5354

Docsis 3.0 Cable Modem /Router with Wireless N User Manual

VER: 1.0

Contents

1	Safet	y Preca	utions	1
2	Over	view		2
	2.1	Appli	cation	2
	2.2	Featu	ıres	2
	2.3	Stand	dards Compatibility and Compliance	3
3	Hard	ware De	scription and Hardware Installation	4
	3.1	Hard	ware Description	4
		3.1.1	Front Panel	4
		3.1.2	Rear Panel	5
	3.2	Hard	ware Installation	5
		3.2.1	Connecting the Device	5
4	PC N	letwork (Configuration and Login	6
	4.1	PC N	etwork Configuration	6
	4.2	Logg	ing In to the 5354 Cable Modem	8
5	Web-	Based N	Management	9
	5.1	Statu	S	9
		5.1.1	Software	9
		5.1.2	Connection	10
		5.1.3	Security	11
		5.1.4	Diagnostics	11
	5.2	Basic	2	12
		5.2.1	Setup	13
		5.2.2	DHCP	15
		5.2.3	DHCPv6	16
		5.2.4	LAN IPv6	17
		5.2.5	DDNS	17
		5.2.6	Backup/Restore	
	5.3	Adva	nced	20
		5.3.1	Options	20
		5.3.2	IP Filtering	
		5.3.3	MAC Filtering	
		5.3.4	Port Filtering	

	5.3.5	Forwarding24
	5.3.6	Port Triggers
	5.3.7	DMZ Host
	5.3.8	RIP Setup
5.4	Firew	29
	5.4.1	Basic
	5.4.2	Event Log
5.5	Parer	ntal Control
	5.5.1	User Setup
	5.5.2	Basic
	5.5.3	ToD Filter
	5.5.4	Event Log
5.6	VPN	
	5.6.1	Basic
	5.6.2	IPsec
	5.6.3	L2TP/PPTP
	5.6.4	Event Log
5.7	Wirel	ess
	5.7.1	Radio
	5.7.2	Primary Network40
	5.7.2 5.7.3	Primary Network
	5.7.2 5.7.3 5.7.4	Primary Network
	5.7.2 5.7.3 5.7.4 5.7.5	Primary Network
	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6	Primary Network
	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7	Primary Network
	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8	Primary Network 40 Guest Network 43 Advanced 44 Access Control 46 WMM 47 Bridging 49 Media 49
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.6 5.7.7 5.7.8 USB	Primary Network 40 Guest Network 43 Advanced 44 Access Control. 46 WMM 47 Bridging. 49 Media 49
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8 USB 5.8.1	Primary Network 40 Guest Network 43 Advanced 44 Access Control 46 WMM 47 Bridging 49 Media 49 50 USB Basic 50
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8 USB 5.8.1 5.8.2	Primary Network 40 Guest Network 43 Advanced 44 Access Control. 46 WMM 47 Bridging 49 Media 49 S0 USB Basic. 50 Approved Devices. 51
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8 USB 5.8.1 5.8.2 5.8.3	Primary Network 40 Guest Network 43 Advanced 44 Access Control. 46 WMM 47 Bridging. 49 Media 49 Storage Basic 50 Storage Basic 52
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8 USB 5.8.1 5.8.2 5.8.3 5.8.4	Primary Network 40 Guest Network 43 Advanced 44 Access Control. 46 WMM 47 Bridging. 49 Media 49 Storage Basic 52 Storage Advanced 52
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8 USB 5.8.1 5.8.2 5.8.3 5.8.4 5.8.5	Primary Network40Guest Network43Advanced44Access Control.46WMM47Bridging49Media49Storage Basic50Storage Basic52Storage Advanced52Media Server53
5.8	5.7.2 5.7.3 5.7.4 5.7.5 5.7.6 5.7.7 5.7.8 USB 5.8.1 5.8.2 5.8.3 5.8.4 5.8.5 Logo	Primary Network 40 Guest Network 43 Advanced 44 Access Control. 46 WMM 47 Bridging. 49 Media 49 Storage Basic 50 Storage Advanced 52 Storage Advanced 52 Media Server 53 ut 54

ii

1 Safety Precautions

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause any power or fire risk.

- Do not place this device on an unstable surface or support.
- The screen of the coaxial cable is intended to be connected to earth in the building installation.

2 Overview

The 5354 is targeted towards DOCSIS/EuroDOCSIS3.0 cable modem, eMTA and gateway. With eight downstream channels and four upstream channels, it supports up to 400Mbs/160Mbs. The 5354 incorporates a variety of industry standard peripheral interfaces including dual IEEE802.3 10/100/1000Mbps interface, one with integrated GPHY, and dual USB2.0 interfaces(Host and Host/Device) with integrated PHYs. The 5354 supports WLAN access. It complies with IEEE 802.11,802.11b/g and 802.11n specifications, WEP, WPA, and WPA2 security specifications. The WLAN of the 5354 supports 2T2R.

2.1 Application

- Home gateway
- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

2.2 Features

- User-friendly GUI for web configuration
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Compatible with all standard Internet applications
- WLAN with high-speed data transfer rates of up to 300 Mbps, compatible with IEEE 802.11b/g/n, 2.4GHz compliant equipment
- IP routing and bridging
- Network/port address translation (NAT/PAT)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- File server for network attached storage (NAS) devices
- Web filtering

- Remote update
- System statistics and monitoring

2.3 Standards Compatibility and Compliance

- Support application level gateway (ALG)
- DOCSIS/EuroDOCSIS3.0
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

3 Hardware Description and Hardware Installation

3.1 Hardware Description

3.1.1 Front Panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description			
		On	The device is powered on and the device			
Power	Green		operates normally.			
		Off	The device is powered off.			
		On	CM has locked D/S frequency			
D/S	Green	Blink	CM scan D/S frequency			
		Off	Device is powered off.			
		On	CM has locked U/S frequency			
	Creat	Blink	CM is range and scan U/S frequency			
0/5	Green	0#	Device is powered off or CM scan D/S			
			frequency.			
		On	The Ethernet interface is connected.			
Ethernet 1/2/3/4	Green	Croon	Plink	Data is being transmitted through the		
		Blink	Ethernet interface.			
		Off	The Ethernet interface is disconnected.			
		On	WLAN is enabled.			
	Croon	Dlink	Data is being transmitted through the			
WLAN	Green	Blink	wireless interface.			
		Off	WLAN is disabled.			
		0.7	Connection succeeds under Wi-Fi			
		On	Protected Setup.			
WPS	Green	Dlink	Negotiation is in progress under Wi-Fi			
		Blink	Protected Setup.			
		Off	Wi-Fi Protected Setup is disabled.			
		0.7	The connection of USB flash disk has			
USB	Green	On	established.			
		Off	No signal is detected.			
•	•	. 4				

3.1.2 Rear Panel

Interface	Description
Antenna	The antenna interface, for connecting the antennas.
Cable	RF cable port, for connecting HFC cable.
Deast	Press the button for at least 1 second and then release it. System
Reset	restores the factory default settings.
	RJ-45 port, for connecting the router to a PC or another network
E(1) 4~1	device.
USB 0~1	USB port, for connecting other USB storage devices.
Power	Power interface, for connecting the power adapter.

The following table describes the interfaces or the buttons on the rear panel.

⚠ Warning:

Do not press the **Reset** button unless you want to clear the current settings. The **Reset** button is in a small circular hole on the rear panel. If you want to restore the default settings, please press the **Reset** button gently for 1 second with a fine needle inserted into the hole and then release the button. The system reboots and returns to the factory defaults.

3.2 Hardware Installation

3.2.1 Connecting the Device

Please follow the steps below to connect the device.

- Step1 Connect the Cable port of the CMRG with HFC cable.
- Step2 Connect the Eth port of the CMRG to the network card of the PC via an Ethernet cable.
- **Step3** Plug one end of the power adapter to the wall outlet and connect the other end to the **Power** port of the CMRG.

4 PC Network Configuration and Login

4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. 5354 provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

6

The following displays the TCP/IP Properties dialog box on Windows XP.

5354 Cable Modem User Manual

Internet	Protocol (TCP/IP) Pro	operties	? 🗙
General	Alternate Configuration		
You car this cap the app	n get IP settings assigned a Jability. Otherwise, you need ropriate IP settings.	utomatically if your network suppor d to ask your network administrator	ts for
🧿 O t	otain an IP address automa	tically	
OU	se the following IP address:		
IP ac	ddress:		
Subr	net mask:	47. 49. 14	
Defa	ult gateway:	+ + +	
📀 Ot	otain DNS server address a	utomatically	
OU	se the following DNS server	r addresses:	
Prefe	erred DNS server:	ter ter ter	
Alten	nate DNS server:	+. +. +	
		Advance	d
		ОК Са	ancel

Figure 1 IP and DNS configuration

TCP/IP configuration steps for Windows XP are as follows:

- Step1 Choose Start > Control Panel > Network Connections.
- Step2 Right-click the Ethernet connection icon and choose Properties.
- Step3 On the General tab, select the Internet Protocol (TCP/IP) component and click Properties.

- Step4 The Internet Protocol (TCP/IP) Properties window appears.
- Step5 Select the Obtain an IP address automatically radio button.

