



FireTunnel 10



LRE1010E User's Manual

Version Release 4.01 (FW:1.xx)
Oct. 2008

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Firetunnel 10 User's Manual

Copyright Information

© 2008 Black Box Corporation

The contents of this publication may not be reproduced in whole or in part, transcribed, stored, translated, or transmitted in any form or any means, without the prior written consent of Black Box Corporation.

Published by Black Box Corporation. All rights reserved.

Disclaimer

Black Box does not assume any liability arising out of the application of use of any products or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Black Box reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Mac OS is a registered trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered trademarks of Microsoft Corporation.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Safety Warnings



Your Firetunnel 10 is built for reliability and long service life. For your safety, be sure to read and follow the following safety warnings.

- Read this installation guide thoroughly before attempting to set up your Firetunnel 10.
- Your Firetunnel 10 is a complex electronic device. DO NOT open or attempt to repair it yourself. Opening or removing the covers can expose you to high voltage and other risks. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
- Connect the power cord to the correct supply voltage.
- Carefully place connecting cables to avoid people from stepping or tripping on them. DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on.
- DO NOT use Firetunnel 10 in environments with high humidity or high temperatures.
- DO NOT use the same power source for Firetunnel 10 as other equipment.
- DO NOT use your Firetunnel 10 and any accessories outdoors.
- If you mount your Firetunnel 10, make sure that no electrical, water or gas pipes will be damaged during installation.
- DO NOT install or use your Firetunnel 10 during a thunderstorm.
- DO NOT expose your Firetunnel 10 to dampness, dust, or corrosive liquids.
- DO NOT use your Firetunnel 10 near water.
- Be sure to connect the cables to the correct ports.
- DO NOT obstruct the ventilation slots on your Firetunnel 10 or expose it to direct sunlight or other heat sources. Excessive temperatures may damage your device.
- DO NOT store anything on top of your Firetunnel 10.
- Only connect suitable accessories to your Firetunnel 10.
- Keep packaging out of the reach of children.
- If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

Table of Contents

Chapter 1: Introduction

1.1 Overview.....	8
1.2 Product Highlights.....	8
1.2.1 Virtual Private Network Support.....	8
1.2.2 Advanced Firewall Security.....	8
1.2.3 Intelligent Bandwidth Management.....	9
1.3 Package Contents.....	9
1.3.1 Front Panel.....	9
1.3.2 Rear Panel.....	10
1.3.3 Rack Mounting.....	11
1.3.4 Cabling.....	11

Chapter 2: Router Applications

2.1 Overview.....	12
2.2 Bandwidth Management with QoS.....	12
2.2.1 QoS Technology.....	13
2.2.2 QoS Policies for Different Applications.....	14
2.2.3 Guaranteed / Maximum Bandwidth.....	15
2.2.4 Policy Based Traffic Shaping.....	16
2.2.5 Priority Bandwidth Utilization.....	17
2.2.6 Management by IP or MAC address.....	18
2.2.7 DiffServ (DSCP Marking).....	19
2.2.8 DSCP (Matching).....	20
2.3 Virtual Private Networking.....	20
2.3.1 General VPN Setup.....	21
2.3.2 Concentrator.....	22

Chapter 3: Getting Started

3.1 Overview.....	23
3.2 Before You Begin.....	23
3.3 Connecting Your Router.....	24
3.4 Configuring PCs for TCP/IP Networking.....	25

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



3.4.1	Overview.....	25
3.4.2	Windows XP.....	26
3.4.2.1	Configuring.....	26
3.4.2.2	Verifying Settings.....	29
3.4.3	Windows 2000.....	32
3.4.3.1	Configuring.....	32
3.4.3.2	Verifying Settings.....	36
3.4.4	Windows 98 / Me.....	37
3.4.4.1	Installing Components.....	37
3.4.4.2	Configuring.....	42
3.4.4.3	Verifying Settings.....	46
3.5	Factory Default Settings.....	48
3.5.1	Username and Password.....	48
3.5.2	LAN and WAN Port Addresses.....	49
3.6	Information From Your ISP.....	49
3.6.1	Protocols.....	49
3.6.2	Configuration Information.....	50
3.7	Web Configuration Interface.....	55

Chapter 4: Router Configuration

4.1	Overview.....	56
4.2	Status.....	57
4.2.1	ARP Table.....	58
4.2.2	Routing Table.....	59
4.2.3	Session Table.....	60
4.2.4	DHCP Table.....	61
4.2.5	IPSec Status.....	62
4.2.6	PPTP Status.....	63
4.2.7	System Status.....	64
4.2.8	System Log.....	64
4.3	Quick Start.....	65
4.3.1	DHCP.....	65
4.3.2	Static IP.....	66
4.3.3	PPPoE.....	67
4.3.4	PPTP.....	68
4.3.5	Big Pond.....	69

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4 Configuration	70
4.4.1 LAN	71
4.4.1.1 Ethernet	71
4.4.1.2 DHCP Server	72
4.4.1.3 LAN Address Mapping	74
4.4.2 WAN	75
4.4.2.1 WAN	75
4.4.2.1.1 DHCP	75
4.4.2.1.2 Static IP	76
4.4.2.1.3 PPPoE	77
4.4.2.1.4 PPTP	78
4.4.2.1.5 Big Pond	79
4.4.2.2 Bandwidth Settings	80
4.4.2.3 WAN IP Alias	81
4.4.3 System	82
4.4.3.1 Time Zone	83
4.4.3.2 Remote Access	84
4.4.3.3 Firmware Upgrade	85
4.4.3.4 Backup / Restore	85
4.4.3.5 Restart	86
4.4.3.6 Password	87
4.4.3.7 Ping & Trace	87
4.4.4 Firewall	88
4.4.4.1 Packet Filter	89
4.4.4.2 URL Filter	91
4.4.4.3 LAN MAC Filter	93
4.4.4.4 Block WAN Request	94
4.4.4.5 Intrusion Detection	95
4.4.5 VPN	96
4.4.5.1 IPSec	96
4.4.5.1.1 IPSec Wizard	96
4.4.5.1.2 IPSec Policy	99
4.4.5.2 PPTP	104
4.4.6 QoS	106
4.4.7 Virtual Server	110
4.4.7.1 DMZ	111
4.4.7.2 Port Forwarding	111

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.8	Advanced.....	114
4.4.8.1	Static Route.....	114
4.4.8.2	Dynamic DNS.....	115
4.4.8.3	Device Management.....	117
4.4.8.4	IGMP.....	119
4.4.8.5	VLAN Bridge.....	119
4.4.8.6	Schedule.....	120
4.5	Log & E-mail Alert.....	122
4.5.1	Log Configuration.....	122
4.5.2	System Log Server.....	122
4.5.3	E-mail Alert.....	123
4.6	Save Configuration To Flash.....	124
4.7	Logout.....	125

Chapter 5: Trouble Shooting

5.1	Basic Functionality.....	126
5.1.1	Router Won't Turn On.....	126
5.1.2	LEDs Never Turn Off.....	126
5.1.3	LAN or Internet Port Not On.....	126
5.1.4	Forgot My Password.....	127
5.2	LAN Interface.....	127
5.2.1	Can't Access Firetunnel 10 from the LAN.....	127
5.2.2	Can't Ping Any PC on the LAN.....	128
5.2.3	Can't Access Web Configuration Interface.....	128
5.2.3.1	Pop-up Windows.....	130
5.2.3.2	Javascripts.....	130
5.2.3.3	Java Permissions.....	131
5.3	WAN Interface.....	132
5.3.1	Can't Get WAN IP Address from the ISP.....	132
5.4	ISP Connection.....	132
5.5	Problems with Date and Time.....	134
5.6	Restoring Factory Defaults.....	134

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Chapter 1: Introduction

1.1 Overview

Congratulations on purchasing Firetunnel 10 Router from Black Box. Combining a router with an Ethernet network switch, Firetunnel 10 is a state-of-the-art device that provides everything you need to get your network connected to the Internet over your Cable or DSL connection quickly and easily. The Quick Start Wizard and DHCP Server will get first-time users up and running with minimal fuss and configuration, while sophisticated Quality of Service (QoS) and traffic management features grant advanced users total control over their network and Internet connection.

This manual illustrates the many features and functions of Firetunnel 10, and even takes you through the various ways you can apply this versatile device to your home or office. Take the time now to familiarize yourself with Firetunnel 10.

1.2 Product Highlights

1.2.1 Virtual Private Network Support

Firetunnel 10 supports comprehensive IPSec VPN protocols for businesses to establish private encrypted tunnels over the Internet to ensure data transmission security among multiple sites, such as a branch office or dial-up connection. Up to 2 simultaneous IPSec VPN connections are possible on Firetunnel 10, with performance of up to 4Mbps.

1.2.2 Advanced Firewall Security

Aside from intelligent broadband sharing, Firetunnel 10 offers integrated firewall protection with advanced features to secure your network from outside attacks. Stateful Packet Inspection (SPI) determines if a data packet is permitted to enter the private LAN. Denial of Service (DoS) prevents hackers from interrupting network services via malicious attacks. In addition, Firetunnel 10 firewall can be configured to alert you via email should your network come under fire, offering both tight network security and peace of mind.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



1.2.3 Intelligent Bandwidth Management

Firetunnel 10 utilizes Quality of Service (QoS) to give you full control over the priority of both incoming and outgoing data, ensuring that critical data such as customer information moves through your network, even while under a heavy load. Transmission speeds can be throttled to make sure users are not saturating bandwidth required for mission-critical data transfers. Priority types of upload data can also be changed, allowing Firetunnel 10 to automatically sort out actual speeds for unmatched convenience.

1.3 Package Contents

Firetunnel 10

Firetunnel 10 iBusiness Security Gateway Small-Office

Bracket x 2 (for rack-mounting)

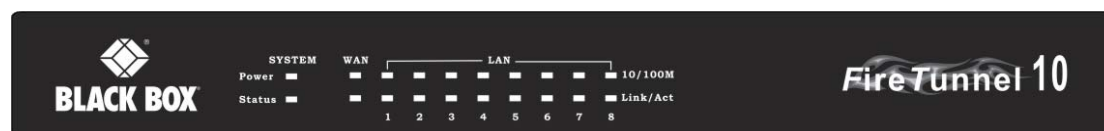
Screw x 4 (for rack-mounting)

Getting Started CD-ROM

Quick Start Guide

AC-DC Power Adapter (12VDC, 1A)

1.3.1 Front Panel



LED	Function
Power	A solid light indicates a steady connection to a power source.
Status	A blinking light indicates the device is writing to flash memory.
WAN	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

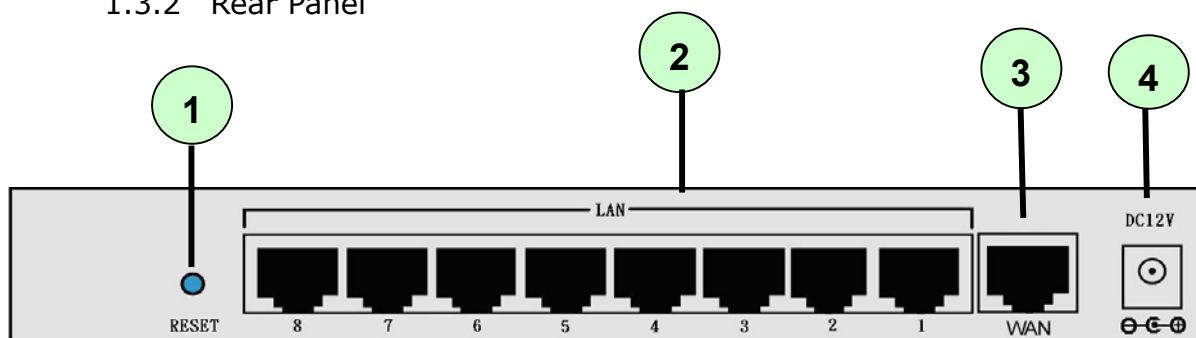
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



	Not lit when connected at 10Mbps. Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.
LAN 1 – 8	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps. Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.

1.3.2 Rear Panel



Port		Meaning
1	RESET	After the device is powered on, press it to reset the device or restore to factory default settings. 0-3 seconds: The Status LED will light 6 seconds above: restore to factory default settings (this is used when you cannot login to the router. E.g. forgot the password)
2	LAN 1X – 8X (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the eight LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
3	WAN	WAN 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
4	DC12V	Connect DC power adapter here.(DC12V Power)

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



1.3.3 Rack Mounting

To rack mount Firetunnel 10, carefully secure the device to your rack on both sides using the included brackets and screws. See the diagram below for a more detailed explanation.



1.3.4 Cabling

Most Ethernet networks currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector.

One of the most common causes of networking problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of Firetunnel 10, verify that the LAN link and WAN line LEDs are lit. If they are not, check to see that you are using the proper cabling.

Chapter 2: Router Applications

2.1 Overview

Your Firetunnel 10 Router is a versatile device that can be configured to not only protect your network from malicious attackers, but also ensure optimal usage of available bandwidth with Quality of Service (QoS). Alternatively, Firetunnel 10 can also be set to handle secure connections with Virtual Private Networking (VPN).

The following chapter describes how Firetunnel 10 can work for you.

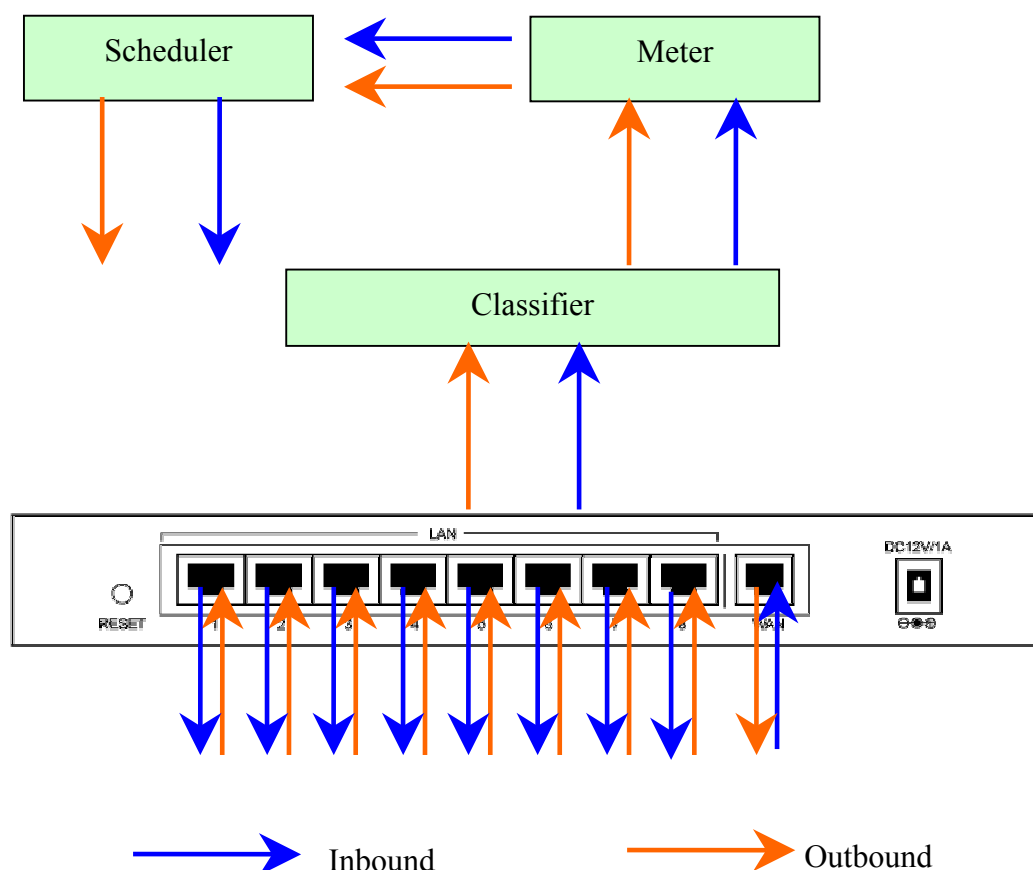
2.2 Bandwidth Management with QoS

Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router. By doing so, the router can ensure that latency-sensitive applications like voice, bandwidth-consuming data like gaming packets, or even mission critical files efficiently move through the router even under a heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

2.2.1 QoS Technology

QoS generally involves the prioritization of network traffic. QoS is comprised of three major components: Classifier, Meter, and Scheduler. Each of these components has a distinct role in ensuring that incoming and outgoing data is managed according to user specifications.

The Classifier analyses incoming packets and marks each one according to configured parameters. The Meter communicates the drop priority to the Scheduler and measures the temporal priorities of the output stream against configured parameters. Finally, the Scheduler schedules each packet for transmission based on information from both the Classifier and the Meter.



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

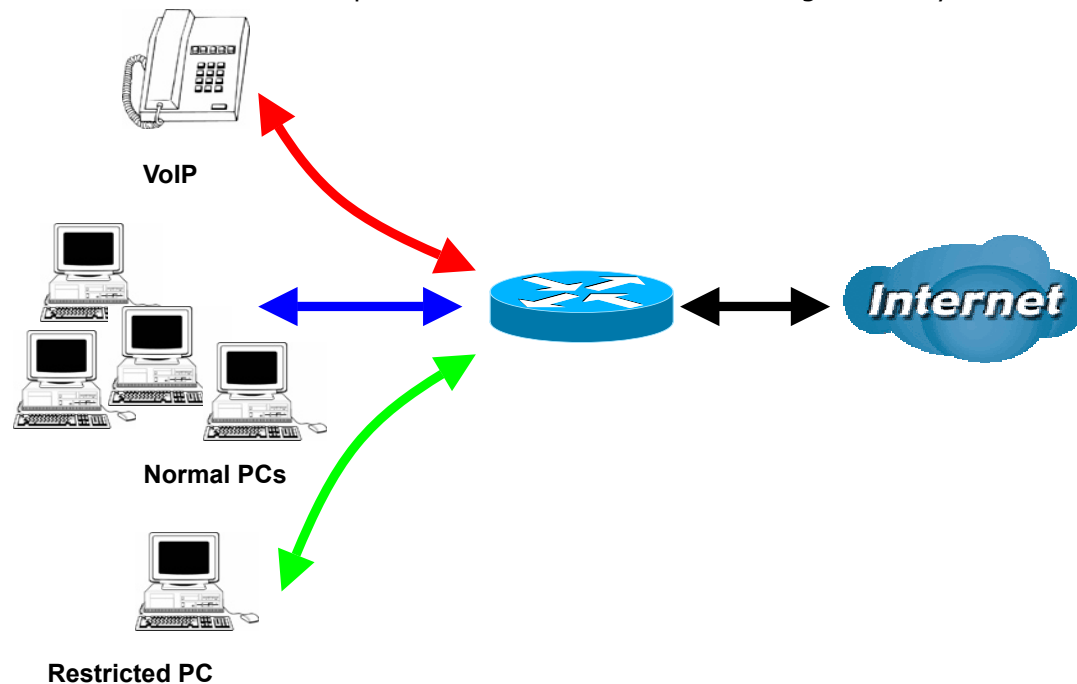
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.2 QoS Policies for Different Applications

By setting different QoS policies according to the applications you are running, you can use Firetunnel 10 to optimize the bandwidth that is being used on your network.



As illustrated in the diagram above, applications such as Voiceover IP (VoIP) require low network latencies to function properly. If bandwidth is being used by other applications such as an FTP server, users using VoIP will experience network lag and/or service interruptions during use. To avoid this scenario, this network has assigned VoIP with a guaranteed bandwidth and higher priority to ensure smooth communications. The FTP server, on the other hand, has been given a maximum bandwidth cap to make sure that regular service to both VoIP and normal Internet applications is uninterrupted.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.3 Guaranteed / Maximum Bandwidth

Setting a Guaranteed Bandwidth ensures that a particular service receives a minimum percentage of bandwidth. For example, you can configure Firetunnel 30 to reserve 10% of the available bandwidth for a particular computer on the network to transfer files.

Alternatively you can set a Maximum Bandwidth to restrict a particular application to a fixed percentage of the total throughput. Setting a Maximum Bandwidth of 20% for a file sharing program will ensure that no more than 20% of the available bandwidth will be used for file sharing.

Quality of Service			
Add QoS Rule			
Interface	WAN1 Outbound		
Application	FTP		
Guaranteed	10	%	
Maximum	20	%	
Priority	6 (Lowest)		
DSCP Marking	Disable		
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address		
Bandwidth Type	<input checked="" type="radio"/> Shared Bandwidth <input type="radio"/> Bandwidth per Source IP Address		
Source IP Address Range	From 192.168.100.1	To	192.168.100.100
Destination IP Address Range	From 0.0.0.0	To	255.255.255.255
Protocol	Any		
Source Port Range	From 1	To	65535
Destination Port Range	From 1	To	65535
DSCP	Any		
Schedule	**Always		
<input type="button" value="Apply"/>			

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.4 Policy Based Traffic Shaping

Policy Based Traffic Shaping allows you to apply specific traffic policies across a range of IP addresses or ports. This is particularly useful for assigning different policies for different PCs on the network. Policy based traffic shaping lets you better manage your bandwidth, providing reliable Internet and network service to your organization.

Quality of Service			
Add QoS Rule			
Interface	WAN1 Outbound		
Application	FTP		
Guaranteed	10	%	
Maximum	20	%	
Priority	6 (Lowest) ▾		
DSCP Marking	Disable ▾		
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address		
Bandwidth Type	<input checked="" type="radio"/> Shared Bandwidth <input type="radio"/> Bandwidth per Source IP Address		
Source IP Address Range	From 192.168.100.1	To	192.168.100.100
Destination IP Address Range	From 0.0.0.0	To	255.255.255.255
Protocol	Any ▾		
Source Port Range	From 1	To	65535
Destination Port Range	From 1	To	65535
DSCP	Any ▾		
Schedule	**Always		
Candidates ▸			
Apply			

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.5 Priority Bandwidth Utilization

Assigning priority to a certain service allows Firetunnel 30 to give either a higher or lower priority to traffic from this particular service. Assigning a higher priority to an application ensures that it is processed ahead of applications with a lower priority and vice versa.

Quality of Service			
Add QoS Rule			
Interface	WAN1 Outbound		
Application	FTP		
Guaranteed	10	%	
Maximum	20	%	
Priority	3 (Normal) ▼		
DSCP Marking	0 (Highest) ▼		
Address Type	1		
Bandwidth Type	2		
Source IP Address Range	3 (Normal) ▼		
Destination IP Address Range	4		
Protocol	5		
Source Port Range	6 (Lowest) ▼		
Destination Port Range	From 100.1 To 192.168.100.100		
DSCP	To 255.255.255.255		
Schedule	Any ▼		
Apply			

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.6 Management by IP or MAC address

Firetunnel 30 can also be configured to apply traffic policies based on a particular IP or MAC address. This allows you to quickly assign different traffic policies to a specific computer on the network.

Quality of Service		
Add QoS Rule		
Interface	WAN1 Outbound	
Application	FTP	
Guaranteed	10	%
Maximum	20	%
Priority	3 (Normal) ▼	
DSCP Marking	Disable ▼	
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address	
Bandwidth Type	<input checked="" type="radio"/> Shared Bandwidth <input type="radio"/> Bandwidth per Source IP Address	
Source IP Address Range	From 192.168.100.1	To 192.168.100.100
Destination IP Address Range	From 0.0.0.0	To 255.255.255.255
Protocol	Any ▼	
Source Port Range Helper ▶	From 1	To 65535
Destination Port Range Helper ▶	From 1	To 65535
DSCP	Any ▼	
Schedule Candidates ▶	**Always	
<input type="button" value="Apply"/>		

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.7 DiffServ (DSCP Marking)

DiffServ (a.k.a. DSCP Marking) allows you to classify traffic based on IP DSCP values. These markings can be used to identify traffic within the network. Other interfaces can match traffic based on the DSCP markings. DSCP markings are used to decide how packets should be treated, and is a useful tool to give precedence to varying types of data.

Quality of Service			
Add QoS Rule			
Interface	WAN1 Outbound		
Application	FTP		
Guaranteed	10	%	
Maximum	20	%	
Priority	3 (Normal) ▾		
DSCP Marking	Disable ▾		
Address Type	Disable		
Bandwidth Type	Best Effort		
Source IP Address Range	Premium		
Destination IP Address Range	Gold service(L)		
Protocol	Gold service(M)		
Source Port Range	Gold service(H)		
Destination Port Range	Silver service(L)		
DSCP	Silver service(M)		
Schedule	Silver service(H)		
	Bronze service(L)		
	Bronze service(M)		
	Bronze service(H)		
	**Always		
<input type="button" value="Apply"/>			

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.2.8 DSCP (Matching)

Just like the DSCP Marking, DSCP is used on traffics (Both inbound rules and outbound rules have DSCP matching). DSCP matching is used to identify traffic for the rule. (It is just like what source IP and destination IP do). When this option of the QoS rule is selected, the QoS rule will only be applied to the packets whose DSCP field's IP header matches the criteria selected. These markings can be used to identify traffic within the network.

Quality of Service	
Add QoS Rule	
Interface	WAN Outbound
Application	<input type="text"/>
Guaranteed	<input type="text" value="1"/> kbps
Maximum	<input type="text" value="102400"/> kbps
Priority	3 (Normal) <input type="button" value="v"/>
DSCP Marking	<input type="text" value="Any"/> <input type="button" value="v"/>
Address Type	<input type="radio"/> Address
Bandwidth Type	<input type="radio"/> Bandwidth per Source IP Address
Source IP Address Range	<input type="text" value="f"/> To <input type="text" value="255.255.255.255"/>
Destination IP Address Range	<input type="text" value="f"/> To <input type="text" value="255.255.255.255"/>
Protocol	<input type="text" value="f"/>
Source Port Range Helper <input type="button" value="▶"/>	<input type="text" value="f"/> To <input type="text" value="65535"/>
Destination Port Range Helper <input type="button" value="▶"/>	<input type="text" value="f"/> To <input type="text" value="65535"/>
DSCP	<input type="text" value="Any"/> <input type="button" value="v"/>
<input type="button" value="Apply"/>	

2.3 Virtual Private Networking

A Virtual Private Network (VPN) enables you to send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link. As such, it is perfect for connecting branch offices to headquarter across the Internet in a secure fashion.

The following section discusses Virtual Private Networking with Firetunnel 10.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

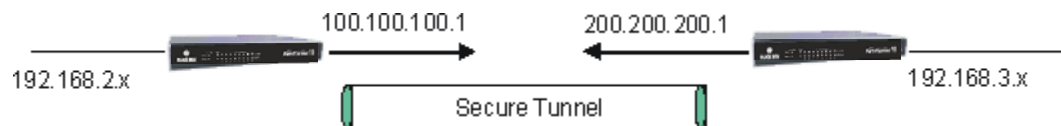
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

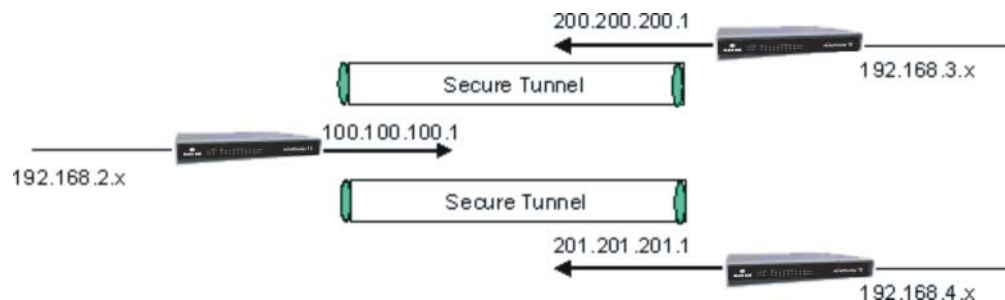


2.3.1 General VPN Setup

There are typically three different VPN scenarios. The first is a **Gateway to Gateway** setup, where two remote gateways communicate over the Internet via a secure tunnel.



The next type of VPN setup is the **Gateway to Multiple Gateway** setup, where one gateway (Headquarter) is communicating with multiple gateways (Branch Offices) over the Internet. As with all VPNs, data is kept secure with secure tunnels.



The final type of VPN setup is the **Client to Gateway**. A good example of where this can be applied is when a remote sales person accesses the corporate network over a secure VPN tunnel.



VPN[D4] provides a flexible, cost-efficient, and reliable way for companies of all sizes to stay connected. One of the most important steps in setting up a VPN is proper planning. The following sections demonstrate the various ways of using Firetunnel 10 to setup your VPN.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2.3.2 Concentrator

The VPN Concentrator provides an easy way for branch offices to connect to headquarter through a VPN tunnel. All branch office traffic will be redirected to the VPN tunnel to headquarter with the exception of LAN-side traffic. This way, all branch offices can connect to each other through headquarter via the headquarter' firewall management. You can also configure Firetunnel 10 to function as a VPN Concentrator.

Chapter 3: Getting Started

3.1 Overview

Firetunnel 10 is designed to be a powerful and flexible network device that is also easy to use. With an intuitive web-based configuration, Firetunnel 10 allows you to administer your network via virtually any Java-enabled web browser and is fully compatible with Linux, Mac OS, and Windows 98/Me/NT/2000/XP operating systems.

The following chapter takes you through the very first steps to configuring your network for Firetunnel 10. Take a look and see how easy it is to get your network up and running.

3.2 Before You Begin

Firetunnel 10 is a flexible and powerful networking device. To simplify the configuration process and increase the efficiency of your network, consider the following items before setting up your network for the first time:

1. Plan your network

You may need a fully qualified domain name either for convenience or if you have a dynamic IP address. See Chapter 2: Router Applications for more information.

2. Set up your accounts

Have access to the Internet and locate the Internet Service Provider (ISP) configuration information.

3. Determine your network management approach

Firetunnel 10 is capable of remote management. However, this feature is not active by default. If you reset the device, remote administration must be enabled again. If you decide to manage your network remotely, be sure to change the default password to something more secure.

4. Prepare to physically connect Firetunnel 10 to Cable or DSL modems and a computer.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Be sure to also review the Safety Warnings located in the preface of this manual before working with your Firetunnel 10.

3.3 Connecting Your Router

Connecting Firetunnel 10 is an easy three-step process:

1. Connect Firetunnel 10 to your LAN by connecting Ethernet cables from your networked PCs to the LAN ports on the router. Connect Firetunnel 10 to your broadband Internet connection via router's WAN port.



2. Plug Firetunnel 10 to an AC outlet with the included AC Power Adapter.



3. Ensure that the Power and WAN LEDs are solidly lit, and that on any LAN port that has an Ethernet cable plugged in the LED is also solidly lit. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that Firetunnel 10 is ready.



If the router does not power on, please refer to **Chapter 5: Troubleshooting** for possible solutions.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



3.4 Configuring PCs for TCP/IP Networking

Now that your Firetunnel 10 is connected properly to your network, it's time to configure your networked PCs for TCP/IP networking.

In order for your networked PCs to communicate with your router, they must have the following characteristics:

1. Have a properly installed and functioning Ethernet Network Interface Card (NIC).
2. Be connected to Firetunnel 10, either directly or through an external repeater hub via an Ethernet cable.
3. Have TCP/IP installed and configured with an IP address.

The IP address for each PC may be a fixed IP address or one that is obtained from a DHCP server. If using a fixed IP address, it is important to remember that it must be in the same subnet as the router. The default IP address of Firetunnel 10 is 192.168.1.254 with a subnet mask of 255.255.255.0. Using the default configuration, networked PCs must reside in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253. However, you'll find that the quickest and easiest way to configure the IP addresses for your PCs is to obtain the IP addresses automatically by using the router as a DHCP server.

If you are unable to access the web configuration interface, check to see if you have any software-based firewalls installed on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of Firetunnel 10.

The following sections outline how to set up your PCs for TCP/IP networking. Refer to the applicable section for your PC's operating system.

