



EZ Connect™ Cable Modem Gateway

Install Guide

SMC8014

Copyright

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2006 by
SMC Networks, Inc.
38 Tesla
Irvine, California 92618

All rights reserved.

Trademarks

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

TABLE OF CONTENTS

CHAPTER 1 | Introduction

- Features and Benefits
- Package Contents
- Minimum Requirements

CHAPTER 2 | Getting to know the EZ Connect™ Cable Modem Gateway

- LED Indicators
- Rear Panel Description
- Resetting and Restoring the EZ Connect™ Cable Modem Gateway

CHAPTER 3 | Installation

- Basic Installation Procedure

CHAPTER 4 | Configuring your Computer

- Configuring Windows 95/98/Me
- Configuring Windows 2000
- Configuring Windows XP
- Configuring a Macintosh Computer

CHAPTER 5 | Configuring the EZ Connect™ Cable Modem Gateway

- Browser Configuration
- Disable Proxy Connection
- Accessing the EZ Connect™ Cable Modem Gateway Web Management

CHAPTER 6 | Navigating the Web-based Administration

- Making Configuration Changes
- System
- LAN
- NAT
- Firewall
- Tools
- Status

APPENDIX A | Telnet/CLI Information

APPENDIX B | Troubleshooting

APPENDIX C | Technical Specifications

APPENDIX D | Compliances

APPENDIX E | Technical Support

CHAPTER 1 | Introduction

Congratulations on your purchase of the EZ Connect™ Cable Modem Gateway. SMC is proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet.

Features and Benefits

- **EZ 3-Click Installation Wizard** - A new and improved way to install your Gateway Modem. In 3 simple clicks, you will be connected to the Internet.
- Internet connection to cable modem service via an integrated cable modem port
- Local network connection via 10/100 Mbps Ethernet ports or 54 Mbps interface.
- 802.11g - interoperable with multiple vendors.
- DHCP for dynamic IP configuration, and DNS for domain name mapping.
- Firewall with Stateful Packet Inspection, client privileges, hacker prevention, DoS, and NAT.
- User-definable application sensing tunnel supports applications requiring multiple connections
- Built-in Parental controls allow you to limit certain web sites - configurable by time and date.
- Easy setup through a web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications



Package Contents

Before installing the EZ Connect™ Cable Modem Gateway, verify that you have the items listed under below. Also be sure that you have the necessary cabling. If any of the items are missing or damaged, contact your local SMC distributor.

- 1 - EZ Connect™ Cable Modem Gateway
- 1 - Power adapter (12V/1.25A)
- 1 - CAT-5 Ethernet cable
- 1 - USB Cable
- Installation CD, including:
 - User Guide
 - USB Drivers

If possible, retain the carton and original packing materials in case there is a need to return the product.

Please register your product on SMC's web site at <http://www.smc.com>.

System Requirements

You must meet the following minimum requirements:

- Provisioned Internet access from a cable operator that has approved the SMC8014
- A computer equipped with a wired network adapter with TCP/IP installed.
- A Java-enabled web browser, such as Microsoft Internet Explorer 5.5 or above, or Netscape Communicator 5.0 or above.
- Windows 98 Second Edition or higher is required for USB driver support.

CHAPTER 2 | Getting to Know the EZ Connect™ Cable Modem Gateway

The EZ Connect™ Cable Modem Gateway is the perfect all in one solution, for the home or business environment. This full-featured device has:

- An approved DOCSIS 1.1 and 2.0 Cable modem
- Advanced SPI Firewall Gateway
- Comprehensive LEDs for network status and troubleshooting
- Reset Button
- 4 - 10/100 Mbps Auto-Sensing LAN ports with Auto-MDI MDIX feature
- 1 - USB 1.1 LAN Port for PC connectivity

NOTE: Cable modems provide up to 38 Mbps downstream and 10 Mbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

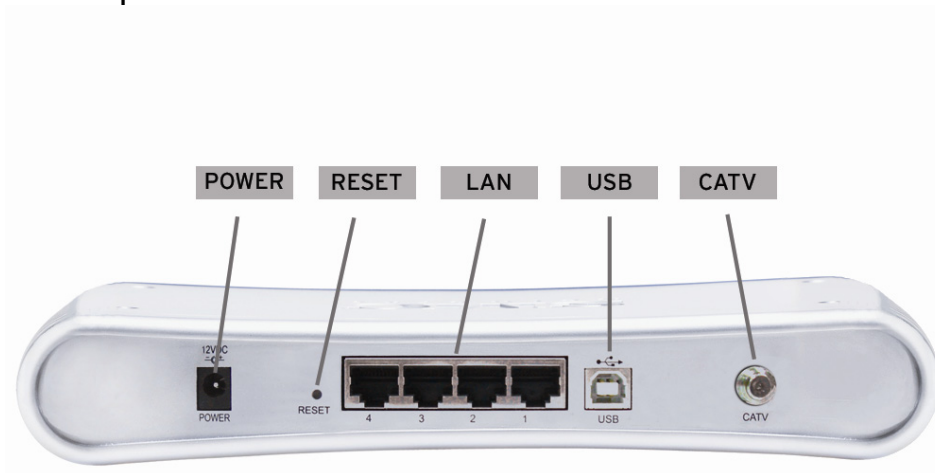
LED Indicators

The Gateway includes LED indicators on the front panel that simplify installation and network troubleshooting.



LABEL	LED COLOR	ON	FLASHING	OFF
Power	Green	Power is supplied to the Gateway	N/A	Power is not supplied to the Gateway
Diag	Amber	System Failure. Reboot Gateway	N/A	Normal Operation
Cable	Green	Successfully connected to cable network	Attempting to connect to network	N/A
Traffic	Green	Cable Modem has finished CMTS registration	Attempting to register with CMTS	N/A
LAN (1-4)	Green	Connected at 10 or 100 Mbps	Data transmitting	No Ethernet link detected
USB	Green	USB port connected	Data transmitting	No USB link detected

Rear Panel Description



Item	Description
Power	Connect the included power adapter to this port.
Reset	Use this button to reset the power or restore the default factory settings.
LAN 1-4	Four 10/100 Auto-sensing switch ports (RJ-45). Connect devices on your local area network to these ports (such as a PC, hub, or switch).
USB	Connect a USB Cable from your PC to this port.
CATV	Connect your cable line to this port.

Rebooting and Restoring the EZ Connect™ Cable Modem Gateway

The Reset button is located on the rear panel of the Gateway. Use a paper clip or a pencil tip to push the Reset button.

Reboot

If the Gateway is having problems connecting to the Internet, simply hold down the reset button for less than 2 seconds then release.

Restore Factory Defaults

If rebooting the Gateway does not resolve your issue, then you can follow these steps:

1. Leave power plugged into the Gateway.
2. Locate the reset button on the back panel, press and hold button for at least 10 seconds.
3. Release reset button.

CHAPTER 3 | Installation

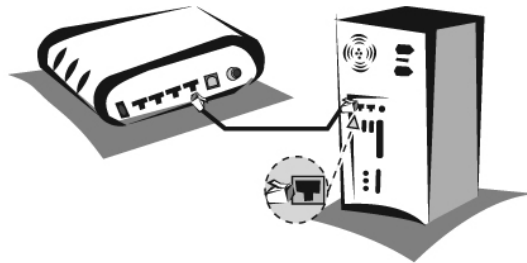
The EZ Connect™ Cable Modem Gateway can be installed in any location where you have cable Internet access, and your cable Internet service provider has approved the Gateway. To confirm you meet these 2 criteria points, please contact your cable operator.

