VisionNet™

M504

ADSL2+ Ethernet Broadband Gateway

4 Port Ethernet USB 2.0

End User Manual

Table of Contents

1. Introduction

Congratulations on becoming the owner of the VisionNet M504 ADSL2+ Broadband Gateway. You will now be able to access the Internet using your high-speed ADSL/2+ connection. The Master series of ADSL2+ modems has the following major features.

Features

- ADSL/2/2+ modem for high speed Internet access
- USB Storage for Media share across your Local Network
- Network Address Translation (NAT) and IP filtering functions to provide network sharing and firewall protection for your computers
- Easy configuration via a WEB browser
- SPI firewall to protect you from outside intruders and attacks
- TR-069 compliant for automatic modem update through your high speed Internet access

This End User Manual will guide you through the installation and configuration of your M504 modem.

System Requirements

Before installing your M504 modem, make sure that you have the following:

- ADSL service up and running on your telephone line, with at least one public Internet address for your LAN
- Computer containing an Ethernet 10Base-T/100Base-T network interface card (NIC)

For system configuration, use the web-based (HTTP) user interface.

Note: Make sure that your computer has a web browser such as Internet Explorer v7.0 or later, or Firefox v3.0 or later.

2. Installation

In addition to this document, your M504 should arrive with the following:

- One power adapter
- One Ethernet cable with RJ-45 connector
- One Telephone cable with RJ-11 connector
- Product Installation CD
- Installation Guide

Front Panel

The Front panel LED light indicates the status of the unit. *(Left to Right)*

M504

Label	Color	Function
Power	Green	On – Solid Green Off – The Modem is Off Red – Power on self test/ Device Malfunction (not bootable) and device malfunction Malfunction is any state which would prevent syncing or passing of data
DSL	Green	Green – DSL Good Sync Off - Powered off Flashing Green - DSL Attempting sync
Internet	Green	Solid Green – IP connected – no traffic passing Device has a public IP via either static/ DHCP/ or IPCP If PPP is used it has been authenticated If IP or PPPOE session is idle and dropped, light to remain green as long as ADSL is still present. Light to turn red if upon attempting new session it fails. Off – Modem Power Off. LED Should remain off if modem is in bridged mode
Ethernet 1-4	Green	Off - Power Off – or – No Device Detected on any LAN port Solid Green – Device connected including wake on LAN on any LAN port Flashing Green – LAN activity present
DLNA	Green	Green – USB storage connected Off - No device detected

Rear Panel

The connectors located at the rear panel have the following functions.

M504

Interface	Function
Switch(Push Button)	Power switch on/off
Power	Connects to the power adapter cable
Reset Button	Resets unit's configuration to factory default
DLNA	USB 2.0/1.1 connection: Connects external storage device to gateway
Ethernet 1-4	RJ-45 connector: Connects to your PC's Ethernet port, or to the uplink port on your LAN's hub/switch
ADSL	RJ-11 connector: Connects to your ADSL line

Connecting the Hardware

Connect the M504 to the phone jack, the power outlet, and your computer or network.

⚠ **WARNING**

Before you begin, turn the power off for all devices. *These include your computer(s), your LAN hub/switch (if applicable), and the M504.*

Step 1. Connect the ADSL cable and optional telephone

Connect one end of the phone cable to the RJ-11 connector on the rear panel of the M504. Connect the other end to the ADSL outlet provided by your service provider (normally MODEM port of the included splitter).

Step 2. Connect the Ethernet cable

Connect one end of the Ethernet cable to the RJ-45 connectors on the rear panel of the M504 and connect the other end to your PCs network adaptor (NIC). If you are connecting a LAN to the Master series, attach one end of the Ethernet cable to a regular hub port and the other end to the LAN port on the M504.

Step 3. Attach the power connector

Connect the AC power adapter to the power connector on the M504 and plug in the adapter to a wall outlet or power extension.

Step 4. Turn on the M504 and power up your systems

Press the Power switch on the back panel of the M504 to the ON position.
Boot up your computer(s) and any LAN devices such as hubs or switches.

Step 5. Configure the M504 through the WEB interface

Please refer to Chapter 3.

Step 6. Save the configurations and Reboot

Save the changes you made on the M504 and it will automatically reboot to make the settings permanent.

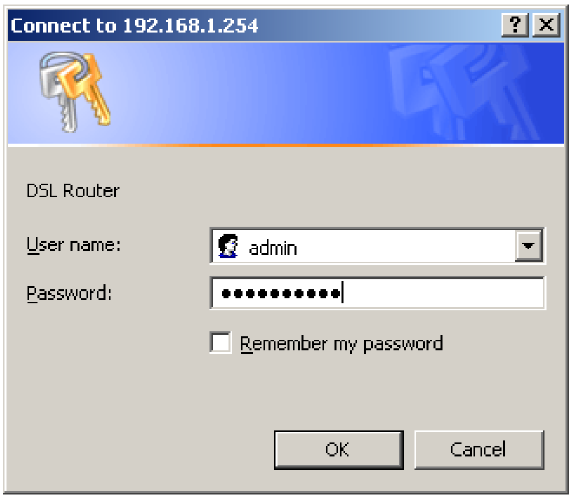
3. Configuration

3.1 - Setup

- Connect your M504 and PC with an RJ-45 Ethernet cable.
- Turn on the M504.
- The default IP address of M504 is 192.168.1.254.

3.2 - Establish the Connection

- Enter the IP address (default: 192.168.1.254) of M504 in the address line of your web browser.
- A Dialogue Box will pop up to request the user to login. (Figure 1)



DSL Router

User name: admin

Password: ●●●●●●●●●●

□ Remember my password

Figure 1. Login dialogue box

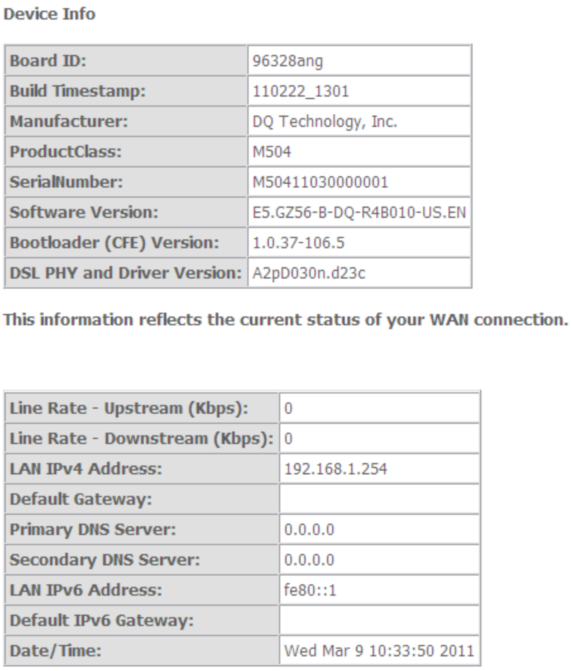
- Please enter the management username/password into the fields then click on the **OK** button (Please contact your ISP for login information).

4. Quick View

Quick View allows you to view all the major statistics and information of your VisionNet M504 Gateway from one easy location on the WEB interface.

The following information is provided:

1. Device Info – Information such as Software revision and Driver version
2. DSL Status – Sync Rate (DSL Connection speed for Downstream and Upstream)
3. WAN Overview – WAN service information
4. ARP – Client connected to the VisionNet M504 Gateway

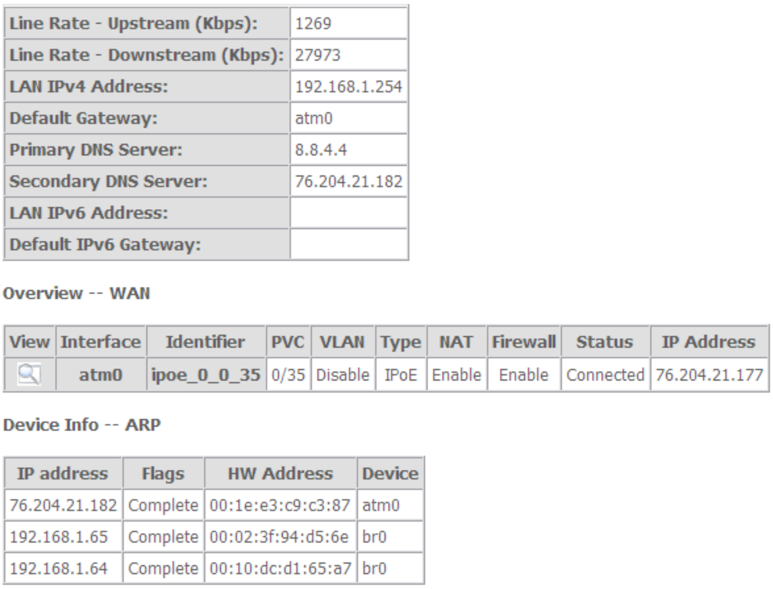


Device Info

Board ID:	96328ang
Build Timestamp:	110222_1301
Manufacturer:	DQ Technology, Inc.
ProductClass:	M504
SerialNumber:	M50411030000001
Software Version:	E5.GZ56-B-DQ-R4B010-US.EN
Bootloader (CFE) Version:	1.0.37-106.5
DSL PHY and Driver Version:	A2pD030n.d23c

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.1.254
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	fe80::1
Default IPv6 Gateway:	
Date/Time:	Wed Mar 9 10:33:50 2011



Line Rate - Upstream (Kbps):	1269
Line Rate - Downstream (Kbps):	27973
LAN IPv4 Address:	192.168.1.254
Default Gateway:	atm0
Primary DNS Server:	8.8.4.4
Secondary DNS Server:	76.204.21.182
LAN IPv6 Address:	
Default IPv6 Gateway:	

Overview -- WAN

View	Interface	Identifier	PVC	VLAN	Type	NAT	Firewall	Status	IP Address
🔍	atm0	ipoe_0_0_35	0/35	Disable	IPoE	Enable	Enable	Connected	76.204.21.177