	5354 Cable Modem User Manual
Step6	Select the Obtain DNS server address automatically radio button.
Step7	Click OK to save the settings.
4.2 Lo	ogging In to the 5354 Cable Modem
To log in to	the 5354cable modem, do as follows:
Step1	Open a Web browser on your computer.
Step2	Enter http://192.168.100.1 (the default IP address of the 5354cable
	modem) in the address bar. The login page appears.
Step3	Enter the user name and the password. The default Username is admin
	and the Password is admin .
Step4	Click Login to log in to the 5354 cable Modem.
	Login
	Please enter username and password to login.

ocomun		
Password		
Login		

Figure 2 Login page

After logging in to the 5354 cable modem, you can query, configure, and modify all the settings, and diagnose the system.

5 Web-Based Management

This chapter describes how to use Web-based management of the Cable Modem, which allows you to configure and control all of cable modem residential gateway features and system parameters in a user-friendly GUI.

5.1 Status

Choose Status, and the submenus of Status are shown as below.



Figure 3 Submenus of status

5.1.1 Software

Choose Status > Software , and the following page appears.

Status	Basic Advanc	ed Firewall	Parental Control	VPN	Wireless	USB	Logo
	Status						
Software	Software						
1.170 March 1.17	Wall course discussion in						
Econection	This page displays in	ormation on the current s	ysiem sonware.				
	Information						
Security	Standard Specification C	ompliant DOCSIS 3.0					
	Hardware Version	V1.1					
Diagnostics	Software Version	5.5.10.2_RC					
	Cable Modern MAC Addr	ess bc 96/80.35/4f.b9					
	Cable Modern Serial Nurr	iber 354fb9					
	CM certificate	Installed					
	A CONTRACTOR OF THE OWNER	5.5.10mp3					
	Status						
	System Up Time	0 days 00h:07m:19s					
	Network Access	Denied					
	Cable Modern IP Address	1 10 1 10 1 10 1 10 1 10 1 10 10 10 10 1					
	10			_			
NAME AND DESCRIPTION OF	a loc. All contra reserved.						

Figure 4 Software page

This page displays information about the hardware version, software version, MAC address, cable modem IP address, serial number, system "up" time, and network registration status.

5.1.2 Connection

-Tear	Connection								
	This name displays info	mation about I	he connection	to the cable of	sharek				
wellion	una paga orapinta mo		in contraction	cito una courte in					
nutly J	a Pourter Provieloning M	lode allocte Du	alt fords						
	enouter Provisioning in	ious enous co							
gnostica 💦	Apply								
	Startup Procedure		-						
	Procedure	Status	Comment						
	Acquire Downstream Chan	nel 517000000 H	Sz Locked						
	Connectivity State	In Progress	IP complete						
	Boot State								
	Configuration File	In Progress							
	Security	Disabled	Disabled						
		100000000	care and sector						
	Downstream Bonded Chan	ncia					In the second		
	Channel Lock Status Modu	lation Channel I	D I requency	Power SN	RC	prrectable	Uncorrectables		
	1 QAM	256	5170000001	1z -7.6 dBmV 45.	5080		0		
	2 Units	own	0 Hz	0.0 dBm/ 0.0	00 0		0		
	S Unics	own	0 Hz	0.0 dBmi/ 0.0	00 0		0		
	a Uniter	own	D Hz	CONE-V CO			0		
	G Union	Sien .	0.14*	0.0 dBml/ 0.0	-0.0		0		
	7 Linko	own	0.14+	0.0 dBm// 0.0	AR 0		0		
	ð Unkn	own	0 Hz	0.0 dBm// 0.0	05 0		0		
	The second second second								
	Total Correctables Total U	ncorrectables							
	0 0								
		-	_	_	_	-			
	Channelli och Statuslits C	harmed Turnel("ht	annet ID Sund	ol Data Francis	men li	lower			
	1 ATCS	LA.	25601	Cavm/sec 210000	00 Hz	7.0 (thm//			
	2 Unko	own	D Key	Tulsec OHE	-	VmBb 0.0			
	3 Unkn	own	O Ksyl	m/sec OHz	1	VmBb 0.0			
	4 Union	own	0 Ksyl	m/sec 0 Hz	1	VmBb 0.0			
	and the second second	12 million							
	CM IP Address Duration D: - H: - M	Expires							
	DownStream Frequecy Sele	11		TUNE					
	Current System Time:								

Figure 5 Connection information

This page displays information about the RF upstream and downstream channels, including downstream channel frequencies, upstream channel IDs, and upstream and downstream signal power and modulation.

This page also displays IP lease information, including the current IP address of the cable modem, the duration of both leases, the expiration time of both leases, and the current system time from the DOCSIS timeserver.

The information on this page can be refreshed at any time by clicking your web browser's Refresh button.

5.1.3 Security

Choose Status > Connection and the following page appears.

Status	Basic Advanced Firewall Parental Control VPN Wireless USB Logout
	Status
Software	Security
Connection	This page allows configuration of administrative access privileges. This page also includes a button to restore the system to factory defaults.
Security	User Name Current Password
Diagnostics	New Password
	Re-Enter New Password
	Reboot O Yes No
	Restore Eactory Defaults O Yes No
	Apply
@2001-2014 Zoom Telephonics, In	nc. All rights reserved.

Figure 6 Security configuration

To restore factory defaults, select the Yes radio button and click Apply. This will cause the device to reset. The factory default password is "Broadcom" and is case sensitive.

Note that you can also change the security password from this page by entering a new password in both the New Password and Re-Enter New Password fields, and the current password in the Current User ID Password field. Clicking Apply will change the password. You do NOT have to restore factory defaults to change the password.

5.1.4 Diagnostics

Choose Status > Diagnostics and the following page appears.

Status	Basic Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
	Status						
	Disquesties						
Software	Diagnostics						
Connection	This page provides diagnostic	s to help with IF	connectivity problems.				
Contraction of the	Utāty Ping V						
- Kilo	Ping Test	Parameters					
Ovegnostics	Ping Size		64 bytes				
	No. of Pings		3				
	Ping Interval	10	00 ms				
	In an a bar and a second						
	Start rest whom rest Callar He	nuo l					
	Results						
	Waiting for input						
	There was an						

Figure 7 Diagnostic information

Two utilities are provided for troubleshooting network connectivity: Ping and Traceroute.

Ping allows you to check connectivity between the CMRG and devices on the LAN. Traceroute allows you to map the network path from the CMRG to a public host. Selecting Traceroute from the drop-down Utility list will present alternate controls for the traceroute utility: To run either utility, make any changes to the default parameters and select Start Test to begin. The window will automatically be refreshed as the results are displayed in the Results table.

5.2 Basic

Choose Basic and the submenus of Basic are shown as below.





Figure 8 Submenus of basic

5.2.1 Setup

Choose **Basic > Setup** , and the following page appears.

Status	Dasic	Advanced	Firewall	Parental Control	ALC: N	Wireless	050	Logout
	Basic							
Setup	Setup							
DIRP	Configure a	and view status of basic	network para	meters.				
		Neb	work Config	uration				
DHCPM	LAN		ante a constant					
LANDE		IPv6 Address	Unspeci	fied				
Dereve		IPv6 Prefix:	:					
DONS		IPv4 Address:	192	168 . 0 . 1				
		MAC Address	bc:96:80):35:4f:bd				
Backup Restore	Interface/Pr	refix						
		None Specified						
	WAN							
		IPv6 Address	Unspeci	fied				
		IPv4 Address		-				
		MAC Address:	bc:96:80):35:4f:bb				
		Duration	D: H: -	M: S:				
		Expires						
		IPv6 DNS Servers	None					
		The second se						
		Nelease WA	N Lease Her	How WAN Lease				
		WAN Conr	nection Type	DHCP V				
		Ipv4 MTU Size	0	(600-1500 octets, 0 =)	use default)			
		Spoofed MAC Add	tress 00 ‡	00 2 00 2 00	:00 :00			
			Apply					
			headerstand					

Figure 9 Setup configuration

Enter the information from the Required Information section as indicated: 1.If your ISP uses DHCP, select "DHCP" for the WAN Connection Type, and enter Host Name and Domain name if required. OR

4	2
L	3

If your ISP uses static IP addressing, select "Static IP" for the WAN Connection Type, and enter the information provided by your ISP for Static IP Address, Static IP Mask, Default Gateway, Primary DNS, and Secondary DNS.

2.Enter a unicast MAC address in the Spoofed MAC Address field. Your ISP may require this to be your PC's MAC address. If not, you can simply supply the WAN side MAC address of the router as your CPE and leave the spoofed MAC address entry set to all 0's, since there will be no spoofing required.

3.Select the Apply button. This will reset the CMRG.

At this point, the CMRG is configured for basic use. To connect to the Internet, you must do the following:

1.Power up the CMRG and wait for it to register with the CMTS and obtain an Internet-routable IP address

2.Get an IP lease from the internal DHCP server for each PC attached to the CMRG.

Note that communication on the LAN will work regardless of whether the WAN connection provided by the cable modem is up. However, you will not be able to access the Internet until the WAN connection is enabled and has an IP address.

Some configurations settings are retrieved only once from non-volatile storage when the CMRG first powers up. One such setting is changing the Static WAN IP address parameters. Any changes to these settings will force the CMRG to reset so that the new configuration can be read from non-volatile storage.

When this mandatory reset is required, the web interface will notify as follows:

5354 Cable Modem User Manual



Figure 10 Reload page

Simply wait for the modem to reboot and click on the "Refresh" link to re-enter the web interface where you made your last change.

Most configuration items may be changed on the fly without a reboot.

5.2.2 DHCP

Choose **Basic > DHCP**, and the following page appears.



Figure 11 DHCP configuration

This page allows configuration and status of the optional internal DHCP server for the LAN.