For general installation please follow the guidelines outlined below to best performance:

- Keep the Gateway away from any heating devices.
- Do not place the Gateway in a dusty or wet environment.

Basic Installation Procedure

1. **Connect the LAN:** You can connect the Gateway to your PC, or to a hub or switch. Run Ethernet cable from one of the LAN ports on the rear of the Gateway to your computer's network adapter or to another network device. You can use either a standard straight through or cross over Ethernet cable since the Gateway incorporates Auto-MDI MDIX functionality.



2. **Connect the WAN:** Connect a coax cable to the CATV port on the back of the Gateway from a cable port located in your home. When connecting to the CATV port, use only manufactured coaxial patch cables with F-type connectors at both ends for all connections.

Note: If this modem was NOT installed by your cable provider (ISP) or is being used to replace another cable modem - please contact your Cable Operator to register the SMC8014. Without registering the modem with your cable operator it will be unable to connect to the cable network system.

3. **Power on:** Connect the power adapter to the Gateway.

Warning: Only use the power adapter that was provided with the Gateway, using another power adapter may damage your unit and void the warranty.

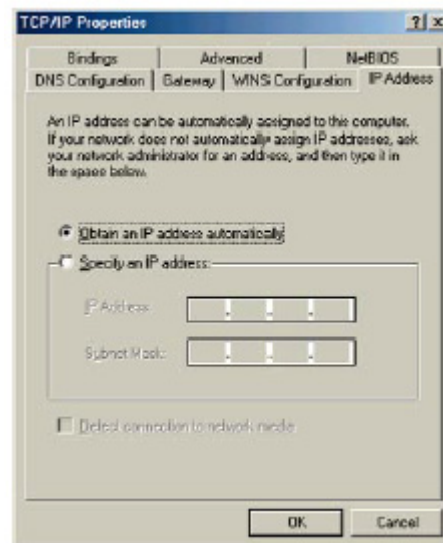
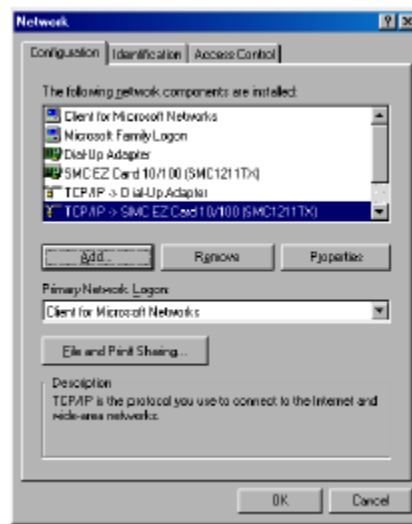
CHAPTER 4 | Configuring your Computer

The information outlined in this chapter will guide you through the configuration for the following Operating Systems:

- Windows 95/98
- Windows Me
- Windows 2000
- Windows XP
- Apple Macintosh

Configuring Windows 95/98/Me

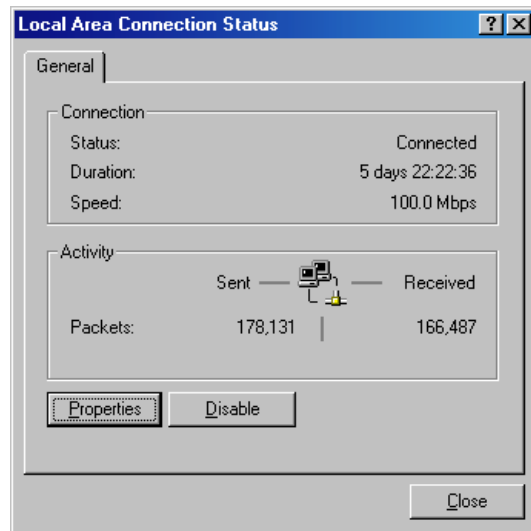
1. Access your Network settings by clicking [Start], choose [Settings], and then select [Control Panel].
2. In the Control Panel, locate and double-click the [Network] icon.
3. Highlight the TCP/IP line that has been assigned to your network card on the [Configuration] tab of the [Network] properties window. (see network dialog box to the right)
4. Next, click the [Properties] button to view that adapter's TCP/IP settings.
5. From the TCP/IP Properties dialog box, click the [Obtain an IP address automatically] option. (see TCP/IP dialog box to the right)
6. Next click on the [Gateway] tab and verify the Gateway field is blank. If there are IP addresses listed in the Gateway section, highlight each one and click [Remove] until the section is empty.
7. Click the [OK] button to close the TCP/IP Properties window.
8. On the Network Properties Window, click the [OK] button to save these new changes.



- NOTE:** Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, for example, D:\win98, D:\win9x. (Assume "D" is your CD-ROM drive).
9. Windows may prompt you to restart the PC. If so, click the [Yes] button. If Windows does not prompt you to restart your computer, do so anyways to ensure your settings.

Configuring Windows 2000

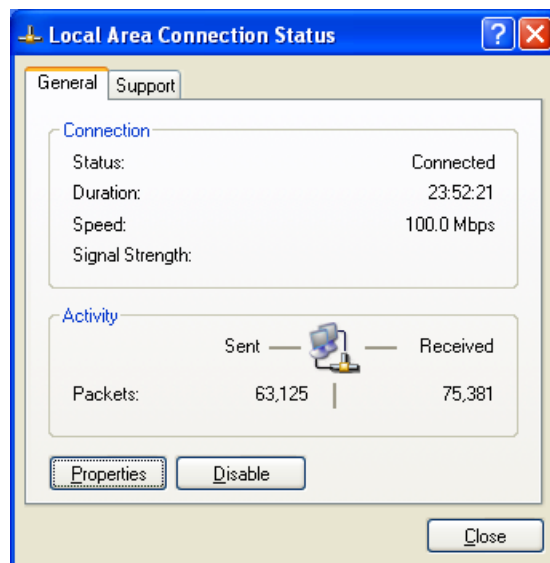
1. Access your Network settings by clicking [Start], choose [Settings], and then select [Control Panel]
2. In the Control Panel, locate and double-click the [Network and Dial-up Connections] icon
3. Locate and double-click the [Local Area Connection] icon for the Ethernet adapter that is connected to the Gateway. When the Status dialog box window opens, click the [Properties] button.
4. On the [Local Area Connection] Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
5. Select Obtain an IP address automatically to configure your computer for DHCP. Click the [OK] button to save this change and close the Properties window.
6. Click the [OK] button again to save these new changes.
7. Reboot your PC.



Configuring Windows XP

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000 outlined above.

1. Access your Network settings by clicking [Start], choose [Control Panel], select [Network and Internet Connections] and then click on the [Network Connections] icon.
2. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Gateway. Next, click the [Properties] button.
3. On the [Local Area Connection] Properties box, verify the box next to Internet Protocol (TCP/IP) is checked. Then highlight the Internet Protocol (TCP/IP), and click the Properties button.
4. Select Obtain an IP address automatically to configure your computer for DHCP. Click the [OK] button to save this change and close the Properties window.
5. Click the [OK] button again to save these new changes.

