

Official Tech Documents
The better way to get your HotBrick product up and running

HotBrick GigaBrick 2600

How To

How To install and use typical features of your GigaBrick 2600

USA

7243 NW 54th Street
33166
Miami, FL
www.hotbrick.com
support@hotbrick.com

EUROPE

Generatorstraat 26
Hengelo (Ov), 7556 RC
Amsterdam - Netherlands
www.hotbrick.nl
support@hotbrick.nl

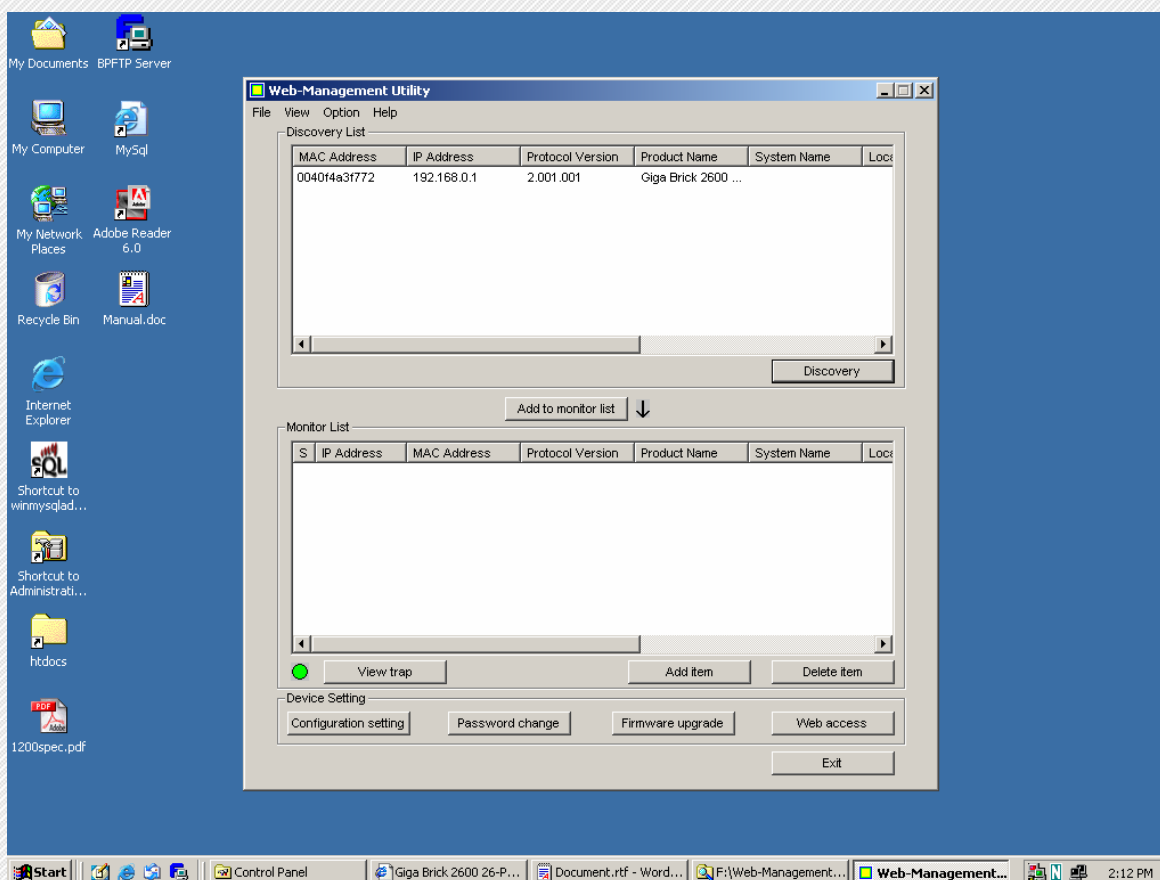
BRAZIL

Francisco Tramontano, 100
05686-010
São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

