Status
3.3.3.1 LACP Aggregation Overview

LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8
Normal								

Legend

	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Refresh

Figure 3-27.

• Port: The port number.

• Port Active: Shows if the port is a member of an active LACP group.

• Partner Port Number: A list of the ports attached at the remote end of this LAG link member.

• Operational Port Key: Current operational value of the key used by this LAG.

3.3.3.2 LACP Port Status

LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	no		
8	no		

Figure 3-28. LACP port status screen.

3.3.4 RSTP Status
3.3.4.1 RSTP VLAN Bridge Overview

RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
12	32780:12-0e-c0-ee-30-e3	2	20	15	Steady	This switch is Root!

Refresh

Figure 3-29. RSTP VLAN bridge overview.

• Hello Time: Interval (in seconds) at which the root device transmits a configuration message.

- Max Age: The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that age out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

- Fwd Delay: The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

- Topology: Indicates if spanning tree topology is steady or undergoing reconfiguration. (The time required for reconfiguration is extremely short, so no values other than "steady" state are likely to be seen in this field.)

- Root ID: The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device, and the port connected to the root device.

3.3.4.2 RSTP Port Status

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP

Figure 3-30. RSTP port status screen.

- Port/Group: The number of a port or the ID of a static trunk.

- Path Cost: The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.

• Edge Port: Shows if this port is functioning as an edge port, either through manual selection (see the RSTP Port Configuration table) or auto-detection.

NOTE: If the switch detects another bridge connected to this port, the manual setting for Edge Port will be overridden, and the port will instead function as a point-to-point connection.

• P2P Port: Shows if this port is functioning as a Point-to-Point connection to exactly one other bridge. The switch can automatically determine if the interface is attached to a point-to-point link or to shared media. If shared media is detected, the switch will assume that it is connected to two or more the switch will assume that it is connected to two or more bridges.

• Protocol: Shows the spanning tree protocol functioning on this port, either STP or STP (that is, STP-compatible mode).

3.3.5 IGMP Status

IGMP Status shows the IGMP Snooping statistics for the entire switch.

• VLAN ID: VLAN ID number.

• Querier: Show whether Querying is enabled.

• Queries transmitted: Show the number of transmitted Query packets.

• Queries received: Show the number of received Query packets.

• v1 Reports: Show the number of received v1 Report packets.

• v2 Reports: Show the number of received v2 Report packets.

• v3 Reports: Show the number of received v2 Report packets.

• v3 Leave: Show the number of v3 leave packets received.

IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
12	Active	1	0	0	0	0	0

Refresh

Figure 3-31. IGMP status screen.

3.3.6 VeriPHY

3.3.6.1 VeriPHY Cable Diagnostics

Users can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open, etc..) and feedback a distance to the fault.

• Cable Diagnostics: Cable diagnostics is performed on a per-port basis. Select the port number from the drop-down list.

• Cable Status: Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

VeriPHY Cable Diagnostics

Port	Port 5 ▾
Mode	Full ▾
	Full
	Anomaly
	Anomaly w/o X-pair

[Apply]

Cable Status

Pair	Length [m]	Status
A	-	-
B	-	-
C	-	-
D	-	-

Figure 3-32.

VeriPHY Cable Diagnostics

Port	Port 5 ▾
Mode	Full ▾

Apply

Cable Status		
Pair	**Length [m]**	**Status**
A	0	Abnormal termination
B	0	Abnormal termination
C	0	Abnormal termination
D	0	Open

Figure 3-33.

VeriPHY Cable Diagnostics

Port	Port 5 ▾
Mode	Anomaly w/o X-pair ▾

Apply

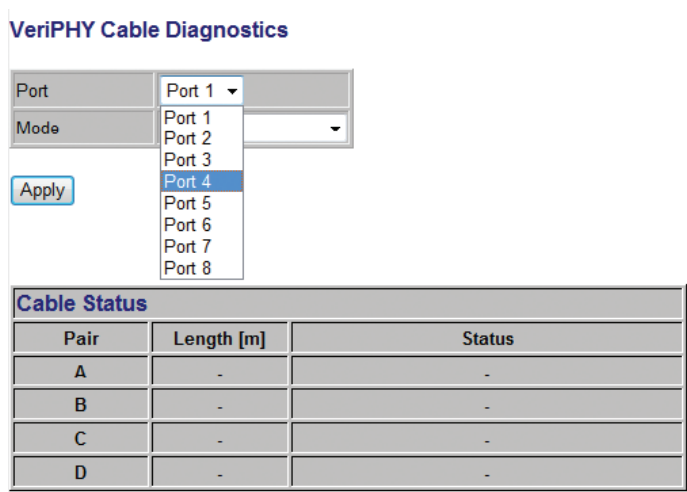| Cable Status		
Pair	**Length [m]**	**Status**
A	0	Abnormal termination
B	0	Abnormal termination
C	0	Abnormal termination
D	0	Open

Figure 3-34.

