

# Comcast Business IP Gateway

---

## User's Guide

---

**Copyright © 2006** Comcast Communications, Inc. All Rights Reserved.

Comcast is a registered trademark of Comcast Corporation. Comcast Business IP Gateway is a trademark of Comcast Corporation.

The Comcast Business IP Gateway is provided to Comcast Workplace customers. Comcast Workplace service is not available in all areas. Not all features are available in all packages. Comcast reserves the right to modify the User's Guide at any time. Service is subject to terms and conditions of Comcast Workplace Service Agreement.

# Table of Contents

<a href="#">WELCOME TO COMCAST</a> .....	4
<a href="#">CHAPTER 1: INSTALLATION</a> .....	5
<a href="#">Initial Installation</a> .....	5
<a href="#">Additional Feature Setup Options</a> .....	5
<a href="#">Gateway Log-In</a> .....	5
<a href="#">Administration Settings</a> .....	5
<a href="#">CHAPTER 2: YOUR LOCAL AREA NETWORK (LAN)</a> .....	7
<a href="#">Setting Up the LAN (Local Area Network)</a> .....	7
<a href="#">IP Setup</a> .....	7
<a href="#">Static Routing Setup</a> .....	8
<a href="#">CHAPTER 3: YOUR FIREWALL</a> .....	10
<a href="#">Firewall Options</a> .....	10
<a href="#">Port Configuration</a> .....	10
<a href="#">Port Forwarding</a> .....	11
<a href="#">Port Triggering</a> .....	12
<a href="#">Port Blocking</a> .....	13
<a href="#">Static IP Port Management</a> .....	14
<a href="#">Web Site Blocking</a> .....	15
<a href="#">Setting Up Web Site Blocking</a> .....	16
<a href="#">Setting Up a Web Site-Blocking Schedule</a> .....	17
<a href="#">DMZ</a> .....	17
<a href="#">CHAPTER 4: GATEWAY OVERVIEW</a> .....	19
<a href="#">Gateway Status</a> .....	19
<a href="#">Network</a> .....	19
<a href="#">Internet Settings</a> .....	19
<a href="#">Local Settings</a> .....	20
<a href="#">Cable Modem</a> .....	20
<a href="#">CHAPTER 5: APPENDICES</a> .....	21
<a href="#">Appendix A: Port Protocol Assignments</a> .....	21
<a href="#">Appendix B: Glossary</a> .....	23

# WELCOME TO COMCAST

Welcome to Comcast Workplace. Comcast Workplace provides a complete business Internet service – everything you need to safely and efficiently connect your business to the Internet. This guide will help you make the most of your Comcast services – specifically the features that are enabled and managed through the Comcast Business IP Gateway.

The Comcast Business IP Gateway, included with your Comcast Workplace service, is designed to help you securely connect your business to the Internet and manage your users' access to it.

The Comcast Business IP Gateway provides:

- **Firewall Protection** – A firewall provides essential protection for your business by blocking unwanted users and data traffic from entering your local area network (LAN).
- **User Access Management** – Using the gateway, you manage your users' access to the Internet. You can block access to specific Web sites or sites with specific inappropriate content.
- **Advanced Security Features** – Includes port forwarding and port triggering to help you manage access to and from your site.

# CHAPTER 1: INSTALLATION

## *Initial Installation*

One of our professionals does the initial installation for you so that your Comcast gateway network is Internet-ready, and you're ready to get to work. Your installer will connect the gateway to your LAN, assign a static Internet Protocol (IP) – if you requested a static IP – and connect your gateway to the Internet.

After the initial installation, when you log on and open your Comcast gateway to access the user feature setup screen, you will see that your LAN has been configured with the following settings:

- An assigned LAN IP address
- An assigned LAN subnet mask
- A domain suffix
- A dynamic Host Configuration Protocol (DHCP) server, enabled with a specific range of DHCP addresses

## *Additional Feature Setup Options*

In addition to the initial feature setup performed by the Comcast installer, there are many additional features and options that you can configure to help protect and manage your network:

- You can block certain Web sites, configure your security features, or block outside computers from the network.
- You can get detailed information on your gateway and change a variety of other settings.
- Should you decide to change or modify your initial LAN IP setup, you can make those changes as well.

## *Gateway Log-In*

Log in to the Comcast Business Gateway by entering <http://10.1.10.1>. The Comcast Business IP Gateway screen will display. Enter the following default username and password so that you can access the feature setup screens:

- The default username is **cusadmin**.
- The default password is **highspeed**.

After you have logged in to the Comcast Business IP Gateway, you can configure the gateway settings listed in the menu. Shortcut icons are also provided for **LAN setup**, **Port Configuration**, and **Gateway Summary**. You can also access specific features by clicking the menu items on the left-hand side of the screen.