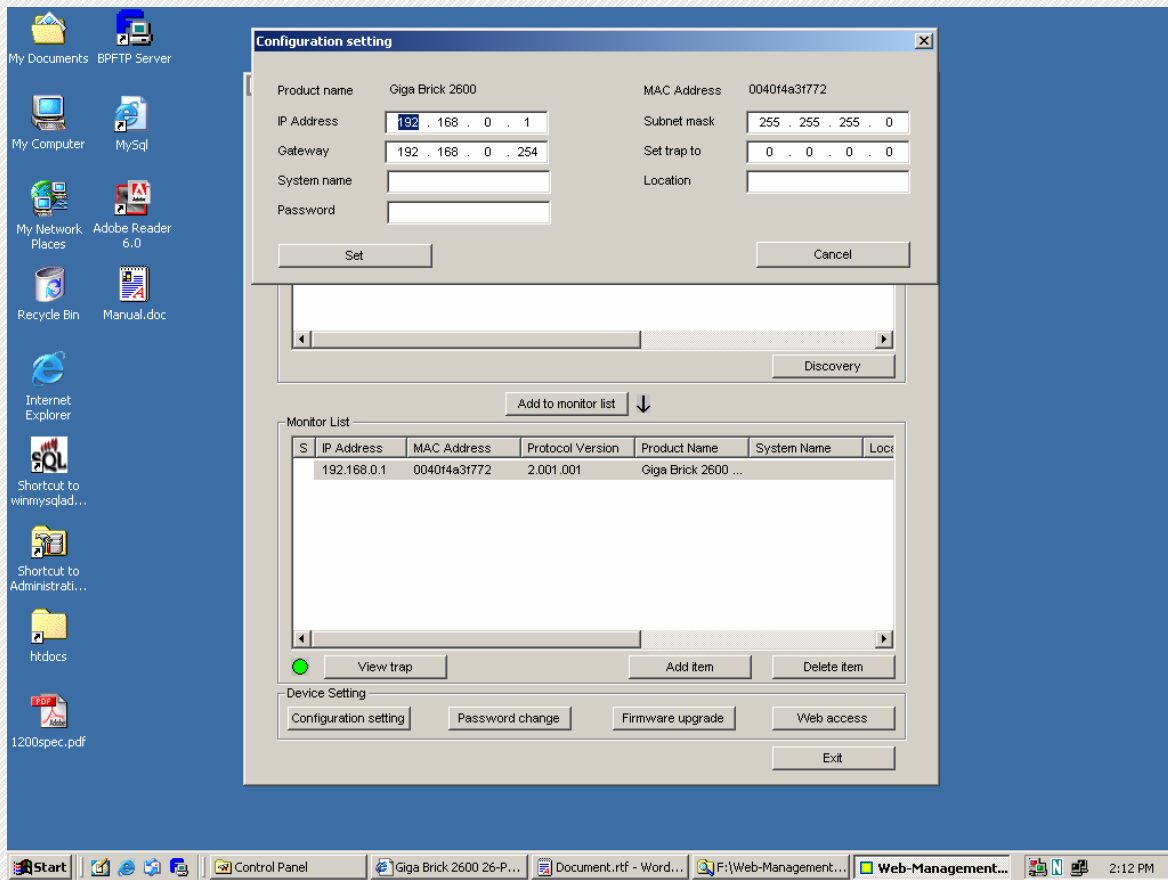
HOTBRICK GIGABRICK 2600 CONFIGURATION

This document describes the initial installation of the Hotbrick Gigabrick 2600 and also the typical functions of a web-managed switch such as VLAN and QoS.

When you have connected the gigabrick you can access the interface by means of the Web-Management Utility. After installing and starting the application you come to the next screen.



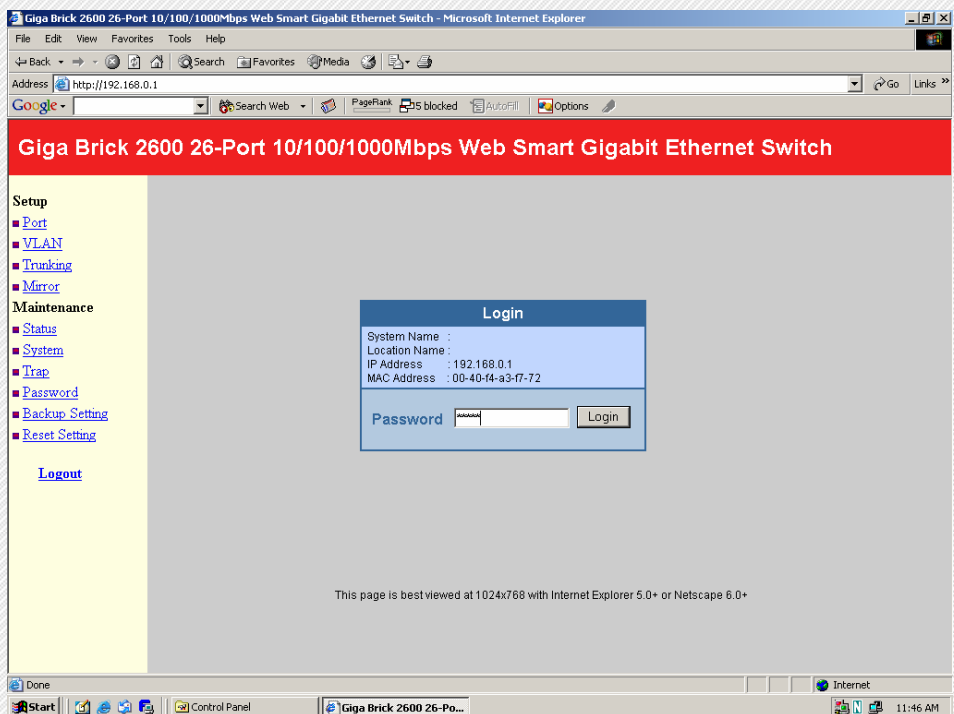
When you select discovery the application will detect the gigabrick as shown on the screenshot. After this you can select the gigabrick and push the "Add to monitor list" button. Then it will appear in the bottom pane and you can select "configuration setting" to go to the next screen.



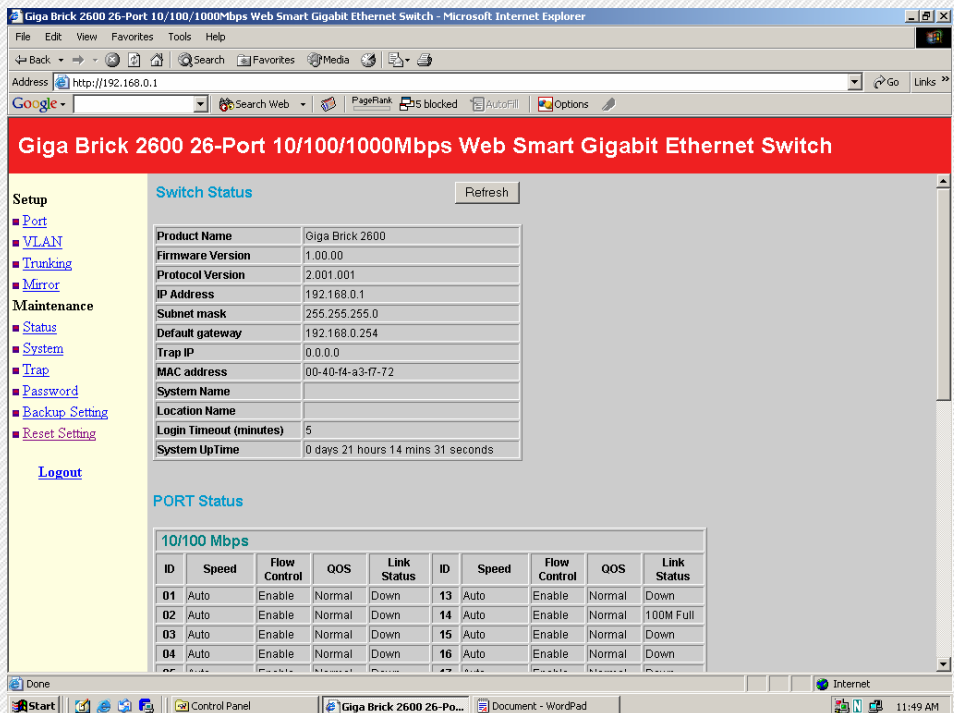
Here you can change the settings that will be needed for your specific network.

Now you can get ready to log on to your gigabrick. In this example we use the default address of 192.168.0.1.