Device Info -- ARP

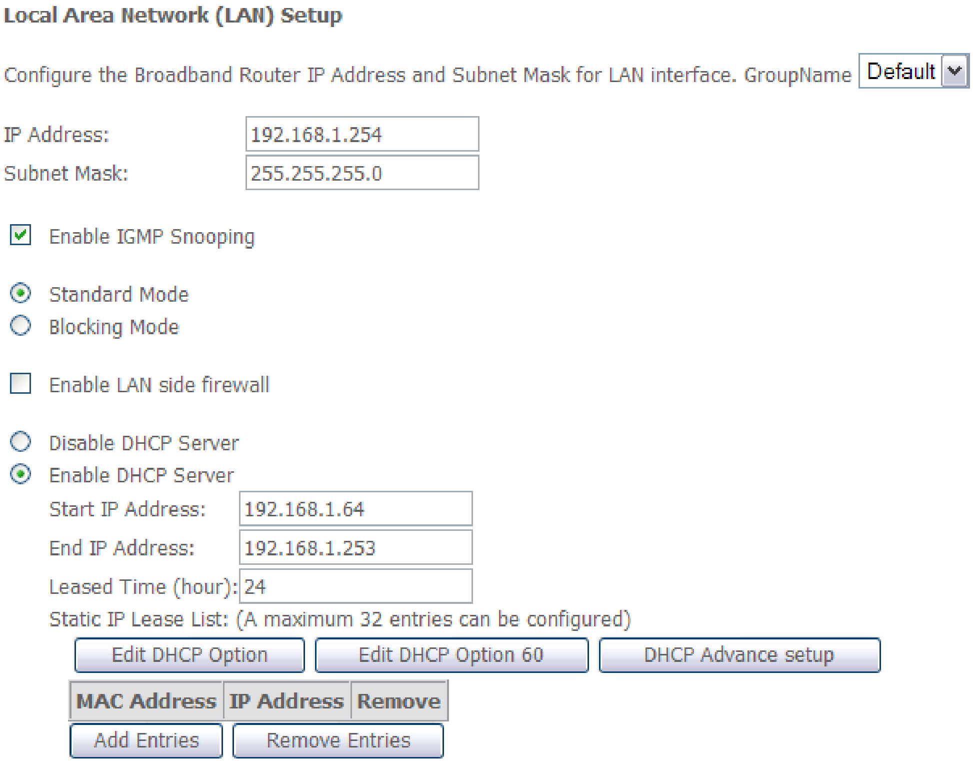
IP address	Flags	HW Address	Device
76.204.21.182	Complete	00:1e:e3:c9:c3:87	atm0
192.168.1.65	Complete	00:02:3f:94:d5:6e	br0
192.168.1.64	Complete	00:10:dc:d1:65:a7	br0

5. LAN

The LAN (Local Area Network) section allows the following settings to be configured on the VisionNet M504 Gateway:

- LAN Setup
- IPv6 LAN Settings

5.1 - LAN



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

□ Enable LAN side firewall

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.64

End IP Address: 192.168.1.253

Leased Time (hour): 24

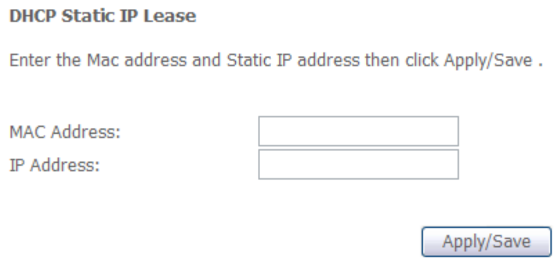
Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

Input the IP Address and Subnet Mask of your M504. *(Default: 192.168.1..254)*

Check the box if you want to enable IGMP Snooping.
Disable/Enable DHCP Server, and change the starting and ending IP address of your server pool if needed.

5.1.2 – Static IP Leasing



DHCP Static IP Lease

Enter the Mac address and Static IP address then click Apply/Save .

MAC Address:

IP Address:

This function allows you to reserve an IP Address for clients connected to the gateway via the client’s MAC address.

Click the “Add new entries” Form, enter the MAC address of the client you wish to reserve an IP address to.

Enter the IP Address that you wish to assign to the client

Click on the “Apply/Save” button to add the new entry.

Warm Reboot the Gateway for the function to take affect. Please see Management Section for instruction on how to Warm Reboot the modem.

6. Security

The Security section allows the following setting to be configured on the VisionNet M504 Gateway:

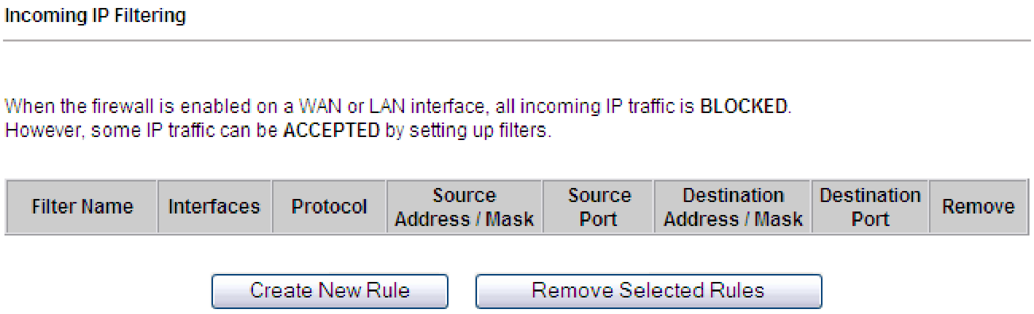
- IP Filtering Rules
- URL Filtering
- Port Forwarding
- Port Triggering
- DMZ Host
- WAN Access Control

6.1 – IP Filtering Rules

Two functions are supported in the IP Filter function of the M504 Gateway: Outgoing IP Filtering and Incoming Filtering.

Incoming IP Filtering

When the firewall option is enabled on a WAN or LAN interface, all incoming IP traffic from the WAN is BLOCKED. However, incoming IP filter rules can be allowed by setting up filtering rules. Choose "Add" to configure incoming IP filters. To remove, check the item and click "Remove".

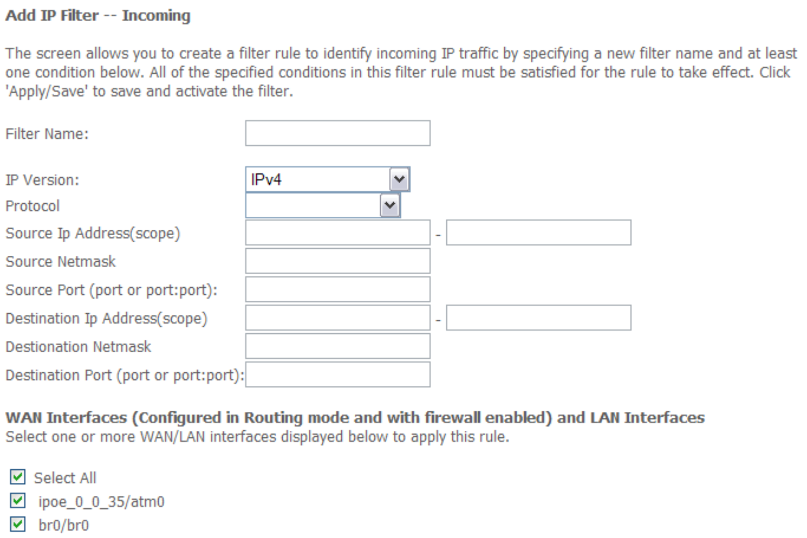


Incoming IP Filtering

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED.
However, some IP traffic can be ACCEPTED by setting up filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Destination Address / Mask	Destination Port	Remove

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a filter name and at least one of the conditions below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Save/Apply" to save and activate the filter.



Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

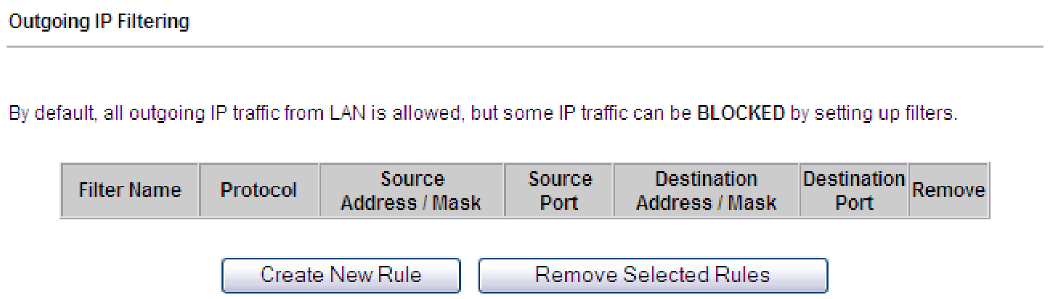
Filter Name:	
IP Version:	IPv4
Protocol	
Source Ip Address(scope)	-
Source Netmask	
Source Port (port or port:port):	
Destination Ip Address(scope)	-
Destionation Netmask	
Destination Port (port or port:port):	

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
Select one or more WAN/LAN interfaces displayed below to apply this rule.

☑ Select All
☑ ipoe_0_0_35/atm0
☑ br0/br0

Outgoing IP Filtering

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. Choose "Add" to configure outgoing IP filters. To remove, check the item and click "Remove".