**Help** will provide additional information regarding configuring the features in the Comcast Business IP Gateway.

## *Administration Settings*

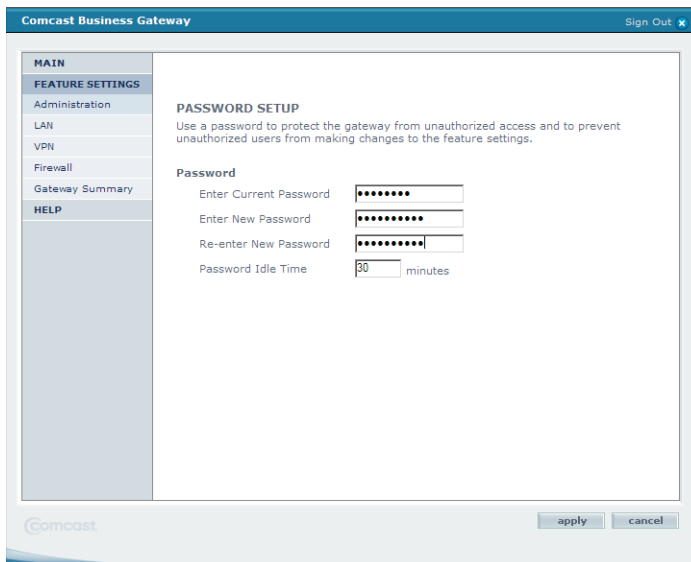
By using a password, the gateway is secured from unauthorized access and prevents unauthorized users from making changes to the feature settings. You can retain the default password to access the feature setup or select a new password.<sup>1</sup>

---

<sup>1</sup> Passwords alone will not protect against unauthorized access or use.

## To change the password:

1. Select **Administration** or **Feature Settings** from the menu on the welcome screen. The **Password Setup** screen will display.
2. Enter the current password (**highspeed**) in the **Enter Current Password** field.
3. In the **Enter New Password** field, enter a new password.
4. Retype the new password in the **Re-enter New Password** field.
5. Enter the **Password Idle Time**. This is the amount of time that the session will remain open when idle. You are automatically logged off if the session remains idle past the idle time.
6. Click **apply**.



The screenshot shows the Comcast Business Gateway web interface. The title bar reads "Comcast Business Gateway" and "Sign Out x". A left-hand navigation menu includes "MAIN", "FEATURE SETTINGS" (with "Administration" selected), "LAN", "VPN", "Firewall", "Gateway Summary", and "HELP". The main content area is titled "PASSWORD SETUP" and contains the following text: "Use a password to protect the gateway from unauthorized access and to prevent unauthorized users from making changes to the feature settings." Below this, under the heading "Password", there are four input fields: "Enter Current Password" (with 7 dots), "Enter New Password" (with 7 dots), "Re-enter New Password" (with 7 dots), and "Password Idle Time" (with a text box containing "30" and the label "minutes"). At the bottom of the page, there are "Comcast" and "apply" buttons, and a "cancel" button.

# CHAPTER 2: YOUR LOCAL AREA NETWORK

## *Setting Up the LAN*

Your LAN IP already has been configured during initial setup. The LAN IP contains the IP information distributed by the gateway to your local network (computers connected to your gateway). If your network uses a different IP addressing scheme, you can make those changes in the LAN IP setup. DHCP is also enabled during setup, and a range of DHCP addresses are assigned by the DHCP server.

## *IP Setup*

The gateway is configured to use private IP addresses on the LAN side and to act as a DHCP server. The gateway's default LAN IP configuration is set to:

- LAN IP address – 10.1.10.1
- Subnet mask – 255.255.255.255
- Domain suffix – wp.comcast.net

**If you have an existing TCP/IP network, you can change the Gateway's default LAN to integrate with it.**

1. Enter in the **LAN IP Address**: The LAN IP address is the IP address of the gateway as seen by users on the local network. The default IP LAN address of your gateway is **10.1.10.1**.
2. Enter the **LAN Subnet Mask**: The LAN subnet mask allows you to define the LAN subnet size to further divide the LAN IP address into additional subnets. The default LAN subnet mask is **255.255.255.0**.
3. Enter the **Domain Suffix**: The default domain name is **wp.comcast.net**.
4. **Enable LAN DHCP**: Default is checked. Allows the LAN DHCP server to automatically allocate IP addresses to the LAN client PCs.
  - a. Select the **Lease Time** for the IP addresses assigned by the LAN DHCP server. A LAN client device that is assigned a LAN DHCP IP address is generally reassigned the same IP upon lease expiration. The default lease time is set to **1 Week**.
  - b. Enter the **DHCP Start IP**. This will be the first available LAN IP address that will be assigned by the LAN DHCP. The default start IP address is **10.1.10.10**.
  - c. Enter the **DHCP End IP**. This will be the last available LAN IP address that will be assigned by the LAN DHCP. The number of IP addresses between the DHCP start IP and DHCP end IP will determine the DHCP IP address pool size. The default DHCP end IP is **10.1.10.199**.

5. **Assign DNS Manually:** Default is unchecked. The domain name system (DNS) system maps human-friendly names to computer-friendly numeric IP addresses. In most cases, the default setting will work well. If the **Assign DNS Manually** is checked, you can manually define the primary and secondary DNS servers that will be assigned to all PCs connected to the LAN via DHCP. If **Assign DNS Manually** is selected:
  - a. Enter the **Primary DNS** server that will be assigned to LAN devices.
  - b. Enter the **Secondary DNS** server that will be assigned to LAN devices.
6. Click **apply**.

## Static Routing Setup

Users can manually add static routes to routers connected to the gateway LAN to create specific paths to a destination.

Setting a static route allows devices routed by the Comcast commercial gateway to communicate with the separate subnet of a router connected to the commercial gateway.