3.4.1 Overview

Before you begin, make sure that the TCP/IP protocol and a functioning Ethernet network adapter is installed on each of your PCs.

The following operating systems already include the necessary software components you need to install TCP/IP on your PCs:

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



- Windows 95/98/Me/NT/2000/XP
- Mac OS 7 and later
- All versions of UNIX/Linux

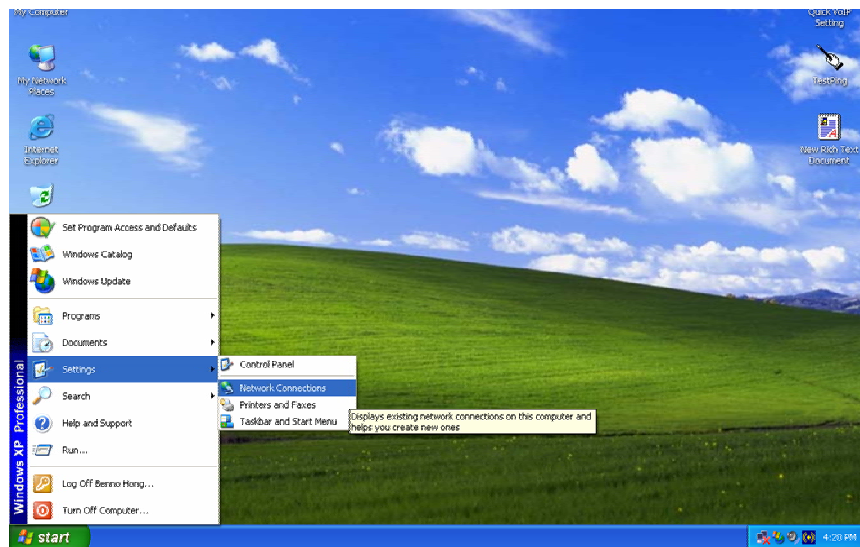
If you are using Windows 3.1, you must purchase a third-party TCP/IP application package.

Any TCP/IP capable workstation can be used to communicate with or through the Firetunnel 10. To configure other types of workstations, please consult the manufacturer's documentation.

3.4.2 Windows XP

3.4.2.1 Configuring

1. Select **Start > Settings > Network Connections**.



Black Box Corporation

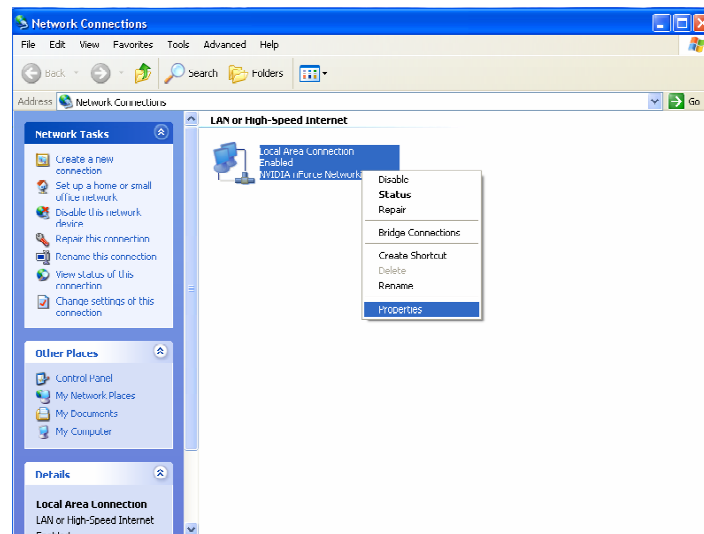
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

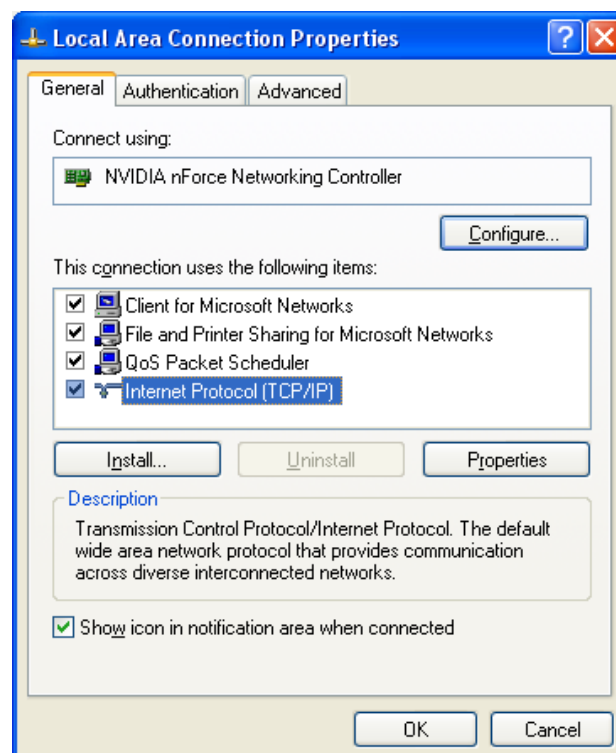
EU, Africa, Asia, South America, Australia: www.blackbox.eu



2. In the **Network Connections** window, right-click **Local Area Connection** and select **Properties**.



3. Select **Internet Protocol (TCP/IP)** and click **Properties**.



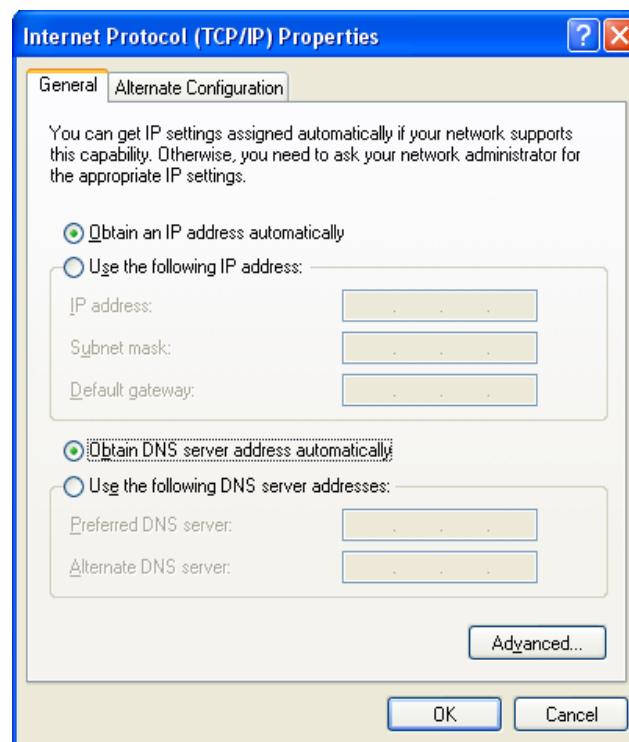
- 4a. To have your PC obtain an IP address automatically, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons.

Black Box Corporation

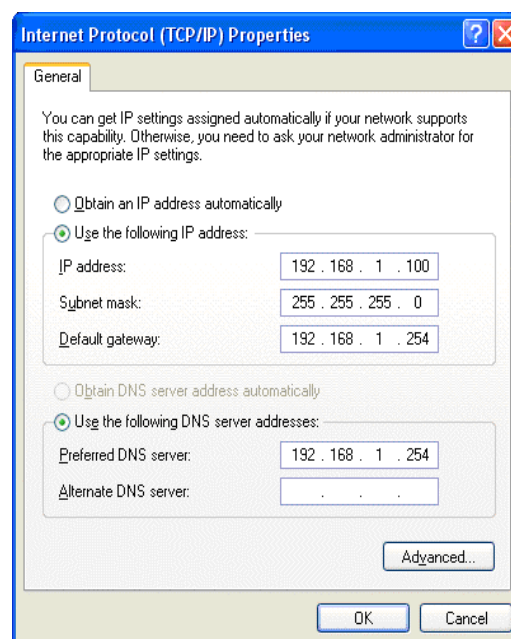
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4b. To manually assign your PC a fixed IP address, select the **Use the following IP address** radio button and enter your desired IP address, subnet mask, and default gateway in the blanks provided. Remember that your PC must reside in the same subnet mask as the router. To designate a DNS server, select the **Use the following DNS server** and fill in the preferred DNS address.



5. Click **OK** to finish the configuration.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

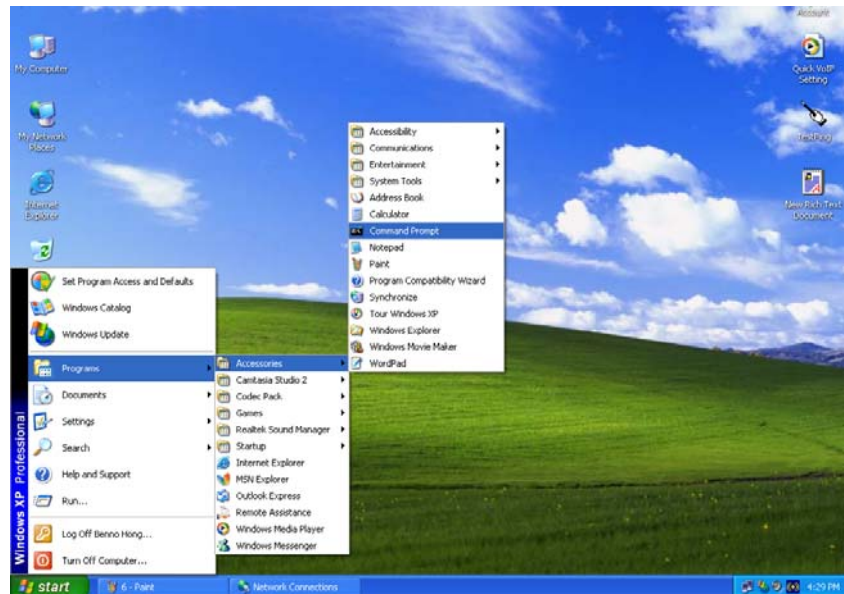
EU, Africa, Asia, South America, Australia: www.blackbox.eu



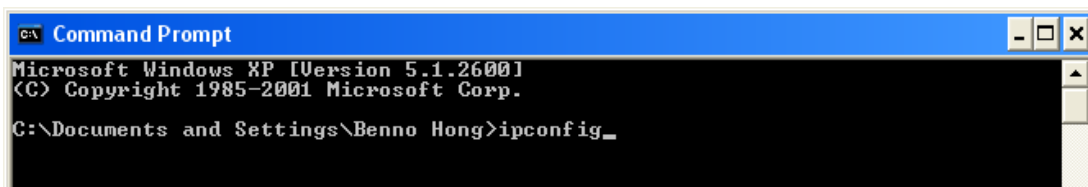
3.4.2.2 Verifying Settings

To verify your settings using a command prompt:

1. Click **Start > Programs > Accessories > Command Prompt**.

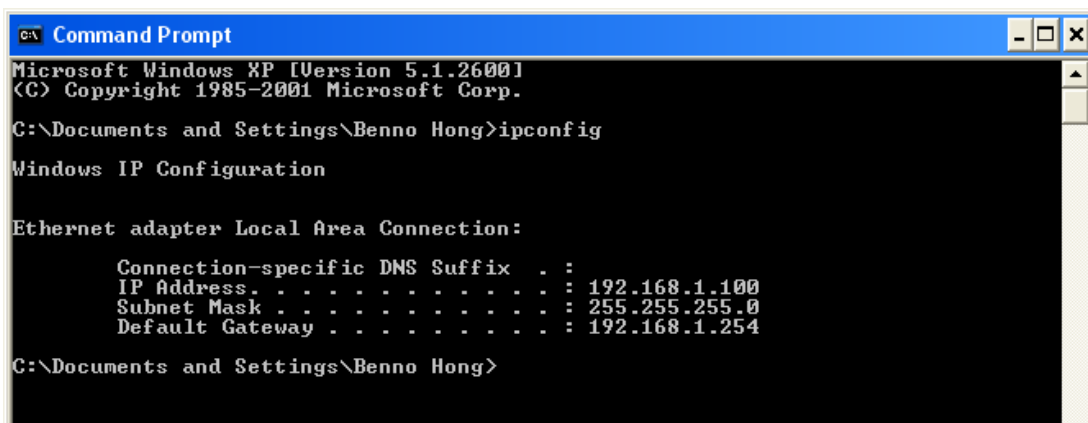


2. In the Command Prompt window, type `ipconfig` and then press **ENTER**.



If you are using Firetunnel 10's default settings, your PC should have:

- An IP address between 192.168.1.1 and 192.168.1.253
- A subnet mask of 255.255.255.0



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

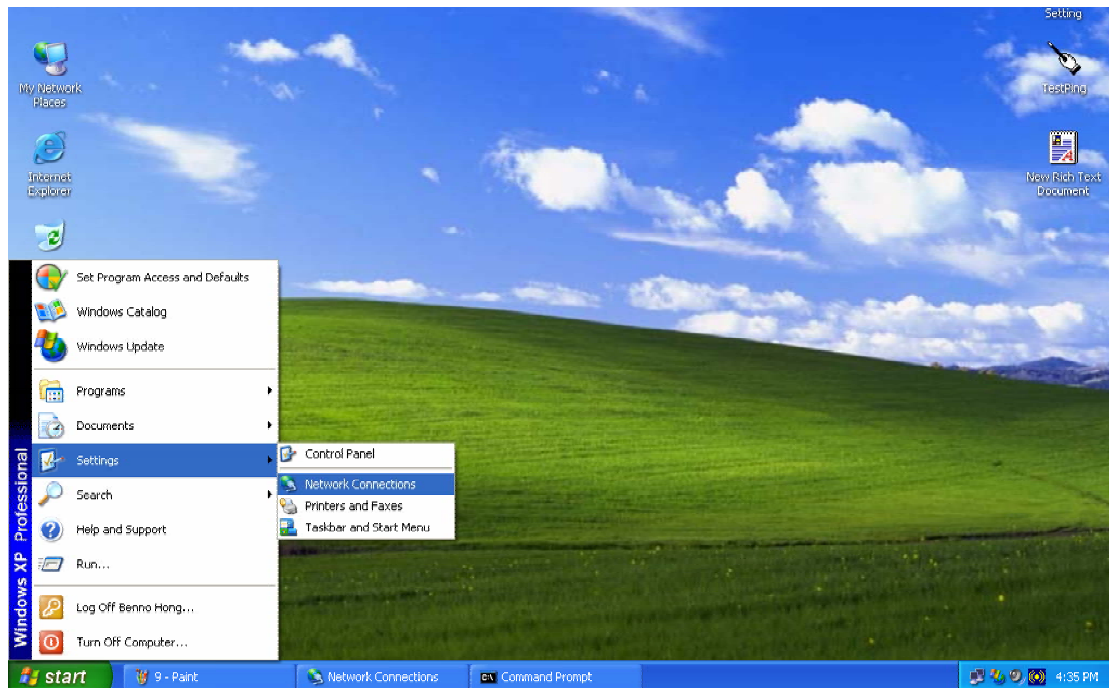
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

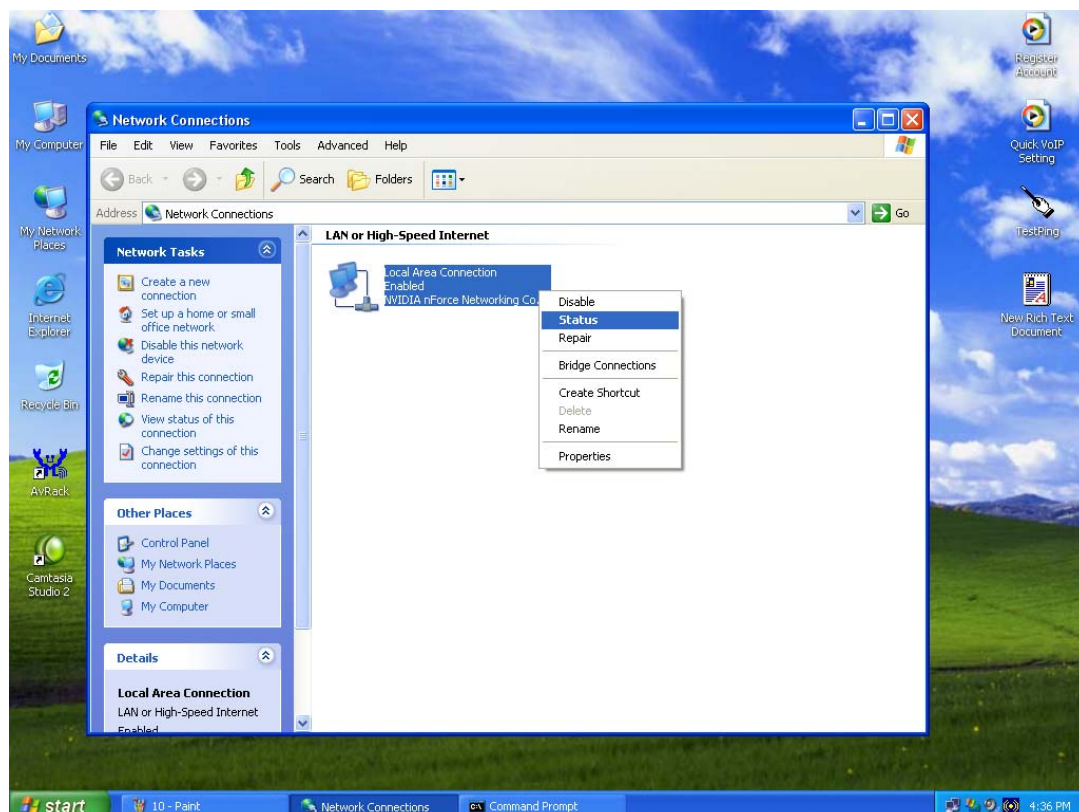


To verify your settings using the Windows XP GUI:

1. Click **Start > Settings > Network Connections**.



2. Right click one of the network connections listed and select **Status** from the pop-up menu.



Black Box Corporation

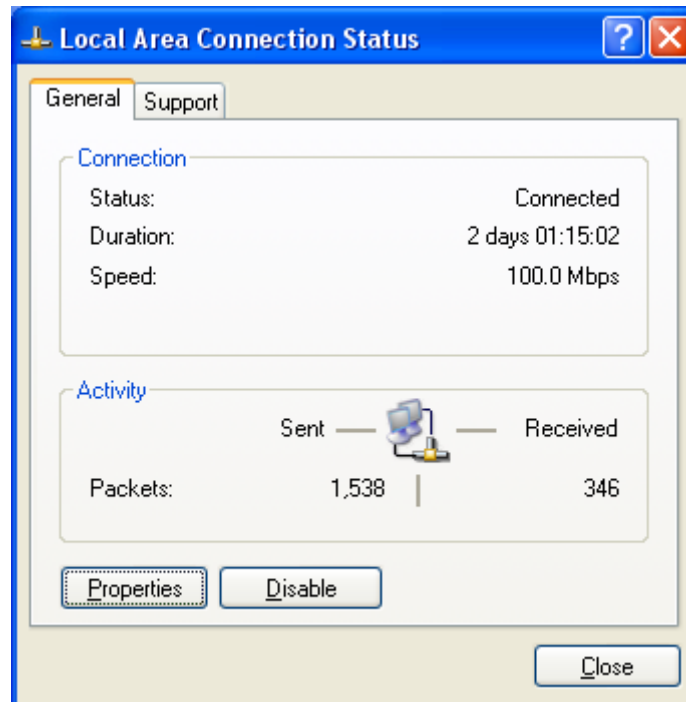
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

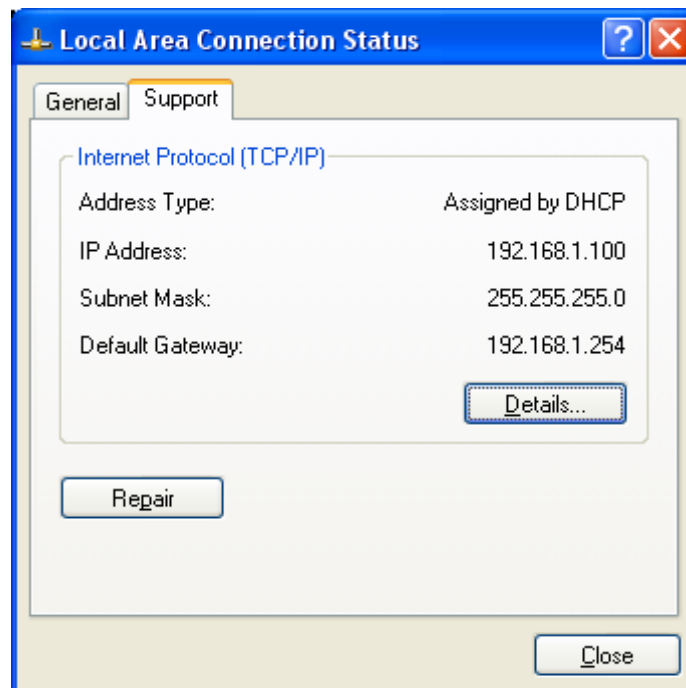


3. Click the **Support** tab.



If you are using Firetunnel 10's default settings, your PC should:

- Have an IP address between 192.168.1.1 and 192.168.1.253
- Have a subnet mask of 255.255.255.0



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

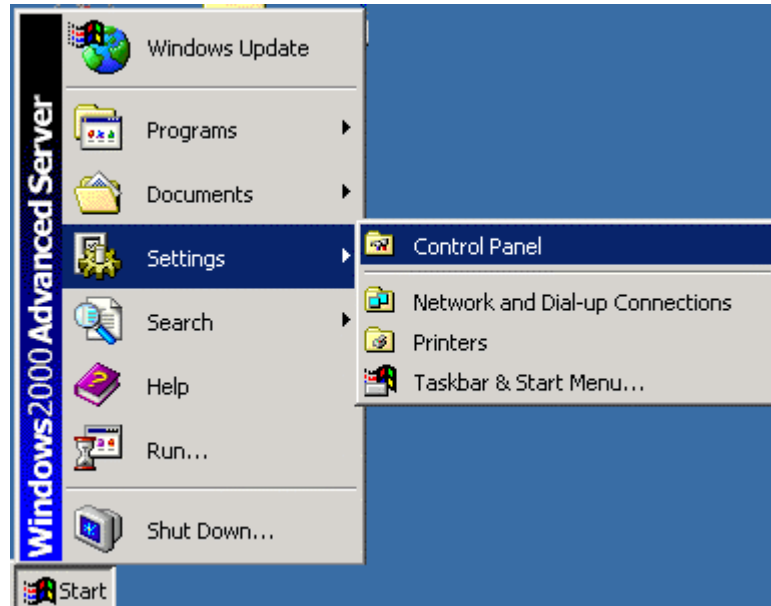
EU, Africa, Asia, South America, Australia: www.blackbox.eu



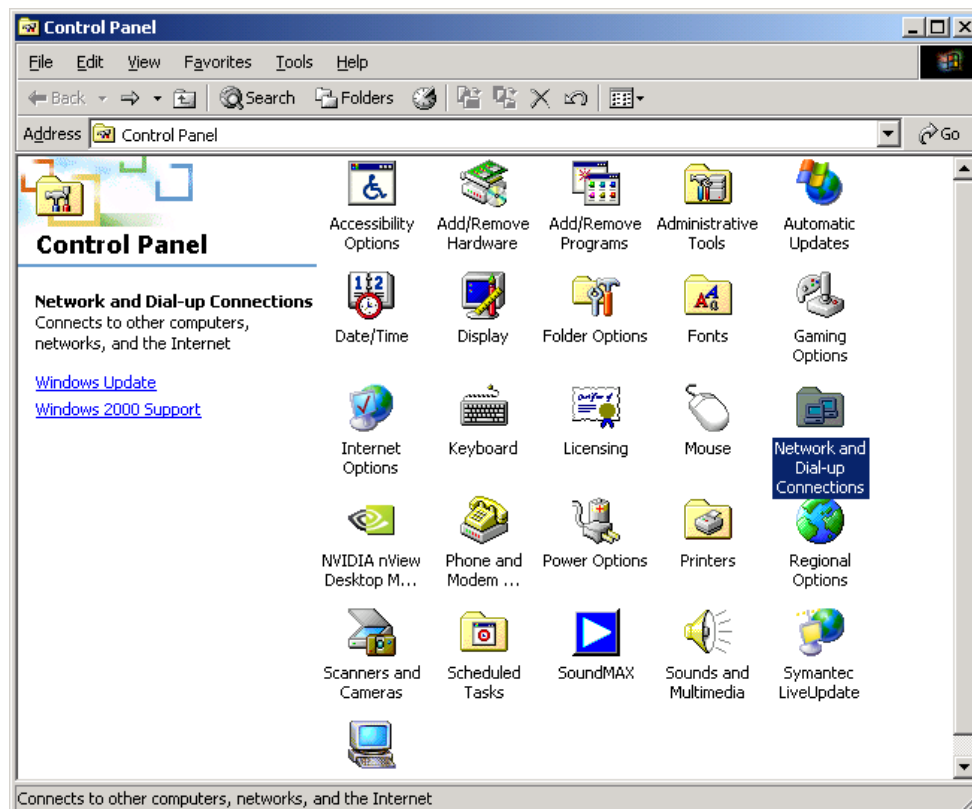
3.4.3 Windows 2000

3.4.3.1 Configuring

1. Select **Start > Settings > Control Panel**.



2. In the Control Panel window, double-click **Network and Dial-up Connections**.



Black Box Corporation

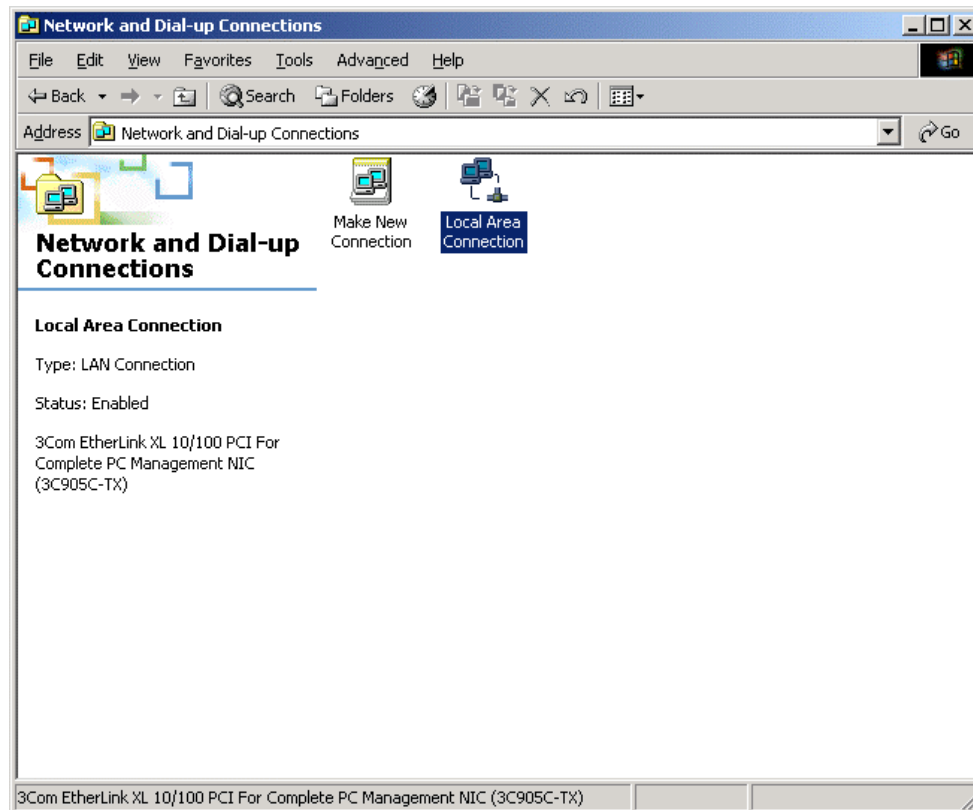
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

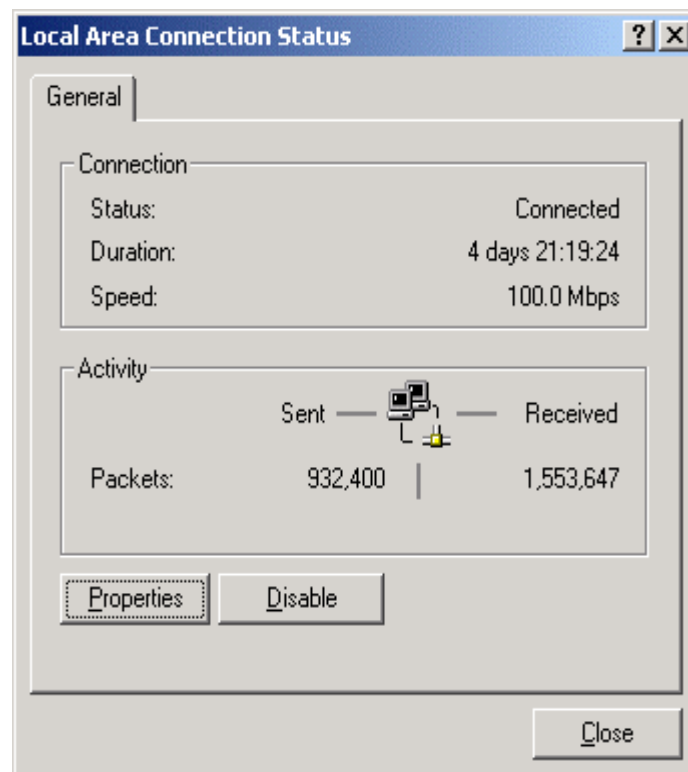
EU, Africa, Asia, South America, Australia: www.blackbox.eu



3. In Network and Dial-up Connections, double-click **Local Area Connection**.



4. In the Local Area Connection window, click **Properties**.



Black Box Corporation

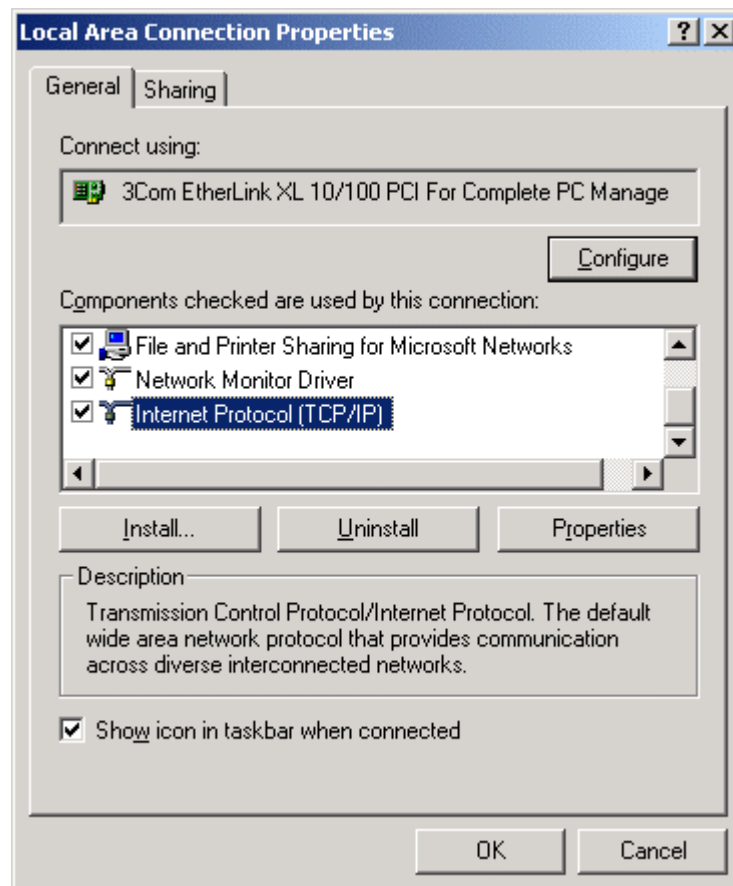
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

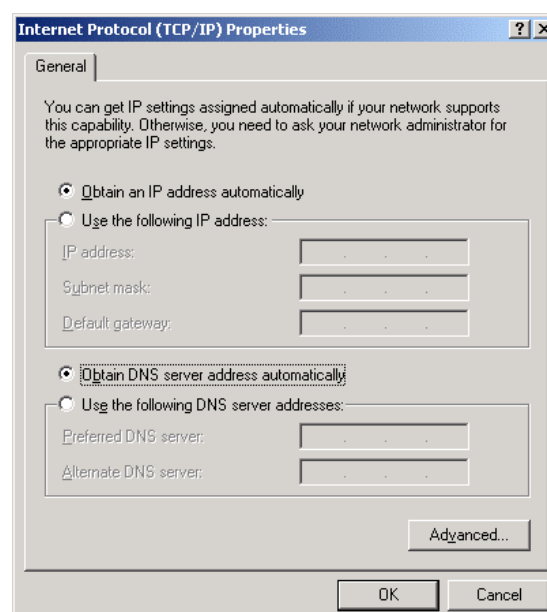
EU, Africa, Asia, South America, Australia: www.blackbox.eu



5. Select **Internet Protocol (TCP/IP)** and click **Properties**.



6a. To have your PC obtain an IP address automatically, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons.