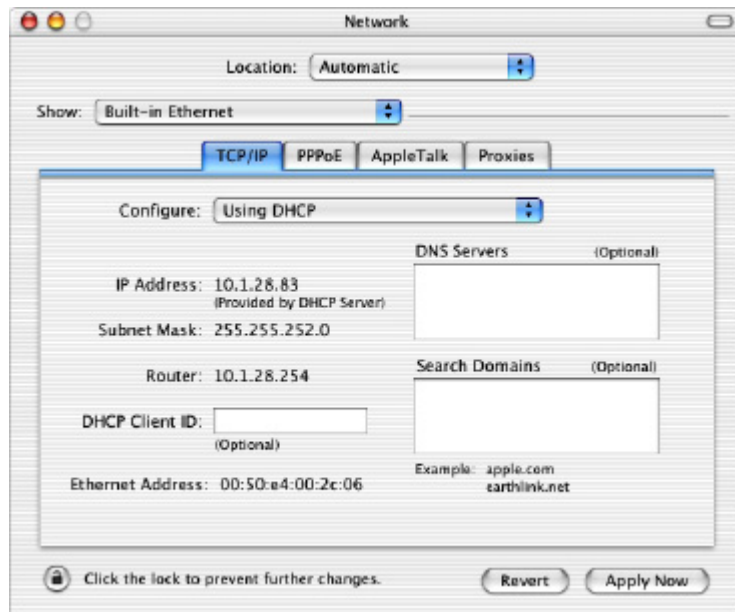


6. Reboot your PC.

Configuring a Macintosh Computer

You may find that the instructions here do not exactly match your screen. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 10.2.

1. Pull down the Apple Menu. Click System Preferences and select Network. Make sure that
2. Built-in Ethernet is selected in the Show field.
3. On the TCP/IP tab, select Using DHCP in the Configure field.
4. Close the TCP/IP dialog box.



CHAPTER 5 | Configuring the EZ Connect™ Cable Modem Gateway

After you have configured TCP/IP on a client computer, use a web browser to configure the EZ Connect™ Cable Modem Gateway. The Gateway can be configured by any Java-supported browser including Internet Explorer 5.0 or above, or Netscape Navigator 5.0 or above. Using the web management interface, you can configure the Gateway features and view its settings.

Before you attempt to log into the Gateway's Web-based Administration, please verify the following:

1. Your browser is configured properly. (see below)
2. Disable any firewall or security software that may be running.
3. Confirm that you have a [link] LED where your computer is plugged into the Gateway. If you don't have a [link] light, try another cable.

Browser Configuration

Confirm your browser is configured for a direct connection to the Internet using the Ethernet cable that is installed in the computer. This is configured through the options/preference section of your browser.

Disable Proxy Connection

You will also need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your web browser will be able to view the web-based configuration pages. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

Internet Explorer (5.0 or above)

1. Open Internet Explorer. Click [Tools], and then select [Internet Options].
2. In the [Internet Options] window, click the [Connections] tab.
3. Click the [LAN Settings] button.
4. Clear all the check boxes and click [OK] to save these LAN settings changes.
5. Click [OK] again to close the [Internet Options] window.

NOTE: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 is configured as follows: Under the menu "Tools/Internet Options/General/Temporary Internet Files/Settings," the setting for "Check for newer versions of stored pages" should be "Every visit to the page."

Netscape (5.0 or above)

1. Open Netscape. Click [Edit], and then select [Preferences].
2. In the [Preferences] window, under [Category], double-click [Advanced], then select the [Proxies] option.
3. Check [Direct connection to the Internet].
4. Click the [OK] button to save the changes.

Accessing the EZ Connect™ Cable Modem Gateway's Web Management

To access the EZ Connect™ Cable Modem Gateway's web-based management screens, follow the steps below:

1. Launch your web-browser.

NOTE: Your computer does not have to be ONLINE to configure the EZ Connect™ Cable Modem Gateway.

2. In the Address Bar, type: `http://192.168.0.1`



3. When the Gateway's Login screen appears, enter the default username and password, and click the [Login] button to access the Gateway.

A screenshot of a web-based login screen. The screen has a blue header with the text "LOGIN USER PASSWORD". Below the header, the text "Login Screen" is centered. There are two input fields: "Username:" and "Password:". Below the input fields are two buttons: "LOGIN" and "CANCEL".

User Login - for use by subscriber

USERNAME: cusadmin

PASSWORD: password

NOTE: Usernames and Passwords are case sensitive

4. Once you have logged into the Gateway's web-based admin screen, you have several options and features which can be configured.

All features available and how to configure each one is outlined in the next section **Chapter 6 | Navigating the Web-based Administration.**

CHAPTER 6 | Navigating the Web-based Administration

The EZ Connect™ Cable Modem Gateway's management interface allows you to configure both basic and advanced features and options. Some of these advanced functions include: hacker attack detection, IP and MAC address filtering, intrusion detection, port forwarding setup, virtual DMZ hosts, as well as other advanced functions.

Making Configuration Changes

Once a configuration change has been made on a page, be sure to click the [Apply] or [Next] button at the bottom of the page to enable the new setting.

SYSTEM

This section is used to configure the device mode and administration options including passwords and idle timeout setting.

To access the System Settings configuration page, on the Side Navigation bar, click on [System] link.

Password Settings

From this section you can configure new passwords for the [cusadmin] account.

You can also set the Idle Time Out value that the SMC8014 will keep an admin account logged in for. The default Idle Time Out value is 10 min.

To access the Password Settings configuration page, on the Side Navigation bar, click on [System] link and then click on the [Password Settings] link.

Password Settings

Set a password to restrict management access to the SMC8014WG. Also a timeout value could be set here for automatic logout if the page is not active for the timeout period.

- Current Password :
- New Password :
- Re-Enter Password for Verification :

• Idle Time Out : 10 Min

HELP APPLY CANCEL

If your password is lost, or you cannot gain access to the user interface, press the Reset button on the rear panel (holding it down for at least ten seconds) to restore the factory defaults.

LAN

From this section you can configure the following settings:

- The **PRIVATE** LAN IP settings, including IP Address, Subnet Mask, and Domain Name.
- Enable or Disable the integrated DHCP server
- Configure the DHCP Lease time for your DHCP clients

To access the LAN configuration page, on the Side Navigation bar, click on [LAN] link.

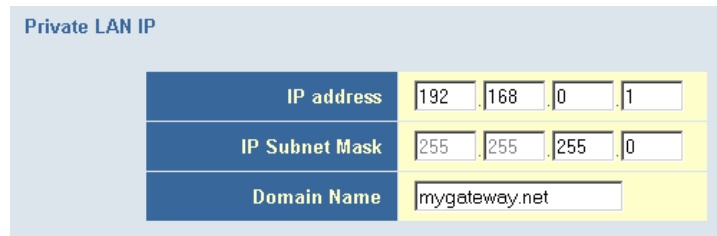
LAN IP

Use the LAN section to configure the LAN IP address for the Gateway and to enable the DHCP server for dynamic client address allocation. You can also configure the Lease Time for the DHCP clients on your network.

Private LAN IP Settings

Define the Gateway's private LAN settings. The IP address configured here is the Gateway's (default: 192.168.0.1).

NOTE: Port Forwarding and Access Control rules will be based on the network scope defined here. If either of these types of rules were previously setup and the Private LAN IP address is changed, then those rules will need to be recreated to reflect the new Private LAN IP network.

