Geavanceerde gebruikers-handleiding internet

Technicolor TC7210

Welkom bij Internet van Ziggo

Van harte welkom bij Internet van Ziggo. Met deze geavanceerde handleiding kunt u de instellingen wijzigen van uw Wi-Fi modem.

Let op!

Het aanpassen van de geavanceerde instellingen is op eigen risico. Ziggo heeft uw Wi-Fi modem standaard zo ingesteld dat het Wi-Fi modem goed werkt bij normaal gebruik. Mocht het Wi-Fi modem niet goed werken nadat u de geavanceerde instellingen gewijzigd heeft, dan adviseren wij u de standaardinstellingen te herstellen. Dit kan via de basisinstellingen of via een hard reset (zie de Gebruikershandleiding Internet). De reguliere Ziggo helpdesk kan u niet adviseren over de geavanceerde instellingen.

Veel plezier met Internet van Ziggo!

Opmerkingen over de installatie en het gebruik van Internet van Ziggo

Internet van Ziggo is bedoeld voor persoonlijk gebruik. Het gebruik en de installatie van Internet van Ziggo zijn gebonden aan de Algemene Basisvoorwaarden Ziggo en de Aanvullende Voorwaarden Ziggo Internet. De meest recente versies kunt u vinden op: **www.ziggo.nl/voorwaarden**.

Inhoudsopgave

1. Internet van Ziggo 5
1.1 Symbolen 5

2. Inloggen op de gebruikers-omgeving 6
2.1 Geavanceerde instellingen 6

3. Connections and setup 9
3.1 Wireless Voice Gateway Overview 9
3.2 Relationship amoung the devices 14
3.3 Connecting the Wireless Voice Gateway to a Single Computer 16

4. Web configuration 19
4.1 Accessing the Web Configuration 19
4.2 Gateway – Status Web Page Group 22
4.3 Gateway – Network Web Page Group 30
4.4 Gateway – Advanced Web Page Group 38
4.5 Gateway – Firewall Web Page Group 49
4.6 Gateway – Parental Control Web Page Group 53
4.7 Gateway – Wireless Web Page Group 54
4.8 Gateway – USB Web Page Group 73
4.9 VoIP – Basic Web Page Group 78

5. Networking 82
5.1 Communications 82
5.2 Type of communication 82
5.3 Cable Modem (CM) Section 83
5.4 Networking Section 83
5.5 Three Networking Modes 84
5.6 Cable Modem (CM) Mode 85
5.7 Residential Gateway (RG) Mode 86

6. Frequently asked questions 88

7. Troubleshooting 90

8. Glossary 92

1. Internet van Ziggo

Deze handleiding leidt u stap voor stap door de geavanceerde instellingen van Internet van Ziggo. Wij adviseren u om deze handleiding op uw computer op te slaan in verband met het eventueel wegvallen van de internetverbinding.

Heeft u hulp nodig? Stel uw vraag aan onze Online Assistent op **www.ziggo.nl/klantenservice** of bekijk het portal op **www.ziggo.nl/WiFimodem**.

De afbeeldingen in deze handleiding kunnen afwijken van de werkelijkheid.

1.1 Symbolen

In deze handleiding komt u de volgende symbolen tegen:

Let op!

... geeft u extra uitleg over mogelijkheden of situaties.

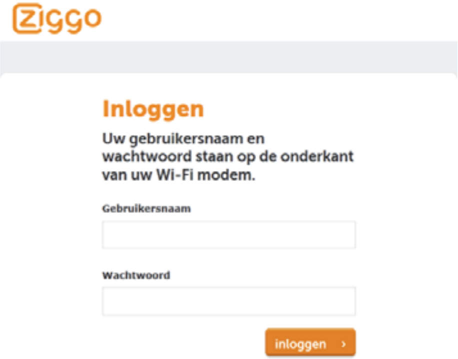
Tip!

... geeft u handige informatie over de toepassing van een functie.

2. Inloggen op de gebruikersomgeving

In de gebruikersomgeving kunt u geavanceerde instellingen van uw Wi-Fi modem wijzigen. Om op de gebruikersomgeving in te loggen volgt u de volgende stappen:

1. Open een internet browser op uw PC.
2. Typ het adres **http://192.168.178.1** in de adresbalk en druk op **Enter**. Het login venster waarin wordt gevraagd om een gebruikersnaam en wachtwoord verschijnt.


Inloggen

Uw gebruikersnaam en wachtwoord staan op de onderkant van uw Wi-Fi modem.

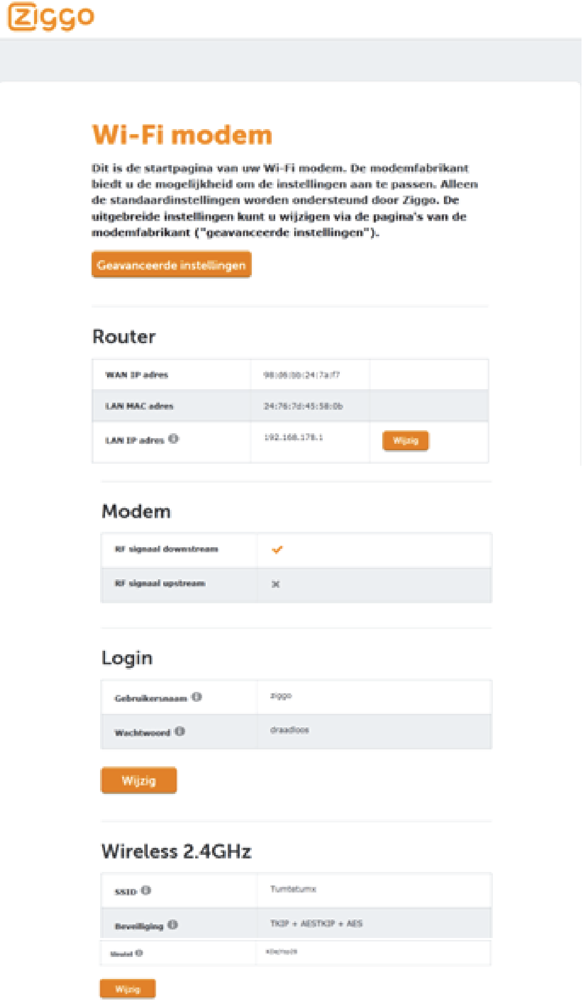
Gebruikersnaam

Wachtwoord

3. Voer uw gebruikersnaam en wachtwoord in en klik op **Inloggen**. Standaard is de gebruikersnaam **ziggo** en het wachtwoord **draadloos.**

2.1 Geavanceerde instellingen

Na het inloggen verschijnt de startpagina van de gebruikersomgeving. Op deze startpagina staat basisinformatie van uw Wi-Fi modem weergegeven. De uitleg over de basisinformatie vindt u in de Gebruikershandleiding Internet.
Via de knop **Geavanceerde instellingen** kunt u geavanceerde instellingen wijzigen.



Wi-Fi modem

Dit is de startpagina van uw Wi-Fi modem. De modemfabrikant biedt u de mogelijkheid om de instellingen aan te passen. Alleen de standaardinstellingen worden ondersteund door Ziggo. De uitgebreide instellingen kunt u wijzigen via de pagina's van de modemfabrikant ("geavanceerde instellingen").

Router

WAN IP adres	98:06:00:24:7a:f7	
LAN MAC adres	24:76:7d:45:58:0b	
LAN IP adres ⓘ	192.168.178.1	Wijzig

Modem

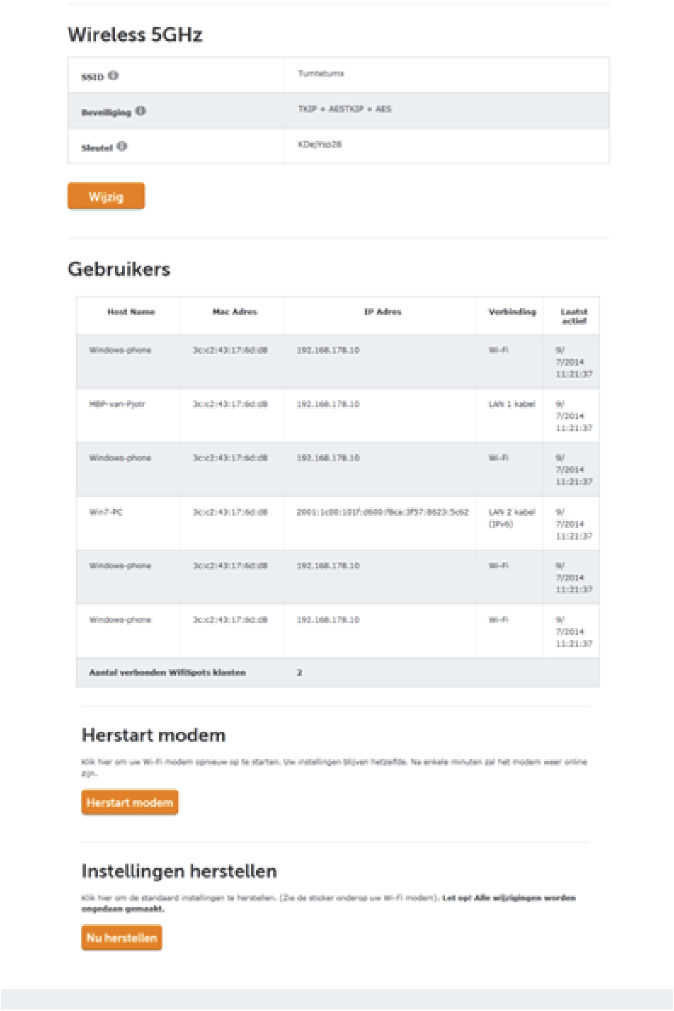
RF signaal downstream	✓
RF signaal upstream	✕

Login

Gebruikersnaam ⓘ	ziggo
Wachtwoord ⓘ	draadloos

Wireless 2.4GHz

SSID ⓘ	Tumtatumx
Beveiliging ⓘ	TKIP + AESTKIP + AES
Sleutel ⓘ	[illegible]



Wireless 5GHz

SSID ⓘ	Tumbetumx
Beveiliging ⓘ	TKIP + AESTKIP + AES
Sleutel ⓘ	KDejYso28

Gebruikers

Host Name	Mac Adres	IP Adres	Verbinding	Laatst actief
Windows-phone	3c:c2:43:17:6d:d8	192.168.178.10	Wi-Fi	9/ 7/2014 11:21:37
MBP-van-Pjotr	3c:c2:43:17:6d:d8	192.168.178.10	LAN 1 kabel	9/ 7/2014 11:21:37
Windows-phone	3c:c2:43:17:6d:d8	192.168.178.10	Wi-Fi	9/ 7/2014 11:21:37
Win7-PC	3c:c2:43:17:6d:d8	2001:1c00:101f:d600:f8ca:3f57:8623:5c62	LAN 2 kabel (IPv6)	9/ 7/2014 11:21:37
Windows-phone	3c:c2:43:17:6d:d8	192.168.178.10	Wi-Fi	9/ 7/2014 11:21:37
Windows-phone	3c:c2:43:17:6d:d8	192.168.178.10	Wi-Fi	9/ 7/2014 11:21:37
Aantal verbonden WifiSpots klanten		2		

Herstart modem

Klik hier om uw Wi-Fi modem opnieuw op te starten. Uw instellingen blijven hetzelfde. Na enkele minuten zal het modem weer online zijn.

Instellingen herstellen

Klik hier om de standaard instellingen te herstellen. (Zie de sticker onderop uw Wi-Fi modem). **Let op! Alle wijzigingen worden ongedaan gemaakt.**

3. Connections and setup

3.1 Wireless Voice Gateway Overview

3.1.1 Front panel

The following illustration shows the front panel:

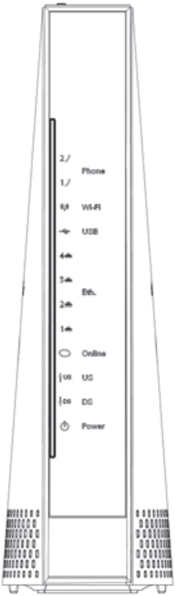


figure 1: Front panel

LED	Description
POWER	Indicates the Power status.
DS	Indicates the status of Data reception by the cable modem from the Network (Downstream Traffic).
US	Indicates the status of Data transmission by the cable modem to the Network (Upstream Traffic).
ONLINE	Displays the status of your cable connection. The light is off when no cable connection is detected and fully lit when the modem has established a connection with the network and data can be transferred.
LAN 1 t/m 4	Indicates the state of Ethernet ports.
USB	Indicates the state of USB host connect.
Wi-Fi	Indicates the traffic on the wireless network.
TEL1-2	Indicates the status of the telephone Phone 1 and Phone 2.

LED

The lights on the front panel LEDs are described in the table below (from left to right): ON = the LED is light, OFF = the LED is gray, FLASH = the LED is blinking.

TC7210	Power	Internet			LAN				USB	Wireless	TEL 1	TEL 2	Description
		DS	US	Online	1	2	3	4					
Boot-up Operation	ON	ON	ON	ON	ON	ON	ON	ON	ON	X	ON	ON	Power on .025 sec
	ON	0.25 SECOND								X			
	ON	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	From power ON to system initialization complete
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Following system initialization complete to (before) DS scanning
		1 SECOND											
DOCSIS Start-up Operation	ON	FLASH	OFF	OFF	X	X	X	X	X	X	X	X	During DS scanning and acquiring SYNC
	ON	ON	FLASH	OFF	X	X	X	X	X	X	X	X	From SYNC completed, receiving UCD to ranging completed
	ON	ON	ON	FLASH	X	X	X	X	X	X	X	X	During DHCP, configuration file download, registration, and Baseline Privacy initialization: DHCP status: 1 second ON and 1 second OFF, TFTP status: 0.25 second ON and 0.25 second OFF
	ON	ON	ON	ON	X	X	X	X	X	X	X	X	Operational (NACO=ON)
	ON	FLASH	FLASH	OFF	X	X	X	X	X	X	X	X	Operational (NACO=OFF)
Channel Bonding Operation	FLASH	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	Wait registration with all DS and all US – Lights Flash sequentially from the right to left Minimum duration 3 seconds
	X	X	X	X	OFF	X	X	X	X	X	X	X	From 1 to 4 DS, from 1 to 4 LEDs are ON From 5 to 8 DS, From 1 to 4 LEDs are flashing Duration 3 seconds
	OFF	X	X	X	X	X	X	X	X	X	X	X	From 1 to 4 US, from 1 to 4 LEDs are ON.
	FLASH	FLASH	FLASH	FLASH	X	X	X	X	X	X	X	X	Wait registration with all DS and all US – Lights Flash sequentially from the left to right
MTA Operation	ON	ON	ON	ON	X	X	X	X	X	X	FLASH	OFF	MTA DHCP
	ON	ON	ON	ON	X	X	X	X	X	X	OFF	FLASH	MTA SNMP/TFTP
	ON	ON	ON	ON	X	X	X	X	X	X	ON	ON	RSIP for NCS/Register for SIP
CPE Operation	ON	X	X	X	OFF ON FLASH	OFF ON FLASH	OFF ON FLASH	OFF ON FLASH	OFF ON FLASH	OFF ON FLASH	X	X	No LAN / Wireless link LAN / Wireless link TX/RX LAN / Wireless traffic
MTA Operation	ON	<CM Normal Operation>									ON	ON	Both Lines On-Hook
	ON										FLASH	ON	Tel1 Off-hook, Tel2 On-hook
	ON										ON	FLASH	Tel1 On-hook, Tel2 Off-hook
	ON										FLASH	FLASH	Both Lines Off-Hook
SW Download Operation	ON	FLASH	FLASH	ON	X	X	X	X	X	X	X	X	A software download and while updating the FLASH memory

LED Status when WPS State is	
In-progress	Green LED will blink with 2 sec On -1 sec OFF cycle
Success	Green LED will remain ON for 300 secs before turning OFF
Error”/ “Timeout	Red LED will blink with 250 msec ON- 250 msec OFF cycle indefinitely
Session overlap	Red LED will turn ON-OFF with 250 msec duration for 2 seconds followed by turning OFF for 500 msec.
This cycle will repeat for a total duration of 120 seconds.	

table 1: LED behaviour

3.1.2 Rear panel

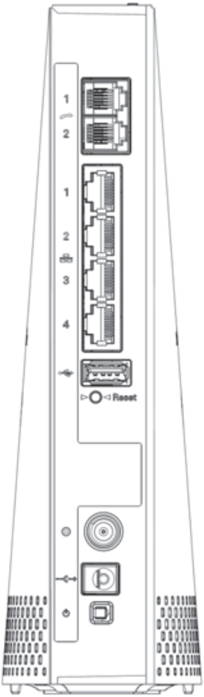


figure 2: Rear panel

Connector	Description
Power switch	Power on, off the Cable modem.
Power jack	Connector for DC12V.
Cable	Connector for the cable network.
Reset	To restart the modem or press over 5 seconds can default the modem.
USB Host	USB 2.0 connector
LAN	4 Gige Ethernet ports, RJ-45 connector.
TEL 1-2	2 Phone RJ11 Connectors.

table 2: Rear panel description

3.1.3 Side panel for WPS

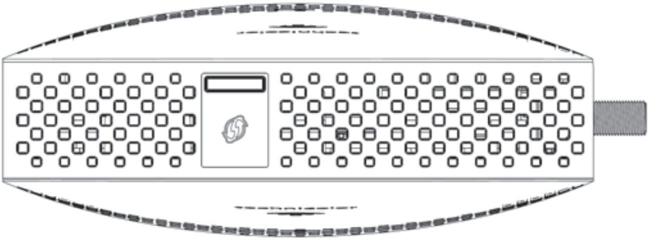


figure 3: Side panel

WPS – Indicates the status of the WPS functionality.

WPS button: Wi-Fi Protected Setup^{TM}.

This button can be used to secure the connection with another device (PC for example) using WPS protocol. A long press (press 2 more seconds) on the button allows you to enable the association of the modem with a PC or other equipment. After link establish. A short press on the button, switch on/off Wi-Fi.

3.2 Relationship amoung the devices

This illustration shows a cable company that offers DOCSIS/Euro-DOCSIS and PacketCable/Euro-PacketCable compliant voice/data services.

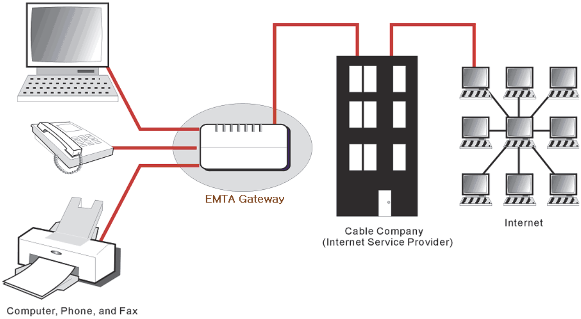


figure 4: Connection overview

3.2.1 What the Modem does

The Wireless Voice Gateway provides high-speed Internet access as well as cost-effective, toll-quality telephone voice and fax/modem services over residential, commercial, and education subscribers on public and private networks via an existing CATV infrastructure. It can inter-operate with the PacketCable compliant head-end equipment and provide the IP-based voice communications. The IP traffic can transfer between the Wireless Voice Gateway and DOCSIS/Euro-DOCSIS compliant head-end equipment. The data security secures upstream and downstream communications.