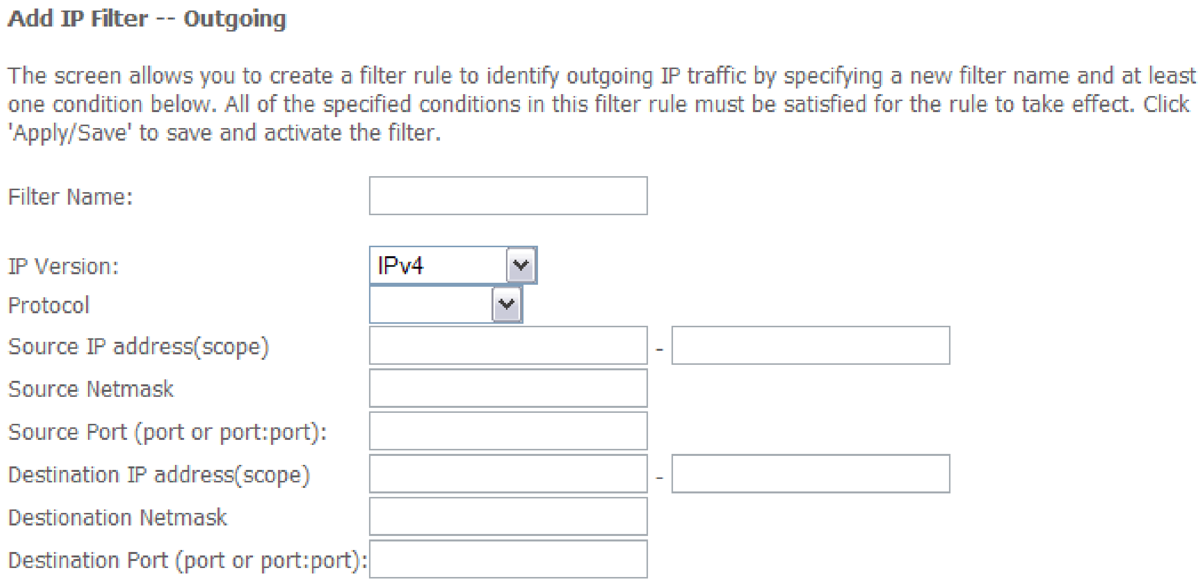


Outgoing IP Filtering

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Destination Address / Mask	Destination Port	Remove

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a filter name and at least one of the conditions below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Save/Apply" to save and activate the filter.



Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version: IPv4

Protocol

Source IP address(scope) -

Source Netmask

Source Port (port or port:port):

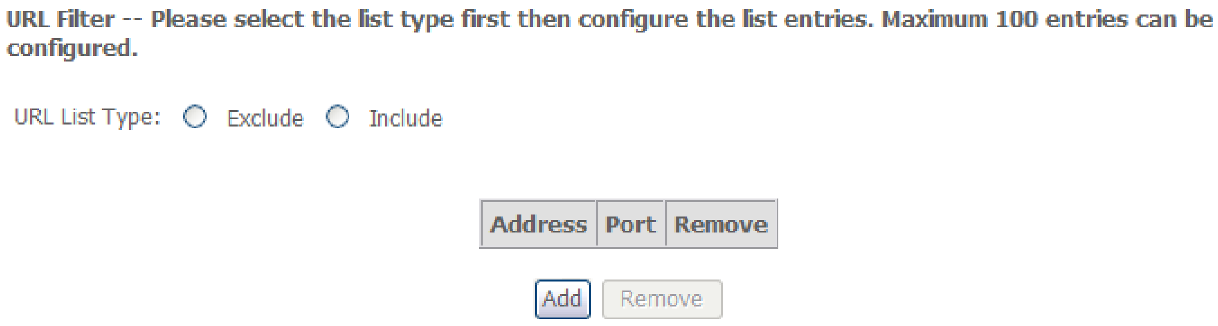
Destination IP address(scope) -

Destionation Netmask

Destination Port (port or port:port):

6.2 – URL Filtering Rules

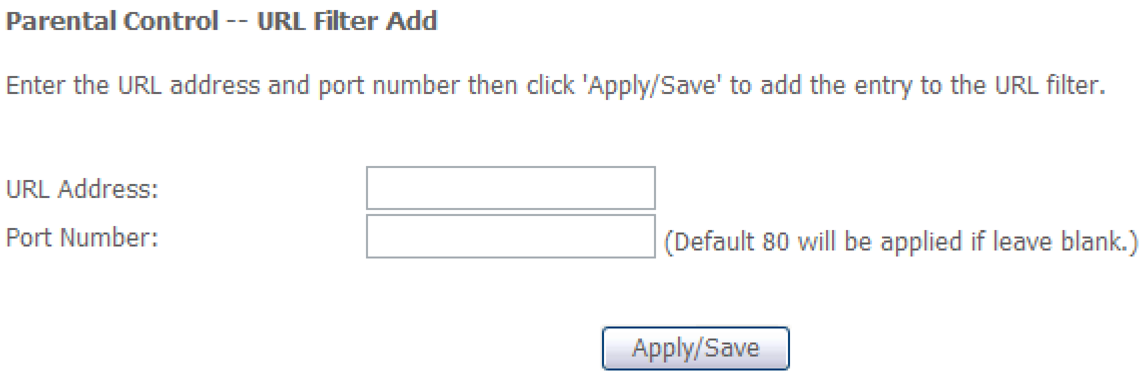
The M504 Gateway allow user to block or allow access to specific URL for clients connected. Setup the URL filters by: Choose “Create New Rule” to add URL (Web Address)



URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove



Parental Control -- URL Filter Add

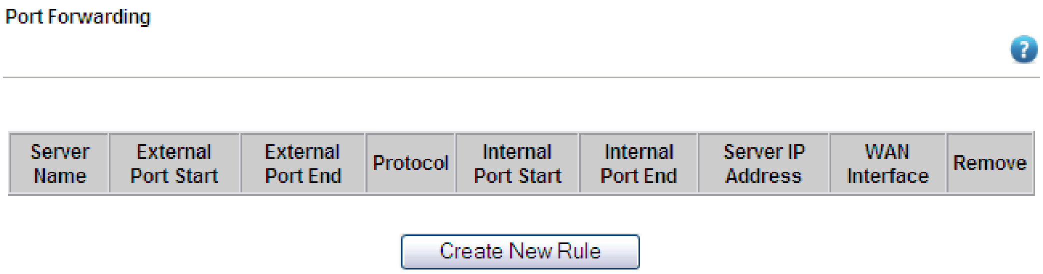
Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

6.3 – Port Forwarding

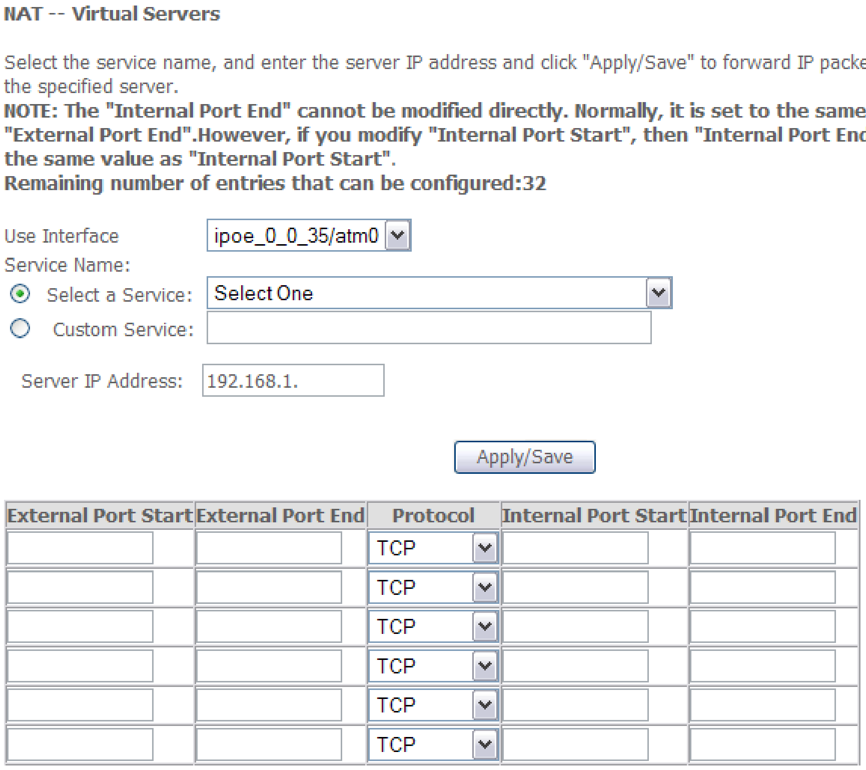
Port Forwarding allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.



Port Forwarding

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove

Click on “**Create New Rule**” to enter configuration page to add your own rule(s). Some common used servers (Web, FTP, Mail, etc.) are already pre-defined for the M504. User can simply select the desired pre-defined application from the pull-down menu and assign the IP address of the local PC for the ports to be forwarded to.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.

NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured:32

Use Interface: ipoe_0_0_35/atm0

Service Name:

● Select a Service: Select One

○ Custom Service:

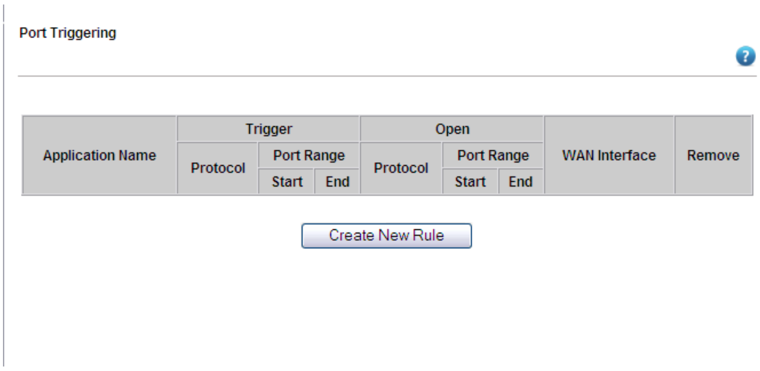
Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

To delete the configured rule(s), check the “Remove” box of the specific rule(s) and click on “Remove”.

6.4 – Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the “Open Ports” in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the “Triggering Ports”. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the “Open Ports”. A maximum of 32 entries can be configured.