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



6b. To manually assign your PC a fixed IP address, select the **Use the following IP address** radio button and enter your desired IP address, subnet mask, and default gateway in the blanks provided. Remember that your PC must reside in the same subnet mask as the router. To designate a DNS server, select the **Use the following DNS server** and fill in the preferred DNS address.

A screenshot of the "Internet Protocol (TCP/IP) Properties" dialog box. The "General" tab is selected. It contains two sections: one for IP address configuration and one for DNS server configuration. In the IP section, the "Use the following IP address:" radio button is selected, and the fields for IP address, subnet mask, and default gateway are filled with "192 . 168 . 1 . 100", "255 . 255 . 255 . 0", and "192 . 168 . 1 . 254" respectively. In the DNS section, the "Use the following DNS server addresses:" radio button is selected, and the "Preferred DNS server:" field is filled with "192 . 168 . 1 . 254". The "Alternate DNS server:" field is empty. At the bottom right of the dialog box, there are "OK" and "Cancel" buttons, and an "Advanced..." button is located above them.

7. Click **OK** to finish the configuration.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

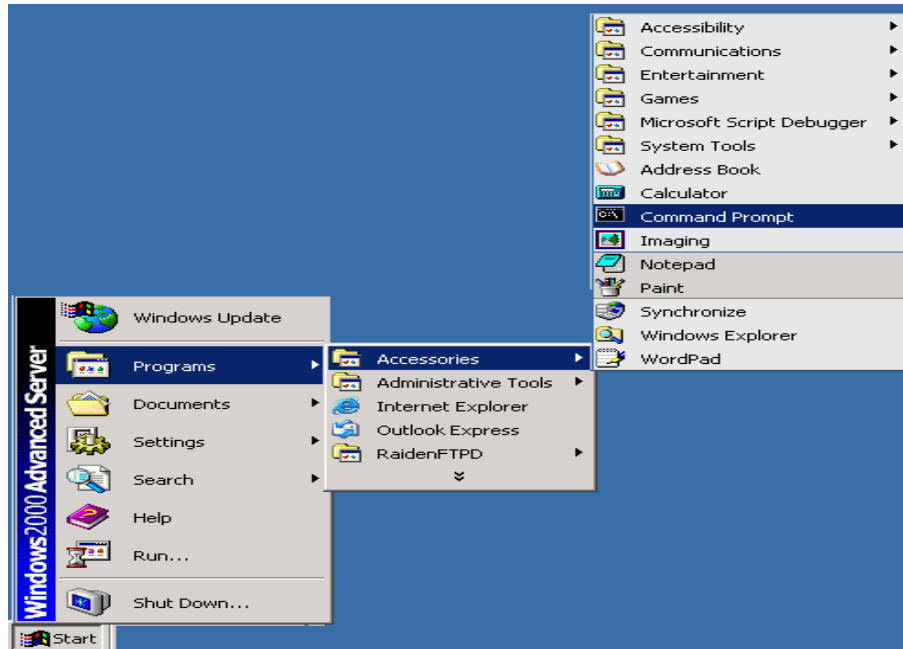
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

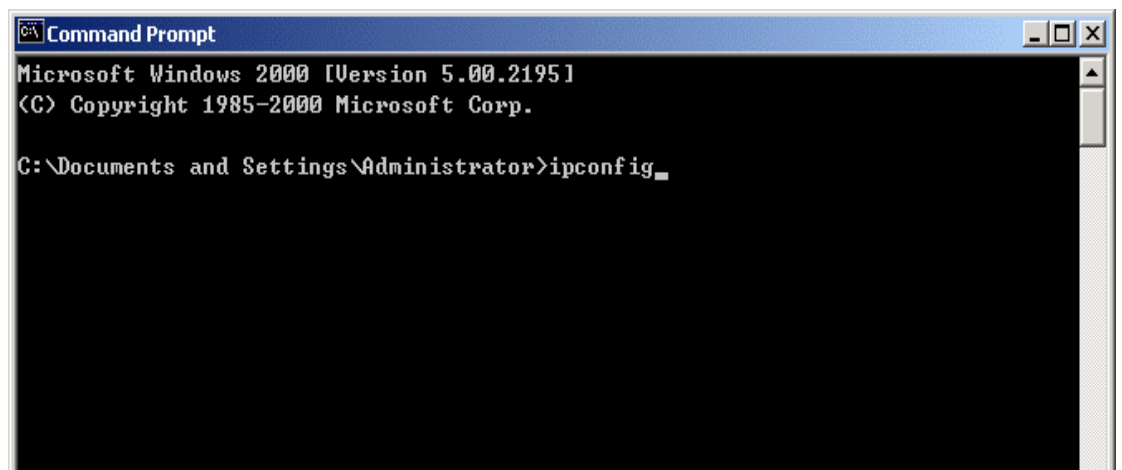


3.4.3.2 Verifying Settings

1. Click **Start > Programs > Accessories > Command Prompt**.



2. In the Command Prompt window, type `ipconfig` and then press **ENTER**.



If you are using Firtunnel 10's default settings, your PC should have:

- An IP address between 192.168.1.1 and 192.168.1.253
- A subnet mask of 255.255.255.0