3.2.2 What the Modem needs to do its job

- The Right Cable Company: Make sure your local cable company provides data services that use cable TV industry-standard DOCSIS/Euro-DOCSIS compliant and PacketCable/Euro-PacketCable compliant technology.
- The Internet/Telephony Service Provider (ISP/TSP): Your cable company provides you access to an Internet Service Provider (ISP) and Telephony Service Provider (TSP). The ISP is your gateway to the Internet and provides you with a pipeline to access Internet content on the World Wide Web (WWW). The TSP provides you with telephony access to other modems or other telephony services over the Public Switched Telephone Network (PSTN).

Check with your cable company to make sure you have everything you need to begin; they'll know if you need to install special software or re-configure your computer to make your cable internet service work for you.

3.2.3 Contact your local cable company

You will need to contact your cable company to establish an Internet account before you can use your gateway. You should have the following information ready (which you will find on the sticker on the gateway):

- The serial number
- The model number
- The Cable Modem (CM) Media Access Control (MAC) address
- The Terminal Adapter (EMTA) MAC address
- Security information: Service Set Identifier (SSID), Encryption key / passphrase (WPA2-PSK by default), channel number. Default values are indicated underneath the modem on the sticker.

Please check the following with the cable company

- The cable service to your home supports DOCSIS/Euro-DOCSIS compliant two-way modem access.
- Your internet account has been set up. (The Media Terminal Adapter will provide data service if the cable account is set up but no telephony service is available.)
- You have a cable outlet near your PC and it is ready for Cable Modem service.

Let op!

It is important to supply power to the modem at all times. Keeping your modem plugged in will keep it connected to the Internet. This means that it will always be ready whenever you need.

Important Information

Your cable company should always be consulted before installing a new cable outlet. Do not attempt any rewiring without contacting your cable company first.

Please verify the following on the Wireless Voice Gateway

The Power LED should be lighted when plug-in the power supply.

3.3 Connecting the Wireless Voice Gateway to a Single Computer

This section of the manual explains how to connect your Wireless Voice Gateway to the Ethernet port on your computer and install the necessary software. Please refer to Figure 1-5 to help you connect your Digital Cable Modem for the best possible connection.

3.3.1 Attaching the Cable TV Wire to the Wireless Voice Gateway

1. Locate the Cable TV wire. You may find it one of three ways:
   a. Connected directly to a TV, a Cable TV converter box, or VCR. The line will be connected to the jack, which should be labeled either IN, CABLE IN, CATV, CATV IN, etc.
   b. Connected to a wall-mounted cable outlet.
   c. Coming out from under a baseboard heater or other location. See Figure 1-6 for the wiring example.

Let op!

For optimum performance, be sure to connect your Wireless Voice Gateway to the first point the cable enters your home. The splitter must be rated for at least 1GHz.

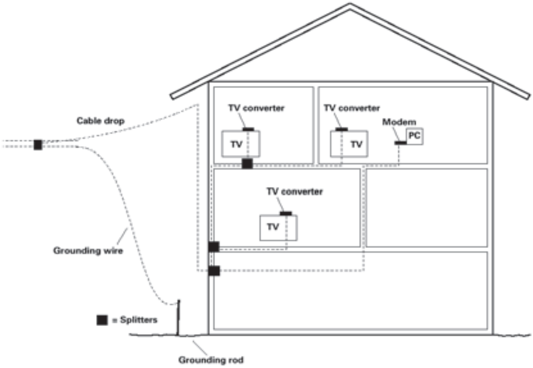


figure 5: Basic home wiring

3.3.2 Installation procedure for connecting to the Ethernet interface

Follow these steps for proper installation. Plug the coaxial cable to the cable wall outlet and the other end to the modem’s cable connector.

Let op!

To ensure a fast registration of the modem, the coaxial cable must be connected to the modem before it is powered on.

Plug the power supply into the socket of the cable modem and two-pin plug in the AC outlet then press the Power Switch, power on the modem.

Let op!

Only use the power supply that comes with the modem. Using another power supply can cause damage to the product, and will void the warranty.

Connect an Ethernet cable (direct connection, see below) to the Ethernet port at the back of the computer, and the other end to the ETHERNET port on the rear panel of the cable modem. The modem will seek the appropriate cable signal on the cable television network and go through the initial registration process on its own. The modem is ready for data transfer after the green LED "ONLINE" is lit continuously.

Let op!

the button "reset" at the back of the modem is used primarily for maintenance.

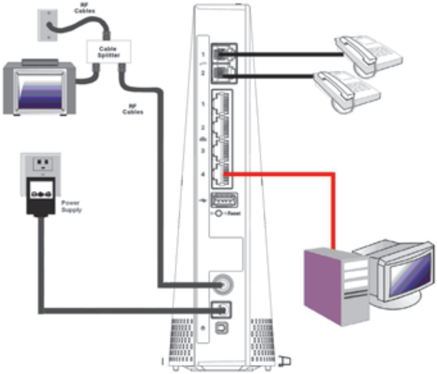


figure 6: Connect to the modem

3.3.3 Telephone or Fax Connection

When properly connected, most telephony devices can be used with the Wireless Voice Gateway just as with a conventional telephone service. To make a normal telephone call, pick up the handset; listen for a dial tone, then dial the desired number. For services such as call waiting, use the hook switch (or FLASH button) to change calls. The following procedures describe some of the possible connection schemes for using telephony devices with the Wireless Voice Gateway.

1. 1. Connect a standard phone line cord directly from the phone (fax machine, answering machine, caller ID box, etc.) to one of the LINE jacks on the Wireless Voice Gateway.
2. If there is a phone line in your home which is NOT connected to another telephone service provider, connect a standard phone line cord from a jack on this line to one of the LINE jacks of the Wireless Voice Gateway. Connect a standard phone line cord directly from the phone (fax machine, answering machine, caller ID box, etc.) to one of the other jacks in the house that uses that line.
3. If you have a multi-line telephone, connect a standard phone line cord (not an RJ-14 type line cord) from the phone to the LINE jacks on the Wireless Voice Gateway. (Other phones can be added to each line by using standard phone line splitters.)

4. Web configuration

To make sure that you can access the Internet successfully, please check the following first.

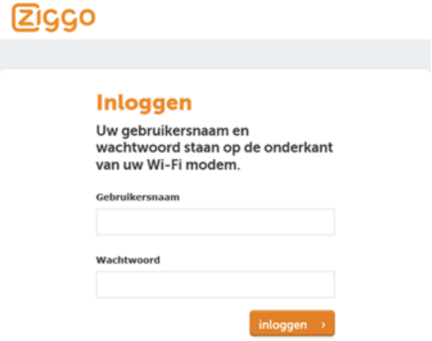
1. Make sure the connection (through Ethernet) between the Wireless Voice Gateway and your computer is OK.
2. Make sure the TCP/IP protocol is set properly.
3. Subscribe to a Cable Company.

4.1 Accessing the Web Configuration

The **Wireless Voice Gateway** offers local management capability through a built-in HTTP server and a number of diagnostic and configuration web pages. You can configure the settings on the web page and apply them to the device.

Once your host PC is properly configured; please proceed as follows:

1. Start your web browser and type the private IP address of the Wireless Voice Gateway on the URL field: **192.168.0.1**
2. After connecting to the device, you will be prompted to enter username and password. By default, the username is **ziggo** and the password is **draadloos**.



Inloggen

Uw gebruikersnaam en wachtwoord staan op de onderkant van uw Wi-Fi modem.

Gebruikersnaam

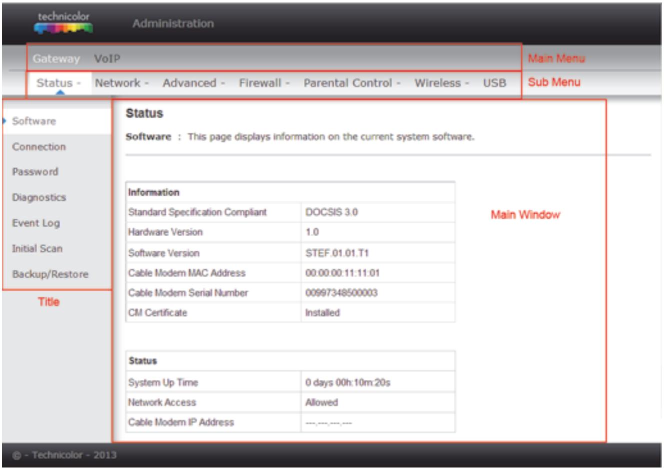
Wachtwoord

figure 7: Login dialogue

If you login successfully, the main page will appear.

4.1.1 Outline of Web Manager

The main screen will be shown as below.



Status

Software : This page displays information on the current system software.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.0
Software Version	STEF.01.01.T1
Cable Modem MAC Address	00:00:00:11:11:01
Cable Modem Serial Number	00997348500003
CM Certificate	Installed

Status	
System Up Time	0 days 00h:10m:20s
Network Access	Allowed
Cable Modem IP Address	---.---.---.---

© - Technicolor - 2013

figure 8: Outline of Web Manager

Main Menu The hyperlinks on the top of the page, including Gateway, VoIP and several sub-menu items

Sub Menu Under the main menu, sub menu use to enter each function, e.g., Status, Network, Firewall...

Title The sidebar on the left side of the page indicates the title of this management interface, e.g., Software in this example

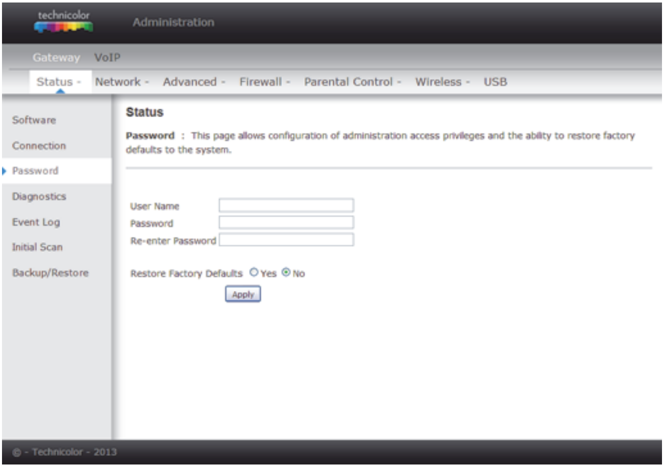
Main Window The current workspace of the web management, containing configuration or status information

For easy navigation, the pages are organized in groups with group in names main menu. Individual page names within each group are provided in the sub menu and sidebar. So to navigate to a page, click the group hyperlink at the top, then the sub menu for the function, finally choose the title on the sidebar.

Your cable company may not support the reporting of some items of information listed on your gateway’s internal web pages. In such cases, the information field appears blank. This is normal.

4.1.2 Warning message to change the password

At your first connection or while the password is the default one, a warning message is displayed on the top banner of each Web configuration page. We want to encourage you to change the password in order to enforce the security of your modem. Please refer to the chapter password page 25 for more information.



Status

Password : This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

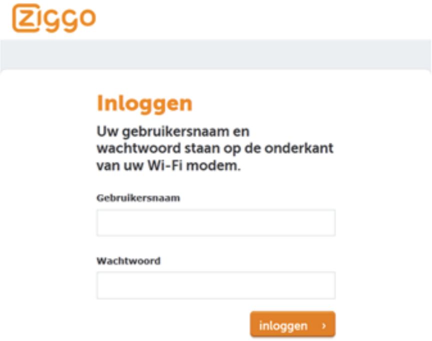
User Name
Password
Re-enter Password

Restore Factory Defaults ○ Yes ● No

figure 9: Gateway\Status\Password

To change the password: type the password, and re-enter it again.

If the password is accepted, you are required to re log on the web pages:



Inloggen

Uw gebruikersnaam en wachtwoord staan op de onderkant van uw Wi-Fi modem.

Gebruikersnaam

Wachtwoord

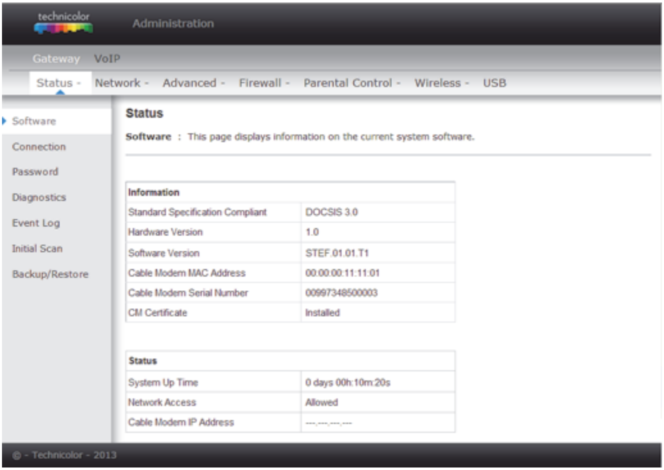
figure 10: Password request dialog

4.2 Gateway – Status Web Page Group

4.2.1 Software

The information section shows the hardware and software information about your gateway.

The status section of this page shows how long your gateway has operated since last time being powered up, and some key information the Cable Modem received during the initialization process with your cable company. If Network Access shows **Allowed**, then your cable company has configured your gateway to have Internet connectivity. If not, you may not have Internet access, and should contact your cable company to resolve this.



Status

Software : This page displays information on the current system software.

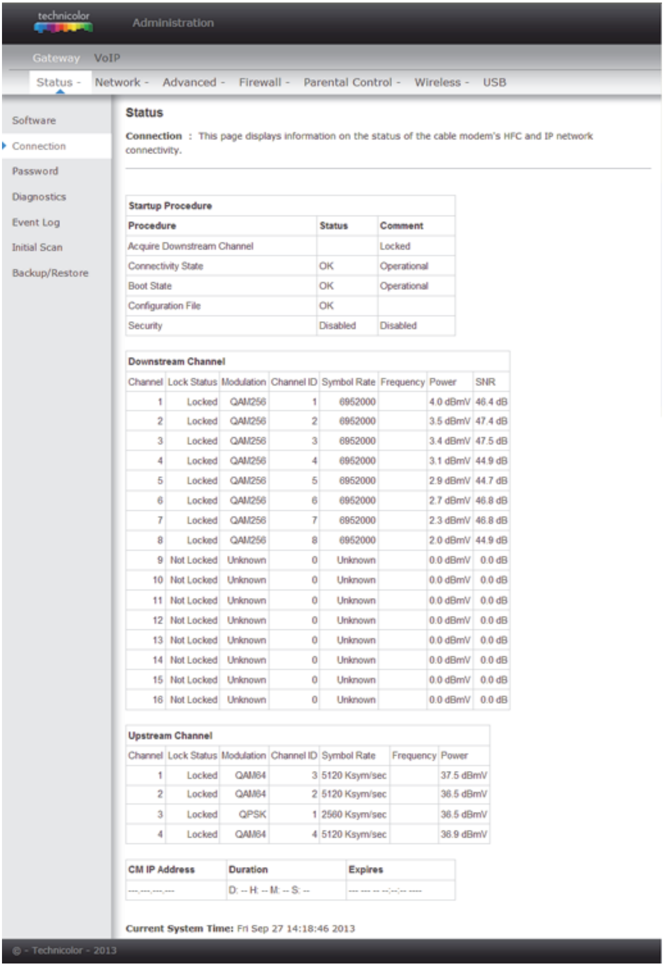
Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1.0
Software Version	STEF.01.01.T1
Cable Modem MAC Address	00:00:00:11:11:01
Cable Modem Serial Number	00997348500003
CM Certificate	Installed

Status	
System Up Time	0 days 00h:10m:20s
Network Access	Allowed
Cable Modem IP Address	---.---.---.---

figure 11: Gateway\Status\Software

4.2.2 Connection

This page reports current connection status containing startup procedures, downstream and upstream status, CM online information, and so on. The information can be useful to your cable company's support technician if you're having problems.



Status

Connection : This page displays information on the status of the cable modem's HFC and IP network connectivity.

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel		Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Configuration File	OK	
Security	Disabled	Disabled

Downstream Channel

Channel	Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power	SNR
1	Locked	QAM256	1	6952000		4.0 dBmV	46.4 dB
2	Locked	QAM256	2	6952000		3.5 dBmV	47.4 dB
3	Locked	QAM256	3	6952000		3.4 dBmV	47.5 dB
4	Locked	QAM256	4	6952000		3.1 dBmV	44.9 dB
5	Locked	QAM256	5	6952000		2.9 dBmV	44.7 dB
6	Locked	QAM256	6	6952000		2.7 dBmV	46.8 dB
7	Locked	QAM256	7	6952000		2.3 dBmV	46.8 dB
8	Locked	QAM256	8	6952000		2.0 dBmV	44.9 dB
9	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
10	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
11	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
12	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
13	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
14	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
15	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB
16	Not Locked	Unknown	0	Unknown		0.0 dBmV	0.0 dB

Upstream Channel

Channel	Lock Status	Modulation	Channel ID	Symbol Rate	Frequency	Power
1	Locked	QAM64	3	5120 Ksym/sec		37.5 dBmV
2	Locked	QAM64	2	5120 Ksym/sec		36.5 dBmV
3	Locked	QPSK	1	2560 Ksym/sec		36.5 dBmV
4	Locked	QAM64	4	5120 Ksym/sec		36.9 dBmV

CM IP Address	Duration	Expires
---.---.---.---	D: -- H: -- M: -- S: --	--- --- -- --:--:-- ----

Current System Time: Fri Sep 27 14:18:46 2013

figure 12: Gateway\Status\Connection

4.2.3 Password

By default, the username is **ziggo** and the password is **draadloos**.
This is set by different actions (non exhaustive list):

- at the manufactory level,
- following a reset factory on the modem,
- following a reset from the operator,
- following a change by the user who wants to come back to the default setting after using its own settings

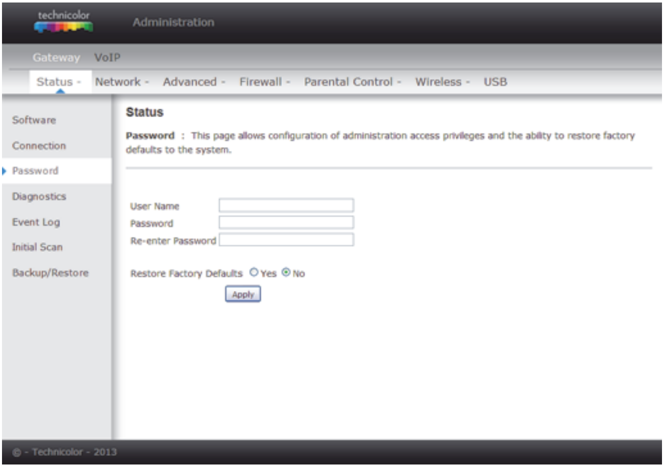
When the current password is the default one, the user is strongly encouraged to change the default web password.

At your first connection or while the password is the default one, a warning message is displayed on the top banner of each Web configuration page. We want to encourage you to change the password in order to enforce the security of your modem.

The password can be a maximum of 8 characters and is case sensitive. In addition, this page can be used to restore the gateway to its original factory settings. Use this with caution, as all the settings you have made will be lost. To perform this reset, set Restore Factory Defaults to Yes and click Apply. This has the same effect as a factory reset using the rear panel reset switch, where you hold on the switch for 5 seconds, then release it.

Let op!

We are always suggesting you to modify the password. This is a basic protection against wrongful access to the Gateway Web pages.

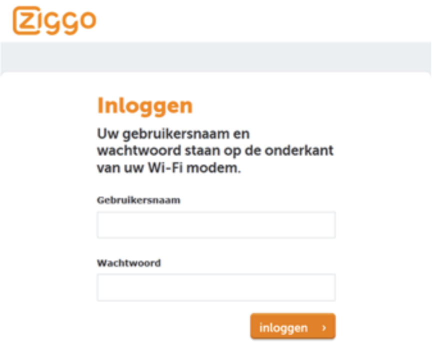


Password : This page allows configuration of administration access privileges and the ability to restore factory defaults to the system.