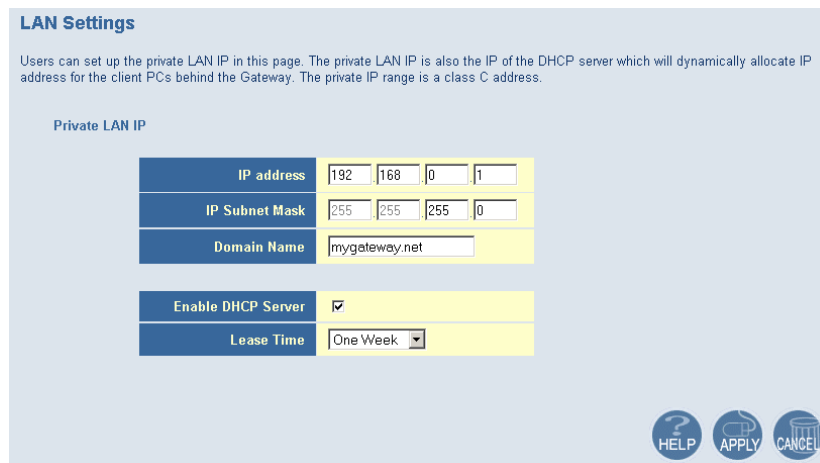


Private LAN IP

IP address	192	168	0	1
IP Subnet Mask	255	255	255	0
Domain Name	mygateway.net			

DHCP Server Settings

The Gateway's DHCP Server can be turned enabled/disabled here. Also the DHCP client Lease Time can be adjusted from the default One Week setting. The Gateway functions as a DNS proxy by default. DNS proxy can be disabled by configuring Primary and Secondary DNS values here, which LAN DHCP clients will receive in their lease.



LAN Settings

Users can set up the private LAN IP in this page. The private LAN IP is also the IP of the DHCP server which will dynamically allocate IP address for the client PCs behind the Gateway. The private IP range is a class C address.

Private LAN IP

IP address	192	168	0	1
IP Subnet Mask	255	255	255	0
Domain Name	mygateway.net			

Enable DHCP Server	<input checked="" type="checkbox"/>
Lease Time	One Week

HELP APPLY CANCEL

NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address.

Port Forwarding

The Gateway supports port forwarding that enables customers to host servers on their LAN. You can configure this feature to redirect the external service request to the appropriate internal server and port.

For example, if you are running a WEB server, you can configure all traffic on port 80 to be redirected to the IP address of the WEB server running on your network.

To access the Port Forwarding configuration page, on the Side Navigation bar, click on [NAT] link and then click on the [Port Forwarding] link.

This Port Forwarding function supports 2 types of Services:

- Predefined Service
- Customer Defined Service

Predefined Service

The Predefined Service option has a pull-down menu with several popular Service Applications, such as HTTP (80), FTP (20/21), and AIM/ICQ (5190).

To configure Port Forwarding with a Predefined Service rule, follow the steps below:

1. Select the [Service] that you want to have access through the firewall to your LAN from the pull-down menu.
2. Enter in the [LAN Server IP] for the LAN PC that is running this service or application
3. You can also configure [Remote IPs] option to allow access to this specific port from the WAN side. This can be configured for 3 different access types:
 - a. Any IP Address [Any] - choose this option to allow access from any public IP address.
 - b. Single IP Address [Single Address] - choose this option to only allow access from a single public IP address.
 - c. IP Address Range [Address Range] - choose the option to only allow a range of public IP addresses.
4. Click the [Apply] button to save your changes and return to the Port Forwarding main screen

Customer Defined Service Rule (Custom)

The Customer Defined Service section allows you to custom configure a Port Forwarding rule with any Traffic type (TCP/UDP/TCP and UDP), Public Port, and Private Port.

Customer Defined Service

Customer-defined service allows users to define their traffic type to be allowed-in from Internet.

Name	
Type	TCP
LAN Server IP	192.168.0.0
Remote IPs	Any
Start IP	0.0.0.0
End IP	0.0.0.0
Public IP Ports	Port Range
Start Public Port	
End Public Port	
Private Ports	<input type="checkbox"/> Enable Port Range

Back Apply Cancel

To configure this custom option, follow the steps below:

1. Enter in a Description [Name] for this custom setting
2. Configure the Traffic or Data [Type] that you want to forward. The options are *TCP* | *UDP* | *TCP/UDP*.
3. Set the [LAN Server IP] of the PC that you want this traffic/data redirected to
4. You can also configure [Remote IPs] option to limit access to this specific port from the WAN side. This can be configured for 3 different access types:
 - a. Any IP Address [Any] - choose this option to allow access from any public IP address.
 - b. Single IP Address [Single Address] - choose this option to only allow access from a single public IP address.
 - c. IP Address Range [Address Range] - choose the option to only allow a range of public IP addresses.
5. Set the [Start Public Port] and [End Public Port] that this application will use on the WAN (Internet) side. The Gateway will listen for incoming traffic/data to its WAN IP on these ports.
6. Set the [Private Ports] that the Gateway will forward this traffic to on the LAN. If there is a range of ports, enter the starting private port in [Private Ports], select [Enable Port Range] checkbox, and the Gateway will automatically calculate the end private port. The LAN PC server will listen for traffic/data on this/these ports.

Below is an example setting for a WEB server on an Internet connection, where port 80 is blocked from the WAN side, but port 8000 is available.

Name: Web Server
Type: TCP
LAN Server IP: 192.168.0.100
Remote IPs: Any (allow access to any public IP)
Public Port: 8000
Private Port: 80

With this configuration, all HTTP (Web) TCP traffic on port 8000 from any IP Address from the WAN side will be redirected through the firewall to the Internal Server (192.168.0.100) on port 80.

NOTE: This configuration is useful because you don't have to reconfigure your web server to accept traffic on a different port, you can do this configuration on the Gateway.

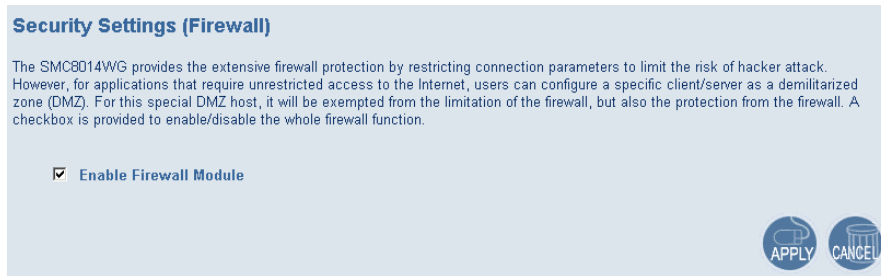
FIREWALL

The Gateway provides a stateful inspection firewall (SPI), which is designed to protect against Denial of Service (DoS) attacks. Its purpose is to allow a private local area network (LAN) to be securely connected to the Internet. To provide a flexible solution, the firewall section has the following features:

Firewall Enable/Disable

To access the Security Settings configuration page, on the Side Navigation bar, click on [Firewall] link.

To enable this feature, check the [Enable Firewall Module] checkbox.