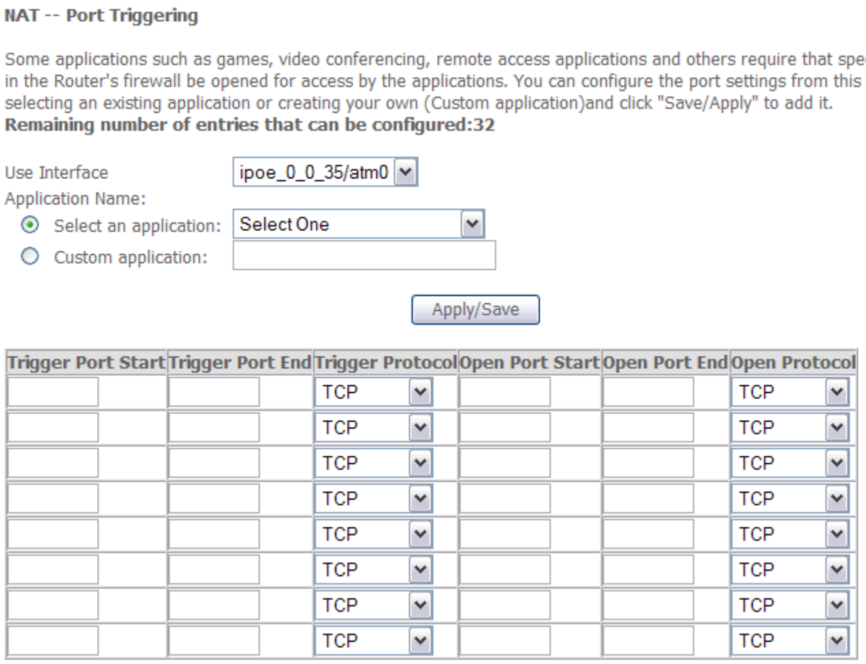


Port Triggering

Application Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

Click on “Create New Rule” to enter the configuration page to add your own rule(s). You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click “Save/Apply” to add it.

To delete the configured rule(s), check the “Remove” box of the specific rule(s) and click on “Remove”.



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.
Remaining number of entries that can be configured:32

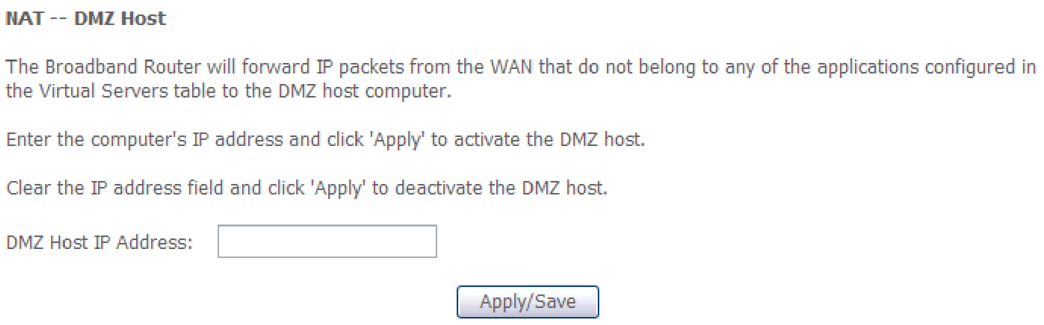
Use Interface: ipoe_0_0_35/atm0
Application Name:
● Select an application: Select One
○ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

6.5 – DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.
Enter the computer's IP address and click “Apply Specified DMZ Host” to activate the DMZ host.

Click on the “Clear/Deactivate DMZ Host” button to disable the DMZ Host function.



NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

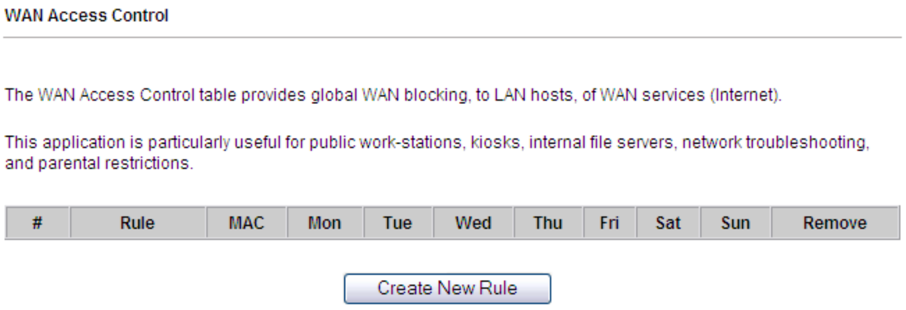
Enter the computer's IP address and click 'Apply' to activate the DMZ host.

Clear the IP address field and click 'Apply' to deactivate the DMZ host.

DMZ Host IP Address:

6.6 – WAN Access Control

WAN Access Control allows users to create time of day restrictions to a specific LAN device connected to the Router. Click "Create New Rule" to configure restriction rules. To remove, check the item and click "Remove".

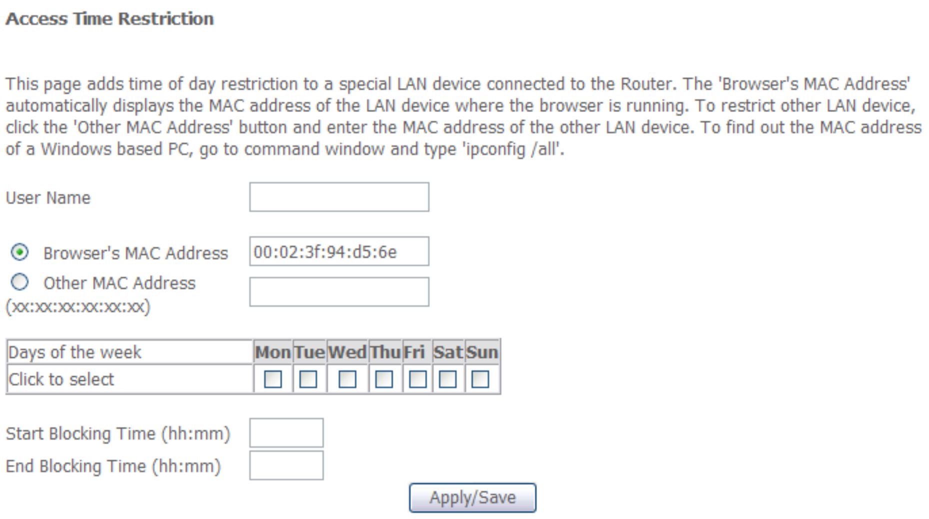


WAN Access Control

The WAN Access Control table provides global WAN blocking, to LAN hosts, of WAN services (Internet).

This application is particularly useful for public work-stations, kiosks, internal file servers, network troubleshooting, and parental restrictions.

#	Rule	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Remove



Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.

User Name

● Browser's MAC Address 00:02:3f:94:d5:6e

○ Other MAC Address (xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

To create a new WAN Access Control Rule:

1. Give the rule a name that can be easily be identified
2. The “Browser’s MAC Address” will show the MAC address of the client currently connected to the gateway WEB Interface. Either select this option if you want the rules to apply to the PC in use or check the Other MAC address radio box and enter the MAC address of the client you wish for the rules to apply to
3. Check the “Block” box and enter the Time of Day (24hour format) of when you would like the Rules to begin and end.
4. Click on the “Save/Apply” button to apply the new WAN Access Control Rule

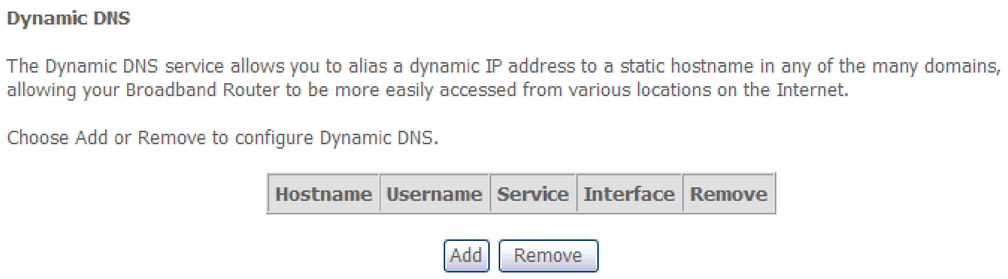
7. DNS

7.1 – Dynamic DNS

The Dynamic DNS service allows you to give a dynamic IP address a static hostname in any of the domains. This function allows your M504 to be more easily accessible from various locations on the Internet.
Choose “Create New Client Service” to configure Dynamic DNS.

Before you proceed, please visit one of these two websites to receive your own Dynamic DNS service: www.dyndns.org or www.tzo.com.

To remove, check the item and click “Remove”



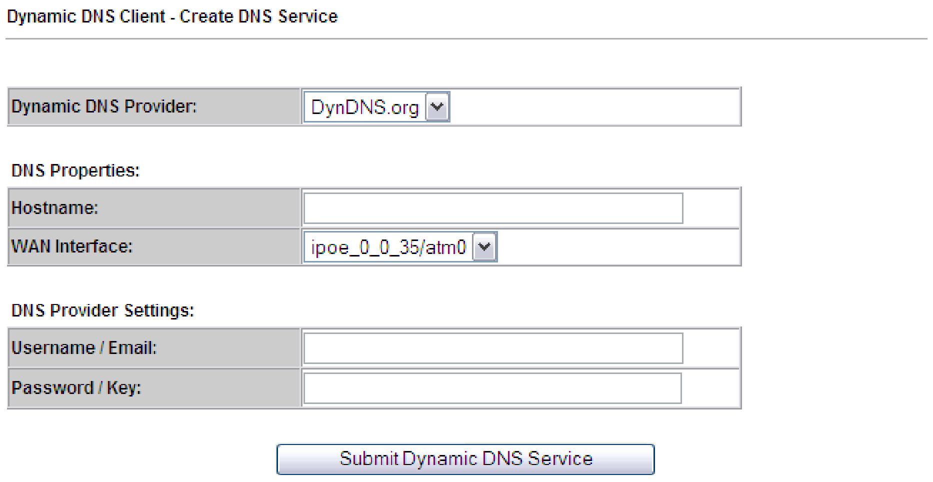
Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Select your Dynamic DNS service provider from ‘D-DNS provider’, and enter your registration information. Click “Submit Dynamic DNS Service” to save the configuration.