Restore Factory Defaults ○ Yes ● No

figure 13: Gateway\Status\Password

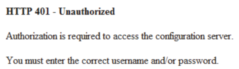
To change the password: type the password, and re-enter it again.
If the password is accepted, you are required to re log on the web pages:



Uw gebruikersnaam en wachtwoord staan op de onderkant van uw Wi-Fi modem.

figure 14: Password request dialog

If the password is not accepted, an error message is displayed:



HTTP 401 - Unauthorized

Authorization is required to access the configuration server.

You must enter the correct username and/or password.

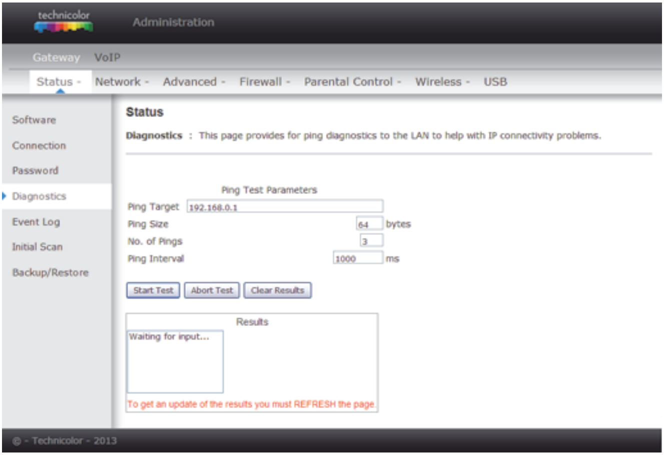
Please reflash the web and wait for Password dialog pop-up, then typing the correct username and password again.

4.2.4 Diagnostics

This page offers basic diagnostic tools for you to use when connectivity problems occur. When you ping an Internet device, you send a packet to its TCP/IP stack, and it sends one back to yours. To use the ping Test, enter the information needed and press **Start Test**; the Result will be displayed in the lower part of the window. Press **Abort Test** to stop, and **Clear Results** to clear the result contents.

Let op!

Firewalls may cause pings to fail but still provide you TCP/IP access to selected devices behind them. Keep this in mind when ping a device that may be behind a firewall. Ping is most useful to verify connectivity with PCs which do not have firewalls, such as the PCs on your LAN side.



Status

Diagnostics : This page provides for ping diagnostics to the LAN to help with IP connectivity problems.

Ping Test Parameters

Ping Target 192.168.0.1

Ping Size 64 bytes

No. of Pings 3

Ping Interval 1000 ms

Results

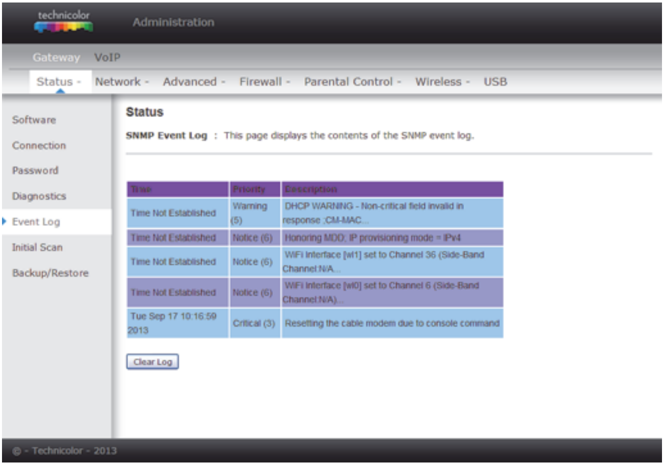
Waiting for input...

To get an update of the results you must REFRESH the page

figure 15: Gateway\Status\Diagnostics

4.2.5 Event Log

This page displays the contents of the SNMP event log. Press **Clear Log** button to clear the logs.



Status

SNMP Event Log : This page displays the contents of the SNMP event log.

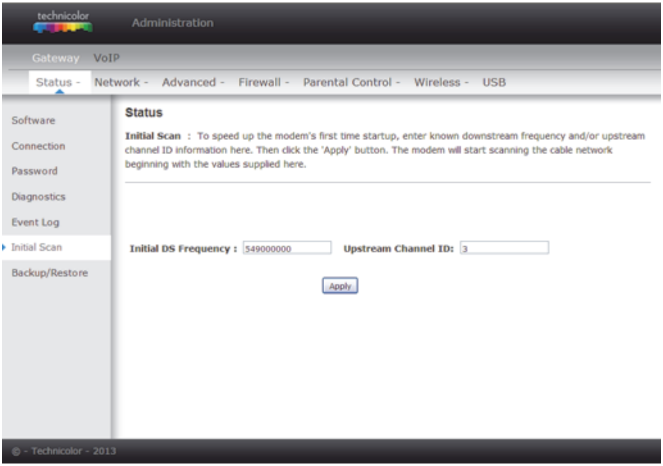
Time	Priority	Description
Time Not Established	Warning (5)	DHCP WARNING - Non-critical field invalid in response ;CM-MAC...
Time Not Established	Notice (6)	Honoring MDD; IP provisioning mode = IPv4
Time Not Established	Notice (6)	WiFi Interface [wl1] set to Channel 36 (Side-Band Channel:N/A...
Time Not Established	Notice (6)	WiFi Interface [wl0] set to Channel 6 (Side-Band Channel:N/A)...
Tue Sep 17 10:16:59 2013	Critical (3)	Resetting the cable modem due to console command

figure 16: Gateway\Status\Event Log

4.2.6 Initial Scan

To speed up the modem’s first time connection, enter known downstream frequency and/or upstream channel ID information here. Then click **Apply and Reboot** button to start scanning the cable network beginning with the values supplied here.

The value is provided in Hertz. So, for 549 MHz, you must type: **549000000**



Status

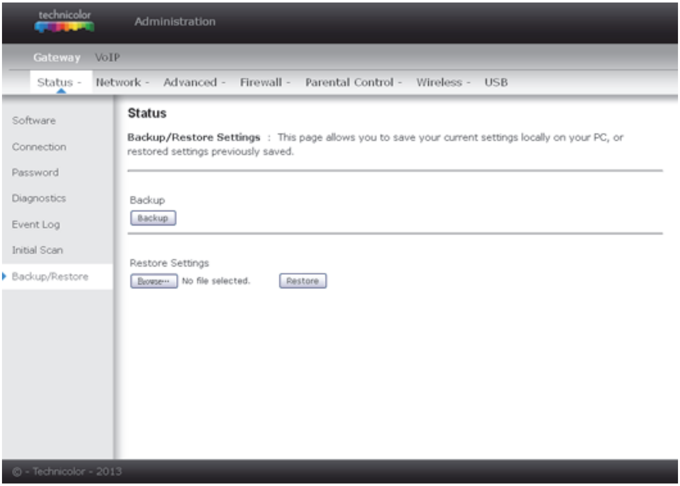
Initial Scan : To speed up the modem's first time startup, enter known downstream frequency and/or upstream channel ID information here. Then click the 'Apply' button. The modem will start scanning the cable network beginning with the values supplied here.

Initial DS Frequency : 549000000 **Upstream Channel ID:** 3

figure 17: Gateway\Status\Initial Scan

4.2.7 Backup/Restore

This page allows you to save your current settings locally on your PC, or restore settings previously saved. The default file name is **GatewaySettings.bin**.



Status

Backup/Restore Settings : This page allows you to save your current settings locally on your PC, or restored settings previously saved.

Backup

Restore Settings

No file selected.

figure 18: Gateway\Status\ Backup/Restore

4.3 Gateway – Network Web Page Group

4.3.1 LAN

You can activate the DHCP server function for the LAN on this page. With this function activated,

- your cable company’s DHCP server provides one IP address for your gateway,
- and your gateway’s DHCP server provides IP addresses, starting at the address you set in IP Address on the LAN page, to your PCs. A DHCP server leases an IP address with an expiration time.

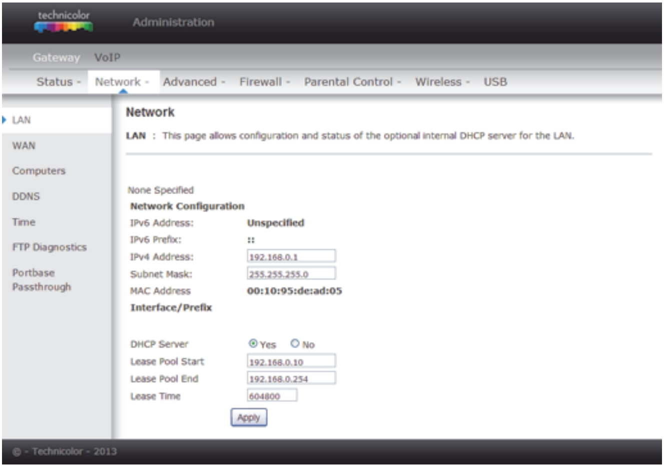
To change the IP address that your gateway will use on the LAN side, enter it into the **IP Address** box and then click **Apply**.

IP Address and Subnet Mask:

A private IP address and Subnet Mask for LAN sub netting.
For example 192.168.0.1./ 255.255.255.0.

DHCP Server:

- Select the check point of **Yes** or **No** to enable or disable a simple DHCP server for LAN.
- Configure the IP address numbers for the DHCP server with **Lease pool start** and **Lease pool end**.
- Configure the IP address lease time with **Lease time** for DHCP server. Default value is 604800 seconds.



Network

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

None Specified

Network Configuration

IPv6 Address:	**Unspecified**
IPv6 Prefix:	**::**
IPv4 Address:	192.168.0.1
Subnet Mask:	255.255.255.0
MAC Address	**00:10:95:de:ad:05**

Interface/Prefix

DHCP Server	● Yes ○ No
Lease Pool Start	192.168.0.10
Lease Pool End	192.168.0.254
Lease Time	604800

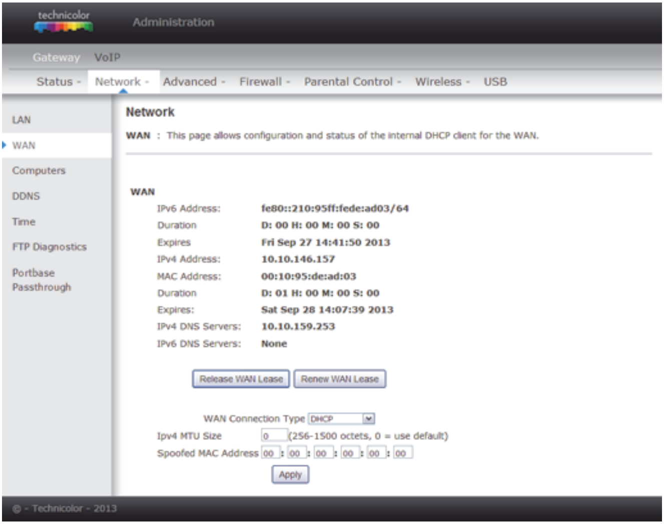
figure 19: Gateway\Network\LAN

4.3.2 WAN

You can configure the optional internal DHCP server for the WAN on this page. This can be required by some ISP providers.

Select different WAN Connection Type will lead to different contents. Take the WAN connection type-DHCP for example, you can release and renew the WAN lease by pressing the buttons.

You can enter a spoofed MAC address that causes your gateway networking stack to use that MAC address when communicating instead of the usual WAN MAC address, e.g., if the MAC address is **00:10:18:de:ad:03**, this spoofed MAC address could be **00:11:e3:df:ad:05** or any desired MAC address.



Network

WAN : This page allows configuration and status of the internal DHCP client for the WAN.

WAN

IPv6 Address:	**fe80::210:95ff:fede:ad03/64**
Duration	**D: 00 H: 00 M: 00 S: 00**
Expires	**Fri Sep 27 14:41:50 2013**
IPv4 Address:	**10.10.146.157**
MAC Address:	**00:10:95:de:ad:03**
Duration	**D: 01 H: 00 M: 00 S: 00**
Expires:	**Sat Sep 28 14:07:39 2013**
IPv4 DNS Servers:	**10.10.159.253**
IPv6 DNS Servers:	**None**

WAN Connection Type DHCP

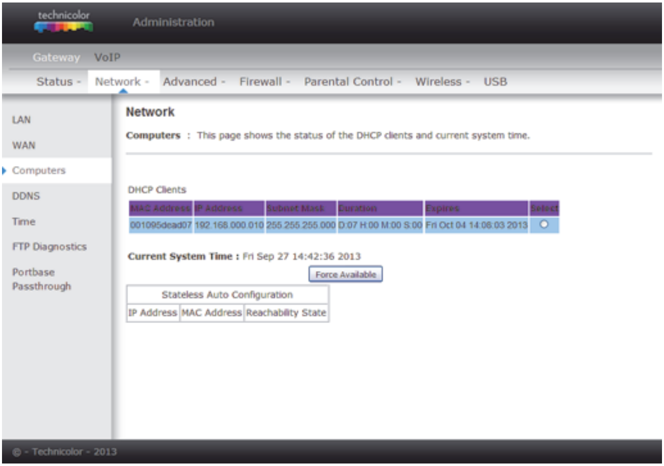
Ipv4 MTU Size 0 (256-1500 octets, 0 = use default)

Spoofed MAC Address 00 : 00 : 00 : 00 : 00 : 00

figure 20: Gateway\Network\WAN

4.3.3 Computers

This page displays the status of the DHCP clients and current system time. You can cancel an IP address lease by selecting it in the DHCP Client Lease Info list and then clicking the Force Available button. If you do so, you may have to perform a DHCP Renew on that PC, so that it can obtain a new lease.



Network

Computers : This page shows the status of the DHCP clients and current system time.

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
001095dead07	192.168.000.010	255.255.255.000	D:07 H:00 M:00 S:00	Fri Oct 04 14:08:03 2013	○

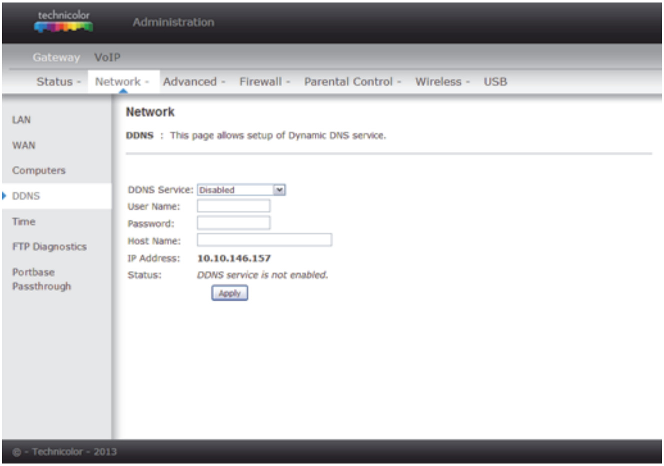
Current System Time : Fri Sep 27 14:42:36 2013

Stateless Auto Configuration		
IP Address	MAC Address	Reachability State

figure 21: Gateway\Network\Computers

4.3.4 DDNS - Dynamic DNS service

This page allows to setup for Dynamic DNS server.



Network

DDNS : This page allows setup of Dynamic DNS service.

DDNS Service: Disabled
User Name:
Password:
Host Name:
IP Address: **10.10.146.157**
Status: *DDNS service is not enabled.*

figure 22: Gateway\Network\DDNS

DDNS Service Choose **Enabled (www.DynDNS.org)** to enable the basic setting. Choose **Disabled** to close the basic setting.

Username The username that you registered with your DDNS provider.

Password The password that you registered with your DDNS provider.

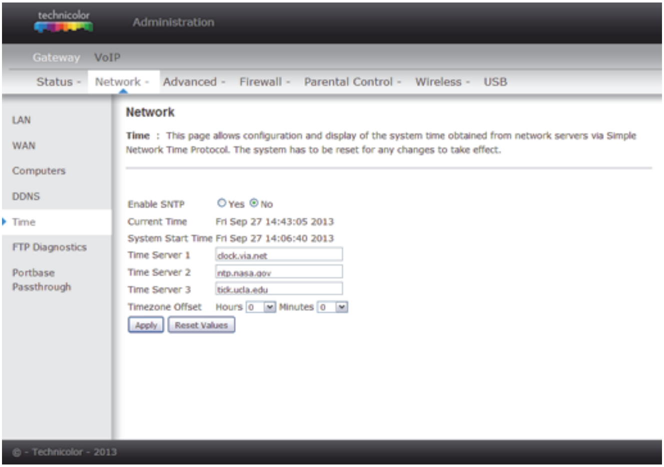
Host Name The domain name or host name that is registered with your DDNS provider.

Status It shows the DDNS service status whether it is enabled or disabled.

Click **Apply** to save the changes.

4.3.5 Time

This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.



Network

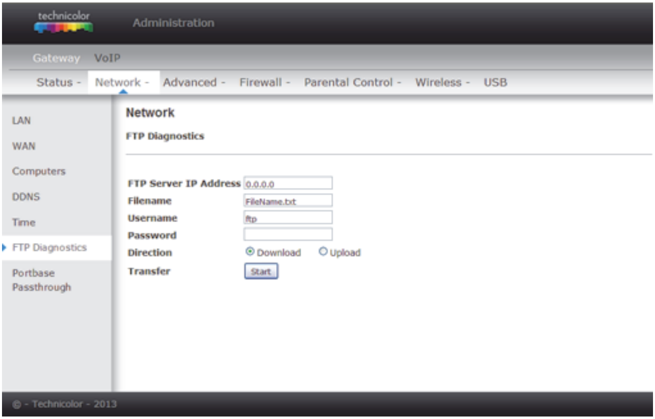
Time : This page allows configuration and display of the system time obtained from network servers via Simple Network Time Protocol. The system has to be reset for any changes to take effect.

Enable SNTP	○ Yes ● No
Current Time	Fri Sep 27 14:43:05 2013
System Start Time	Fri Sep 27 14:06:40 2013
Time Server 1	clock.via.net
Time Server 2	ntp.nasa.gov
Time Server 3	tick.ucla.edu
Timezone Offset	Hours 0 Minutes 0

figure 23: Gateway\Network\Time

4.3.6 FTP Diagnostics

This page allows to test download and upload transmit rate through FTP. Choose known FTP server and Filename with correct username and password then choose direction to Download or Upload. Press the **Start** button to start.



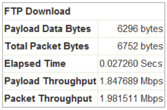
Network

FTP Diagnostics

FTP Server IP Address	0.0.0.0
Filename	FileName.txt
Username	ftp
Password	
Direction	● Download ○ Upload
Transfer	Start

figure 24: Gateway\Network\FTP Diagnostics

You will see the result on the page, when transmit done.