For example, a stand-alone router (IP subnet address “10.1.10.33”) is connected to the Comcast commercial gateway (IP address “10.1.10.1”). The stand-alone router is configured with a static route rule to route the subnet “111.222.33.0,” subnet mask “255.255.255.0.” By adding a static route called “My Router” and configuring the destination IP to “111.222.33.0,” the subnet mask to “255.255.255.0” and the gateway IP to “10.1.10.33,” all PCs on the router subnet “111.222.33.0” will be able to communicate with the PCs on Comcast commercial gateway’s subnet “10.1.10.0.”

A maximum of eight static routes may be added. To set up a static route rule, you must first know the destination IP address, the subnet mask of the destination IP address, and your LAN IP assigned to the router by the Comcast commercial gateway.

### To create a static routing rule:

1. Enter a **Name** for the router that will make the route easier to remember (has no effect on the static routing function).
2. Enter the **Destination IP**.
3. Enter the **Subnet Mask** of the destination IP.
4. Enter your local LAN **Gateway IP** address (The LAN IP assigned to the router connected to the Comcast commercial gateway).

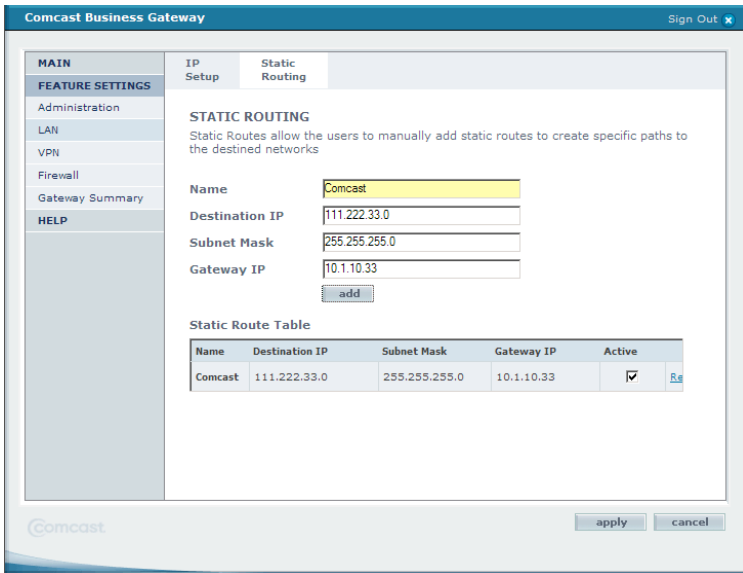


5. Click **add**. The new static route will be added to the static routing table.
6. Repeat steps 1 through 5 to add additional static routes.
7. Click **apply** to activate the static routes.

An example of setting a static route rule is shown in Appendix A.

**To remove a static routing setting:**

Click the **Remove** link on the static routing table to remove the route. The entire route is removed.



## CHAPTER 3: YOUR FIREWALL

A firewall is designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent Internet users from accessing private networks connected to the Internet, especially intranets or LANS.

The Comcast IP gateway incorporates a stateful packet inspection firewall. 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.

The gateway also supports network address translation (NAT), allowing several hosts to share one public IP address for Internet access.

### *Firewall Options*

You can disable portions of the gateway firewall by selecting one of the following options. Remember that disabling part of your firewall opens holes for possible threats. Only disable those options required by your network setup.

1. Check **Disable Firewall for True Static IP Subnet Only** to disable all firewall functionality for devices assigned an IP from the static IP subnet.
2. Check **Disable Gateway Smart Packet Detection** to disable the threat detection feature for all devices connected to the gateway.

### *Port Configuration*

Firewall rules are used to block or allow specific traffic passing through from one side to the other. The traffic is managed by blocking or allowing certain traffic, based on the ports that this traffic generally uses. Port numbers are assigned to specific network or Internet services; e.g., HTTP, or Web, traffic uses port 80 or 8080; HTTPS, or secure, traffic uses port 443; and SMTP and POP, or e-mail, traffic use ports 25 and 80.

Inbound rules (from the Internet to your LAN) restrict access by outsiders to private resources, selectively allowing outside users to access specific resources on your private IP (e.g., mail, Web, or FTP server). Instructions for setting up inbound rules are covered in the port forwarding and port triggering sections.

Outbound rules (from computers or users on your LAN to the Internet) determine what outside resources local users can have access to and are covered in the port blocking section.

The three firewall rules that can be configured to parse inbound traffic are:

- **Port Forwarding** (inbound): Allows you to direct inbound Internet traffic to connect to a specific application or computer within a private LAN via a predefined port(s).
- **Port Triggering** (inbound): Provides the ability to dynamically open a specific inbound port based on a request from a local computer or user.
- **True Static IP Port Management** (inbound): Allows you to open or close specific inbound ports to connected computers or firewalls configured with a public routable IP address (for use by static IP customers only).

The following firewall rule can be configured to parse outbound traffic:

- **Port Blocking** (outbound): Enables you to restrict specific local hosts from accessing particular Internet applications.

## Port Forwarding

By defining an inbound rule, port forwarding can open a window so that incoming traffic can be directed to your computer. The rule tells the gateway to direct inbound traffic for a particular service to one local computer, based on the destination port number. A list of commonly used public ports is listed in Appendix A.