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254

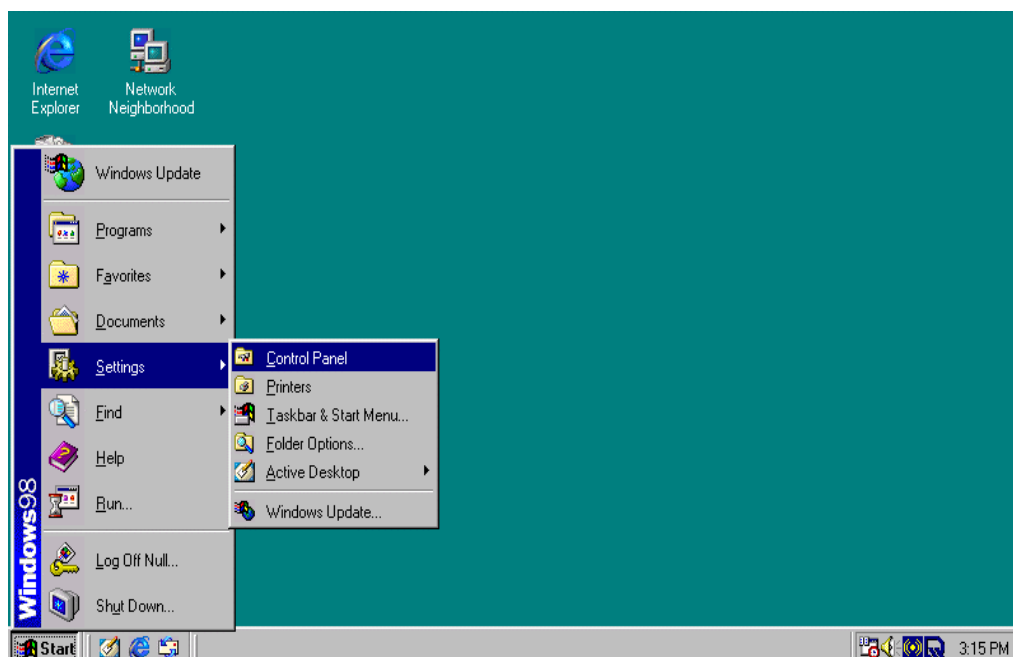
C:\Documents and Settings\Administrator>
```

3.4.4 Windows 98 / Me

3.4.4.1 Installing Components

To prepare Windows 98/Me PCs for TCP/IP networking, you may need to manually install TCP/IP on each PC. To do this, follow the steps below. Be sure to have your Windows CD handy, as you may need to insert it during the installation process.

1. On the Windows taskbar, select **Start > Settings > Control Panel**.



Black Box Corporation

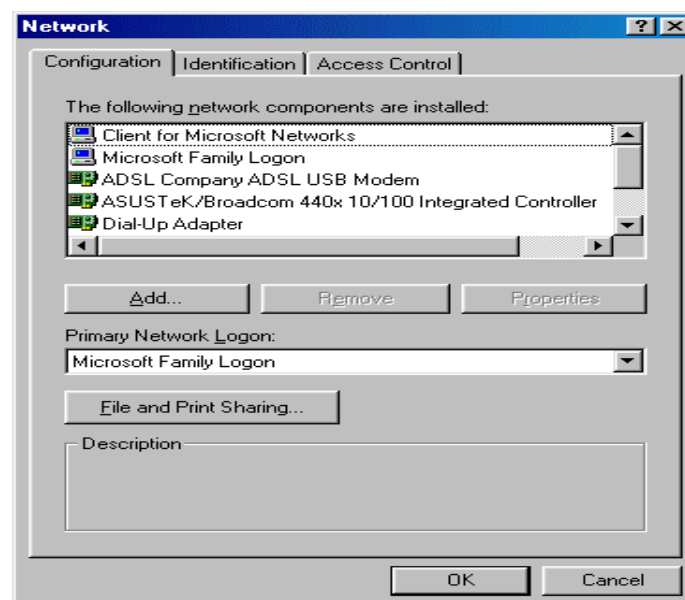
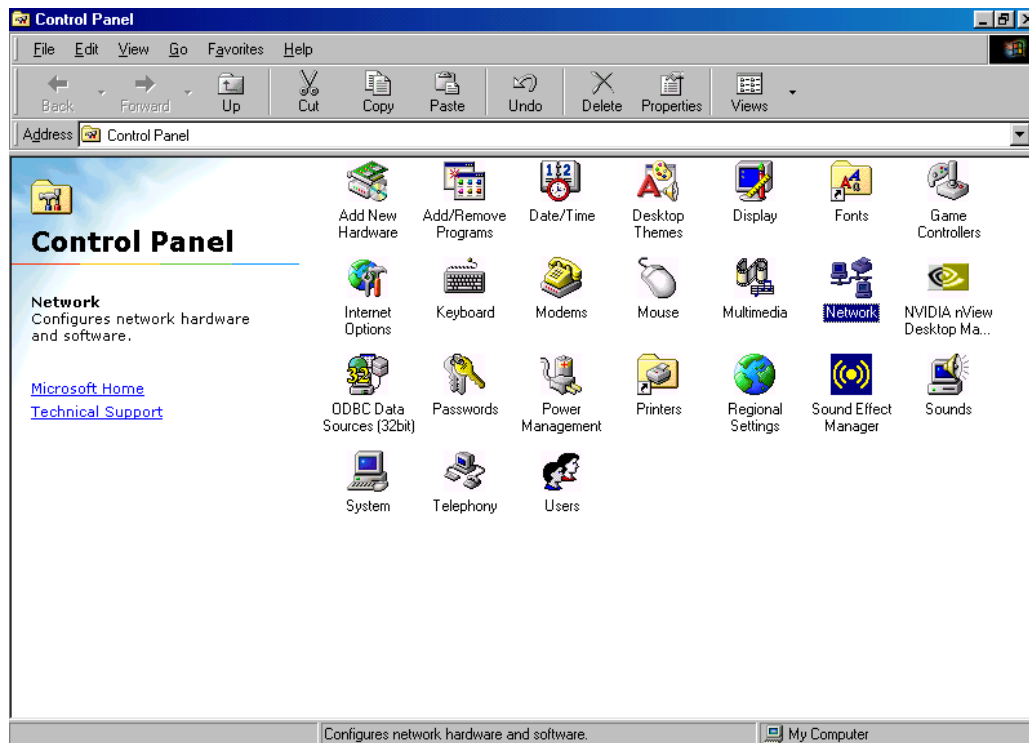
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2. Double-click the **Network** icon. The Network window displays a list of installed components.



You must have the following installed:

- An Ethernet adapter
- TCP/IP protocol
- Client for Microsoft Networks

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

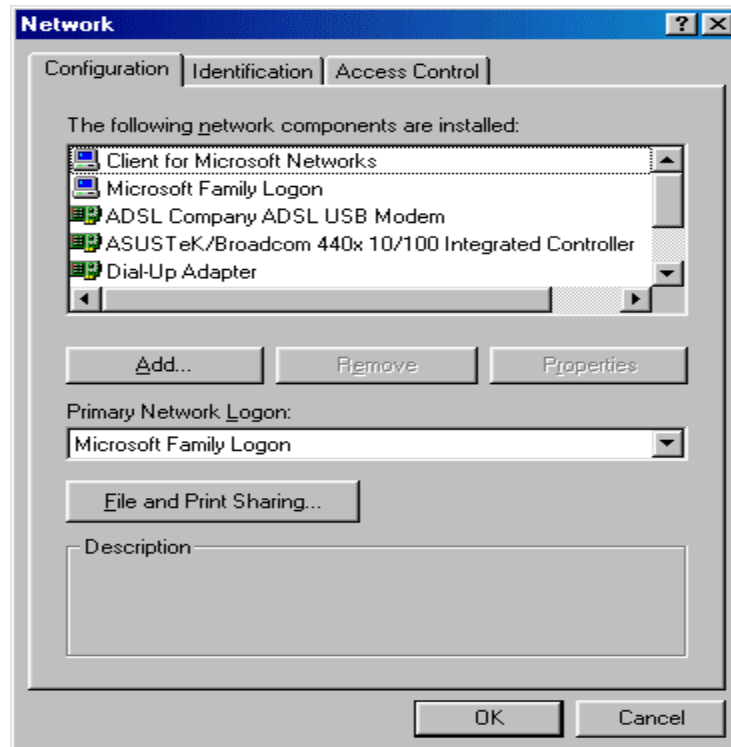
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

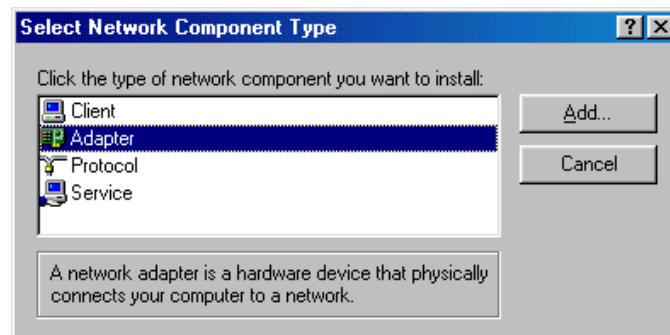


If you need to install a new Ethernet adapter, follow these steps:

- a. Click **Add**.



- b. Select **Adapter**, then **Add**.



Black Box Corporation

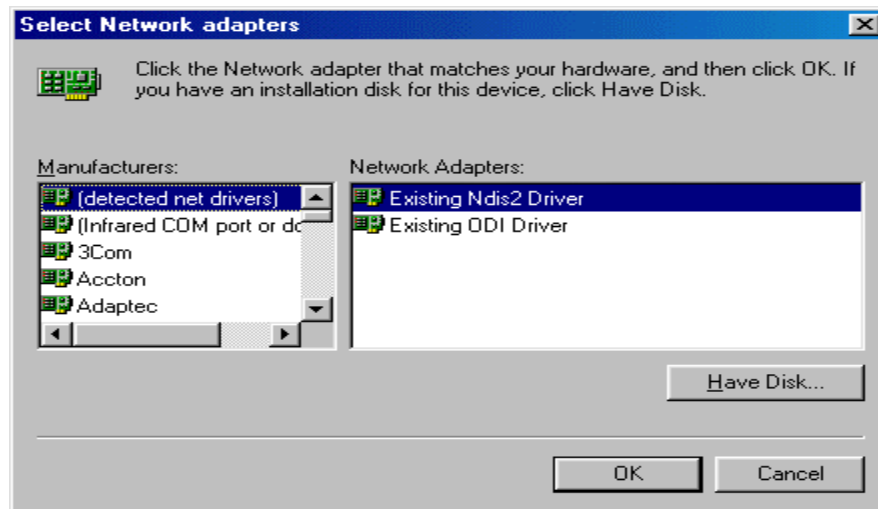
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

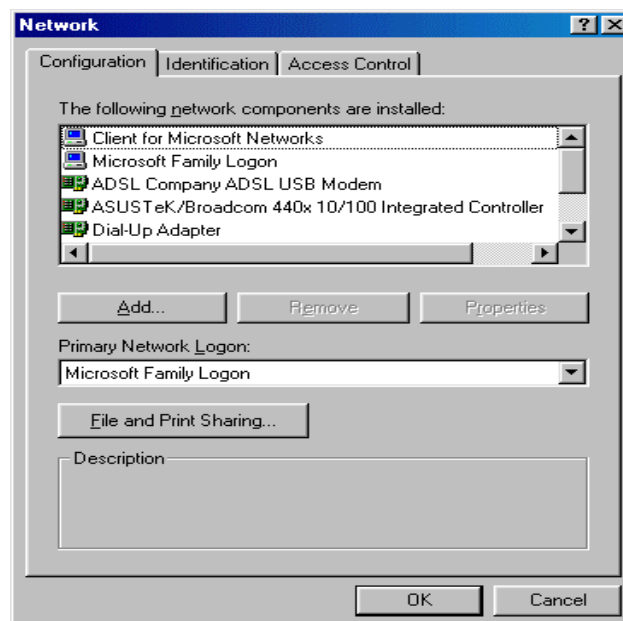


- c. Select the manufacturer and model of your Ethernet adapter, then click **OK**.

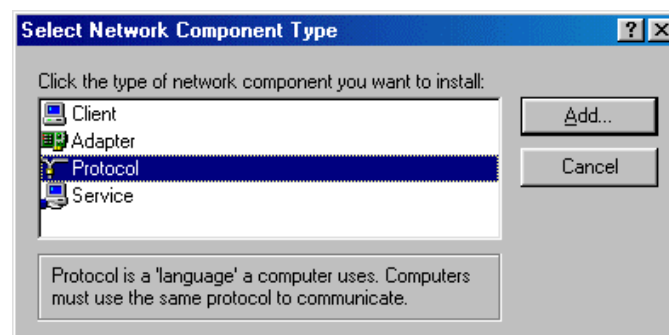


If you need TCP/IP:

- a. Click **Add**.



- b. Select **Protocol**, then click **Add**.



Black Box Corporation

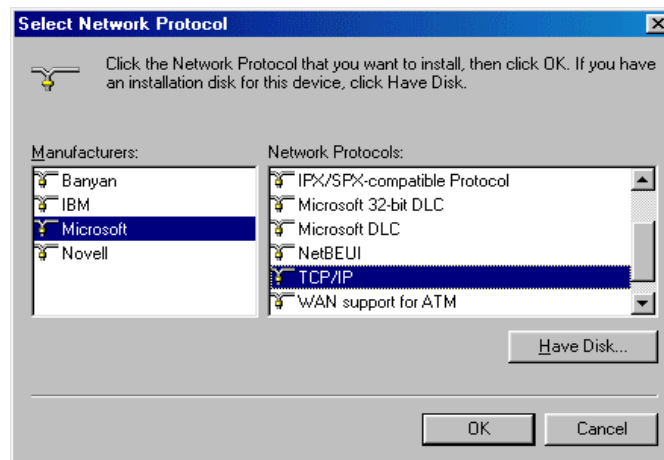
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

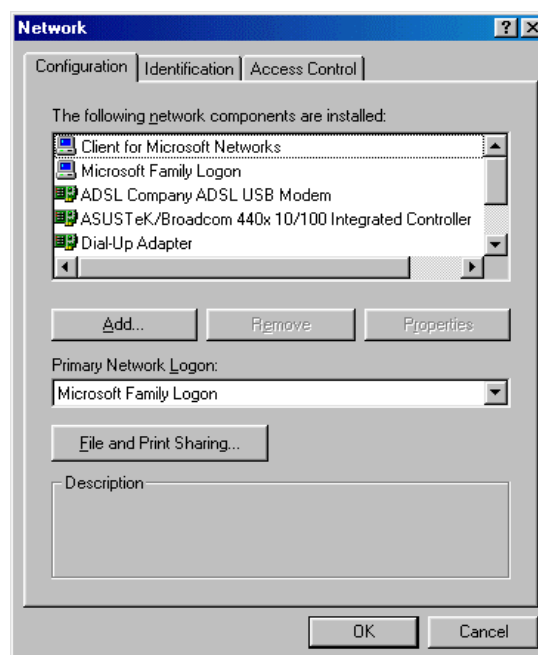


c. Select **Microsoft**. → **TCP/IP**, then **OK**.

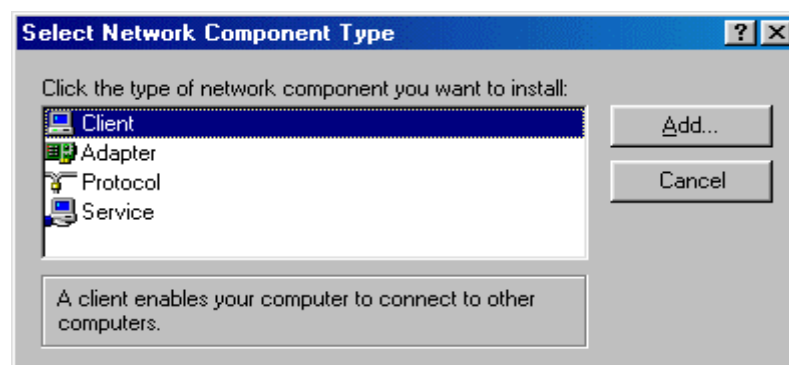


If you need Client for Microsoft Networks:

a. Click **Add**.



b. Select **Client**, then click **Add**.



Black Box Corporation

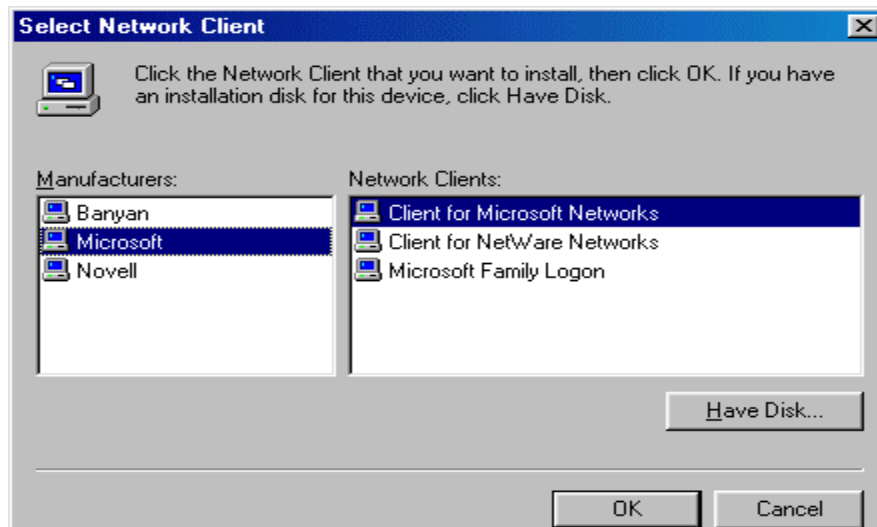
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



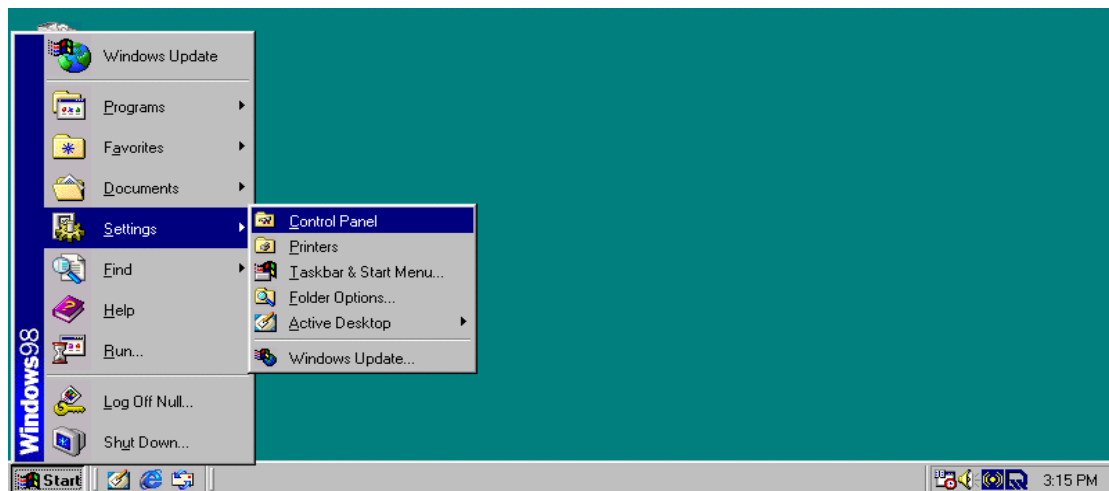
- c. Select **Microsoft**. → **Client for Microsoft Networks**, and then click **OK**.



3. Restart your PC to apply your changes.

3.4.4.2 Configuring

1. Select **Start > Settings > Control Panel**.



Black Box Corporation

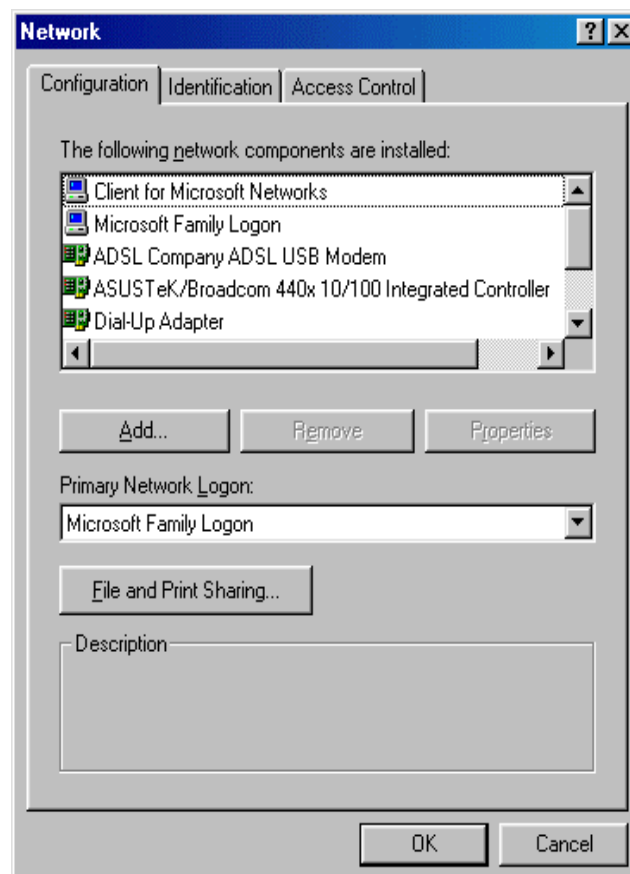
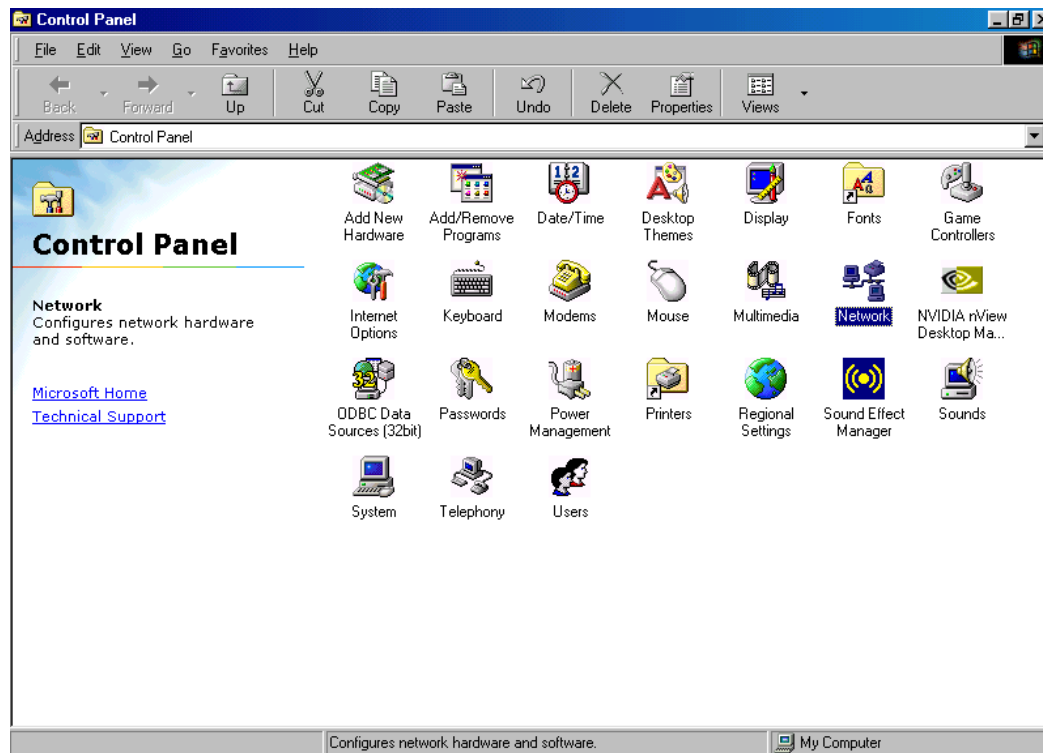
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2. In the Control Panel, double-click **Network** and choose the **Configuration** tab.



Black Box Corporation

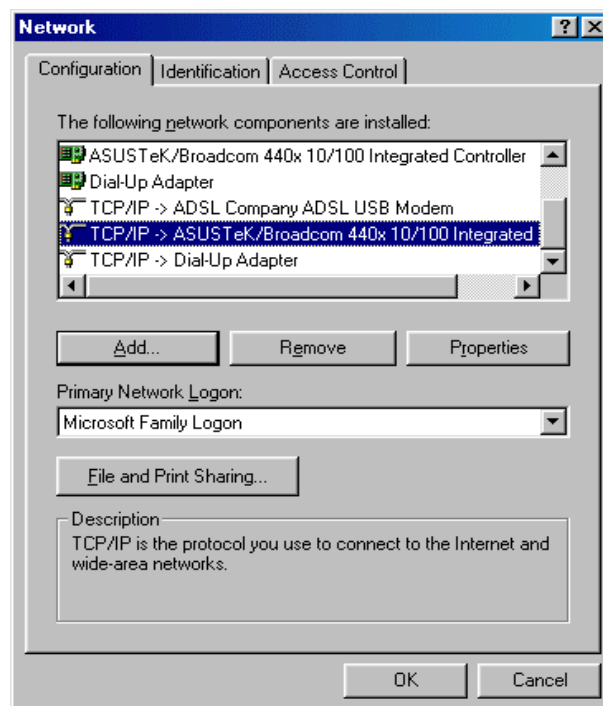
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

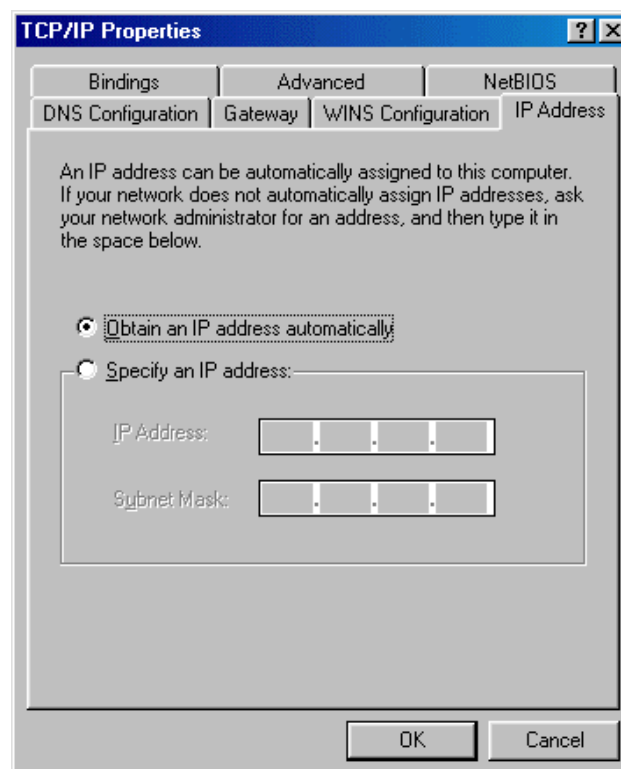
EU, Africa, Asia, South America, Australia: www.blackbox.eu



3. Select the name of your PC's **TCP/IP** Network Interface Card (NIC) and click **Properties**. TCP/IP > ASUSTeK is illustrated in the example below.



4. Select the **IP Address** tab and click the **Obtain an IP address automatically** radio button.



Black Box Corporation

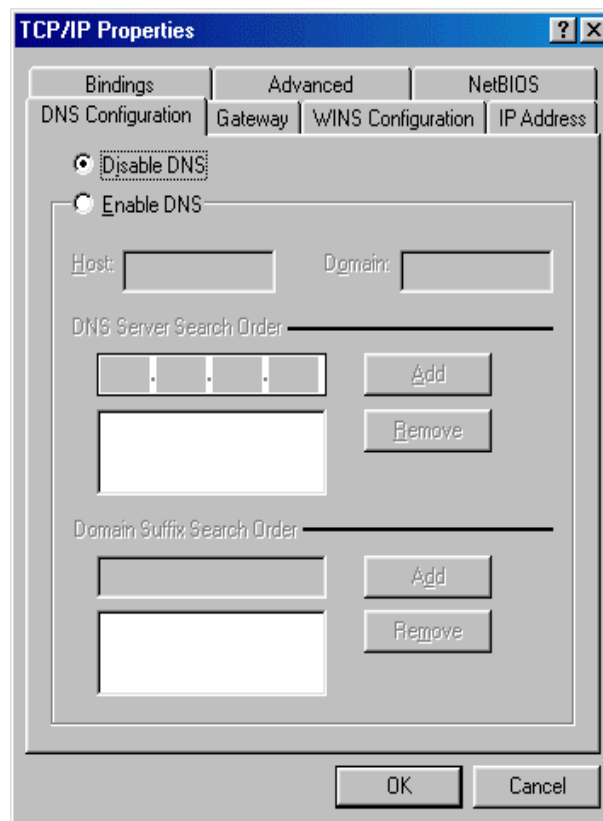
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

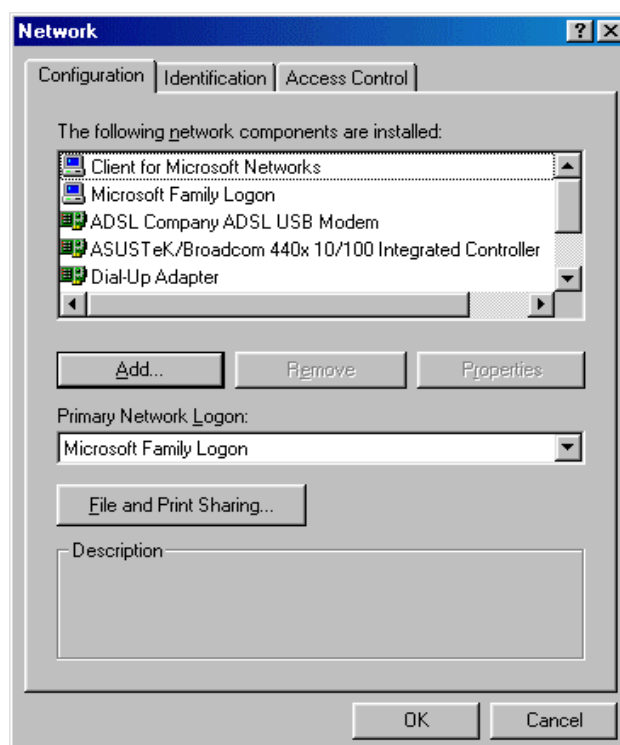
EU, Africa, Asia, South America, Australia: www.blackbox.eu



5. Select the **DNS Configuration** tab and select the **Disable DNS** radio button.



6. Click **OK** to apply the configuration.



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

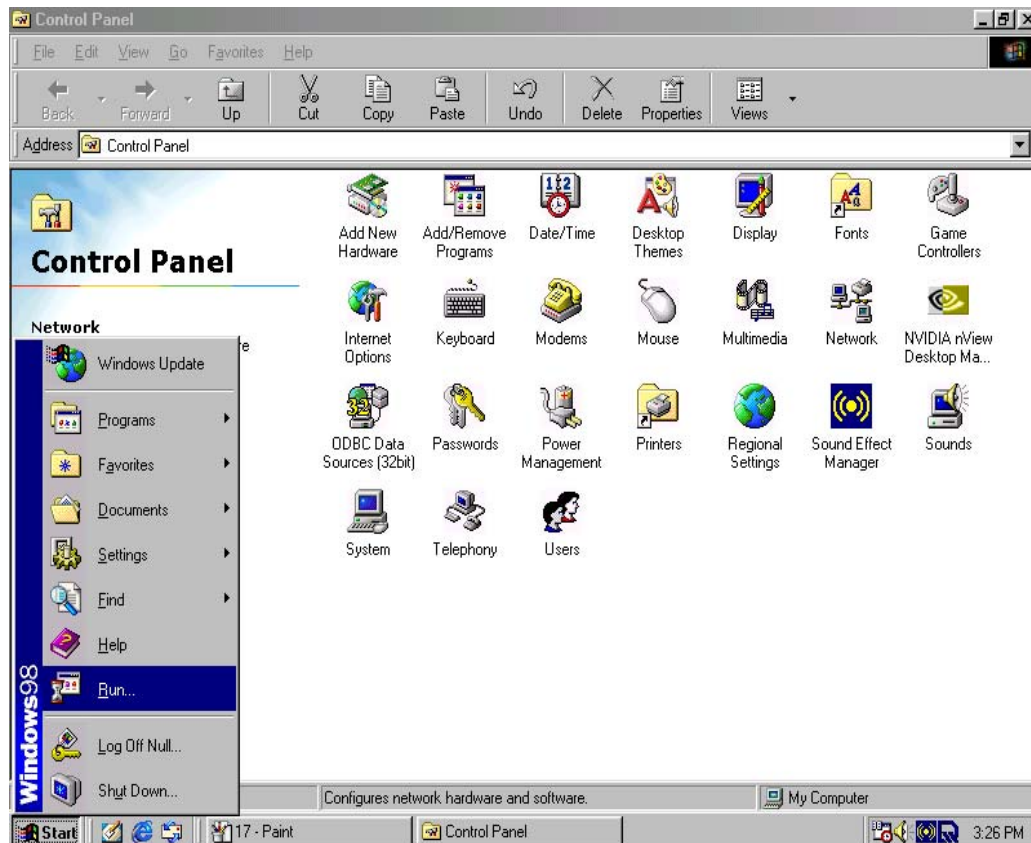
EU, Africa, Asia, South America, Australia: www.blackbox.eu



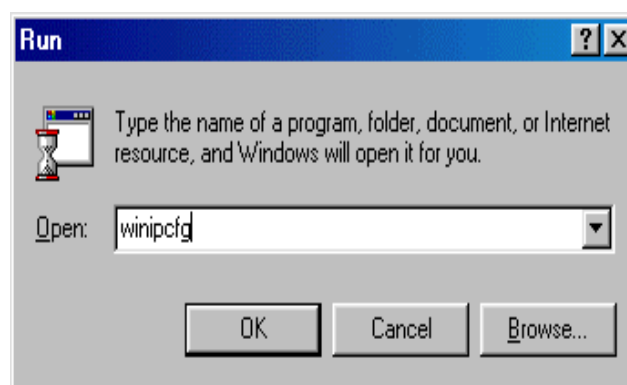
3.4.4.3 Verifying Settings

To check the TCP/IP configuration, use the winipcfg.exe utility:

1. Select **Start** > **Run**.



2. Type winipcfg, and then click **OK**.



Black Box Corporation

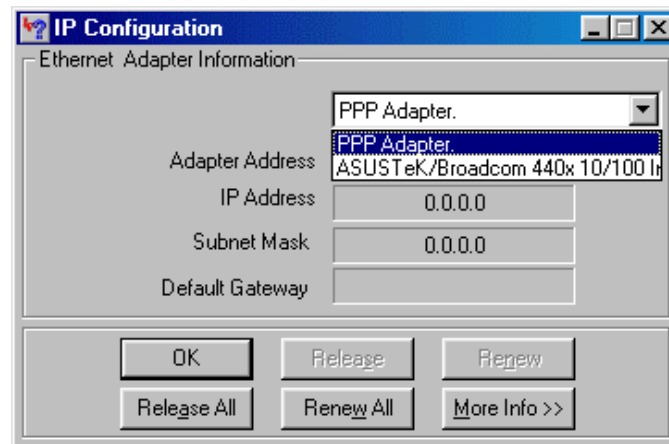
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

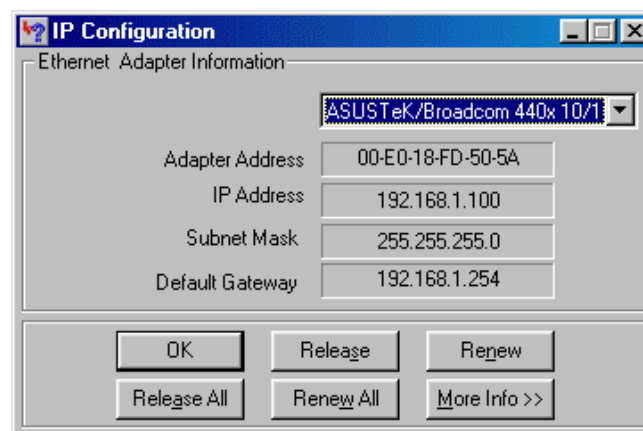


3. From the drop-down box, select your Ethernet adapter.



The window is updated to show your settings. Using the default Firetunnel 10 settings, your PC should have:

- An IP address between 192.168.1.1 and 192.168.1.253
- A subnet mask of 255.255.255.0
- A default gateway of 192.168.1.254



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



3.5 Factory Default Settings

Before configuring your Firetunnel 10, you need to know the following default settings:

Web Interface:

Username: admin

Password: admin

LAN Device IP Settings:

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

ISP setting in WAN site:

Obtain an IP Address automatically (DHCP Client)

DHCP server:

DHCP server is enabled.

Start IP Address: 192.168.1.100

End IP Address: 192.168.1.199

3.5.1 Username and Password

The default user name and password are "admin" and "admin" respectively.

If you ever forget your user name and/or password, you can restore your Firetunnel 10 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. Please note that doing this will also erase any previous router settings that you have made. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that Firetunnel 10 is ready.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



3.5.2 LAN and WAN Port Addresses

The default values for LAN and WAN ports are shown below:

LAN Port		WAN Port
IP address	192.168.1.254	The DHCP Client is <i>enabled</i> to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

3.6 Information From Your ISP

3.6.1 Protocols

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP, Static IP, PPPoE, or PPTP. The following table outlines each of these protocols:

DHCP	Configure this WAN interface to use DHCP client protocol to get an IP address from your ISP automatically. Your ISP provides an IP address to the router dynamically when logging in.
Static IP	Configure this WAN interface with a specific IP address. This IP address should be provided by your ISP.

PPPoE	PPPoE (PPP over Ethernet) is known as a dial-up DSL or cable service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure.
PPTP	If your ISP provides a PPTP connection, you can use the PPTP protocol to establish a connection to your ISP.
Big Pond	The Big [D5] Pond login for Telstra cable in Australia.

If your account uses PPP over Ethernet (PPPoE), you will need to enter your login name and password when configuring your Firetunnel 10. After the network and firewall are configured, Firetunnel 10 will login automatically, and you will no longer need to run the login program from your PC.

3.6.2 Configuration Information

If your ISP does not dynamically assign configuration information but instead uses fixed configurations, you will need the following basic information from your ISP:

- An IP address and subnet mask
- A gateway IP address
- One or more domain name server (DNS) IP addresses

Depending on your ISP, a host name and domain suffix may also be provided. If any of these items are dynamically supplied by the ISP, your Firetunnel 10 will automatically acquire them.

If an ISP technician configured your computer or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window before reconfiguring your computer for use with Firetunnel 10. The following sections describe how you can obtain this information.

This section uses illustrations from Windows XP. However, other versions of

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

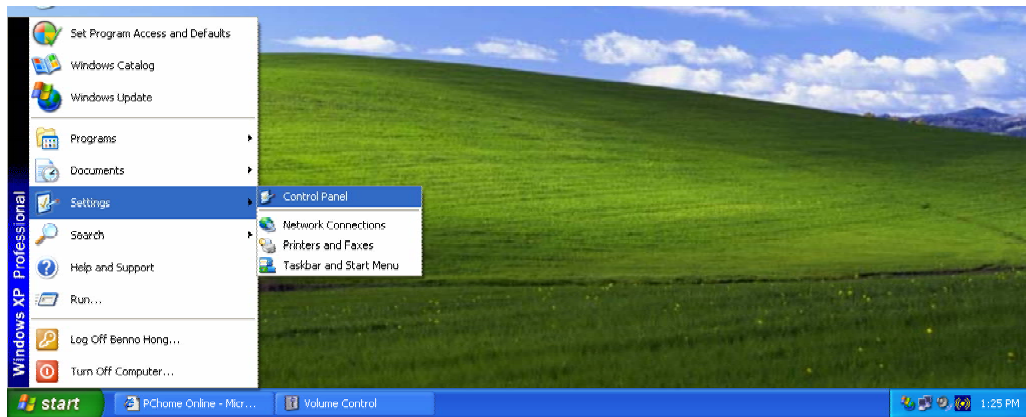
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu

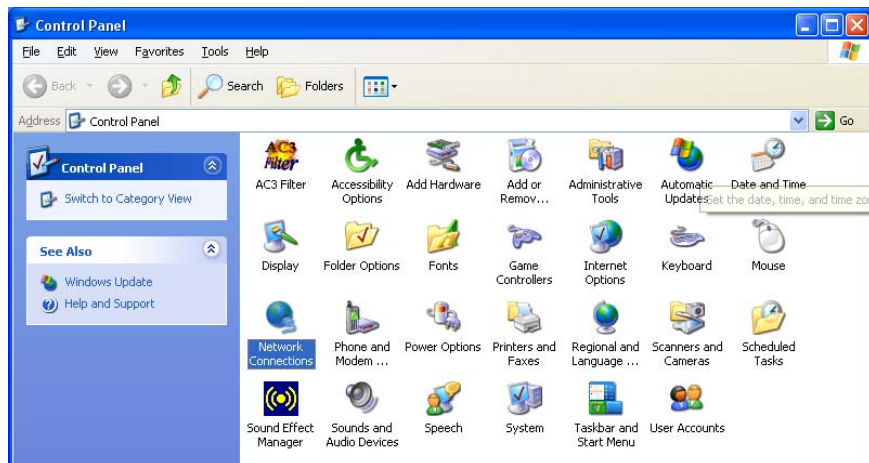


Windows will follow a similar procedure. Have your Windows CD handy, as it may be required during the configuration process.

1. Select **Start > Settings > Control Panel**.



2. Double-click the **Network** icon.



Black Box Corporation

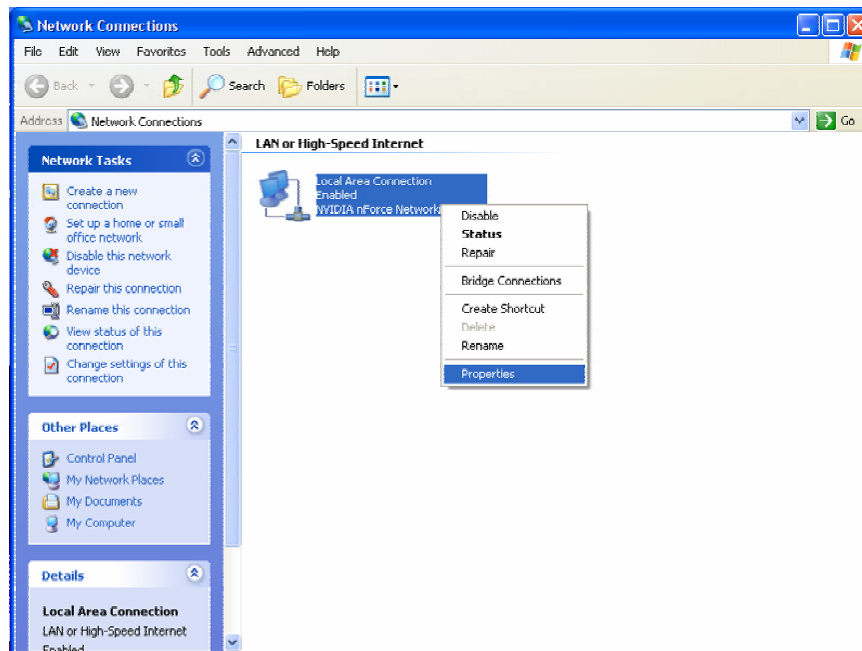
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

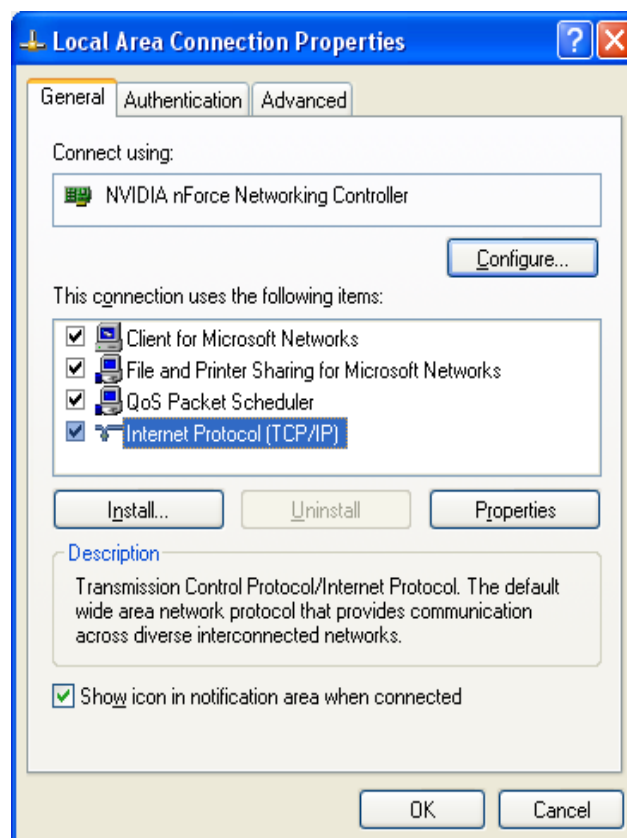
EU, Africa, Asia, South America, Australia: www.blackbox.eu



3. In the **Network Connections** window, right-click **Local Area Connection** and select **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Black Box Corporation

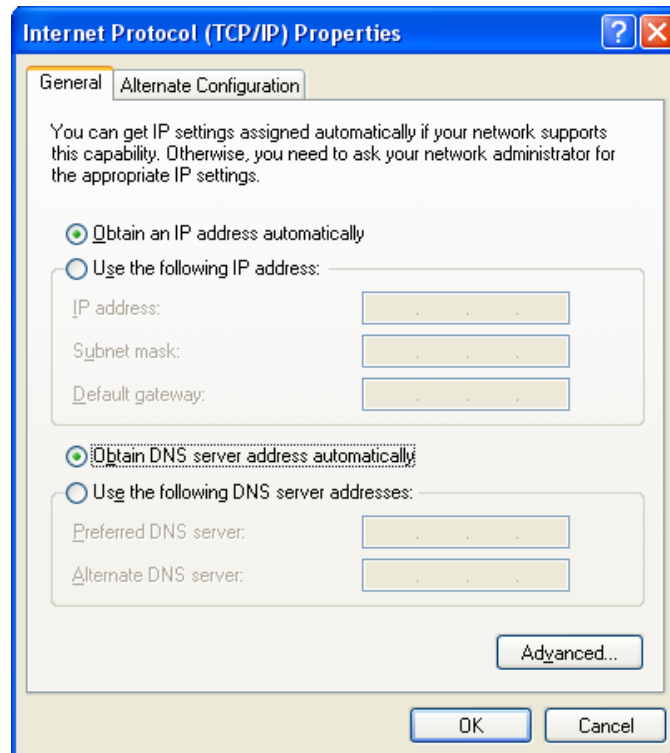
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

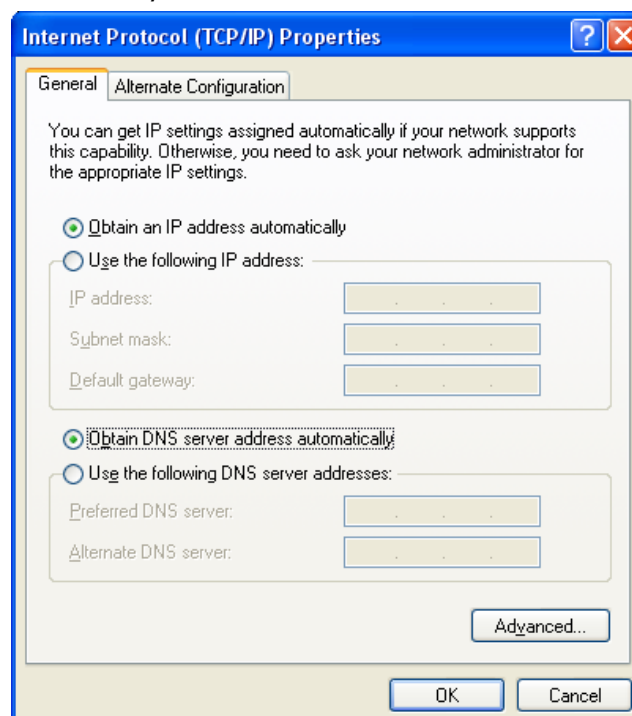
EU, Africa, Asia, South America, Australia: www.blackbox.eu



5. If an **IP address**, **subnet mask** and a **Default gateway** are shown, write down the information. If no address is present, your account's IP address is dynamically assigned. **Click the Obtain an IP address automatically** radio button.



6. If any DNS server addresses are shown, write them down. Click the Obtain DNS server address automatically radio button.



Black Box Corporation

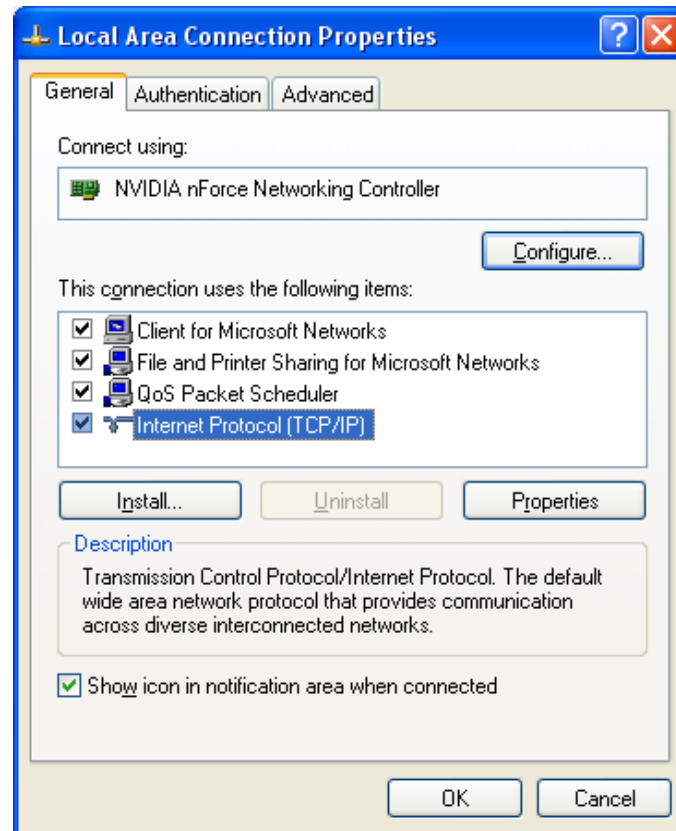
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



7. Click **OK** to save your changes.



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



3.7 Web Configuration Interface

Firetunnel 10 includes a Web Configuration Interface for easy administration via virtually any browser on your network. To access this interface, open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**. A user name and password window prompt will appear. Enter your user name and password (the default user name and password are "admin" and "admin") to access the Web Configuration Interface.

A screenshot of a web browser dialog box titled "Enter Network Password". It contains a key icon and the text "Please type your user name and password." Below this, there are fields for "Site:" (192.168.1.254), "Realm:" (WebAdmin), "User Name:" (admin), and "Password:" (masked with asterisks). There is a checkbox for "Save this password in your password list" which is unchecked. At the bottom are "OK" and "Cancel" buttons.

Site:	192.168.1.254
Realm:	WebAdmin
User Name:	admin
Password:	*****
<input type="checkbox"/> Save this password in your password list	

A screenshot of the Black Box FireTunnel 10 web configuration interface. The top header shows the Black Box logo and "FireTunnel 10 Black Box FireTunnel Series". On the left is a navigation menu with links: Status, Quick Start, Configuration, Log & E-mail Alert, and Save Config to Flash. The main content area is titled "Status" and includes a "Refresh" button. It displays device information in a table format, including device name, system up time, current time, MAC addresses, firmware version, and home URL. Below this are sections for LAN and WAN configuration. At the bottom are buttons for "SAVE CONFIG", "RESTART", and "LOGOUT".

Device Information	
Device Name	Firetunnel 10
System Up Time	2:22:53:45 (day:hour:min:sec)
Current Time	Thu Aug 4 10:53:26 2005 Sync Now
Private LAN MAC Address	00:04:ed:11:c7:09
Public WAN MAC Address	00:04:ed:11:c7:0a
Firmware Version	2.02f
Home URL	BlockBox

LAN	
IP Address	192.168.1.254
Netmask	255.255.255.0
DHCP server	Enabled

WAN	
Connection Method	No Link
IP Address	
Netmask	
Gateway	
DNS Server	
Up Time	

[D6]

If the Web Configuration Interface appears, congratulations! You are now ready to configure your Firetunnel 10. If you are having trouble accessing the interface, please refer to **Chapter 5: Troubleshooting** for possible resolutions.

Chapter 4: Router Configuration

4.1 Overview

The Web Configuration Interface makes it easy for you to manage your network via any PC connected to it. On the Web Configuration homepage, you will see the navigation pane located on the left hand side. From it, you will be able to select various options used to configure your router.



1. Click **Apply** if you would like to apply the settings on the current screen to the device. The settings will be effective immediately, however the configuration is not saved yet and the settings will be erased if you power off or restart the device.
2. Click **SAVE CONFIG** to save the current settings permanently to the device.
3. Click **RESTART** to restart the device. There are two options to restart the device.
 - Select **Current Settings** if you would like to restart using the current configuration.
 - Select **Factory Default Settings** if you would like to restart using the factory default configuration.
4. To exit the router's web interface, click **LOGOUT**. Please ensure that you have saved your configuration settings before you logout. Be aware that the router is restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



access the page after a user-defined period (5 minutes by default).

The following sections will show you how to configure your router using the Web Configuration Interface.

4.2 Status

The Status menu displays the various options that have been selected and a number of statistics about your Firetunnel 10. In this menu, you will find the following sections:

- ARP Table
- Routing Table
- Session Table
- DHCP Table
- IPSec Status
- PPTP Status
- System Status
- System Log

A screenshot of the Black Box FireTunnel 10 web interface. The page has a black header with the Black Box logo and "FireTunnel 10 Black Box FireTunnel Series". On the left is a sidebar with navigation links: Status, Quick Start, Configuration, Log & E-mail Alert, and Save Config to Flash. The main content area is titled "Status" and contains a "Refresh" button. It displays device information in a table, including Device Name (Firetunnel 10), System Up Time (2:22:53:45), Current Time (Thu Aug 4 10:53:26 2005), Private LAN MAC Address (00:04:ed:11:c7:09), Public WAN MAC Address (00:04:ed:11:c7:0a), Firmware Version (2.02f), and Home URL (BlockBox). Below this is a section for LAN settings, showing IP Address (192.168.1.254), Netmask (255.255.255.0), and DHCP server (Enabled). The WAN section shows Connection Method (No Link) and other fields for IP Address, Netmask, Gateway, DNS Server, and Up Time. At the bottom of the page are buttons for SAVE CONFIG, RESTART, and LOGOUT.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.1 ARP Table

The Address Resolution Protocol (ARP) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine the MAC address of your PC's network interface to use with the router's Firewall – MAC Address Filter function. See the **Firewall** section of this chapter for more information on this feature.

Status	ARP Table				
ARP Table	IP ↔ MAC List				
Routing Table	No.	IP Address	MAC Address	Interface	Static
Session Table	1	192.168.1.150	00:0B:5D:08:BF:C1	LAN	no
DHCP Table					
IPSec Status					
PPTP Status					
System Status					
System Log					
Quick Start					
Configuration					
Log & E-mail Alert					
Save Config to Flash					

No.: Number of the list.

IP Address: A list of IP addresses of devices on your LAN.

MAC Address: The Media Access Control (MAC) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP address connects to.

Static: Static status of the ARP table entry.

NO indicates dynamically-generated ARP table entries.

YES indicates static ARP table entries added by the user.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.2 Routing Table

The Routing Table displays the current path for transmitted packets. Both static and dynamic routes are displayed.

Status	Routing Table				
ARP Table	Routing Table				
Routing Table	No.	Destination	Netmask	Gateway/Interface	Cost
Session Table	1	192.168.1.0	255.255.255.0	0.0.0.0/ LAN	0
DHCP Table					
IPSec Status					
PPTP Status					
System Status					
System Log					
Quick Start					
Configuration					
Log & E-mail Alert					
Save Config to Flash					

No.: Number of the list.

Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway/Interface: The IP address of the gateway or existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.3 Session Table

The NAT Session Table displays a list of current sessions for both incoming and outgoing traffic with protocol type, source IP, source port, destination IP and destination port, each page shows 10 sessions.

Status	Session Table					
ARP Table	Session Table					
Routing Table	No.	Protocol	From IP	From Port	To IP	To Port
Session Table	1	TCP	192.168.1.150	2021	192.168.1.254	80
DHCP Table	2	TCP	192.168.1.150	2023	192.168.1.254	80
IPSec Status	3	TCP	192.168.1.150	2025	192.168.1.254	80
PPTP Status	4	TCP	192.168.1.150	2019	192.168.1.254	80
System Status	Session 1 - 4 of 4, 1/1.					
System Log	Filter	From IP	From Port	To IP	To Port	
Quick Start	First	Previous	Next	Last	Jump to session	GO
Configuration						
Log & E-mail Alert						
Save Config to Flash						

No.: Number of the list.

Protocol: Protocol type of the Session.

From IP: Source IP of the session.

From Port: source port of the session.

To IP: Destination IP of the session.

To Port: Destination port of the session.

Sessions:

Filter: when the presented field is filled, please click Filter button.

From IP: please input the source IP you would like to filter.

From port: please input the source port you would like to filter.

To IP: please input the destination IP you would like to filter.

To port: please input the destination port you would like to filter.

First: To the first page.

Previous: To the previous page.

Next: To the next page.

Last: To the last page.

Jump to the session: please input the session number you would like to see and press "GO"

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.4 DHCP Table

The DHCP Table displays a list of IP addresses that have been assigned to PCs on your network via Dynamic Host Configuration Protocol (DHCP).

Status	DHCP Table				
ARP Table	DHCP IP Assignment Table				
Routing Table	No.	IP Address	Device Name	MAC Address	Lease Time
Session Table	<input type="button" value="Refresh"/>				
DHCP Table					
IPSec Status					
PPTP Status					
System Status					
System Log					
Quick Start					
Configuration					
Log & E-mail Alert					
Save Config to Flash					

No.: Number of the list.

IP Address: A list of IP addresses of devices on your LAN.

Device Name: The host name (computer name) of the client.

MAC Address: The MAC address of client.

Lease Time: The time of these listed IP address has been assigned.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.5 IPSec Status

The IPSec Status window displays the status of the IPSec Tunnels that are currently configured on your Firetunnel 10.

Status	IPSec Status						
ARP Table	IPSec Tunnels						
Routing Table	Name	Enable	Status	Local Network	Remote Network	Remote Gateway	SA
Session Table							
DHCP Table							
IPSec Status							
PPTP Status							
System Status							
System Log							
Quick Start							
Configuration							
Log & E-mail Alert							
Save Config to Flash							

Name: The name you assigned to the particular IPSec entry.

Enable: Whether the IPSec connection is currently Enable or Disable.

Status: Whether the IPSec is Active, Inactive or Disable.

Local Network: The local IP address or subnet used.

Remote Network: The subnet of the remote site.

Remote Gateway: The remote gateway IP address.

SA: The Security Association for this IPSec entry.

Action: Manually connect or drop the tunnel.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.6 PPTP Status

The PPTP Status window displays the status of the PPTP Tunnels that are currently configured on your Firetunnel 10.

Status

ARP Table

Routing Table

Session Table

DHCP Table

IPSec Status

PPTP Status

System Status

System Log

Quick Start

Configuration

Log & E-mail Alert

Save Config to Flash

PPTP Server Status

PPTP Accounts

Name	Enable	Status	Type	Peer Network	Connect By	Action
------	--------	--------	------	--------------	------------	--------

PPTP Client Status

PPTP Accounts

Enable	Client IP	Client IP	Status	Peer Network	Action
×			Not Connected		

Name: The name you assigned to the particular PPTP entry.

Enable: Whether the PPTP connection is currently Enable or Disable.

Status: Whether the PPTP is Active, Inactive or Disable.

Type: Whether the Connection type is Remote Access or LAN to LAN

Peer Network: The Remote subnet for LAN to LAN as connection type.

Connect by: The remote address when connected.

Action: Manually drop the tunnel.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.2.7 System Status

The System Status window displays both device processor's name, usage and system memory's usage.

Status	System Statistics
ARP Table	Statistics
Routing Table	Processor Intel XScale-IXP425 rev 1 (v5b)
Session Table	Mem Total 30516 kB
DHCP Table	Mem Free 9528 kB
IPSec Status	Ramdisk Free 131 kB
PPTP Status	CPU Status 16.03%
System Status	
System Log	
Quick Start	
Configuration	
Log & E-mail Alert	
Save Config to Flash	

4.2.8 System Log

This window displays Firetunnel 10's System Log entries. Major events are logged on this window.

Status	System Log
ARP Table	Logs
Routing Table	If you would like to save the log to a text file, right click here and select "Save Target As ..."
Session Table	Display: All Logs Refresh Clear Log Send Log
DHCP Table	No. Time Message Source Destination
IPSec Status	1 Aug 1 12:34:21 SysMan HTTP Server - Successful login 192.168.1.150
PPTP Status	2 Aug 4 10:53:26 SysMan HTTP Server - Successful login 192.168.1.150
System Status	3 Aug 4 11:20:09 SysMan HTTP Server - Successful login 192.168.1.150
System Log	<< First < Previous 1 / 1 Next > Last >>
Quick Start	
Configuration	
Log & E-mail Alert	
Save Config to Flash	

Display: There are several options in display, **All logs** allows the system to show all types of system logs, and there are also specific event logs such as; **System Maintenance, System Errors, Access Control, Packet Filter, LAN MAC Filter, URL Filter, Intrusion Detection, Call Data Record, PPP, Remote Access, and IPSEC.**

Refresh: Refresh the System Log.

Clear Log: Clear the System Log.

Send Log: Send the System Log to your email account. You can set the email address in **Configuration > System > Email Alert**. See the **Email Alert** section for more details.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Save Log: Save the System log to a text file.

There are several links at the bottom right of the table indicating '<<First', '<Previous', a **dropdown menu** for the number of pages, 'Next>' and 'Last>>'. **First** directs the page number for the table to the 1st page, **previous** directs the page number for the table to the one page before, the **dropdown menu** allows the user to specifically select the page number to view, **next** directs the page number for the table to the one page after current page, and **last** directs the page number for the table to the last page of the table.

Please refer to **Appendix E: IPSec Log Events** for more information on log events.

4.3 Quick Start

The Quick Start menu allows you to quickly configure your network for Internet access using the most basic settings.

Status Quick Start Configuration Log & E-mail Alert Save Config to Flash	Quick Start WAN	
	DHCP	
	Connection Method	Obtain an IP Address Automatically ▾
	Host Name	Obtain an IP Address Automatically
	Static IP Setting PPPoE Setting PPTP Setting Big Pond Setting	
	Apply Reset	

Connection Method: Select your router's connection to the Internet. Selections include **Obtain an IP Address Automatically**, **Static IP Settings**, **PPPoE Settings**, **PPTP Settings**, and **Big Pond Settings**.

4.3.1 DHCP

The following is information regarding your ISP that you will need to enter in order to properly configure your Internet connection. If you select to **Obtain an IP Address Automatically**, these will be automatically set for you, provided that your ISP dynamically assigns an IP address.

Status Quick Start Configuration Log & E-mail Alert Save Config to Flash	Quick Start WAN	
	DHCP	
	Connection Method	Obtain an IP Address Automatically ▾
	Host Name	BBOX
	Apply Reset	

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.3.2 Static IP

<div>Status</div> <div>Quick Start</div> <div>Configuration</div> <div>Log & E-mail Alert</div> <div>Save Config to Flash</div>	Quick Start WAN				
	Static IP				
	Connection Method	Static IP Setting			
	IP Assigned by Your ISP	0	0	0	0
	IP Subnet Mask	0	0	0	0
	ISP Gateway Address	0	0	0	0
	Primary DNS	0	0	0	0
	Secondary DNS	0	0	0	0
	<div>Apply</div> <div>Reset</div>				

IP assigned by your ISP: Enter the assigned IP address from your IP.

IP Subnet Mask: Enter your IP subnet mask.

ISP Gateway Address: Enter your ISP gateway address.

Primary DNS: Enter your primary DNS.

Secondary DNS: Enter your secondary DNS.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.3.3 PPPoE

<div>Status</div> <div>Quick Start</div> <div>Configuration</div> <div>Log & E-mail Alert</div> <div>Save Config to Flash</div>	Quick Start WAN	
	PPPoE	
	Connection Method	PPPoE Setting ▾
	Username	<input type="text"/>
	Password	<input type="password"/>
	Retype Password	<input type="password"/>
	Connection	Always Connect ▾
	Idle Time	10 minutes ▾
	<div>Apply</div> <div>Reset</div>	

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.3.4 PPTP

Quick Start WAN	
PPTP	
Connection Method	PPTP Setting <input type="button" value="v"/>
Username	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
PPTP client IP	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
PPTP client IP Netmask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
PPTP client IP Gateway	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
PPTP server IP	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Connection	Always Connect <input type="button" value="v"/>
Idle Time	10 Minutes <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

PPTP Client IP: Enter the PPTP Client IP provided by your ISP.

PPTP Client IP Netmask: Enter the PPTP Client IP Netmask provided by your ISP.

PPTP Client IP Gateway: Enter the PPTP Client IP Gateway provided by your ISP.

PPTP Server IP: Enter the PPTP Server IP provided by your ISP.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPTP session when starting up and to automatically re-establish the PPTP session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPTP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.3.5 Big Pond

Status Quick Start Configuration Log & E-mail Alert Save Config to Flash	Quick Start WAN			
	Big Pond			
	Connection Method	Big Pond Setting <input type="button" value="v"/>		
	Username	<input type="text"/>		
	Password	<input type="password"/>		
	Retype Password	<input type="password"/>		
	Login Server	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Login Server: Enter the IP of the Login server provided by your ISP.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

For detailed instructions on configuring WAN settings, please refer to the **WAN** section of this chapter.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4 Configuration

The **Configuration** menu allows you to set many of the operating parameters of the Firetunnel 10. In this menu, you will find the following sections:

- LAN
- WAN
- Bandwidth Settings
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced

These items are described below in the following sections.

Configuration
LAN
WAN
System
Firewall
VPN
QoS
Virtual Server
Advanced

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

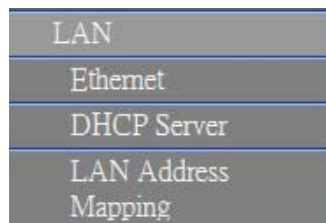
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.1 LAN

There are three items within this section: **Ethernet**, **DHCP Server** and **LAN Address Mapping**.



4.4.1.1 Ethernet

<div>Status</div> <div>Quick Start</div> <div>Configuration</div> <div>LAN</div> <div>Ethernet</div> <div>DHCP Server</div> <div>LAN Address Mapping</div> <div>WAN</div> <div>System</div> <div>Firewall</div> <div>VPN</div> <div>QoS</div> <div>Virtual Server</div> <div>Advanced</div> <div>Log & E-mail Alert</div> <div>Save Config to Flash</div>	Ethernet				
	Parameters				
	IP Address	192	168	1	254
	Subnet Mask	255	255	255	0
	RIP	Disable <input type="button" value="v"/> <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M			
	<div>Apply</div> <div>Reset</div>				

IP Address: Enter the internal LAN IP address for Firetunnel 10 (192.168.1.254 by default).

Subnet Mask: Enter the subnet mask (255.255.255.0 by default).

RIP: RIP v2 Broadcast and RIP v2 Multicast. Check to enable RIP.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.1.2 DHCP Server

In this menu, you can disable or enable the Dynamic Host Configuration Protocol (DHCP) server. The DHCP protocol allows your Firetunnel 10 to dynamically assign IP addresses to PCs on your network if they are configured to automatically obtain IP addresses.

DHCP Server	
Status	Parameters
Quick Start	DHCP Server Functions <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Configuration	IP Pool Range From 192.168.1.100
LAN	IP Pool Range to 192.168.1.199
Ethernet	Primary DNS Server 0.0.0.0
DHCP Server	Secondary DNS Server 0.0.0.0
LAN Address Mapping	Primary WINS Server 0.0.0.0
WAN	Secondary WINS Server 0.0.0.0
System	Gateway 0.0.0.0
Firewall	Domain Name
VPN	
QoS	
Virtual Server	
Advanced	
Log & E-mail Alert	
Save Config to Flash	

[Fixed Host](#)

To disable the router's DHCP Server, select the **Disable** radio button, and then click **Apply**. When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (192.168.1.254 by default).

To configure the router's DHCP Server, select the **Enable** radio button, and then configure parameters of the DHCP Server including the IP Pool (starting IP address and ending IP address to be allocated to the PCs on your network), DNS Server, WINS Server, and Domain Name. These details are sent to each DHCP client when they request an IP address from the DHCP server. Click **Apply** to enable this function.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Fixed Host allows specific computer/network clients to have a reserved IP address.

A screenshot of a web-based configuration interface for a network device. On the left is a vertical sidebar menu with options: Status, Quick Start, Configuration, LAN, Ethernet, DHCP Server, LAN Address Mapping, WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, Log & E-mail Alert, and Save Config to Flash. The main area is titled "Fixed Host" and contains a "Fixed Host Table" section. This section has input fields for "Name", "Active" (with radio buttons for "Enable" and "Disable"), "IP Address", and "MAC Address". Below these fields are "Add" and "Cancel" buttons. A large empty table area is below the input fields. At the bottom of the main area are "Delete" and "Submit" buttons.

Name: The name you want to call your Fixed Host table item.

Active: Choose whether to **Enable** or **Disable** this item rule.