If you have your own DHCP server servicing the LAN side (or choose to "hardcode" all of your PC's IP addresses), you can disable the internal DHCP server by selecting the No radio button. If you do this, make sure the IP address assigned to the CMRG is on the same subnet as the external DHCP server (the subnet mask is always 255.255.255.255.0), or you won't be able to access the CMRG from the LAN. The IP address of the CMRG can be set from the Basic Setup page.

You can also set the starting IP address for IP leases available to the LAN, and change the number of PCs supported on the LAN. In the case above, addresses 192.168.0.2 through 192.168.0.9 can be used as hard-coded IP addresses with no fear of IP address conflict with the DHCP pool. Configured WINS server addresses can also be passed to CPEs behind the CMRG via DHCP.

5.2.3 DHCPv6

Choose Basic > DHCPv6 , and the following page appears.

Status	Basic Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
	Basic						
Setup	DhcpV6						
0100	This page allows configuration Prefix first, and press Apply st	on of the internal so that the system	DhcpV6 server for the L n can calculate its LAN	AN. When modi Delegated Prefo	ifying the System Del x.	egated Prefix, set	the System Delegat
LAN IPHS	System Delegated Prefix						
DONS Backup/Restore	Server Settings LAN Delegated Prefix will be of Enabled @ LAN Delegated Prefix Start Address Number of addresses 256 Valid Lifetime 3600 Enable Rapid Commt @ Enable Rapid Commt @ Enable Stateless Dhcpv6 Apply Restore Dhcpv6 Detaut	lerived from Syst	em Delegated Prefix an	d Start Address	will have the same p	refor as the LAN C	belegated Prefix.

Figure 12 DHCPv6 configuration

This page allows configuration of the internal DhcpV6 server for the LAN. When modifying the System Delegated Prefix, set the System Delegated Prefix first, and press Apply so that the system can calculate its LAN Delegated Prefix.

5.2.4 LAN IPv6

Choose Basic > LAN IPv6 , and the following page appears.

Status	Basic Advanced	Firewall Parental Control	VPN V	fireless	USB 1	ogout
	Basic					
Setup	LAN IPv6					
DHCP	This page displays information	related to IPv6 on the LAN.				
C DICPUS	Stateless Auto Configuration					
C LAN IPVS						
DONS						
Backup/Restore						
	N. Al colds research					

Figure 13 LAN IPv6 information

This page displays information related to IPv6 on the LAN.

5.2.5 DDNS

Choose Basic > DDNS , and the following page appears.

Figure 14 DDNS setup

This page is used to configure DDNS. Dynamic DNS (DDNS) allows a dynamic IP address to be aliased to a static, pre-defined host name so that the host can be

easily contacted by other hosts on the internet even if its IP address changes. The CMRG supports a dynamic DNS client compatible with the Dynamic DNS service (<u>http://www.dyndns.com/</u>).

To activate the DDNS client:

1. Go to the DynDNS website and create an account for the Dynamic DNS service. You will create a username and password, and be asked to choose a host name for your server, and the dynamic DNS domain to which your host will be assigned. You will also be asked for your host's current IP address. This is the WAN IP address that has been assigned to your CMRG during provisioning. (See WAN IP Address on the Basic / Setup web page.)

2. Enter your account information on the Basic / DDNS web page, enable the service by selecting www.DynDNS.org from the DDNS Service drop-down list, and click Apply.

3. The DDNS client will notify the DDNS service whenever the WAN IP address changes so that your chosen host name will be resolved properly by inquiring hosts. The current status of the service is shown at the bottom of the DDNS web page.

5.2.6 Backup/Restore

Choose Basic > Backup/Restore and the following page appears.

Setup	Basic Backup/Restore Settings
CHICP DHCP	This page allows you to save your current settings locally on your PC, or restore settings previously saved.
O DIGPH	MR Restore Backup
LANIPH	
DONS	
Backup/Restore	

Figure 15 Backup/Restore setup

In this page, you can save the current CMRG configuration settings to a local PC. You can then later restore these settings if you need restore a particular configuration, or to recover from changes you may have made that have had an undesirable effect.

To backup the current configuration, click Backup and follow the prompts.

5354 Cable Modem User Manual

To restore a previous configuration, click Browse and use the navigation window to locate the file. (Usually GatewaySettings.bin, unless you rename it before saving.) Once the file has been located, click Restore to restore the settings. Note that once the settings are restored, the device will reboot.

5.3 Advanced

Choose Advanced and the submenus of Advanced are shown as below.

Figure 16 Submenus of advanced

5.3.1 Options

Choose **Advanced > Options** to display the following page.

5354 Cable Modem User Manual

Options	
This page allows configuration of advance	ed features of the cable modern's router.
WAN Blocking	2 Enable
Ipsec PassThrough	Enable
PPTP PassThrough	Enable
Remote Config Management	D Enable
Multicast Enable	₽ Enable
UPnP Enable	Enable Enable
Primary Network Bridged	C Enable
PassThrough Mar Addresses (example il	1-23-45-67-89-4B)
Add Max Addresses (Maniple, 0	123300100700
Addresses entered: 0	V32
Remove Mac Address Clear All	
NAT ALC State	16
RSVP	G Enable
FTP	Q Enable
TETP	R Frahla
Kerb88	St Enable
NotBos	2 Enable
IKE	R Enable
RTSP	R Enable
Kerb1293	P Enable
H225	2 Enable
PPTP	C Enable
MSN	P Enable
cip	C Enchin
ICO	2 Enable
IDOSES	Q Enable
ICOT all	Q Eaching
Net2Dhone	C Cratte
IDC7000	So Enable
1001000	S Endole
INCOUR	SC ETHIONE

Figure 17 Options configuration

This page allows you to configure the accessible features. To enable a feature, click the appropriate check box until it is "checked". When you are satisfied with your selections, click on the Apply button. These features can be modified on the fly without a system reset.

"WAN Blocking" prevents the CMRG or the PCs behind it from being visible to the WAN. For instance, pings to the CMRG's WAN IP address or the PCs behind it are not returned. Therefore, it will be more difficult for hacker to discover your WAN IP address to begin an attack on your private LAN.

"IpSec" and "PPTP" (Point-to-Point Tunneling Protocol) pass-through modes enable these protocols to be used through the CMRG such that a VPN device (or software) may communicate properly with the WAN.

"Remote Configuration Management" allows the CMRG to be administered (configured) from the WAN via surfing to the WAN IP address on port 8080 of the CMRG from anywhere on the Internet (e.g. at the browser URL window enter http://WanIPAddress:8080/ to access the CMRG remotely).

"Multicast Enable" allows multicast specific traffic (denoted by a multicast specific

address) to be passed to and from the PC's on the private network behind the CMRG. "UPnP Enable" enables the UPnP agent in the CMRG. If you are running a CPE application that requires UPnP, check this box.

5.3.2 IP Filtering

Choose **Advanced > IP Filtering** to display the following page.

		Advanced		
	Options	IP Filtering		
	IP Filling	Enter LAN IP A	ddresses to block	raffic that co
-	HICCO.		IP Filtering	
	More Fallering	Start Address	End Address	Enabled
-	Port Fillering	192.168.0.0	192.168.0.0	
		192.168.0.0	192.168.0.0	
-	Forwarding	192.168.0.0	192.168.0.0	
-	Port Trimmers	192.168.0.0	192.168.0.0	
	a de la companya de la	192.168.0.0	192.168.0.0	
-	DM2 Host	192.168.0.0	192.168.0.0	
-	OIP Setup	192.168.0.0	192.168.0.0	
-		192.168.0.0	192.168.0.0	
		192.168.0.0	192.168.0.0	
		192.168.0.0	192.168.0.0	0
		Line and the second sec	Apply	
			Tuesday 1	

Figure 18 IP Filtering configuration

This page allows you to configure the CMRG to prevent local PCs from getting access to the WAN by specifying those IP addresses that should be filtered.

By entering starting and ending IP address ranges, you can configure which local PCs are denied access to the WAN. Note that you only need to enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the CMRG IP address. To activate the IP address filter, you must also check the "enable" box and click apply. The enable box allows you to store filter settings commonly used but not have them active.

5.3.3 MAC Filtering

Choose Advanced > MAC Filtering to display the following page.

5354 Cable Modem User Manual

Figure 19 MAC filtering configuration

This page is used to prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC address

This is useful for the fact that the MAC address of a specific NIC card never changes, unlike its IP address which can be assigned via DHCP server or hard-coded to various addresses over time.

5.3.4 Port Filtering

Choose Advanced > Port Filtering to display the following page.

	Advanced		
	Port Filtering		
EP Fallering	Enter destination ports to block outgoin are blocked.	ig traffic addressed to those ports. This can be used to block ac	cess to Internet service
MAC Fillening	Port Filtering		
Dest research	Start Port End Port Protocol Enabled		
- Certification	1 65535 Both 🗸 🗋		
Lorwarding	1 65535 Both 🗸 🗌		
NAMES OF A DESCRIPTION OF	1 65535 Both 🗸 🗌		
Port Inggers	1 65535 Both 🗸 🗌		
DMZ Host	1 65535 Both 🗸 🗌		
	1 66535 Both 🗸 🗌		
RCP Setup	1 65535 Both 🛩 🗌		
	1 66535 Both 🗸 🗌		
	1 65535 Both 🗸 🗌		
	1 65535 Both -		
	Apply		

Figure 20 Port Filtering configuration

This page is used to prevent PCs from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers.