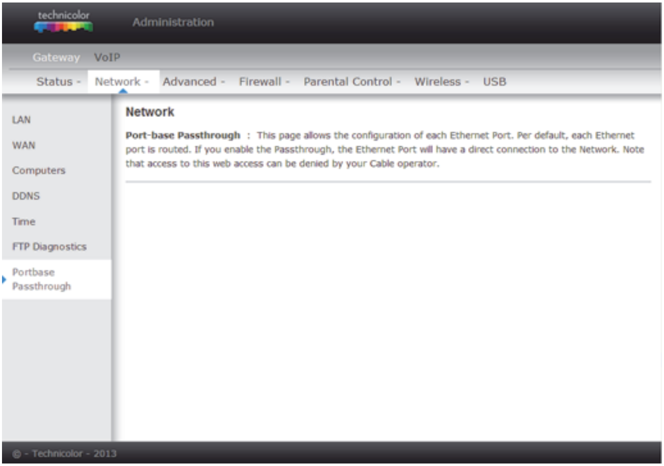


FTP Download	
Payload Data Bytes	6296 bytes
Total Packet Bytes	6752 bytes
Elapsed Time	0.027260 Secs
Payload Throughput	1.847689 Mbps
Packet Throughput	1.981511 Mbps

figure 25: Gateway\Network\FTP Diagnostics\test result

4.3.7 Port-base Passthrough

This page allows the configuration of each Ethernet Port. Per default, each Ethernet port is routed. If you enable the Passthrough, the Ethernet Port will have a direct connection to the Network. Note that access to this web access can be denied by your Cable operator.



Network

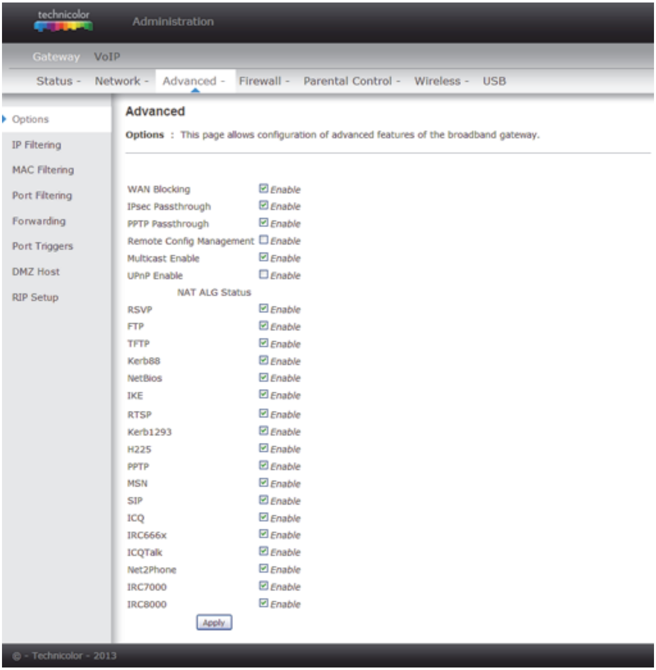
Port-base Passthrough : This page allows the configuration of each Ethernet Port. Per default, each Ethernet port is routed. If you enable the Passthrough, the Ethernet Port will have a direct connection to the Network. Note that access to this web access can be denied by your Cable operator.

figure 26: Gateway\Network\Port-base Passthrough

4.4 Gateway – Advanced Web Page Group

4.4.1 Options

This page allows you to enable/disable some features of the Wireless Voice Gateway.



Advanced

Options : This page allows configuration of advanced features of the broadband gateway.

WAN Blocking	☑ Enable
IPsec Passthrough	☑ Enable
PPTP Passthrough	☑ Enable
Remote Config Management	□ Enable
Multicast Enable	☑ Enable
UPnP Enable	□ Enable
NAT ALG Status	
RSVP	☑ Enable
FTP	☑ Enable
TFTP	☑ Enable
Kerb88	☑ Enable
NetBios	☑ Enable
IKE	☑ Enable
RTSP	☑ Enable
Kerb1293	☑ Enable
H225	☑ Enable
PPTP	☑ Enable
MSN	☑ Enable
SIP	☑ Enable
ICQ	☑ Enable
IRC666x	☑ Enable
ICQTalk	☑ Enable
Net2Phone	☑ Enable
IRC7000	☑ Enable
IRC8000	☑ Enable

figure 27: Gateway\Advanced\Options

WAN Blocking	Prevents others on the WAN side from being able to ping your gateway. With WAN Blocking enabled, your gateway will not respond to pings it receives, effectively “hiding” your gateway.
PPTP PassThrough	Enables PPTP type packets to pass between WAN and LAN. PPTP (Point to Point Tunneling Protocol) is another mechanism sometimes used in VPNs.

Remote Config Management
Mmakes the configuration web pages in your gateway accessible from the WAN side. Note that page access is limited to only those who know the gateway access password. When accessing your gateway from a remote location, your must use HTTP port 8080 and the WAN IP address of the gateway. e.g., if the WAN IP address is 157.254.5.7, you would navigate to **http://157.254.5.7:8080** to reach your gateway.

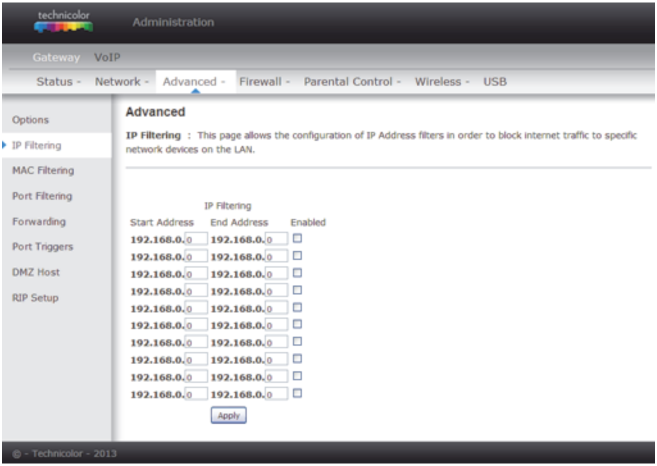
Multicast Enable
Enables multicast traffic to pass between WAN and LAN. You may need to enable this to see some types of broadcast streaming and content on the Internet

UPnP
Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

NAT ALG
NAT ALG (application layer gateways) allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as RSVP, FTP, TFTP, Kerb88, NetBios, IKE, RTSP, Kerb1293, H225, PPTP, MSN, SIP, ICQ, IRC666x, ICQTalk, Net2Phone, IRC7000, IRC8000 file transfer in IM applications etc.
In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

4.4.2 IP Filtering

This page enables you to enter the IP address ranges of PCs on your LAN that you don’t want to have outbound access to the WAN. These PCs can still communicate with each other on your LAN, but packets they send to WAN addresses are blocked by the gateway.



Advanced

IP Filtering : This page allows the configuration of IP Address filters in order to block internet traffic to specific network devices on the LAN.

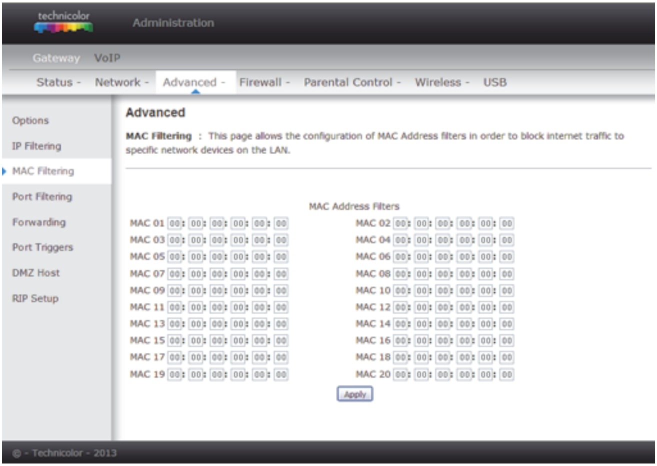
IP Filtering

Start Address	End Address	Enabled
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	☐
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	☐
192.168.0.0	192.168.0.0	☐
192.168.0.0	192.168.0.0	☐

figure 28: Gateway\Advanced\IP Filtering

4.4.3 MAC Filtering

This page enables you to enter the MAC address of specific PCs on your LAN that you do not wish to have outbound access to the WAN. As with IP filtering, these PCs can still communicate with each other through the gateway, but packets they send to WAN addresses are blocked.



Advanced

MAC Filtering : This page allows the configuration of MAC Address filters in order to block internet traffic to specific network devices on the LAN.

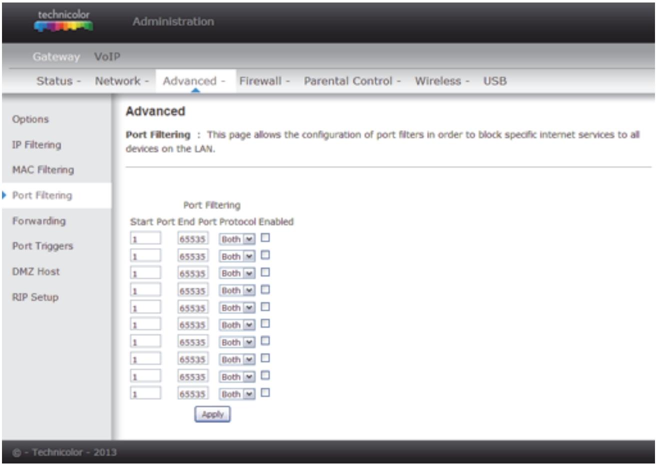
MAC Address Filters

MAC 01	00:00:00:00:00:00	MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00	MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00	MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00	MAC 08	00:00:00:00:00:00
MAC 09	00:00:00:00:00:00	MAC 10	00:00:00:00:00:00
MAC 11	00:00:00:00:00:00	MAC 12	00:00:00:00:00:00
MAC 13	00:00:00:00:00:00	MAC 14	00:00:00:00:00:00
MAC 15	00:00:00:00:00:00	MAC 16	00:00:00:00:00:00
MAC 17	00:00:00:00:00:00	MAC 18	00:00:00:00:00:00
MAC 19	00:00:00:00:00:00	MAC 20	00:00:00:00:00:00

figure 29: Gateway\Advanced\MAC Filtering

4.4.4 Port Filtering

This page allows you to enter ranges of destination ports (applications) that you don't want your LAN PCs to send packets to. Any packets your LAN PCs send to these destination ports will be blocked. For example, you could block access to worldwide web browsing (http = port 80) but still allow email service (SMTP port 25 and POP-3 port 110). To enable port filtering, set Start Port and End Port for each range, and click Apply. To block only one port, set both Start and End ports with the same value.



Advanced

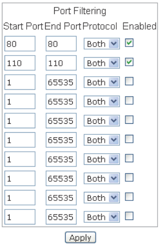
Port Filtering : This page allows the configuration of port filters in order to block specific internet services to all devices on the LAN.

Port Filtering

Start Port	End Port	Protocol	Enabled
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□

figure 30: Gateway\Advanced\Port Filtering

For example: To block HTTP (port 80) browse and restrict mail send from POP-3(port 110), setting as following:



Port Filtering

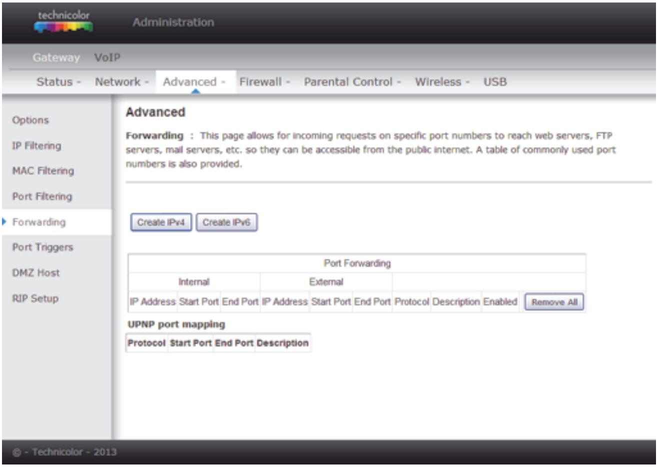
Start Port	End Port	Protocol	Enabled
80	80	Both	☑
110	110	Both	☑
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□
1	65535	Both	□

figure 31: Gateway\Advanced\Port Filtering

Setting port value, block protocol (Both for TCP & UDP), check **Enable** then **Apply**.

4.4.5 Forwarding

For LAN to WAN communications, the gateway normally only allows you to originate an IP connection with a PC on the WAN; it will ignore attempts of the WAN PC to originate a connection onto your PC. This protects you from malicious attacks from outsiders. However, sometimes you may wish for anyone outside to be able to originate a connection to a particular PC on your LAN if the destination port (application) matches one you specify.



Advanced

Forwarding : This page 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.

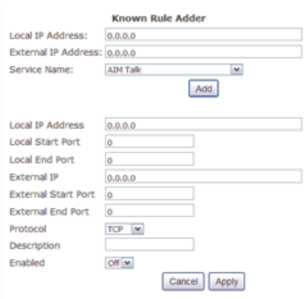
Port Forwarding									
Internal			External						
IP Address	Start Port	End Port	IP Address	Start Port	End Port	Protocol	Description	Enabled	Remove All

UPNP port mapping

Protocol	Start Port	End Port	Description

figure 32: Gateway\Advanced\Forwarding

Press **Create IPv4** button you will see follow options shows on the page. To specify rules, choose **Service Name** or **Port number range** to set up. IP Address 0.0.0.0 means allow all IP address.



Known Rule Adder

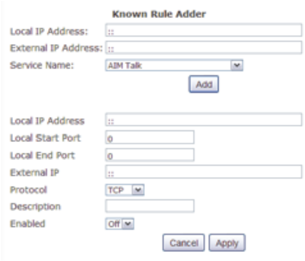
Local IP Address:	0.0.0.0
External IP Address:	0.0.0.0
Service Name:	AIM Talk

Local IP Address	0.0.0.0
Local Start Port	0
Local End Port	0
External IP	0.0.0.0
External Start Port	0
External End Port	0
Protocol	TCP
Description	
Enabled	Off

figure 33: Gateway\Advanced\Forwarding setting

This page allows you to specify up to rules. For example, to specify that outsiders should have access to an FTP server you have running at 192.168.0.5, create a rule with that address and Start Port =20 and End Port =21 (FTP port ranges) and Protocol = TCP (FTP runs over TCP and the other transport protocol, UDP), and click Apply. This will cause inbound packets that match to be forwarded to that PC rather than blocked. As these connections are not tracked, no entry is made for them in the Connection Table. The same IP address can be entered multiple times with different ports.

Press **Create IPv6** button you will see follow options shows on the page. To specify rules, choose **Service Name** or **Port number range** to set up. IP Address 0.0.0.0 means allow all IP address.



Known Rule Adder

Local IP Address:	::
External IP Address:	::
Service Name:	AIM Talk

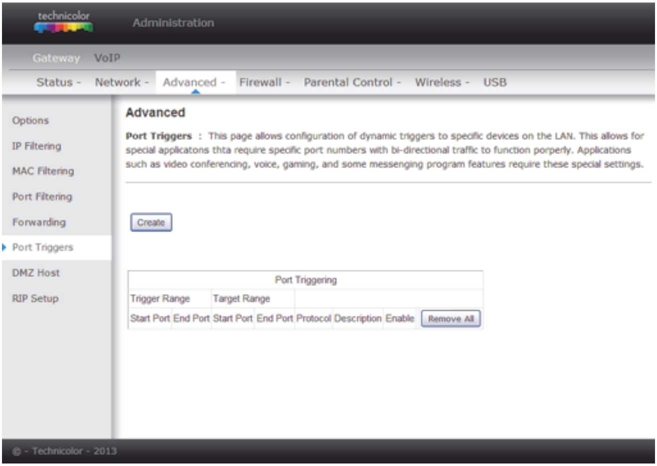
Local IP Address	::
Local Start Port	0
Local End Port	0
External IP	::
Protocol	TCP
Description	
Enabled	Off

figure 34: Gateway\Advanced\Forwarding setting

This page allows you to specify up to rules. For example, to specify that outsiders should have access to an FTP server you have running at 192.168.0.5, create a rule with that address and Start Port =20 and End Port =21 (FTP port ranges) and Protocol = TCP (FTP runs over TCP and the other transport protocol, UDP), and click Apply. This will cause inbound packets that match to be forwarded to that PC rather than blocked. As these connections are not tracked, no entry is made for them in the Connection Table. The same IP address can be entered multiple times with different ports.

4.4.6 Port Triggers

Some Internet activities, such as interactive gaming, require that a PC on the WAN side of your gateway be able to originate connections during the game with your game playing PC on the LAN side. You could use the Advanced-Forwarding web page to construct a forwarding rule during the game, and then remove it afterwards (to restore full protection to your LAN PC) to facilitate this. Port triggering is an elegant mechanism that does this work for you, each time you play the game.



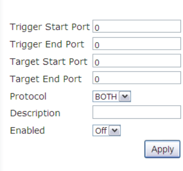
Advanced

Port Triggers : This page allows configuration of dynamic triggers to specific devices on the LAN. This allows for special applicatons thta require specific port numbers with bi-directional traffic to function porperly. Applications such as video conferencing, voice, gaming, and some messenging program features require these special settings.

Port Triggering							
Trigger Range		Target Range					
Start Port	End Port	Start Port	End Port	Protocol	Description	Enable	Remove All

figure 35: Gateway\Advanced\Port Triggers

Press **Create** button to specify rules.



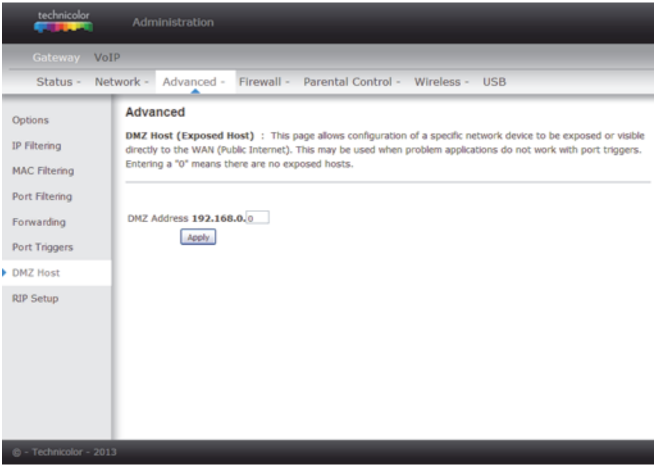
Trigger Start Port	0
Trigger End Port	0
Target Start Port	0
Target End Port	0
Protocol	BOTH
Description	
Enabled	Off

figure 36: Gateway\Advanced\Port Triggers

Port Triggering works as follows. Imagine you want to play a particular game with PCs somewhere on the Internet. You make one time effort to set up a Port Trigger for that game, by entering into **Trigger Start Port** and **Trigger End Port** the range of destination ports your game will be sending to, and entering into **Target Start Port** the range of destination ports the other player (on the WAN side) will be sending to (ports your PC's game receives on). Application programs like games publish this information in user manuals. Later, each time you play the game, the gateway automatically creates the forwarding rule necessary. This rule is valid until 10 minutes after it sees game activity stop. After 10 minutes, the rule becomes inactive until the next matched outgoing traffic arrives.
e.g., suppose you specify Trigger Range from 6660 to 6670 and Target Range from 113 to 113. An outbound packet arrives at the gateway with your game-playing PC source IP address 192.168.0.10, destination port 666 over TCP/IP. This destination port is within the Trigger destined for port 113 to your game-playing PC at 192.168.0.10.

4.4.7 DMZ Host

Use this page to designate one PC on your LAN that should be left accessible to all PCs from the WAN side, for all ports. e.g., if you put an HTTP server on this machine, anyone will be able to access that HTTP server by using your gateway IP address as the destination. A setting of “0” indicates NO DMZ PC. **Host** is another Internet term for a PC connected to the Internet.



Advanced

DMZ Host (Exposed Host) : This page allows configuration of a specific network device to be exposed or visible directly to the WAN (Public Internet). This may be used when problem applications do not work with port triggers. Entering a "0" means there are no exposed hosts.