This feature is used primarily for devices on your local network that can be accessed from the Internet. The **Enable** box must be checked in order to enforce a specific port forwarding rule.

Before implementing port forwarding, consider the following:

- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, you can assign a static IP address to your server outside the range that is assigned by DHCP but in the same subnet as the rest of your LAN.
- Local computers must access the local server using the computers' local LAN address (10.1.10.x, by default). Attempts by local computers to access the server using the external WAN IP address will fail. Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network.

### To add a new port forwarding rule:

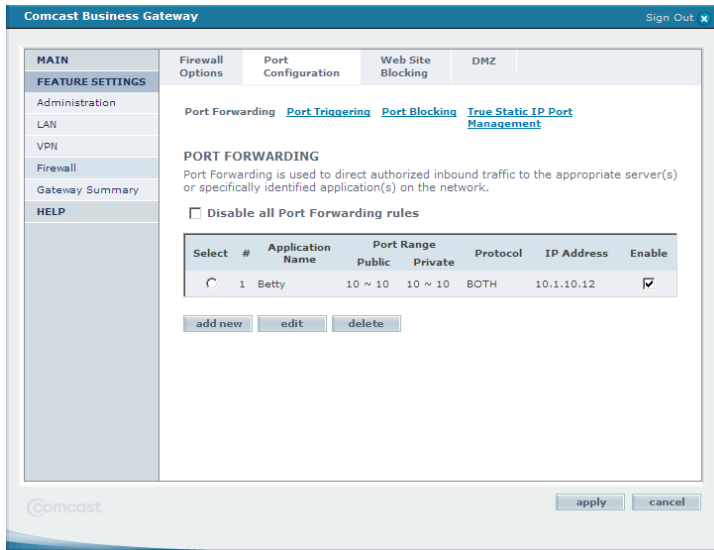
1. Click **add new**. The **Port Forwarding add/edit** screen will display.
2. In the **Application Name** field, enter an application name to identify this rule.
3. Enter the port number range in the **Public** port field. The assignable ports are between 1 and 65535. Users on the Internet will use the public port to connect to the LAN device for which you are creating this forwarding rule.<sup>2</sup>
4. Enter the first port of the port range in the **Private** port field. The assignable ports are between 1 and 65535. The private port is the port on the LAN PC, where this rule will forward traffic. The size of the private port range must match the size of the public port range and is automatically calculated for you.
5. Select the appropriate protocol from the **Protocol** drop-down menu (TCP, UDP, or both).
6. Enter the IP address of the computer you want the traffic to be forwarded to in the **IP Address** field. Click **Connected Computers** to locate the IP addresses of the computers connected to your gateway.
7. Click **apply**. The new port forwarding rule will display in the port forwarding table.

### To edit an existing rule:

1. Select the rule from the port forwarding rule table, and click **edit**. The **Port Forwarding add/edit** screen will display.
2. Edit the rule configuration steps that apply.
3. Click **apply**.

---

<sup>2</sup> A guide to generally accepted port numbers is located in Appendix A.



### To disable a port forwarding rule:

1. Check the **Disable All Port Forwarding Rules**. All of the port forwarding rules will be disabled, as well as access to adding or editing rules.

### To delete a port forwarding rule:

1. Check the box in the **Select** column opposite the port forwarding rule you want to delete.
2. Click **delete**.

## Port Triggering

Port triggering is an advanced feature that allows you to dynamically open inbound ports based on outbound traffic. It allows a PC behind the gateway to access special applications on the Internet (e.g., messaging programs). When an application such as messaging software performs an outgoing request for a port, the port triggering rule opens up the port for the local computer running the software and allows traffic to flow back and forth for as long as the program is in use. When the trigger port is no longer in use, the router waits a short time and then forwarding is switched off.

Port triggering is a little more secure than port forwarding, because the incoming ports are not open all the time. They are open only when a program is actively using the trigger port. Like most security solutions, there is a downside to this as well: When the application that requested the inbound traffic does not generate outbound traffic on the port being forwarded, the router will close the port after some time, causing incoming traffic to be blocked. This can be bothersome when trying to download large files, since there is no longer any outbound traffic after the initial request to open the port.

The **Enable** box must be checked to enforce a specific port triggering rule.

## To add a new port triggering rule:

1. Click **add new**. The **Port Triggering add/edit** screen will display.
2. Enter the application name in the **Application Name** field to identify this rule.
3. Enter the trigger **Port Range**. This is the outbound port range that will be monitored for activity and used by the special application that will trigger this rule.
4. Enter the target **Port Range**. These are the inbound ports that the return traffic will be forwarded to on the local client PC.
5. Select the appropriate **Protocol** from the drop-down menu.
6. Click **apply**. The new port triggering rule will display in the port triggering table.

## To edit an existing rule:

7. Select the rule from the port triggering rule table, and click **edit**. The **Port Triggering add/edit** screen will display.
8. Edit the rule configuration steps that apply.
9. Click **apply**.

Comcast Business Gateway Sign Out x

MAIN  
FEATURE SETTINGS  
Administration  
LAN  
VPN  
Firewall  
Wireless Settings  
Gateway Summary  
HELP

Firewall Options | **Port Configuration** | Web Site Blocking | DMZ

[Port Forwarding](#) | [Port Triggering](#) | [Port Blocking](#) | [True Static IP Port Management](#)

**PORT TRIGGERING**  
Port Triggering is used to allow computers on your local area network access specific applications on the Internet.