By specifying a starting and ending port range, you may determine what TCP/UDP traffic is allowed out to the WAN on a per-port basis. Note the specified port ranges are blocked for ALL PCs and this setting is not IP address or MAC address specific. For instance, if you would like to block all PCs on the private LAN from accessing HTTP sites (or "web surfing"), you would set the "Start Port" to 80, the "End Port" to 80, the "Protocol" to TCP, check the "Enabled" box, and click Apply.

5.3.5 Forwarding

Status	Dasic Advanceo Prewan Parenan Control VPA miletess 0.55 Logout
	Advanced
Options	Forwarding
C P Filtering	Forwarding allows requests from the public Internet to reach specific devices on your private network or LAN. Such devices may include web FTP servers, mail servers, etc. Enter the IP Addresses and ports of devices and applications that you want to forward to. You may optionally of
MAC Filtering	Addresses of External devices on the public Internet, doing so will restrict access to those devices only. If you enter no External device Addre any device on the public Internet may access your devices. Click Create Rule to save your forwarding configuration.
Port Editoring	Application Part
Forwarding	Create IPv6 Rule Create IPv6 Rule 877 25
Port Inggers	Popp 110 Not7P 110 Local External Televi 22
OM2 Host	IP Address Start Port End Port Address Start Port End Port Prod Description Enabled Remove All Remove All
RIP Selup	Whith 40 Hubbert 407 LLAP 249
	0007 60
Same and the second second	

Figure 21 Forwarding

This allows for incoming requests on specific port numbers to reach web servers, FTP servers, mail servers, etc. so they can be accessible from the public internet. A table of commonly used port numbers is also provided.

Forwarding allows you to run a publicly accessible server on the LAN by specifying the mapping of TCP/UDP ports to a local PC

To specify a mapping, you must enter the range of port numbers that should be forwarded locally, and the IP address to which traffic to those ports should be sent. If only a single port specification is desired, enter the same port number in the "start" and "end" locations for that IP address. A table of commonly used Port numbers is supplied on the page for convenience.

If both external and Local/internal port numbers are present, the Local port number is a mandatory field and the external port number is optional. If the external port number is used, the RG will perform a translation from external port number to internal port number.

5.3.6 Port Triggers

Choose Advanced > Port Triggers to display the following page.

Figure 22 Port Triggers

Port Triggers are similar to Port Forwarding except that they are not static ports held open all the time. When the CMRG detects outgoing data on a specific IP port number set in the "Trigger Range", the resulting ports set in the "Target Range" are opened for incoming (or sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the "Trigger Range" ports for 10 minutes, the "Target Range" ports will close. This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.

5.3.7 DMZ Host

Choose Advanced > DMZ Host to display the following page.

Figure 23 DMZ Host setup

DMZ (De-militarized Zone) hosting (also commonly referred to as "Exposed Host") allows you to specify the "default" recipient of WAN traffic that NAT is unable to translate to a known local PC. This can also be described as a computer or small sub-network that sits between the trusted internal private LAN, and the untrusted public Internet.

You may configure one PC to be the DMZ host. This setting is generally used for PC's using "problem" applications that use random port numbers and do not function correctly with specific port triggers or port forwarding setups mentioned earlier. If a specific PC is set as a DMZ Host, remember to set this back to "0" when finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

5.3.8 RIP Setup

Choose Advanced > RIP Setup to display the following page.

Options IP Faltering MAC Faltering	Advanced Routing Information Pro This page allows configuration automatically identifies and use	of RIP	Setup paramet	ers rela vn and e	ted to authe	ntication, te to any	destinati given der	ion IP Ad	dress, sut Address,	bnet mas	k, and rep	orting inter	vals. RIP
Pott I storing	RIP Enable RIP Authentication		able able	_									
Part Tragers	RIP Authentication Key ID RIP Reporting Interval	0	secon	cfs									
C DMZ Host	RIP Destination IP Address RIP Destination IP Subnet Mask	0	265	0	= 0 - 0								
100° Senap		pply											

Figure 24 RIP Setup

²⁶

RIP (Router Information Protocol) is used in WAN networks to identify and use the best known and quickest route to given destination addresses to help reduce network congestion and delays.

NOTE: RIP messaging will only be sent upstream when running in Static IP Addressing mode on the Basic – Setup page. You must enable Static IP Addressing and the set the Wan IP network information! RIP is normally a function that is tightly controlled via the ISP. RIP Authentication Keys and IDs are normally held as secret information from the end user to prevent unauthorized RIP settings.

RIP is a protocol that requires negotiation from both sides of the network (i.e. CMRG and CMTS). The ISP would normally set this up because of their knowledge of their CMTS settings to match the configuration in the CMRG.

To enable the CMRG to perform RIP, do the following (this example uses BRCMV2 as the RIP Authentication Key and 1 as the Key ID):

1.) To turn on RIP MD5 Authentication, check the "Enable" box.

2.) To specify a RIP MD5 Authentication Key String, type "BRCMV2" for this example. key name = a string value to match CMTS key name value

3.) To specify a RIP MD5 Auth Key ID, type "1"

key number = a number to match the CMTS key number value

4.) To change the RIP annoucement interval, type in a number in seconds.reporting interval by default = 30 seconds

5.) To specify a RIP unicast destination IP address, enter the IP address and subnet mask.

To enable the CMTS for RIPv2 with MD-5 authentication (Cisco uBR example shown below):

1.) The following steps go through configuring RIPv2 for a Cisco CMTS. The network number used in this configuration will vary from network to network so use the network number that matches your set-up.

7223#configure terminal

7223(config)#key chain ubr

7223(config-keychain)#key 1

7223(config-keychain-key)#key-str BRCMV2

7223(config-keychain-key)#exit

7223(config-keychain)#exit

7223(config)#router rip

7223(config-router)#ver 2

7223(config-router)#no validate-update

7223(config-router)#passive-interface cable 2/0

7223(config-router)#network 10.0.0.0

7223(config-router)#exit

7223(config)#inter cable 2/0

7223(config-if)#ip rip receive ver 2

7223(config-if)#ip rip authentication mode md5

7223(config-if)#ip rip authentication key-chain ubr

7223(config-if)#exit

7223(config)#exit

In this example, we have named the key chain 'ubr'. This was chosen arbitrarily. You can use any name you like as long as you specify the correct name when specifying which key chain to use for RIPv2 authentication.

2.) The next step is enable RIP debugging to ensure that the CMTS is receiving and authenticating messages from the residential gateway.

7223#debug ip rip

RIP protocol debugging is on

7223#term mon

The CMTS is now configured to accept RIPv2 messages. If the CMRG is registered on the CMTS, you should see messages that are similar to the message below:

00:28:41: RIP: received packet with MD5 authentication

00:28:41: RIP: received v2 update from 10.24.81.148 on Cable2/0

00:28:41: 10.24.81.0/24 via 10.24.81.148 in 1 hops

The CMRG has broadcast that is connected to the network 10.24.81.0/24 through the interface 10.24.81.148. This information is not very useful to the CMTS because it already knows that the network 10.24.81.0/24 is connected directly to one of its interfaces (Cable2/0). It ignores this message and doesn't add any information to the IP routing table. Here is the IP routing table after the CMTS has received RIPv2 messages:

7223#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

- * candidate default, U per-user static route, o ODR
- P periodic downloaded static route

Gateway of last resort is 10.24.95.17 to network 0.0.0.0

- 10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
 - C 10.24.80.0/24 is directly connected, Cable2/0
 - C 10.24.81.0/24 is directly connected, Cable2/0
 - C 10.24.95.16/28 is directly connected, FastEthernet0/0
 - S* 0.0.0.0/0 [1/0] via 10.24.95.17

In the example above, the CMRG was set up to send RIPv2 messages to the CMTS.

The CMTS was also set up to receive these messages.

5.4 Firewall

Choose Firewall and the submenus of Firewall are shown as below.

Figure 25 submenus of Firewall

5.4.1 Basic

Choose Firewall > Basic to display the following page.

This page is used to block or exclusively allow different types of data through the CMRG from the WAN to the LAN.

5354 Cable Modem User Manual

Statun	Basic Advanced F	rewall Parental Control	VPN Win	oless USB	Logout
	Firewall				
Base	Basic				
EventLog	Select the desired Firewall Protection disable local and remote logging. Clin	a level, and enable extra features ck Apply to save changes.	via the checkboxes as de	sired. Note that turning Firev	vall Protection Off will
		Allowed S	rvices		
	IPv4 Firewall Protection IPv6 Firewall Protection On ♥	No Ports Restricted			
	Block Fragmented IP Packets Enal	ble			
	Port Scan Detection	ble			
	IP Flood Detection	ble			
	Apply				

Figure 26 Basic configuration

The "low" setting does not block any services/ports, however it does protect against invalid packets and well known attacks. The "medium" setting will cause the firewall to drop a packet unless it is on a specific port of allowed services, The allowed services are listed on the same page. The "high" setting is similar to "medium", but allows access to even fewer services. The "off" setting allows all traffic to pass.

Block Fragmented IP packets prevents all fragmented IP packets from passing through the firewall. Port Scan Detection detects and blocks port scan activity originating on both the LAN and WAN. IP Flood Detection detects and blocks packet floods originating on both the LAN and WAN. The Apply button must be clicked in order to activate any of the checkbox items. All of these settings can be activated on-the-fly without a CMRG reboot.

5.4.2 Event Log

Choose Firewall > Event Log to display the following page.