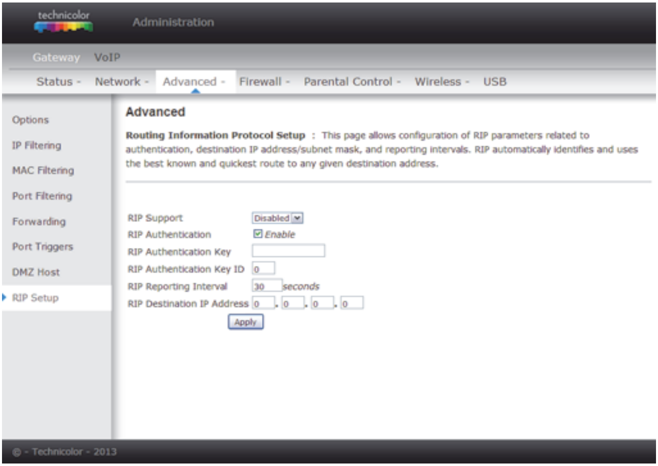
DMZ Address **192.168.0.** 0

figure 37: Gateway\Advanced\DMZ Host

4.4.8 RIP (Routing Information Protocol) Setup

This feature enables the gateway to be used in small business situations where more than one LAN (local area network) is installed. The RIP protocol provides the gateway a means to “advertise” available IP routes to these LANs to your cable operator, so packets can be routed properly in this situation.

Your cable operator will advise you during installation if any setting changes are required here.



Advanced

Routing Information Protocol Setup : This page allows configuration of RIP parameters related to authentication, destination IP address/subnet mask, and reporting intervals. RIP automatically identifies and uses the best known and quickest route to any given destination address.

RIP Support: Disabled
RIP Authentication: ☑ *Enable*
RIP Authentication Key:
RIP Authentication Key ID: 0
RIP Reporting Interval: 30 *seconds*
RIP Destination IP Address: 0 . 0 . 0 . 0

figure 38: Gateway\Advanced\RIP Setup

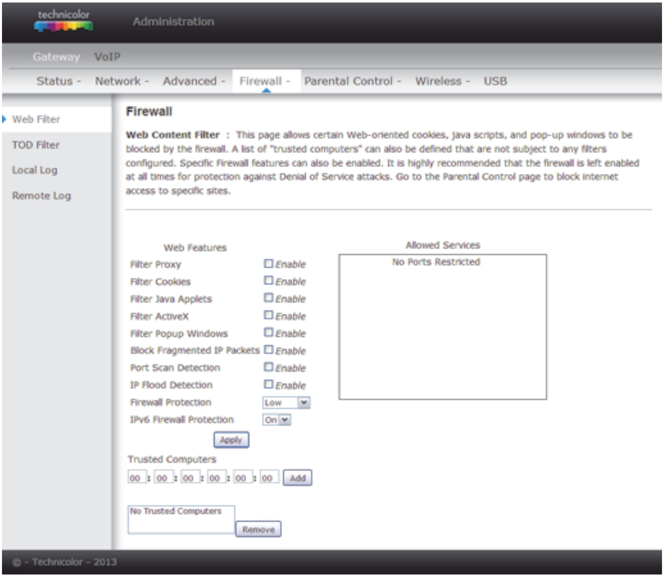
4.5 Gateway – Firewall Web Page Group

4.5.1 Web Content Filtering

These pages allow you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking **Apply**.

The web-related filtering features you can activate from the Web Content Filter page include Filter Proxy, Filter Cookies, Filter Java Applets, Filter ActiveX, Filter Popup Windows, and Firewall Protection.

If you want the gateway to exclude your selected filters to certain computers on your LAN, enter their MAC addresses in the Trusted Computers area of this page.



Firewall

Web Content Filter : This page allows certain Web-oriented cookies, java scripts, and pop-up windows to be blocked by the firewall. A list of "trusted computers" can also be defined that are not subject to any filters configured. Specific Firewall features can also be enabled. It is highly recommended that the firewall is left enabled at all times for protection against Denial of Service attacks. Go to the Parental Control page to block internet access to specific sites.

Web Features	
Filter Proxy	□ Enable
Filter Cookies	□ Enable
Filter Java Applets	□ Enable
Filter ActiveX	□ Enable
Filter Popup Windows	□ Enable
Block Fragmented IP Packets	□ Enable
Port Scan Detection	□ Enable
IP Flood Detection	□ Enable
Firewall Protection	Low
IPv6 Firewall Protection	On

Allowed Services

No Ports Restricted

Trusted Computers

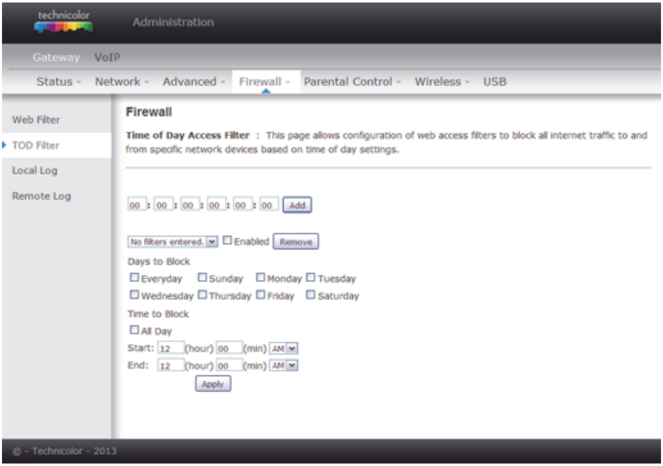
00 : 00 : 00 : 00 : 00 : 00

No Trusted Computers

figure 39: Gateway\Firewall\Web Filter

4.5.2 TOD Filtering

Use this page to set rules that will block specific LAN side PCs from accessing the Internet, but only at specific days and times. Specify a PC by its hardware MAC address, and then use the tools to specify blocking time. Finally, click the **Apply** button to save your settings.



Firewall

Time of Day Access Filter : This page allows configuration of web access filters to block all internet traffic to and from specific network devices based on time of day settings.

00 : 00 : 00 : 00 : 00 : 00

No filters entered. □ Enabled

Days to Block

□ Everyday □ Sunday □ Monday □ Tuesday
□ Wednesday □ Thursday □ Friday □ Saturday

Time to Block

□ All Day

Start: 12 (hour) 00 (min) AM
End: 12 (hour) 00 (min) AM

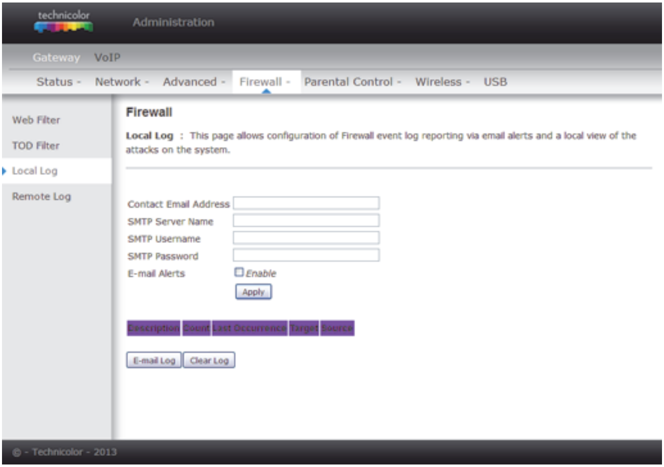
© - Technicolor - 2013

figure 40: Gateway\Firewall\TOD Filtering

4.5.3 Local Log

The gateway builds a log of firewall blocking actions that the firewall has taken. Using the Local Log page lets you specify an email address to which you want the gateway to email this log. You must also tell the gateway your outgoing (i.e. SMTP) email server's name, so it can direct the email to it. Enable Email Alerts has the gateway forward email notices when Firewall protection events occur. Click **E-mail Log** to immediately send the email log. Click **Clear Log** to clear the table of entries for a fresh start.

The log of these events is also visible on the screen. For each blocking event type that has taken place since the table was last cleared, the table shows Description, Count, Last Occurrence, Target, and Source.



Firewall

Local Log : This page allows configuration of Firewall event log reporting via email alerts and a local view of the attacks on the system.

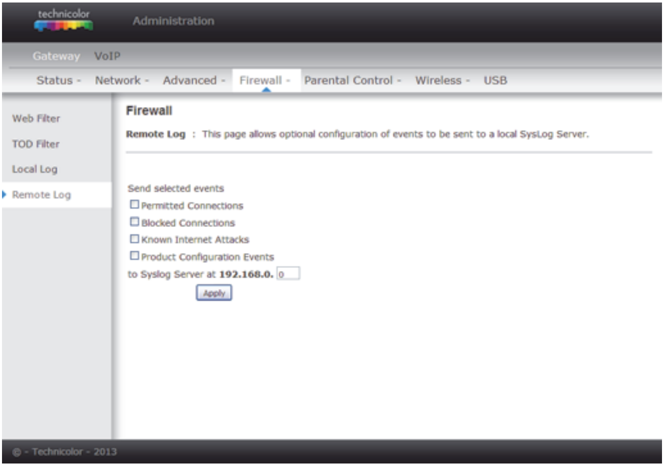
Contact Email Address
SMTP Server Name
SMTP Username
SMTP Password
E-mail Alerts ☐ *Enable*

Description	Count	Last Occurrence	Target	Source

figure 41: Gateway\Firewall\Local Log

4.5.4 Remote Log

The Remote Log page allows you to specify the IP address where a SysLog server is located on the LAN Side and select different types of firewall events that may occur. Then, each time such an event occurs, notification is automatically sent to this log server.



Firewall

Remote Log : This page allows optional configuration of events to be sent to a local SysLog Server.

Send selected events

□ Permitted Connections
□ Blocked Connections
□ Known Internet Attacks
□ Product Configuration Events

to Syslog Server at **192.168.0.** 0

Apply

figure 42: Gateway\Firewall\Remote Log

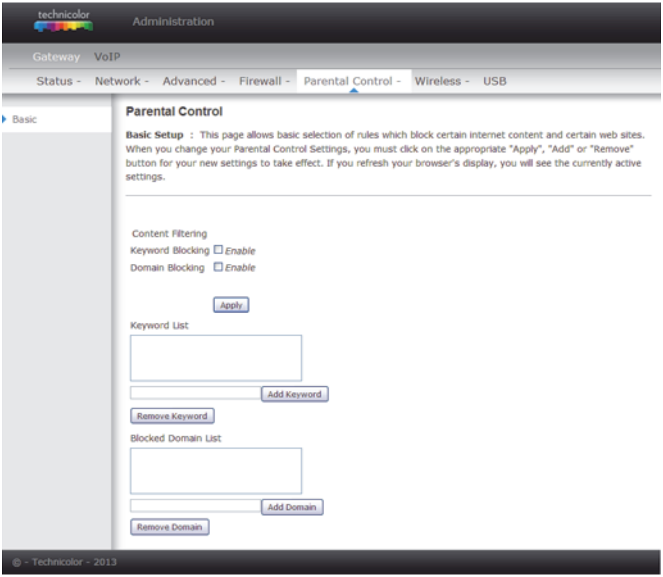
4.6 Gateway – Parental Control Web Page Group

4.6.1 Basic

This page allows you to enable, disable, and configure a variety of firewall features associated with web browsing, which uses the HTTP protocol and transports HTML web pages. On these pages, you designate the gateway packet types you want to have forwarded or blocked. You can activate settings by checking them and clicking **Apply**.

Here are some of your choices on the Parental Control page:

- Activate **Keyword Blocking** and specify some keywords in the **Keyword List** to cause blocking of web pages on the WAN side with the specified keyword in the content.
- Activate **Domain Blocking** and specify some Domain Names (e.g. www.ABC.com) in the **Domain List**.



Parental Control

Basic Setup : This page allows basic selection of rules which block certain internet content and certain web sites. When you change your Parental Control Settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.

Content Filtering
Keyword Blocking □ *Enable*
Domain Blocking □ *Enable*

figure 43: Gateway\Parental Control\Basic

4.7 Gateway – Wireless Web Page Group

The Wireless web pages group enables a variety of settings that can provide secure and reliable wireless communications for even the most demanding tech-savvy user.

The Wireless Voice Gateway offers a choice of 802.11b/g/n, WPA and WPA-PSK authentication of your PCs to the gateway, 64 and 128 bit WEP encryption of communication between the gateway and your PCs to guaranty security, and an Access Control List function that enables you to restrict wireless access to only your specific PCs.

Performance

Because your wireless communication travels through the air, the factory default wireless channel setting may not provide optimum performance in your home if you or your neighbors have other interfering 2.4GHz or 5 GHz devices such as cordless phones. If your wireless PC is experiencing very sluggish or dramatically slower communication compared with the speed you achieve on your PC that is wired to the gateway, try changing the channel number. See the 802.11b/g/n Basic Web Page discussion below for details.

Authentication

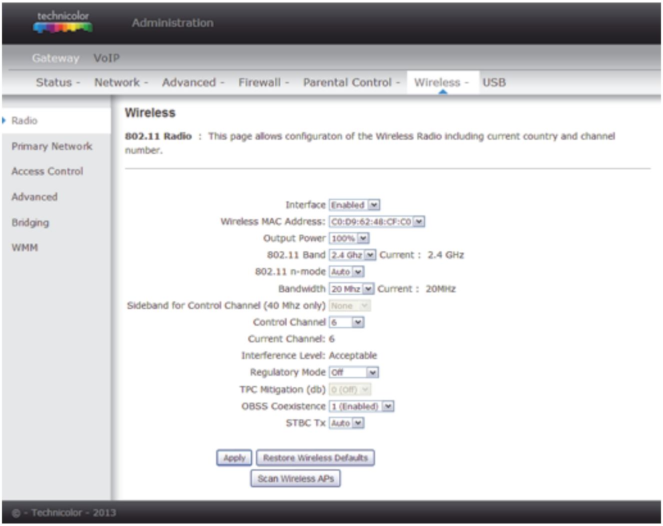
Authentication enables you to restrict your gateway from communicating with any remote wireless PCs that aren't yours. The following minimum authentication-related changes to factory defaults are recommended. See the 802.11b/g/n Basic and Access Control Web Page discussions below for details.
Network Name (SSID) – Set a unique name you choose
Network Type – Set to Open
Access Control List – Enter your wireless PCs' MAC addresses

Security

Security secures or scrambles messages traveling through the air between your wireless PCs and the gateway, so they can't be observed by others. The following minimum security setting changes to factory defaults are recommended. See the 802.11b/g/n Security Web Page discussion below for details.

4.7.1 Radio

To set the basic configuration for the wireless features, click RADIO from the Wireless menu. These must match the settings you make on your wireless-equipped PC on the LAN side.



Wireless

802.11 Radio : This page allows configuraton of the Wireless Radio including current country and channel number.

Interface Enabled
Wireless MAC Address: C0:D9:62:48:CF:C0
Output Power 100%
802.11 Band 2.4 Ghz Current : 2.4 GHz
802.11 n-mode Auto
Bandwidth 20 Mhz Current : 20MHz
Sideband for Control Channel (40 Mhz only) None
Control Channel 6
Current Channel: 6
Interference Level: Acceptable
Regulatory Mode Off
TPC Mitigation (db) 0 (Off)
OBSS Coexistence 1 (Enabled)
STBC Tx Auto

figure 44: Gateway/Wireless/Radio

Interface

The wireless radio in your gateway can be completely de-activated by changing Interface to Disabled. Click the Apply button to save your settings. Activated by changing interface to enabled

Wireless MAC address

The MAC address for this wireless device will be displayed in this field automatically.

Output power

This setting decides the output power of this device. You may use it to economize on electricity by selecting lower percentage of power output. Control the range of the AP by adjusting the radio output power.

802.11 Band

It Support 2.4 GHz and 5 GHz band. This default band was 2.4 GHz.

802.11 n-mode It may help you to Enable or Disable the 11N mode. To enable you need to select Auto, to disable you need to select Off, and so force the AP to operate in 802.11 n-mode.

Bandwidth Select wireless channel width 20 MHz is for default value (bandwidth taken by wireless signals of this access point.)

Sideband for Control Channel (40 MHz only) There is “Lower” and “Upper” can be selected if Bandwidth 40 MHz was Enabled.

Control Channel In 802.11 Band 2.4GHz, there are 1 to 13 channels. In 802.11 Band 5GHz, there are 36, 40, 44, 48 total 4 channels for all country. Choose the one that is suitable for this device.

Current Channel The channel that you choose will be displayed in this field.

Regulatory Mode suppose 802.11d and 802.11h to satisfy specific environment and request.

TPC Mitigation (db) Fixed Maximum TX Power Level, options 0 ~ 4 db

OBSS Coexistence Overlapping BBS coexistence, here to control this function Enable or Disable, default was enabled.

STBC Tx Space–time block coding is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data-transfer. Default was “Auto”.

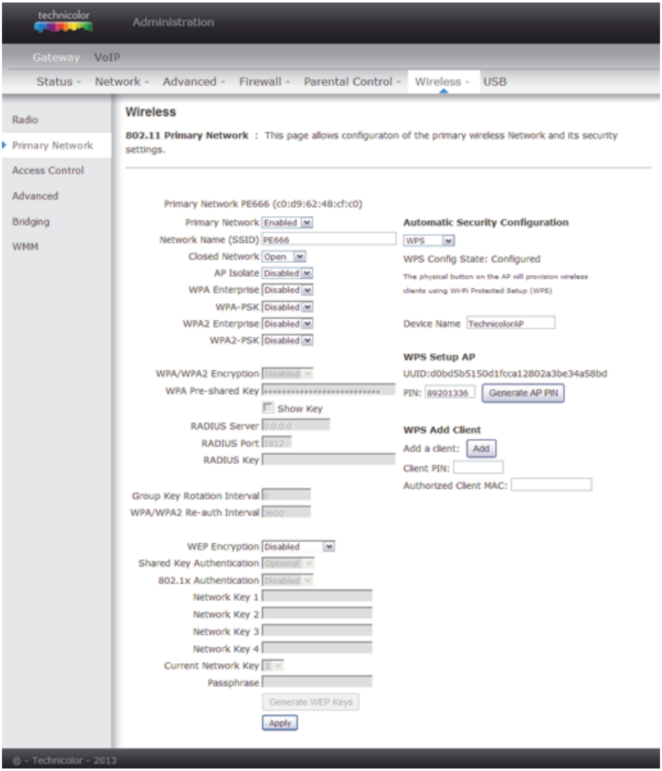
Restore Wireless defaulfs To recover to the default settings, press this button to retrieve the settings then click Apply.

Setting	Description	Value List or Range	Default
Network Name (SSID)	Set the Network Name (also known as SSID) of this network.	Up to 32-character string containing ASCII characters only	PExxx
Network Type	Select Closed to hide the network from active scans. Select Open to reveal the network to active scans.	Open, Closed	Open
New Channel	Select a particular channel on which to operate.	1-13	1 or 6 or 11
Interface	Enable or disable the wireless interface.	Enabled, Disabled	Enabled

table 3: Basic Settings Definitions

4.7.2 Primary Network

This page allows you to configure the Network Authentication. It provides several different modes of wireless security. You will have to enter proper information according to the mode you select.