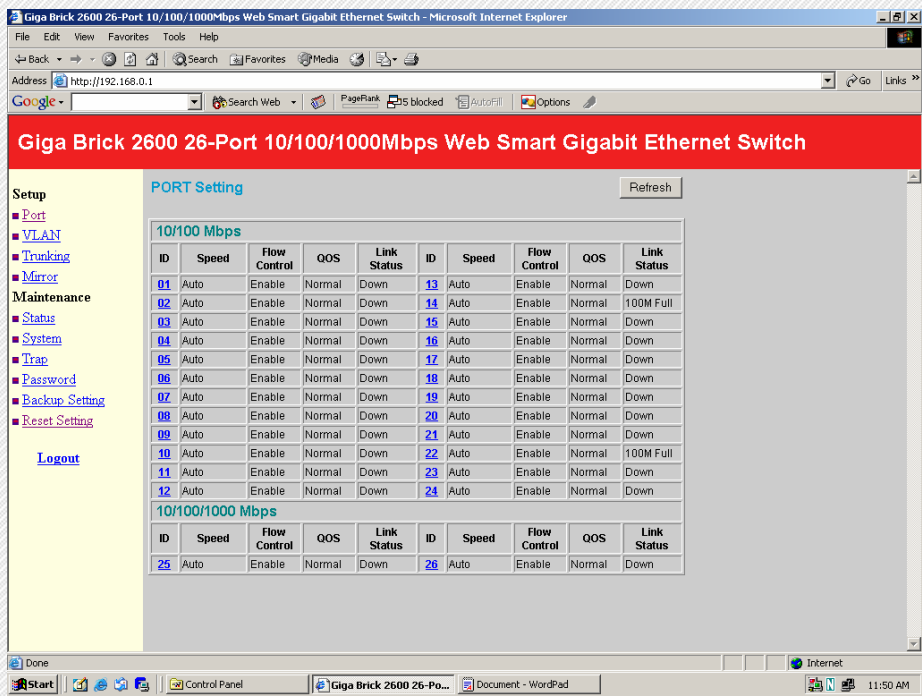
After accessing this address from your browser you will come to the login screen where the password is admin, or you can just use the WEB ACCESS button on the utility.



After login you come to the switch status page where you can check current settings and the status of the switch.

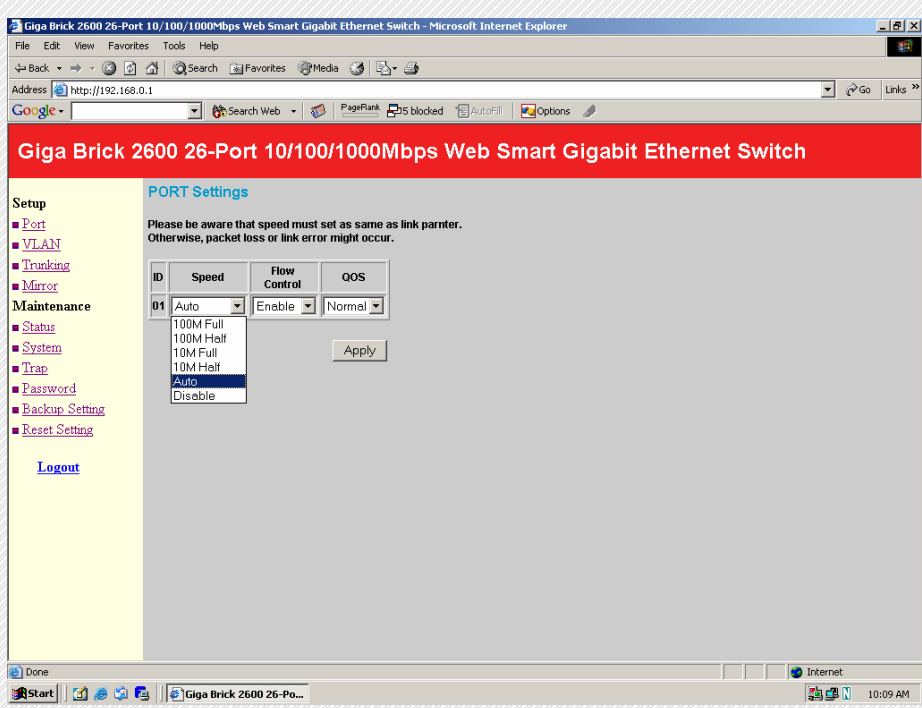


Now we will take a look at the setup starting with the port setting.



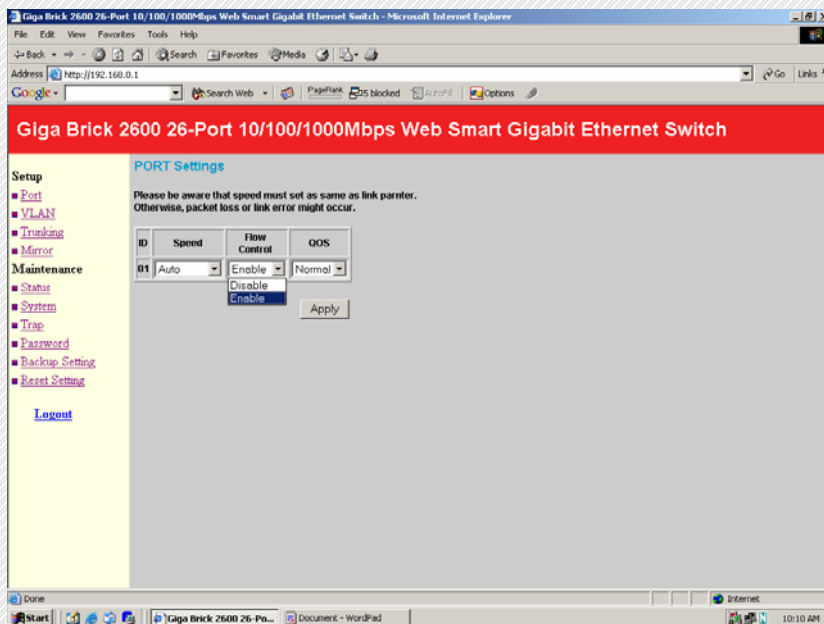
You can change the setting of the port by pressing the blue number of the port.