5354 Cable Modem User Manual

Status	Besic Advanced	Firewall	Parental Control	VPN	Wireless	U\$8	Logout
	Firewall						
Base	Event Log						
Eventing	Configure the router to log a re events that you want logged a the email address and SMTP that you can view the most ree	ecord of events t nd/or you want t information when cent entries of th	to a local sysLog server to be warned about. Server re you want warnings to e log information you h	on your LAN, a cond, enter the be sent, if appl ave selected at	ind/or set up email al address of your local licable. Finally, click / the bottom of the pag	erts to warn of the SysLog server, if \pply for the settin le	events. First, select the you have one. Third, enter gs to take effect. Note
	Send selected events Permitted Connections Blocked Connections Blocked Connections Product Configuration Event to SysLog server at 192.168.0. Contact Email Address SMTP Server Name SMTP Deswerd E-mail Alerts	s o Enab	le				
	Description Court Last Occurrent	in Target Bource					
	E-mail Log Clear Log						
	and the second sec						

Figure 27 Event Log configuration

Configure the router to log a record of events to a local sysLog server on your LAN, and/or set up email alerts to warn of the events. First, select the events that you want logged and/or you want to be warned about. Second, enter the address of your local SysLog server, if you have one. Third, enter the email address and SMTP information where you want warnings to be sent, if applicable. Finally, click Apply for the settings to take effect. Note that you can view the most recent entries of the log information you have selected at the bottom of the page.

5.5 **Parental Control**

Choose Parental Control and the submenus of Parental Control are shown as below.

Figure 28 Submenus of Parental Control

5.5.1 User Setup

Choose VPN > Basic to display the following page.

	Parental Control
Unite Service	User Setup
Teo Fitter	Add users who will be affected by Parental Control, and assign Policies to these users. (See Basic page). The White List Only feature limits th to those sales specified in the Alaxwed Domain List of the Policy you have assigned to tim or her. Click the Add User and Remove User buffor appropriate lower Changes.
Count Link	User Configuration
	Add User
	User Settings
	1. Default - Enable Remove User
	Password
	Re-Enter Password
	Trusted User Enable
	Content Rule White List Access Only 1. Default V
	Time Access Rule
	Session Duration 0 min
	Inactivity time 0 min
	Acoly
	Trusted Computers Optionality, the user profile displayed above can be assigned to a computer to bypass the Parental Control login on that computer to b computer computers Bit Trusted Computers Hemove

Figure 29 User Setup

Add users who will be affected by Parental Control, and assign Policies to these users. (See Basic page). The White List Only feature limits the user to those sites specified in the Allowed Domain List of the Policy you have assigned to him or her. Click the Add User and Remove User buttons as appropriate to save changes.

5.5.2 Basic

Choose Parental Control > Basic to display the following page.

Status	Basic Advanced	Firewall Pares	ntal Control VPN	Wireless	usa	Logout
	Parental Control					
Unit Setup	Basic Setup					
000	Make rules to block access t and Remove Policy buttons	o certain web sites, and all as appropriate to save char	w access to others. Do this b iges. Click your browser's Ref	y defining one or mo fresh bullion to see th	re Policies. Click to the currently active	he Apply, Add New Policy settings
ToD Fitter	Parental Control Activation 1	This box must be checked to	o turn on Parental Control DE	nable Parental Cont	rol Apply	
Event Log	Content Policy Conf Asi New Content Policy List	guration Poley				
	Keyword List anonymizer	Blocked Domain List anonymizer.com	Allowed Domain List			
	Add Keyword	Add Domain	Add Allowed	Dumain		
	Ramove Keyword	Remove Domain	Remove Adowed Domain	are and		
	Override Password If you encounter a blocked we Password Re-Enter Password Access Duration Acress Duration	bshe, you can overside the	block by entering the followin	g password		

Figure 30 Basic configuration

Make rules to block access to certain web sites, and allow access to others. Do this by defining one or more Policies. Click the Apply, Add New Policy and Remove Policy buttons as appropriate to save changes. Click your browser's Refresh button to see the currently active settings.

5.5.3 ToD Filter

Choose Parental Control > ToD Filter and the following page will be shown.

	Parental Control
User Setup	Time of Day Access Policy
Basic	Create a policy or policies to block all Internet access on certain days and/or times of day.
TOD Filler	Time Access Policy Configuration
EventLog	Create a new policy by giving it a descriptive name, such as "Weekend" or "Working Hours" Add New Policy.
	Time Access Policy List Time Access Policy List Time Access Policy List Exergidant State Stat

- -

Figure 31 ToD Filter configuration

Create a policy or policies to block all Internet access on certain days and/or times of day.

5.5.4 Event Log

Choose Parental Control > Event Log and the page will be shown as below.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
	Parent	al Control						
User Setup	Event L	og						
Uasic	This page	displays the Parent	tal Control event	log				
ToO Filter	Last Occur	rence Action Target L	iser Bource					
EventLog	Clear Log							
Committee of								
			_					

Figure 32 Event Log information

This page displays the Parental Control event log.

5.6 VPN

Choose VPN and the submenus of VPN are shown as below.

Figure 33 Submenus of VPN

5.6.1 Basic

Choose **VPN > Basic** to display the following page.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	058	Logout
	VPN							
time	Basic							
Con Parce 1	This page a	llows you to enab	le VPN protocols	s and manage VPN tunne	als.			
LZTEMPTP	L2TP / PPTF L2TP Server	Disabled Y						
EventLog	Configure	Distances -						
	IPsec IPsec Endpoi	nt Disabled V						
		Nam	ne	Status		Control		Configure
	Add New Tur	wei.		and the second second		2141 (24:224)		and the second
		Coroccal .						
	Sector Contractor							

Figure 34 Basic settings

This page will show the status of configured tunnels .To start the process of manually adding a new tunnel , select the "Add New Tunnel" button.

5.6.2 IPsec

Choose **VPN > IPsec** to display the following page.

5354 Cable Modem User Manual

Status	Basic Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
	VPN						
	VIII						
Dasie	IPsec						
	This capp allows configuration	of IDeac tunnels					
IParc .	This page allows conliguration	OF IF SEC TOURIES.					
100 million	Tunnel	Tunnel list is EMPTY	~	Delete Tunnel			
Lander	Name	(mull)		Add New Tunnel			
EventLog	2	Disabled ¥		Apply			
	Local endpoint settings						
	Address group type	IP subnet					
	Subnet	192.168.0.0	and the second second				
	Mask	255.255.255.	0				
	Identity type	IP address	~				
	Identity	(null)					
	Remote endpoint settings	marine and					
	Address group type	IP subnet					
	Subnet	0 <u>40 40</u>					
	hitesk	o Ho Ho	Hol				
	Identity type	IP BOORESS		-			
	Network address type	UP address	~				
	Remote Address	0000	1000				
	IPsec settings						
	Pre-shared key	(null)					
	Phase 1 DH group	Group 1 (768 bits)	~				
	Phase 1 encryption	DES ¥	3				
	Phase 1 authentication	MD5 Y					
	Phase 1 SA lifetime	o seco	nds				
	Phase 2 encryption	DES 👻					
	Phase 2 authentication	MD5 Y					
	Phase 2 SA lifetime	o seco	nds				
	Show Advanced Settings						
	Apply						
		_		_	_	_	_

Figure 35 IPsec

In this page, you are allowed to configure all aspects of the IPSec tunnel.

5.6.3 L2TP/PPTP

Choose VPN > L2TP/PPTP to display the page below.

Status	Basic	Advanced	Firewall	Parentai Co	intro1	VPN	Witchess	0.88	Logout
	VPN								
Basic	Basic								
IPsec	This page allo	ws configuration	of L2TP and Pl	PTP server op	lions				
	PPP Address Ri	ange							
LETPOPTP		Start	10	0 0	1				
EventLog	PPP Security	End	10	0.0	254				
	Users Usernam Password Confirm P User List User List L2TP Server Pre	MPPE End	[]	~					

Figure 36 L2TP/PPTP setting This page allows configuration of L2TP and PPTP server options.

5.6.4 Event Log

Choose **VPN > Event Log** to display the following page.

210101	Dasic Advanced Filewan Parenal Control VIA Mileess 0.50 Logout
	And a second
	VPN
lissic D	Event Log
Piec	This page allows you to view the VPN Event Log.
Latepptp	Time
	Event log is empty.
EventLop	Refresh Clear
excellencial from Learning in	ic. Al forth interved
and and the second s	

Figure 37 Event Log information

This page allows you to view the VPN Event Log.

5.7 Wireless

Choose Wireless and the submenus of Wireless are shown as below.

Figure 38 The submenus of Wireless

5.7.1 Radio

Choose Wireless > Radio to display the following page.

SERION	base Advanced Filewall Parental Control VPN WHOLES USB Logout
	Wireless
Radio	802.11 Radio
	Change of the set of the COD of a Darks and dark the shared and the Circle And in some shares.
Primary Network	Change settings for the 602 11 Foldo, including the channel number. Click Apply to save changes.
Guest Network	Wireless Interfaces: 00:90 4C 64 4A 19 V
	Output Power 100% V
Advanced	802.11 Band 2.4 GHz V Current: 2.4 GHz
Access Control	802.11 n-mode Off V
WMM	Sideband for Control Channel (40 Mhz only) None 🛩
	Control Channel Current: 1 ***Interference Level: Acceptable
Undging	Regulatory Mode Off
Media	OBSS Coexistence 1 Enabled
	STBC Tx Auto V
	Apply Restore Wireless Defaults
	Scan Wireless APs

Figure 39 Radio setting

This page allows configuration of the physical parameters of your wireless network. The MAC address of the wireless interface is displayed at the top of the page.