IP Address: Enter the IP address that you want to reserve for the above MAC address.

MAC Address: Enter the MAC address of the PC or server you wish to be assigned a reserved IP.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

Click the **Apply** button to add the configuration into the Host Table. Press the **Delete** button to delete a configuration from the Host Table.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.1.3 LAN Address Mapping

Allow user to define multiple IP / subnet on LAN side for the device. User can pick up an IP address in "WAN IP Address" field (user can also define WAN IPs in WAN IP alias page first), user can obtain different Internet IP address to be used for each subnet.

Status	LAN Address Mapping LAN Address Mapping Table <table border="1"><thead><tr><th>No.</th><th>Name</th><th>IP Address</th><th>Netmask</th><th>WAN IP</th><th></th><th></th></tr></thead><tbody><tr><td colspan="7">Create</td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr><tr><td colspan="7"> </td></tr></tbody></table>	No.	Name	IP Address	Netmask	WAN IP			Create																																																																																																								
No.		Name	IP Address	Netmask	WAN IP																																																																																																												
Create																																																																																																																	
Quick Start																																																																																																																	
Configuration																																																																																																																	
LAN																																																																																																																	
Ethernet																																																																																																																	
DHCP Server																																																																																																																	
LAN Address Mapping																																																																																																																	
WAN																																																																																																																	
System																																																																																																																	
Firewall																																																																																																																	
VPN																																																																																																																	
QoS																																																																																																																	
Virtual Server																																																																																																																	
Advanced																																																																																																																	
Log & E-mail Alert																																																																																																																	
Save Config to Flash																																																																																																																	

Create: Click **Create** to add an entry to LAN Address Mapping.

Status	LAN Address Mapping Add Subnet <table border="1"><tr><td>Name</td><td colspan="4"><input type="text"/></td></tr><tr><td>IP Address</td><td><input type="text"/></td><td><input type="text"/></td><td><input type="text"/></td><td><input type="text"/></td></tr><tr><td>Netmask</td><td><input type="text"/></td><td><input type="text"/></td><td><input type="text"/></td><td><input type="text"/></td></tr><tr><td>WAN IP Address</td><td>Candidates</td><td><input type="text"/></td><td><input type="text"/></td><td><input type="text"/></td></tr><tr><td colspan="5"><input type="button" value="Apply"/></td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr><tr><td colspan="5"> </td></tr></table>	Name	<input type="text"/>				IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Netmask	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	WAN IP Address	Candidates	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Apply"/>																																																						
Name		<input type="text"/>																																																																										
IP Address		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																							
Netmask		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																							
WAN IP Address		Candidates	<input type="text"/>	<input type="text"/>	<input type="text"/>																																																																							
<input type="button" value="Apply"/>																																																																												
Quick Start																																																																												
Configuration																																																																												
LAN																																																																												
Ethernet																																																																												
DHCP Server																																																																												
LAN Address Mapping																																																																												
WAN																																																																												
System																																																																												
Firewall																																																																												
VPN																																																																												
QoS																																																																												
Virtual Server																																																																												
Advanced																																																																												
Log & E-mail Alert																																																																												
Save Config to Flash																																																																												

Name: Enter the name you wish to call this LAN Address Mapping entry.

IP Address: Enter the IP Address.

Netmask: Enter the Netmask.

WAN IP Address: Enter the WAN IP Address that you will like to map the LAN IP Address to. Click on Candidate to search for current available WAN IP address.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.2 WAN

WAN refers to your Wide Area Network connection. In most cases, this means your router's connection to the Internet through your ISP.

4.4.2.1 WAN

Status	WAN
Quick Start	DHCP
Configuration	Connection Method: Obtain an IP Address Automatically
LAN	Host Name: Obtain an IP Address Automatically
WAN	MAC Address: Static IP Setting
WAN	Candidates: PPPoE Setting
Bandwidth Settings	Big Pond Setting
WAN IP Alias	DNS: Primary DNS: 0.0.0.0
System	Secondary DNS: 0.0.0.0
Firewall	RIP: Disable
VPN	MTU: 1500
QoS	Network Address Translation: Enable
Virtual Server	
Advanced	
Log & E-mail Alert	
Save Config to Flash	

Connection Method: Select how your router will connect to the Internet. Selections include **Obtain an IP Address Automatically**, **Static IP Settings**, **PPPoE Settings**, **PPTP Settings**, and **Big Pond Settings**. For each WAN port, the factory default is DHCP. If your ISP does not use DHCP, select the correct connection method and configure the connection accordingly. Configurable items will vary depending on the connection method selected.

4.4.2.1.1 DHCP

Status	WAN
Quick Start	DHCP
Configuration	Connection Method: Obtain an IP Address Automatically
LAN	Host Name:
WAN	MAC Address: <input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
WAN	Candidates: MAC Address: 00.00.00.00.00.00
Bandwidth Settings	<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
WAN IP Alias	DNS: Primary DNS: 0.0.0.0
System	Secondary DNS: 0.0.0.0
Firewall	RIP: Disable
VPN	MTU: 1500
QoS	Network Address Translation: Enable
Virtual Server	
Advanced	
Log & E-mail Alert	
Save Config to Flash	

Host Name: Some ISPs authenticate logins using this field.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Network Address Translation (NAT): Choose whether to **Enable** or **Disable** NAT.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.4.2.1.2 Static IP

WAN	
Static IP	
Connection Method	Static IP Setting
IP Assigned by Your ISP	0 . 0 . 0 . 0
IP Subnet Mask	0 . 0 . 0 . 0
ISP Gateway Address	0 . 0 . 0 . 0
MAC Address	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
Candidates	MAC Address 00 - 00 - 00 - 00 - 00 - 00
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
MTU	1500
Network Address Translation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

IP assigned by your ISP: Enter the static IP assigned by your ISP.

IP Subnet Mask: Enter the IP subnet mask provided by your ISP.

ISP Gateway Address: Enter the ISP gateway address provided by your ISP.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

Primary DNS: Enter the primary DNS provided by your ISP.

Secondary DNS: Enter the secondary DNS provided by your ISP.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Network Address Translation (NAT): Choose whether to **Enable** or **Disable** NAT.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.2.1.3 PPPoE

Status	WAN	
Quick Start	PPPoE	
Configuration	Connection Method	PPPoE Setting
LAN	Username	
WAN	Password	
WAN	Retype Password	
Bandwidth Settings	Connection	Always Connect
WAN IP Alias	Idle Time	10 minutes
System	IP Assigned by Your ISP	<input checked="" type="radio"/> Dynamic (IP Assigned by Your ISP) <input type="radio"/> Fixed (Your ISP requires you to input IP address)
Firewall		
VPN	MAC Address	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
QoS	Candidates	MAC Address - 00 00 00 00 00 00
Virtual Server		<input type="checkbox"/> Your ISP requires you to manually setup DNS settings
Advanced	DNS	Primary DNS 0 0 0 0 Secondary DNS 0 0 0 0
Log & E-mail Alert	RIP	Disable <input type="checkbox"/> IP-2B RIPQM
Save Config to Flash	MTU	1492
	Network Address Translation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Deferred Start Time	0 seconds
	<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

IP Assigned by your ISP: If your IP is dynamically assigned by your ISP, select the **Dynamic** radio button. If your IP assigns a static IP address, select the **Static** radio button, and input your IP address in the blank provided.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

Network Address Translation (NAT): Choose whether to **Enable** or **Disable** NAT.

4.4.2.1.4 PPTP

The screenshot shows the PPTP configuration page. The left sidebar contains a navigation menu with items: Status, Quick Start, Configuration, LAN, WAN, WAN, Bandwidth Settings, WAN IP Alias, System, Firewall, VPN, QoS, Virtual Server, Advanced, Log & E-mail Alert, and Save Config to Flash. The main content area is titled 'WAN' and 'PPTP'. It includes the following fields and options:

- Connection Method: PPTP Setting (dropdown)
- Username: [text input]
- Password: [text input]
- Retype Password: [text input]
- PPTP client IP: [0][0][0][0] (four digit inputs)
- PPTP client IP Netmask: [0][0][0][0] (four digit inputs)
- PPTP client IP Gateway: [0][0][0][0] (four digit inputs)
- PPTP server IP: [0][0][0][0] (four digit inputs)
- Connection: Always Connect (dropdown)
- Idle Time: 10 minutes (dropdown)
- IP Assigned by Your ISP:
 - ☒ Dynamic (IP Assigned by Your ISP)
 - ☐ Fixed (Your ISP requires you to input IP address)
- MAC Address:
 - ☐ Your ISP requires you to input WAN Ethernet MAC
 - MAC Address: [00][00][00][00][00][00] (six digit inputs)
 - ☐ Your ISP requires you to manually setup DNS settings
- DNS:
 - Primary DNS: [0][0][0][0] (four digit inputs)
 - Secondary DNS: [0][0][0][0] (four digit inputs)
- RIP: Disable (dropdown) ☒ P-2B RIP ON
- MTU: 1432 (text input)
- Network Address Translation: ☒ Enable ☐ Disable

At the bottom, there are 'Apply' and 'Reset' buttons.

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

PPTP Client IP: Enter the PPTP Client IP provided by your ISP.

PPTP Client IP Netmask: Enter the PPTP Client IP Netmask provided by your ISP.

PPTP Client IP Gateway: Enter the PPTP Client IP Gateway provided by your ISP.

PPTP Server IP: Enter the PPTP Server IP provided by your ISP.

Connection: Select whether the connection should **Always Connect** or **Trigger on Demand**. If you want the router to establish a PPTP session when starting up and to automatically re-establish the PPTP session when disconnected by the ISP, select **Always Connect**. If you want to establish a PPTP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet), select **Trigger on Demand**.

Idle Time: Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



if **Trigger on Demand** is selected.

IP Assigned by your ISP: If your IP is dynamically assigned by your ISP, select the **Dynamic** radio button. If your IP assigns a static IP address, select the **Static** radio button. This will take you to another page for inputting the IP address information.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Network Address Translation (NAT): Choose whether to **Enable** or **Disable** NAT.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

4.4.2.1.5 Big Pond

Status	WAN
Quick Start	Big Pond
Configuration	Connection Method Big Pond Setting
LAN	Username <input type="text"/>
WAN	Password <input type="password"/>
WAN	Retype Password <input type="password"/>
Bandwidth Settings	Loginserver <input type="text"/>
WAN IP Alias	MAC Address <input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC
System	MAC Address <input type="text"/>
Firewall	DNS <input type="checkbox"/> Your ISP requires you to manually setup DNS settings
VPN	Primary DNS <input type="text"/>
QoS	Secondary DNS <input type="text"/>
Virtual Server	RIP Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
Advanced	MTU <input type="text"/>
Log & E-mail Alert	Network Address Translation <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Save Config to Flash	<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Username: Enter your user name.

Password: Enter your password.

Retype Password: Retype your password.

Login Server: Enter the IP of the Login server provided by your ISP.

MAC Address: If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

DNS: If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

RIP: To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



disable RIP, select **Disable** from the drop down menu.

MTU: Enter the Maximum Transmission Unit (MTU) for your network.

Network Address Translation (NAT): Choose whether to **Enable** or **Disable** NAT.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

A simpler alternative is to select **Quick Start** from the main menu. Please see the **Quick Start** section of this chapter for more information.

4.4.2.2 Bandwidth Settings

Under Bandwidth Settings, you can easily configure both inbound and outbound bandwidth.

Bandwidth Settings			
Max Bandwidth Provided by ISP			
WAN	Outbound Bandwidth	102400	kbps
	Inbound Bandwidth	102400	kbps
<input type="button" value="Apply"/>			

WAN: Enter your ISP inbound and outbound bandwidth for WAN. **[LL8]**

NOTE: These values entered here are referenced by QoS.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.2.3 WAN IP Alias

Allow user to define multiple WAN IP for the device. This can be used when there is more than one IP address assigned to the user by ISP. User can pick up different IP addresses among WAN IP aliases in virtual server configuration so that different public IP address mapping to different internal server. Besides, user can also pick up different LAN subnet in the LAN address mapping page so that when user at LAN side in the specified subnet were going out, it will use specified WAN IP address.

Status	WAN IP Alias WAN IP Alias Table <table border="1"><thead><tr><th>NO.</th><th>Name</th><th>IP Address</th></tr></thead><tbody><tr><td colspan="3">Create</td></tr></tbody></table>	NO.	Name	IP Address	Create		
NO.		Name	IP Address				
Create							
Quick Start							
Configuration							
LAN							
WAN							
WAN							
Bandwidth Settings							
WAN IP Alias							
System							
Firewall							
VPN							
QoS							
Virtual Server							
Advanced							
Log & E-mail Alert							
Save Config to Flash							

Create: Click **Create** to add an entry to WAN IP Alias.

Status	WAN IP Alias Add WAN IP <table border="1"><tr><td>Name</td><td><input type="text"/></td></tr><tr><td>IP Address</td><td><input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/></td></tr><tr><td colspan="2"><input type="button" value="Apply"/></td></tr></table>	Name	<input type="text"/>	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	<input type="button" value="Apply"/>	
Name		<input type="text"/>					
IP Address		<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>					
<input type="button" value="Apply"/>							
Quick Start							
Configuration							
LAN							
WAN							
WAN							
Bandwidth Settings							
WAN IP Alias							
System							
Firewall							
VPN							
QoS							
Virtual Server							
Advanced							
Log & E-mail Alert							
Save Config to Flash							

Name: Type the name for the WAN IP Alias entry.

IP Address: Type the IP Address for the WAN IP Alias.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.3 System

The System menu allows you to adjust a variety of basic router settings, upgrade firmware, set up remote access, and more. In this menu are the following sections: Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart, Password, Ping & Trace.

System
Time Zone
Remote Access
Firmware Upgrade
Backup / Restore
Restart
Password
Ping&tracert

Black Box Corporation


1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.3.1 Time Zone

<ul style="list-style-type: none">StatusQuick StartConfigurationLANWANSystemTime ZoneRemote AccessFirmware UpgradeBackup / RestoreRestartPasswordPing&tracertFirewallVPNQoSVirtual ServerAdvancedLog & E-mail AlertSave Config to Flash	Time Zone	
	Parameters	
	Time Zone	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Local Time Zone (+-GMT Time)	(GMT-07:00)Mountain Time (US & Canada) ▼
	NTP Server Address	<input type="text" value="carl.css.gov"/> <input type="text" value="india.colorado.edu"/> <input type="text" value="time.nist.gov"/> <input type="text" value="time-b.nist.gov"/>
	Daylight Saving	<input type="checkbox"/> Automatic
	Resync Period	<input type="text" value="1440"/> minutes
		
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Firetunnel 10 does not use an onboard real time clock; instead, it uses the Network Time Protocol (NTP) to acquire the current time from an NTP server outside your network. Simply choose your local time zone, enter NTP Server IP Address, and click **Apply**. After connecting to the Internet, Firetunnel 10 will retrieve the correct local time from the NTP server you have specified. Your ISP may provide an NTP server for you to use.

To have Firetunnel 10 automatically adjust for Daylight Savings Time, check the **Automatic** checkbox.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.3.2 Remote Access

Remote Access	
Remote Access Function	
Action	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
* HTTPS Port	443
<i>* : This setting will become effective after you save to flash and restart the router.</i>	
<input type="button" value="Apply"/>	

Remote Access Table			
No.	IP Address		
Create			

To allow remote users to configure and manage Firetunnel 10 through the Internet, select the Enable radio button. To deactivate remote access, select the **Disable** radio button. This function also enables you grant access from any PC or from a specific IP address. Click **Apply** to save your settings.

Create: Click **Create** to create a new rule for the Remote Access.

Remote Access	
You may permit remote administration of this network device (HTTPS).	
Allow Remote Access By	<input checked="" type="radio"/> Everyone (Everyone)
	<input type="radio"/> Only this PC: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	<input type="radio"/> PC from this subnet: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input type="button" value="Apply"/>	

Everyone: Anyone can remote access this device.

Only this PC: Specify an IP address so only that IP address can remote access this device.

PC from this subnet: Specify a subnet so only PCs under this subnet can remote access this device.

NOTE: When enabling remote access, be sure to change the default administration password to something more secure.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.3.3 Firmware Upgrade

Firmware Upgrade		
You may upgrade the system software on your network device		
New Firmware Image	<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Upgrade"/>		

Upgrading your Firetunnel 10's firmware is a quick and easy way to enjoy increased functionality, better reliability, and ensure trouble-free operation. To upgrade your firmware, simply visit Black Box's website (<http://www.Black Box.com>) and download the latest firmware image file for Firetunnel 10. Next, click **Browse** and select the newly downloaded firmware file. Click **Upgrade** to complete the update.

NOTE: DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Interrupting the firmware upgrade process could damage the router.

4.4.3.4 Backup / Restore

Backup/Restore		
Allows you to backup the configuration settings to your computer, or restore configuration from your computer.		
Backup Configuration		
Backup configuration to your computer.		
<input type="button" value="Backup"/>		
Restore Configuration		
Configuration File	<input type="text"/>	<input type="button" value="Browse..."/>
<i>"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.</i>		
<input type="button" value="Restore"/>		

This feature allows you to save and backup your router's current settings, or restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy. It is advisable to backup your router's settings before making any significant changes to your router's

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



configuration.

To backup your router's settings, click **Backup** and select where to save the settings backup file. You may also change the name of the file when saving if you wish to keep multiple backups. Click **OK** to save the file.

To restore a previously saved backup file, click **Browse**. You will be prompted to select a file from your PC to restore. Be sure to only restore setting files that have been generated by the Backup function, and that were created when using the same firmware version. Settings files saved to your PC should not be manually edited in any way. After selecting the settings file you wish to use, clicking **Restore** will load those settings into the router.

4.4.3.5 Restart

Restart	
After restarting. Please wait for several seconds to let the system restart	
Restart Router with	<input checked="" type="radio"/> Current Settings
	<input type="radio"/> Factory Default Settings
<input type="button" value="Restart"/>	

The Restart feature allows you to easily restart Firetunnel 10. To restart with your last saved configuration, select the **Current Settings** radio button and click **Restart**.

If you wish to restart the router using the factory default settings, select **Factory Default Settings** and click **Restart** to reboot Firetunnel 10 with factory default settings.

You may also reset your router to factory default settings by holding the Reset button on the router until the Status LED begins to blink. Once Firetunnel 10 completes the boot sequence, the Status LED will stop blinking.

Black Box Corporation


1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.3.6 Password

Password	
Parameters	
Password	<input type="password"/>
Confirm	<input type="password"/>
 <i>Note: number of maximum characters of password is 32 characters.</i>	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

In order to prevent unauthorized access to your router's configuration interface, it requires the administrator to login with a password. You can change your password by entering your new password in both fields. Click **Apply** to save your changes. Click **Reset** to reset to the default administration password (admin).

4.4.3.7 Ping & Trace

Ping Message Testing	
Ping testing	
Destination IP & Domain name	<input type="text"/>
<input type="button" value="PingTesting"/>	
Trace route testing	
Trace IP	<input type="text"/>
Max TTL value	<input type="text" value="16"/>
Wait time	<input type="text" value="3"/> ms
<input type="button" value="TraceTesting"/>	

This function allows Firetunnel 10 to test the system if it's well connected. Type in the IP address or domain name you want to Ping and click the **PingTesting**. Type in the IP address connected to WAN 1 or 2, and set the Max TTL value, the default is 16. Set the wait time then click **TraceTesting** button.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.4 Firewall

Firetunnel 10 includes a full Stateful Packet Inspection (SPI) firewall for controlling Internet access from your LAN, and preventing attacks from hackers. Your router also acts as a "natural" Internet firewall when using Network Address Translation (NAT), as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet. Please see the WAN configuration section for more details.

Firewall
Packet Filter
URL Filter
LAN MAC Filter
Block WAN Request
Intrusion Detection

You can find five items under the Firewall section: **Packet Filter**, **URL Filter**, **LAN MAC Filter**, **Block WAN Request** and **Intrusion Detection**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.4.1 Packet Filter

Packet Filter										
Packet Filter Table										
ID	Enable	Action	Direction	Src. IP	Dest. IP	Protocol	Src. Port	Dest. Port		
Create										

The Packet Filter function is used to limit user access to certain sites on the Internet or LAN. The Filter Table displays all current filter rules. If there is an entry in the Filter Table, you can click **Edit** to modify the setting of this entry, or click **Delete** to remove this entry, or click **Move** to change this entry's priority.

When the entry is upper, the priority is higher.

To create a new filter rule, click **Create**.

Packet Filter																				
Add Filtering Rules																				
ID	<input type="text" value="1"/>																			
Rule	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																			
Action When Matched	Drop																			
Direction	Outgoing																			
Source IP	Any	Start IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>														
		End IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>														
		Netmask	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>														
Destination IP	Any	Start IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>														
		End IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>														
		Netmask	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>														
Protocol	Any																			
Source Port Range	Helper	<input type="text" value="1"/>	~	<input type="text" value="65535"/>																
Destination Port Range	Helper	<input type="text" value="1"/>	~	<input type="text" value="65535"/>																
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable																			
<input type="button" value="Apply"/>																				

ID: This is an identify that allows you to move the rule by before or after an ID.

Rule: Enable or Disable this entry.

Action When Matched: Select to **Drop** or **Forward** the packet specified in this filter entry.

Direction: Incoming Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet. Outgoing Packet Filter rules prevent unauthorized computers or applications accessing the Internet. Select if the new filter rule is incoming or outgoing.

Source IP: Select **Any**, **Subnet**, **IP Range** or **Single Address**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



Starting IP Address: Enter the source IP or starting source IP address this filter rule is to be applied.

End IP Address: Enter the End source IP Address this filter rule is to be applied. (for IP Range only)

Netmask: Enter the subnet mask of the above IP address.

Destination IP: Select **Any**, **Subnet**, **IP Range** or **Single Address**.

Starting IP Address: Enter the destination IP or starting destination IP address this filter rule is to be applied.

End IP Address: Enter the End destination IP Address this filter rule is to be applied. (for IP Range only)

Netmask: Enter the subnet mask of the above IP address.

Protocol: Select the Transport protocol type (Any, TCP, UDP).

Source Port Range: Enter the source port number range. If you only want to specify one service port, then enter the same port number in both boxes.

Destination Port Range: Enter the destination port number range. If you only want to specify one service port, then enter the same port number in both boxes.

Helper: You could also select the application type you would like to apply for automatic input.

Log: Choose whether to Enable or Disable the logging service for this rule.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.4.2 URL Filter

URL Filter	
Configuration	
URL Filtering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Keyword Filtering	<input type="checkbox"/> Enable Details ▶
Domains Filtering	<input type="checkbox"/> Enable Details ▶
Restrict URL Features	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block ActiveX
	<input type="checkbox"/> Block Web proxy
	<input type="checkbox"/> Block Cookie
	<input type="checkbox"/> Block Surfing by IP Address
Log	<input type="checkbox"/> Enable
<input type="button" value="Apply"/>	
Exception List	
Name	IP Address
Create ▶	

The URL Filter is a powerful tool that can be used to limit access to certain URLs on the Internet. You can block web sites based on keywords or even block out an entire domain. Certain web features can also be blocked to grant added security to your network.

URL Filtering: You can choose to Enable or Disable this feature.

Keyword Filtering: Click the checkbox to enable this feature. To edit the list of filtered keywords, click Details.