That will get you to the next screen:



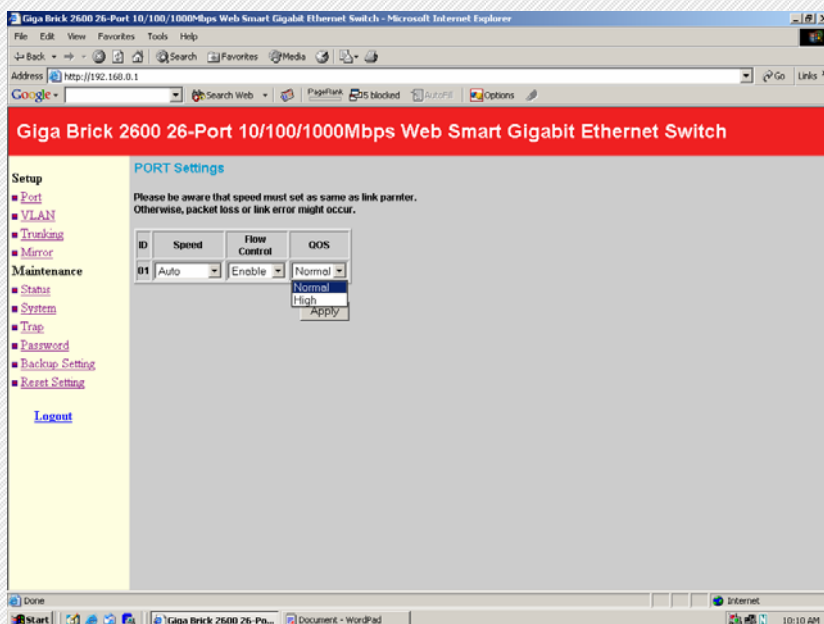
The first setting is the port speed. You probably only need this when you have different speed sub-nets when using a VLAN. In normal conditions you will leave it on auto.

The second setting is flow control. Set it to enable to avoid data transfer overflow.



The third setting is Quality of service. You can set it to normal or high.

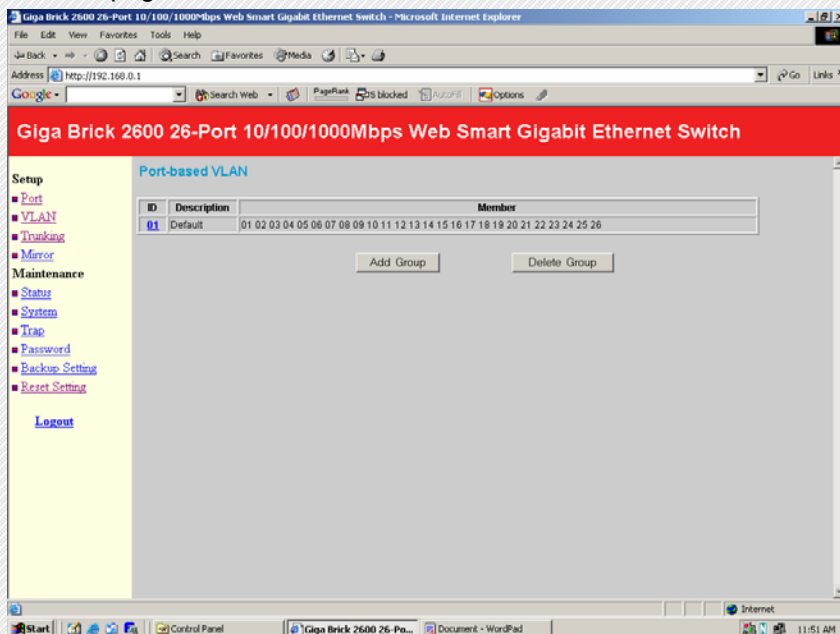
When set to high then the port has a high priority to manage data.



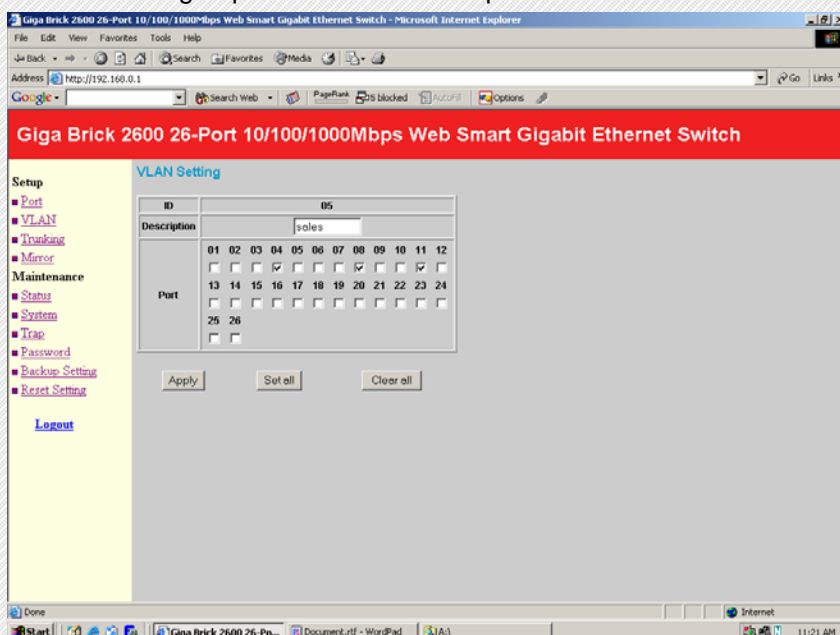
A few points follow for using this setting however:

- It isn't needed when there is enough capacity on your network.
- It works well when the priority ports are a small percentage of the total ports.
- It doesn't help when you run out of capacity or have too many of the priority ports.

The next page is the VLAN function.



You can add a group as in the next example.



USA

7243 NW 54th Street
Miami, FL 33166
www.hotbrick.com
support@hotbrick.com

EUROPE

Generatorstraat 26
Hengelo (Ov), 7556 RC Amsterdam
Netherlands
www.hotbrick.nl

BRAZIL

Francisco Tramontano, 100
05686-010 – São Paulo/SP
www.hotbrick.com.br
suporte@hotbrick.com.br

You can “group” ports to create networks that are independent of the other ports.

There are 2 types of VLANs: layer 3 based and layer 2 based.