Wireless

802.11 Primary Network : This page allows configuraton of the primary wireless Network and its security settings.

Primary Network PE666 (c0:d9:62:48:cf:c0)

Primary Network	Enabled
Network Name (SSID)	PE666
Closed Network	Open
AP Isolate	Disabled
WPA Enterprise	Disabled
WPA-PSK	Disabled
WPA2 Enterprise	Disabled
WPA2-PSK	Disabled
WPA/WPA2 Encryption	Disabled
WPA Pre-shared Key	**************************
	□ Show Key
RADIUS Server	0.0.0.0
RADIUS Port	1812
RADIUS Key	
Group Key Rotation Interval	0
WPA/WPA2 Re-auth Interval	3600
WEP Encryption	Disabled
Shared Key Authentication	Optional
802.1x Authentication	Disabled
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	1
Passphrase	

Automatic Security Configuration

WPS

WPS Config State: Configured

The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)

Device Name: TechnicolorAP

WPS Setup AP

UUID:d0bd5b5150d1fcca12802a3be34a58bd

PIN: 89201336

WPS Add Client

Add a client:

Client PIN:

Authorized Client MAC:

figure 45: Gateway\Wireless\Primary Network

802.11x Authentication introduction

If you enable the 802.11x authentication function, you will have to offer the following information.

WPA/WPA2 (Wi-fi Protected Access) It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It can provide stronger encryption and authentication solution than none WPA modes. WPA2 is the second generation of WPA security.

WPA-PSK/WPA2-PSK (WPA-Pre-Shared Key) It is useful for small places without authentication servers such as the network at home. It allows the use of manually-entered keys or passwords and is designed to be easily set up for home users.

RADIUS Server RADIUS Server is a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. Please key in the IP Address for the RADIUS Server.

RADIUS Port Besides the IP address of the RADIUS Server, you have to enter the port number for the server. Port 1812 is the reserved RADIUS-authentication port described in RFC 2138. Earlier AP (RADIUS clients) use port 1945. The default value will be shown on this box. You can keep and use it.

RADIUS Key A RADIUS Key is like a password, which is used between IAS and the specific RADIUS client to verify identity. Both IAS and the RADIUS client must be use the same RADIUS Key for successful communication to occur. Enter the RADIUS Key.

WPA/WPA2

For the WPA/WPA2 network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, RADIUS Server, RADIUS Port, RADIUS Key, Group Key Rotation Interval, and WPA/WPA2 Re-auth Interval.

WPA/WPA2 Encryption

There are two types that you can choose, **AES, TKIP+AES**.

TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this mater key. Then it regularly changes and rotates the encryption keys so that the same encryption key will never be used twice

AES provides security between client workstations operating in ad hoc mode. It uses a mathematical ciphering algorithm that employs variable key sizes of 128, 192 or 256 bits.

RADIUS Server / RADIUS Port / RADIUS Key

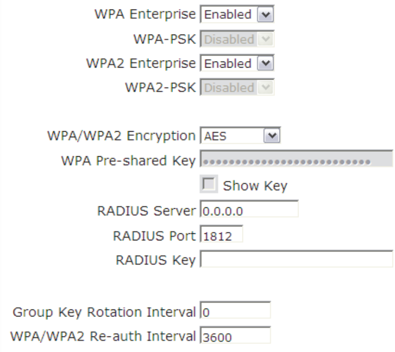
Please refer to the previous page.

Group Key Rotation Interval

Key in the time for the WAP group key rotation interval. The unit is second. With increasing rekey interval, user bandwidth requirement is reduced.

WPA/WPA2 re-auth Interval

When a wireless client has associated with the Wireless Voice Gateway for a period of time longer than the setting here, it would be disconnected and the authentication will be executed again. The default value is 3600, you may modify it.



WPA Enterprise: Enabled
WPA-PSK: Disabled
WPA2 Enterprise: Enabled
WPA2-PSK: Disabled

WPA/WPA2 Encryption: AES
WPA Pre-shared Key: ••••••••••••••••••••••••••
□ Show Key
RADIUS Server: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:

Group Key Rotation Interval: 0
WPA/WPA2 Re-auth Interval: 3600

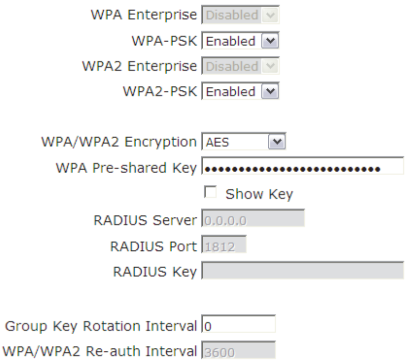
figure 46: WPA/WPA2

WPA-PSK/ WPA2-PSK

For the WPA-PSK/WPA2-PSK network Authentication, the settings that you can adjust including WPA/WPA2 Encryption, WPA Pre-Shared Key, and Group key Rotation Interval.

WPA Pre-Shared Key

Please type the key to be between 8 and 63 characters, or 64 hexadecimal digits. Only the devices with a matching key that you set here can join this network.



WPA Enterprise: Disabled
WPA-PSK: Enabled
WPA2 Enterprise: Disabled
WPA2-PSK: Enabled

WPA/WPA2 Encryption: AES
WPA Pre-shared Key: ••••••••••••••••••••••••••
□ Show Key
RADIUS Server: 0.0.0.0
RADIUS Port: 1812
RADIUS Key:

Group Key Rotation Interval: 0
WPA/WPA2 Re-auth Interval: 3600

figure 47: WPA-PSK / WPA2-PSK

WEP Encryption

You can choose **64-bit** or **128-bit** according to your needs. If you choose **Disabled**, the Network Keys will not be shown on this page. If selected, the data is encrypted using the key before being transmitted. e.g., If you set 128-bit in this field, then the receiving station must be set to use the 128 Bit Encryption, and have the same Key value too. Otherwise, it will not be able to decrypt the data.

Let op!

You need to connect one end of the Ethernet cable to the Ethernet port on the back of your computer, and the other end to the ETHERNET port on the Wireless Voice Gateway.

If you select WEP (**64-bit** or **128-bit**), you can adjust the following settings.

Shared Key Authentication Decide whether to set the shared key **Optional** or **Required** by selecting from the drop-down menu

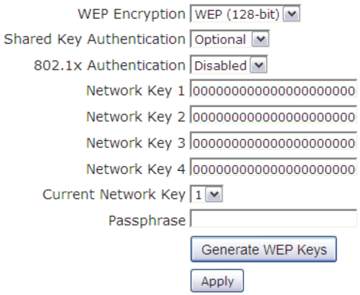
Network Key 1 to 4 The system allows you to enter four sets of the WEP key. For **64-bit** WEP mode, the key length is 5 characters or 10 hexadecimal digits. As for **128-bit** WEP mode, the key length is 13 characters or 26 hexadecimal digits

Current Network Key Select one set of the network key (from 1 to 4) as the default one.

Passphrase You can enter ASCII codes into this field. The range is from 8 characters to 64 characters. For ASCII characters, you can key in 63 characters in this field. If you want to key in 64 characters, only hexadecimal characters can be used.

Generate WEP Keys Click this button to generate the Passphrase.

Apply After proper configuration, click Apply to invoke the settings.



WEP Encryption: WEP (128-bit)
Shared Key Authentication: Optional
802.1x Authentication: Disabled
Network Key 1: 000000000000000000000
Network Key 2: 000000000000000000000
Network Key 3: 000000000000000000000
Network Key 4: 000000000000000000000
Current Network Key: 1
Passphrase:

figure 48: WEP (64-bit) / WEP (128-bit)

Automatic Security Configuration

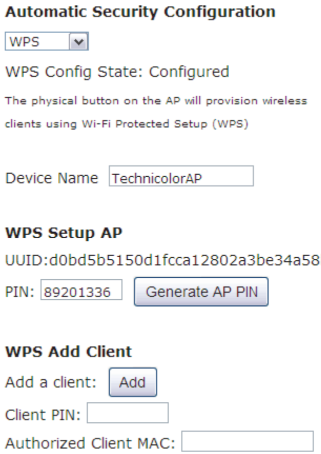
Wi-Fi Protected Setup^{TM} (WPS) is an easy and secure way of configuring and connecting your Wireless access point. In this case, the Wireless Voice Gateway is the Access Point (AP), and Your PC (or Wireless Device) is called the STA. When configuring your Wireless Network via WPS, Messages are exchanged between the STA and AP in order to configure the Security Settings on both devices.

WPS Configuration
It will help you to **Enable** or **Disable** the WPS feature. To enable you need to select **WPS**, to disable you need to select **Disabled**.
Note: After you Enable the WPS you will get the options as show in Fig.2-36 and the WPS Configuration State box will show its configuration status.

Device Name
By using this you can change the factory default to a name of your choice which is up to 32 characters long as like **SSID**.

WPS Setup AP
Here you do not need to change anything, just skip this step.

WPS Add Client
There are two methods type"Client PIN" and "Authorized Client MAC". Type in the client information you want. Then press button "add".



Automatic Security Configuration

WPS

WPS Config State: Configured

The physical button on the AP will provision wireless clients using Wi-Fi Protected Setup (WPS)

Device Name: TechnicolorAP

WPS Setup AP

UUID:d0bd5b5150d1fcca12802a3be34a58bd

PIN: 89201336 [Generate AP PIN]

WPS Add Client

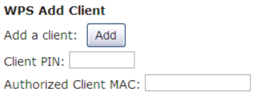
Add a client: [Add]

Client PIN:

Authorized Client MAC:

figure 49: Automatic Security Configuration

If you type in **Client PIN**, then the **WPS Add Client** option will appear as shown below.



WPS Add Client

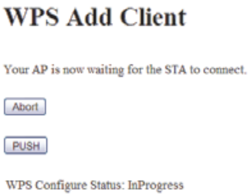
Add a client: [Add]

Client PIN:

Authorized Client MAC:

figure 50: WPS/Push-Button

And then if you click “Add” button then WPS Add Client page will appear as shown in Fig. 38.



WPS Add Client

Your AP is now waiting for the STA to connect.

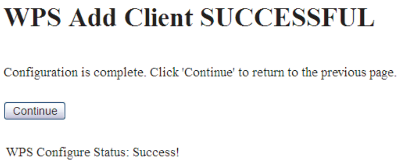
[Abort]

[PUSH]

WPS Configure Status: InProgress

figure 51: WPS Setup AP/PUSH

And **WPS Configure Status** will be “In progress”, after establishing the connection the **WPS Configure Status** will be “Success!” as shown below. After succesful connection the client will get IP adress from AP and then internet will be accessible.



WPS Add Client SUCCESSFUL

Configuration is complete. Click 'Continue' to return to the previous page.

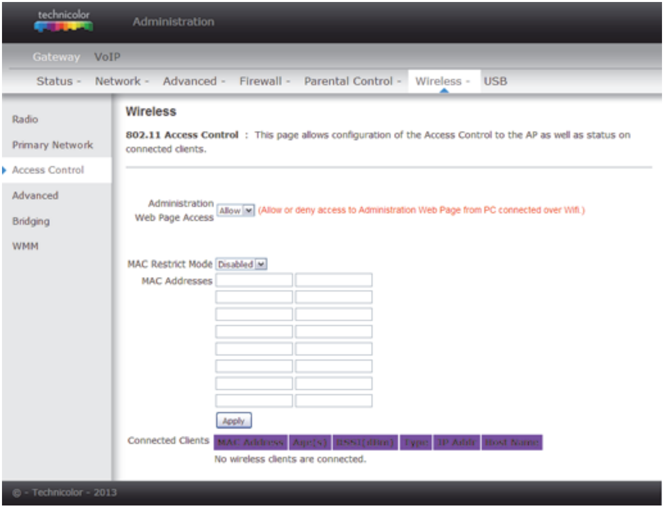
WPS Configure Status: Success!

figure 52: WPS Setup AP successful/PUSH

WPS Add Client process also can finish with type in Authorized Client MAC.

4.7.3 Access Control

This page allows you to control device that can connect to the AP and list all connected clients. Control is made by Mac Address.



Wireless

802.11 Access Control : This page allows configuration of the Access Control to the AP as well as status on connected clients.

Administration Web Page Access: Allow (Allow or deny access to Administration Web Page from PC connected over Wifi.)

MAC Restrict Mode: Disabled

MAC Addresses

Connected Clients

MAC Address	Age(s)	RSSI(dBm)	Type	IP Addr	Host Name

No wireless clients are connected.

figure 53: Gateway\Wireless\Access Control

Administration Web Page Access	This field let you decide if a PC connected over Wi-Fi to the Gateway can have access to the Gateway Web Pages.

MAC Restrict Mode Click **Disabled** to welcome all of the clients on the network; select **Allow** to permit only the clients on the list to access the cable modem; or choose **Deny** to prevent the clients on the list to access this device.

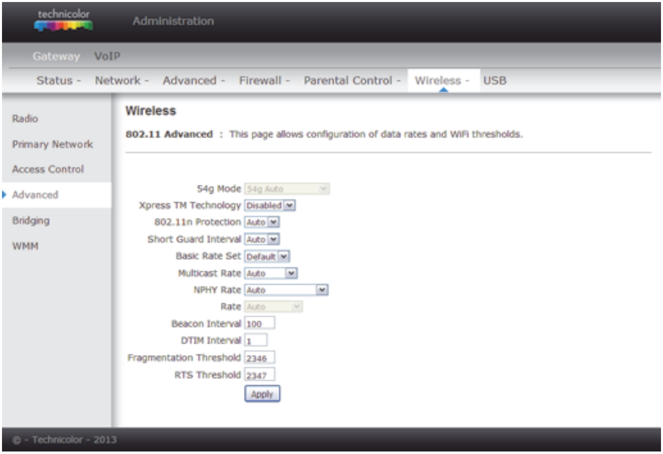
MAC Address Your Gateway identifies wireless PCs by their Wireless MAC Address. This address consists of a string of 6 pairs of numbers 0-9 and letters A-F, such as 00 90 4B F0 FF 50. It is usually printed on the Wireless card of the device (e.g. the PCMCIA card in a laptop).

Apply After proper configuration, click Apply to invoke the settings.

Connected Clients: The information of currently connected clients will be displayed here.

4.7.4 Advanced

This page allows you to configure some advanced settings. The factory default values should provide good results in most cases. We don't recommend you change these settings unless you have technical knowledge of 802.11 wireless technology. For expert users, details of all settings on this web page are provided below.



Wireless

802.11 Advanced : This page allows configuration of data rates and WiFi thresholds.

54g Mode: 54g Auto
Xpress TM Technology: Disabled
802.11n Protection: Auto
Short Guard Interval: Auto
Basic Rate Set: Default
Multicast Rate: Auto
NPHY Rate: Auto
Rate: Auto
Beacon Interval: 100
DTIM Interval: 1
Fragmentation Threshold: 2346
RTS Threshold: 2347

figure 54: Gateway\Wireless\Advanced

54^{TM} Mode

Except Auto Mode, there are three modes for you choose, please check the specification of your wireless card and choose a proper setting.

Xpress^{TM} Technology

When Xpress is turned on, aggregate throughput (the sum of the individuel throughput speeds of each client on the network) can improve by up to 27% in 802.11g-only networks, and up to 75% in mixed networks comprised of 802.11g and 802.11b standard equipment.

801.11n Protection

This method provides 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Default is “Auto”.

Short Guard Interval

To reduce complexity, manufacturers typically only implement a shot guard interval as a final rate adaptation step when the device is running at it's highest data rate. Default is “Auto”.

Basis Rate Set The rates that for all clients want to associate with. Choose “Default” and “All” for the 802.11a/b/g/n/ac.

Multicast Rate The baseline levels that wireless device able to deliver in order to connect to the wireless voice gateway. Lower multicast rates mean weaker, farther signals are allowed to connection. Higher multicast rates mean that only close, strong signals are allowed.

NPHY Rate Set the Physical Layer rate. The rate always set “Use Legacy Rate”.

Rate It decides the speed of data transmission. There are serveral rates provided here for you to choose. Choose any one of it according to your needs by using the drop-down menu.

Beacon Interval Set the period of beacon transmissions to allow mobile stations to locate and identify a BSS. The measure unit it “time units” (TU) of 1024 microseconds. (Value range: 1~65535).

DTIM Interval The value you set here is used to inform mobile stations when mutlicast frames that have been buffered at the Wireless Voice Gateways will be delivered and how often that delivery occurs (Value range: 1~255).

Fragmentation Threshold Set the number of the fragmentating frames to make the data to be delivered without errors induced by the interference. Frames longer than the value you set here are fragmented before the initial transmission into fragments no longer than the value of the threshold (Value range: 256~2346).

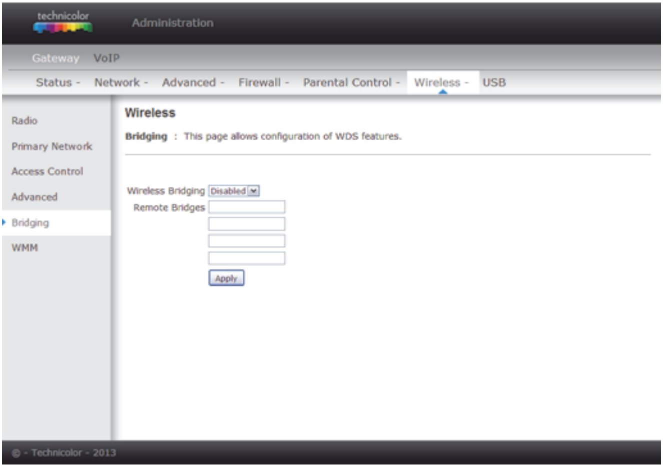
RTS Threshold Set the value for sending a request to the destination. All the frames of a length greater than the threshold that you set here will be sent with the four-way frame exchange. And, a lenth less than or equal to the value that you set will not be proceeded by RTS (Value range: 0~2347).

4.7.5 Bridging

The Bridging page provides a location where settings can be adjusted related to the WDS (**Wireless Distribution System**) feature.

WDS is a system that enables the interconnection of access points wirelessly. It may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging).

The wireless gateway can be placed in a mode that allows the gateway to communicate with other “extender” wireless access points either exclusively or mixed with communications to local PCs. Use this page to designate the Remote Bridges the gateway is allowed to communicate with, and to select the Wireless Bridging mode.



Wireless

Bridging : This page allows configuration of WDS features.

Wireless Bridging: Disabled

Remote Bridges

figure 55: Gateway\Wireless\Bridging

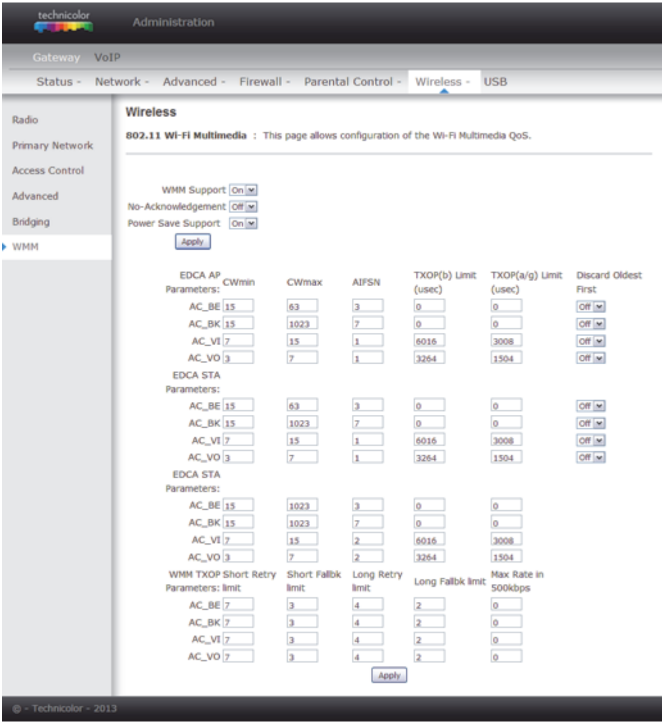
Wireless Bridging
Choose “Disabled” to shutdown this function; select Enabled to turn on the function of WDS.