Wireless:

Allows the wireless interface to be enabled and disabled.

Output Power:

Control the range of the AP by adjusting the radio output power.

802.11 Band:

Select whether the radio operates in the 2.4 GHz or 5 GHz band. There may be less interference from other wireless networks and household devices in the 5 GHz band, but 802.11b/g devices will not be able to connect.

802.11 n-mode:

Switch this to Off to force the AP to operate in 802.11g mode.

802.11 N Support Required:

If the 802.11 N support required field is set to "on", then only .n capable stations are allowed to associate with the CM. If it's set to "off" then b/g/n are all allowed. **Bandwidth:**

802.11b/g channels are only 20 MHz wide, but 802.11n channels may be 40 MHz wide. There are some backward compatibility issues with 40 MHz channels though. These issues are more likely to be encountered in the 2.4 GHz band where legacy (802.11b/g) devices may be operating using 20 MHz channels.

Sideband for Control Channel (40 MHz only):

Whether the 20 MHz control channel uses the upper or lower half of the 40 MHz channel. Changes to this setting may change the control channel setting. For example (in the 2.4 GHz band), if the upper 20 MHz is selected as the sideband for the control channel, then the lowest control channel available would be channel 5 to allow the lower 20 MHz for data.

Regulatory Mode:

Selects either 802.11d or 802.11h modes of operation. These are amendments to the 802.11 specifications for solving interference issues with other transmission systems such as satellite or radar, and also transmission requirements in different parts of the world.

TPC Mitigation (dB):

Transmit Power Control mitigation factor in dB. Transmit Power Control is used to automatically reduce the transmission power when other networks are within range. This setting is only used when the Regulatory Mode is set to 802.11h.

OBSS Coexistence:

Enable/Disable Overlapping BSS Coexisistence. OBSS coexistence refers to the ability of the AP to support 20 MHz devices within 40 MHz channels. It also allows the AP to better deal with nearby 20 MHz devices that are interfering with part of its 40 MHz channel.

STBC Tx:

STBC :Space Time Block Code. Switch to on will obtain the full antenna gain. Scan Wireless AP's:

Force the Modems Access Point to scan for other AP's within receive range. Apply:

When any of the above settings are changed, the Apply button must be clicked in order to activate them.

5.7.2 Primary Network

Choose Wireless > Primary Network to display the following page.

The second second second				
Wireless				
802 11 Primar	v Network			
	,			
Configure the wir	eless Primary Network and	d its security settings.		
NAME OF TAXABLE PARTY.	XXXX (00:90:4C:64:	4A:19)		
Prima	ry Network Enabled 🛩		Automatic Security	Configuration
Network Na	me (SSID) xxx		WP8 Y	
Close	ed Network Disabled V		WPS Config State: Conf	figured
Mode	e Required None V		The physical button on the AP an provision wireless clients using	
	AP Isolate Disabled V		WI-Fi Protected Setup (VIPS)	
	WPA Desibled		Device Name Broad	romAP
ng J	WPA-PSK Enabled		Defice Hume Lorono	CONTRACT
	WPA2 Disabled		WPS Setup AP	
	VPA2-PSK [Enabled]		UUID 48493782769	e05ada393d92ea8690cd
WPANPA2	Encountion AES		PIN: 12345670	Generate AP PIN
WPA Pre-S	hared Key	Show Key	Configure by Externa	al Registrar Allow 🛩
RADI	US Server Dooo	-		
RA	DIUS Port 1812		WPS Add Client	
R	ADIUS Key		Add a client via PBC	or PIN Add
			have is equivalent to pushing the	WPS ballen an
Group Key Rotat	on Interval		yeur cable modern/router. After i activate VIPS in a silent (o.g. a F	doking the Add button; IC or tablet)
WPA/WPA2 Re-at	uth Interval 3600		that supports WPS to propagate	the security settings.
			Then press the Add butter to pr	opagate the security settings.
WEP	Encryption Disabled	1	Client PIN:	
Net	work Key 1	Show Key	Authorized Client M/	VC
Net	work Key 2			
Net	work Key 3			
Net	work Key 4			
Current Ne	etwork Key			
P	assPhrase	Generate WEP Keyt		
	Apply			

Figure 40 Primary Network configuration

40

This page allow you to configure the Primary Wireless Network.

Primary Network:

Enable or Disable the primary network. Guest networks may still be operational when the primary network is disabled.

Network Name (SSID):

Sets the Network Name (also known as SSID) of the primary network. This is a 1-32 ASCII character string.

Closed Network:

The Network Name is not broadcast by the AP in a Closed Network. Therefore, only clients who already know the network name will be able to connect.

WPA:

Wi-Fi Protected Access is a slightly older and less secure algorithm for securing a wireless network. This is the Enterprise variant that requires configuration of a RADIUS server.

WPA-PSK:

The Pre-Shared Key mode of the WPA algorithm which does not require use of a RADIUS server. This is also known as WPA Personal. WPA and WPA-PSK cannot be used at the same time.

WPA2:

An advanced form of WPA that is more secure. This is the Enterprise mode of WPA2 which requires the use of a RADIUS server. WPA2 and WPA may be used at the same time to provide backward compatibility with devices that do not support WPA2.

WPA2-PSK:

The Pre-Shared Key mode of WPA2, also known as WPA2 Personal. WPA2 and WPA2-PSK cannot be used at the same time. WPA2-PSK and WPA-PSK may be used at the same time to provide backward compatibility with devices that do not support WPA2.

WPA/WPA2 Encryption:

When using any of the WPA authentication schemes, AES, or TKIP + AES encryption modes can be set. AES provides the strongest encryption, while TKIP provides strong encryption with improved backward compatibility. The TKIP + AES mode allows both TKIP and AES-capable clients to connect.

WPA Pre-Shared Key:

Sets the WPA Pre-Shared Key (PSK). This is an 8-63 ASCII character string, or a 64-digit hex number. Enabled when the Network Authentication method is WPA-PSK or WPA2-PSK.

RADIUS Server:

Sets the IP address of the RADIUS server to use for client authentication. The RADIUS server may be on either the public network (WAN) or private network (LAN). This is only for WPA or WPA2 (Enterprise) modes.

RADIUS Port:

Sets the UDP port number of the RADIUS server. The default is 1812.

RADIUS Key:

Sets the shared secret for the RADIUS connection. The key is a 0 to 255 character ASCII string.

Group Key Rotation Interval:

The rotation interval in seconds indicating how often transmission keys should be rotated. Set to zero to disable periodic rekeying.

WPA/WPA2 Re-auth Interval:

This value indicates how often a station using Enterprise security needs to contact the RADIUS server.

WEP Encryption:

Sets the WEP encryption mode. Both 64-bit and 128-bit WEP encryption modes are supported. When running Shared Key or 802.1x authentication, WEP encryption must be enabled. WEP encryption cannot be used at the same time as WPA or WPA2.

Network Key 1 thru Network Key 4:

When WEP encryption is enabled, sets the static WEP keys. Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key. Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

Current Network Key:

When WEP encryption is enabled, selects the encryption (transmit) key.

PassPhrase:

Sets the text to use for WEP key generation.

Generate WEP Keys:

When WEP encryption is enabled, this action button converts the passphrase entered to a set of WEP keys. Remember to click the Apply button to save the keys.

Automatic Security Configuration

Wi-Fi Protected Setup (WPS);

WPS is the standard method to achieve the same goal as Broadcom's SES. The protocol is described in a specification issued by the Wi-Fi Alliance.

Device Name:

The name of the device that will advertised to wireless stations.

WPS Setup AP:

Set the PIN and click the 'Configure' button in this section when using an External Registrar.

WPS Add Client:

Add a new wireless client using the Internal Registrar. Choose to add either by push-button or PIN method and then click the 'Add' button.

5.7.3 Guest Network

Choose Wireless > Guest Network to display the following page.

Status	Basic Advanced	Firewall	Parental Control	VPN	Wireless	058	Logout
	Wireless						
	NAMES AND ADDRESS OF ADDRESS						
Radio	802.11 Guest Network						
Dimare Haberet	This page allows configuration	of one or more gu	est networks.				
	Gue	st Network BROAD	COM GUEST 0 0 (02:90.4)	-64 (A 1A) 🗸			
Gaest Network	Guest W	Fi Security Settin	05	Gu	est LAN Settings		
	Guest Network	nabled 🛩		Net	work Guest ~		
Advanced	Guest Network Name (SSID)	ROADCOM_GUEST_	0_0	IP Add	tress 192.168.1.1		
Access Control	Closed Network	isabled V		Subnet I	Mask 255 255 255.0		
	Mode Required N	Ione V		Lease Pool	Start 192 168 1 10		
WMM	AP Isolate	Disabled 💙		Lease Pool	End 192.168.1.99		
	WPA	lisabled 🗸		Lease	Time (86400		
Bridging	WPA-PSK	isabled V		UPpP Er	able Enabled		
and the second second	WPA2	V beidani		Firewall Er	able Disabled V		
	WPA2-PSK	nabled 💌		DHCPv6 S	erver Enabled V		
					Apply		
	WPA/WPA2 Encryption	ES V		Restor	e Guest Network Defaults	1	
	WPA Pre-Shared Key		Show Key	Literen		4	
	RADIUS Server	0.0.0					
	RADIUS Port	812					
	RADIUS Key						
	and the second se						
	Group Key Rotation Interval						
	WPA/WPA2 Re-auth Interval	600					
	and the second sec						
	WEP Encryption	Jisabled 🕑					
	Network Key 1		Show Key				
	Network Key 2						
	Network Key 3	1					
	Network Key 4						
	Current Network Key						
	PassPhrase						
		Generate WEP Keys					
		Apply					

Figure 41 Guest Network configuration

The page allows you to configure a secondary guest network on the wireless interface. This network is isolated from the LAN. Any clients that associate with the guest network SSID will be isolated from the private LAN and can only communicate with WAN hosts. Most of the configuration points on the guest network page are identical to those on the Primary Network page. A few extras are explained below. **DHCP Server:**

JHCP Server:

Enables the DHCP server to gives out leases to guest network clients from the specified lease pool. If the DHCP server is disabled, guest network STAs need to be assigned static IP addresses.