The hotbrick is layer 2 based, a so-called port-based VLAN. One of the advantages is that switches that use layer 2 information for VLAN are generally quicker than those that use layer 3 information. End-users that use an unroutable protocol can not be a part of a layer 3 VLAN (netbios). Furthermore Layer 2 VLANs are more effective with IPX or Appletalk.

VLAN implementation benefits:

1. Reduction in the cost of handling user moves and changes. Since these costs can be substantial this argument can be compelling.
2. VLAN implementation will result in a vastly increased ability to manage dynamic networks and realize substantial cost savings. This value proposition is most valid for IP networks. Normally, when a user moves to a different subnet, IP addresses must be manually updated in the workstation. This updating process can consume a substantial amount of time that could be used for more productive endeavors such as developing new network services. VLANs eliminate that issue because VLAN membership is not tied to a workstation's location in the network. This allows moved workstations to retain their original IP addresses and subnet membership.
3. Reduction of Routing for Broadcast Containment Switch. When you can, route only when you must. Although switches certainly provide substantial performance enhancements over layer 3 packet forwarding (routing), switches normally do not filter LAN broadcast traffic; in general, they replicate it on all ports. This not only can cause large switched LAN environments to become flooded with broadcasts, it is also wasteful of precious wide area network bandwidth. As a result, users have traditionally been forced to partition their networks with routers that act as broadcast “firewalls.” Hence, simple switches alone do not allow users to phase out routers completely. One of the primary benefits of VLANs is that LAN switches supporting VLANs can be used to effectively control broadcast traffic, reducing the need for routing. Broadcast traffic from servers and end-stations in a particular VLAN is replicated only on those switch ports connected to end-stations belonging to that VLAN. Broadcast traffic is blocked from ports with no end-stations belonging to that VLAN, in effect creating the same type of broadcast firewall that a router provides. Only packets that are destined for addresses outside the VLAN need to proceed to a router for forwarding.

There are multiple reasons for utilizing VLANs to reduce the need for routing in the network:

1. **Higher Performance and Reduced Latency.** As the network expands, more and more routers are required to divide the network into broadcast domains. As the number of routers increase, latency begins to degrade network performance. A high degree of latency in the network is a problem now for many legacy applications, but it is particularly troublesome for newer applications that feature delay-sensitive multimedia and interactivity. Switches that employ VLANs can accomplish the same division of the network into broadcast domains, but can do so at latencies much lower than those of routers. In addition, performance, measured in packets per second, is usually much higher for switches than for traditional routers. Additionally, latency is also highly correlated to the number of hops a packet must traverse, no matter what internetworking device (switch or router) is located at each hop.
2. **Ease of Administration.** Routers require much more complex configuration than switches; they are “administratively rich.” Reducing the number of routers in the network saves time spent on network management.
3. **Cost.** Router ports are more expensive than switch ports. Also, by utilizing cheaper switch ports, switching and VLANs allow segmentation at a lower cost than would be the case if routers alone were used for segmentation. In comparing VLANs with routing, VLANs have their

disadvantages as well. The primary benefits of VLANs over routing are the creation of broadcast domains without the disadvantages of routing and a reduction in the cost of moves and changes in the network.