Domain Filtering: Click the "enable" checkbox to enable filtering by Domain Name. Click the "Disable all WEB traffic except for trusted domains" check box to allow web access only for trusted domains.

Restrict URL Features: Click "Block Java Applet" to filter web access with Java Applet components. Click "Block ActiveX" to filter web access with ActiveX components. Click "Block Web proxy" to filter web proxy access. Click "Block Cookie" to filter web access with Cookie components. Click "Block Surfing by IP Address" to filter web access with an IP address as the domain name.

Exception List: You can input a list of IP addresses as the exception list for URL filtering.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Log: Choose whether to Enable or Disable the logging service for this rule.

Keywords Filtering		
Create		
Keyword	<input type="text"/>	
<input type="button" value="Apply"/>		
Block WEB URLs which contain these keywords		
No.	Keyword	

Enter a keyword to be filtered and click **Apply**. Your new keyword will be added to the filtered keyword listing.

Domains Filtering: Click the top checkbox to enable this feature. You can also choose to disable all web traffic except for trusted sites by clicking the bottom checkbox. To edit the list of filtered domains, click **Details**.

Domains Filtering		
Create		
Domain Name	<input type="text"/>	
Type	<input type="text" value="Forbidden Domain"/>	
<input type="button" value="Apply"/>		
Trusted Domain Table		
No.	Domain	
Forbidden Domain Table		
No.	Domain	

Enter a domain and selected whether this domain is trusted or forbidden with the pull-down menu. Next, click **Apply**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously.

Restrict URL Features: Use this to disable certain web features. Select the options you want (Block Java Applet, Block ActiveX, Block Web proxy, Block Cookie, Block Surfing by IP Address) and click **Apply** to save your changes.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



You may also designate which IP addresses are to be excluded from these filters by adding them to the Exception List. To do so, click **Add**.

Exception				
Create				
Name	<input type="text"/>			
IP Address	Candidates ▶	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Apply"/>				

Enter a name for the IP Address and then enter the IP address itself. Click **Apply** to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect.

4.4.4.3 LAN MAC Filter

LAN MAC Filter					
Default Rule					
Action	<input checked="" type="radio"/> Forward <input type="radio"/> Drop				
<input type="button" value="Apply"/>					
Rule Lists					
No.	Enable	Action	MAC Address		
Create ▶					

LAN Mac Filter can decide that Firetunnel will serve those devices at LAN side or not by MAC Address.

Default Rule: Forward or Drop all LAN requests. (Forward by default)

Create: You can also input a specified MAC Address to be dropped or Forward without depending on the default rule.

LAN MAC Filter	
Create Rule	
Rule	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Action When Matched	<input type="text" value="Drop"/> ▼
Mac Address	Candidates ▶ <input type="text"/>
Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/>	

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Rule: Enable or disable this entry.

Action When Matched: Select to **Drop** or **Forward** the packet specified in this filter entry.

MAC Address: The MAC Address you would like to apply.

Candidates: You can also select the **Candidates** which are referred from the ARP table for automatic input.

4.4.4.4 Block WAN Request

Block WAN Request	
Enable for preventing any ping test from Internet, such as hacker attack.	
Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

Blocking WAN requests is one way to prevent DDoS attacks by preventing ping requests from the Internet. Use this menu to enable or disable function.

4.4.4.5 Intrusion Detection

Intrusion Detection	
Enable for preventing hacker attack from Internet.	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ARP Protection	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Session Limit	<input checked="" type="radio"/> No Limit <input type="radio"/> Limit maximum sessions per IP to <input type="text" value="200"/> <input type="radio"/> Limit maximum sessions per IP to <input type="text" value="200"/> <input checked="" type="radio"/> , reject new session from this IP in <input type="text" value="5"/> minutes. <input type="radio"/> , drop all packets from this IP in <input type="text" value="5"/> minutes.
<input type="button" value="Apply"/>	

Intrusion Detection can prevent most common DoS attacks from the Internet or from LAN users.

Intrusion Detection: Enable or disable this function.

Intrusion Log: All the detected and dropped attacks will be shown in the system log.

ARP Protection: ARP protection is used to protect users on the LAN against ARP virus. When enabled, ARP Protection will only protect computers that were set in **Fixed Host (refer to page 72)** so that the ARP table of the hosts can be updated. Periodically Firetunnel10 will send ARP packets to these computers to refresh their ARP tables. Enabling ARP Protection can prevent potential viruses infecting computers within the local network. Enabling this option will mitigate the effect of ARP virus attack on LAN.

Session Limit: Allows administrators to self-define the amount of sessions that currently allowed to connect to Firetunnel10. This function limits the number of connections on per-user basis. This is useful when controlling users who will use the applications which create a large number of connections (such as P2P software).

No Limit: No restrictions on the amount of sessions allowed to connect to Firetunnel10.

Limit Maximum sessions per IP to: Restricts an upper limit of sessions allowed to connect to Firetunnel10, additional sessions beyond the maximum limit will not be allowed to connect.

Limit Maximum sessions per IP to (with reject and drop options): Just

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



like the previous option, this option expands on what to do with additional sessions above the maximum limit. You can either reject the additional sessions for a period of time or just drop all packets from those sessions for a period of time.

4.4.5 VPN

4.4.5.1 IPSec

IPSec is a set of protocols that enable Virtual Private Networks (VPN). VPN is a way to establish secured communication tunnels to an organization's network via the Internet.

4.4.5.1.1 IPSec Wizard

A screenshot of the "Step 1 of 3: Connection Information" screen from the IPSec Wizard. The screen has a light gray background. At the top, the title "Step 1 of 3: Connection Information" is in bold. Below the title, there are three main sections: "Connection Name" with a text input field, "PreShared Key" with a text input field, and "Connection Type" with a list of radio button options. The "Connection Type" section is highlighted with an orange background. The options for "Connection Type" are: "LAN to LAN" (selected with a green dot), "LAN to LAN (Mobile LAN)", "LAN to Host", "LAN to Host (Mobile Client)", and "LAN to Host (For Firetunnel VPN Client)". At the bottom left, there is a "Next" button.

Connection Name: A user-defined name for the connection.

Interface: Select the interface the IPSec tunnel will apply to.

WAN1: Select interface WAN1

WAN2: Select interface WAN2

Auto: The device will automatically apply the tunnel to WAN1 or WAN2 depending on which WAN interface is active when the IPSec tunnel is being established. Note. Auto only applies to Fail Over mode. For Load Balance mode, please do not select "Auto". In Load Balance mode, Auto will be forced to WAN1 interface if Auto is selected.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



pre-shared key into both sides (router or hosts).

Connection Type:

There are 5 connection types:

(1) LAN to LAN: Firetunnel would like to establish an IPSec VPN tunnel with remote router using Fixed Internet IP or domain name by using main mode.

IPSec Wizard				
Step 2 of 3: Remote Information				
Remote Secure Gateway Address (or Hostname)		<input type="text"/>		
Remote Network	IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
	Netmask	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>				

Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Remote Network: The subnet of the remote network. Allows you to enter an IP address and netmask.

Back: Back to the Previous page.

Next: Go to the next page.

(2) LAN to Mobile LAN: Firetunnel would like to establish an IPSec VPN tunnel with remote router using Dynamic Internet IP by using aggressive mode.

IPSec Wizard				
Step 2 of 3: Remote Information				
Remote Identifier		<input type="text"/>		
Remote Network	IP Address	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
	Netmask	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>				

Remote Identifier: The Identifier of remote gateway, all input value type will be auto-defined as IP Address, FQDN(DNS) or FQUN(E-mail).

Remote Network: The subnet of the remote network. Allows you to enter an IP address and netmask.

Back: Back to the Previous page.

Next: Go to the next page.

(3) LAN to Host: Firetunnel would like to establish an IPSec VPN tunnel with

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



remote client software using Fixed Internet IP or domain name by using main mode.

IPSec Wizard	
Step 2 of 3: Remote Information	
Remote Secure Gateway Address (or Hostname)	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Back: Back to the Previous page.

Next: Go to the next page.

(4)LAN to Mobile Host: Firetunnel would like to establish an IPSec VPN tunnel with remote client software using Dynamic Internet IP by using aggressive mode.


IPSec Wizard	
Step 2 of 3: Remote Information	
Remote Identifier	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Remote Identifier: The Identifier of remote gateway, all input value type will be auto-defined as IP Address, FQDN(DNS) or FQUN(E-mail).

Back: Back to the Previous page.

Next: Go to the next page.

(5)LAN to Host (for Firetunnel VPN Client only): Firetunnel would like to establish an IPSec VPN tunnel with Firetunnel VPN Client software C01 by using aggressive mode.

IPSec Wizard	
Step 2 of 3: Remote Information	
VPN Client IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="100"/> . <input type="text" value="1"/>
 1. Please note that this field must be consistent with the setting of VPN Client. 2. Be sure that each client must use different VPN Client IP Address.	
<input type="button" value="Back"/> <input type="button" value="Next"/>	

VPN Client IP Address: The VPN Client Address for Firetunnel VPN Client, this value will be apply on both **remote ID** and remote **Network** as single address.

Back: Back to the Previous page.

Next: Go to the next page.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



<ul style="list-style-type: none"> Status Quick Start Configuration LAN WAN System Firewall VPN IPSec IPSec Wizard IPSec Policy PPTP PPTP Client QoS Virtual Server Advanced Log & E-mail Alert Save Config to Flash 	IPSec Wizard				
	Configuration Summary				
	Connection Name		BBOX		
	Tunnel		Enabled		
	Interface		WAN1		
	Local	ID	WAN IP Address	Type	IP Address
		Network	192.168.1.254/255.255.255.0	Type	Subnet
	Remote	Secure Gateway	BBOX TPE	Type	IP Address/ Hostname
		ID	Remote Secure Gateway IP Address	Type	IP Address
	Proposal	Network	192.168.1.1/255.255.255.255	Type	Subnet
		Secure Association	Main Mode		
		Method	ESP		
		Encryption Protocol	3DES		
		Authentication Protocol	MD5		
		Perfect Forward Secure	Enabled		
		Key Group	Group 2		
		PreShared Key	blackbox		
		IKE Life Time	3600 seconds		
		Key Life Time	28800 seconds		
	<input type="button" value="Back"/> <input type="button" value="Done"/>				

After your configuration is done, you will see a **Configuration Summary**.

Back: Back to the Previous page.

Done: Click **Done** to apply the rule.

4.4.5.1.2 IPSec Policy

IPSec						
IPSec Tunnels						
Name	Enable	Local Network	Remote Network	Remote Gateway	IPSec Proposal	
<input type="button" value="Create"/>						

Click **Create** to create a new IPSec VPN connection account.

Configuring a New VPN Connection

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Connection Name	<input type="text"/>		
Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Local			
ID	<input type="text" value="IP Address"/>	Data	<input type="text"/>
Network	<input type="text" value="Any Local Address"/>	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		End IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		Netmask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Remote			
Secure Gateway	<input type="text" value="IP Address/ Hostname"/>	Data	<input type="text"/>
ID	<input type="text" value="IP Address"/>	Data	<input type="text"/>
Network	<input type="text" value="Subnet"/>	IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		End IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		Netmask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Proposal			
Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key		
Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Protocol	<input type="text" value="3DES"/>		
Authentication Protocol	<input type="text" value="MD5"/>		
Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
PreShared Key	<input type="text"/>		
IKE Life Time	<input type="text" value="28800"/>	Seconds	
Key Life Time	<input type="text" value="3600"/>	Seconds	
Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
DPD Setting			
DPD Function	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
Detection Interval	<input type="text" value="30"/>	seconds	
Idle Timeout	<input type="text" value="4"/>	consecutive times	

Connection Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate this tunnel. Select **Disable** to deactivate this tunnel.

Local: This section configures the local host.

ID: This is the identity type of the local router or host. Choose from the following four options:

WAN IP Address: Automatically use the current WAN Address as ID

IP Address: Use an IP address format.

FQDN DNS(Fully Qualified Domain Name): Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.

FQUN E-Mail(Fully Qualified User Name): Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.

Data: Enter the ID data using the specific ID type.

Network: Set the IP address, IP range, subnet, or address range of the local

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



network.

Any Local Address: Will enable any local address on the network.

Subnet: The subnet of the local network. Selecting this option enables you to enter an IP address and netmask.

IP Range: The IP Range of the Local network.

Single Address: The IP address of the local host.

Remote: This section configures the remote host.

Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

ID: The identity type of the local host. Choose from the following three options:

Remote IP Address: Automatically use the remote gateway Address as ID with ID type – IP Address.

IP Address: Use an IP address format.

FQDN DNS(Fully Qualified Domain Name): Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.

FQUN E-Mail(Fully Qualified User Name): Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.

Data: Enter the ID data using the specific ID type.

Network: Set the subnet, IP Range, single address, or gateway address of the remote network.

Subnet: The subnet of the remote network. Selecting this option allows you to enter an IP address and netmask.

IP Range: The IP Range of the remote network.

Single Address: The IP address of the remote host.

Gateway Address: The gateway address of the remote host.

Proposal:

Secure Association (SA): SA is a method of establishing a security policy between two points. There are three methods of creating SA, each varying in degrees of security and speed of negotiation:

Main Mode: Uses the automated Internet Key Exchange (IKE) setup; most secure method with the highest level of security.

Aggressive Mode: Uses the automated Internet Key Exchange (IKE) setup; mid-level security. Speed is faster than Main mode.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



Manual Key: Standard level of security. It is the fastest of the three methods.

Method: There are two methods of checking the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. AH data will be authenticated but not encrypted.

Encryption Protocol: Select the encryption method from the pull-down menu. There are several options: DES, 3DES, and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

DES: Stands for Data Encryption Standard. It uses a 56-bit encryption method.

3DES: Stands for Triple Data Encryption Standard. It uses a 168-bit encryption method.

AES: Stands for Advanced Encryption Standard. You can use 128, 192 or 256 bits as encryption method.

Authentication Protocol: Authentication establishes data integrity and ensures it is not tampered with while in transit. There are two options: Message Digest 5 (MD5), and Secure Hash Algorithm (SHA1). While slower, SHA1 is more resistant to brute-force attacks than MD5.

MD5: A one-way hashing algorithm that produces a 128-bit hash.

SHA1: A one-way hashing algorithm that produces a 160-bit hash.

Perfect Forward Secure: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over the Internet.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

IKE Life Time: Allows you to specify the timer interval for renegotiation of the IKE security association. The value is in seconds, e.g. 28800 seconds = 8 hours.

Key Life Time: Allows you to specify the timer interval for renegotiation of another key. The value is in seconds e.g. 3600 seconds = 1 hour.

Netbios Broadcast: Allows Firetunnel to send local Netbios Broadcast packet through the IPSec Tunnel, please select **Enable** or **Disable**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Click the **Apply** button to save your changes.

After you have created the IPSec connection, the account information will be displayed:

IPSec							
IPSec Tunnels							
Name	Enable	Local Network	Remote Network	Remote Gateway	IPSec Proposal		
Tunnel1	✓	192.168.2.0/24	192.168.3.0/24	200.200.200.1	MAIN Mode ESP [3DES: MD5]	Edit	Delete
Create							

Name: This is the user-defined name of the connection.

Enable: This function activates or deactivates the IPSec connection.

Local Subnet: Displays IP address and subnet of the local network.

Remote Subnet: Displays IP address and subnet of the remote network.

Remote Gateway: This is the IP address or Domain Name of the remote VPN device that is connected and has an established IPSec tunnel.

IPSec Proposal: This is the selected IPSec security method.

For examples on how to apply IPSec to your network, see **Appendix E: IPSec Logs and Events**.

4.4.5.2 PPTP

PPTP is a set of protocols that enable Virtual Private Networks (VPN). VPN is a way to establish secured communication tunnels to an organization's network via the Internet.

PPTP					
General Setting					
PPTP function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Auth. Type	Pap or Chap ▾				
Data Encryption	Enable ▾				
Encryption Key Length	Auto ▾				
Peer Encryption Mode	Only Stateless ▾				
IP Addresses Assigned to Peer	Start from: 192.168.1.200				
Idle Timeout	0 Min.				
(!) Enable data encryption will use MS-CHAPv2 to authenticate the peer.					
<input type="button" value="Apply"/>					
Account Setting					
Name	Enable	Type	Peer Network		
<input type="button" value="Create"/>					

PPTP function: Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

Auth. Type: The authentication type, **Pap or Chap, PaP, Chap.**

Data Encryption: Select **Enable** or **Disable** the Data Encryption.

Encryption Key Length: **Auto, 40 bits** or **128 bits**.

Peer Encryption Mode: **Only Stateless** or **Allow Stateless and Stateful**.

IP Addresses Assigned to Peer Start from: 192.168.1.x: please input the IP assigned range from **1 ~ 254** (except Firetunnel 10's LAN IP address with **192.168.1.254** as Firetunnel 10's default LAN IP address and IP pool range of DHCP server settings with **100~199** as Firetunnel 10's default DHCP IP pool range.)

Idle Timeout " " Min: Specify the time for remote peer to be disconnected without any activities, from **0~120**.

Click **Create** to create a new PPTP VPN connection account.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



PPTP	
Add PPTP Account	
Connection Name	<input type="text"/>
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="password"/>
Retype Password	<input type="password"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN
Peer Network IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Peer Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Netbios Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/>	

Connection Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate this tunnel. Select **Disable** to deactivate this tunnel.

Username: Please input the username for this account.

Password: Please input the password for this account.

Retype Password: Please repeat the same password as previous field.

Connection Type: Select **Remote Access** for single user, Select **LAN to LAN** for remote gateway.

Peer Network IP: Please input the IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

Netbios Broadcast: Allows Firetunnel to send local Netbios Broadcast packet through the PPTP Tunnel, please select **Enable** or **Disable**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.6 QoS

Firetunnel 10 can optimize your bandwidth by assigning priority to both inbound and outbound data with QoS. This menu allows you to configure QoS for both inbound and outbound traffic.

Quality of Service		
WAN Outbound		
QoS function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Rule Table ▶
Max ISP Bandwidth	102400 kbps	Bandwidth Settings ▶
WAN Inbound		
QoS function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Rule Table ▶
Max ISP Bandwidth	102400 kbps	Bandwidth Settings ▶
<input type="button" value="Apply"/>		

The first menu screen gives you an overview of which WAN ports currently have QoS active, and the bandwidth settings for each.

WAN [LL9] Outbound:

QoS Function: QoS status for WAN outbound. Select **Enable** to activate QoS for WAN's outgoing traffic. Select **Disable** to deactivate.

Max ISP Bandwidth: The maximum bandwidth afforded by the ISP for WAN's outbound traffic.

WAN Inbound:

QoS Function: QoS status for WAN inbound. Select **Enable** to activate QoS for WAN's incoming traffic. Select **Disable** to deactivate.

Max ISP Bandwidth: The maximum bandwidth afforded by the ISP for WAN's inbound traffic.

Creating a New QoS Rule

To get started using QoS, you will need to establish QoS rules. These rules tell the Firetunnel 10 how to handle both incoming and outgoing traffic. The following example shows you how to configure WAN Outbound QoS. Configuring the other traffic types follows the same process.

Black Box Corporation


1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



To make a new rule, click **Rule Table**. This will bring you to the Rule Table which displays the rules currently in effect.

Quality of Service					
WAN Outbound QoS Rule Table (total 0 rules used / maximum 40 rules.)					
Application	Guaranteed	Maximum	Priority		
Non-Assigned Bandwidth		102400 kbps (100%)			
Create 					

Next, click **Create** to open the QoS Rule Configuration window.

Quality of Service					
Add QoS Rule					
Interface	WAN Outbound				
Application	<input type="text"/>				
Guaranteed	<input type="text" value="1"/>	kbps			
Maximum	<input type="text" value="102400"/>	kbps			
Priority	<input type="text" value="3 (Normal)"/>				
DSCP Marking	<input type="text" value="Gold service(L)"/>				
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address				
Bandwidth Type	<input checked="" type="radio"/> Shared Bandwidth <input type="radio"/> Bandwidth per Source IP Address				
Source IP Address Range	From <input type="text" value="0.0.0.0"/>	To	<input type="text" value="255.255.255.255"/>		
Destination IP Address Range	From <input type="text" value="0.0.0.0"/>	To	<input type="text" value="255.255.255.255"/>		
Protocol	<input type="text" value="Any"/>				
Source Port Range Helper	From <input type="text" value="1"/>	To	<input type="text" value="65535"/>		
Destination Port Range Helper	From <input type="text" value="1"/>	To	<input type="text" value="65535"/>		
DSCP	<input type="text" value="Any"/>				
<input type="button" value="Apply"/>					

Application: User defined application name for the current rule.

Packet Type: The type of packet this rule applies to. Choose from **Any**, **TCP**, **UDP**, or **ICMP**.

Guaranteed: The guaranteed amount of bandwidth for this rule as a percentage.

Maximum: The maximum amount of bandwidth for this rule as a percentage.

Priority: The priority assigned to this service. Select a value from 0 to 6, 0 being highest.

DSCP Marking: Used to classify traffic. Select from **Best Effort**, **Premium**, **Gold Service (High Medium, Low)**, **Silver (H,M,L)**, and **Bronze (H,M,L)**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Address Type: The type of address this rule applies to. Select **IP Address** or **MAC Address**.

For IP Address (default)...

Source IP Address Range: The range of source IP Addresses this rule applies to.

Destination IP Address Range: The range of destination IP Addresses this rule applies to.

Source Port Range: The range of source ports this rule applies to.

Destination Port Range: The range of destination ports this rule applies to.

Helper: You could also select the application type you would like to apply for automatic input.

Click **Apply** to save your changes.

For MAC Address:

Quality of Service			
Add QoS Rule			
Interface	WAN Outbound		
Application	<input type="text"/>		
Guaranteed	<input type="text" value="1"/>	kbps	
Maximum	<input type="text" value="102400"/>	kbps	
Priority	<input type="text" value="3 (Normal)"/> ▼		
DSCP Marking	<input type="text" value="Gold service(L)"/> ▼		
Address Type	<input type="radio"/> IP Address <input checked="" type="radio"/> MAC Address		
Source MAC Address	Candidates ▶	<input type="text" value="00:00:00:00:00:00"/>	(ex. xx:xx:xx:xx:xx:xx)
Protocol	<input type="text" value="Any"/> ▼		
Source Port Range	Helper ▶	From <input type="text" value="1"/>	To <input type="text" value="65535"/>
Destination Port Range	Helper ▶	From <input type="text" value="1"/>	To <input type="text" value="65535"/>
DSCP	<input type="text" value="Any"/> ▼		
<input type="button" value="Apply"/>			

Source MAC Address: The source MAC Address of the device this rule applies to.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

Source Port Range: The range of source ports this rule applies to.

Destination Port Range: The range of destination ports this rule applies to.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Click **Apply** to save your changes.

Helper: You could also select the application type you would like to apply for automatic input.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.7 Virtual Server

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the Internet Assigned Numbers Authority (IANA), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. peer-to-peer applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server. The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN Configuration** section of this manual for more information on NAT.

Firetunnel 10 can also be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

Virtual Server (Port Forwarding)						
DMZ						
Enable DMZ Function		<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
DMZ IP Address Candidates		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>				
<input type="button" value="Apply"/>						
Port Forwarding Table						
Application	Protocol	External IP	External Port	Internal IP	Internal Port	
Create						

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.7.1 DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

Caution: Such Local computer exposure to the Internet may face a variety of security risks.

Virtual Server (Port Forwarding)	
DMZ	
Enable DMZ Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ IP Address Candidates	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<input type="button" value="Apply"/>	

Enable DMZ function:

Enable: Activates your router's DMZ function.

Disable: Default setting. Disables the DMZ function.

DMZ IP Address: Give a static IP address to the DMZ Host when the **Enable** radio button is selected. Be aware this IP will be exposed to the WAN/Internet.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

Select the **Apply** button to apply your changes.

4.4.7.2 Port Forwarding

Because NAT can act as a "natural" Internet firewall, your router protects your network from being accessed by outside users, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request is received, it will be forwarded to the corresponding internal server.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Port Forwarding Table						
Application	Protocol	External IP	External Port	Internal IP	Internal Port	
Create						

Click **Create** to add a new port forwarding rule. There are two port forwarding modes: **Port Range Mapping** and **Port Redirection**.

This function allows any incoming data addressed to a range of service port numbers (from the Internet/WAN Port) to be re-directed to a particular LAN private/internal IP address. This option gives you the ability to handle applications that use more than one port such as games and audio/video conferencing.

Virtual Server	
Add Forwarding Rule	
Application Helper	<input type="text"/>
Protocol	Any
External Port	1 ~ 65535
Redirect Port	1 ~ 65535
External IP Address Candidates	0 . 0 . 0 . 0
Internal IP Address Candidates	0 . 0 . 0 . 0
<input type="button" value="Apply"/>	

Application: User defined application name for the current rule.

Helper: You could also select the application type you would like to apply for automatic input.

Protocol type: please select protocol type

External Port: Enter the port number of the service that will be sent to the Internal IP address.

Redirect Port: Enter a new port number for the service that will be sent to the Internal IP address.

External Port Range: Enter the port number of the service that will be sent to the Internal IP address.