Access Control

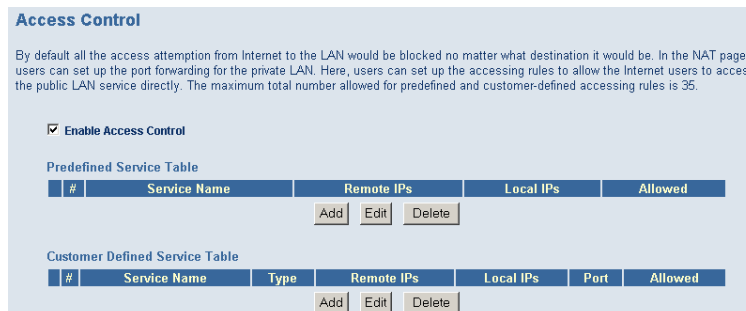
The Access Control section allows the setting of two types of rules: enable access to services on your *public LAN* network from the Internet or to block services on the *private LAN* from accessing the Internet. Access Rules can be configured to a specific LAN IP Address or a range of LAN IP Address's.

To access the Access Control configuration page, on the Side Navigation bar, click on [Firewall] link and then click on the [Access Control] link.

To enable this feature, check the [Enable Access Control] checkbox.

There are 2 sections in that can be configured for Access Control Rules.

The first section is used to configure the Access Rules for the Public LAN from the Internet. These rules will enable services on the public LAN to be accessed by the Internet.



The second section is used to configure Access Rules for the Private LAN to the Internet. These rules will block services on the private LAN to the Internet.

The following two tables allow users to define the traffic type not-permitted from LAN site to the Internet. This page includes predefined IP filtering and customer-defined IP filtering. The maximum total number allowed for predefined and customer-defined filters is 35.

Predefined Filtering Table

#	Service Name	LAN IPs	Blocked
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Customer Defined Filtering Table

#	Service Name	Type	LAN IPs	Port	Blocked
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					

For convenience, each Access Control section includes 2 filtering options:

- Predefined Filtering
- Customer Defined Filtering

Predefined Filtering Access Rule:

1. On the Side Navigation bar, click on [Firewall] then select [Access Control]
2. Under the Predefined Section, click on the [Add] button
3. On the Predefined Filter page, select the service that you want to block from the pull-down menu

Predefined Filter

Predefined filter allows users to choose the traffic type to be blocked from LAN site to the Internet.

Service	AIM/ICQ(TCP:5190)
LAN IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0

4. Select the [LAN IPs] that you want this access rule to apply to. You can choose to apply this rule to Any IP Address, a Single IP Address, or a Range of IP Addresses.
 - a. Any IP Address [Any] - choose this option to block all LAN clients. You don't need to configure the [Start IP] or [End IP] options.
 - b. Single IP Address [Single address] - choose this option to block a single LAN client. Enter the LAN IP address of the PC in the [Start IP] field.
 - c. IP Address Range [Address Range] - choose this option to block a range of LAN clients. Enter the starting LAN IP address in the [Start IP] field and the ending LAN IP address of the range you want in the [End IP] field.
5. When your configuration is complete, click the [Apply] button to save your changes and return to the main Access Control page.

Customer Defined Filtering Access Rule (Custom):

1. On the Side Navigation bar, click on [Firewall] then select [Access Control]
2. Under the Customer Defined Section, click on the [Add] button

3. On the Customer Defined Filter page, define a Name for the service/application that you want to block.

Name	<input type="text"/>
Type	TCP
LAN IPs	Any
Start IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
End IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
From Port	<input type="text"/>
To Port	<input type="text"/>

Back Apply Cancel

NOTE: The Name is only for reference purposes.

4. Then select the protocol type from the pull-down menu that they would like to block. The options are **TCP | UDP | TCP/UDP**.
5. Select the [LAN IPs] that you want this access rule to apply to. You can choose to apply this rule to Any IP Address, a Single IP Address, or a Range of IP Addresses.
 - a. Any IP Address [Any] - choose this option to block all LAN clients. You don't need to configure the [Start IP] or [End IP] options.
 - b. Single IP Address [Single address] - choose this option to block a single LAN client. Enter the LAN IP address of the PC in the [Start IP] field.
 - c. IP Address Range [Address Range] - choose this option to block a range of LAN clients. Enter the starting LAN IP address in the [Start IP] field and the ending LAN IP address of the range you want in the [End IP] field.
6. To complete the configuration enter in the [From Port] and [To Port] information will be blocked on the network.

NOTE: Usually every application has its own corresponding port number. Users should find out the correct port number from the application vendor. For example, if you are trying to block access to a Peer-2-Peer file sharing application then you should visit that applications web site to see the ports that application uses.

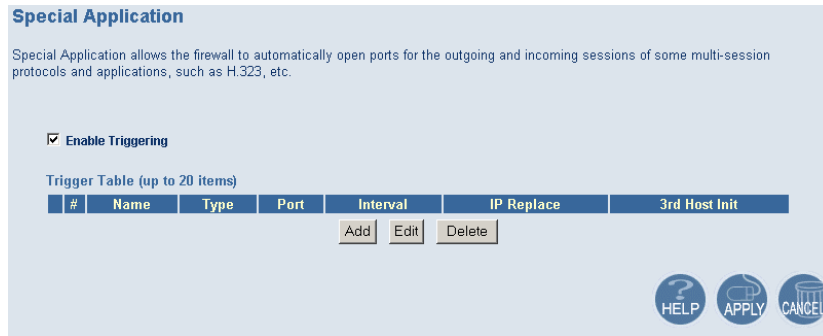
7. When your configuration is complete, click the [Apply] button to save your changes and return to the main Access Control page.

Special Application

Some applications, such as Internet gaming, videoconferencing, Internet telephony, and others require multiple connections. Rules are based on the port or range of ports that the application sends data to the server on (destination port). When the Gateway sees traffic sent to the configured port(s), it dynamically allows all incoming traffic from the server on any port for the specified time.

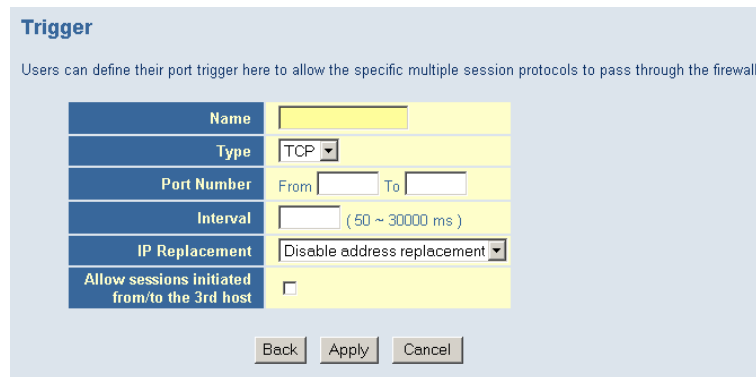
To access the Special Application configuration page, on the Side Navigation bar, click on [Firewall] link and then click on the [Special Application] link.

To enable this option, click the [Enable Triggering] checkbox.



To configure a Special Application Rule, follow the steps outlined below:

1. On the Side Navigation bar, click on [Firewall] then select [Special Application]
2. Click on the [Add] button on the Special Application page to access the [Trigger] configuration section.



3. Enter in the [Name] that you want to use for this rule.
4. In the [Type] pull-down menu, select the data/traffic type that this rule will apply to. The options are **TCP | UDP**.
5. Configure the [Port Number] that your application will be using as the outgoing trigger ports.
6. Set the [Interval] of the rule. This is the time in between the outgoing and incoming data traffic.

NOTE: If you set this value too low, the incoming ports will be closed before the return data arrives at the firewall and the connection will be broken and the application will not work.