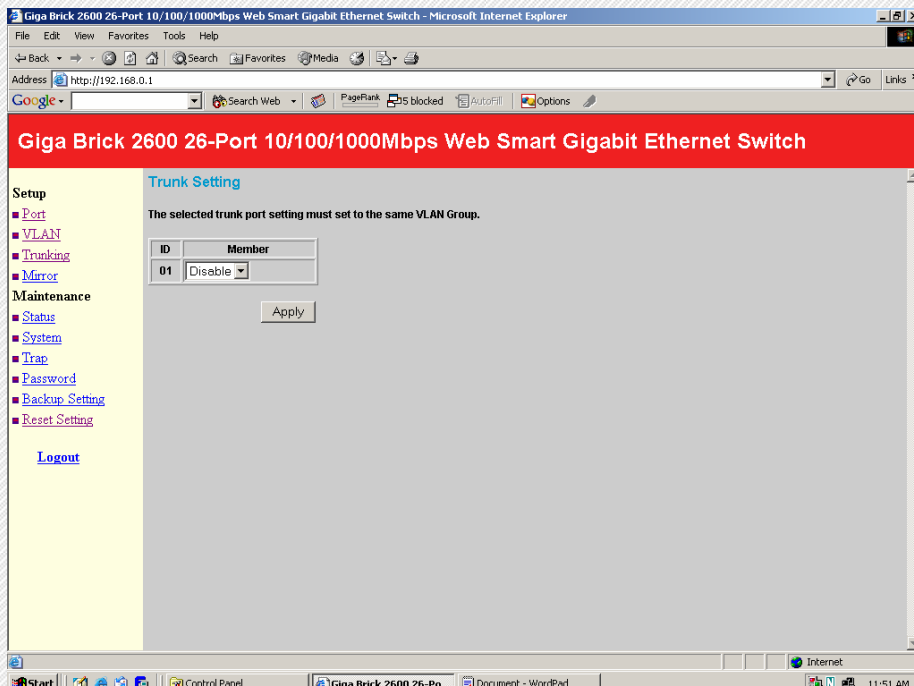
Security

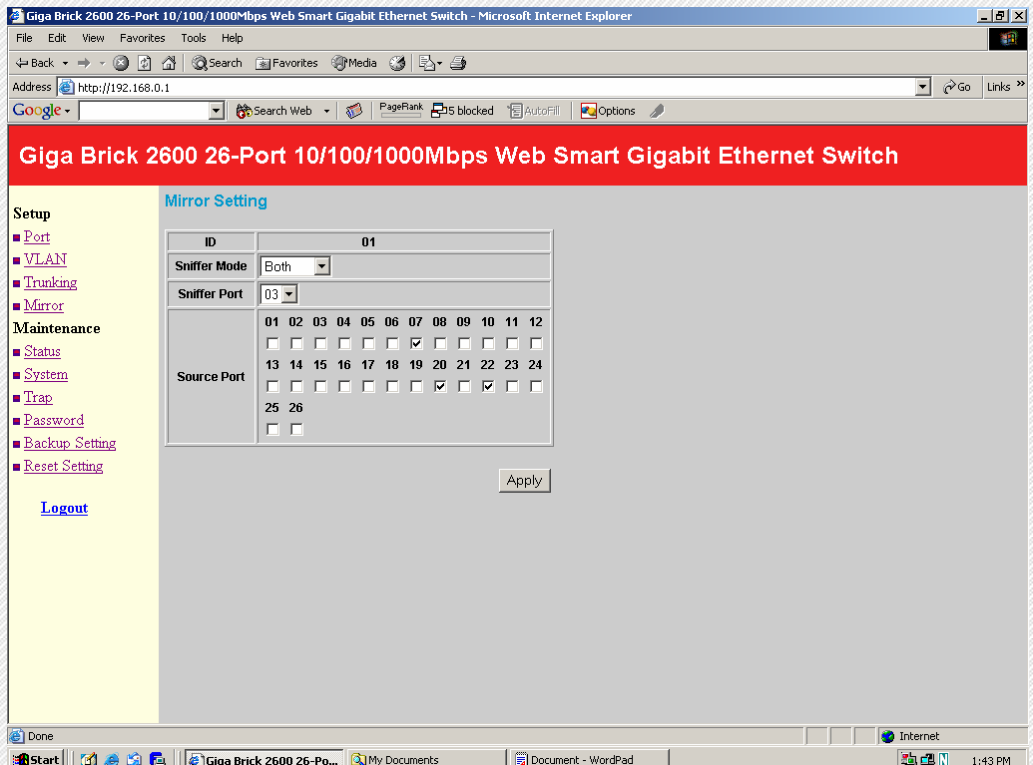
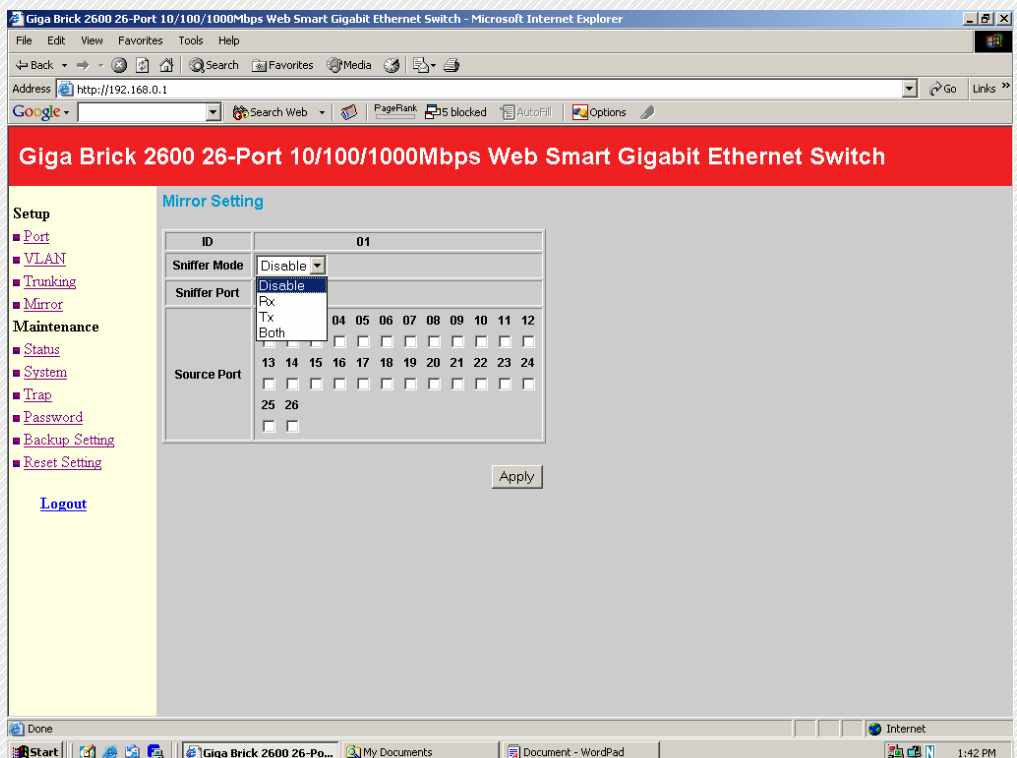
The ability of VLANs to create firewalls can also satisfy more stringent security requirements and thus replace much of the functionality of routers in this area. This is primarily true when VLANs are implemented in conjunction with private port switching. The only broadcast traffic on a single-user segment would be from that user's VLAN (that is, traffic intended for that user). Conversely, it would be impossible to "listen" to broadcast or unicast traffic not intended for that user (even by putting the workstation's network adapter in promiscuous mode), because such traffic does not physically traverse that segment.

WLAN

This is particularly important when you use Wireless Access points in your LAN. Because wireless LAN is the most insecure part of your network you can make a special wireless VLAN group. Even if the security of this group is breached there is no way to listen in on the rest of the network.