Dynamic DNS Client - Create DNS Service

Dynamic DNS Provider:	DynDNS.org

DNS Properties:

Hostname:	
WAN Interface:	ipoe_0_0_35/atm0

DNS Provider Settings:

Username / Email:	
Password / Key:	

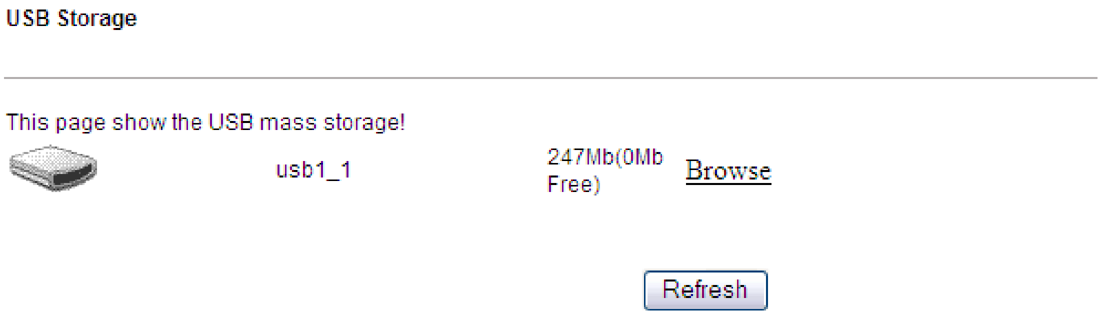
8. Network Access Storage (DLNA)

The M504 have the ability to share content of an USB storage device to Windows based PC's connected on the LAN.

To utilize this function: connect a USB storage device (External Hard drive, USB Thumb Drive, etc.) to the USB port of the M504 gateway.

The M504 will recognize the device after a few seconds and the USB storage information will appear in the WEB interface.

To browse the content of the storage device, select the "Browse" link located on the page. An Explorer window will open and list the directories/files currently in the storage device.



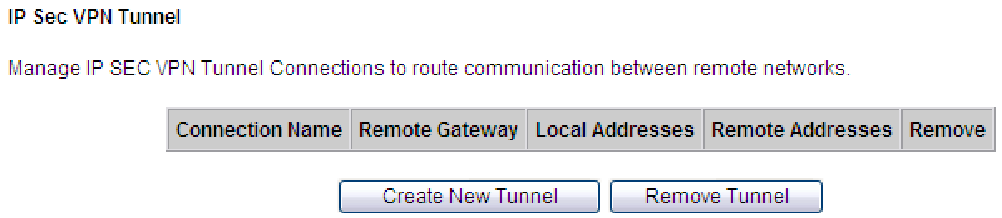
USB Storage

This page show the USB mass storage!

usb1_1 247Mb(0Mb Free)

9. IPSEC

The M504 also have the ability to create a VPN (Virtual Private Network) tunnel using IPSec as the security measure. VPN allows user to remotely connect to a network using their Broadband connection. Click on the “Create New Tunnel” to create new IPSEC connection



IP Sec VPN Tunnel

Manage IP SEC VPN Tunnel Connections to route communication between remote networks.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove

Enter the following critical information in the VPN Tunnel Settings:

1. Enter a name for this IPSec connection.

2. Enter the Public IP address of the remote gateway in the next field.

3. Select “**Subnet**” for Tunnel access from local IP addresses.

4. Enter the network address for the “IP address for VPN” field. (If your IP is X.X.X.X the network address is usually X.X.X.0 for class C addresses)

5. Enter the local subnet mask in the field.

6. Select “**Subnet**” for Tunnel access from local IP addresses.

7. Enter the network address for the “**IP address for VPN**” field. (Note: *you can not have the same network address for both local and remote networks*.)

8. Enter the remote subnet mask in the next field.

9. Set the **Key Exchange Method** to “**Auto(IKE)**”

10. Select “**Pre-Shared Key**” for authentication method.

11. Enter a key for the “**Pre-Shared Key**” field.

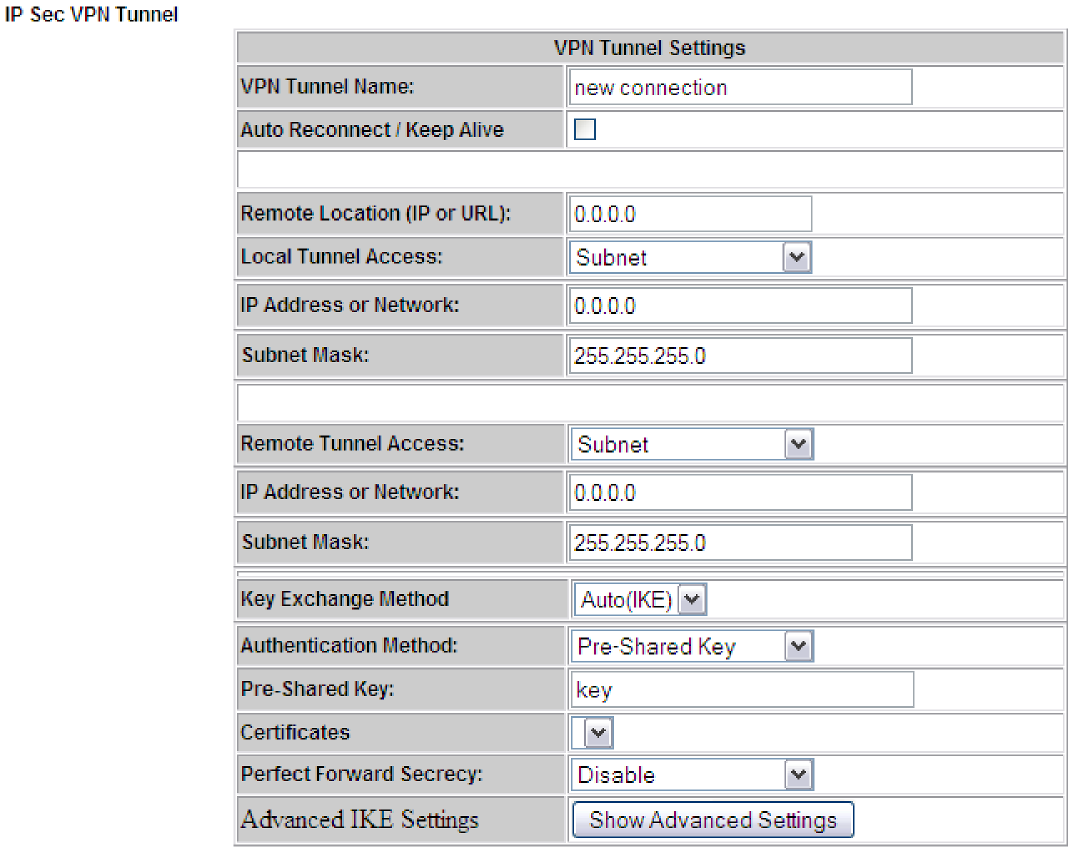
12. Select Disable for “**Perfect Forwarded Security**”

13. Click “**Save/Apply**” to save this connection.

14. Click the **Enable** check box to activate this connection.

15. Configure the remote IPSec gateway in the same manner. However, the local ip parameters will be remote ip parameters.

16. Once established, you can connect to clients in the remote network using their local IPs.



IP Sec VPN Tunnel

VPN Tunnel Settings	
VPN Tunnel Name:	new connection
Auto Reconnect / Keep Alive	□
Remote Location (IP or URL):	0.0.0.0
Local Tunnel Access:	Subnet
IP Address or Network:	0.0.0.0
Subnet Mask:	255.255.255.0
Remote Tunnel Access:	Subnet
IP Address or Network:	0.0.0.0
Subnet Mask:	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method:	Pre-Shared Key
Pre-Shared Key:	key
Certificates	
Perfect Forward Secrecy:	Disable
Advanced IKE Settings	Show Advanced Settings

10. System Diagnostic

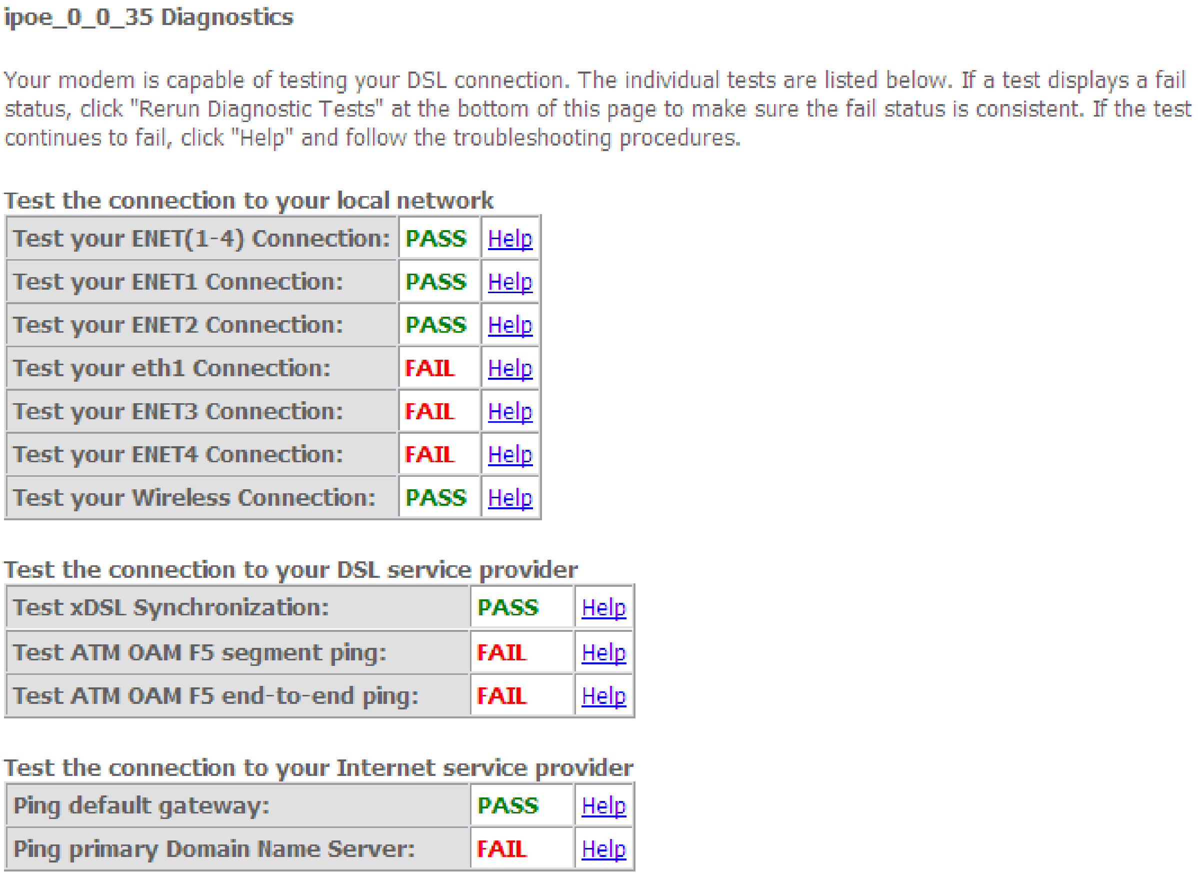
The System Diagnostic section allows the tools for troubleshooting purpose

- System Diagnostic
- Inbound Toolkit
- Outbound Toolkit

10.1 – System Diagnostic

The System Diagnostic function will run a test for Physical Port connectivity, DSL status, and Internet WAN connection status.