7. The last 2 options are for Advanced Users, most users can leave this at the default settings:
 - IR Replacement - Default Setting: Disable address replacement
 - Allow sessions initiated from/to the 3rd host - Default Setting: unchecked
8. When your configuration is complete, click the [Apply] button to save your changes and return to the main Special Application page.

URL Blocking

This section allows you to control the content network. This feature is good for both business and parents looking to control the content accessible from a web browser.

To access the URL Blocking configuration page, on the Side Navigation bar, click on [Firewall] link and then click on the [URL Blocking] link.

To enable this option, click the [Enable Keyword Blocking] checkbox

URL Blocking

You can block access to certain Web sites from all internal PCs by entering either a full URL address or just a keyword of the Web site.

You also can specify a particular PC which will be exempted from the "URL Blocking" and allowed to have full access to all web sites.

Enable Keyword Blocking

Add exempted PC 0 0 0 0 0 0 **Add Trusted Host**

Exempted PC List (up to 10 hosts):

Delete **Clear All**

Keyword/Domain Name Type new Keyword/Domain here **Add Keyword**

Blocked Keyword/Domain Name List (up to 50 items):

Delete **Clear All**

To configure URL blocking, follow the steps outlined below:

1. On the Side Navigation bar, click on [Firewall] then select [URL Blocking]
2. Check the [Enable Keyword Blocking] checkbox to turn URL blocking on.
3. Enter in a new keyword or URL address that you want to block in the [Keyword/Domain Name] input box.
4. Press the [Add Keyword] button to save this keyword or URL.
5. The new keyword or URL address would be listed in the text box below.

NOTE: This list will support 50 Keywords or URLs.

If you want a PC on your network to bypass these rules you will need to set that PC as an Exempted PC/Trusted Host. To configure this option, check the [Add Trusted Host] option and enter the LAN IP address of the PC that you want to bypass the URL/Keyword blocking function with.

Schedule Rule

This feature will block Internet content based on the URL blocking function for PCs on your network based on the day and or time.

NOTE: The URL/Keyword blocking feature must be configured to use this schedule rule.

To access the Schedule Rule configuration page, on the Side Navigation bar, click on [Firewall] link and then click on the [Schedule Rule] link.

To enable this option, click the [Enable Schedule Function] checkbox.

Schedule Rule

This page defines the schedule rule you want to use with the "URL Blocking" page.

Week Day	
<input checked="" type="checkbox"/>	Every Day
<input checked="" type="checkbox"/>	Sunday
<input checked="" type="checkbox"/>	Monday
<input checked="" type="checkbox"/>	Tuesday
<input checked="" type="checkbox"/>	Wednesday
<input checked="" type="checkbox"/>	Thursday
<input checked="" type="checkbox"/>	Friday
<input checked="" type="checkbox"/>	Saturday

All Day

Start Time: 12 (hour) 0 (min) AM

End Time: 12 (hour) 0 (min) AM

HELP APPLY CANCEL

To configure Schedule Rules, follow the steps outlined below:

1. On the Side Navigation bar, click on [Firewall] then select [Schedule Rule]
2. In the [Week Day] table check the Days that you want to apply URL/Keyword Blocking.
3. Define the appropriate settings for a schedule rule.
4. Click the [OK] button to approve rule.
5. Then click the [APPLY] button to save your settings.

DMZ Host (Demilitarized Zone)

If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ host to this screen. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

To access the DMZ configuration page, on the Side Navigation bar, click on [Firewall] link and then click on the [DMZ] link.

To enable this option, click the [Enable DMZ Host] checkbox.

DMZ (Demilitarized Zone)

If you have a local client PC that cannot run an Internet application properly behind the NAT firewall, then you can set this client up to unrestricted two-way Internet access by setting it to be the Virtual DMZ Host. Please be careful since this setting is also meaning there is no protection for this host.

Enable DMZ Host: 192 168 0 .

HELP APPLY CANCEL

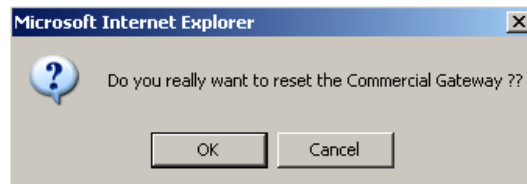
To configure a DMZ host, Enter in the LAN IP Address of the PC on your network in the input fields.

TOOLS

The Tools menu allows a user to Reboot the Gateway.

To reboot the Gateway, follow the steps below:

1. Click the [Apply] button
2. Click [OK] on the confirmation dialog box



3. The Gateway will reboot.

NOTE: The Reboot will be complete when the power LED stops blinking.

STATUS

The Status screen summarizes important information about the Gateway including WAN/LAN connection status, software version and hardware versions, and uptime statistics.

Status

You can use the Status screen to see the connection status for the SMC8014WG WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your SMC8014WG.

RG Functions: Enabled

Current Time: SAT JAN 01 21:30:07 2005 System Up Time: 000 days 21h:30m:24s

INTERNET WAN IP: 0.0.0.0 WAN Subnet Mask: 0.0.0.0 WAN Gateway IP: 0.0.0.0 Primary DNS: 0.0.0.0 Secondary DNS: 0.0.0.0	GATEWAY DHCP Gateway IP Address: 192.168.0.1 Subnet Mask: 255.255.255.0 DNS Proxy IP Address: 192.168.0.1	INFORMATION Software Version: 4.01.04-TWC Hardware Version: 1A RF Cable MAC Address: 00:13:F7:05:40:82 USB MAC Address: 00:13:F7:05:40:83 Wireless MAC Address: 00:13:F7:05:40:84 RG WAN MAC Address: 00:13:F7:05:40:86 Serial Num: 5007054082
---	--	---

WIRELESS SSID: WLAN Encryption Type: WEP Encryption length: 128 Bits Encryption Pass Phrase: Channel Being Used: 1	Interfaces Uptime and Traffic Count LAN Uptime: 21h:30m:24s ,Receiving 341772 bytes , Sending 1223621 bytes WAN Uptime: 21h:30m:24s ,Receiving 0 bytes , Sending 0 bytes
--	---

The Network Log shows both firewall and network activity.

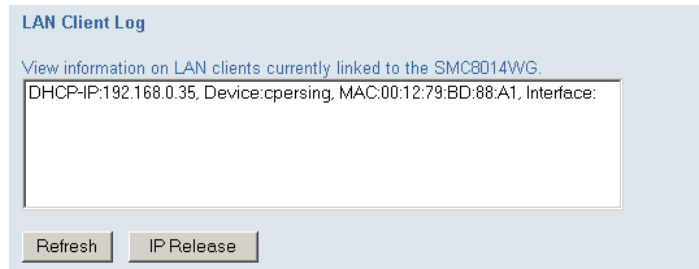
Network Log

View network activity and security logs.

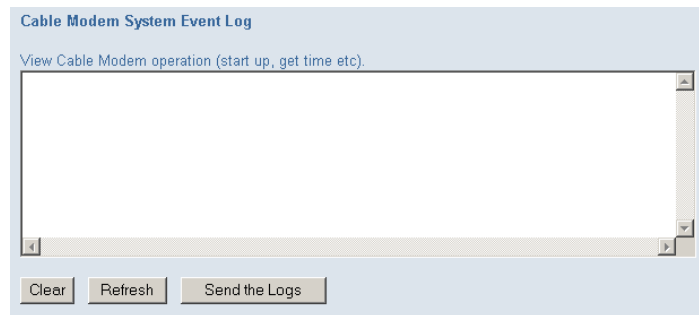
```
{1/1/05 04:19:14} 192.168.0.35 mso logout  
{1/1/05 04:19:18} 192.168.0.35 mso login
```

Clear Refresh Send the Logs

The LAN Client Log shows the clients connected to the Gateway and the type of connection. This also shows the IP address assigned to the client and the MAC Address of the client's network adapter.