Internal IP Address: Enter the LAN server/host IP address that the service request from the Internet will be sent to.

Candidates: You can also select the Candidates which are referred from the ARP table for automatic input.

NOTE: You need to give your LAN server/host a static IP address for the Virtual

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Server to work properly.

Click **Apply** to save your changes.

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason, using specific Virtual Server entries just for the ports your application requires, instead of using DMZ is recommended.

4.4.8 Advanced


Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of Firetunnel 10. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Advanced
Static Route
Dynamic DNS
Device Management
IGMP
VLAN Bridge
Schedule

There are six items within the Advanced section: Static Route, Dynamic DNS and Device Management, IGMP, VLAN Bridge and Schedule.

4.4.8.1 Static Route

The static route settings enable the router to route IP packets to another network (subnet). The routing table stores the routing information so the router knows where to redirect the IP packets.

Static Route						
Static Route Table						
No.	Enable	Destination	Netmask	Gateway/Interface		
Create 						

Click on **Static Route** and then click **Create** to add a routing table.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Static Route							
Create Rule							
Rule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable						
Destination	0	0	0	0			
Netmask	0	0	0	0			
Gateway	0	0	0	0	Interface	LAN ▼	
Cost	0 ▼						
<div>Apply</div>							

Rule: Select Enable to activate this rule, Disable to deactivate this rule.

Destination: This is the destination subnet IP address.

Netmask: This is the subnet mask of the destination IP addresses based on above destination subnet IP.

Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop.

Click **Apply** to save your changes.

4.4.8.2 Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful when hosting servers via your WAN connection, so that anyone wishing to connect to you may use your domain name, rather than having to use a dynamic IP address that changes periodically. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. Click **Edit** in the Dynamic DNS Settings Table to set related parameters for a specific interface.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Dynamic DNS Settings	
Parameters	
Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	<input type="text" value="www.dyndns.org (dynamic)"/>
Wildcard	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Domain Name	<input type="text" value="yourdomain.dyndns.org"/>
Username	<input type="text" value="username"/>
Password	<input type="password" value="••••••••"/>
<input type="button" value="Apply"/>	

You will first need to register and establish an account with the Dynamic DNS provider using their website,

Example: DYNDNS

<http://www.dyndns.org/>

(Firetunnel 10 supports several Dynamic DNS providers , such as

www.zoneedit.com , www.orgdns.org , www.dhs.org , www.dyns.cx ,
www.3domain.hk , www.dyndns.org , www.3322.org) **[D10]**

Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The following fields will be activated and required:

Dynamic DNS Server: Select the DDNS service you have established an account with.

Wildcard: Select this check box to enable the DYNDNS Wildcard.

Domain Name: Enter your registered domain name for this service.

Username: Enter your registered user name for this service.

Password: Enter your registered password for this service.

Click **Apply** to save your changes.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.4.8.3 Device Management

The Device Management Advanced Configuration settings allow you to control your router's security options and device monitoring features.

Device Management			
Device Name			
Name	Firetunnel 10		
Web Server Settings			
* HTTP Port	80	(80 is default HTTP port)	
Management IP Address	0	0	0
Expire to auto-logout	300	seconds	
SNMP Access Control			
SNMP Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write		
* : This setting will become effective after you save to flash and restart the router.			
Apply			

Device Name

Name: Enter a name for this device.

Web Server Settings

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

Example: User A changes HTTP port number to 100, specifies their own IP address of 192.168.1.100 and sets the logout time to be 100 seconds. The router will only

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



allow User A access from the IP address 192.168.1.100 to logon to the Web GUI by typing: `http://192.168.1.254:100` in their web browser. After 100 seconds, the device will automatically logout User A.

SNMP Access Control

SNMP Function: Select **Enable** to activate this function, **Disable** to deactivate this function.

SNMP V1 and V2

Read Community: Input the string for Read community to match your SNMP software.

Write Community: Input the string for Write community to match your SNMP software.

Trap Community: Input the string for Trap community to match your SNMP software.

IP Address: Input the device IP address with SNMP software installed.

SNMP V3

Username: Input the Username for your SNMP software.


Password: Input the Password for your SNMP software.

Access Right: Select Read to allow your SNMP software to read the information.

Select Read/Write to allow your SNMP software to read and write the information.

4.4.8.4 IGMP

IGMP snooping and IGMP proxy are functions to be used for home users who will access IPTV applications.

<ul style="list-style-type: none"> Status Quick Start Configuration LAN WAN System Firewall VPN QoS Virtual Server Advanced Static Route Dynamic DNS Device Management IGMP VLAN Bridge Schedule Log & E-mail Alert Save Config to Flash 	IGMP	
	Parameters	
	IGMP Snooping	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	IGMP Proxy	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	 : This setting will become effective after you save to flash and restart the router.	
	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

IGMP Snooping: Please select enable or disable IGMP Snooping function.

IGMP Proxy: Please select enable or disable the IGMP Proxy function.

Click **Apply** to apply this function, and please note that the setting will become effective after you save to flash and restart the router.

4.4.8.5 VLAN Bridge

This section allows you to create VLAN group and specify the member.

<ul style="list-style-type: none"> Status Quick Start Configuration LAN WAN System Firewall VPN QoS Virtual Server Advanced Static Route Dynamic DNS Device Management IGMP VLAN Bridge Schedule Log & E-mail Alert Save Config to Flash 	VLAN Bridge					
	VLAN Mode					
	VLAN Mode				<input type="radio"/> Disable	
					<input checked="" type="radio"/> Bridge Mode	
					<input type="radio"/> Tagging Mode	
	<input type="button" value="Apply"/>					
	VLAN Bridge Table					
	Name	VLAN ID	Tagged Ports	UnTagged Ports	Edit	Delete
	Default	1		P1,P2,P3,P4,P5,P6,P7,P8	Edit	
	Create					

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



VLAN Mode: Select **Disable** to disable VLAN mode, select **Bridge Mode** to use VLAN Bridge function and select **Tagging Mode** to use the VLAN Tagging mode option.

Click **Create** to create another VLAN group.

Create VLAN	
Parameters	
VLAN Name	<input type="text"/> VLAN ID <input type="text" value="0"/> (1~4000)
Tagged Member Port(s)	<input type="checkbox"/> WAN <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5 <input type="checkbox"/> P6 <input type="checkbox"/> P7 <input type="checkbox"/> P8
Untagged Member Port(s)	<input type="checkbox"/> WAN <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P5 <input type="checkbox"/> P6 <input type="checkbox"/> P7 <input type="checkbox"/> P8
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>	

VLAN Name: Please input VLAN name of this rule.

VLAN ID: Please input VLAN ID that will be used for Tagged member port(s).

Tagged Member port(s): Please check the interface that you would like to use in this VLAN ID group.

Untagged Member port(s): Please check the interface that you would like to use in this VLAN ID group.

Click **Apply** to add this rule.

4.4.8.6 Schedule

You can configure the Firtunnel 10 WAN connection schedule here.

Status	Schedule						
Quick Start	Schedule Table						
Configuration	<table border="1"><thead><tr><th>Name</th><th>Day in a week</th><th>Time</th></tr></thead><tbody><tr><td>**Always</td><td>Sun. Mon. Tue. Wed. Thu. Fri. Sat.</td><td>From 00:00 To 24:00</td></tr></tbody></table>	Name	Day in a week	Time	**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00
Name	Day in a week	Time					
**Always	Sun. Mon. Tue. Wed. Thu. Fri. Sat.	From 00:00 To 24:00					
LAN	<input type="button" value="Create"/>						
WAN							
System							
Firewall							
VPN							
QoS							
Virtual Server							
Advanced							
Static Route							
Dynamic DNS							
Device Management							
IGMP							
VLAN Bridge							
Schedule							
Log & E-mail Alert							
Save Config to Flash							

Click **Create** to configure the details.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Schedule	
Create	
Name	<input type="text"/>
Day	<input checked="" type="checkbox"/> Sun. <input checked="" type="checkbox"/> Mon. <input checked="" type="checkbox"/> Tue. <input checked="" type="checkbox"/> Wed. <input checked="" type="checkbox"/> Thu. <input checked="" type="checkbox"/> Fri. <input checked="" type="checkbox"/> Sat.
Start Time	08 : 00
End Time	18 : 00
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Name: Enter the schedule's name you want to create.

Day: Check the box of Firetunnel 10 working day.

Start Time: Set the connection start time.

End Time: Set the connection end time.

Click the **Apply** to complete the configuration or **Cancel** to return.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

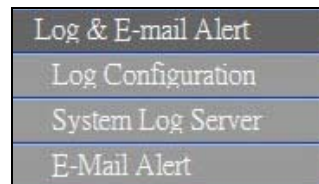
EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.5 Log & E-mail Alert

You can configure the Log Statistics and E-mail Alert options under this menu.

There're three section, Log Configuration, System Log Server and E-mail Alert.



4.5.1 Log Configuration

The Firetunnel 10 incorporates industry-standard alert protocols for capturing network activity information. The information can then be written to a log, sent to an external server, or to a selected E-mail address.

Status	Log Configuration			
Quick Start	Parameters			
Configuration	Categories	System Log	Syslog Server ▾	E-mail Alert ▾
Log & E-mail Alert	System Maintenance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Log Configuration	System Errors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Log Server	Access Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-Mail Alert	Packet Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Save Config to Flash	LAN MAC Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	URL Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Intrusion Detection	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Call Data Record	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	PPP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Remote Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	IPSEC	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="button" value="Apply"/>			

Select **System/SSL VPN Log** to capture to a log.

Select **Syslog Server** to capture and send to a specified external server. Select **Email Alert** to send information log to a pre-specified E-mail account.

4.5.2 System Log Server

System Log Server	
Parameters	
Send Log To Remote Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Log Server IP Address	192 . 168 . 1 . 1
<input type="button" value="Apply"/>	

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



This function allows Firetunnel 10 to send system logs to an external Syslog Server. Syslog is an industry-standard protocol used to capture information about network activity. To enable this function, select the **Enable** radio button and enter your Syslog server IP address in the **Log Server IP Address** field. Click **Apply** to save your changes.

To disable this feature, simply select the **Disable** radio button and click **Apply**.

4.5.3 E-mail Alert

E-Mail Alert	
Parameters	
E-Mail Alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Recipient's E-Mail Address	<input type="text"/>
Sender's E-Mail Address	<input type="text"/>
SMTP Mail Server	<input type="text"/>
Mail Server Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="password"/>
Alert via E-Mail when	<input type="radio"/> Immediately
	<input type="radio"/> Hourly
	<input type="radio"/> Daily <input type="text" value="12:00"/> <input checked="" type="radio"/> A.M. <input type="radio"/> P.M.
	<input type="radio"/> Weekly <input type="text" value="Sunday"/> <input type="text"/>
	<input checked="" type="radio"/> When log is full
<input type="button" value="Apply"/>	

The Email Alert function allows a log of security-related events (such as System Log and IPSec Log) to be sent to a specified email address.

Email Alert: You may enable or disable this function by selecting the appropriate radio button.

Recipient's Email Address: Enter the email address where you wish the alert logs to be sent.

SMTP Mail Server: Enter your email account's outgoing mail server. It may be an IP address or a domain name.

Sender's Email Address: Enter the email address where you wish the alert logs to be

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



sent by which address.

Mail Server Login: some SMTP servers may request users to login before serving.

Select **Enable** to activate SMTP server login function, **disable** to deactivate.

Username: Input the SMTP server's username.

Password: Input the SMTP server's password.

Alert via Email when: Select the frequency of each email update. Choose one of the five options:

Immediately: The router will send an alert immediately.

Hourly: The router will send an alert once every hour.

Daily: The router will send an alert once a day. The exact time can be specified using the pull down menu.

Weekly: The router will send an alert once a week.

When log is full: The router will send an alert only when the log is full.

4.6 Save Configuration To Flash

After changing the router's configuration settings, you must save all of the configuration parameters to flash memory to avoid them being lost after turning off or resetting your router. Click **Apply** to write your new configuration to flash memory.

Save Config to Flash
Please confirm that you wish to save the configuration.
<i>There will be a delay while saving as configuration information is written to FLASH chips.</i>
<input type="button" value="Apply"/>

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



4.7 Logout

To exit the router's web interface, click **Logout**. Please ensure that you have saved your configuration settings before you logout.



Be aware that the router is restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can access the page after a user-defined period (5 minutes by default). You can modify this value using the **Advanced > Device Management** section of the Web Configuration Interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

5.1 Basic Functionality

This section deals with issues regarding your Firetunnel 10's basic functions.

5.1.1 Router Won't Turn On

If the Power and other LEDs fail to light when your Firetunnel 10 is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by Black Box for this product.

If the error persists, you may have a hardware problem, and should contact technical support.

5.1.2 LEDs Never Turn Off

When your Firetunnel 10 is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there may be a hardware problem.

If all LEDs are still on one minute after powering up:

- Cycle the power to see if the router recovers.
- Clear the configuration to factory defaults.

If the error persists, you may have a hardware problem, and should contact technical support.

5.1.3 LAN or Internet Port Not On

If either the LAN LEDs or Internet LED does not light when the Ethernet connection is made, check the following:

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



- Make sure each Ethernet cable connection is secure at the firewall and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable. When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

5.1.4 Forgot My Password

Try entering the default User Name and Password:

User Name: admin

Password: admin

Please note that both the User Name and Password are case-sensitive.

If this fails, you can restore your Firetunnel 10 to its factory default settings by holding the Reset button on the back of your router until the Status LED begins to blink. Then enter the default User Name and Password to access your router.

5.2 LAN Interface

Refer to this section for issues relating to Firetunnel 10's LAN Interface.

5.2.1 Can't Access Firetunnel 10 from the LAN

If there is no response from Firetunnel 10 from the LAN:

- Check your Ethernet cable types and each connection.
- Make sure the computer's Ethernet adapter is installed and functioning properly.

If the error persists, you may have a hardware problem, and should contact technical support.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



5.2.2 Can't Ping Any PC on the LAN

If PCs connected to the LAN cannot be pinged:

- Check the 10/100 LAN LEDs on Firetunnel 10's front panel. One of these LEDs should be on. If they are both off, check the cables between Firetunnel 10 and the hub or PC.
- Check the corresponding LAN LEDs on your PC's Ethernet device are on.
- Make sure that driver software for your PC's Ethernet adapter and TCP/IP software is correctly installed and configured on your PC.
- Verify the IP address and the subnet mask of Firetunnel 10 and the computers are on the same subnet.

5.2.3 Can't Access Web Configuration Interface

If you are having trouble accessing Firetunnel 10's Web Configuration Interface from a PC connected to the network:

- Check the connection between the PC and the router.
- Make sure your PC's IP address is on the same subnet as the router.
- If your Firetunnel 10's IP address has changed and you don't know the current IP address, reset the router to factory defaults by holding the Reset button on the back of your router for 6 seconds. This will reset the router's IP address to 192.168.1.254.
- Check to see if your browser had Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to ensure that the Java applet is loaded.
- Try closing the browser and re-launching it.
- Make sure you are using the correct **User Name and Password**. User Names and Passwords are case-sensitive, so make sure that **CAPS LOCK** is not on when entering this information.
- Try clearing your browser's cache.

1. With Internet Explorer, click **Tools > Internet Options**.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

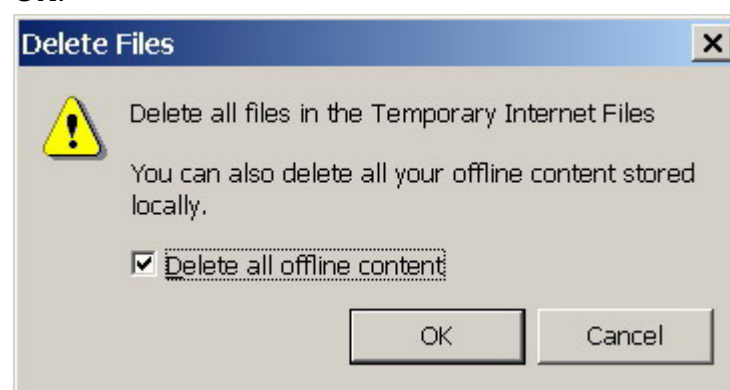
EU, Africa, Asia, South America, Australia: www.blackbox.eu



2. Under the **General** tab, click **Delete Files**.



3. Make sure that the **Delete All Offline Content** checkbox is checked, and click **OK**.



4. Click **OK** under **Internet Options** to close the dialogue.

- In Windows, type **arp -d** at the command prompt to clear you computer's ARP table.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



5.2.3.1 Pop-up Windows

To use the Web Configuration Interface, you need to disable pop-up blocking. You can either disable pop-up blocking, which is enabled by default in Windows XP Service Pack 2, or create an exception for your Firetunnel 10's IP address.

Disabling All Pop-ups

In Internet Explorer, select **Tools > Pop-up Blocker** and select **Turn Off Pop-up Blocker**.

[D12]

You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab of the **Internet Options** dialogue.

1. In Internet Explorer, select **Tools > Internet Options**.
2. Under the **Privacy** tab, clear the **Block pop-ups** checkbox and click **Apply** to save your changes.

Enabling Pop-up Blockers with Exceptions

If you only want to allow pop-up windows with your Firetunnel 10:

1. In Internet Explorer, select **Tools > Internet Options**.
2. Under the **Privacy** tab, click **Settings** to open the **Pop-up Blocker Settings** dialogue. [D13]
3. Enter the IP address of your router.
4. Click **Add** to add the IP address to the list of **Allowed sites**.
5. Click **Close** to return to the **Privacy** tab of the **Internet Options** dialogue.
6. Click **Apply** to save your changes.

5.2.3.2 Javascripts

If the Web Configuration Interface is not displaying properly in your browser, check to make sure that JavaScripts are allowed.

1. In Internet Explorer, click **Tools > Internet Options**.

Black Box Corporation

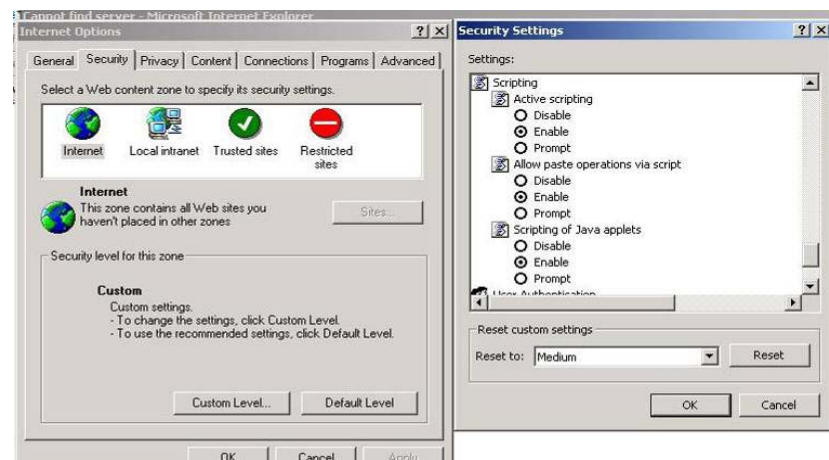
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2. Under the **Security** tab, click **Custom Level**.



3. Under **Scripting**, check to see if **Active scripting** is set to **Enable**.

4. Ensure that **Scripting of Java applets** is set to **Enable**.

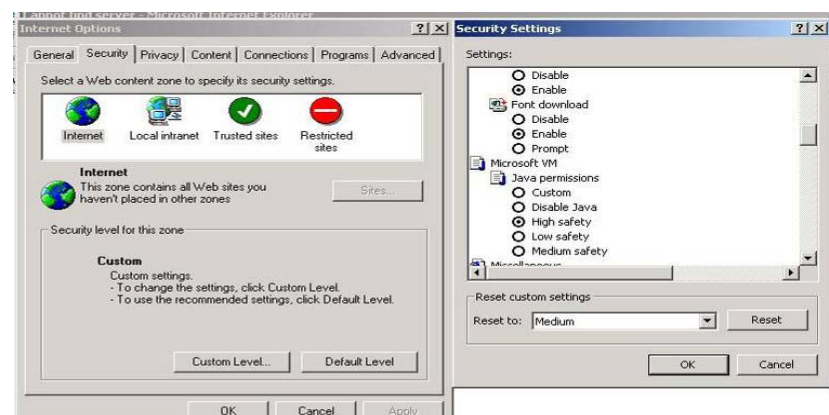
5. Click **OK** to close the dialogue.

5.2.3.3 Java Permissions

The following Java Permissions should also be given for the Web Configuration Interface to display properly:

1. In Internet Explorer, click **Tools > Internet Options**.

2. Under the **Security** tab, click **Custom Level**.



3. Under **Microsoft VM***, make sure that a safety level for **Java permissions** is selected.

4. Click **OK** to close the dialogue.

NOTE: If Java from Sun Microsystems is installed, scroll down to **Java (Sun)** and ensure that the checkbox is filled.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



5.3 WAN Interface

If you are having problems with the WAN Interface, refer to the tips below.

5.3.1 Can't Get WAN IP Address from the ISP

If the WAN IP address cannot be obtained from the ISP:

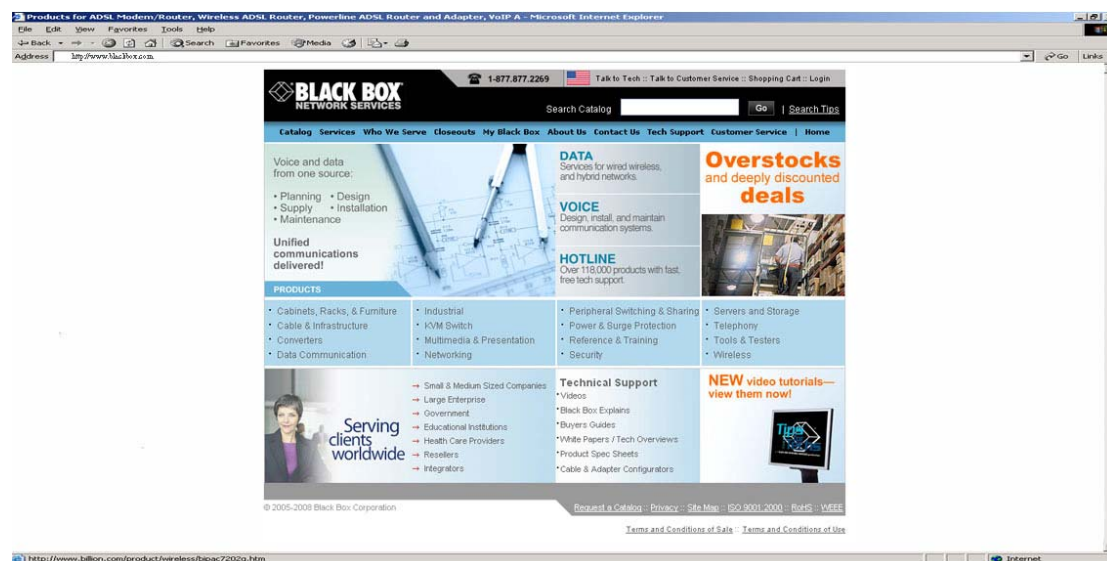
- If you are using PPPoE or **[S14]** PPTP, you will need a user name and password. Ensure that you have entered the correct **Service Type**, **User Name**, and **Password**. Note that user names and passwords are case-sensitive.
- If your ISP requires MAC address authentication, clone the MAC address from your PC on the LAN as Firetunnel 10's WAN MAC address.
- If your ISP requires host name authentication, configure your PC's name as Firetunnel 10's system name.

5.4 ISP Connection

Unless you have been assigned a static IP address by your ISP, your Firetunnel 10 will need to request an IP address from the ISP in order to access the Internet. If your Firetunnel 10 is unable to access the Internet, first determine if your router is able to obtain a WAN IP address from the ISP.

To check the WAN IP address:

1. Open your browser and choose an external site (i.e. www.BlackBox.com).



Black Box Corporation

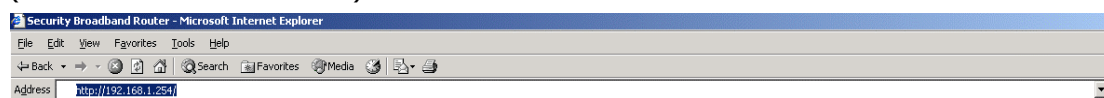
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



2. Access the Web Configuration Interface by entering your router's IP address (default is 192.168.1.254).



3. The WAN IP Status is displayed on the first page.

A screenshot of the WAN IP Status page in the router's web interface. On the left is a sidebar menu with options like Status, ARP Table, Routing Table, Session Table, DHCP Table, IPsec Status, PPTP Status, System Status, System Log, Quick Start, Configuration, Log & E-mail Alert, and Save Config to Flash. The main content area is titled "Status" and includes a "Refresh" button. It is divided into sections: "Device Information" (showing Device Name: Firetunnel 10, System Up Time: 3:4:38:16, Current Time: Thu Aug 4 16:37:58 2005, Private LAN MAC Address: 00:04:ed:11:c7:09, Public WAN MAC Address: 00:04:ed:11:c7:0a, Firmware Version: 2.02f, Home URL: BlockBox), "LAN" (showing IP Address: 192.168.1.254, Netmask: 255.255.255.0, DHCP server: Enabled), and "WAN" (showing Connection Method: No Link, IP Address, Netmask, Gateway, DNS Server, Up Time).

4. Check to see that the WAN port is properly connected to the ISP. If a **Connected by (x)** where **(x)** is your connection method is not shown, your router has not successfully obtained an IP address from your ISP.

If an IP address cannot be obtained:

1. Turn off the power to your cable or DSL modem.
2. Turn off the power to your Firetunnel 10.
3. Wait five minutes and power on your cable or DSL modem.
4. When the modem has finished synchronizing with the ISP (generally shown by LEDs on the modem), turn on the power to your router.

If an IP address still cannot be obtained:

- Your ISP may require a login program. Consult your ISP whether they require PPPoE or some other type of login.
- If your ISP requires a login, check to see that your User Name and Password are entered correctly.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



- Your ISP may check for your PC's host name. Assign the PC Host Name of your ISP account as your PC's host name on the router.
- Your ISP may check for your PC's MAC address. Either inform your ISP that you have purchased a new network device and ask them to use your router's MAC address, or configure your router to spoof your PC's MAC address.

If an IP address can be obtained, but your PC cannot load any web pages from the Internet:

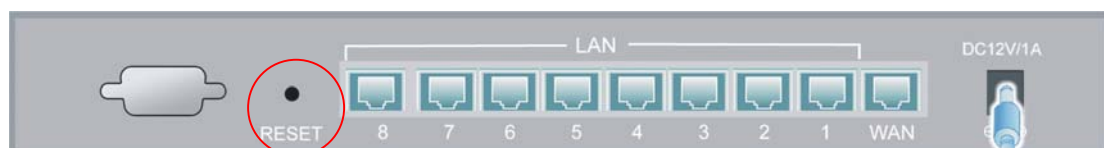
- Your PC may not recognize DNS server addresses. Configure your PC manually with DNS addresses.
- Your PC may not have the router correctly configured as its TCP/IP gateway.

5.5 Problems with Date and Time

If the date and time is not being displayed correctly, be sure to set it for your Firetunnel 10 via the Web Configuration Interface. Both date and time can be found under **Configuration > System > Time Zone**.

5.6 Restoring Factory Defaults

You can restore your Firetunnel 10 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. This will reset your router to its default settings.



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Appendix A: Product Specifications

A.1 Firetunnel 10 Product Specifications



Virtual Private Network

- IPSec VPN, supports up to 10 IPSec tunnels
- IPSec VPN performance is up to 20 Mbps
- PPTP VPN, support up to 4 PPTP tunnels
- PPTP VPN performance is up to 10 Mbps
- Manual key, Internet Key Exchange (IKE) authentication and Key Management
- Authentication (MD5 / SHA-1)
- DES/3DES encryption
- AES 128/192/256 encryption
- IP Authentication Header (AH)
- IP Encapsulating Security Payload (ESP)
- Dynamic VPN (FQDN) support
- Supports remote access and office-to-office IPSec Connections

Firewall

- Stateful Packet Inspection (SPI) and Denial of Service (DoS) prevention
- Packet filter un-permitted inbound (WAN)/Inbound
- (LAN) Internet access by IP address, port number and packet type
- Email alert and logs of attack
- Intrusion detection

Content Filtering

- URL Filter settings prevent user access to certain sites on the Internet
- Java Applet/Active X/Cookie Blocking

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



Quality of Service Control

- Supports DiffServ approach
- Traffic prioritization and bandwidth management based-on IP protocol, port number and IP or MAC[S15] address

Web-Based Management

- Easy-to-use WEB interface
- Firmware upgradeable[D16] via WEB interface
- Local and remote management via HTTP & HTTPS

Network Protocols and Features

- Web Diagnostics
- System Logs
- PPPoE, PPTP, Big Pond and DHCP client connections to the ISP
- NAT, static routing and RIP-2
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- DHCP Server
- NTP

Physical Interface

Ethernet WAN 1 ports (10/100 Base-T), support Auto- Crossover (MDI/MDIX)

Ethernet LAN 8 ports (10/100 Base-T) switch, support Auto- Crossover (MDI/MDIX)

Physical Specifications

Dimensions: 18.98" x 6.54" x 1.77" (482mm x 166 mm x 45mm, with Bracket)

9.84" x 6.54" x 1.38" (250mm x 166 mm x 35mm, non Bracket)

Power Requirement

Input: 12VDC, 1A

Operating Environment

- Operating temperature: 0 ~ 40 degrees Celsius
- Storage temperature: -20 ~ 70 degrees Celsius
- Humidity: 20 ~ 95% non-condensing

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

Appendix B: FCC Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply within the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice:

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

Appendix C: Network, Routing, and Firewall Basics

C.1 Network Basics

C.1.1 IP Addresses

With the number of TCP/IP networks interconnected across the globe, ensuring that transmitted data reaches the correct destination requires each computer on the Internet has a unique identifier. This identifier is known as the IP address. The Internet Protocol (IP) uses a 32-bit address structure, and the address is usually written in dot notation.

A typical IP address looks like this:

198.25.12.8

The 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, while the second part identifies the host node or station on the network. How the address is divided depends on the address range and the application.

The five standard IP address classes each have different methods to determine the network and host sections of the address, which makes multiple hosts on a network possible. TCP/IP software identifies each address class by reading a unique bit pattern that precedes each address type. Once the address class has been recognized, the software can then correctly determine the addresses' host section. With this structure, IP addresses can uniquely identify each network and node.

C.1.1.1 Netmask

With each address class, the size of the two subdivided parts (network address and host address) is implied by the class. A net mask associated with an IP address can also express this partitioning. A net mask 32-bit quantity yields the network address when combined with an IP address. As an example, the net masks for Class A, B, and C are 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

Instead of dotted-decimal notation, the net mask can also be written in terms of the number of ones from the left. This number is added to the IP address, following a

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