IP Address:

This specifies the gateway IP relayed to guest clients in DHCP lease offers.

Subnet Mask:

This specifies the subnet mask for the guest network.

Lease Pool Start:

This specifies the starting IP address for the guest network lease pool.

Lease Pool End:

This specifies the ending IP address for the guest network lease pool.

Lease Time:

This specifies the lease time for the guest network lease pool, once the CMRG completes WAN provisioning.

5.7.4 Advanced

Choose Wireless > Advanced to display the following page.

	Wireless				
	The cost				
Radio 20	802.11 Advanced				
Alexandra and	This page allows configuration of	riata ratac ar	vi WiCi thrachaide		
Primary Network	This page allows computation of	uata rates ai	Na WIFT UNCONDUCT.		
Const Manual A	54g ** Mo	de 549 Auto	~		
	XPress [™] Technolo	gy Enabled			
Advanced	802.11n Protect	ON Auto			
	Short Guard Inter	val Auto ~			
Access Control	Dasic Rate :	set Desaut V			
and the second s	MULLICASE PA	tio Line Lease	v Date v		
	Lenary R	ate Auto			
Fieldging	Beacon Inter	val 100			
Statement of the local division of the local	OTIM Inter				
(Nota)	Eragmentation Thresh	old 2246			
	DTC Thresh	ald 2340			
	RT3 Thesia	un leaves			
	Vireless Multicast Ecowarding (WM	E) Enabled	2		
	incluse maneual i cinarang (in	I TE HOTEL			
		Apply			
and the second	and an other states				

Figure 42 Advanced setting

This page allows you to configure advanced wireless settings. 54g[™] Mode:

Sets the network mode. Choices are 54g Auto, 54g Performance, 54g LRS, and 802.11b Only. 54g Auto accepts 54g, 802.11g, and 802.11b clients, but optimizes performance based on the type of clients connected. 54g Performance accepts only 54g[™] clients and provides the highest throughout; nearby 802.11b networks may have degraded performance. 54g LRS interoperates with the widest variety of 54g[™], 802.11g, and 802.11b clients. 80211b.accepts only 802.11b clients.

54g[™] Protection:

In Auto mode the AP will use RTS/CTS protection to improve 802.11g performance in mixed 802.11g + 802.11b networks. Turn protection Off to maximize 802.11g throughput under most conditions.

Xpress Technology:

Enable Broadcom proprietary method of block frame acknowledgement for 802.11g frames. This feature may improve throughput, but may cause problems.

Afterburner Technology

This feature removes the need for the acknowledgement of data frames. It may improve throughput, but may cause problems.

802.11n Protection:

Similar to 54g protection except it applies to 802.11n devices.

Basic Rate Set:

Determines which rates are advertised as "basic" rates. Default uses the driver defaults. Sets all available rates as basic rates.

Multicast Rate:

This is the rate at which you send out multicast packets to stations. Multicast packets are not acknowledged.

NPHY Rate:

Choose 802.11n rate to be applied to all unicast packets.

Legacy Rate:

"N" mode must be off on the "radio" webpage for this control to be active. When active the user can force the rate in which the AP will operate.

Beacon Interval:

Sets the beacon interval in milliseconds for the AP. The default is 100, which is fine for nearly all applications.

DTIM Interval:

Sets the wakeup interval for clients in power-save mode. When a client is running in power save mode, lower values provide higher performance but result in decreased client battery life, while higher values provide lower performance but result in increased client battery life.

Fragmentation Threshold:

Sets the fragmentation threshold. Packets exceeding this threshold will be fragmented into packets no larger than the threshold before packet transmission.

RTS Threshold:

Sets the RTS threshold. Packets exceeding this threshold will cause the AP to perform an RTS/CTS exchange to reserve the wireless medium before packet transmission.

5.7.5 Access Control

Choose Wireless > Access Control to display the following page.

	Wireless					
-	802.11 Access Co	ontrol				
Liney Belevil	Enable MAC Restrict be authorized to acce	Mode and enter the I ss your network.	MAC Addresses o	of wireless clients to restrict ac	cess to those clients only.	Only those clients whose MAC Addresses you i
Garet Network	Wireless Interface xxxx	(00.90.40.84.44.19)		•		
Advanced	MAC Restrict Mode Da	abled 🛩				
Access Collect	MAC Addresses					
Can Bridgere						
- Medi	F					
	Connected Clients	C Actives Acess	Distantion in a	CONT Design Nameri Liste Corre	-	
	No	wireless clients are c	onnected			

Figure 43 Access Control setting

This page allows you to control which wireless clients can access your wireless network. It also provides information about wireless clients connected to your access point.

MAC Restrict Mode:

Selects whether wireless clients with the specified MAC address are allowed or denied wireless access. To allow all clients, select Disabled.

MAC Addresses:

A list of wireless client MAC addresses to allow or deny based on the Restrict Mode setting. Valid input MAC address formats are XX:XX:XX:XX:XX:XX:XX and XX-XX-XX-XX-XX.

Connected Clients:

A list of connected wireless clients. When a client connects (associates) to the network, it is added to the list; when a client leaves (disassociates) from the network, it is removed from the list. For each client, the age (in seconds), estimated average receive signal strength (in dBm), IP address, and host name are presented. The age is the amount of time elapsed since data was transmitted to or received from the client.

5.7.6 WMM

Choose Wireless > WMM to display the following page.

Radio	802.11 Wi-Fi Multin	nedia					
	This page allows config	uration of W	I-Fi Multimedia QoS				
oy Inclosed	WARK Support						
et Network	No-Acknowledgement	~					
	Power Save Support						
tvanced	Acply						
as Control	1	-				11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	
	EDCA AP Parameters	CWINN	CWenax	AIFSN	TXOP(D)	TXOP(A(g))	Discard First
****	AC BE	15	63	3	0	0	07 -
ridging	AC BR	15	1023	7	0	0	01 4
	AC V	7	15	1	6016	3008	01 -
Media	AC_VO	3	7	1	3264	1504	Off M
	EDGA STA Parametera						
	AO_BE	15	1023	3	0	0	
	AC_BH	15	1023	7	0	0	
	AC_V	7	15	2	6016	3000	
	AC_VC	3	7	2	3264	1504	
	WIM IXOP Parameters	PROT HELT	Lama Bright - Baby L	and Long Repry	Lanut Long Harbert	anne Maximang an sis	
	40.00	7	3	4	12	0	
	AC 1	7	3	4	2		
	AC VO	7	3	4	2	0	
			L	Apply	A	· · · · · ·	

Figure 44 WMM configuration

This page allows you to configure WiFi Multi-Media (WMM). WMM is an implementation of Quality of Service (Qos) which is defined by the IEEE standard 802.11e.

WMM Support:

Sets WMM support. Choices are Auto, On, or Off. If enabled (Auto or On), the WME Information Element is included in beacon frame.

No-Acknowledgement:

Sets No-Acknowledgement support. Choices are On or Off. When enabled, acknowledgments for data are not transmitted.

Power Save Support:

Sets Power Save support. Choices are On or Off. When Power Save is enabled, the AP queues packets for STAs that are in power-save mode. Queued packets are transmitted when the STA notifies AP that it has left power-save mode.

EDCA AP Parameters:

Specifies the transmit parameters for traffic transmitted from the AP to the STA for the four Access Categories: Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

There are also two AP-specific settings: Admission Control and Discard Oldest First. Admission control specifies if admission control is enforced for the Access Categories. Discard Oldest First specifies the discard policy for the queues. On discards the oldest first; Off discards the newest first.

EDCA STA Parameters:

Specifies the transmit parameters for traffic transmitted from the STA to the AP for the four Access Categories: Best Effort (AC_BE), Background (AC_BK), Video (AC_VI), and Voice (AC_VO). Transmit parameters include Contention Window (CWmin and CWmax), Arbitration Inter Frame Spacing Number (AIFSN), and Transmit Opportunity Limit (TXOP Limit).

5.7.7 Bridging

Choose Wireless > Bridging to display the following page.

Status	Basic Advanced	Firewall Parental Control	VPN Wireless	USB Logout
	Wireless			
Radio	802.11 Bridging			
Pomary Network	This page allows configuration	on of WDS features.		
Garrat Network	Wireless Bridging Disabled V Remote Bridges			
Advanced				
Access Control				
	Apply			
Dridging	Scan Wireless APs			
Carl Meda				
62001-2014 Zoom Telephonics, I	nc. All rights reserved.			

Figure 45 Bridging setting

This page allows you to configure wireless bridging, which is also known as Wireless Distribution System (WDS). Bridging allows you connect multiple wireless access points together to form a single network using wireless point-to-point links.