The Cable Modem System Event Log shows diagnostic information about your connection and cable system.



The Cable Status page shows the users the initialization process the SMC8014 has been through, and also includes the information about the downstream channel and the upstream channel on which the modem is connected.

Cable Status

Cable status shows the users the cable initialization procedures, also the cable downstream and upstream status.

Initialization Procedure

Initialize Hardware	Success
Acquire Downstream Channel	Success
Upstream Ranging	Success
DHCP Bound	Success
Set Time-of-Day	Success
Downloading CM Config File	Success
Registration	Success

Traffic Enable!

Downstream Channel

Downstream Frequency	609000000 Hz
Lock Status	Locked
Modulation	64 QAM
Symbol Rate	5.056941 Msym/sec
Downstream Power	-2.2 dBmV
SNR	35.128 dB

Upstream Channel

Upstream Frequency	25000000 Hz
Lock Status	Locked
Modulation	QPSK
Symbol Rate	2560000 sym/sec
Upstream Power	48.2 dBmV
Channel ID	5

APPENDIX A | Telnet and SSH CLI Commands

Refer to the 8014 CLI document for command specifics.

APPENDIX B | Troubleshooting

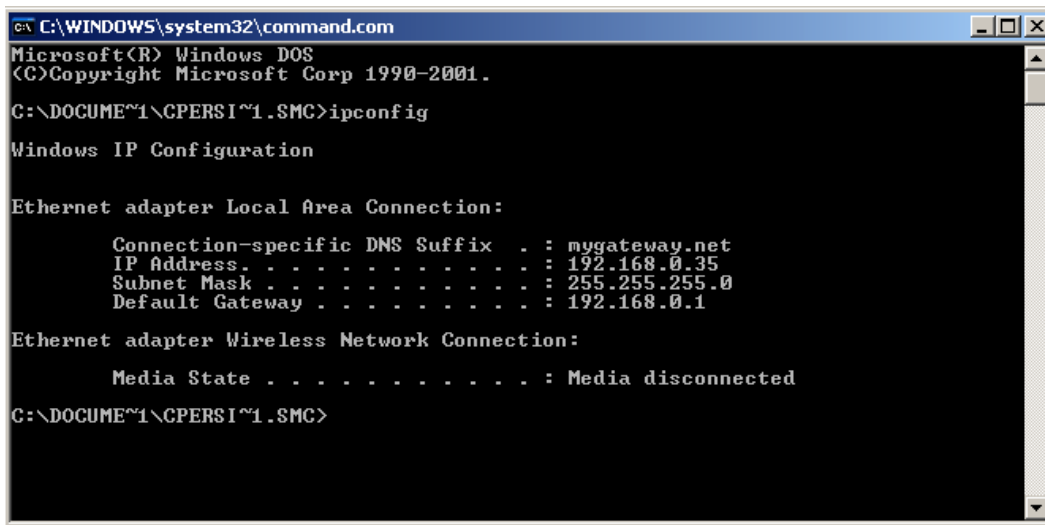
This appendix describes common problems you may encounter and possible solutions to them.

B.1 | Verify you are connected to the EZ Connect™ Cable Modem Gateway

If you are unable to access the Gateway's web-based administration pages, then you may not be properly connected or configured. The screen shots in this section were taken on a Windows 2000 machine, but the same steps will apply to Windows 95/98/Me/XP.

To determine your TCP/IP configuration status, please follow the steps below:

1. Click [Start] then choose [Run]
2. Type "cmd" or "command" (without the quotes) to open a DOS prompt.
3. In the DOS window, type "ipconfig" and verify the information that is displayed.
4. If your computer is setup for DHCP, then your TCP/IP configuration should be similar to the information displayed:
 - IP Address: 192.168.0.X (x is number between 100 and 199)
 - Subnet: 255.255.255.0
 - Gateway: 192.168.0.1



```
C:\WINDOWS\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\DOCUMENTS\CPERSI\1.SMC>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : mygateway.net
    IP Address. . . . .                : 192.168.0.35
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.0.1

Ethernet adapter Wireless Network Connection:

    Media State . . . . .              : Media disconnected

C:\DOCUMENTS\CPERSI\1.SMC>
```

If you have an IP address that starts with 169.254.XXX.XXX then see section A.2.

If you have another IP address configured, see section A.3.

B.2 | I am getting an IP Address that starts with 169.254.XXX.XXX

If you are getting this IP Address, then you need to check that you are properly connected to the EZ Connect™ Cable Modem Gateway.

Confirm that you have a good link light on the Gateway's port to which this computer is connected. If not, please try another cable.

If you have a good link light, please open up a DOS window as described in section A.1 and type "ipconfig /renew" (without the quotes)

If you are still unable to get an IP Address from the Gateway, reinstall your network adapter. If anti-virus software is running on your computer, disable it before reinstalling the network adapter. Please refer to your adapter manual for instructions.

B.3 | I have another IP Address displayed

If you have another IP address listed, then the PC may not be configured for a DHCP connection. Please refer to [Chapter 4 | Configure your Computer](#) for information.

Once you have confirmed your computer is configured for DHCP, follow the steps below.

1. Open a DOS window as described above.
2. Type "ipconfig /release" (without the quotes)

```
C:\WINDOWS\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~1\CPERSI~1.SMC>ipconfig /release

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its me
dia disconnected.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected

C:\DOCUME~1\CPERSI~1.SMC>_
```

3. Then type "ipconfig /renew" (without the quotes)

```
C:\WINDOWS\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~1\CPERSI~1.SMC>ipconfig /renew

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its me
dia disconnected.

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : mygateway.net
    IP Address . . . . . : 192.168.0.35
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected

C:\DOCUME~1\CPERSI~1.SMC>_
```

Once you are able to get a valid IP address from the Gateway, you can now access the web-based Administration pages.

If you still are not getting an IP address from the Gateway, please reset the hardware as outlined in [Chapter 2](#) and follow the steps outlined in this appendix again. Note: all configured

settings will be erased!

If you still cannot access the Gateway once you have reset it, please contact your cable operator for assistance.