Disable all Port Triggering rules

Select	#	Application Name	Port Range Public	Port Range Private	Protocol	Timeout (ms)	Enable
<input type="radio"/>	1	Application 1	11 ~ 20	11 ~ 20	TCP	100	<input type="checkbox"/>
<input type="radio"/>	2	Application 2	550 ~ 660	550 ~ 660	Both	130	<input type="checkbox"/>

Comcast

## Port Blocking

LAN port blocking allows you to restrict a computer within your LAN from accessing certain Internet traffic by IP address and logical port. For example, you can restrict Web access or instant messaging from specific computers by creating a rule that blocks them from using ports 80 and 443 (Web), or port 5190 (IM).

Logical ports are assigned numbers to identify Internet traffic that is generated by a software application. The assignable logical port range is between 1 and 65535. Your gateway supports up to 100 LAN port blocking rules.

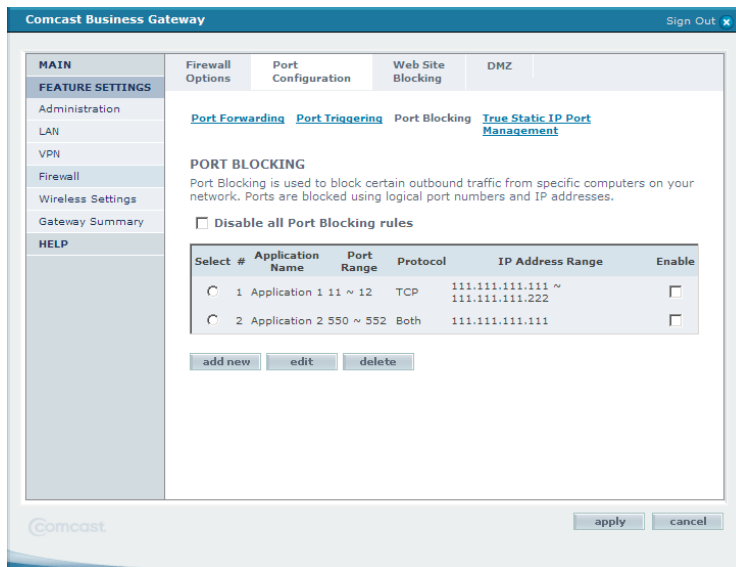
The **Enable** box must be checked to enforce a specific port blocking rule.

### To add a new port blocking rule:

1. Click **add new**. The **Port Blocking add/new** screen will display.
2. Type an application name in the **Application Name** field to identify this rule.
3. Enter the logical port range in the **Port Range** fields.
4. Select the appropriate **Protocol** from the drop-down menu.
5. Enter the IP address range in the LAN **IP Address Range** fields (Click **Connected Computers** to view the IP addresses of the computers connected to your gateway).
6. Click **apply**. Your new port blocking rule will be added to the port blocking table.

### To edit an existing rule:

1. Select the rule from the port blocking rule table, and click **edit**.
2. Edit the rule configuration steps that apply.
3. Click **apply**.



## Static IP Port Management

Static IP port management allows you to restrict inbound traffic to computers within your local network by IP address and logical port number.

The **Enable** box must be checked to enforce a specific rule. The **True Static IP Port Management** rules table can be set up to either block all ports but allow exceptions, or to allow all ports to open but block exceptions. You can also override the true static IP port management rules by checking the **Disable all rules and allow inbound traffic through** box.

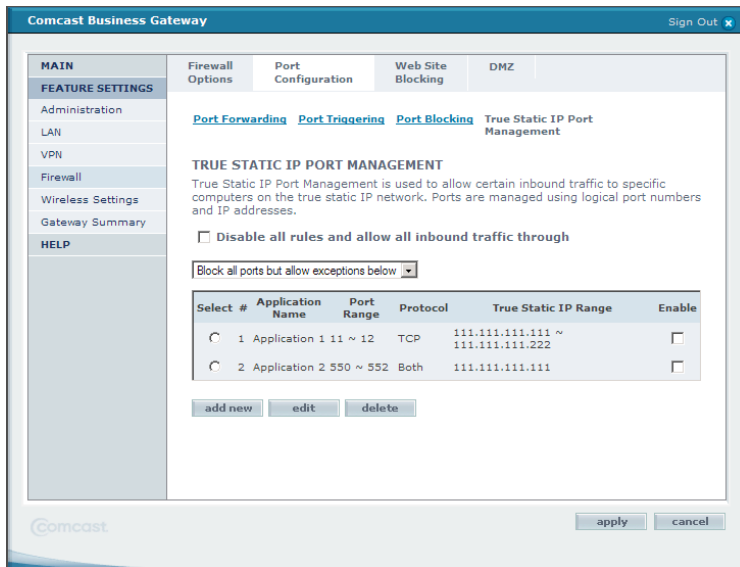
## To add a new static IP port management rule:

Click **add new**. The **True Static IP Port Management add/edit** screen will display.