The test takes a few second to complete. Once it is completed the results will be shown in each category. In case of failure, rerun the test to ensure that the results are consistent. Click on the Help link next to the test categories to get more information for troubleshooting.



ipoe_0_0_35 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET(1-4) Connection:	PASS	Help
Test your ENET1 Connection:	PASS	Help
Test your ENET2 Connection:	PASS	Help
Test your eth1 Connection:	FAIL	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

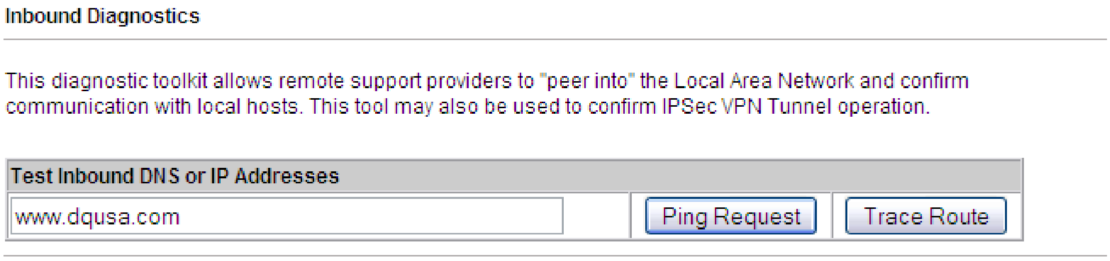
Test xDSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

Test the connection to your Internet service provider

Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	FAIL	Help

10.2 – Inbound Toolkit

This function allows you to ping device locally in your network. Type in the URL or IP address of the device you would like to ping. If there is a Ping reply, that verify that the connection is up and not block.



Inbound Diagnostics

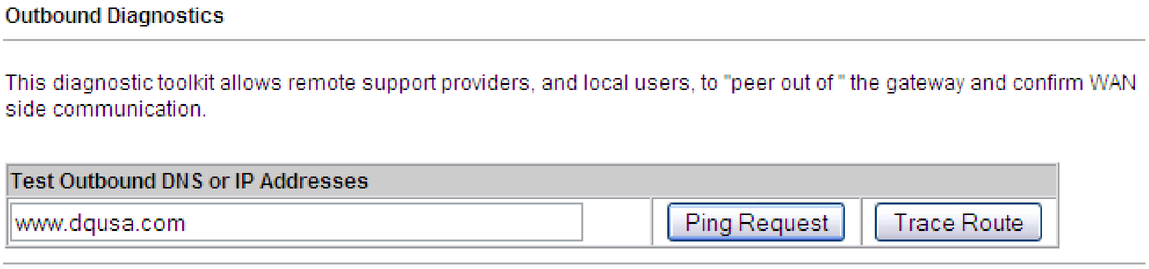
This diagnostic toolkit allows remote support providers to "peer into" the Local Area Network and confirm communication with local hosts. This tool may also be used to confirm IPSec VPN Tunnel operation.

Test Inbound DNS or IP Addresses

www.dqusa.com

10.3 – Outbound Toolkit

This function allows you to ping devices on the WAN side. Type in the URL or IP address of the device you would like to ping. If there is a Ping reply, that verify that the connection is up and not block.



Outbound Diagnostics

This diagnostic toolkit allows remote support providers, and local users, to "peer out of " the gateway and confirm WAN side communication.

Test Outbound DNS or IP Addresses

www.dqusa.com

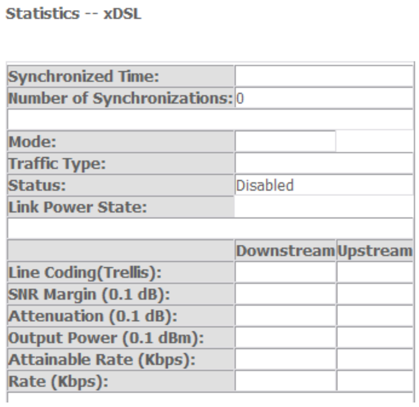
11. Gateway Statistics

The Gateway Statistics section allows viewing of the following category statistics:

- xDSL
- ATM
- WAN
- LAN
- Host
- Route Table
- DHCP

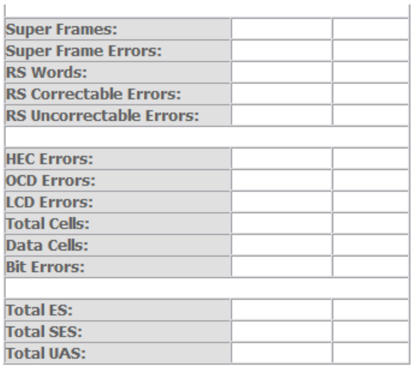
11.1 – xDSL

This will display all DSL statistics of the modem.



Statistics -- xDSL

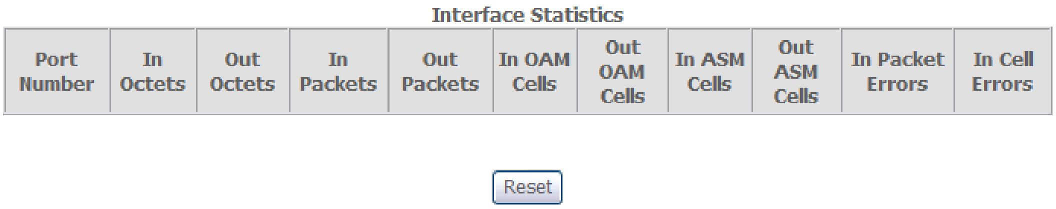
Synchronized Time:		
Number of Synchronizations:	0	
Mode:		
Traffic Type:		
Status:	Disabled	
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		



Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

11.2 – ATM

This will display ATM statistics of the current active WAN connection:



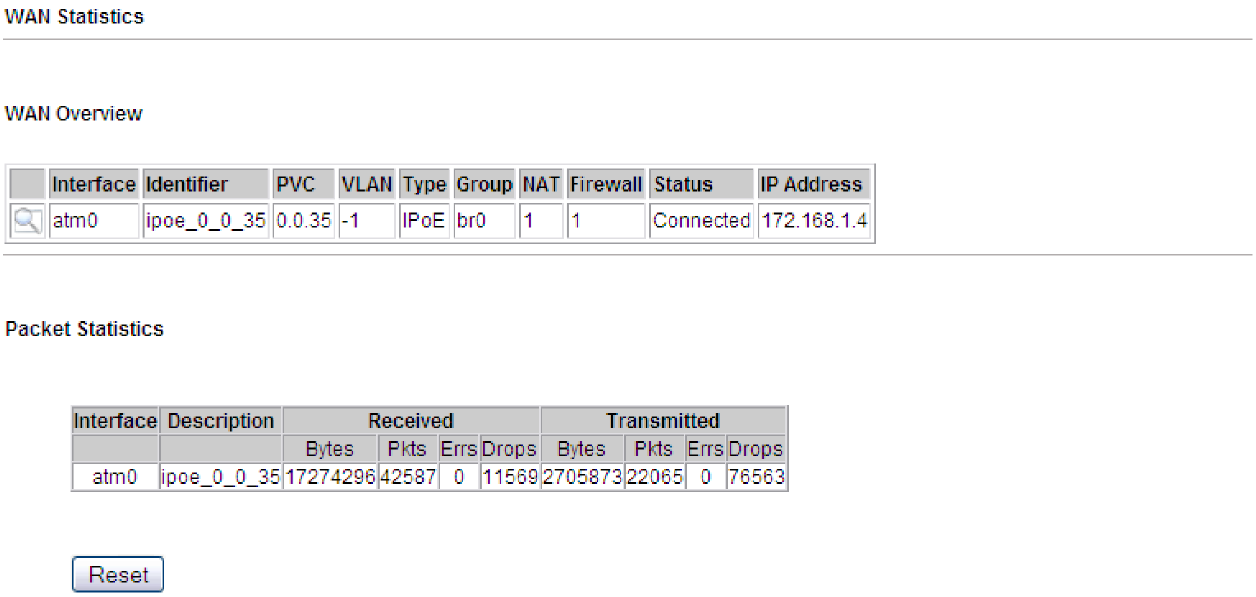
Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors

11.3 – WAN Statistics

The WAN Statistics page is broken into 2 parts:

1. WAN Overview – Information concerning the WAN protocol currently in used by the M504 to connect to the Internet. In the figure below: The modem is currently in IPoE mode, IGMP option is disabled, PVC 0/35, the connection is Up and the WAN IP address that the modem receives from the Internet Service Provider Equipment.
2. Packet Statistics –Information concerning Packets Received and Transmitted on the WAN side based on the Protocol used by the M504 (example shows IPoE connection).