Wireless Bridging:

This setting enables or disables wireless bridging.

Remote Bridges:

Table of remote bridge MAC addresses authorized to establish a wireless bridge. Up to 4 remote bridges may be connected. Typically, you will also have to enter your AP's MAC address (see section 0) on the remote bridge, too.

5.7.8 Media

Choose Wireless > Media and the follow page will be shown.

Figure 46 Media setting This page allows configuration of Wireless Media features.

5.8 USB

Choose USB and the submenus of USB are shown as below.

Figure 47 The Submenus of USB

5.8.1 USB Basic

Choose **USB > USB Basic** to display the following page.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
	USB	Connected De	evices					
IN THE OWNER	Basic S	Settings						
Usutune								
Approved Devices	This pag	e allows basic contro	ol of the USB dev	ices shared over the ne	twork.			
Storage David	Enable US	8 Devices connecte	d to the USB por	t • All	OApproved	ONone	Approved Devices	
	Enable US	8 Devices to be Shi	ared Storage	• Yes	ONo		Storage Configuration	
Storage Advanced	Enable the	Media Server (DLN	IA)	• Yes	ONo		Media Server Configuration	
Media Server	Apply							
			_			_		_
CONTRACTOR CONTRACTOR	Inc. All rights set	proph.						

Figure 48 USB Basic setting

This page allows you to configure Linux based servers. The buttons on the right side of the page are short cuts to the buttons on the left side frame.

5.8.2 Approved Devices

Choose USB > Approved Devices to display the following page.

Status	Basic Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
USB Basic Approved Devices Storage Basic	Network Attached St Approved Device Setting This page allows the configura	torage gs tion of the USB	storage devices shared	over the networ	k		
Storage Advanced	Enable USB Devices connected Apply Charges	to the USB por	t. All OApproved O	None			
	Approved USB Devices Select Volume Name Manufacturer P	Product Free Spa	ce Used Space Total Space	SMART Status			
	Remove						
	Select Volume Name Manufacturer I	Product Free Spa	ce Used Space Total Space	SMART Status			
	Add						
	Refresh List						
	Safely Remove Device					_	

Figure 49 Approved Devices setting

This page allows you to choose if any USB storage device plugged into the modem can be used or only approved devices. If approved device is selected then each device must be manually approved on this page. USB storage devices can be safely removed after selecting the Safely Remove Device button. The user will be asked which device they want to remove.

5.8.3 Storage Basic

Choose USB > Storage Basic to display the following page.

USB React Network Attached Storage Basic Settings This page shows the status of the USB folders shared over the network. Storage Rate: Network/Device Name: (BRCI44.VG) Vector Marine: Network/Device Name: (BRCI44.VG) Vector Metwork: Network Access Write Access Free Space: Used Space: Total Space Eff: Referent	Status	Basic Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
USD Desic Approved Devices Storage Advanced Media/Server		Network Attached S	Storage					
Approval basics This page shows the status of the USB folders shared over the network. Storage Mariner Network/Device Name; [BRCM-LVG] Storage Advanced • Share specified folders and all approved devices Modulation • Share Specified folders Approved Mariner • Share Specified folders Modulation • Share Specified folders Approved Mariner • Share Specified folders Approved Mariner • Share Name Device Folder Read Access With Access Fire Space Used Space; Total Space Edd Refresh	USB Basic	Basic Settings						
Storage Task: Network/Device Name: BRCM4.V/G Storage Advanced Default Sharing: Models Server Default Sharing: Share Name: Specified folders and all approved devices Omly share specified folders Adplu: Share Name: Device Folder Read Access Write Access Free Space Used Space Total Space Edit Refresh	Approved Devices	This page shows the status	of the USB folders	shared over the netwo	ork.			
Storage Advanced Default Sharing: • Share specified folders and all approved devices Orders Apply Share Name Device Folders Share Name Device Folder Read Access Write Access Fire Space Used Space Total Space Edd Refresh	Storage Basic	Network/Device Name: BRCM	-LVG					
Storage Advanced • Share specified folders and all approved devices Only share specified folders Adviserer Modelserver Adviserer Adviserer Inhared Methods Folders Shared Network Folder Read Access Write Access Free Space Used Space Total Space Edit Refresh	and the second sec	Default Sharing:		7.				
Modelserver Ophy share specified folders /Act/v Shared Network Folders Shared Network Folders Share Name Device Folder Read Access With Access Free Space Used Space Total Space Edit Edit Refresh	Storage Advanced	Share specified folders and the specified folders and the specified folders are specified folders.	nd all approved dev	rices				
Apply Shared Network Folders Share Name Device Folder Read Access Write Access Free Space Used Space Total Space Edit Refresh		Only share specified folde	HS					
Shared Network Polders Share Name Device Folder Read Access Write Access Free Space Used Space Total Space Edit Reflexit	Media Server	Apply						
Shared Network Folders Share Name Device Folder Read Access Write Access Free Space Used Space Total Space Edit Refresh Refresh		Contraction of the second						
Share Name Device Folder Read Access Write Access Five Space Used Space Total Space Edd		Shared Network Folders						
Edd Refresh		Share Name Device Folder Real	d Access Write Acce	ss Free Space Used Sp	ace Total Space			
Edit Reference		(married)						
Refresh		Edt						
2011-7014 Zoom Transmorts for All roths merced		Refresh						
2005-2014 Zoom Telephone, Inc. 40 onthe searched								
a se i re aveni i integri si ne i re i ngri si interi re i	92001-2014 Zoom Telephones, In	c. All rights reserved.						

Figure 50 Storage Basic setting

This page allows you to configure the device name and what folders should be shared.

5.8.4 Storage Advanced

Choose USB > Storage Advanced to display the following page.

Status	Basic	Advanced	Firewall	Parental Control	VPN	Wireless	USB	Logout
	Networ	k Attached S	Storage					
	Advance	A Settings						
USR Basic	Aurunes	u octungs						
Approved Devices	This page	allows configuratio	n of the USB folde	rs shared over the net	twork.			
Storage Basic								
Storage Advanced								
MediaServer	Network/De	evice Name: BRCM	-LVG					
	Workgroup	Name: WORKGRO	UP					
	Set Admin N	ame/Password						
	Protocols							
	Enable	Access Method	X.	Link		Port	-	
	2	Windows Netwo	ork Connection	IIBRCM-LVG				
		FTP (via interne	et)	ftp://192.168.0.1	10/	Port 21		
	Apply							
	Available Ne	ntwork Folders						
	Actions	Share Name	Device Folder	Read Access	Write Access	Free Space	Used Space	Total Space
	Create Netw	ork Folder						
	1.							
	Refresh List							
							-	

Figure 51 Storage Advanced setting

This page allows you to configure the device name. Additionally the workgroup name can is configured here. The Windows Network and FTP support can be enabled or disabled on this page. The IP address displayed in the link field is the Linux IP stack address that should be used for the FTP server address in the FTP clients.

5.8.5 Media Server

Choose **USB > Media Server** to display the following page.

Figure 52 Media Server setting

⁵³

This page allows you to configure the DLNA media server. The media server name and the file names that will be scanned on the USB storage devices are configured using this page. If desired the media Server can scan the device periodically to check for new files.

5.9 Logout

Choose Logout to logout Account and the following page will be shown after logout.

	Logout You are now logged out.
	Back to Login
©2001-2014 Zoom Telephor	ics Inc. All rights reserved

Figure 53 The logout page

6 Q&A

(1) **Q**: Why all the indicators are off?

A: Check the following:

- The connection between the power adaptor and the power socket.
- The status of the power switch.
- (2) **Q**: Why the **Ethernet** indicator is off?
 - A: Check the following:
 - The connection between the Cable Modem and your computer, hub, or switch.
 - The running status of your PC, hub, or switch.
- (3) **Q**: Why the **ONLINE** indicator is off?
 - A: Check CM DS/US LED is on. Check the connection between the Cable Line and the wall HFC.

Apply customer :

Name : Zoom Telephonics Inc Address: 207 South Street, Boston Massachusetts 02111 USA Contact Person: Paul Prohodski Title: Director of Quality Assurance and Technical Services Telephone: 617-423-1072 Ext 3100 Fax: 617-423-1075

For applicable power supplies :

1, EU : S24B13-120A200-Y4 Brand : Shenzhen Gongjin Electronics Co., Ltd 2, US: S24B12-120A200-Y4 Brand : Shenzhen Gongjin Electronics Co., Ltd

FCC statement

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

NOTE: 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 harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

"FCC RF Radiation Exposure Statement Caution: To maintain compliance with the FCC's RF exposure guidelines, place the product at least 20cm from nearby persons."

keep 20cm away warning :

FCC, IC and CE Radiation Exposure Statement for Mobile Devices

This equipment complies with FCC, IC and CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 7-7/8" (200 mm) between the radiator and your body. The transmitt er must not be collocated or operating in conjunction with any other antenna or transmitter.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inf érieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonn ée équivalente (p. i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autoris é e aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement. Déclaration FCC, IC et CE d'exposition aux rayonnements pour les appareils mobiles Cet équipement est conforme aux limites FCC, IC et CE d'exposition aux rayonnements stipulées pour un environnement non contr?lé. Il doit être installé et utilisé en laissant une distance minimale de 7-7/8" (200 mm) entre le radiateur et votre corps. L'émett eur ne doit pas être place au même emplacement que celui d'une autre antenne ou d'un autre émett eur, et ne doit pas fonctionner en même temps que de tels dispositifs.