Remote Bridges
Enter the MAC addresses of the remote Bridges to realy the signals for each other.

Apply
After proper configuration, click Apply to invoke the settings.

4.7.6 802.11 Wi-fi Multimedia

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). The QoS assigns priority to the selected network traffic and prevents packet collisions and delays thus improving VoIP calls and watching video over WLANs.



Wireless

802.11 Wi-Fi Multimedia : This page allows configuration of the Wi-Fi Multimedia QoS.

WMM Support: On

No-Acknowledgement: Off

Power Save Support: On

EDCA AP Parameters:	CWmin	CWmax	AIFSN	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Discard Oldest First
AC_BE	15	63	3	0	0	Off
AC_BK	15	1023	7	0	0	Off
AC_VI	7	15	1	6016	3008	Off
AC_VO	3	7	1	3264	1504	Off
EDCA STA Parameters:						
AC_BE	15	63	3	0	0	Off
AC_BK	15	1023	7	0	0	Off
AC_VI	7	15	1	6016	3008	Off
AC_VO	3	7	1	3264	1504	Off
EDCA STA Parameters:						
AC_BE	15	1023	3	0	0	
AC_BK	15	1023	7	0	0	
AC_VI	7	15	2	6016	3008	
AC_VO	3	7	2	3264	1504	

WMM TXOP Parameters:	Short Retry limit	Short Fallbk limit	Long Retry limit	Long Fallbk limit	Max Rate in 500kbps
AC_BE	7	3	4	2	0
AC_BK	7	3	4	2	0
AC_VI	7	3	4	2	0
AC_VO	7	3	4	2	0

figure 56: Gateway\Wireless\WMM

Enable WWM	This field allows you to enable WMM to improve multimedia transmission.
Enable WWM No-Acknowledgment	This field allows you to enable WMM No-Acknowledgement.
Power Save Support	This field allows you to enable WMM Power-Save-Support.

EDCA AP parameters

proposal : specifies the transmit parameter for traffic transmitted from the AP to the STA for the 4 Access Categories: Best effort (AC_BE), Background (AC_BK) Video (AC_VI) and voice (AC_VO). Transmit parameters include contention window (CWmin CWmax), arbitration Inter Frame Spacing Number AIFSN, and Transmit opportunity Limit (TXOP limit). Admission Control specifies if admission control is enforced for the Access categories. Discard Oldest first specified the discard policy for the queues , On discards the oldest first; off discards the newest first.

EDCA STA parameters

proposal : specifies the transmit parameter for traffic transmitted from the STA to the AP for the 4 Access Categories: Best effort (AC_BE), Background (AC_BK) Video (AC_VI) and voice AC_VO. Transmit parameters include contention window (CWmin CWmax), arbitration Inter Frame Spacing Number AIFSN, and Transmit opportunity Limit (TXOP limit).

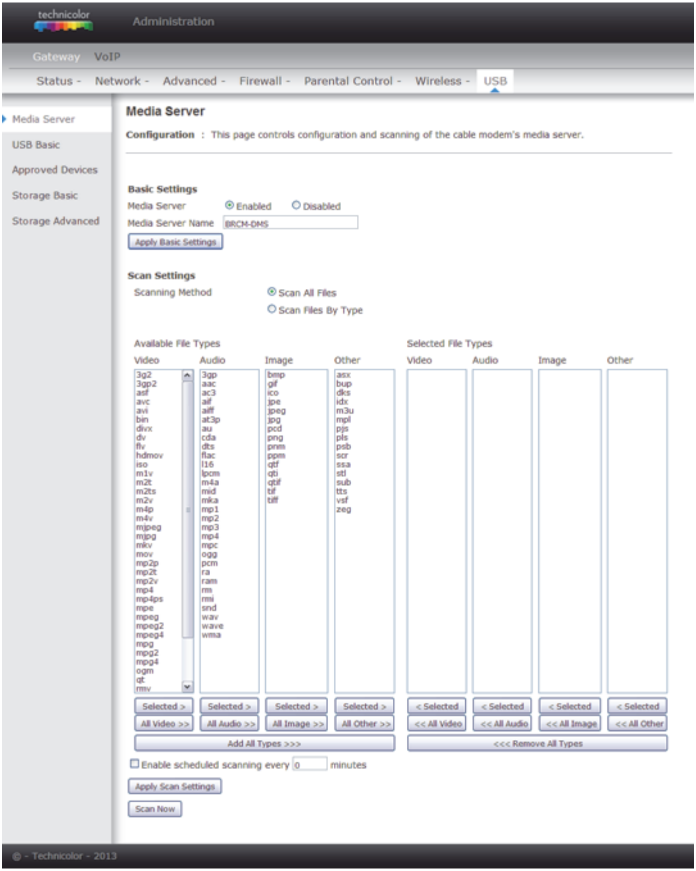
WMM TXOP parameters

proposal : specifies the transmit parameter for traffic transmitted from the TXOP to the AP for the 4 Access Categories: Best effort (AC_BE), Background (AC_BK) Video (AC_VI) and voice(AC_VO). Transmit parameters include Short Retry Limit, Short Fallbk Limit, Long Retry Limit, Long Fallbk Limit, and Max Rate in 500kbps.

4.8 Gateway – USB Web Page Group

4.8.1 Media Server

This page controls configuration and scanning of the Gateway's media server. Choose Scan all Files will scan your approved USB devices for sharing files. Scan Files by Type for specific file type or all of types for sharing. Choose file types form **Available File Types** to **Selected File Types**.



Media Server

Configuration : This page controls configuration and scanning of the cable modem's media server.

Basic Settings

Media Server ● Enabled ○ Disabled

Media Server Name BRCM-DMS

Scan Settings

Scanning Method ● Scan All Files ○ Scan Files By Type

□ Enable scheduled scanning every 0 minutes

figure 57: Gateway/USB/Media Server

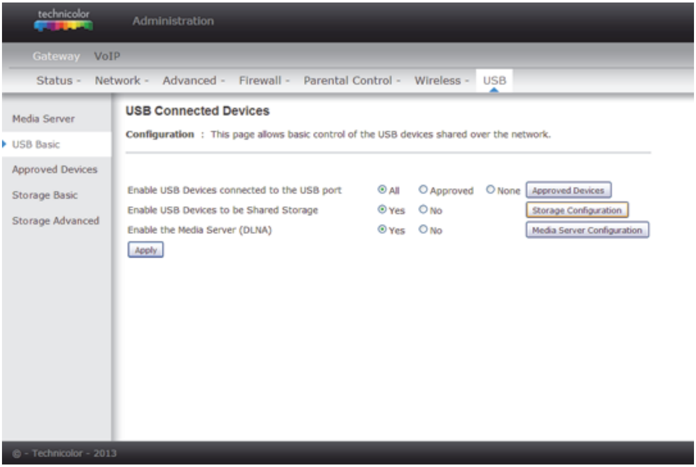
4.8.2 USB Basic settings

This page allows basic control of the USB devices shared over the network.

Enable USB Devices connected to the USB port: This field controls which USB device (Key or Hard Disk) can be connected to the Gateway. **All** will authorize all USB devices. **Approved** will authorize devices that have been previously approved on this gateway. **None** will block any USB Device on the Gateway. To approve devices (PC), click on the button **Approved Devices**.

Enable USB Devices to be Shared Storage **Yes** or **No** to decide if you share or not the content of the USB device. Click on **Storage Configuration** button to access the web pages to configure the Storage Device.

Enable the Media Server (DLNA) **Yes** or **No** to activate or the not the DLNA Server (DLNA: Digital Living Network Alliance). To configure the DLNA server, click on the button **Media Server Configuration**.



USB Connected Devices

Configuration : This page allows basic control of the USB devices shared over the network.

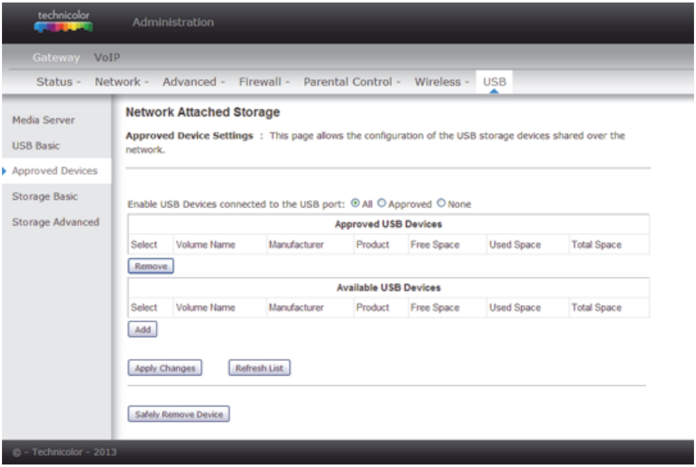
Enable USB Devices connected to the USB port ● All ○ Approved ○ None [Approved Devices]
Enable USB Devices to be Shared Storage ● Yes ○ No [Storage Configuration]
Enable the Media Server (DLNA) ● Yes ○ No [Media Server Configuration]
[Apply]

figure 58: Gateway/USB/USB Basic

4.8.3 Approved Devices settings

This page allows the configuration of the USB storage device(s) shared over the network.

Add **Available USB Devices** as **Approved USB Devices** then apply changes. If you want to remove USB devices, propose you press **Safely Remove Device** button first.



Network Attached Storage

Approved Device Settings : This page allows the configuration of the USB storage devices shared over the network.

Enable USB Devices connected to the USB port: ● All ○ Approved ○ None

Approved USB Devices

Select	Volume Name	Manufacturer	Product	Free Space	Used Space	Total Space

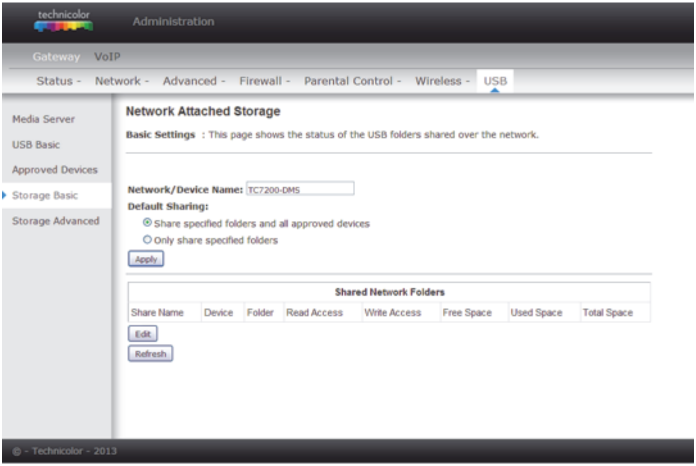
Available USB Devices

Select	Volume Name	Manufacturer	Product	Free Space	Used Space	Total Space

figure 59: Gateway/USB/Approved Devices

4.8.4 Storage Basic

This page shows the status of the USB folders shared over the network. Basic option defines shared files in all approved devices and specified folders or only specified folders. You can edit **Shared Network Folders** and observe the detail of folders.



Network Attached Storage

Basic Settings : This page shows the status of the USB folders shared over the network.

Network/Device Name: TC7200-DMS

Default Sharing:

● Share specified folders and all approved devices

○ Only share specified folders

Apply

Shared Network Folders							
Share Name	Device	Folder	Read Access	Write Access	Free Space	Used Space	Total Space

Edit

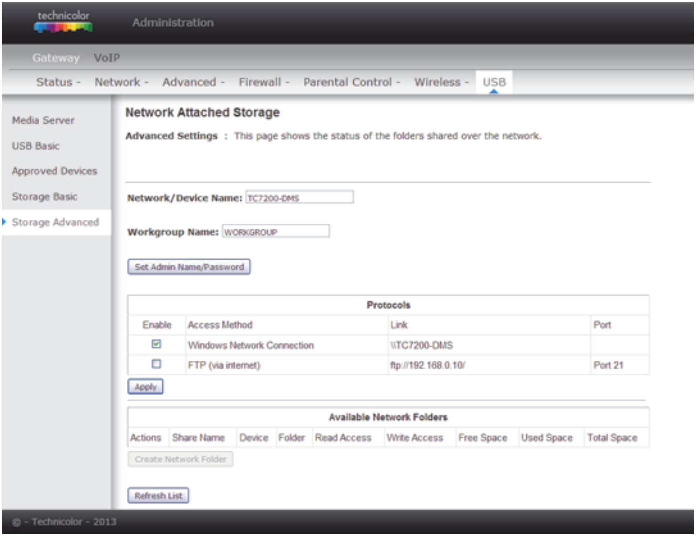
Refresh

© - Technicolor - 2013

figure 60: Gateway/USB/Storage Basic

4.8.5 Storage Advanced

This page shows the status of the folders shared over the network. Advanced option provides FTP option to share files as a FTP server.



Network Attached Storage

Advanced Settings : This page shows the status of the folders shared over the network.

Network/Device Name: TC7200-DMS

Workgroup Name: WORKGROUP

Set Admin Name/Password

Protocols			
Enable	Access Method	Link	Port
☑	Windows Network Connection	\\TC7200-DMS	
□	FTP (via internet)	ftp://192.168.0.10/	Port 21

Apply

Available Network Folders								
Actions	Share Name	Device	Folder	Read Access	Write Access	Free Space	Used Space	Total Space

Create Network Folder

Refresh List

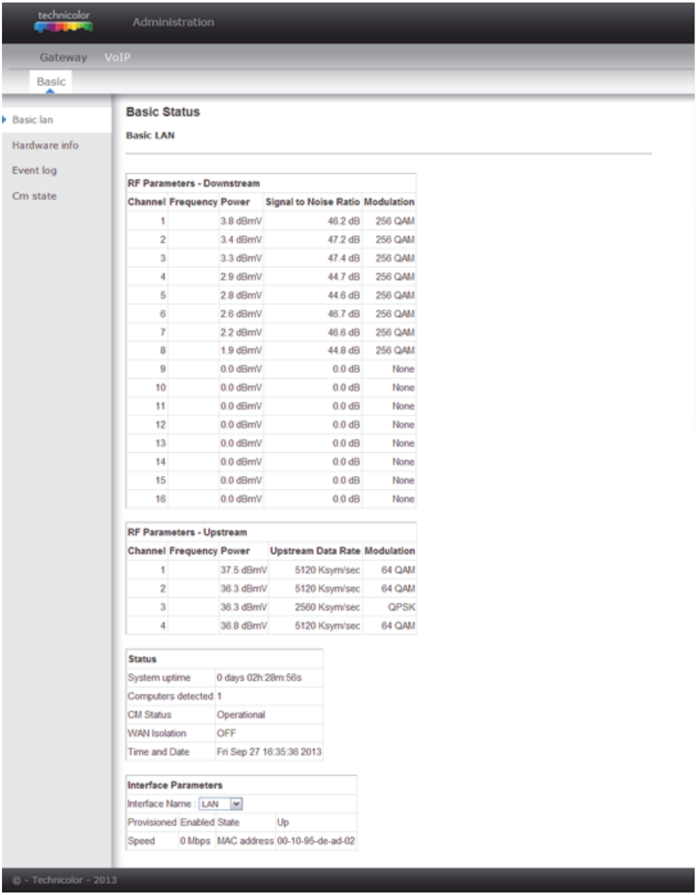
© - Technicolor - 2013

figure 61: Gateway/USB/Storage Advanced

4.9 VoIP – Basic Web Page Group

4.9.1 Basic LAN

This page displays the basic LAN status of this device, including the downstream and upstream status, device information, and interface parameters. You can select specific interface from the **Interface Name** drop-down menu.



Basic Status

Basic LAN

RF Parameters - Downstream				
Channel	Frequency	Power	Signal to Noise Ratio	Modulation
1		3.8 dBmV	46.2 dB	256 QAM
2		3.4 dBmV	47.2 dB	256 QAM
3		3.3 dBmV	47.4 dB	256 QAM
4		2.9 dBmV	44.7 dB	256 QAM
5		2.8 dBmV	44.6 dB	256 QAM
6		2.6 dBmV	46.7 dB	256 QAM
7		2.2 dBmV	46.6 dB	256 QAM
8		1.9 dBmV	44.8 dB	256 QAM
9		0.0 dBmV	0.0 dB	None
10		0.0 dBmV	0.0 dB	None
11		0.0 dBmV	0.0 dB	None
12		0.0 dBmV	0.0 dB	None
13		0.0 dBmV	0.0 dB	None
14		0.0 dBmV	0.0 dB	None
15		0.0 dBmV	0.0 dB	None
16		0.0 dBmV	0.0 dB	None

RF Parameters - Upstream				
Channel	Frequency	Power	Upstream Data Rate	Modulation
1		37.5 dBmV	5120 Ksym/sec	64 QAM
2		36.3 dBmV	5120 Ksym/sec	64 QAM
3		36.3 dBmV	2560 Ksym/sec	QPSK
4		36.8 dBmV	5120 Ksym/sec	64 QAM

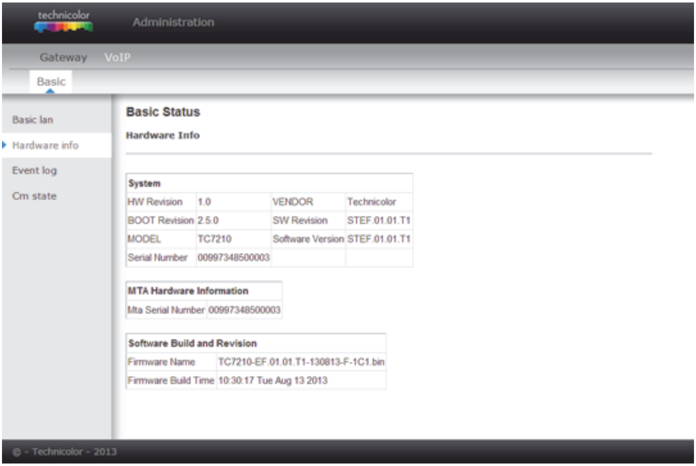
Status	
System uptime	0 days 02h:28m:56s
Computers detected	1
CM Status	Operational
WAN Isolation	OFF
Time and Date	Fri Sep 27 16:35:38 2013

Interface Parameters			
Interface Name : LAN			
Provisioned	Enabled	State	Up
Speed	0 Mbps	MAC address	00-10-95-de-ad-02

figure 62: VoIP\Basic\Basic LAN

4.9.2 Hardware Info

The hardware Info is displayed on this page.



Basic Status

Hardware Info

System			
HW Revision	1.0	VENDOR	Technicolor
BOOT Revision	2.5.0	SW Revision	STEF.01.01.T1
MODEL	TC7210	Software Version	STEF.01.01.T1
Serial Number	00997348500003		

MTA Hardware Information	
Mta Serial Number	00997348500003

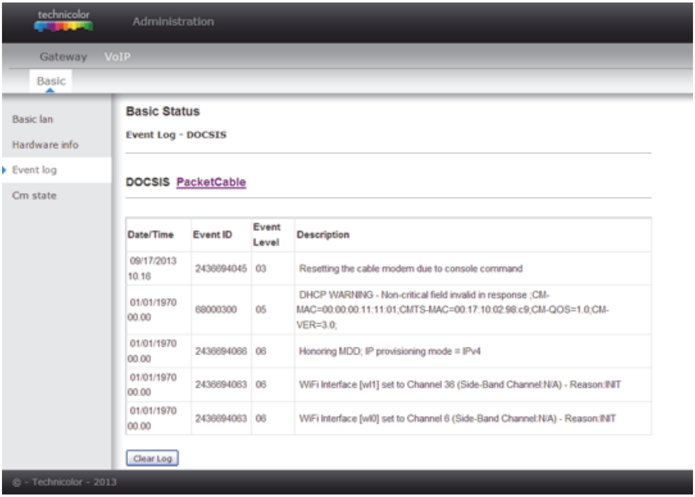
Software Build and Revision	
Firmware Name	TC7210-EF.01.01.T1-130813-F-1C1.bin
Firmware Build Time	10:30:17 Tue Aug 13 2013

© - Technicolor - 2013

figure 63: VoIP\Basic\Hardware Info

4.9.3 Event Log

The Docsis and PacketCable event logs are displayed on this web page.