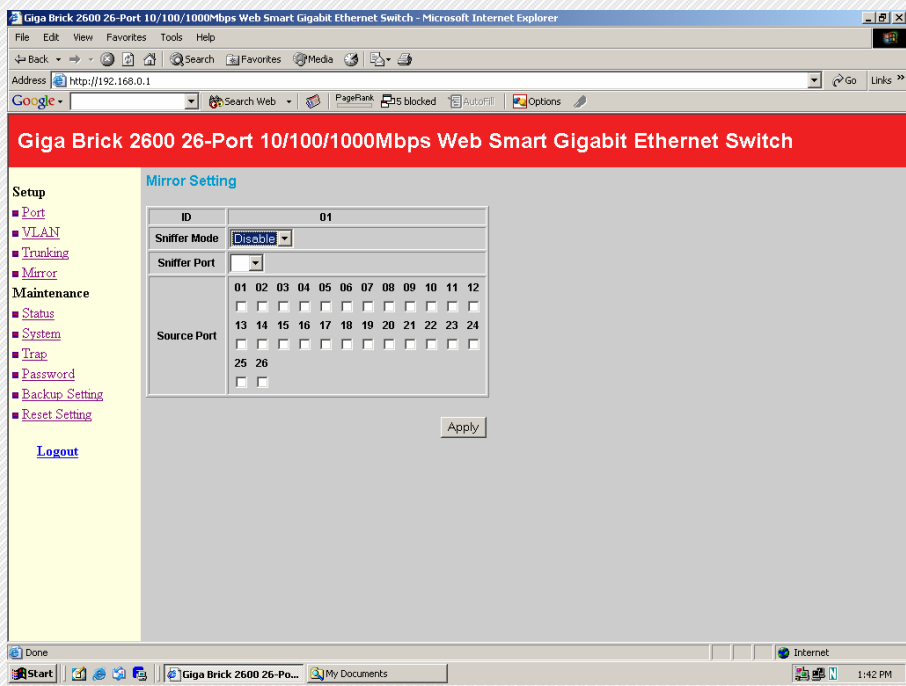
Trunk setting





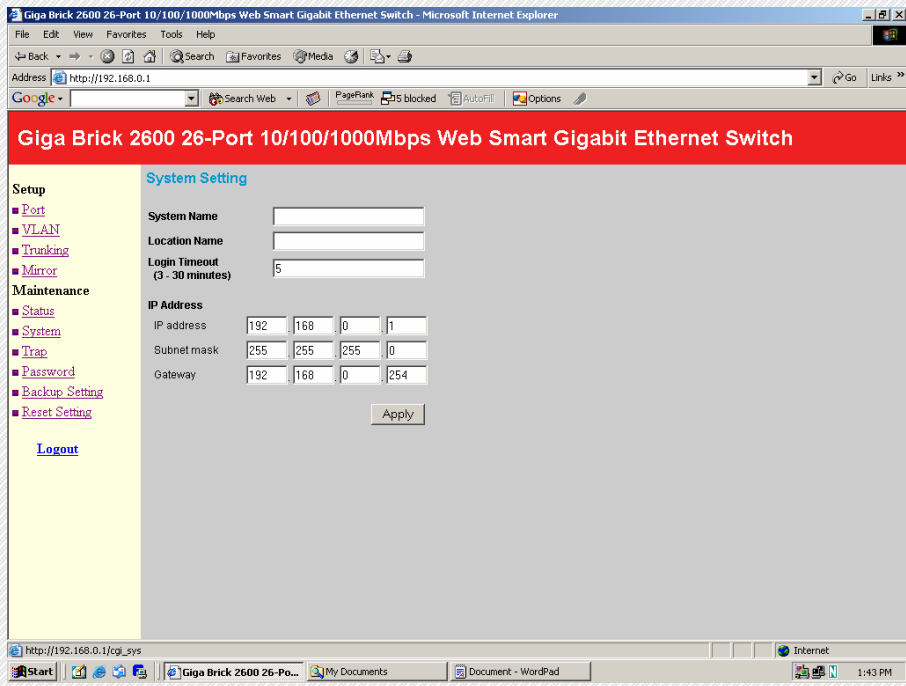
This setting is for cascading 2 or more gigabricks to multiply your number of switch ports.

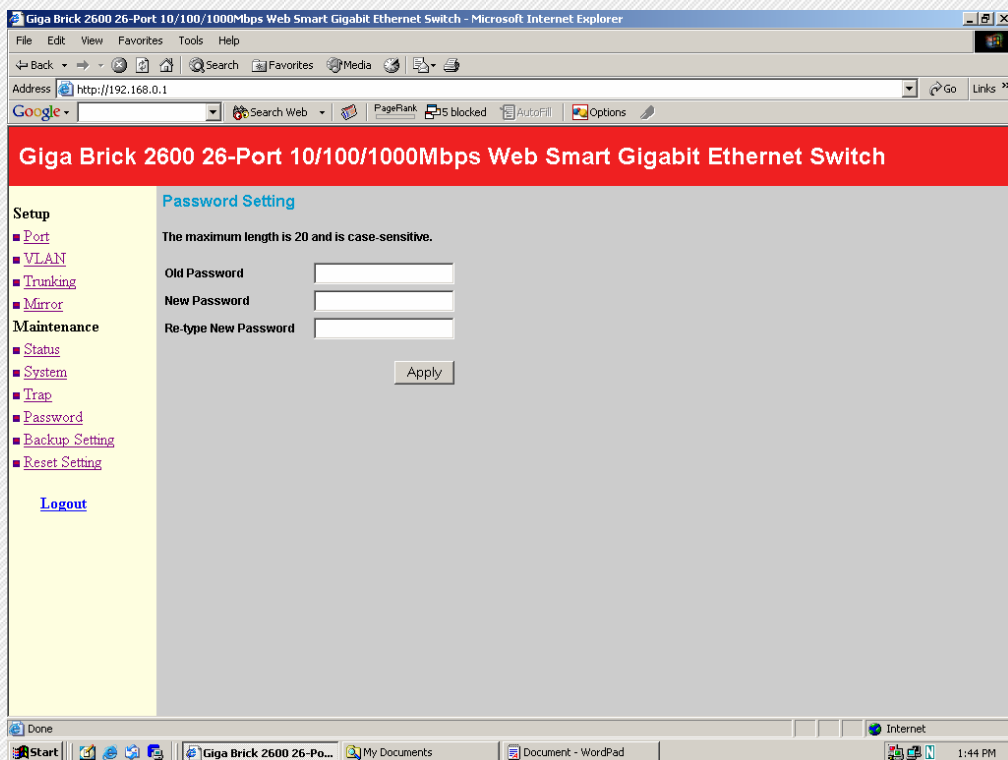
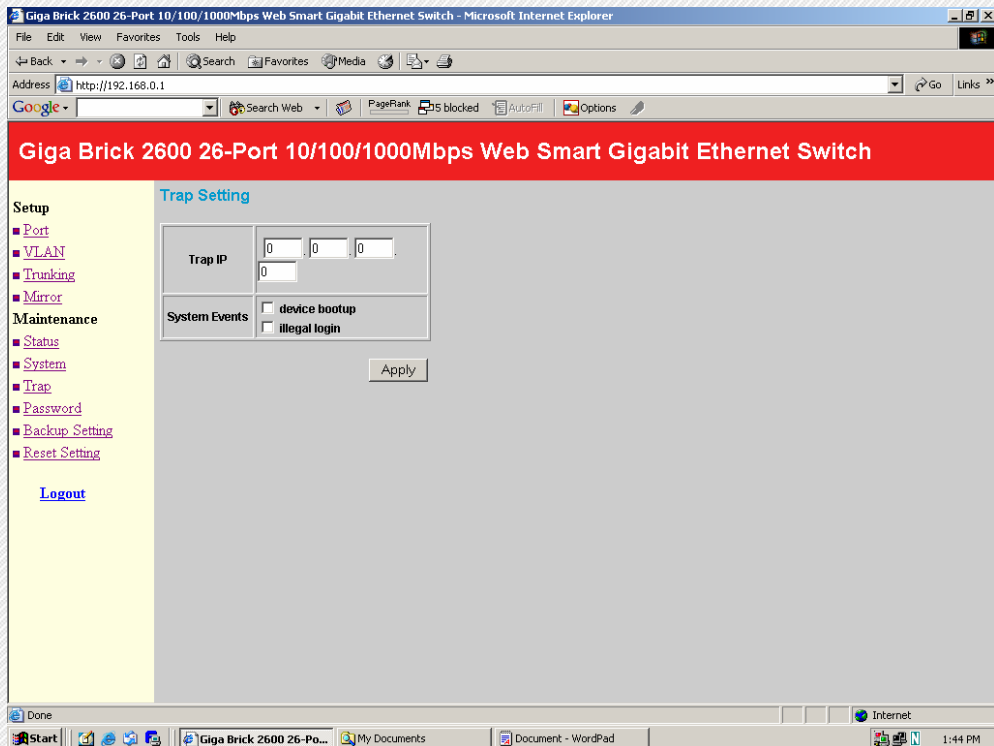
Port mirror setting