back slash (/). For example, a typical Class C address could be written as 192.168.234.245/24, which means that the net mask is 24 ones followed by 8 zeros. (11111111 11111111 11111111 00000000).

C.1.1.2 Subnet Addressing

Subnet addressing enables the split of one IP network address into multiple physical networks. These smaller networks are called subnetworks, and these subnetworks can make efficient use of each address when compared to needing a different network number at each end of a routed link. This technique is especially useful in smaller network environments, such as small office LANs.

A Class B address provides 16 bits of node numbers, which enable 65,536 nodes. Since most organizations don't require such a large number of nodes, the free bits can be reassigned with subnet addressing.

Multiple Class C addresses can be made from a Class B address. For example, the IP address of 172.20.0.0 allows eight extra bits to use as a subnet address, since node addresses are limited to a maximum of 255. The IP address of 172.20.52.212 would be read as IP network address 172.20, subnet number 52, and node number 212.

Besides extending the number of available addresses, this technique also allows a network manager to design an address scheme for the network by using different subnets. This can be useful when trying to distinguish other geographical locations in the network or other departments in the organization.

C.1.1.3 Private IP Addresses

When isolated from the Internet, the hosts on your local network may be assigned IP addresses with no conflicts. However, the Internet Assigned Numbers Authority (IANA) has reserved several blocks of IP addresses for private networks. These include:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.16.255.255

192.168.0.0 - 192.168.255.255

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



When assigning IP addresses to your private network, be sure to use IP addresses from these ranges.

C.1.2 Network Address Translation (NAT)

Traditionally, multiple PCs that needed simultaneous Internet access also required a range of IP addresses from the Internet Service Provider (ISP). Not only was this method very costly, but the number of available IP addresses for PCs is limited. Instead, Firetunnel 10 uses a type of address sharing called Network Address Translation to grant Internet access to several PCs on the same network through the same Internet account. This method translates internal IP addresses to a single address that is unique on the Internet. This unique address can either be fixed or dynamic, depending on the type of Internet account, and the internal LAN IP addresses may also be either private or registered addresses[D17].

NAT also offers firewall-like protection to your network, since internal LAN addresses are shielded from the public Internet. All incoming traffic to the public IP address is handled by the router, which means added security for your network from intruders. If a particular PC on your LAN requires access from outside PCs, you can use port forwarding to accomplish this. For information on how to configure port forwarding on Firetunnel 10, refer to the **Virtual Server** section of **Chapter 4: Router Configuration**.

C.1.3 Dynamic Host Configuration Protocol (DHCP)

If the PCs on a LAN require access to the Internet, each PC must be configured with an IP address, a gateway address, and one or more DNS server addresses. Rather than configuring each PC manually, you can instead configure a network device to act as a Dynamic Host Configuration Protocol (DHCP) server. PCs on the network can automatically obtain IP addresses from a list of addresses stored on the DHCP server. In addition, other information such as gateway and DNS address can also be assigned with a DHCP server. When connecting to the ISP, Firetunnel 10 also functions as a DHCP client. Firetunnel 10 can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.

C.2 Router Basics

C.2.1 What is a Router?

A router is a device that forwards data packets along networks. A router is connected to at least two networks. Usually, this is a LAN and a WAN that is connected to an ISP network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols to communicate with each other and configure the best route between any two hosts.

Routers can vary in performance and scale, the types of physical WAN connection they support, and the number of routing protocols supported. Firetunnel 10 offers a convenient and powerful way for small-to-medium businesses to connect their networks.

C.2.2 Why use a Router?

While large bandwidth can easily and inexpensively be provided in a LAN, having high bandwidth between a LAN and the Internet can be prohibitively expensive. Because of this, Internet access is usually done through a slower WAN link, such as a cable or DSL modem. To efficiently use this slower connection, a router acts as a mechanism for selecting and transmitting data meant for the Internet. By using a router, organizations can enjoy relatively inexpensive Internet access, while maintaining a high-speed local area network.

C.2.3 Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing table information. Routers periodically update each other with RIP, changing their routing tables when necessary.

Firetunnel 10 supports the RIP protocol. RIP also supports subnet and multicast protocols. RIP is not required for most home applications.

C.3 Firewall Basics

C.3.1 What is a Firewall?

Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. With the functionality of a NAT router, the firewall adds features that deal with outside Internet intrusion and attacks. When an attack or intrusion is detected, the firewall can be configured to log the intrusion attempt, and can also notify the administrator of the incident. With this information, the administrator can work with the ISP to take action against the hacker. Against some types of attacks, the firewall can discard intruder packets, thereby fending off the hacker from the private network.

C.3.1.1 Stateful Packet Inspection

Firetunnel 10 uses Stateful Packet Inspection (SPI) to protect your network from intrusions and attacks. Unlike less sophisticated Internet sharing routers, SPI ensures secure firewall filtering by intercepting incoming packets at the network layer, and analyzing them for state-related information that is associated with all network connections. User-level applications such as Web browsers and FTP can make complex network traffic patterns, which Firetunnel 10 analyzes by looking at groups of connection states.

All state information is stored in a central cache. Traffic passing through the firewall is analyzed against these states, and then is either allowed to pass through or rejected.

C.3.1.2 Denial of Service (DoS) Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

C.3.2 Why Use a Firewall?

With a LAN connected to the Internet through a router, there is a chance for hackers to access or disrupt your network. A simple NAT router provides a basic level of protection by shielding your network from the outside Internet. Still, there are ways for more dedicated hackers to either obtain information about your network or disrupt your network's Internet access. Your Firetunnel 10 provides an extra level of protection from such attacks with its built-in firewall.

Appendix D: Virtual Private Networking

D.1 What is a VPN?

A Virtual Private Network (VPN) is a shared network where private data is segmented from other traffic so that only the intended recipient has access. It allows organizations to securely transmit data over a public medium like the Internet. VPNs utilize tunnels, which allow data to be safely delivered to the intended recipient.

Because private networks lack data security, IPSec-based VPNs employ encryption technologies that protect a private network from data theft or tampering. These private networks can be implemented over any type of IP network, which allows for excellent flexibility.

D.1.1 VPN Applications

VPNs are traditionally used three ways:

- Extranets: Extranets are secure connections between two or more organizations. IPSec-based VPNs are ideal for extranet connections, as they can be quickly and inexpensively installed. Extranets are often used to securely share a company's information with suppliers, vendors, customers, or other businesses.
- Intranets: Intranets are private networks that connect an organization's locations together. These locations range from a headquarter, to branch offices, to a remote employee's home. Intranets are often used for email and for sharing applications and files. A firewall protects Intranets from unauthorized access.
- Remote Access: Remote access enables mobile workers to access email and business applications. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.

D.2 What is IPSec?

Internet Protocol Security (IPSec) is a set of protocols and algorithms that provide data authentication, integrity, and confidentiality as data is transferred across IP networks. IPSec provides data security at the IP packet level, and protects against possible security risks by protecting data. IPSec is widely used to establish VPNs.

There are three major functions of IPSec:

- Confidentiality: Conceals data through encryption.
- Integrity: Ensures that contents did not change in transit.
- Authentication: Verifies that packets received are actually from the claimed sender.

D.2.1 IPSec Security Components

IPSec contains three major components:

- Authentication Header (AH): Provides authentication and integrity.
- Encapsulating Security Payload (ESP): Provides confidentiality, authentication, and integrity.
- Internet Key Exchange (IKE): Provides key management and Security Association (SA) management.

These components are discussed below.

D.2.1.1 Authentication Header (AH)

The Authentication Header (AH) is a protocol that provides authentication and integrity, protecting data from tampering. It provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.

The AH can also protect packets from unauthorized re-transmission with anti-replay functionality. The presence of the AH header allows us to verify the integrity of the message, but doesn't encrypt it. Thus, AH provides authentication but not privacy. ESP protects data confidentiality. Both AH and ESP can be used together for added protection.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



A typical AH packet looks like this:

Next Header	Payload Length	Reserved
SPI		
Sequence Number		
Authentication Data		

D.2.1.2 Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) provides privacy for data through encryption. An encryption algorithm combines the data with a key to encrypt it. It then repackages the data using a special format, and transmits it to the destination. The receiver then decrypts the data using the same algorithm. ESP is usually used with AH to provide added data security.

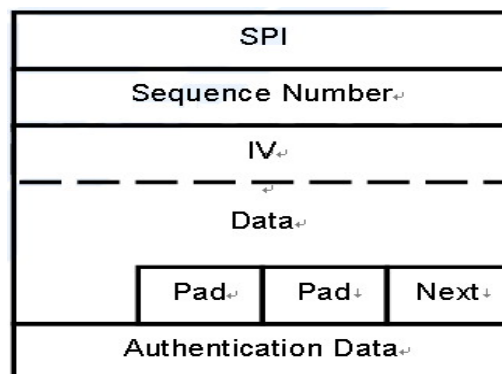
ESP divides its fields into three components...

ESP Header: Placed before encrypted data, the ESP Header contains the SPI and Sequence Number. Its placement depends on whether ESP is used in transport mode or tunnel mode.

ESP Trailer: Placed after the encrypted data, the ESP Trailer contains padding that is used to align the encrypted data.

ESP Authentication Data: This contains an Integrity Check Value (ICV) for when ESP's optional authentication feature is used.

ESP provides authentication, integrity, and confidentiality, which provides data content protection, and protects against data tampering. A typical ESP packet looks like this:



D.2.1.3 Security Associations (SA)

Security Associations are a one-way relationships between sender and receiver that specify IPsec-related parameters. They provide data protection by using the defined IPsec protocols, and allow organizations to control according to the security policy in effect, which resources may communicate securely.

SA is identified by 3 parameters:

- Security Parameters Index (SPI), a locally unique value
- Destination IP Address
- Security Protocol: (AH or ESP, but not both)

There are several other parameters associated with an SA that are stored in a Security Association database.

D.2.2 IPsec Modes

To exchange data between different types of VPNs, IPsec provides two major modes:

- Tunnel Mode :

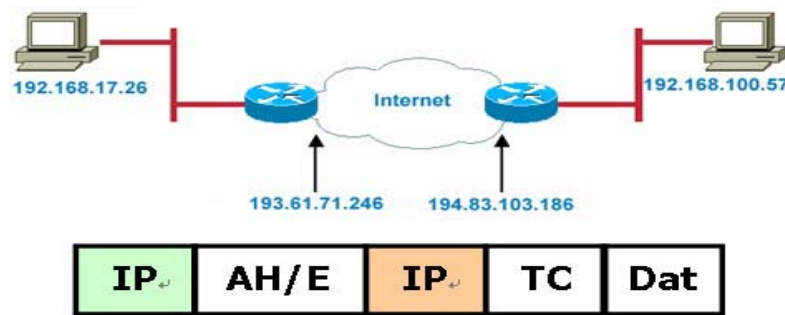
This mode is used for host-to-host security. Protection extends to the payload of IP data, and the IP addresses of the hosts must be public IP addresses.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

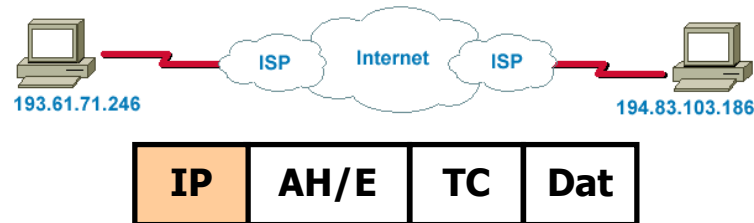
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Transport Mode :

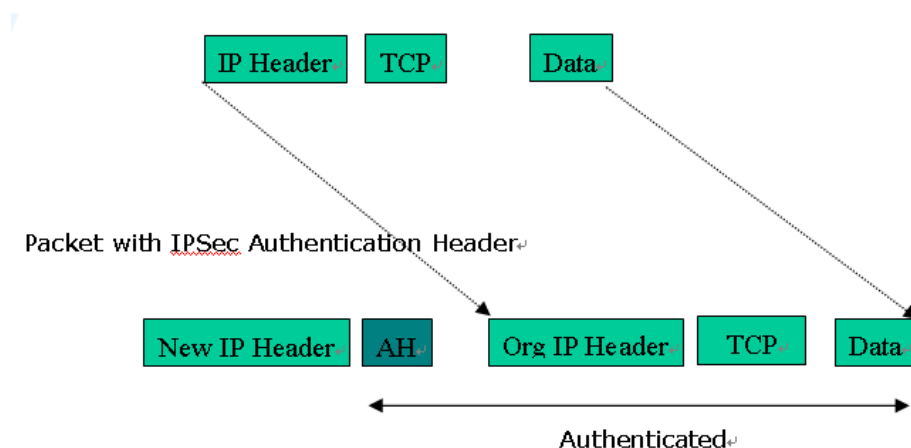
- This mode is used to provide data security between two networks. It provides protection for the entire IP packet and is sent by adding an outer IP header corresponding to the two tunnel end-points. Since tunnel mode hides the original IP header, it provides security of the networks with private IP address space.



D.2.3 Tunnel Mode AH

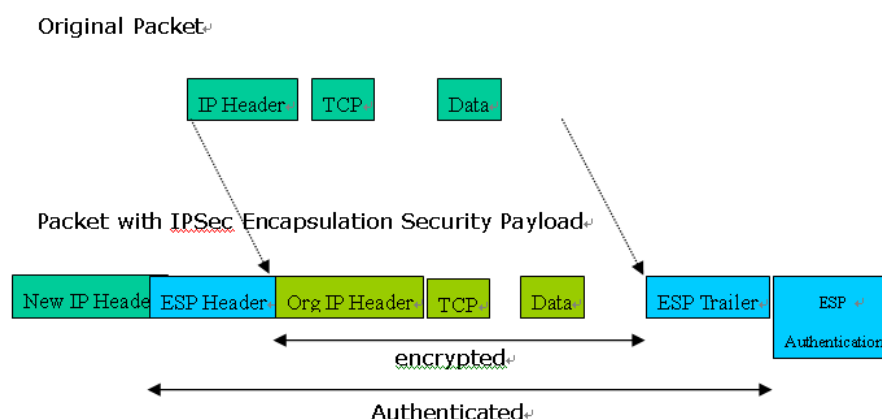
AH is typically applied to a data packet in the following manner:

Original Packet:



D.2.4 Tunnel Mode ESP

Here is an example of a packet with ESP applied:



D.2.5 Internet Key Exchange (IKE)

Before either AH or ESP can be used, it is necessary for the two communication devices to exchange a secret key that the security protocols themselves will use. To do this, IPsec uses Internet Key Exchange (IKE) as a primary support protocol. IKE facilitates and automates the SA setup, and exchanges keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it. These keys need to be re-created or refreshed frequently so that the parties can communicate securely with each other. Refreshing keys on a regular basis ensures data confidentiality.

There are two phases to this process. Phase I deals with the negotiation and management of IKE and IPsec parameters. This phase can be carried out in either one of two modes: Main Mode or Aggressive Mode. Main mode utilizes three message pairs that negotiate IKE parameters, establish a shared secret and derive session keys, and exchange and provide identities, retroactively authenticating the information sent. This method is very secure, but when using the pre-shared key method for authentication, it is possible to use IDs other than the packets's IP addresses. Aggressive mode reduces this process to three messages, but parameter negotiation is limited, identity protection is lacking except when using public key encryption, and is more vulnerable to Denial of Service attacks.

Phase II, known as Quick Mode, establishes symmetrical IPsec Security Associations for both AH and ESP. It does this by negotiating IPsec parameters, exchange nonces to derive session keys from the IKE shared secret, exchange DH values to generate a new key, and identify which traffic this SA bundle will protect using selectors (IDi and IDr payloads).

Black Box Corporation

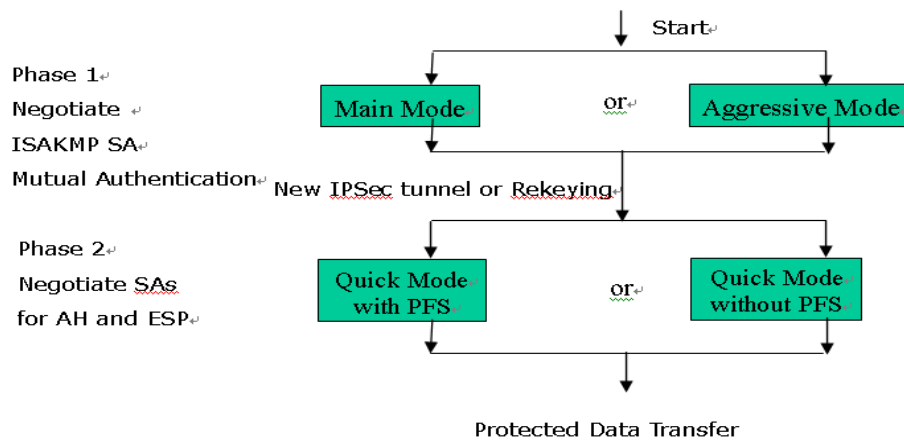
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



The following is an illustration on how data is handled with IKE:



Appendix E: IPSec Logs and Events

E.1 IPSec Log Event Categories

There are three major categories of IPSec Log Events for your Firetunnel 10. These include:

1. IKE Negotiate Packet Messages
2. Rejected IKE Messages
3. IKE Negotiated Status Messages

The table in the following section lists the different events of each category, and provides a detailed explanation of each.

E.2 IPSec Log Event Table

IKE Negotiate Packet Messages	
Log Event	Explanation
Send Main mode initial message of ISAKMP	Sending the first initial message of main mode (phase I). Done to exchange encryption algorithm, hash algorithm, and authentication method.
Send Aggressive mode initial message of ISAKMP	Sending the first message of aggressive mode (phase I).
Received Main mode initial message of ISAKMP	Received the first message of main mode.
Send Main mode first response message of ISAKMP	Sending the first response message of main mode. Done to exchange encryption algorithm, hash algorithm, and authentication method.
Received Main mode first response message of ISAKMP	Received the first response message of main mode. Done to exchange encryption algorithm, hash algorithm, and authentication method.
Send Main mode second	Sending the second message of main mode. Done to

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

message of ISAKMP	exchange key values.
Received Main mode second message of ISAKMP	Received the second message of main mode. Done to exchange key values.
Send Main mode second response message of ISAKMP	Sending the main mode second response message. Done to exchange key values.
Received Main mode second response message of ISAKMP	Received the main mode second response message. Done to exchange key values.
Send Main mode third message of ISAKMP	Sending the third message of main mode. Done for authentication.
Received Main mode third message of ISAKMP	Received the third message of main mode. Done for authentication.
Send Main mode third response message of ISAKMP	Sending the third response message of main mode. Done for authentication.\
Received Main mode third response message of ISAKMP	Received the third response message of main mode. Done for authentication.
Received Aggressive mode initial ISAKMP Message	Received the first message of aggressive mode.
Send Aggressive mode first response message of ISAKMP	Sending the first response message of aggressive mode. Done to exchange proposal and key values.
Received Aggressive mode first response message of ISAKMP	Received the first response message of aggressive mode. Done to exchange proposal and key values.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

Send Aggressive mode second message of ISAKMP	Sending the second message of aggressive mode. Done to exchange proposal and key values.
Received Aggressive mode second ISAKP Message	Received the second message of aggressive mode. Done to exchange proposal and key values.
Send Quick mode initial message	Sending the first message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Received Quick mode initial message	Received the first message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Send Quick mode first response message	Sending the first response message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Received Quick mode first response message	Received the first response message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Send Quick mode second message	Sending the second message of quick mode (Phase II).
Received Quick mode second message	Received the second message of quick mode (Phase II).
ISAKMP IKE Packet	Indicates IKE packet.
ISAKMP Information	Indicates Information packet.
ISAKMP Quick Mode	Indicates quick mode packet.
Rejected IKE Messages	
NO PROPOSAL CHOSEN: No acceptable Oakley Transform	
NO PROPOSAL CHOSEN: No acceptable Proposal in IPsec SA	

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

NO PROPOSAL CHOSEN: PFS is required in Quick Initial SA.
NO PROPOSAL CHOSEN: PFS is not required in Quick Initial SA.
NO PROPOSAL CHOSEN: Initial Aggressive Mode message from %s but no connection has been configured
NO PROPOSAL CHOSEN: Initial Main Mode message received on %s:%u but no connection has been authorized
INVALID ID: Require peer to have ID %s, but peer declares %s
INVALID ID INFORMATION: Initial Aggressive Mode packet claiming to be from %s on %s but no connection has been authorized
INVALID ID: Require peer to have ID %s, but peer declares %s
INVALID ID INFORMATION: Initial Aggressive Mode packet claiming to be from %s on %s but no connection has been authorized
IKE Negotiated Status Messages
Received Delete SA payload and deleting IPSEC State (<i>integer</i>)
Received Delete SA payload: Deleting ISAKMP State (<i>integer</i>)
(Main/Aggressive) mode peer ID is (identifier string)
ISAKMP SA Established
IPsec SA Established

Appendix F: Bandwidth Management with QoS

F.1 Overview

In a home or office environment, users constantly have to transmit data to and from the Internet. When too many are accessing the Internet at the same time, service can slow to a crawl, causing service interruptions and general frustration. Quality of Service (QoS) is one of the ways Firetunnel 10 can optimize the use of bandwidth, ensuring a smooth and responsive Internet connection for all users.

F.2 What is Quality of Service?

QoS is a feature that prioritizes and guarantees bandwidth to achieve optimal service performance. QoS can maximize the use of available network bandwidth by prioritizing time-sensitive traffic to avoid latencies and delays. By ensuring that time-sensitive applications such as VoIP and streaming video get priority access to bandwidth, users in both home and office environments can enjoy smooth and responsive data transmission no matter which applications they are running.

If you've ever experienced slow Internet speeds due to other network users using bandwidth-consuming applications like P2P, you'll understand why QoS is such a breakthrough for home users and office users. Black Box makes itself unique by integrating QoS in its routers for both inbound and outbound traffic.

QoS helps users manage bandwidth and effectively prioritize data traffic. It gives you full control over the traffic of any type of data. Employed on DiffServ (Differentiated Services) architecture, data traffic is given priority by the router; ensuring latency-sensitive applications like voice and mission-critical data such as VPN move through the router at lightning speeds, even under heavy load. You can throttle the speed of different types of data passing through the router, limit the speed of unimportant or bandwidth-consuming applications, and even distribute the bandwidth for different groups of users at home or in the office. QoS keeps your Internet connection smooth and responsive.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018
USA, Canada: www.blackbox.com,
EU, Africa, Asia, South America, Australia: www.blackbox.eu



F.3 How Does QoS Work?

QoS employs three different methods for optimizing bandwidth:

- Prioritization: Assigns different priority levels for different applications, prioritizing traffic. High, Normal and Low priority settings.
- Outbound and Inbound IP Throttling: Controls network traffic and allows you to limit the speed of each application.
- DiffServ Technology: Manages priority queues and DSCP tagging through the Internet backbone. Manages traffic among Ethernet, wireless, and ADSL interfaces.

F.4 Who Needs QoS?

QoS is ideal for home and office users who need to use a variety of real-time applications like VoIP, on-line games, P2P, video streaming, and FTP simultaneously. With QoS, you can optimize your bandwidth to accommodate several of these applications without experiencing latency or service interruptions.

F.4.1 Home Users

Low latency is everything for gamers. Most home users feel frustrated when trying to play an online game over a shared ADSL connection. Unfortunately, most routers have no way of determining the importance of the packet at any given time. All the traffic is treated equally, so a packet containing an "urgent" command may be delayed. QoS gives you the ability to control the bandwidth. Using IP Throttling, bandwidth limits can be enforced on a particular application or any system within the LAN. Prioritization specifies which packets have priority and should not be delayed, and which packets have lower priority and should be moved to the end of the upload queue.

Suppose there are four students sharing a three-floor house with one single broadband connection. Tom, a college freshman, is playing the online game with his group members, while Mary, a sophomore student, is talking to her net pal via Skype. Meanwhile, Jacky is downloading a movie file by using the P2P application program. Sophia, however, is just trying to log on to the website to send her photos to her family. As a result, the net speed slows to a crawl and affects everyone sharing the Internet connection. QoS is designed for managing traffic flow and bandwidth to solve this problem. You can first classify different applications (online

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



games, FTP, Skype, email) as shown in the table below. Then, you can manage and prioritize the flow of bandwidth at different levels (e.g. 30% for games, 20% for downloads, 10% for email, 20% for FTP, and 35% for others). QoS can be used to identify different applications and assign priority to enable a smooth and responsive broadband connection.

Application	Data Ratio (%)	Priority
On-line games	30%	High
Skype	5%	High
Email	10%	High
FTP	20%	Upload (High), Download (Normal)
Other	35%	

F.4.2 Office Users

QoS is also ideal for small businesses using an office server as a web server. With QoS control, web pages served to your customers can be given top priority and delivered first so that it will not be impeded by email and office web browsing.

Here is a good example of how QoS can work in an office environment. A CEO is holding a videoconference with international clients in the meeting room. However, the streaming video and voice frequently lag. Sales people are talking to international agencies via VoIP phone, while sending orders via email to vendors for production. However, some staff are downloading MP3 music files, large-size photos and watching video streaming online. Consequently, the Internet connection slows down. This is why business users need QoS to manage data traffic. With QoS, the network administrator can define and classify important packets; specify a minimum guaranteed rate for each application, and ensure that important packets have priority to ensure a good quality of broadband connection for the entire organization.

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

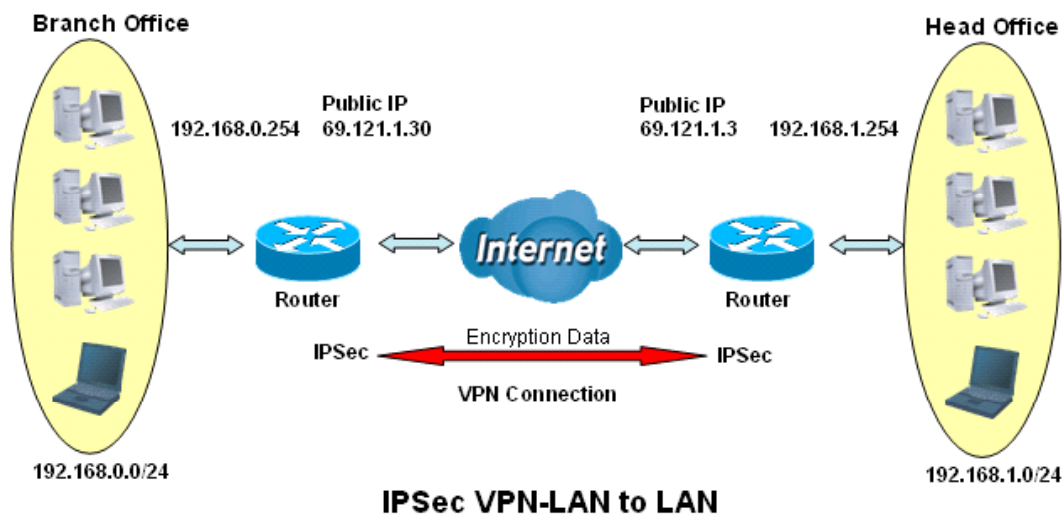
Application	Data Ratio (%)	Priority
Videoconferencing	30%	High
VoIP	20%	High
Email	10%	High
FTP	10%	Upload (High), Download (Normal)
Other	30%	MP3 (Low), MSN (Normal)

Appendix G: Router Setup Examples

G.1 VPN Configuration

This section outlines some concrete examples on how you can configure Firetunnel 10 for your VPN.

G.1.1 LAN to LAN



	Branch Office	Head Office
Local		
ID	IP Address	IP Address
Data	69.121.1.30	69.121.1.3
Network	Any Local Address	Any Local Address
IP Address	192.168.0.0	192.168.1.0
Netmask	255.255.255.0	255.255.255.0
Remote		
Secure Gateway	69.121.1.3	69.121.1.30

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,EU, Africa, Asia, South America, Australia: www.blackbox.eu

Address(or Hostname)		
ID	IP Address	IP Address
Data	69.121.1.3	69.121.1.30
Network	Subnet	Subnet
IP Address	192.168.1.0	192.168.0.0
Netmask	255.255.255.0	255.255.255.0
Proposal		
IKE Pre-shared Key	12345678	12345678
Security Algorithm	Main Mode; ESP: MD5 3DES PFS	Main ESP MD5 3DES PFS

Black Box Corporation

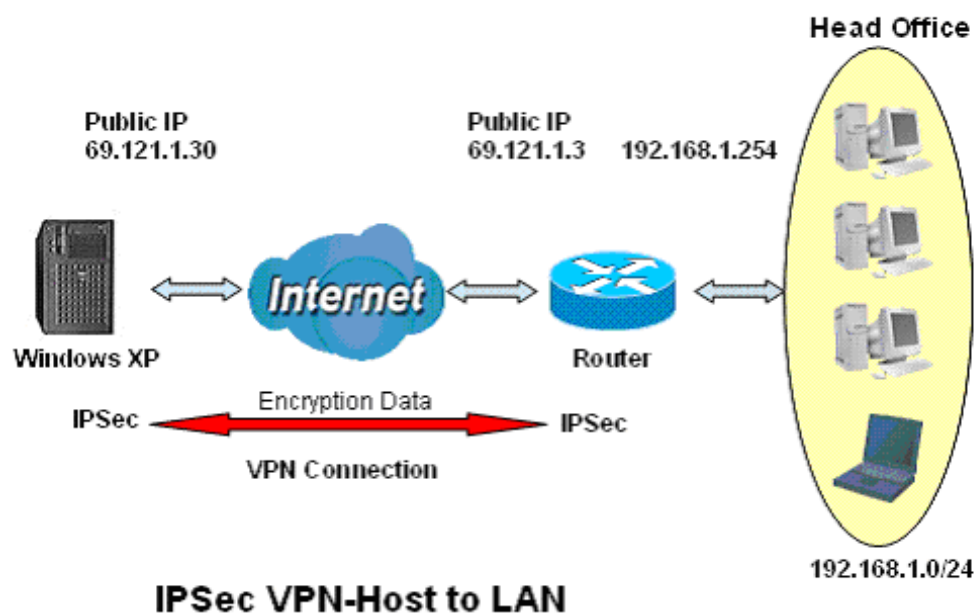
1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



G.1.2 Host to LAN



	Single client	Head Office
Local		
ID	IP Address	IP Address
Data	69.121.1.30	69.121.1.3
Network	Any Local Address	Any Local Address
IP Address	0.0.0.0	192.168.1.0
Netmask	0.0.0.0	255.255.255.0
Remote		
Secure Gateway Address(or Hostname)	69.121.1.3	69.121.1.30

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

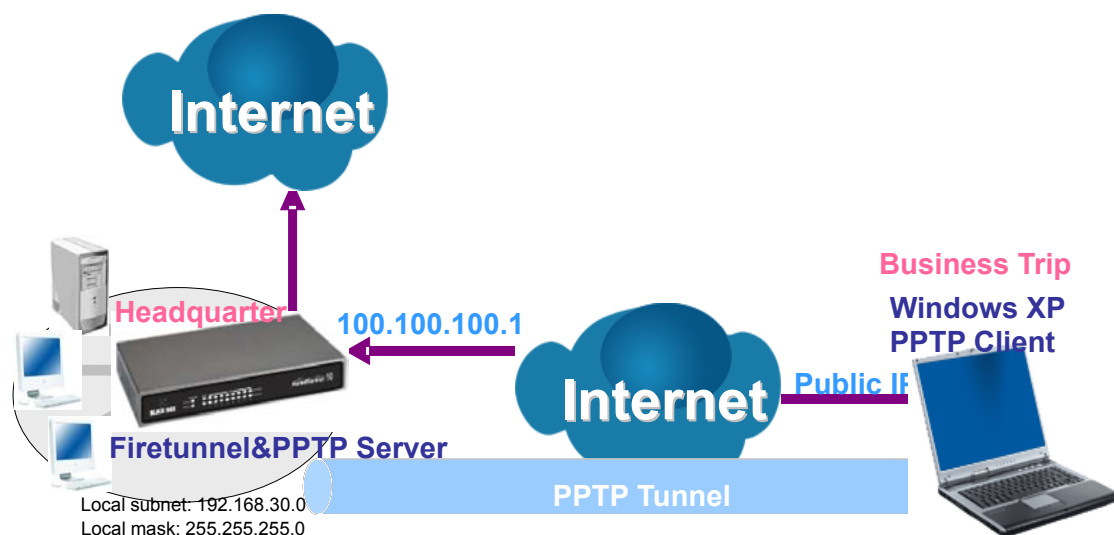
USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



ID	IP Address	IP Address
Data	69.121.1.3	69.121.1.30
Network	Subnet	Single Address
IP Address	192.168.1.0	69.121.1.30
Netmask	255.255.255.0	255.255.255.255
Proposal		
IKE Pre-shared Key	12345678	12345678
Security Algorithm	Main Mode; ESP: MD5 3DES PFS	Main ESP MD5 3DES PFS

G.1.3. PPTP Remote Access by Windows XP



Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Step1: Go to **Configuration > VPN > PPTP** and Enable the PPTP function, Click **Apply**.

PPTP					
General Setting					
PPTP function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Auth. Type	Pap or Chap				
Data Encryption	Disable				
Encryption Key Length	Auto				
Peer Encryption Mode	Only Stateless				
IP Addresses Assigned to Peer	Start from: 192.168.1.200				
Idle Timeout	0 Min.				
(⚠ Enable data encryption will use MS-CHAPv2 to authenticate the peer.)					
<input type="button" value="Apply"/>					
Account Setting					
Name	Enable	Type	Peer Network		
<input type="button" value="Create"/>					

Step2: Click **Create** to create a PPTP Account.

PPTP					
Add PPTP Account					
Connection Name	WinXP				
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Username	test				
Password	••••				
Retype Password	••••				
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN				
Peer Network IP					
Peer Netmask					
Netbios Broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
<input type="button" value="Apply"/>					

Black Box Corporation

1000 Park Drive, Lawrence, PA 15055-1018

USA, Canada: www.blackbox.com,

EU, Africa, Asia, South America, Australia: www.blackbox.eu



Step3: Click **Apply**, you can see the account is successfully created.

PPTP					
General Setting					
PPTP function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Auth. Type	Pap or Chap				
Data Encryption	Enable				
Encryption Key Length	Auto				
Peer Encryption Mode	Only Stateless				
IP Addresses Assigned to Peer	Start from: 192.168.10.200				
Idle Timeout	0 Min.				
(Enable data encryption will use MS-CHAPv2 to authenticate the peer.)					
<input type="button" value="Apply"/>					
Account Setting					
Name	Enable	Type	Peer Network		
WinXP	✓	Remote Access	-----	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="button" value="Create"/>					

Step4: Click **Save Config** to save all changes to flash memory.

Step5: In Windows XP, go **Start > Settings > Network Connections**.

Step6: In **Network Tasks**, Click **Create a new connection**, and press **Next**.

Step7: Select **Connect to the network at my workplace** and press **Next**.

Step8: Select Virtual **Private Network connection** and press **Next**.

Step9: Input the user-defined name for this connection and press **Next**.

Step10: Input PPTP Server Address and press **Next**.

Step11: Please press **Finish**.

Step12: Double click the connection, and input **Username** and **Password** that defined in Firetunnel PPTP **Account Settings**.