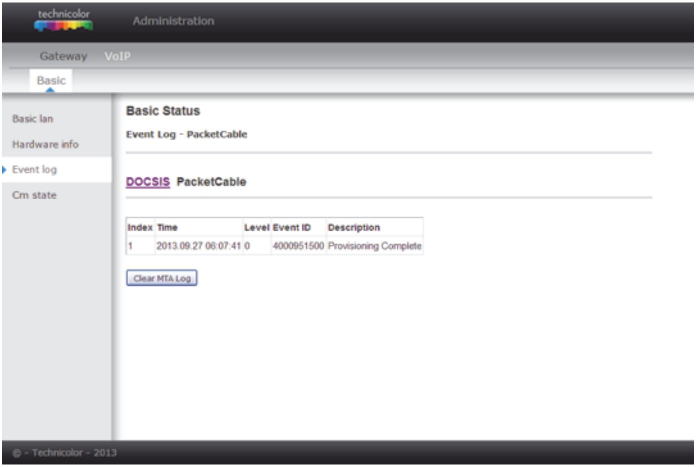
Basic Status

Event Log - DOCSIS

DOCSIS PacketCable

Date/Time	Event ID	Event Level	Description
09/17/2013 10.16	2436694045	03	Resetting the cable modem due to console command
01/01/1970 00.00	68000300	05	DHCP WARNING - Non-critical field invalid in response ;CM-MAC=00:00:00:11:11:01;CMTS-MAC=00:17:10:02:98:c9;CM-QOS=1.0;CM-VER=3.0;
01/01/1970 00.00	2436694066	06	Honoring MDD; IP provisioning mode = IPv4
01/01/1970 00.00	2436694063	06	WiFi Interface [wl1] set to Channel 36 (Side-Band Channel:N/A) - Reason:INIT
01/01/1970 00.00	2436694063	06	WiFi Interface [wl0] set to Channel 6 (Side-Band Channel:N/A) - Reason:INIT

figure 64: VoIP\Basic\Event log\DOCSIS



Basic Status

Event Log - PacketCable

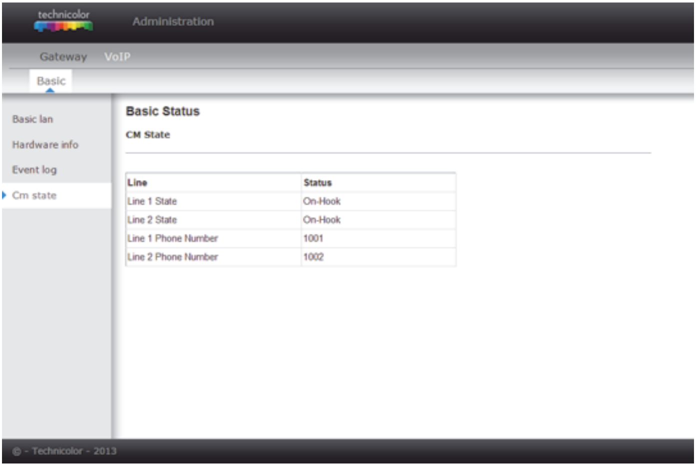
DOCSIS PacketCable

Index	Time	Level	Event ID	Description
1	2013.09.27 06:07:41	0	4000951500	Provisioning Complete

figure 65: VoIP\Basic\Event log\PacketCable

4.9.4 CM State

This page shows the current state of the cable modem.



Basic Status

CM State

Line	Status
Line 1 State	On-Hook
Line 2 State	On-Hook
Line 1 Phone Number	1001
Line 2 Phone Number	1002

figure 66: VoIP\Basic\Cm state

5. Networking

5.1 Communications

Data communication involves the flow of packets of data from one device to another. These devices include personal computers, Ethernet, cable modems, digital routers and switches, and highly integrated devices that combine functions, like the Wireless Cable Gateway.
The gateway integrates the functionality often found in two separate devices into one. It's both a cable modem and an intelligent wireless voice gateway networking device that can provide a host of networking features, such as NAT and firewall. Fig.3-1 illustrates this concept, with the cable modem (CM) functionality on the left, and networking functionality on the right. In this figure, the numbered arrows represent communication based on source and destination, as follows:

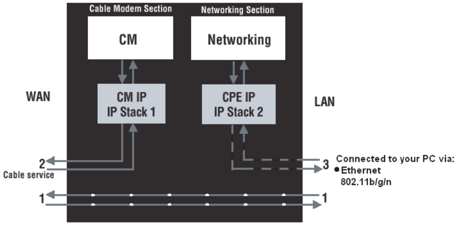


figure 67: Communication between your PCs and the network side

5.2 Type of communication

1. Communication between the Internet and your PCs Example: The packets created by your request for a page stored at a web site, and the contents of that page sent to your PC.
2. Communication between your cable company and the cable modem side.
   Example:
   When your cable modem starts up, it must initialize with the cable company, which requires the cable company to communicate directly with the cable modem itself.

3. Communication between your PCs and the networking side.
   Example:
   The Wireless Cable Gateway offers a number of built-in web pages which you can use to configure its networking side; when you communicate with the networking side, your communication is following this path. Each packet on the Internet addressed to a PC in your home travels from the Internet down- stream on the cable company's system to the WAN side of your Wireless Cable Gateway. There it enters the Cable Modem section, which inspects the packet, and based on the results, proceeds to either forward or block the packet from proceeding on to the Networking section. Similarly, the Networking section then decides whether to forward or block the packet from proceeding on to your PC. Communication from your home device to an Internet device works similarly, but in reverse, with the packet traveling upstream on the cable system.

5.3 Cable Modem (CM) Section

The cable modem (or CM) section of your gateway uses DOCSIS or EURO-DOCSIS Standard cable modem technology. DOCSIS or EURO-DOCSIS specifies that TCP/IP over Ethernet style data communication be used between the WAN interface of your cable modem and your cable company.
A DOCSIS or EURO-DOCSIS modem, when connected to a Cable System equipped to support such modems, performs a fully automated initialization process that requires no user intervention. Part of this initialization configures the cable modem with a CM IP (Cable Modem Internet Protocol) address, as shown in Figure 3-2, so the cable company can communicate directly with the CM itself.

5.4 Networking Section

The Networking section of your gateway also uses TCP/IP (Transmission Control Protocol/ Internet Protocol) for the PCs you connected on the LAN side. TCP/IP is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TCP/IP requires that each communicating device be configured with one or more TCP/IP stacks, as illustrated by Fig.3-2. On a PC, you often use software that came with the PC or its network interface (if you purchased a network interface card separately) to perform this configuration. To communicate with

the Internet, the stack must also be assigned an IP (Internet Protocol) address. 192.168.100.1 is an example of an IP address. A TCP/IP stack can be configured to get this IP address by various means, including a DHCP server, by you directly entering it, or sometimes by a PC generating one of its own.
Ethernet requires that each TCP/IP stack on the Wireless Cable Gateway also have associated with it an Ethernet MAC (Media Access Control) address. MAC addresses are permanently fixed into network devices at the time of their manufacture. 00:90:64:12:B1:91 is an example of a MAC address.
Data packets enter and exit a device through one of its network interfaces. The gateway offers Ethernet and 802.11b/g/n wireless network interfaces on the LAN side and the DOCSIS network interface on the WAN side.
When a packet enters a network interface, it is offered to all the TCP/IP stacks associated with the device side from which it entered. But only one stack can accept it — a stack whose configured Ethernet address matches the Ethernet destination address inside the packet. Furthermore, at a packet’s final destination, its destination IP address must also match the IP address of the stack.

Each packet that enters a device contains source MAC and IP addresses telling where it came from, and destination MAC and IP addresses telling where it is going to. In addition, the packet contains all or part of a message destined for some application that is running on the destination device. IRC used in an Internet instant messaging program, HTTP used by a web browser, and FTP used by a file transfer program are all examples of applications. Inside the packet, these applications are designated by their port number. Port 80, the standard HTTP port, is an example of a port number.
The Networking section of the router performs many elegant functions by recognizing different packet types based upon their contents, such as source and destination MAC address, IP address, and ports.

5.5 Three Networking Modes

Your gateway can be configured to provide connectivity between your cable company and your home LAN in any one of three Networking Modes: CM, RG, and CH. This mode setting is under the control of your cable company, who can select the mode to match the level of home networking support for which you have subscribed. All units ship from the factory set for the RG mode, but a configuration file which the cable company sends the cable modem section during its initialization can change it.

5.6 Cable Modem (CM) Mode

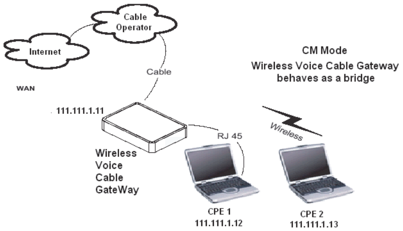


figure 68: Cable Modem Mode

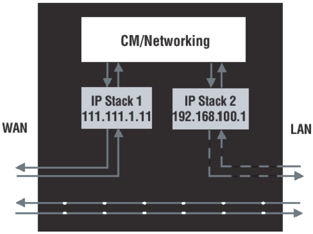


figure 69: Two IP stacks are activated in cable modem mode

CM (Cable Modem) Mode provides basic home networking. In this mode, two IP stacks are active:

- IP Stack 1 - for use by the cable company to communicate with the cable modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable gateway.
- IP Stack 2 - for use by you, the end user, to communicate with the cable modem and Networking sections, to access the internal web page diagnostics and configuration. This stack uses a fixed IP address: 192.168.100.1. It uses a MAC address 00:10:95:FF:FF:FE.

With CM Mode, your cable company must provide one IP address for the CM section, plus one for each PC you connect from their pool of available addresses. Your cable company may have you or your installer manually enter these assigned addresses into your PC, or use a DHCP Server to communicate

them to your PCs, or use a method that involves you entering host names into your PCs.
Note that in CM Mode, packets passing to the Internet to/from your PCs do not travel through any of the IP stacks; instead they are directly bridged between the WAN and LAN sides.

5.7 Residential Gateway (RG) Mode

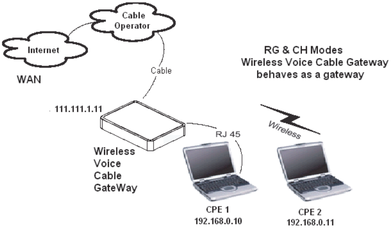


figure 70: Residential Gateway Mode

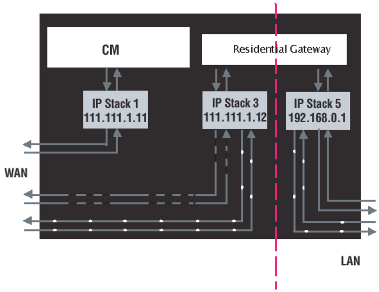


figure 71: Three IP stacks are activated in cable modem mode

RG (Residential Gateway) Mode provides basic home networking plus NAT (Network Address Translation). In this mode, three IP stacks are active:

1. IP Stack 1 - for use by the cable company to communicate with the Cable Modem section only. This stack receives its IP address from the cable company during CM initialization. It uses the MAC address printed on the label attached to the Wireless Cable Gateway.
2. IP Stack 3 - for use by you to remotely (i.e. from somewhere on the WAN side, such as at your remote workplace) communicate with the Cable Modem and Networking sections, to remotely access the internal web page

diagnostics and configuration. This stack is also used by your cable company to deliver packets between the Internet and the gateway's networking section so they can be routed to/from your PCs. This stack requires an IP address assigned by the cable company from their pool of available addresses. Your cable company may have you or your installer manually enter assigned addresses into your gateway, or use a DHCP Server to communicate them, or use a method that involves you entering host names. This stack uses a MAC address of MAC label + 2 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:93.

3. IP Stack 5 - for use by you to locally (i.e. from somewhere on the LAN side in your home) communicate with the Cable Modem and Networking sections, to access the internal web page diagnostics and configuration. This stack is also used by the gateway's networking section to route packets between the gateway's Networking section and your PCs. This stack uses a fixed IP address: 192.168.0.1. It uses a MAC address of MAC label + 4 (the MAC label is found on the bottom of the unit). E.g., if the MAC address is 00:90:64:12:B1:91, this MAC address would be 00:90:64:12:B1:95.

With RG Mode, your cable company must provide one IP address for the CM section, plus one for the Networking section, from their pool of available addresses. With RG Mode, each PC you connect gets an IP address from a DHCP Server that is part of the Networking section of the gateway.

6. Frequently asked questions

It seems that the wireless network is not working

Check the Wireless LED on the front panel. If it is no lighted, press on the WPS button shortly, less than 1 second, on the side of the modem, and then check again the Wireless LED. If it is lighted, then the Wireless transmission is enabled.

Can I watch TV, surf the Internet, and talk to my friends through the Wireless Voice Gateway at the same time?

Absolutely!

What do you mean by “Broadband?”

Simply put, it means you’ll be getting information through a “bigger pipe,” with more bandwidth, than a standard phone line can offer. A wider, “broader” band means more information, more quickly.

What is Euro-DOCSIS and what does it mean?

“Data over Cable Service Interface Specifications” is the industry standard that most cable companies are adopting as they upgrade their systems. Should you ever decide to move, the Wireless Voice Gateway will work with all upgraded cable systems that are Euro-DOCSIS-compliant.

What is Euro-PacketCable and what does it mean?

Euro-PacketCable is the industry standard for telephony services that most cable companies are adopting as they upgrade their systems. Should you ever decide to move, the Wireless Voice Gateway will work with all upgraded cable systems that are Euro-PacketCable compliant.

What is Xpress Technology and what does it mean?

It is one of the popular performance-enhancing Wi-Fi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks. When Xpress is turned on, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by up to 27% in

802.11g-only networks, and up to 75% in mixed networks comprised of 802.11g and 802.11b standard equipment. The technology achieves higher throughput by re-packaging data, reducing the number of overhead control packets, so that more useful data can be sent during a given amount of time.

7. Troubleshooting

You can correct most problems you have with your product by consulting the troubleshooting list that follows.

I can’t access the internet.

- Check all of the connections to your Wireless Voice Gateway.
- Your Ethernet card may not be working. Check each product’s documentation for more information.
- The Network Properties of your operating system may not be installed correctly or the settings may be incorrect. Check with your ISP or cable company.

I can’t get the modem to establish an Ethernet connection.

- Even new computers don’t always have Ethernet capabilities – be sure to verify that your computer has a properly installed Ethernet card and the driver software to support it.
- Check to see that you are using the right type of Ethernet cable.

The modem won’t register a cable connection.

- If the modem is in Initialization Mode, the INTERNET light will be flashing. Call your Cable Company if it has not completed this 5-step process within 30 minutes, and note which step it is getting stuck on.
- The modem should work with a standard RG-6 coaxial cable, but if you’re using a cable other than the one your Cable Company recommends, or if the terminal connections are loose, it may not work. Check with your Cable Company to determine whether you’re using the correct cable.
- If you subscribe to video service over cable, the cable signal may not be reaching the modem. Confirm that good quality cable television pictures are available to the coaxial connector you are using by connecting a television to it. If your cable outlet is “dead”, call your Cable Company.
- Verify that the Cable Modem service is Euro-DOCSIS compliant and PacketCable compliant by calling your cable provider.

I don’t hear a dial tone when I use a telephone.

- Telephone service is not activated. If the rightmost light on the Wireless Voice Gateway stays on while others flash, check with your TSP or cable company. If the Wireless Voice Gateway is connected to existing house telephone wiring, make sure that another telephone service is not connected. The other service can normally be disconnected at the Network Interface Device located on the outside of the house.
- If using the second line on a two-line telephone, use a 2-line to 1-line adapter cable.

8. Glossary

10/100/1000 BaseT

Unshielded, twisted pair cable with an RJ-45 connector, used with Ethernet LAN (Local Area Network). “10/100/1000” indicates speed (10/100/1000 BaseT), “Base” refers to baseband technology, and “T” means twisted pair cable.

Authentication

The process of verifying the identity of an entity on a network.

DHCP (Dynamic Host Control Protocol)

A protocol which allows a server to dynamically assign IP addresses to workstations on the fly.

Ethernet adapters

A plug-in circuit board installed in an expansion slot of a personal computer. The Ethernet card (sometimes called a Network Interface Card , network adapter or NIC) takes parallel data from the computer, converts it to serial data, puts it into a packet format, and sends it over the 10/100/1000 BaseT LAN cable.

DOCSIS (Data Over Cable Service Interface Specifications)

A project with the objective of developing a set of necessary specifications and operations support interface specifications for Cable Modems and associated equipment.

F Connector

A type of coaxial connector, labeled CABLE IN on the rear of the Wireless Voice Gateway that connects the modem to the cable system.

HTTP (HyperText Transfer Protocol)

Invisible to the user, HTTP is used by servers and clients to communicate and display information on a client browser.

Hub

A device used to connect multiple computers to the Wireless Voice Gateway.

IP Address

A unique, 32-bit address assigned to every device in a network. An IP (Internet Protocol) address has two parts: a network address and a host address. This modem receives a new IP address from your cable operator via DHCP each time it goes through Initialization Mode.

Key exchange

The swapping of mathematical values between entities on a network in order to allow encrypted communication between them.

MAC Address

The permanent “identity” for a device programmed into the Media Access Control layer in the network architecture during the modem’s manufacture.

NID

Network Interface Device, the interconnection between the internal house telephone wiring and a conventional telephone service provider’s equipment. These wiring connections are normally housed in a small plastic box located on an outer wall of the house. It is the legal demarcation between the subscriber’s property and the service provider’s property.

PacketCable

A project with the objective of developing a set of necessary telephony specifications and operations support interface specifications for Wireless Voice Gateways and associated equipment used over the DOCSIS based cable network.

PSTN (Public Switched Telephone Network)

The worldwide voice telephone network which provides dial tone, ringing, full-duplex voice band audio and optional services using standard telephones.

Provisioning

The process of enabling the Media Terminal Adapter (MTA) to register and provide services over the network.

TCP/IP (Transmission Control Protocol/Internet Protocol)

A networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems.

TFTP

Trivial File Transfer Protocol, the system by which the Media Terminal Adapter's configuration data file is downloaded.

TSP

Telephony Service Provider, an organization that provides telephone services such as dial tone, local service, long distance, billing and records, and maintenance.

Universal Serial Bus (USB)

USB is a "plug-and-play" interface between a computer and add-on devices, such as a Wireless Voice Gateway.

Xpress Technology

One of the popular performance-enhancing WiFi technologies, designed to improve wireless network efficiency and boost throughput. It is more efficient in mixed environments, and it can work with 802.11a/b/g networks.

Ondanks alle aan deze handleiding bestede zorg kan Ziggo geen aansprakelijkheid aanvaarden voor schade die het gevolg is van enige onvolkomenheid of fout in deze uitgave. De handleiding is uitdrukkelijk niet bedoeld ter nadere invulling of toelichting op de algemene voorwaarden. Derhalve kunnen er geen rechten aan ontleend worden.