WAN Statistics

WAN Overview

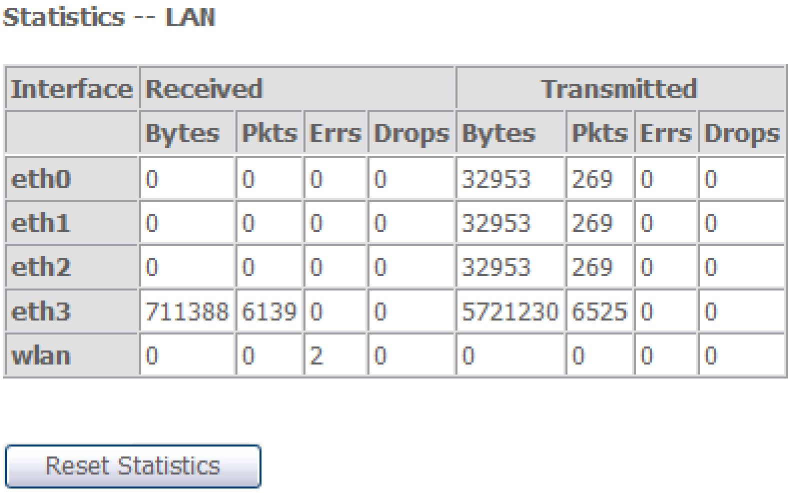
	Interface	Identifier	PVC	VLAN	Type	Group	NAT	Firewall	Status	IP Address
🔍	atm0	ipoe_0_0_35	0.0.35	-1	IPoE	br0	1	1	Connected	172.168.1.4

Packet Statistics

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0	ipoe_0_0_35	17274296	42587	0	11569	2705873	22065	0	76563

11.4 – LAN

This will display all LAN statistics of the M504:

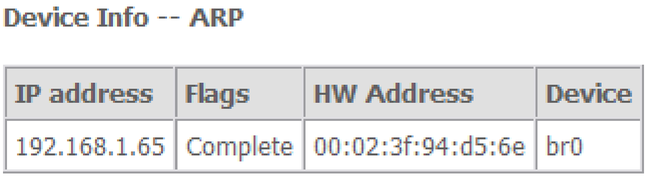


Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	32953	269	0	0
eth1	0	0	0	0	32953	269	0	0
eth2	0	0	0	0	32953	269	0	0
eth3	711388	6139	0	0	5721230	6525	0	0
wlan	0	0	2	0	0	0	0	0

11.5 – Host

This will display all Host/ARP statistics of the M504:

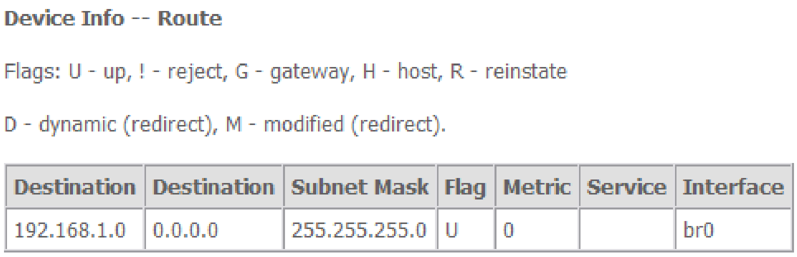


Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.65	Complete	00:02:3f:94:d5:6e	br0

11.6 – Route table

This will display all current Route table of the M504:



Device Info -- Route

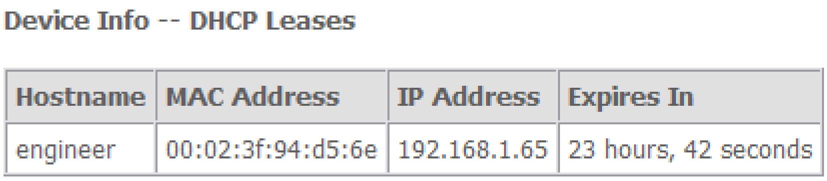
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate

D - dynamic (redirect), M - modified (redirect).

Destination	Destination	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

11.7 – DHCP

This will display all DHCP Clients connected to the M504



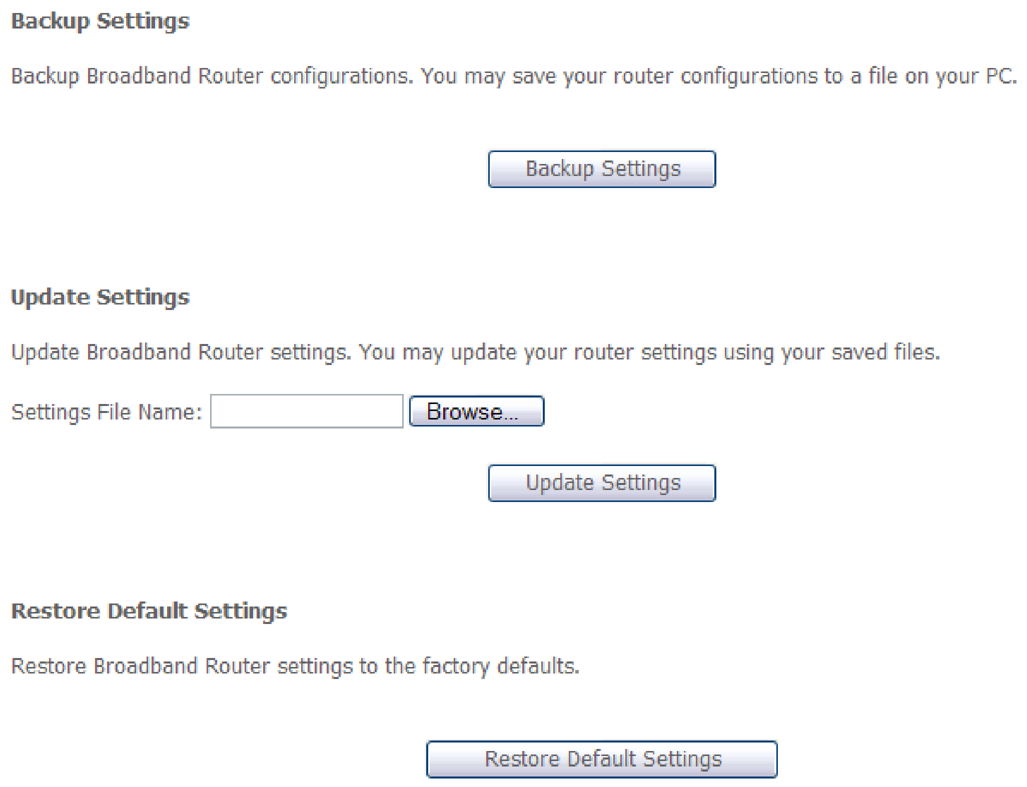
Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
engineer	00:02:3f:94:d5:6e	192.168.1.65	23 hours, 42 seconds

12. Management

12.1 – Settings

This page allows backup the current configuration, restore the modems from a configuration file or restore the modem to its default configuration.



Backup Settings

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

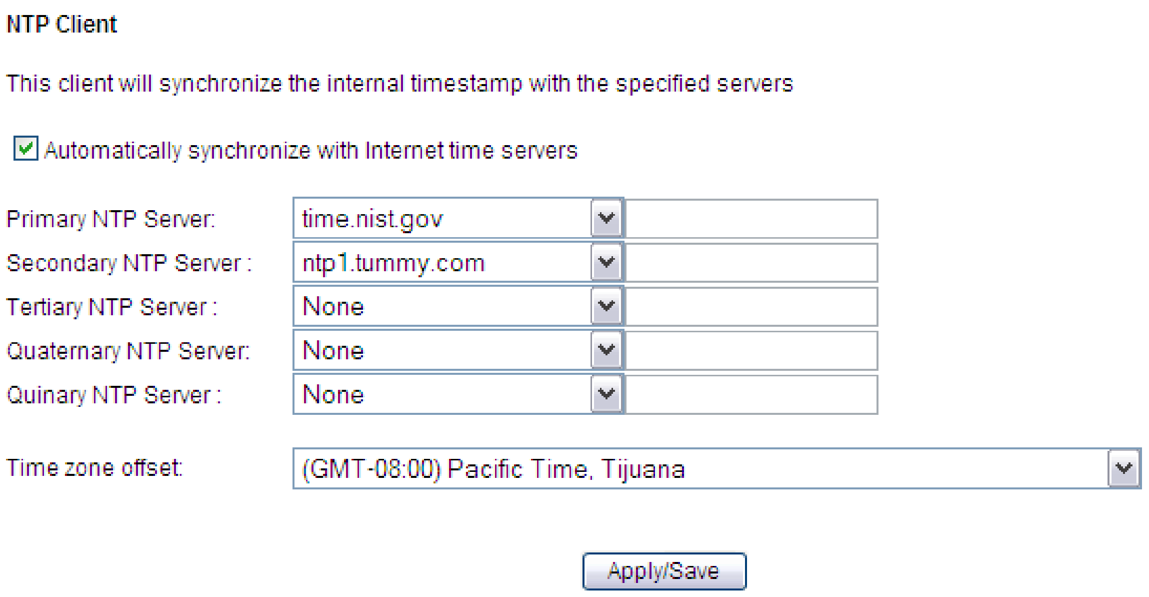
Restore Default Settings

Restore Broadband Router settings to the factory defaults.

If you wish to erase the running the configuration from the gateway and revert back to the modem default settings: click on the “Restore Default Settings”.

12.2 – NTP Client

This option allows you to configure the NTP (Network Time Protocol) of the Gateway.



NTP Client

This client will synchronize the internal timestamp with the specified servers

☑ Automatically synchronize with Internet time servers

Primary NTP Server:	time.nist.gov
Secondary NTP Server :	ntp1.tummy.com
Tertiary NTP Server :	None
Quaternary NTP Server:	None
Quinary NTP Server :	None
Time zone offset:	(GMT-08:00) Pacific Time, Tijuana

Select the Check box "Automatically synchronize with Internet time server" box.