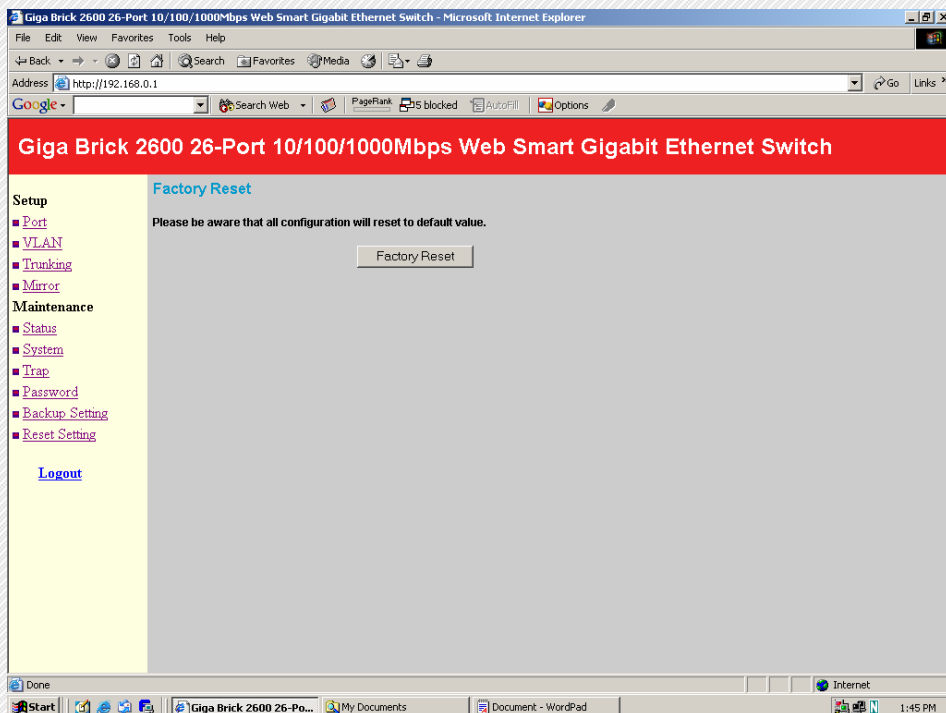
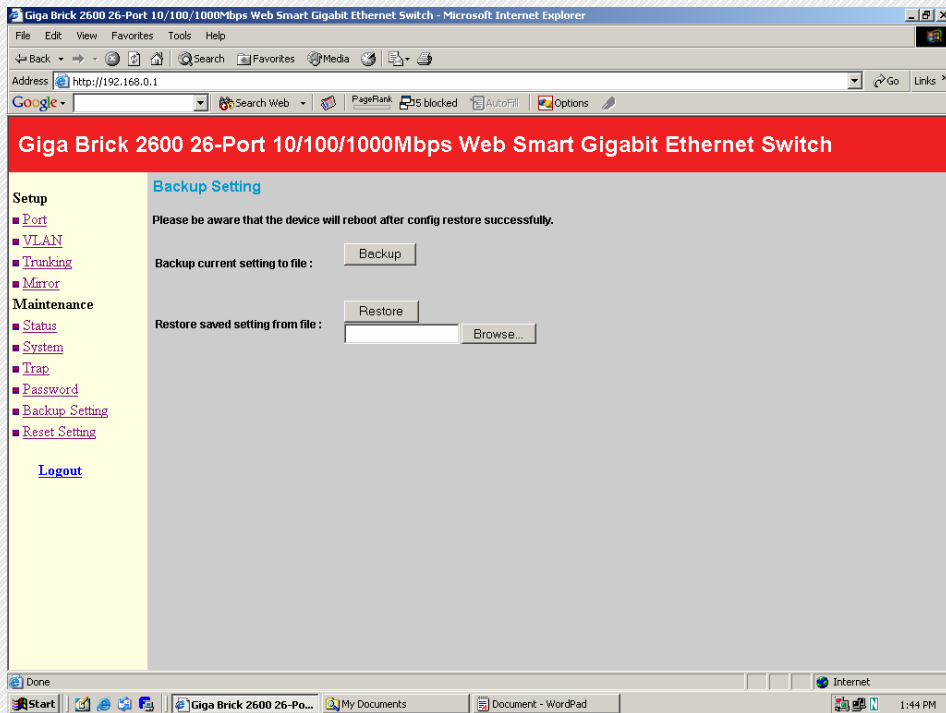


With this option you can forward traffic from a specific port or ports to a sniffer port. Some settings:

The rest of the settings are reasonably straightforward so I will only provide screenshots.







We have covered the settings of the Hotbrick Gigabrick 2600 at this point.

Note that the firmware can be updated for additional functionality; you should use the Web Management Utility in order to do this.

Good luck with your implementation!