B.4 | Pinging the EZ Connect™ Cable Modem Gateway

To verifying Your TCP/IP Connection is configured properly and you are able to access the EZ Connect™ Cable Modem Gateway's web-based management screens - you can use the 'Ping' command in DOS. To access the DOS dialog window please follow the steps below:

1. Click Start, then choose Run
2. Windows 98/Me users type "command" and click the [OK] button.
Windows 2000/XP users type "cmd" and click the [OK] button.
3. At the prompt, type: ping 10.1.10.1
After you click [enter] to execute the PING command you will get some information back, below is an outline of the possible return messages:

Good Connection

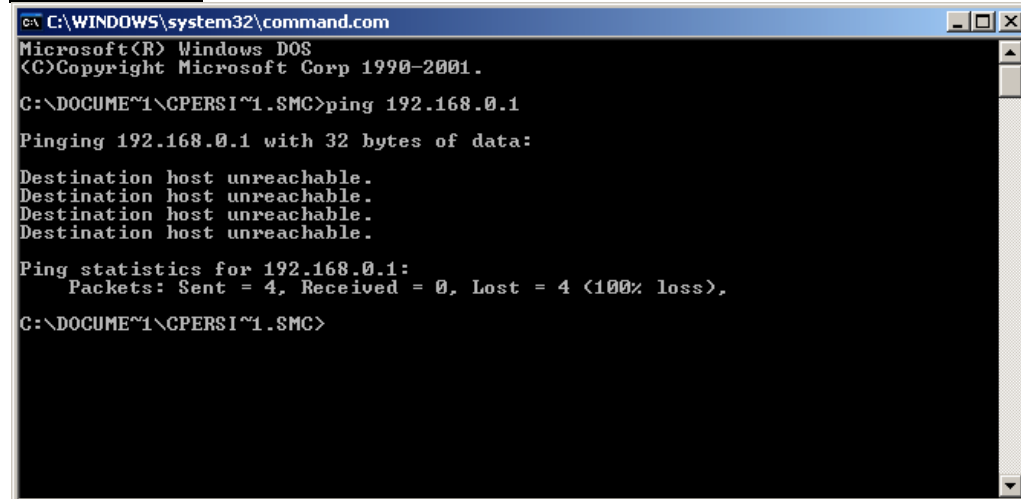
```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=48ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 48ms, Average = 12ms
```

Bad Connection



```
ca C:\WINDOWS\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\DOCUME~1\CPERSI~1.SMC>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\DOCUME~1\CPERSI~1.SMC>
```

There may be something wrong in your installation procedure. Check the following items in sequence:

1. Is the Ethernet cable correctly connected between the Gateway and the computer?
2. The LAN LED on the Gateway and the Link LED of the network card on your computer must be on.
3. Is TCP/IP properly configured on your computer?

B.5 | Symptom / Action Troubleshooting

The Gateway can be easily monitored through panel indicators to identify problems. Please refer to Chapter 2 - Section 2.0 | LED Definitions to confirm you have the correct LED status. If not, then refer to the symptoms and actions outlined below:

SYMPTOM: Power LED is Off

ACTION:

- Check connections between the Gateway, the external power supply, and the wall outlet.
- If the power indicator does not light when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply.
- If the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet.
- If you cannot isolate the problem, then the external power supply may be defective. In this case, contact your cable operator for assistance.

SYMPTOM: Diag LED is On

ACTION:

- Power Cycle the Gateway. Unplug the Gateway - wait 5 seconds - plug it back into power.
- If the Diag LED is still on, reset the hardware as outlined in Chapter 2 and power cycle the Gateway again.
- If this does not resolve your problem, contact your cable operator for assistance.

SYMPTOM: Cable LED is Off or Flashing

ACTION:

- Power Cycle the Gateway. Unplug the Gateway - wait 5 seconds - plug it back into power.
- Confirm your cable operator is not having network issues and the network is up and running.
- If you cannot isolate the problem contact your cable operator for assistance.

SYMPTOM: Cannot connect using the web browser

ACTION:

- Confirm that you are using a Java-supported browser such as Internet Explorer 5.0 or above, or Netscape Navigator 5.0 or above.
- Disable any firewall or security software that may be running on your PC.
- You will also need to verify that the “HTTP Proxy” feature of your web browser is disabled. Refer to **Chapter 5 | Configuring the EZ Connect™ Cable Modem Gateway** for more information.
- Check that you have a valid network connection to the Gateway.
- Check the network cabling between the management station and the Gateway.

SYMPTOM: Forgot or lost the password

ACTION:

- Contact your cable operator for assistance.

SYMPTOM: Internet users can not access my service/server hosted on a LAN computer

ACTION:

- Configure a Port Forwarding rule as described in the **NAT section of CHAPTER 6**.
- Contact your cable operator for assistance if you do not have this option available in your login.

SYMPTOM: My VPN, VoIP, multimedia, or other application is not working

ACTION:

- Configure a Special Application rule as described in the **Firewall section of CHAPTER 6.**
- Confirm that an Access Control (Port Filtering) rule is not blocking the ports used by the application. Refer to the **Firewall section of CHAPTER 6.**
- Contact your cable operator for assistance if you do not have this option available in your login.

APPENDIX C | Technical Specifications

Standards

- 802.3 10BaseT Ethernet
- 802.3u 100BaseTX Fast Ethernet
- 802.11g

WAN Interface

- F-type RF Connector

LAN Interfaces

- 4 - 10BASE-T/100BASE-TX RJ-45 ports
- 1 - USB 1.1 Type B Connector
- 1 - 801.11g Access Point

Wireless Interface

- 54Mbps IEEE 802.11g Wireless LAN
- WPA encryption
- 64/128 bit WEP encryption
- Auto data rate of: 54, 48, 36, 24, 18, 12, 9, 6 Mbps (802.11g) and 11, 5.5, 2, and 1 Mbps (802.11b)

Cable Modem Interface

- DOCSIS 1.1 and 2.0 RFI compliant
- 64/256QAM auto detection
- Supports maximum DOCSIS transfer rates
- Independent resets for downstream and upstream blocks
- Fragmentation and concatenation enabling

Networking

- IEEE 802.1d compliant bridging
- DHCP Client and Server
- DNS Relay
- ICMP, FTP/TFTP, and Telnet

Security

- Password protected configuration access
- Stateful Packet Inspection (SPI) Firewall
- Network Address Translation (NAT)
- Application Level Gateways (ALG)
- WPA and WEP encryption
- Wireless MAC filtering
- Disable SSID Broadcast
- Intrusion Detection logging
- Denial of Service (DoS) prevention
- Email Alerts

Management

- Browser-based management

Indicator Panel

- Power - Green
- Diagnostics - Green
- Cable - Green
- Traffic - Green
- WLAN - Green
- LAN (1-4) (10Mbps - Amber / 100 Mbps - Green)
- USB - Green

Dimensions

- 10.5" x 8" x 1.64"

Weight

- 1.35lbs

Input Power

- 12V/1.25A

Operating Environment

- Operating Temp. 0C to 40C (32F to 104F)
- Storage Temp. -20C to 70C (-4F to 158F)

Humidity

- 5% to 85% (non-condensing)

Compliances

- FCC Part 15B Class B
- FCC Part 68
- CD mark EN55024
- FCC Part 15C Class B
- CE Class B
- VCCI Class B
- CSA International
- UL

Warranty

- One-year

APPENDIX D | Compliances

FCC Interference Statement

This equipment has been tested and found to comply with 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B, and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the member states relation to electromagnetic compatibility.

Compliances

APPENDIX E | Technical Support

At this time, the SMC8014 is only distributed through cable operators. Contact your cable operator with any technical support needs you may have.

PHONE

From U.S.A. and Canada (24 hours a day, 7 days a week)

- (800) SMC-4-YOU
- (949) 679-8000
- Fax: (949) 679-1481

From Europe (8:00 AM - 5:30 PM UK Time)

- 44 (0) 118 974 8700
- Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:

- techsupport@smc.com
- european.techsupport@smc-europe.com

Driver updates:

- http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:

- <http://www.smc.com/>
- <http://www.smc-europe.com/>

SMC Networks, Inc.
38 Tesla
Irvine, CA
92618

Rev. 1.0 – 4.02.05-TWC

SMC8014