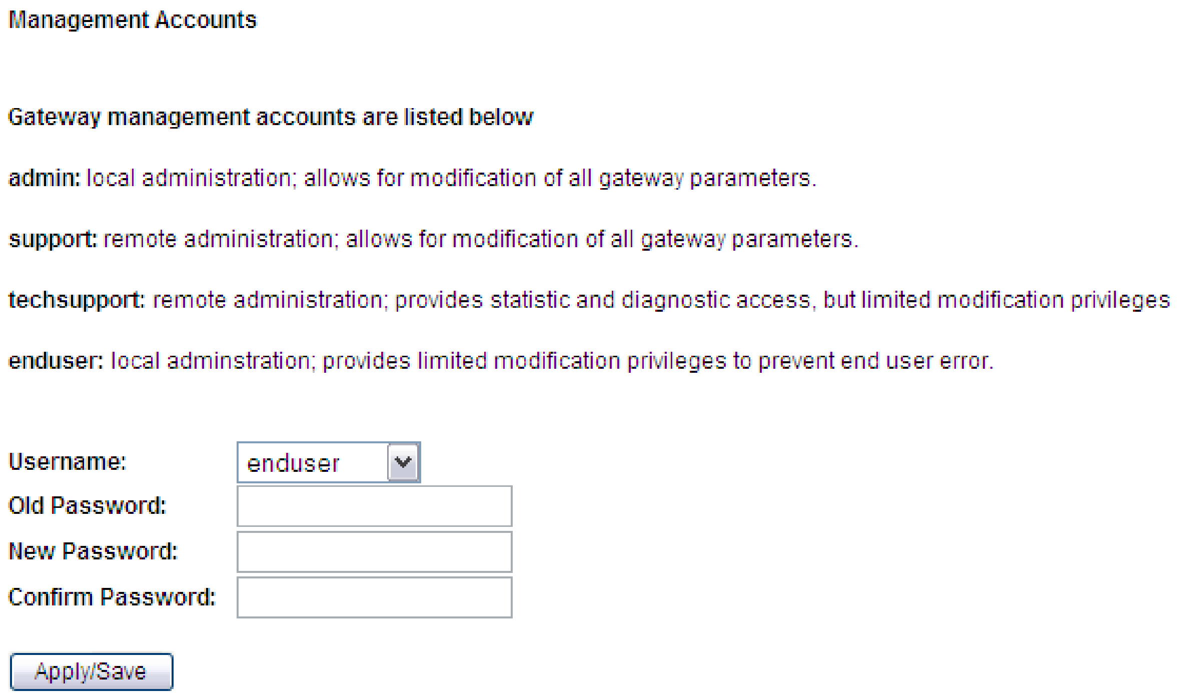
Choose the NTP Server from the dropdown list

Finally, select the Timezone from the dropdown list.

Click the "Apply/Save" button for apply this function.

12.3 – Management Account

This page allows you to modify the log-in password to the management interface of the gateway.



Management Accounts

Gateway management accounts are listed below

admin: local administration; allows for modification of all gateway parameters.

support: remote administration; allows for modification of all gateway parameters.

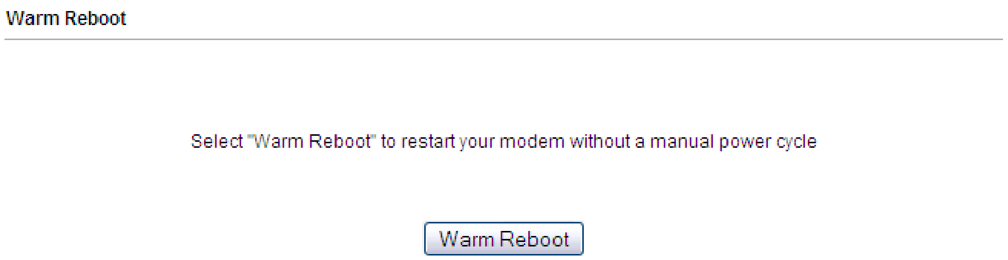
techsupport: remote administration; provides statistic and diagnostic access, but limited modification privileges

enduser: local adminstration; provides limited modification privileges to prevent end user error.

Username:	enduser
Old Password:	
New Password:	
Confirm Password:	

12.4 – Warm Reboot

Click “Warm Reboot” button to reboot M504.



Warm Reboot

Select "Warm Reboot" to restart your modem without a manual power cycle

13. Appendix A – Specifications

A1. Hardware Specifications

- Local Interface
  - Four 10/100BaseT Ethernet port (IEEE 802.3, RJ-45 connector)
  - USB 2.0 Type A Interface
- WAN ADSL Line Interface
  - Complies with G.dmt (G.992.1) Annex A
  - Complies with G.lite (G.992.2) and T1.413
  - Complies with ADSL2 (G.992.3)
  - Complies with ADSL2+ (G.992.5)
  - Connector: RJ-11
- OAM&P
  - Remote: Telnet, SSH or Web browser
- Environment
  - Operation Temperature: 0°C ~ 40°C
  - Operation Humidity: 10% ~ 95%
  - Storage Temperature: -20 ~ 70°C
  - Storage Humidity: 5%~95%
- Power
  - AC Adapter :Input 100-240V AC50/60Hz; Output 12VDC 1A
- Certificates
  - FCC Part 68 and 15 Class B, UL

A2. Software Specifications

- ATM
  - ATM Cell over ADSL, AAL5
  - Supports UBR, CBR & VBR-nrt
  - VPI Range (0-255) and VCI range (1-65535)
  - Supports up to 8 PVCs
  - Supports OAM F4/F5, and loop back cells
  - Payload Encapsulation --
    - RFC2684 (RFC1483), multi-protocol over ATM
    - RFC2364, PPP over ATM (CHAP and PAP supported)
    - RFC2516, PPPoE (PPP over Ethernet) over ATM
- Bridging
  - Transparent Bridging (IEEE 802.1D)
  - RFC2684 (RFC1483) Bridged
  - Spanning Tree Protocol (IEEE 802.1D)
  - Bridge Filtering
- Routing
  - IP Address Forwarding
  - MAC Encapsulated Routing
  - Routing Information Protocol (RIP) v1, v2
  - DHCP Client (to the DSL network)
  - DHCP relay agent
  - NAT/PAT – RFC1631 (basic Firewall support)
  - Support Point-to-Point Protocol (PPP)
  - PAP for user authentication
  - RFC2684 (RFC1483) Routed

- DNS relay
- UPnP
- IGMP-Proxy

■ Configuration and Network Management

- DHCP server for IP management
- HTTP (Web Server) for configuration and firmware upgrade
- TFTP Server
- FTP Server

■ Firewall

- NAT ALG
- IPSEC pass-through
- Ping of Death
- SYN Flood LAND
- Protection against IP and MAC address spoofing
- Packet Filtering
- Stateful Packet Inspection (SPI)
- UPnP NAT Traversal

14. Appendix B – Warranties

DQ Technology adheres to the strictest Quality Assurance processes to ensure that our products are free from defects prior to shipping. DQ Technology provides a standard 1 year limited warranty for all products and provides an extended warranty option for North American customers.

Please note that standard warranty terms apply to all equipment sold by DQ Technology unless an extended warranty has been purchased.

The 1 year limited warranty offered by DQ Technology Inc. is non-transferrable. End Users who purchased equipment from a Service Provider, or other source, should contact the company from whom they purchased the equipment for all warranty and returns.

This warranty is not transferable and does not include service, repair, or replacement to correct any damage caused by improper installation or maintenance, improper connection with any peripheral, external electrical fault, accident, disaster, misuse, abuse, or modifications to the DSL modem not approved in writing by DQ Technology. All implied warranties are hereby limited to a One (1) year term. DQ Technology hereby disclaims all express warranties not included in these terms.

DQ Technology warrants that all products are free from defective material and workmanship and, subject to the conditions set forth below, agrees to repair or replace any part of a product, which proves defective by reason of improper workmanship or materials without charge for parts and labor.

If a Product does not perform as warranted herein, owner's sole remedy shall be repair or replacement as provided below. In no event will DQ Technology be liable for damages, lost revenue, lost wages, lost savings, or any other incidental or consequential damages arising from purchase, use, or inability to use this product, even if DQ Technology has been advised of the possibility of such damages. Any defective Product should be returned to the address above unless otherwise instructed by this notice, along with a copy of your sales slip, the product serial number (if applicable), and a detailed description of the problem(s) you are experiencing.

No express or implied warranty is made for DQ Technology Products damaged by accident of use, misuse, natural or personal disaster or any unauthorized disassembly, repair or modification.

DQ Technology's Warranty covers only repair or replacement of defective Products

DQ Technology is not liable for, and does not cover under Warranty, any costs associated with servicing or installation of Products.

If you experience any difficulty during installation or subsequent use of Products, please contact Technical Support at 1-866-286-XDSL or email rma@dqusa.com.

DQ Technology warrants that all solid-state memory products are free from defect in material and workmanship. Subject to the conditions and limitations set forth below, DQ Technology will repair or replace any part of a Product that proves defective by reason of improper workmanship or materials.

Repair parts or replacement Products will be furnished on an exchange basis and will be either new or refurbished to be functionally equivalent to new.

15. Appendix C – Regulations

C1. FCC Part 68 Statement

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the back of this equipment is a label that contains, among other information, a product identifier in the format
US: DQ1DL01BM504. If requested, this number must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: DQ1DL01BM504. The digits represented by 01 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Company: DQ Technology, Inc.

Address: 5111 Johnson Drive, Pleasanton, CA, 94588

Tel no.: +1 925 730 3940

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

C2. FCC Part 15 Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

CAUTION:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

C3. UL Safety Regulations

- Disconnect TNV circuit connector or before removing cover or equivalent.
- Disconnect TNV circuit connector(s) before disconnecting power.
- Do not use this product near water for example, near a bathtub, washbowl, and kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord batteries indicated in this manual. Do not dispose of batteries in a fire, as they may explode. Check with local codes for possible special disposal instructions.

No. 26 AWG Telephone Line Cord shall either be provided with the equipment or shall be described in the safety instruction. If fuse (F1) is not present, see the caution statement listed below:

C4. IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Contact Information

You can help us to serve you better by sending us your comments and feedback. Listed below are the addresses, and telephone and fax numbers of our offices. You can also visit us on the World Wide Web at www.dqusa.com for more information. We look forward to hearing from you!

World Headquarters
5111 Johnson Dr.
Pleasanton, CA 94588
Tel: (925) 730-3940 Fax: (925) 730-3950
info@dqusa.com

Technical Support
(866) 286-xDSL (9375)
support@dqusa.com