Figure 3-35.

3.3.7 Ping

This command sends ICMP echo request packets to another node on the network.

3.3.7.1 Ping Parameters

• Target IP Address: IP address of the host.

• Count: Number of packets to send. (Range: 1–20)

• Time Out: setting the time period the host will Ping.

Use the ping command to see if another site on the network can be reached.

The following are some results of the ping command:

• Normal response: The normal response occurs in one to ten seconds, depending on network traffic.

• Destination does not respond: If the host does not respond, a "timeout" appears in ten seconds.

• Destination unreachable: The gateway for this destination indicates that the destination is unreachable.

• Network or host unreachable: The gateway found no corresponding entry in the route table.

Press <Esc> to stop pinging.

Ping Parameters

Target IP address	
Count	1 ▾
Time Out (in secs)	1 ▾

Apply

Ping Results

Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Figure 3-36.

Ping Parameters

Target IP address	192.168.0.1
Count	1
Time Out (in secs)	5 / 10 / 20

Apply

Ping Results

Target IP address	192.168.0.1
Status	Test starting...
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Figure 3-37.

Ping Parameters

Target IP address	192.168.0.1
Count	1
Time Out (in secs)	1 / 5 / 10 / 30

Apply

Ping Results

Target IP address	192.168.0.1
Status	Test starting...
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Figure 3-38.

4. Maintenance

4.1 Warm Restart

Press the "Yes" button to restart the switch. The reset will be complete when the power lights stop blinking.

Warm Restart

Are you sure you want to perform a Warm Restart? Yes No

Figure 4-1. Warm Reset screen.

4.2 Factory Default

This function forces the switch back to the original factory settings. To reset the switch, select "Reset to Factory Defaults" from the drop-down list and click "Apply." The LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory default settings.

Software Upload

瀏覽...

Upload

Figure 4-2. Factory Default screen.

4.3 Software upload

Select "Upgrade Firmware" from the Tools drop-down list then click on the "Browse" button to select the firmware file. Click the APPLY button to upgrade the selected switch firmware file. User can download firmware files for user's switch from http://ftp.blackbox.com/lan/switches/FW/most%20current%20fw.
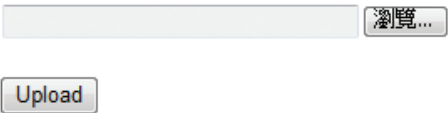
Software Upload

Figure 4-3.

4.4 Configuration File Transfer

Configuration file transfer allows you to save the switch's current configuration or restore a previously saved configuration back to the device. Configuration files can be saved to any location on the web management station. "Upload" the configuration file to save a configuration or "Download" to restore a configuration. Use the "Browse" button to choose a file location on the Web management station, or to find a saved configuration file.

Configuration Upload
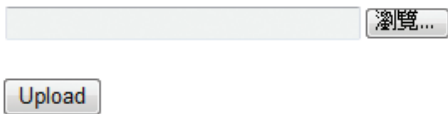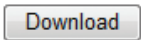

Configuration Download

Figure 4-4.

4.5 Logout

The administrator has write access for all parameters governing the onboard agent. The user should assign a new administrator password as soon as possible, and store it in a safe place.

4.6 Reset Button for the Factory Default Setting

Follow these steps to reset the Web Smart Switch back to the original default:

STEP 1: Turn on the Web Smart Switch

STEP 2: Press and hold the reset button continuously for 5 seconds and release the reset button.

STEP 3: The switch will reboot for 20 seconds and the switch configuration will revert back to the default setting.

724-746-5500 | blackbox.com

724-746-5500 | blackbox.com

Tech support the
way it should be.

Great tech support is just 60 seconds away at
724-746-5500 or blackbox.com.

About Black Box

Black Box provides an extensive range of networking and infrastructure products.
You'll find everything from cabinets and racks and power and surge protection
products to media converters and Ethernet switches all supported by free, live 24/7
Tech support available in 60 seconds or less.

LGB624A, version 2