1. Enter an application name to identify this rule in the **Application Name** field.
2. Enter the logical port range in the **Port Range** fields.
3. Select the appropriate **Protocol** from the drop-down menu.
4. Enter the true static IP address range in the **True Static IP Range** fields (click **Connected Computers** to view the IP addresses of the computers connected to your gateway).
5. Click **apply**. The new static IP port management rule will be added to the port management table.

## To edit an existing rule:

1. Select the rule from the **True Static IP Port Management** rule table, and click **edit**.
2. Edit the rule configuration steps that apply.
3. Click **apply**.



The screenshot shows the Comcast Business Gateway web interface. The main navigation menu on the left includes MAIN, FEATURE SETTINGS, Administration, LAN, VPN, Firewall, Wireless Settings, Gateway Summary, and HELP. The current page is titled 'True Static IP Port Management' and is part of the 'Port Configuration' section. It contains a description of the feature, a checkbox to 'Disable all rules and allow all inbound traffic through', and a dropdown menu to 'Block all ports but allow exceptions below'. Below this is a table with two columns: 'Select #' and 'Application Name'. The table lists two rules: Rule 1 for 'Application 1' with port range '11 ~ 12' and protocol 'TCP', and Rule 2 for 'Application 2' with port range '550 ~ 552' and protocol 'Both'. Each rule has an 'Enable' checkbox. At the bottom of the table are 'add new', 'edit', and 'delete' buttons. The overall page has 'apply' and 'cancel' buttons at the bottom right.

Select #	Application Name	Port Range	Protocol	True Static IP Range	Enable
1	Application 1	11 ~ 12	TCP	111.111.111.111 ~ 111.111.111.222	<input type="checkbox"/>
2	Application 2	550 ~ 552	Both	111.111.111.111	<input type="checkbox"/>

## Web Site Blocking

The gateway provides a variety of options for blocking Internet-based content and communications services. With its content-filtering feature, the gateway prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for key words within Web addresses. You can set up to 10 rules.

Key content-filtering options include:

- Blocking access from your LAN to Internet locations that contain key words that you specify.
- Blocking access to Web sites that you specify as off-limits.

### ***Setting Up Web Site Blocking***

Web site blocking allows you to restrict access to certain Web sites. You can block Web sites based on a key word or a specific Web site address. For example:

- If you enter “www.example.org,” only that address is blocked; if you enter only “example,” then all Web addresses containing that word are blocked (e.g., www.example.org, www.example.net, www.example.com).
- If the key word “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the key word “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- Enter the key word “.” to block all Internet browsing access.

#### **To set up Web site blocking:**

1. Check **Enable Web Site Blocking**.
2. In the **New Key Word/URL** field, enter either the full Web site address (e.g., “www.example.com”) to block a specific Web site or enter a key word to block all addresses containing that word.
3. Click **add**. The key word or Web site address will appear in the **Blocked Key Words/URLs** list.

#### **To remove entries from the list:**

Highlight the entry you want to remove and click **remove**, or clear the entire list by clicking **clear list**.

Trusted computers allow you to exempt any connected computers from the Web site blocking rules.

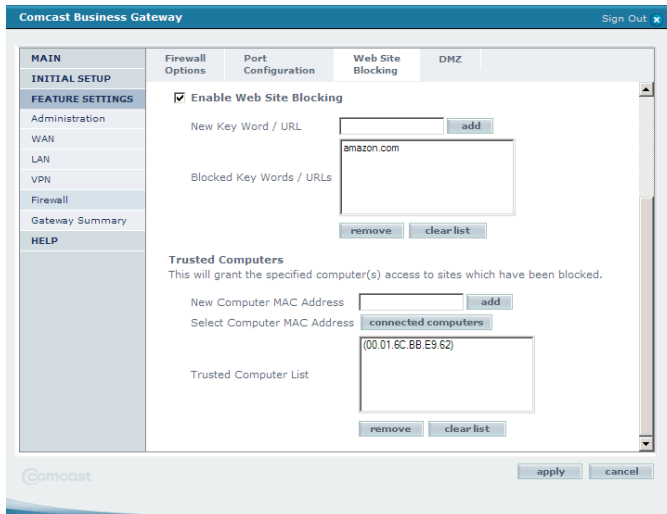
#### **To build a list of trusted computers:**

Do one of the following:

1. Click **Connected Computers** and select a computer from the **Connected Computers** table by checking the **add** box. Click **apply**.
2. Enter the MAC address of one of the computers in your LAN in the **New Computer MAC Address** field. Click **add**.

The MAC address of the computer you selected will appear in the **Trusted Computer List**.





### To remove a computer from the Trusted Computer List:

1. Select the computer's MAC address from the **Trusted Computer List**.
2. Click **Remove**.

### To enable Web site blocking:

Click **apply**.

## ***Setting Up a Web Site-Blocking Schedule***

The Web site-blocking schedule allows you to apply your Web site-blocking rules at different times of the day or week. For example, workers on a particular shift may not need Internet access.

### To set up a Web site-blocking schedule:

1. In **Days of the Week**, select the day or days to which you wish to apply Web site blocking.
2. In **Time of Day**, select either **All Day**, or choose a start time (e.g., 2 p.m.) and an end time (e.g., 6 p.m.) to which you want to apply Web site blocking.
3. Click **apply**.

## ***DMZ***

This feature is commonly used for gaming and videoconferencing – applications that will not function through NAT. The DMZ (demilitarized zone) allows a selected computer to bypass the firewall features of the gateway and permits unrestricted access from the Internet to that computer.

**Note:** For security, you should avoid using the DMZ feature when not needed. When a computer is designated as a DMZ server, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the gateway, unless the traffic is in response to one of your local computers or a service that you have configured in the port forwarding or port triggering menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the DMZ host.

**To assign a computer or server to be a DMZ host:**

1. From the main menu under **Firewall**, select **DMZ**.
2. Check **Enable DMZ Host**.
3. Enter the IP address of the LAN PC that you wish to place in the DMZ. Or click **Connect Computers** and select a computer from the connected computers table.
4. Click **apply**.

**To disable the DMZ Host:**

Uncheck the **Enable DMZ Host** box and click **apply**.

## CHAPTER 4: GATEWAY OVERVIEW

### *Gateway Status*

**Gateway Status:** The gateway status section provides information on the hardware and software provided within the gateway.

**Vendor Name:** The name of this gateway's manufacturer.

**Hardware Version:** The hardware version identifies the version of the hardware design of the gateway.

**Serial Number:** The serial number identifies a unique number and bar code format assigned to every gateway manufactured by the manufacturer.

**Firmware Version:** The firmware version identifies the number assigned to the programming code that is inserted, much like software, into your gateway on a semi-permanent basis. Occasionally, manufacturers update their firmware with new and improved features and add a new version number.

**Operating Mode:** The gateway has several modes of operation that will be helpful to support personnel should you encounter any issues. The operating mode field will detail what mode your gateway is currently running in.

**System Up Time:** The "system up" time displays the period of time the gateway has been functioning properly.

**Date:** The current date.

**Time:** The current time.

### *Network*

**Internet Settings:** The information displayed in the network Internet settings section is the Internet information provided by Comcast.

**Cable MAC Address:** The gateway Media Access Control (MAC) address is a unique number assigned by the manufacturer to any networking device, which allows the network to identify it at the hardware level. This is the unique address for the cable modem interface of the gateway.

**WAN-DATA MAC Address:** Similar to the way that a cable MAC address works, this is the unique address for the WAN-DATA interface of the gateway.

**WAN-MAN MAC Address:** The unique address for the cable home interface of the gateway.

**WAN-DATA IP Address:** The IP address is assigned by Comcast to the gateway. As a Comcast customer, your IP can be dynamic or static (in some markets). The changing gateway IP will not affect your Internet connectivity. The gateway IP address can be seen by external users on the Internet.

**WAN-MAN IP Address:** This address is reserved for troubleshooting purposes by Comcast.

**Subnet Mask:** The subnet mask represents the range of IP addresses assigned by Comcast. The default subnet is 255.255.255.0.

**Default Gateway:** The default gateway is the IP address that the gateway uses to forward all traffic that is not addressed to a client within Comcast's network.

**DNS:** The domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. Multiple IP DNS settings are common.

**DHCP Remaining Time:** The DHCP remaining time identifies in days, hours, minutes, and seconds the amount of time a network user has until the allowed use or "lease" expires on the gateway's WAN port of the current dynamic IP address.

**Date:** Current date as reported by the "time of day" server on the Comcast network.

**Static IP Block:** If the gateway is configured to utilize the RIP protocol, this field displays the RIP IP block assigned to the gateway. If the gateway is configured to receive its IP address dynamically, this field will have no values.

## ***Local Settings***

The information detailed in this section is the IP information distributed by the gateway to your local network (computers connected to your gateway).

**Gateway IP Address:** The gateway IP address is the IP assigned to the gateway. This is the gateway's IP address as seen by users on the local network. This address is also used to determine the DHCP range for DHCP addresses for your local network.

**Subnet Mask:** The LAN subnet mask allows further division of the host part of the LAN IP address into additional subnets.

**DHCP Server:** The Dynamic Host Configuration Protocol (DHCP) server in the gateway automatically assigns IP addresses to each computer on your local network.

**IP Range (start):** The beginning range of IP addresses that the gateway can assign to computers on your local network.

**IP Range (end):** The ending range of IP addresses that the gateway can assign to computers on your local network.

**Connected Computers:** Displays the computer name, IP address, MAC address, and interface (the method in which the computer is connected to the gateway: wireless or Ethernet) of all computers connected to your gateway. Only computers that are running will display in the connected computers list.

## ***Cable Modem***

**Cable Modem:** The cable modem status page shows the completed initialization procedure steps for your gateway, verifies that traffic has been enabled, and verifies the status of the upstream and downstream channels, of the connected modem.

## CHAPTER 5: APPENDICES

### ***Appendix A: Port Protocol Assignments***

In TCP/IP and UDP networks, a port is an end point to a logical connection and the way a client program specifies a specific server program on a computer in a network. Some ports have numbers that are preassigned to them by the IANA, and these are known as well-known ports (specified in RFC 1700). Port numbers range from 0 to 65536, but only port numbers 0 to 1024 are reserved for privileged services and designated as well-known ports.

When setting up the port forwarding feature, the following table lists some of the most common ports used by the server process as its contact port. For a more extensive list of ports, see <http://www.iana.org/assignments/port-numbers>.

<b>Port Number</b>	<b>Protocol</b>	<b>Description</b>
20	TCP	FTP – File Transfer Protocol (Data)
21	TCP	FTP – File Transfer Protocol (Control)
22	TCP	SSH Remote Log-in Protocol: secure log-ins, file transfers (SCP, SFTP), and port forwarding
23	TCP	Telnet – Nonsecure text communications
25	TCP	SMTP – Simple Mail Transfer Protocol: e-mail
49	TCP	Log-in Host Protocol (Log-in)
53	TCP/UDP	DNS – Domain Name System
69	UDP	TFTP – Trivial File Transfer Protocol
70	TCP	Gopher Services
79	TCP	Finger
80	TCP	HTTP – HyperText Transfer Protocol: www
110	TCP	POP3 – Post Office Protocol: e-mail
115	TCP	SFTP – Simple File Transfer Protocol
119	TCP	NNTP – Used for usenet news groups
137	TCP	NetBIOS – Name Service
139	TCP	NetBIOS – Datagram Service
143	TCP	IMAP – Interim Mail Access Protocol: e-mail
161	TCP	SNMP
194	TCP	IRC – Internet Relay Chat
197	TCP	DLS – Directory Location Service
389	TCP	LDAP – Lightweight Directory Access Protocol

<b>Port Number</b>	<b>Protocol</b>	<b>Description</b>
443	TCP	HTTPS – Used for securely transferring Web pages
444	TCP	SNPP – Simple Network Paging Protocol
445	TCP/UDP	Microsoft DS
458	TCP	Apple QuickTime
546	TCP	DHCP Client
547	TCP	DHCP Server
569	TCP	MSN
1080	TCP	Socks proxy

## ***Appendix B: Glossary***

Use the list below to find definitions for technical terms used in this manual.

**Broadcast:** A packet sent to all devices on a network.

**Default Gateway:** The routing device used to forward all traffic that is not addressed to a computer on the local subnet.

**Dynamic Host Configuration Protocol (DHCP):** A protocol that centrally automates the assignment of IP (IP) addresses in a network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When Comcast sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. DHCP lets Comcast distribute IP addresses and automatically sends a new IP address when a computer is plugged in to the high-speed Internet network. DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary.

**Demilitarized Zone (DMZ):** Allows one IP address (or computer) to be placed in between the firewall and the Internet (usually for gaming and videoconferencing). This allows risky, open access to the Internet.

**Domain Name System (DNS):** An Internet service that locates and translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time you use a domain name, a DNS service translates the name into the corresponding IP address. The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

**Domain:** A subnetwork comprised of a group of clients and servers under the control of one security database.

**Domain Name:** A descriptive name for an address or group of addresses on the Internet. Domain names are in the form of a registered entity name plus one of a number of predefined top-level suffixes, such as .com, .edu, .uk, etc.

**Ethernet:** A standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. It forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

**Firewall:** Firewalls are highly effective methods of blocking unsolicited traffic from outside the connected computers in your gateway.

**Gateway:** A local device, usually a router, that connects hosts on a local network to other networks – sometimes with different incompatible communication protocols.

**Internet Protocol (IP):** The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to be able to understand each other. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

**IP Address:** In the most widely installed level of the IP today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in packet form

across the Internet. When you request a Web page or send an e-mail, the IP part of TCP/IP includes your IP address in the message and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator (URL) you requested or in the e-mail address to which you are sending a note. A dynamic IP address is an IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

**Internet Service Provider (ISP):** A company that provides individuals and companies access to the Internet and other related services.

**Local Area Network (LAN):** A group of computers and associated devices such as printers and servers that share a common communication line and other resources within a small geographic area.

**Media Access Control (MAC) Address:** A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. Usually written in the form 01:23:45:67:89:ab.

**Megabits per Second (Mbps):** One million bits per second; unit of measurement for data transmission.

**MTU:** The size in bytes of the largest packet that can be sent or received.

**Network Address Translation (NAT):** A technique by which several hosts or computers share a single IP address for access to the Internet. NAT enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, and provides a type of firewall by hiding internal IP addresses.

**NetBIOS (Network Basic Input Output System):** An API that augments the DOS BIOS by adding special functions for LANs. Almost all Windows-based LANs for PCs are based on the NetBIOS.

**Packet:** A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a check sum.

**RIP:** A protocol in which routers periodically exchange information with one another so that they can determine minimum-distance paths between sources and destinations.

**Router:** A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

**Subnet:** A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 10.1.10 would be part of the same subnet. IP networks are divided using a subnet mask.

**Subnet Mask:** Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router. A number that explains which part of an IP address comprises the network address and which part is the host address on that network.

**Transmission Control Protocol (TCP):** A method (protocol) used with the IP to send data in the form of message units (datagrams) between network devices over a LAN or WAN. While IP handles the actual delivery of the data (routing), TCP keeps track of the individual units of data (packets) that a message is divided into for efficient delivery over the network. TCP requires the receiver of a packet to return an acknowledgment of receipt to the sender of the packet.



**Transmission Control Protocol/Internet Protocol (TCP/IP):** The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols.

**Wide Area Network (WAN):** A long-distance link or computer network that spans a relatively large geographical area that connects remotely located LANs. Typically, a WAN consists of two or more LANs. The Internet is a large WAN.